Provable Security Workshop 2018

(in conjunction with the 12th International Conference on Provable Security)

25th October 2018
Jeju Island, Republic of Korea

Organized by

UNIVERSITY OF WOLLONGONG AUSTRALIA

SCH 순천향대학교 SOON CHUN HYANG UNIVERSITY SCHOOL OF GLOBAL EDUCATION AND EXCHANGE

Associated with

제주대학교 JEJU NATIONAL UNIVERSITY

Contents

ProvSec Workshop 2018 is also in association with

- KIISC Research Group on 5G Security
- Innovative Information Science & Technology Research Group, Korea

I. Welcome to ProvSec 2018

ProvSec 2018 is organized by the Institute of Cybersecurity and Cryptology at the University of Wollongong and the Laboratory of Mobile Internet Security at Soonchunhyang University.

The first ProvSec conference was started in Wollongong, Australia in 2007. The series of ProvSec conferences were then held successfully in Shanghai, China (2008), Guangzhou, China (2009), Malacca, Malaysia (2010), Xian, China (2011), Chengdu, China (2012), Malacca, Malaysia (2013) , Hong Kong, China (2014), Kanazawa Japan (2015), Nanjing, China (2016) and Xian, China (2017). This was the first ProvSec held in Korea. This year we received 48 submissions of high quality from 19 countries.

Among the accepted regular papers, the paper that received the highest weighted review mark was given the Best Paper Award: *"Security Notions for Cloud Storage and Deduplication"* by Colin Boyd, Gareth T. Davies, Kristian Gjøsteen, Håvard Raddum and Mohsen Toorani.

The program also included an invited talk presented by Prof. Jung Hee Cheon from Seoul National University, Korea, titled *"Recent Development of Homomorphic Encryptions and Their Applications".*

ProvSec Workshop 2018 is jointly held with the conference. Twelve selected papers will be presented during the workshop.

We deeply thank all the authors of the submitted papers. We also greatly appreciate time and effort that the Program Committee members and external reviewers put to evaluate and select the papers for the program. Our gratitude extends to our sponsors - Jeju National University, Korea and Innovation Information Science and Technology Research Group, Korea. We are also grateful to the team at Springer for their continuous support of the conference and for their assistance in the production of the conference proceedings.

October 2018

Ilsun You
Kyung Hyune Rhee
Joonsang Baek
Willy Susilo

II. ProvSec 2018 Conference/Workshop Organization

General Chairs

Ilsun You	Soonchunhyang University, Korea
Kyung Hyune Rhee	Pukyung National University, Korea

Program Chairs

Joonsang Baek	University of Wollongong, Australia
Willy Susilo	University of Wollongong, Australia

Publication Chair

Jongkil Kim	University of Wollongong, Australia

Organization Chair

Namje Park	Jeju National University, Korea

Program Committee

Elena Andreeva	K.U. Leuven, Belgium
Man Ho Au	The Hong Kong Polytechnic University, Hong Kong
Donghoon Chang	IIIT-Delhi, India
Jie Chen	East China Normal University, China
Liqun Chen	University of Surrey, UK
Xiaofeng Chen	Xidian University, China
Cheng-Kang Chu	Huawei, Singapore
Bernardo David The	Tokyo Institute of Technology, Japan
Jean Paul Degabriele	TU Darmstadt, Germany
Robert Deng	Singapore Management University, Singapore
Keita Emura	NICT, Japan
Zekeriya Erkin	TU Delft, Netherlands
Jinguang Han	University of Surrey, UK
Ryo Kikuchi	NTT, Japan
Jongkil Kim	University of Wollongong, Australia
Hyung Tae Lee	Chonbuk National University, Korea
Jooyoung Lee	KAIST, Korea
Joseph Liu	Monash University, Australia
Bernardo Magri	Friedrich-Alexander-University, Germany
Barbara Masucci	University of Salerno, Italy
Bart Mennink Radboud	University, Netherlands
Chris Mitchell	Royal Holloway, University of London, UK
Kirill Morozov	University of North Texas, USA
Khoa Nguyen	Nanyang Technological University, Singapore

Abderrahmane Nitaj	Université de Caen Normandie, France
Josef Pieprzyk	CSIRO/Data61, Australia
Kouichi Sakurai	Kyushu University, Japan
Rainer Steinwandt Florida	Atlantic University, USA
Chunhua Su	Osaka University, Japan
Katsuyuki Takashima	Mitsubishi Electric, Japan
Atsushi Takayasu The	University of Tokyo, Japan
Qiang Tang	New Jersey Institute of Technology, USA
Joseph Tonien	University of Wollongong, Australia
Damien Vergnaud	ENS, France
Shota Yamada	AIST, Japan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Guomin Yang	University of Wollongong, Australia
Xun Yi	RMIT University, Australia
Yong Yu	Shaanxi Normal University, China
Tsz Hon Yuen	The University of Hong Kong, Hong Kong
Aaram Yun	UNIST, Korea

Workshop Organization

Program Co-Chairs

Jongkil Kim	University of Wollongong, Austraila
Joonsang Baek	University of Wollongong, Austraila

Program Committee

Taekyong Kwon	Yonsei University, South Korea
Jong-Hyouk Lee	Sangmyung University, South Korea
Nan Li	University of Newcastle, Australia
Deepak Puthal	University of Technology Sydney, Australia
Vishal Sharma	Soonchunhyang University, South Korea
Pairat Thorncharoensri	University of Wollongong, Australia
Ilsun You	Soonchunhyang University, South Korea

III. List of Papers

1. A Study of Distributed Mobility Management for 5G Networks
   Soohyun Kwon (Soonchunhyang University), Jiyoon Kim (Soonchunhyang University), Takshi Gupta (Soonchunhyang University) and Ilsun You (Soonchunhyang University)
2. A Framework for Cloud IVS Management through FedRAMP Analysis
   Jiyeon Kim (Jeju National University) and Namje Park (Jeju National University)
3. Intelligent Information Technology-based ICT Education and Creativity Education Develop Core Competencies
   Yujin Jung (Jeju National University), Namje Park (Jeju National University) and Heuipil Kim (Jeju National University)
4. The Rigidity of Rectangular Frameworks
   Keunbae Choi(Jeju Naltional University) and Namje Park (Jeju National University)
5. Strong Designated Verifier Signcryption Scheme
   Neetu Sharma (PRS University), Rajeev Anand Sahu (Universite Libre de Bruxelles), Vishal Saraswat (IIT Jammu), Gaurav Sharma (Universite Libre de Bruxelles), Veronika Kuchta (Monash University), Olivier Markowitch (Universite Libre de Bruxelles)
6. Securely outsourcing machine learning with multiple users
   Ping Li (Guangzhou University), Hongyang Yan (Nankai University), Chong-Zhi Gao (Guangzhou University), Yu Wang (Guangzhou University), Liaoliang Jiang (Guangzhou University) and Yuefang Huang (Guangzhou University)
7. Lattice-Based Simulatable VRFs: Challenges and Future Directions
   Carlo Brunetta (Chalmers University of Technology), Bei Liang (Chalmers University of Technology) and Aikaterini Mitrokotsa (Chalmers University of Technology)
8. An SDN-based Secure Mobility Model for UAV-Ground Communications
   Rajesh Kumar (TIET), Mohd. Abuzar Sayeed (TIET), Vishal Sharma (Soonchunhyang University), Ilsun You (Soonchunhyang University)
9. Expressive Ciphertext-Policy Attribute-Based Encryption with Fast Decryption
   Hikaru Tsuchida (NEC Corporation), Takashi Nishide (University of Tsukuba) and Eiji Okamoto (University of Tsukuba)
10. Achieving Strong Security and Member Registration for Lattice-based Group Signature Scheme with Verifier-local Revocation
    Maharage Nisansala Sevwandi Perera (Saitama University) and Takeshi Koshiba (Waseda University)
11. A Type-based Formal Specification for Cryptographic Protocols
    Paventhan Vivekanandan (Indiana University Bloomington)
12. A Novel Non-Interactive Multi-party Key Exchange from Homomorphic Encryption
    Rakyong Choi (KAIST) and Kwangjo Kim (KAIST)

A Study of Distributed Mobility Management for 5G Networks

Soonhyun Kwon[1], Jiyoon Kim[1], Takshi Gupta[1], Ilsun You[1*]

[1]Department of Information Security Engineering, Soonchunhyang University,

Asan-si – 31538, The Republic of Korea

tnsgus08@gmail.com, 74jykim@gmail.com,

takshi_gupta2012@hotmail.com, ilsunu@gmail.com

Abstract. In order to meet the requisites of the high-speed network, astronomically immense-capacity mobile traffic, and sizably voluminous-scale contrivance connection, 3GPP is working on standardization and technology development for the next generation of wireless networks. Currently, 3GPP adopts Proxy Mobile Internet Protocol Version – 6 (PMIPv6) as a standard technology for Evolved Packet Core (EPC) which is a 4th generation mobile communication technology, but since it has a centralized structure, it is arduous to apply to 5G, which requires handling of a substantial amount of data traffic. Predominantly, the Internet Engineering Task Force (IETF) is working on the standardization of Distributed Mobility Management (DMM) technology by engendering a working group to assure the mobility of mobile contrivances for efficient distribution of the data. Considering that the network environment changes to different standards, it is much required to present a study on DMM considering configurations of 5G networks. Consequently, this paper discusses subsisting as well as possible variations of DMM architecture for 5G networks.

1. Introduction

Due to the rapid development of mobile communication and mobile Internet, users are able to exchange data through smart phones anytime and anywhere as all the objects are connected to the network. According to statistics of the Ministry of Science and Technology, as of March 2018, the mobile traffic amounted to about 7047.5TB and the number of Long-Term Evolution (LTE) subscribers reached about 5,166,000 confirming that the number of mobile devices and mobile traffic increased rapidly in recent years [1] The 3rd Generation Partnership Project (3GPP) [2][3], which is a mobile communication standardization group, adopts Proxy Mobile Internet Protocol Version – 6 (PMIPv6) [4] [5] as a standard technology for Evolved Packet Core (EPC), which is a 4th generation mobile communication technology. But PMIPv6 is a centralized structure and is not capable enough to handle explosive data traffic [6] [7].

For this reason, the Internet Engineering Task Force (IETF) is working on the standardization of Distributed Mobility Management (DMM) technology that disseminates mobile device data effectively and efficiently [8]. In addi-

tion, standardization and technology development for the next generation networks, i.e., 5G, is underway in the current 3GPP, and as the network environment changes to 5G, distribution of data planes and management of control planes become important requirements. In particular, Lee et al. [9] [10] proposed the DMM scheme that satisfies these corresponding requirements. However, there is a limited study in this direction. Therefore, this paper analyzes the basic structure of 5G and analyzes and proposes variants for 5G DMM architecture based on the techniques proposed by Lee et al. [9].

2. Preliminaries and Related Works

This section describes the basic structure of the 5G network and existing research for DMM and describes the DMM architecture proposed by Lee et al [9]. The standard terminology of 5G and terms used throughout this paper are given in Table 1.

Table 1. The details of terms used in this article.

Terms	Meaning
MN	Mobile Node
CN	Corresponding Node
MAAR	Mobility Anchor and Access Router
MCDB	Mobility Context Database
ABU	Access Binding Update
ABA	Access Binding Acknowledgement
MCReq	Mobility Context Request
MCRes	Mobility Context Response
RA	Router Acknowledgement
SMF	Session Management Function
AMF	Access Management Function
UPF	User Plane Function

AUSF	Authentication Server Function
ARPF	Authentication Credential Repository and Processing Function

2.1 5G Network

5G is a next-generation network defined under standard processing in 3GPP to solve problems such as mobile devices and traffic increase. Considering the existing problems of wireless networks, the basic performance indicators defined for the 5G are shown in Table 2 [6].

Table 2. Major performance indicators for 5G networks.

Main performance	Characteristic
The perceived transmission rate	100Mbps – 1Gbps
Maximum transfer rate	10Gbps – 50Gbps
Speed	Up to 500Km/h
Transmission delay	~ 1ms (radio interface)
Connected device density	10^6– 10^7 per Km^2
Energy efficiency	50 to 100 times more efficient than IMT-A
Frequency efficiency	5 to 15 times more efficient than IMT-A
Capacity per area	1TB – 10TB/s/Km^2 *

The existing EPC comprises entities such as Mobility Management Entity (MME), Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW). However, in the 5G core network, the entire network is defined through specialized network function, as shown in Figure 1.

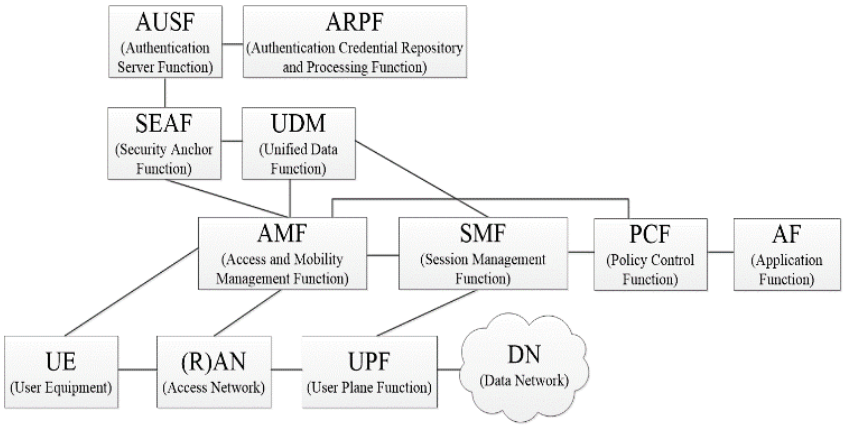


Figure 1. Core architecture and functional modules of 5G networks[1].

In the existing 4G network, the S-GW and the P-GW play roles of MN anchor, mobility management, and session management, and the MME and the HSS perform the role of mobility management state storage and authentication. In the 5G network, AMF, SMF, and UPF perform functions such as access management, mobility management, session management, billing, and data processing. In addition, SEAF, AUSF, and ARPF are responsible for the MN's authentication and mobility management status.

2.2 Lee et al.'s DMM architecture

Lee et al [9]. proposed network-based DMM scheme, which is implemented by distributing data through the tunneling of anchors accessed by the MN during handover. This makes data processing much more efficient than traditional PMIPv6, where data is centrally processed. Since the control plane is managed separately through the MCDB that manages the MN's mobility context, the anchor does not have any burden on the control data. Figure 2 shows the network-based DMM as proposed by Lee et al [9].

[1]https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.01.00_60/ts_133501v150100p.pdf

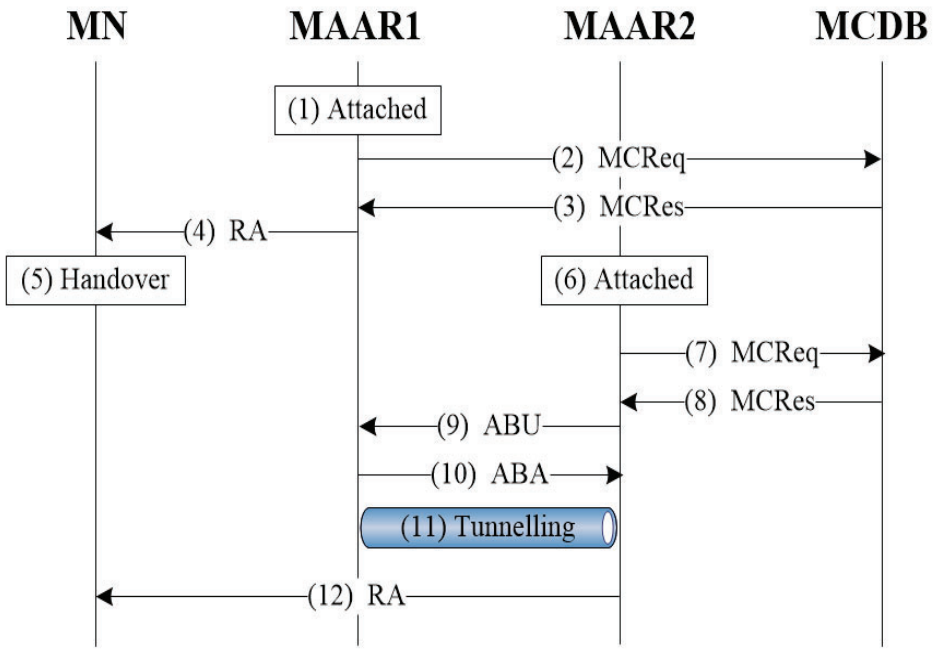
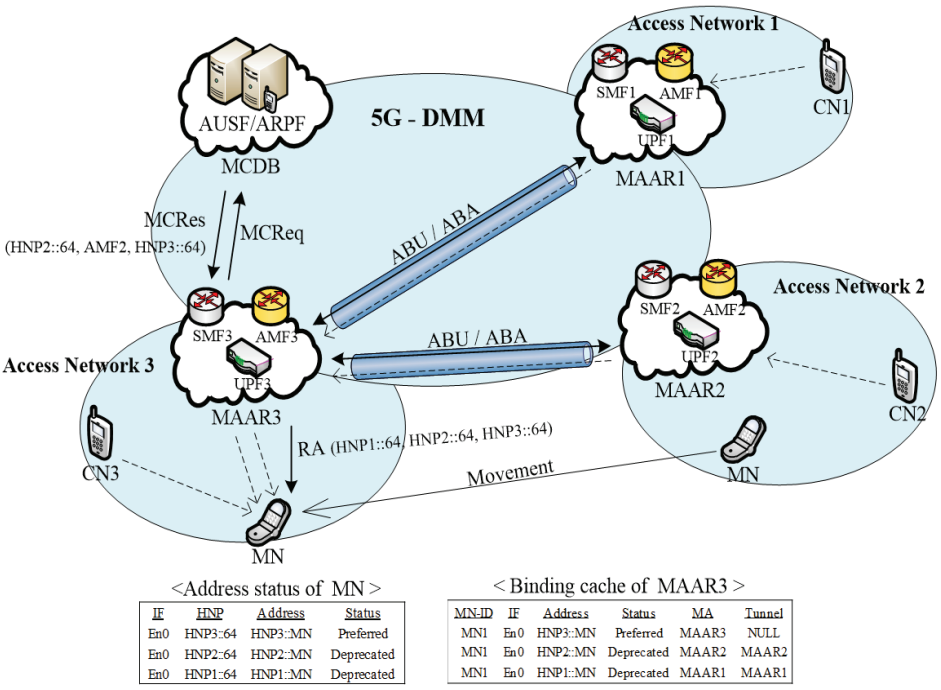


Figure 2. Network-based DMM by Lee et al [9].

In this scheme, the handover of the MN is detected by MAAR, which is an Access Router (AR), and MAAR receives the MN's mobility information from the MCDB, thereby acquiring the MN's previous MAAR. Thereafter, tunneling is performed through the binding process with the previous MAAR, and data is forwarded through the formed tunnel.

3. Proposed Approach: A variant of DMM for 5G networks

In this section, DMM architecture for the 5G network is proposed and analyzed with its components. The separation of the data plane and control plane is also analyzed in this section of the paper. An exemplary overview of the proposed 5G-DMM architecture is shown in Figure 3.



<Address status of MN >

IF	HNP	Address	Status
En0	HNP3::64	HNP3::MN	Preferred
En0	HNP2::64	HNP2::MN	Deprecated
En0	HNP1::64	HNP1::MN	Deprecated

< Binding cache of MAAR3 >

MN-ID	IF	Address	Status	MA	Tunnel
MN1	En0	HNP3::MN	Preferred	MAAR3	NULL
MN1	En0	HNP2::MN	Deprecated	MAAR2	MAAR2
MN1	En0	HNP1::MN	Deprecated	MAAR1	MAAR1

Figure 3. An overview of the proposed variant of DMM architecture for 5G networks.

3.1 5 G-DMM structures and component analysis

In the existing DMM scheme, MAAR acts as an anchor of MN's access network, but in 5G, the role of MAAR is subdivided so that three entities can be composed of one MAAR, which are

- AMF: It manages the registration, access and mobility of the MN and delivers a session management message between the MN and the SMF.
- SMF: It manages the session and IP of the MN, and charges the data generated in the UPF.
- UPF: It is responsible for processing User Plane Data.

The MAAR, which is composed of the above entities, requests the Mobility Context of the MN to the MCDB when it detects the MN's handover. The Mobility Context contains MN's previous network prefix, the previous MAAR’s information, and the current network’s prefix. The MCDB itself comprises two entities, namely,

- AUSF: It serves as a proxy or authentication server to deliver MN's mobility and authentication information.
- ARPF: It has MN's mobility information and authentication information and acts as a certification server.

Based on the Mobility Context received, the new MAAR performs tunneling with the previous MAAR in all access networks that MNs have visited previously. After that, the binding cache function updates the status of visited MAARs of the MN to Deprecated/Disable and updates itself to the active state.

3.2 Control Plane

The access and control data of 5G-DMM is managed by AMF and SMF among the entities constituting MAAR, and the mobility information and authentication information of MN are managed by AUSF and ARPF constituting MCDB. When the AMF detects the handover of the MN, it requests the MN's mobility information from the MCDB and informs the SMF of the received information. The AMF then performs tunneling with the MN's previous MAARs and informs the SMF of the tunnel negotiation information. The SMF informs the UPF of the information it has received from the AMF. At this time, the UPF knows the information of the previous UPFs that the MN has visited. In the 5G-DMM, the AMF only processes data such as the MN's mobility information request and connection with the previous network, and the SMF can manage the control plane more effectively by processing the MN's IP settings and data with the UPF.

3.3 Data Plane

The data plane of the 5G-DMM is managed by the UPF that constitutes the MAAR. As illustrated in Figure 3, the data sent to MN can be sent via the UPF of the network that MN visited earlier to the current UPF on the network they are accessing. The UPF knows the information of the previous UPFs through the information received from the SMF, and it requests forwarding the data transmitted to the previous address of the MN to the current address through the tunnel with the previous MAARs formed through AMF. The forwarded User Plane data is managed and processed by the UPF, and the UPF does not perform the processing on the mobility information, thereby reducing the burden on the excessively generated data.

4. Conclusion and Future Research

In this paper, Distributed Mobility Management (DMM) architecture felicitous for the 5G network environment was analyzed. Centralized mobility management is less efficient in performance because the centralized anchor participates in data forwarding and tunneling of the MN, which degrades the transmission rates as well as lowers the security. A DMM is required to manage mobile terminals as a substantial amount of traffic is expected to explode in the 5G environment. In the proposed 5G-DMM, the MAAR is subdivided into each function and the control plane and the data plane are individually processed, which is more efficacious in handling astronomically immense-scale data traffic. Future studies plan to design authentication and key exchange structures at the 5G DMM by studying its security by analysis of standard 5G authentications and security architecture. Such a study of 5G networks where security and reliability are the most paramount can avail in developing secure and efficient solutions for the management of contrivances with high and diverse mobility.

References

[1]. Korean ICT in the world, http://english.msit.go.kr/english/main/main.do, [Last Accessed on July 25, 2018].

[2]. Lee J, Kim Y, Kwak Y, Zhang J, Papasakellariou A, Novlan T, Sun C, Li Y. LTE-advanced in 3GPP Rel-13/14: an evolution toward 5G. IEEE Communications Magazine. 2016 Mar;54(3):36-42.

[3]. Chunbo WA, Nilsson D, Rommer S, inventors; Telefonaktiebolaget LM Ericsson AB, assignee. Method and nodes for handling access to epc services via a non-3gpp network. United States patent application US 15/572,981. 2018 May 24.

[4]. Guan J, Sharma V, You I, Atiquzzaman M. Extension of MIH to Support FPMIPv6 for Optimized Heterogeneous Handover. arXiv preprint arXiv:1705.09835. 2017 May 27.

[5]. Chiang MS, Huang CM, Dao DT, Pham BC. The Backward Fast Media Independent Handover for Proxy Mobile IPv6 Control Scheme (BFMIH-PMIPV6) over Heterogeneous Wireless Mobile Networks. JOURNAL OF INFORMATION SCIENCE AND ENGINEERING. 2018 May 1;34(3):765-80.

[6]. Hsu YC, Tzeng SS. A Pragmatic Design for 3GPP/WLAN RAN Level Interworking. Wireless Personal Communications. 2017 Sep 1;96(1):867-78.

[7]. Shin D, Sharma V, Kim J, Kwon S, You I. Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. IEEE Access. 2017;5:11100-17.

[8]. Sharma V, You I, Palmieri F, Jayakody DN, Li J. Secure and Energy-Efficient Handover in Fog Networks Using Blockchain-Based DMM. IEEE Communications Magazine. 2018 May;56(5):22-31.

[9]. Lee JH, Bonnin JM, Seite P, Chan HA. Distributed IP mobility management from the perspective of the IETF: motivations, requirements, approaches, comparison, and challenges. IEEE Wireless Communications. 2013 Oct;20(5):159-68.

[10]. Lee J. and Kim Y. Topology-Based Distributed Mobility Anchoring in Pmipv6, IETF draftjaehwoon- dmm-topology–mobility-anchoring-00, 2016; https://tools.ietf.org/html/draft-jaehwoon-dmm-topology– mobility-anchoring-00, [Last Accessed on July 25, 2018].

A Framework for Cloud IVS Management through FedRAMP Analysis

Jiyeon Kim[1,2] and Namje Park[2,3,†],

[1] Department Convergence Information Security, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
jykim1230@gmail.com, jykim07@swu.ac.kr

[2] Center for Creative Education, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea

[3] Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
namjepark@jejunu.ac.kr

Abstract. Intelligent Video Surveillance (IVS) is becoming a prevalent way of keeping public and private places safe. Cloud computing enables video surveillance systems to store video footage in the cloud and to find meaningful clues through intelligent analytics based on Big data. Despite the high demand for the cloud-based IVS systems, it is challenging for public agencies to manage the systems due to a lack of guidelines and standards. We propose a framework for the secure adoption and management of Cloud IVS by examining FedRAMP (Federal Risk and Authorization Management Program), a U.S Government program for safe and efficient deployment of cloud systems. Our framework is designed from the security and operational perspective.

1 Introduction

Video surveillance systems have evolved into large-scale Intelligent Video Surveillance (IVS) systems with IT paradigms such as Cloud computing, Big data, and Artificial Intelligent. Cloud computing enables video surveillance systems to store video footage in the cloud and to analyze it employing intelligent analytics [1]. IVS is widely used for a variety of purposes such as defense and residential security. According to a market forecast [1], the global market for IVS, broadly including video analytics, video content analytics (VCA), and intelligent surveillance reconnaissance (ISR), is expected to grow from $11891M in 2016 to $32188M by 2022. Fig.1 shows the global IVS market size by 11 vertical sub-markets. The IVS for defense is expected to

* This paper was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT)[2017-0-00207, Development of Cloud-based Intelligent Video Security Incubating Platform] and this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A3A03918513).
† Corresponding author. (namjepark@jejunu.ac.kr)

have the highest market share over the entire period (especially 48.1% in 2022). The IVS for safe and smart cities is expected to be ranked next (especially 15.8% in 2022). The average growth rate of all the sub-markets is expected to be 18.1% for 8 years.

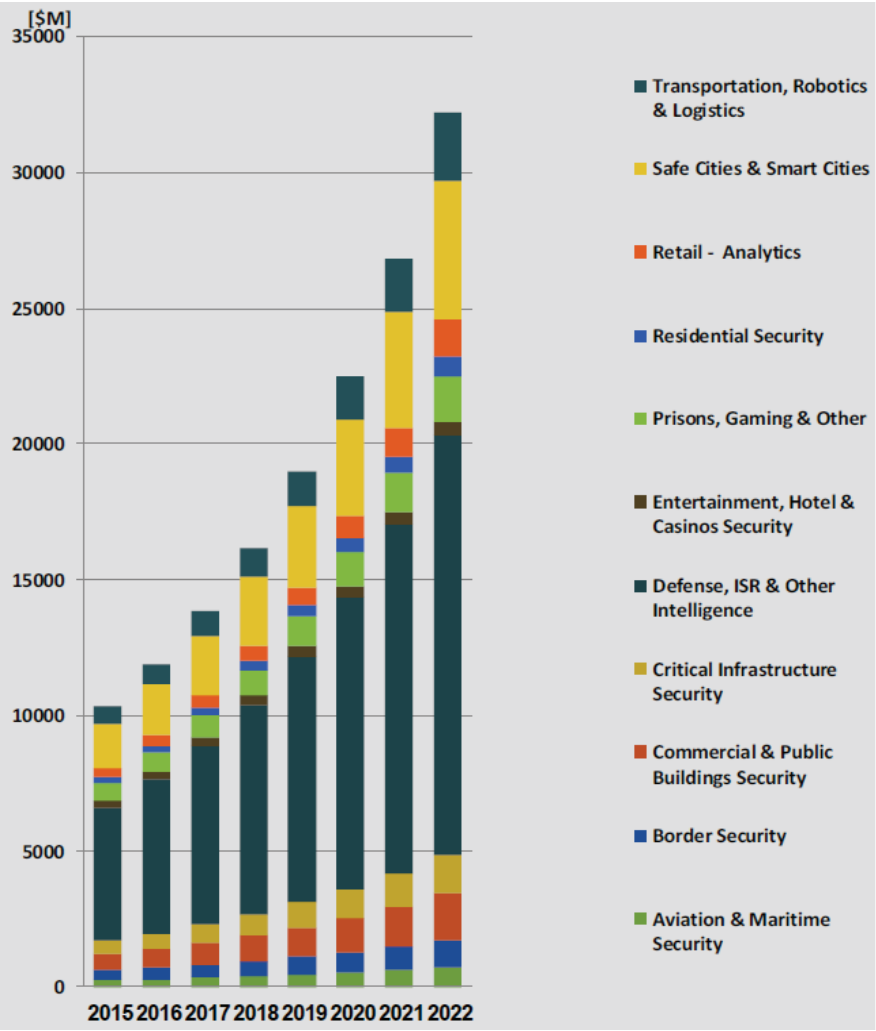


Fig. 1. Global IVS market by vertical sub-markets from 2015 to 2022 [1]

Although there is a high demand for IVS from public agencies, it is still challenging to adopt and manage the Cloud IVS systems due to a lack of guidelines and standards.

We propose a framework for Cloud IVS management by examining FedRAMP (Federal Risk and Authorization Management Program). FedRAMP has developed to provide a standardized approach to managing cloud products and services in federal agencies. Complying with FedRAMP, the agencies are able to rapidly adopt secure and cost-effective cloud systems [2]. We examine FedRAMP to develop a standard-

ized approach to not only operational processes but security requirements of Cloud IVS. The remainder of this paper is organized as follows. We review FedRAMP in Section 2. Section 3 designs the operational and security framework for the Cloud IVS management. Finally, the conclusion is presented in Section 4.

2 FedRAMP

FedRAMP is a U.S Government program to accelerate the adoption of secure cloud solutions [2]. FedRAMP standardizes the way of applying Federal Information Security Management Act (FISMA) to cloud services. Complying with FedRAMP, Government entities are able to reduce the cost of FISMA compliance and to secure sensitive data [3]. FedRAMP is governed by executive branch entities as shown in Fig. 2.

Fig. 2. FedRAMP governance entities [3]

OMB (Office of Management and Budget) establishes federal policies for protection of cloud services. CIO (Chief Information Officer) council provides a guidance for ISIMC (Information Security and Identity Management Committee).

NIST (National Institute of Standards and Technology) develops FISMA compliance and provides technical advisors and specifications. DHS (Department of Homeland Security) sets the continuous monitoring strategy and manages US-CERT (United States Computer Emergency Readiness Team) for incident response. FedRAMP GSA (General Services Administration) establishes RFI (Request for Information) as well as RFQ (Request for Quotation) for all the federal agencies.

Among the stakeholders, GSA has the FedRAMP PMO (Program Management Office), which is responsible for the development and operation of FedRAMP program. The CIOs (Chief Information Officer) of DHS, GSA, and DoD are members of Federal JAB (Joint Authorization Board). The JAB closely works with the FedRAMP PMO

for the security assessment as well as authorizations of 3PAOs (Third Party Assessment Organization) and CSPs (Cloud Service Provider).

Since Cloud IVS provides an IVS technique as a service on cloud platforms, we are able to establish guidelines for the Cloud IVS by looking at the FedRAMP requirements.

3 A Framework of Cloud IVS Management

We design security and operational frameworks for the adoption and operation of Cloud IVS considering the FedRAMP requirements for the CSPs and 3PAOs.

3.1 Operational framework

For the secure and cost-effective operation of Cloud IVS, a systematic strategy across all phases is required. Once we have the systematic framework for the Cloud IVS management, we can reuse the framework whenever necessary.

We define 5 phases of the operational process for Cloud IVS as shown in Fig. 3.

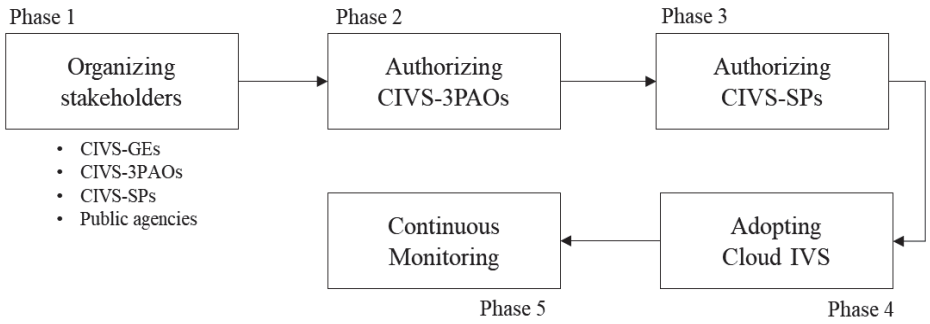


Fig. 3. Operational process for the management of Cloud IVS

The first phase is to organize stakeholders and to define each role. The stakeholders can be divided into four groups such as CIVS-GEs (Cloud IVS Governance Entities), CIVS-SPs (Cloud IVS Service Providers), CIVS-3PAOs (Cloud IVS Third Assessment Organizations), and public agencies.

The CIVS-GEs are responsible to establish security and operational policies for Cloud IVS and to authorize the CIVS-SPs and CIVS-3PAOs [4]. The public agencies should comply with the policies by the CIVS-GEs when they adopt and manage Cloud IVS. The second and third phases are to authorize CIVS-3PAOs and CIVS-SPs. The CIVS-GEs should evaluate whether the CIVS-3PAOs have the ability to assess CIVS-SPs based on the requirements. The authorized CIVS-3PAOs is responsible for the assessment of the CIVS-SPs in accordance with the contract clause with CIVS-GEs.

The next phase is to adopt the Cloud IVS systems. The public agencies are responsible to select the authorized CIVS-SPs and CIVS-3PAOs, and to prove that their systems are in compliance with the policies by CIVS-GEs.

The last phase is to perform a continuous monitoring. The CIVS-SPs are responsible to assess security controls and to cooperate for the operational visibility, change control, and incident response [5].

3.2 Security framework

Security controls listed in NIST SP 800-53 [6] can be incorporated in the security framework for Cloud IVS as FedRAMP. The security controls are classified into 18 groups including access control, contingency planning, media protection, maintenance, personnel security, risk assessment, program management, security assessment and authorization. Each of the 18 groups is given its own identifier and is managed with control baselines (low, moderate, and high).

The CIVS-GEs can define suitable security controls for Cloud IVS at the first phase of the operational process. Once the security controls have been selected, the CIVS-SPs are able to assess the security controls for the continuous monitoring and to verify their qualifications.

4 Conclusion

IVS is widely used for the public purpose with intelligent analytics based on Cloud Computing, Big data, and Artificial Intelligence. For the secure and cost-effective adoption of Cloud IVS in public agencies, a standardized approach to managing the Cloud IVS systems are required. We have proposed a framework for Cloud IVS from the security and operational perspective. We defined 5 phases for the operational framework and described each phase through the role description of the stakeholders. For the security framework, we have suggested security controls also used in FedRAMP. We will specify our framework considering the type of IVS platforms and will extend the security controls for the Cloud IVS in the future.

Acknowledgement

This paper was supported by Institute for Information & communications Technology Promo-tion(IITP) grant funded by the Korea government(MSIT)[2017-0-00207, Development of Cloud-based Intelligent Video Security Incubating Platform] and this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A3A03918513). Corresponding author. (namjepark@jejunu.ac.kr)

References

1. Homeland Security Research Corp : Global Video Analytics, VCA, ISR & Intelligent Video Surveillance Market, 2017.
2. FedRAMP homepage : https://www.fedramp.gov/

3. FedRAMP : FedRAMP Security Assessment Framework, Version 2.4, 2017.
4. RedRAMP : FedRAMP Agency Authorization Roles & Responsibilities for FedRAMP CSPs & Agencies, 2017.
5. FedRAMP : FedRAMP Continuous Monitoring Strategy Guide, Version 3.2, 2018
6. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 2013.
7. FedRAMP : FedRAMP General Document Acceptance Criteria, Version 2.1, 2018.
8. Cloud Security Alliance : The Treacherous 12: Cloud Computing Top Threats in 2016, Top Threats Working Group
9. Cloud Security Alliance : Cloud Computing Vulnerability incidents : A statistical Overview, Cloud Vulnerabilities Working Group
10. JAMES, BD : Security and privacy challenges in cloud computing environments, IEEE Security and Privacy Magazine, January 2011.
11. Rong, Chunming, Son T. Nguyen, and Martin Gilje Jaatun : Beyond lightning: A survey on security challenges in cloud computing, Computers & Electrical Engineering Vol. 39, No. 1, pp. 47-54, 2013.
12. Srinivasan, Madhan Kumar, et al : State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment, Proceedings of the international conference on advances in computing, communications and informatics. ACM, 2012.

Intelligent Information Technology-based ICT Education and Creativity Education Develop Core Competencies

Yujin Jung[1], Namje Park[2, †], and Heuipil Kim[3]

[1] Center for Creative Education, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
{yujinjung, edu}@jejunu.ac.kr

[2] Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
namjepark@jejunu.ac.kr

[3] Department of Practicall Atrs Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
khp@jejunu.ac.kr

Abstract. This paper investigates today's teaching of creativity and the importance of school teachers in such teaching and accordingly proposes a new model for training the teachers on creativity-teaching. Intelligent Information Technology is applied to a wide range of industries such as intelligent robotics, smart manufacturing and blockchain, and is giving rise to massive innovation in economy and society as a whole. Viewed in the context of such significance, ICT competencies and IIT are the subjects that should henceforth be addressed with importance in school education.

1 Introduction

For the prosperity in the 21st century that is evolving rapidly, students need more than what they have learned. In the future society, students must get used to ceaseless cooperation, communication and problem solving, and it can be developed through social and emotional learning(SEL). The abilities developed through SEL along with technical competencies that have been demanded traditionally will help students succeed in the rapidly evolving society, and they are regarded as the core competencies of the creativity education of the new era. The 16 important competencies for SEL are the 6 "foundational lieracies" including Litercy, Numeracy, and 10 abilities called as "competencies" or "character qualities". For SEL, childhood is a crucial period. Chil-

* This paper was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government. And, this work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2017S1A5A2A01026664).

† Corresponding author. (namjepark@jejunu.ac.kr)

dren accept SEL best and the strategies targeting children in this stage can have a lasting influence on their whole life while social and emotional skills can be taught to all classes. There are 30 strategies to develop 16 competencies defined by SEL. In this paper, the class model was proposed based on SEL to help elementary school students develop creativity and study.

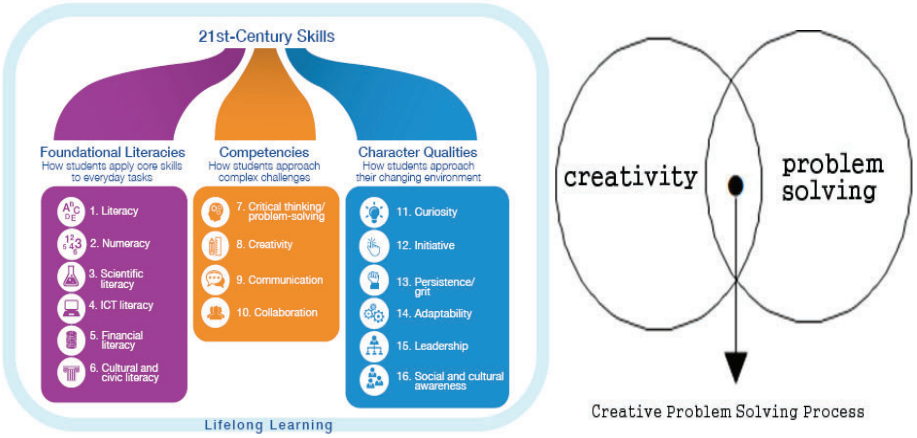


Fig. 1. SEL-based Learning Strategies to Creativity Education Development.

2 Theoretical Background

2.1 Teaching of Creativity

The world today is heading for a system marked by unlimited competition and as such greater creativity and innovation are in demand. In the context thereof, creativity has been variously defined by researchers and refers, on the whole, to an individual's ability to utilize the basic knowledge about his/her chosen field of expertise to create a product that is useful to the society to which he/she belongs.

Meanwhile, the concept of teaching creativity (hereinafter, "creativity-teaching") as a way of teaching in relation to creativity can be viewed in roughly three ways[6]. First, creativity-teaching may refer to teaching about creativity, meaning teaching that helps students become aware of the importance of creativity by leading them to learn about the concept of creativity, development process, etc. Second, creativity-teaching may alternatively refer to teaching creatively, which entails the use of a new and original approach to make the learning of certain subjects more interesting and effective. Last, creativity-teaching points to teaching for creativity, where education guides students to self-awareness of their own potential creativity and helps them use such creativity as a stepping stone towards producing creative outcomes. The three foregoing ideas overlap with one another rather than being separate notions; however, institutional endeavors for creativity-teaching should especially focus on establishing implementation strategies for and investigating 'teaching creatively'[3].

2.2 ICT Competencies and Intelligent Information Technology

ICT competencies basically refer to one's ability to search and use information/data by utilizing information and communication technology (ICT). More concretely, ICT competencies point to a set of skills that allow one to recognize all necessary information, understand where such information is located, be able to gain access to the best possible source, identify the necessary information within the source and collect and systematically organize it, and apply the outcomes therefrom to problem-solving[7]. As previously mentioned, ICT competencies are being considered one of the essential competencies along with creativity for preparing against future society.

In relation to the mentioned ICT competencies, intelligent information technologies (IIT) ―known to be the direct driver for the latest fourth industrial revolution (4IR)― refer to a set of skills where IIT and data utilization skills are employed to materialize the high-level human information processing capabilities (e.g., cognition, learning, reasoning, etc.)[8]. Nowadays IIT is applied to a wide range of industries such as intelligent robotics, smart manufacturing and blockchain, and is giving rise to massive innovation in economy and society as a whole[9]. Viewed in the context of such significance, ICT competencies and IIT are the subjects that should henceforth be addressed with importance in school education.

3 Creativity Education Training Program Development Process

The creativity-teaching training model for school administrators (the topic of this paper) was invented based on the ADDIE framework which consists of five phases, i.e., analysis, design, development, implementation, and evaluation, that constitute an actual process common to instructional systems design (ISD). This study introduces the process, with focus on the analysis, design, and development phases[5].

3.1 Analysis

What is important in this phase is the analysis of the learner and of the task[19]. To address these, review was conducted on studies about school administrators' awareness of creativity-teaching and the extent to which the administrators demand training thereupon, and literature on creative teaching methods and the latest IC and II technologies. The literature review so conducted is broad in scope based not only on research databases but on various books and newspaper articles as well.

3.2 Design

The design phase is where an instructional design (document) is created addressing how the content identified in the analysis phase should be taught, and where plans regarding teaching and learning strategies, learning time, learning materials, etc. are established[5]. To that end, the study actually implemented major creative-teaching methods as the learning strategies, by which the participants were led to experience creative-teaching techniques more naturally while receiving the training. In terms of

the learning materials, the training program aggressively utilized as the learning materials the facilities in the study site (Jeju) where the training took place in parallel with classroom lectures. The inclusion of the facilities as a venue for hands-on activities was part of the study design where further internalization of the attained knowledge was intended for the administrators.

3.3 Development

Based on the implemented analysis and design phases, the development of the training program was undertaken. In the development of training materials, various experts in creative-teaching methods, ICT and IIT participated, and the lecture notes and learning materials produced by them were used to issue a training sourcebook[5]. Furthermore, a questionnaire was composed to examine the trainees' satisfaction and training effectiveness. The instrument was designed such that not only multiple choice questions but also open-ended ones were included so the respondents could freely state their opinions about the training.

4 Result of Training Program Development

The analysis phase came up with the following results. First, the analysis of the relevant literature on the learners' (school administrators') awareness of creativity-teaching and levels of their demand for the training showed that the administrators rated 'knowledge about teaching/learning and evaluation methods regarding creativity-teaching' as the most important in the training. Hence, the focus was placed on teaching/learning and evaluation methods for creativity-teaching. And to this end, creative teaching methods to be addressed during the training were selected based on discussions between the experts and the results of literature review. Table 1 lists a brief summary of the teaching/learning methods.

Table 1. Major creative teaching techniques employed for the training

Teaching/ Learning technique	Details
Visual thinking	A method by which the learner expresses and documents information and ideas using both texts and images
Paper sculpture	A technique where ideas are recorded on index cards, followed by arrangement of the cards and organization of related cards into groups
Chavrusa	Pairing-up of peers encouraging debate and discussion towards learning

Role-playing	A method wherein learners assume different roles and interact with one another representing respective points of view so as to attain knowledge or adopt an attitude
Gamification	Applying game-related techniques to learning so that learners can be led to immersion
PMI technique	A technique where learners examine the plus, minus, and interesting aspect about an idea before deciding on the best possible idea

Second, in terms of training content, the topics listed in Table 2 were selected following the analysis of research literature on creativity-teaching and the meetings of the experts. The selection of content considered primarily the novelty and timeliness found in each topic. In the training-design phase, features of the aforementioned creative teaching methods were taken into consideration and were implemented appropriately for each part of the training content. The training courses were accordingly designed as shown in Table 2. Moreover, the trainees were given choices about a course(s) they would like to take.

Table 2. Main training content and course details

Topic	Course details
Core principles for and ethics of AI	Content: Learning about the principles of artificial intelligence (AI) through unplugged activities; today's emerging ethical issues relating to AI
	Option 1: Core AI principles and ethics using visual thinking
	Option 2: Core AI principles and ethics using paper sculptures
Hyper connectivity communications for the future	Content: A communication technology aiming at accomplishing communication and interaction between people and things in close connectivity
	Option 1: Hyper connectivity communications in the future using the Chavrusa technique
	Option 2: Hyper connectivity communications in the future using role-playing
Future cloud computing and security	Content: Searching cloud computing technology for data storage and security technologies
	Option 1: Future cloud computing and security using gamification

	Option 2: Future cloud computing and security using the PMI process

4 Conclusion

The purpose of this paper was to present the process and result of developing a training model that was designed specifically for school administrators on teaching of creativity ("creativity-teaching"). The development was materialized using the ADDIE process, and the training content was organized based on the analysis of relevant literature and discussions held between professionals who specialize in information and communication (IC) and education. Results of the development showed that the training program includes a wide range of creative teaching methods which were implemented for the novel and timely intelligent information technology (IIT) principles that emerged in recent years, thereby ensuring creative learning takes place in the school administrators spontaneously. Furthermore, resources of the study site were utilized for the program so the trainees' hands-on activities relating to creativity-teaching could bring in effectiveness.

Acknowledgement

This work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE) and, this work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2017S1A5A2A01026664). Corresponding author. (namjepark@jejunu.ac.kr)

References

1. Feldman,D.H.: Creativity: Dreams, insights, and transformations. In R. J. Sternberg (Ed.), The nature of creativity: Contemporary psychological perspectives, NY: Cambridge University Press, pp.271-297, 1993.
2. Eisenberg, M. B. & Robert E.B.: Helping with Homework: A parent's Guide to Information Problem-Solving. Syracuse, New York: Clearinghouse on Information Technology, Syracuse University,1996.
3. Neapolitan, R. E & Jiang, X.: Contemporary Artificial Intelligence, CRC press, 2013.
4. Allen, W. C.: Overview and evolution of the ADDIE training system. Advances in Developing Human Resources, 8(4), pp.430-441, 2006.
5. Joonmo Yun, Namje Park : The Korea Association of Information Education 2018 Summer Conference, pp.49-54, Aug. 2018

The Rigidity of Rectangular Frameworks

Keunbae Choi[1], Namje Park[2, *]
[1] Dept. of Mathematics Education, Jeju National University
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
kbchoe@jejunu.ac.kr

[2] Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
namjepark@jejunu.ac.kr

Abstract. In general, the stability problem of rectangular frameworks consisting of rectangular array of girder beams and riveted joints is determined by the connectivity of the bipartite graph. In this paper, we study how to solve the stability problem using the rank of the matrix induced by the rectangular framework.

1 Introduction

Many buildings are maintained by steel frame structures consisting of rectangular array of girder beams and welded or riveted joints. Especially, this is the case when designing high-rise buildings. However, for many reasons, these structures are treated as planar structures with pin-joints rather than rigid welds when joining the beams together. The simplest form is a rectangle consisting of four beams and four pin-joints (see, Fig. 1).

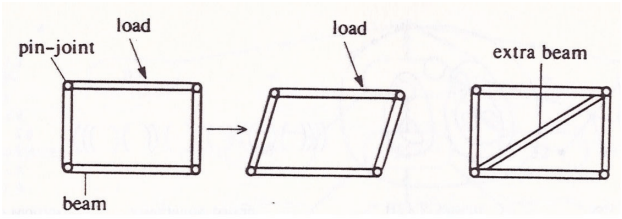


Fig. 1. Simplest form of rectangular framework(Wilson & Wakins, 1990)

This structure is unstable because it can be easily deformed under sufficiently high loads as Fig. 1. For the stability of the structure, it must be braced by extra beam. In the case of larger structure (Fig. 2.) containing many rectangular cells, it is possible to

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2017S1A5A2A01026664).
* Corresponding author. (namjepark@jejunu.ac.kr)

ensure the rigidity by attaching support rods (extra beams) to all the rectangular cells, but it is costly in terms of economy.

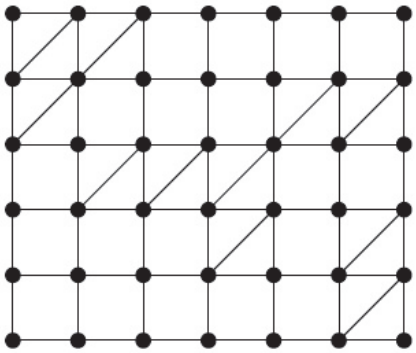


Fig. 2. Rectangular framework with many cells

Here, we can have the following two mathematical problems.

The rigidity problem: whether the rectangular framework with bracings is rigid or not.

Optimization problem: what is the minimum number of braces when the braced rectangular framework is rigid.

It is well known that the above problem can be solved with the connectivity of the bipartite graph induced by a braced rectangular framework (see, Bolker & Henry, 1997; Graver, 2001; Lee, Kwon & Choi, 2016; Laine, 2006; Servatius, 1995; Wilson & Wakins, 1990).

In particular, in Lee, et al. (2016), the rigidity of a rectangular framework is verified in more detail by using the relationship between the connectivity of the bipartite graph induced by given rectangular framework and the variation of angles of parallelograms constituting the rectangular framework.

In this paper, we study how to solve the stability problem using the rank of the matrix induced by the braced rectangular framework.

2 On the Bracing Rectangular Frameworks

Let R_{mn} be a m x n rectangular framework with bracings. For each $i, j(1 \le i \le m,\ 1 \le j \le n)$, we let θ_{ij} be the angle of the upper left corner of the parallelogram that lies in the i-th row and j-th column of R_{mn} (See, Fig. 5). If $\theta_{ij} = 90$ for each $i, j(1 \le i \le m,\ 1 \le j \le n)$, then the rectangular framework R_{mn} is rigid. Notice that the angle of the upper left corner of a parallelogram with bracing is 90. In Fig. 5., $\theta_{11} = \theta_{14} = \theta_{22} = \theta_{23} = \theta_{31} = \theta_{34} = 90$, to determine the rigidity of the framework, we have to examine the remaining corner angles are also right angle.

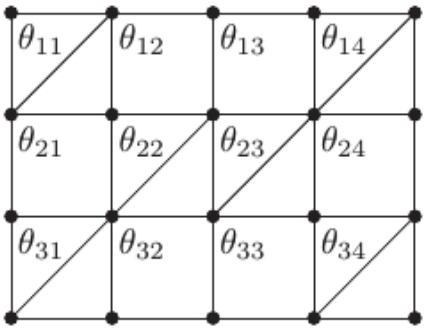


Fig. 5. The upper left corner angles in rectangular frameworks

The following lemma plays an important role in our approaches.

Lemma 2.1. *Let R_{mn} be a m x n rectangular framework. For each i, j($1 \leq i < m$, $1 \leq j < n$), we have*

$$\theta_{ij} + \theta_{i+1j+1} = \theta_{ij+1} + \theta_{i+1j}$$

Proof. This is because the torsional motion of a rectangular framework is eventually depend on the torsional motion of the parallelograms that make up each cell in rectangular framework.

In Fig. 5, we have the following equations.

$$\begin{cases} \theta_{11} + \theta_{22} = \theta_{12} + \theta_{21} \\ \theta_{12} + \theta_{23} = \theta_{13} + \theta_{22} \\ \theta_{13} + \theta_{24} = \theta_{14} + \theta_{23} \end{cases}, \quad \begin{cases} \theta_{21} + \theta_{32} = \theta_{22} + \theta_{31} \\ \theta_{22} + \theta_{33} = \theta_{23} + \theta_{32} \\ \theta_{23} + \theta_{34} = \theta_{24} + \theta_{33} \end{cases}$$

Equivalently,

$$FY = O, \tag{2.1}$$

Where O is zero matrix,

$$F = \begin{bmatrix} A & -A & O \\ O & A & -A \end{bmatrix}$$

with

$$A = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix},$$

and

$$Y = [\theta_{11}\,\theta_{12}\,\theta_{13}\,\theta_{14}\,\theta_{21}\,\theta_{22}\,\theta_{23}\,\theta_{24}\,\theta_{31}\,\theta_{32}\,\theta_{33}\,\theta_{34}]^t$$

Equivalently, if we consider bracings in Fig. 5., then we have

$$F_R\,X = B, \tag{2.2}$$

where

$$F_R = \begin{bmatrix} -1 & 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 & 0 & -1 \end{bmatrix},$$

$X = [\theta_{12}\,\theta_{13}\,\theta_{21}\,\theta_{24}\,\theta_{32}\,\theta_{33}]^t$, and

$$B = -90^\circ \left(\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right)$$
$$= \begin{bmatrix} -180^\circ \\ 0^\circ \\ 180^\circ \\ 180^\circ \\ 0^\circ \\ -180^\circ \end{bmatrix}$$

Clearly, the system (2.2) of linear equations is consistent. In particular, for all *i, j*($1 \le i \le 3,\ 1 \le j \le 4$), θ_{ij} = 90 is a solution of the system. Thus we have that the rectangular framework in Fig. 5. is rigid if and only if the rank of the matrix F_R is 6. But since rank(F_R)=5, the rectangular framework in Fig.5. is not rigid.

In general, for a rectangular framework R_{mn}, we have the following equations; for each *i=1,2, ... , m-1*,

$$\begin{cases} \theta_{i1} + \theta_{i+1\,2} = \theta_{i2} + \theta_{i+1\,1} \\ \theta_{i2} + \theta_{i+1\,3} = \theta_{i3} + \theta_{i+1\,2} \\ \cdots \\ \theta_{i\,n-1} + \theta_{i+1\,n} = \theta_{in} + \theta_{i+1\,n-1} \end{cases}$$

Equivalently, we have

(2.3) $$FY = O,$$

where

$$F = \begin{bmatrix} A & -A & O & O & \cdots & O & O & O \\ O & A & -A & O & \cdots & O & O & O \\ & & & & \ddots & & & \\ O & O & O & O & \cdots & O & A & -A \end{bmatrix}_{\{(m-1)\times(n-1)\}\times(m\times n)}$$

with

$$A = \begin{bmatrix} 1 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ & & & & \ddots & & & \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & -1 \end{bmatrix}_{(n-1)\times n},$$

$O = [0]_{(n-1)\times n}$, and $Y = [\theta_{11}\theta_{12}\cdots\theta_{1n}\theta_{21}\theta_{22}\cdots\theta_{2n}\cdots\theta_{m1}\theta_{m2}\cdots\theta_{mn}]^t$

Now, if we consider the bracings of given rectangular framework R_{mn}, then we have the following system of linear equations from (2.3),

(2.4) $$F_R X = B,$$

where

- F_R is the matrix obtained by deleting θ_{ij} columns in F corresponding to braced parallelograms in R_{mn}.
- X is the matrix obtained by deleting θ_{ij} columns in Y corresponding to braced parallelograms in R_{mn}. That is to say, X is determined by non-braced parallelograms in R_{mn}.

- B is the matrix obtained by deleted θ_{ij} columns in F corresponding to braced parallelograms in R_{mn}.

Theorem 2.2. *Let R_{mn} be a m x n (m, n ≥2) rectangular framework. Then R_{mn} is rigid if and only if the rank of F_R is the number of columns of F_R.*

Proof. Clearly, the system $F_R X = B$ of (2.4) is consistent. Thus we have that the rank of F_R is equal to the number of columns of F_R if and only if the system $F_R X = B$ has only one solution, say $X = [90\ 90\ \cdots\ 90]^t$.

Corollary 2.3. *Let R_{mn} be a m x n (m, n ≥2) rectangular framework. Then $m+n-1$ is the minimum number of supports for R to be rigid.*

Proof. Notice that

$$mn - (m + n - 1) = (m - 1)(n - 1) = \operatorname{rank}(F) \geq \operatorname{rank}(F_R)$$

This completes the proof.

References

1. Bolker, E. D. and Henry Crapo., *Bracing Rectangular Frameworks I*, SIAM J. Appl. Math. Vol. 36 (1997) 473–490.
2. Graver, J. E., Counting on frameworks: Mathematics to Aid the design of Rigid Structures, the Mathematical Association of America, United States of America. 2001.
3. Lee, J., Kwon, Y. S and Choi, K., *A Study on the Bracing Rectangular Frameworks*, J. Korea Soc. Math. Ed. Ser. E: Communications of Mathematical Education, Vol. 30 (2) (2016), 251-262.
4. Laine, S. T., The Grid Bracing Problem and a Generalization, Master's Thesis of Worcester Polytechnic Institute, United States of America. 2006.
5. Servatius, Brigitte., *Graphs, Digraphs, and the Rigidity of Grids*, The UMAP Journal, Vol. 16 (1995), 37-63.
6. Wilson, R. J. and Wakins, J. J., Graphs; An introductory Approach, John Wiley and Sons, Inc. 1990.

Strong Designated Verifier Signcryption Scheme

Neetu Sharma[1], Rajeev Anand Sahu[2], Vishal Saraswat[3], Gaurav Sharma[2],
Veronika Kuchta[4], Olivier Markowitch [2]

PRS University, Raipur, India[1],
Université Libre de Bruxelles, Belgium[2]
Indian Institute of Technology, Jammu, India[3]
Monash University, Australia[4]
* rajeev.sahu@ulb.ac.be

Abstract. Recall two important cryptographic primitives. *Strong designated verifier signature* (SDVS), which is an *almost* anonymous signature that can be verified only by the designated receiver, and *signcryption*, which is a hybrid cryptographic primitive that offers functionality of digital signature as well as that of encryption in a single phase. Applications of SDVS have been observed in many privacy-preserving algorithms including those for cloud security. Signcryption is useful for electronic transactions where authentication and privacy are desired together, for example in secure routing, multicast key distribution etc. However, in a usual SDVS, the message is always sent with the signature, which is not desired for some classified messages. Instead, to ensure the confidentiality of the message an encryption can be used. To address this issue, in this paper, we have combined these two primitives, *Strong designated verifier signature* (SDVS) and *signcryption* to propose a condensed construction of strong designated verifier signcryption (SDVSigncryption) which achieves message confidentiality and can be verified only by the intended recipient. The scheme fulfils all the security properties of the individual components. The proposed scheme is also adaptively unforgeable against chosen message attack and chosen identity attack under the standard assumption, Computational Bilinear Diffie-Hellman Assumption (CBDHA). Moreover, the scheme is well suited for the environments where less computational cost with strong security is prime concern.

1 Introduction

As fast the electronic communication is outreaching to the sensitive domains of our daily life, their security requires highest attention. At the basic level, the fundamental security properties like confidentiality, authentication, integrity, non-repudiation, access control etc. are necessarily important for a secure communication. In general, confidentiality and access control can be achieved by an encryption scheme and rest of the properties can be achieved by digital signature using a hash function. But, there may be situations where all these properties are required simultaneously. Signcryption is an important cryptographic primitive which achieves the properties of both a digital signature and an encryption scheme in a compact algorithm. But if the signature scheme inbuilt in the signcryption is a regular signature, then authenticity of the communication can be checked publicly, which may not be desired in various applications for example in communication of a sensitive report to a news agency. For such a situation and for similar applications, a signcryption is also required to be anonymous (achieving sender's annonymity) and designated verifier. To achieve the required features in such communications, in this paper we formalize the definition and concrete scheme of strong designated verifier signcryption scheme, we call it SDVSigncryption, on the identity(ID)-based setting using the functionalities of bilinear pairings.

1.1 Related work

In 1984, Shamir[21] suggested the seminal idea of ID-based cryptography to eliminate the burden of key management. The first practical and provably secure ID-based encryption scheme was realized by Boneh and Franklin in 2001 [2] by the means of functionality of Weil pairing. Since then

application of bilinear pairing have been explored vastly in construction of many cryptographic protocols [3,12,8,15,9]. The notion of ID-based signcryption scheme was introduced in 2002 [16], to achieve the low computational cost for the 'sign-then-encrypt' or 'encrypt-then-sign' procedure on ID-based setup. However, Libert et al. [15] pointed out security flaws in [16] that the scheme [16] is not semantically secure as the verification requires private key of user or zero knowledge interactive protocol without disclosing the receiver's secret key. To overcome this weakness they proposed three provably secure ID-based signcryption schemes [15]. They claimed that all the proposed schemes are semantically secure under the random oracle model. Soon after the proposal, Chow et al. [10] observed a shortcoming in [15] and proposed a construction to fulfil the gap. The first multipurpose signcryption was proposed in [4]. Chen et al. [7] claimed that the scheme in [4] is not efficient for many practical applications and proposed provably more secure and efficient scheme. they also improved the efficieny of [4]. Till 2005, the most efficient scheme was due to Barreto et al. [1]. In 2009, Yu et al. [25] introduced the first ID-based signcryption scheme secure in the standard model. Since then, a wide range of study and research have been taken place in this topic [26,27,20].
Chow et al. [10] proposed the signcryption scheme with public verifiability property secure under the hardness assumption of computational Diffie-Hellman problem. For various real world practical applications, the public verifiability property of a signature scheme may be undesirable to share sensitive information between the parties. To overcome such situation, the signer needs to bind a verifier with control over verification process. Chaum et al. [6] introduced the idea of undeniable signature which grants a signer to have full control over the verification. In this concept, the verification requires participation of the signer, in order to avoid undesirable verifiers getting convinced of the validity of the signature. To improve this shortcomings, Jakobsson et al. [13] proposed the concept of designated verifier signature (DVS) at Eurocrypt'96. In 2003, Saeednia et al. [19] introduced the property of *strongness* and proposed the first strong designated verifier signature (SDVS) scheme. The property strongness refers to the anonymity of the signer, in the sense that a SDVS from signer S_i to designated verifier V_i is indistinguishable from a SDVS from signer S_j to designated verifier V_j, for $i \neq j$. Recently, [22] introduced an efficient SDVS using ID-based setting. This scheme was strongly existentially unforgeable against adaptive chosen message and adaptive chosen identity attack under the hardness of the computational bilinear Diffie-Hellman problem. Moreover, they also provided the formal security proofs of unverifiability and strongness of the proposed scheme. Their scheme was more efficient in the view of computation and operation time than the existing other similar schemes. Some useful applications of the proposed scheme in E-Tendering and Electronic Health Record have been discussed in the full version of this paper.

1.2 Our Contribution

In this paper we present the definition and concrete construction of ID-based SDVSigncryption from bilinear pairings. The proposed scheme is unforgeable against adaptive chosen message and adaptive chosen identity attack under the computational bilinear Diffie-Hellman assumption. Additionally, we do an efficiency comparison and show that the proposed scheme is more efficient than the existing similar schemes.

1.3 Outline of the Paper

The reminder of this paper is organized as follows. Section 2 explains some basic definitions, assumptions and mathematical problems. Section 3 describes the generic model of id-based strong designated verifier signcryption (ID-SDVSigncryption) scheme and its security. In 4 our proposed ID-SDVSigncryption is presented. In Section 5 the security of our scheme is briefly addressed and in Section 6 we do an efficiency comparison of our scheme with some existing similar schemes. Finally a conclusion of our result is presented in Section 7.

2 Preliminaries

In this section, we put forward some mathematical definitions, problems and assumptions.
A probabilistic polynomial time (PPT) algorithm is a probabilistic/randomized algorithm that runs in time polynomial in the length of input. We denote by $y \leftarrow A(x)$ the operation of running a randomized or deterministic algorithm A with input x and storing the output to the variable y. If X is a set, then $v \xleftarrow{\$} X$ denotes the operation of choosing an element v of X according to the uniform random distribution on X. We say that a given function $f : N \rightarrow [0,1]$ is *negligible in n* if $f(n) < 1/p(n)$ for any polynomial p for sufficiently large n [17]. For a group G and $g \in G$, we write $G = \langle g \rangle$ if g is a generator of G.

Definition 1 (Bilinear Pairing).
Let G_1 be an additive cyclic group and G_2 be a multiplicative cyclic group. Let both the groups have the same prime order q. A map $e : G_1 \times G_1 \rightarrow G_2$ is called a cryptographic bilinear map *or a* pairing *if it satisfies the following properties:*
Bilinearity: *For all $a,b \in \mathbb{Z}_q^*$, $e(aP,bP) = e(P,P)^{ab}$, or equivalently, for all $Q,R,S \in G_1$, $e(Q+R,S) = e(Q,S)e(R,S)$ and $e(Q,R+S) = e(Q,R)e(Q,S)$.*
Non-Degeneracy: *There exists $Q,R \in G_1$ such that $e(Q,R) \neq 1$. Note that since G_1 and G_2 are groups of prime order, this condition is equivalent to the condition $g := e(P,P) \neq 1$, which again is equivalent to the condition that $g := e(P,P)$ is a generator of G_2.*
Computability: *There exists an efficient algorithm (like Miller's algorithm [18]) to compute $e(Q,R) \in G_2$ for all $Q,R \in G_1$.*

Definition 2 (Computational Bilinear Diffie-Hellman Problem (CBDHP)). For any $a,b,c \in Z_q^*$, given $aP,bP,cP \in G_1$, where G_1 is an additive cyclic group with generator P, the *Computational Bilinear Diffie-Hellman Problem* (CBDHP) is to compute $e(P,P)^{abc}$.

Definition 3 (Computational Bilinear Diffie-Hellman Assumption (CBDHA)). Let $Adv_\lambda(\mathcal{A})$ be the advantage that an algorithm $\mathcal{A}$ has in solving the CBDH problem. It is defined as the probability that the algorithm $\mathcal{A}$ computes $e(P,P)^{abc}$ on input $(\lambda, G_1, G_2, e, P, aP, bP, cP)$, where λ is the security parameter, G_1, G_2, e are as defined above, P is a random generator of G_1, a,b,c are random elements of Z_q^*. Then the CBDH assumption is that $Adv_\lambda(\mathcal{A})$ is negligible for all efficient algorithms $\mathcal{A}$.

3 ID-Based Strong Designated Verifier Signcryption Scheme (ID-SDVSigncryption)

This section formalize the generic model of an ID-SDVSigncryption scheme and security properties for it as follows:

3.1 ID-SDVSigncryption Scheme

An ID-SDVSigncryption scheme consists of the following algorithms:
1. $params \leftarrow \mathsf{Setup}(\lambda)$: Given a security parameter λ this algorithm outputs a master secret s, which is kept confidential and the public parameters *params*, which is publicly known.
2. $(Q_{ID}, S_{ID}) \leftarrow \mathsf{KeyExtract}(\mathsf{ID}, params)$: For an ID, the private key generator (PKG) outputs key pair (public key, private key) $(Q_{\mathsf{ID}}, S_{\mathsf{ID}})$ using *params*.
3. $\sigma \leftarrow \mathsf{DVSigncrypt}(\mathsf{S}_{\mathsf{ID}_S}, \mathsf{Q}_{\mathsf{ID}_V}, params, \mathsf{m})$: A randomized algorithm run by the signcrypter. It takes the signcrypter's private key S_{ID_S}, the designated verifier's public key Q_{ID_V}, public parameters *params*, message m, and outputs a ID-SDVSigncryption σ.
4. $m \leftarrow \mathsf{DVUnsigncrypt}(\mathsf{S}_{\mathsf{ID}_V}, \mathsf{Q}_{\mathsf{ID}_S}, \sigma, params)$: A deterministic algorithm run by the verifier. It takes verifier's secret key S_{ID_V} the signcrypter's public key Q_{ID_S}, an ID-SDVSigncryption σ, public parameters *params* and outputs the message m if the ID-SDVSigncryption is valid, otherwise $\perp$.

5. $\widehat{\sigma} \leftarrow \mathsf{DVTrans}(\mathsf{S}_{\mathsf{ID}_\mathcal{V}}, \mathsf{Q}_{\mathsf{ID}_\mathcal{S}}, \mathsf{Q}_{\mathsf{ID}_\mathcal{V}}, \mathsf{m})$: A deterministic algorithm run by the verifier. It takes verifier's secret key $S_{\mathsf{ID}_\mathcal{V}}$, and public keys $Q_{\mathsf{ID}_\mathcal{S}}$ and $Q_{\mathsf{ID}_\mathcal{V}}$ of the signcrypter and designated verifier and a message m to generate a ID-SDVSigncryption $\widehat{\sigma}$.

3.2 Security Properties for ID-Based Strong Designated Verifier Signcryption Scheme

This section provides the formal security properties for an ID-SDVSigncryption scheme as follows:

1. *Correctness*: This property holds between signcrypter and designated verifier. The signcrypter $\mathsf{ID}_\mathcal{S}$ computes the correct signcryption σ on a message m which can be easily verified by the designated verifier $\mathsf{ID}_\mathcal{V}$. That is,

$$Prob[1 \leftarrow \mathsf{DVUnsigncrypt}(\mathsf{S}_{\mathsf{ID}_\mathcal{V}}, \mathsf{Q}_{\mathsf{ID}_\mathcal{S}}, \mathsf{m}, \mathsf{DVSigncrypt}(\mathsf{Q}_{\mathsf{ID}_\mathcal{V}}, \mathsf{S}_{\mathsf{ID}_\mathcal{S}}, \mathsf{m}))] = 1$$

2. *Unforgeability*: In this model, an adversary $\mathcal{A}$ playing against the signcrypter, tries to forge the proposed signcryption scheme. The adversary $\mathcal{A}$ has been given the oracle path to ask Extraction queries, Hash queries and Signcryption adaptively. The goal of adversary $\mathcal{A}$ is to develop a valid signcryption (say σ^*) on a new message (say m^*) for the chosen ID (say $ID^* \neq ID$). To show the inability of adversary in doing so, we show that if the adversary $\mathcal{A}$ succeed in forging the proposed ID-SDVSigncryption scheme, then there is another adversary $\mathcal{B}$ who, following the oracle access to $\mathcal{B}$, solve the DBDHP.

3. *Confidentiality*: As an encryption scheme is inherently associated with a signcryption, the security of the encryption is required to be achieved for a secure signcryption. Confidentiality is the best known security property of an encryption scheme in cryptography, which has been defined to be achieved by the means of the property of indistinguishability.

4. *Non-transferability*: The non-transferability property of an ID-SDVSigncryption scheme refers that it is infeasible for any PPT adversary $\mathcal{A}$ to decide whether σ was produced by the signcrypter or by the designated verifier, even if $\mathcal{A}$ is also given the private keys of the signcrypter and the designated verifier. In other words, the designated verifier cannot prove to an outsider that the signcryption is actually generated by the signcrypter.

5. *Strongness*: The strongness property of an ID-SDVSigncryption scheme refers to the fact that a signcryption σ (which was actually produced by the signcrypter S for the verifier V) could have been produced by any third party S^* other than S, for some designated verifier V^* other than V.

Remark 1. The detailed definitions of security properties and the description of the security games associated to the corresponding security models have been omitted due to the page constrained. All the security definitions and games are described in the full version of this paper.

4 Proposed Scheme

The proposed ID-SDVSigncryption scheme is as follows:

Setup**:** In this phase, PKG on input security parameter λ, generates the system's master secret key $s \in \mathbb{Z}_q^*$ and the system's public parameters $params = (\lambda, G_1, G_2, q, e, H_1, H_2, H_3, P, P_{pub})$, where G_1 is an additive cyclic group of prime order q with generator P, G_2 is a multiplicative cyclic group of prime order q, $e : G_1 \times G_1 \longrightarrow G_2$ is bilinear pairing as defined in section 2, $H_1 : \{0,1\}^* \longrightarrow G_1$, $H_2 : \{0,1\}^* \times G_1 \longrightarrow \mathbb{Z}_q^*$ and $H_3 : G_2 \longrightarrow \{0,1\}^*$ are cryptographic secure hash functions and $P_{pub} = sP \in G_1$ is system's public key.

KeyExtract**:** In this phase, on input public parameters P_{pub}, the PKG calculates public key as $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in G_1$ and its associated secret key as $S_{\mathsf{ID}} = sQ_{\mathsf{ID}} \in G_1$, for a user with $\mathsf{ID} \in \{0,1\}^*$.

DVSigncrypt**:** To signcrypt a message $m \in \{0,1\}^*$ for designated verifier $\mathcal{V}$, the singcrypter $\mathcal{S}$ chooses $r, u \xleftarrow{\$} \mathbb{Z}_q^*$ and computes

– $U = rQ_{\mathsf{ID}_\mathcal{S}} \in G_1$; and $R = uP$

– $h = H_2(m,U) \in \mathbb{Z}_q^*$;
– $V = (r+h)S_{\mathsf{ID}_S} \in G_1$;
– $T = e(uP_{pub}, Q_{\mathsf{ID}_\mathcal{V}})$;
– $\alpha = H_3(T) \oplus (\mathsf{ID}_S||m)$;
– $\sigma = e(V, Q_{\mathsf{ID}_\mathcal{V}})$;
The ciphertext is (U,R,α,σ).

DVUnsigncrypt**:** On receiving (U,R,α,σ), the designated verifier $\mathcal{V}$ recovers the original message m and verifies its validity as follows:
– $T = e(R, S_{\mathsf{ID}_\mathcal{V}})$
– $(ID_S||m) = \alpha \oplus H_3(T)$.
– $h = H_2(m,U) \in \mathbb{Z}_q^*$
and adopt the signature if and only if the following equality holds:
– $\sigma = e(U + hQ_{\mathsf{ID}_S}, S_{\mathsf{ID}_\mathcal{V}})$

DVTrans**:** The designated verifier $\mathcal{V}$ chooses $\widehat{r}, \widehat{u} \xleftarrow{\$} \mathbb{Z}_q^*$ and computes
– $\widehat{U} = \widehat{r}Q_{\mathsf{ID}_S} \in G_1$;
– $\widehat{R} = \widehat{u}P \in G_1$;
– $\widehat{h} = H_2(m,\widehat{U}) \in \mathbb{Z}_q^*$;
– $\widehat{V} = (\widehat{r}+\widehat{h})Q_{ID_S} \in G_1$; and
– $\widehat{T} = e(\widehat{R}, S_{\mathsf{ID}_\mathcal{V}})$;
– $\widehat{\alpha} = H_3(\widehat{T}) \oplus (\mathsf{ID}_S||m)$;
– $\widehat{\sigma} = e(\widehat{V}, S_{ID_V})$.

5 Analysis of the Proposed Scheme

5.1 Correctness of the Proposed Scheme

$$\begin{aligned} e(U + hQ_{\mathsf{ID}_S}, S_{\mathsf{ID}_\mathcal{V}}) &= e(rQ_{\mathsf{ID}_S} + hQ_{\mathsf{ID}_S}, sQ_{\mathsf{ID}_\mathcal{V}}) \\ &= e((r+h)S_{\mathsf{ID}_S}, Q_{\mathsf{ID}_\mathcal{V}}) \\ &= e(V, Q_{\mathsf{ID}_\mathcal{V}}) \\ &= \sigma. \end{aligned}$$

5.2 Unforgeability

The proposed ID-SDVSigncryption scheme is unforgeable which is established by the following theorem:

Theorem 1. *For a security parameter λ, if there is a PPT $(q_{H_1}, q_{H_2}, q_{H_3}, q_E, q_S, q_U, t, \varepsilon_\mathcal{A}(\lambda))$-adversary $\mathcal{A}$ given only the public parameter as input. If $\mathcal{A}$ can forge the proposed ID-SDVSigncryption scheme in polynomial time t with a non-negligible success probability $\varepsilon_\mathcal{A}(\lambda)$. Then there exists another PPT adversary $\mathcal{B}$ which solves an instance of CBDHP with advantage at least*

$$\varepsilon_\mathcal{B}(\lambda) \geq \Big(1 - \frac{1}{q^2}\Big)\Big(1 - \frac{2}{q_{H_1}}\Big)^{q_E+q_U}\Big(1 - \frac{2}{q_{H_1}(q_{H_1}-1)}\Big)^{q_S}\Big(\frac{2}{q_{H_1}(q_{H_1}-1)}\Big)\varepsilon_\mathcal{A}(\lambda)$$

in time at most

$$t' \leq (q_{H_1} + q_E + 5q_S + q_V)S_{G_1} + (2q_S + 2q_V)P_e + q_S O_{G_1} + O_{G_2} + S_{G_2} + t$$

where S_{G_1} (resp. S_{G_2}) is the time taken for one scalar multiplication in G_1 (resp. G_2), O_{G_1} (resp. O_{G_2}) is the time taken for one group operation in G_1 (resp. G_2), and P_e is the time taken for one pairing computation.

Remark 2. The detailed proof of all the security properties: Unforgeability, Confidentiality, Non-transferability and Strongness have been omitted due to the page constrained. The full version of this paper can be referred for the detailed proofs of all the properties.

6 Efficiency Analysis

In this section we do an efficiency comparison of our proposed scheme with the existing similar schemes. For the computation of operation time in pairing-based scheme, to achieve the 1024-bit RSA level security, Tate pairing defined over the supersingular elliptic curve $E = F_p : y^2 = x^3 + x$ with embedding degree 2 was used, where q is a 160-bit Solinas prime $q = 2^{159} + 2^{17} + 1$ and p a 512-bit prime satisfying $p + 1 = 12qr$, using MIRACL [**?**], a standard cryptographic library, and the hardware platform is a PIV 3 GHZ processor with 512 M bytes memory and the Windows XP operating system. To compute the operation time in various schemes in the below table, we use the operation time for one bilinear pairings (P) which is 20.04ms, for one map-to-point hash functions (H) which is 3.04ms, for one modular exponentiation (E) which is 5.31ms, for one scalar multiplication (SM) it is 6.38ms. The consequent operation time is denoted by (OT). For the computation of operation time, we have referred the methods adopted in [5,11]. From the table 1 it can be observed that the proposed scheme is more efficient in the view of computation with compare to the existing similar schemes [16,24,14,23].

Scheme	SM	E	H	P	OT(ms)
Malone-Lee [16]	3	0	0	1	39.18
Yu et al. [24]	0	4	0	1	41.28
Lal et al. [14]	0	6	0	1	51.90
Shen et al. [23]	0	6	0	0	31.86
Our Scheme	**4**	**0**	**0**	**2**	**65.60**

Signcryption

Scheme	SM	E	H	P	OT(ms)
Malone-Lee [16]	0	1	0	4	85.47
Yu et al. [24]	0	3	0	3	76.05
Lal et al. [14]	0	1	0	3	65.43
Shen et al. [23]	0	2	0	5	110.82
Our Scheme	**0**	**0**	**0**	**2**	**40.08**

Unsigncrypt

Scheme	Sign	Verification	Total
Malone-Lee [16]	39.18	85.47	124.65
Yu et al. [24]	41.28	76.05	117.33
Lal et al. [14]	51.90	65.43	117.33
Shen et al. [23]	31.86	110.82	142.68
Our Scheme	**65.60**	**40.08**	**105.68**

Overall Operation Time (in ms) of Schemes

Table 1: Efficiency Comparision

7 Conclusion

We have proposed an identity-based strong designated verifier signcryption (ID-SDVSigncryption) scheme. The proposed scheme is adaptive unforgeable and achieves confidentiality under the hardness assumption of computational bilinear Diffie-Hellman problem (CBDHP). Furthermore, computational cost and operation time of our scheme is significantly less than the existing similar schemes with offering additional features. Lastly, some applications of the proposed scheme are also suggested.

References

1. Paulo SLM Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *International conference on the theory and application of cryptology and information security*, pages 515–532. Springer, 2005. 2
2. Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *CRYPTO'01*, pages 213–229. Springer, 2001. 1
3. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *Journal of cryptology*, 17(4):297–319, 2004. 2
4. Xavier Boyen. Multipurpose identity-based signcryption. In *Annual International Cryptology Conference*, pages 383–399. Springer, 2003. 2
5. Xuefei Cao, Weidong Kou, and Xiaoni Du. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, 180(15):2895–2903, 2010. 6
6. David Chaum and Hans Van Antwerpen. Undeniable signatures. In *Conference on the Theory and Application of Cryptology*, pages 212–216. Springer, 1989. 2
7. Liqun Chen and John Malone-Lee. Improved identity-based signcryption. In *International Workshop on Public Key Cryptography*, pages 362–379. Springer, 2005. 2
8. Jae Cha Choon and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In *PKC'03*, pages 18–30. 2003. 2
9. Sherman SM Chow, Siu-Ming Yiu, and Lucas CK Hui. Efficient identity based ring signature. In *International Conference on Applied Cryptography and Network Security*, pages 499–512. Springer, 2005. 2
10. Sherman SM Chow, Siu-Ming Yiu, Lucas CK Hui, and KP Chow. Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In *International Conference on Information Security and Cryptology*, pages 352–369. Springer, 2003. 2
11. He Debiao, Chen Jianhua, and Hu Jin. An id-based proxy signature schemes without bilinear pairings. *annals of telecommunications-annales des télécommunications*, 66(11-12):657–662, 2011. 6
12. Florian Hess. Efficient identity based signature schemes based on pairings. In *SAC'03*, pages 310–324, 2003. 2
13. Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 143–154. Springer, 1996. 2
14. Sunder Lal and Prashant Kushwah. Id based generalized signcryption. *IACR Cryptology ePrint Archive*, 2008:84, 2008. 6
15. Benoit Libert and Jean-Jacques Quisquater. A new identity based signcryption scheme from pairings. In *Information Theory Workshop, 2003. Proceedings. 2003 IEEE*, pages 155–158. IEEE, 2003. 2
16. John Malone-Lee. Identity-based signcryption. *IACR Cryptology ePrint Archive*, 2002:98, 2002. 2, 6
17. Wenbo Mao. *Modern cryptography: theory and practice*. Prentice Hall Professional Technical Reference, 2003. 3
18. Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985. 3
19. Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch. An efficient strong designated verifier signature scheme. In *International conference on information security and cryptology*, pages 40–54. Springer, 2003. 2
20. S Sharmila Deva Selvi, S Sree Vivek, Dhinakaran Vinayagamurthy, and C Pandu Rangan. On the security of id based signcryption schemes. *IACR Cryptology ePrint Archive*, 2011:664, 2011. 2
21. Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO'84*, pages 47–53. Springer, 1984. 1
22. Neetu Sharma, Rajeev Anand Sahu, Vishal Saraswat, and Birendra Kumar Sharma. Adaptively secure strong designated signature. In *Progress in Cryptology–INDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings 17*, pages 43–60. Springer, 2016. 2
23. Xiaoqin Shen, Yang Ming, and Jie Feng. Identity based generalized signcryption scheme in the standard model. *Entropy*, 19(3):121, 2017. 6
24. Gang Yu, Xiaoxiao Ma, Yong Shen, and Wenbao Han. Provable secure identity based generalized signcryption scheme. *Theoretical Computer Science*, 411(40-42):3614–3624, 2010. 6
25. Yong Yu, Bo Yang, Ying Sun, and Sheng-lin Zhu. Identity based signcryption scheme without random oracles. *Computer Standards & Interfaces*, 31(1):56–62, 2009. 2

26. Bo Zhang. Cryptanalysis of an identity based signcryption scheme without random oracles. *Journal of Computational Information Systems*, 6(6):1923–1931, 2010. 2
27. Mingwu Zhang, Pengcheng Li, Bo Yang, Hao Wang, and Tsuyoshi Takagi. Towards confidentiality of id-based signcryption schemes under without random oracle model. In *Pacific-Asia Workshop on Intelligence and Security Informatics*, pages 98–104. Springer, 2010. 2

Securely outsourcing machine learning with multiple users*

Ping Li[1]✉, Hongyang Yan[2], Chong-Zhi Gao[1], Yu Wang[1],
Liaoliang Jiang[1], and Yuefang Huang[1]

[1] School of Computer Science, Guangzhou University, Guangzhou 510006, China
liping26@mail2.sysu.edu.cn
[2] College of Computer and Contorl Engeineering, Nankai University, Tianjin 300000, China
hyang.yan@foxmail.com

Abstract. In recent years, machine learning has been widely used in data analysis for predicting models, such as face/pattern recognition, image processing, simultaneous interpretation and speech recognition. However, these massive data are sensitive, which raises privacy concerns. Therefore, to protect the data privacy, in this paper, we design a scheme for securely training machine learning model on the jointed data that provided from different sources. Our scheme falls in the two-server-aided model and allows one server to conduct most of computations, and another server to provides auxiliary computation. We prove the security of our scheme in the semi-honest model.

Keywords: privacy-preserving · outsourcing computation · machine learning.

1 Introduction

Machine learning has became an indispensable tool for learning/mining knowledge from massive data in recent years. Due to the openness of cloud computing platform data resources and the clouds are not fully trusted, machine learning has aroused data privacy concerns. For example, images data, medical health data and credit recordings may contain personal sensitive items—users' face, medical history, your consumption record. If these data leaked, attackers can learn/mine some "knowledge" from these data and use "knowledge" illegally. This may lead to economic loss or personal safety. Consequently, data privacy and confidentiality is necessary to be protected when processing machine learning related outsourcing computations [1, 8, 10, 11]. One way to preserve the data privacy and confidentiality is to pre-process the data by using cryptographic methods before uploading it to the server [2, 5, 6, 9].

In this paper, we focus on machine learning model for training neural networks over combining data from different sources and utilize the two-server-aided model. There are two phases included in our proposed scheme: in the setup phase, multiple users secretly share and encrypt their data among two non-colluding and independent cloud servers; in the training phase, based on the jointed data, two non-colluding and independent

* This work was supported by Guangzhou scholars project for universities of Guangzhou (No. 1201561613).

cloud servers train neural network models and get nothing except the trained model. Specifically, the main contributions of this paper are summarized as follows:

- Our scheme is designed to conduct the data encrypted under different public keys and to preserve the data privacy of users. Users only perform the encryption/decryption operation.
- Our scheme is divided into two independent phases: setup phase and training phase. Two non-colluding cloud servers only perform the computation operation in training phase.
- To efficiently compute the active function, we use secure multi-party computation (MPC) as the key technique and the weight vector can be treated as weight matrix for multiple input vectors.

2 Preliminaries

BCP Homomorphic Encryption [4]. In this paper, to realize the privacy-preserving machine learning over the jointed data, we take the BCP cryptosystem as our encryption scheme, which consists of the following algorithms.

1) $(\mathtt{pp}, \mathtt{msk}) \leftarrow \mathsf{ParaGen}(1^\kappa)$: the parameter generation algorithm takes as input a security parameter κ, and outputs the *master key* $\mathtt{msk} = (p', q')$ and the system's *public parameters* $\mathtt{pp} = (N, k, g)$: let $N = pq$ be a safe prime RSA-modulus with bit-length κ, where $p = 2p' + 1$ and $q = 2q' + 1$ for distinct prime p' and q'. Given a value $g \in \mathbb{Z}^*_{N^2}$ with order $pp'qq'$ such that $g^{p'q'} \equiv 1 + kN \pmod{N^2}$ for $k \in [1, N-1]$.
2) $(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathsf{KeyGen}(1^\kappa)$: given a random element $a \in \mathbb{Z}_{N^2}$ and set $h = g^a \bmod N^2$, the key generation algorithm returns the public key $\mathtt{pk} = h$ and the private key $\mathtt{sk} = a$.
3) $(A, B) \leftarrow \mathsf{Enc}_{(\mathtt{pp},\mathtt{pk})}(m)$: encryption algorithm outputs a ciphertext (A, B), where $A = g^r \bmod N^2$ and $B = h^r(1 + mN) \bmod N^2$.
4) $m \leftarrow \mathsf{uDec}_{(\mathtt{pp},\mathtt{sk})}(A, B)$: user decryption algorithm returns message m as $m = \frac{\frac{B}{A^a} - 1 \bmod N^2}{N}$, or the special symbol ' $\perp'$ if it is an invalid ciphertext.
5) $m \leftarrow \mathsf{mDec}_{(\mathtt{pp},\mathtt{pk},\mathtt{msk})}(A, B)$: master decryption algorithm outputs message m or the special symbol ' $\perp'$ if it is an invalid ciphertext. Firstly, compute the user private key as $a \bmod N = \frac{h^{p'q'} - 1 \bmod N^2}{N} \cdot k^{-1} \bmod N$. Secondly, compute $r \bmod N = \frac{A^{p'q'} - 1 \bmod N^2}{N} \cdot k^{-1} \bmod N$, then set $\tau = ar \bmod N$. Finally, the massage m can be computed as $m = \frac{(\frac{B}{g^\tau})^{p'q'} - 1 \bmod N^2}{N} \cdot \alpha^{-1} \bmod N$, where k^{-1} and α^{-1} denote the inverse of $k \bmod N$ and $p'q' \bmod N$, respectively.

Pseudorandom Generator. Loosely speaking, a secure pseudorandom generator (PRG) [3] is a deterministic algorithm that expands short random seeds (with some fixed length) into much longer bit sequences that appear to be "random". In other words, the PRG is security if the output sequences of PRG on a uniformly random seed and the truly random sequences are computationally indistinguishable.

Neural networks. In general, most neural networks are constructed by groups of unites called layers: *input layer-hidden layer-output layer*. Assume that x_{ji} is the i-th input to neuron j (with corresponding weight w_{ji}). Let $net_j = \sum_i w_{ji}x_{ji}$ be the inner product of input and weight for neuron j and $f_j = f(net_j)$ be the output computed by activation function f. The target output of neuron j is y_j. The error function $E_d(\cdot)$ for the training sample d can be defined as $E_d(\mathbf{w}) = \frac{1}{2}\sum_{k\in D'}(f_k - y_k)^2$, where D' is the set of output neurons in the neural networks.

To train an acceptable weight vector, we need to modify the weight at each step according to the perceptron training rule: $w_{ji} = w_{ji} + \triangle w_{ji}$, where $\triangle w_{ji} = -\eta \frac{\partial E_d(\mathbf{w})}{\partial w_{ji}}$. To compute $\triangle w_{ji}$, two cases should be considered when handle this task:

1. Neuron j is an output neuron for the backward propagation network: the weight update rule is implemented by $\triangle w_{ji} = -\eta \frac{\partial E_d(\mathbf{w})}{\partial w_{ji}} = \eta(y_j - f_j)f_j(1-f_j)x_{ji}$.
2. Neuron j is an hidden neuron in the backward propagation network: the training rule for w_{ji} is influenced by the neurons whose direct inputs include the output of neuron j. We use D to denote all these neurons. Each element j in D, net_j can influence the outputs and the error function $E_d(\cdot)$. Therefore, $\frac{\partial E_d(\mathbf{w})}{\partial net_j} = \sum_{k\in D}\frac{\partial E_d(\mathbf{w})}{\partial net_k} \cdot \frac{\partial net_k}{\partial net_j} = \sum_{k\in D}(\frac{\partial E_d(\mathbf{w})}{\partial net_k}) \cdot (w_{kj} \cdot (f_j(1-f_j)))$. Finally, $\triangle w_{ji} = -\eta \frac{\partial E_d(\mathbf{w})}{\partial w_{ji}} x_{ji} = \eta \delta_j x_{ji}$, where $\delta_j = f_j(1-f_j)\sum_{k\in D}\delta_k w_{kj}$.

3 Problem Formulation

3.1 System Model

In this subsection, we consider a architecture of privacy-preserving machine learning over the jointed data. As illustrated in Fig.1, our system consists of three parties: Users, Clouds ($\mathscr{C}_0$ and $\mathscr{C}_1$) and a Key Generation Center (KGC).

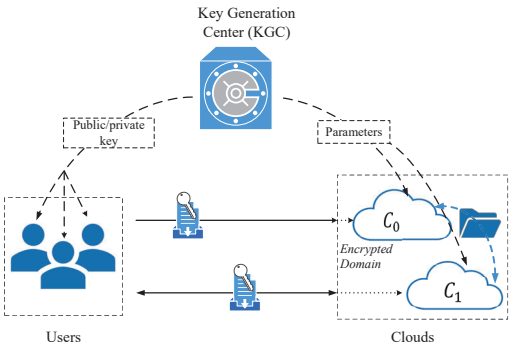


Fig. 1. Our system model under consideration

- Key Generation Center (KGC). In our system we assume that KGC is an authority entity trusted by all the parties. KGC setups the BCP cryptosystem and distributes the parameters and keys to the Clouds and Users.
- Users. Let Users be a set with n mutually distrusting users $\{\mathsf{U}_1, \mathsf{U}_2, \cdots, \mathsf{U}_n\}$. In our system, the data can be arbitrarily (i.e., vertically or horizontally) partitioned. To protect the data privacy against unauthorized access, each user secretly shares its plaintext and sends the ciphertexts of shares which encrypted under its public key to two non-colluding cloud servers.
- Clouds. Clouds are composed of two non-colluding and independent servers $\mathscr{C}_0$, $\mathscr{C}_1$. They perform several cryptographic interactive protocols with each other such that the outsourced data from Users are transformed into data encrypted under a unified pubic key. And they jointly execute a secure machine learning model by using some interactive protocols.

3.2 Security Model

To protect the data privacy and achieve the goal of privacy-preserving machine learning, we assume Users and Clouds are *semi-honest*, and require Clouds are *non-colluding* and *independent*. Specially, we stress that there is no collusion between $\mathscr{C}_0$ and $\mathscr{C}_1$, between any two of users or between any user and at most one of Clouds. In this semi-honest model, Clouds only *passively* perform the protocol and have no ability to *actively* modify the data flow. Specifically, Clouds only obtain the size of data.

3.3 Attack Model

We assume a semi-honest adversary $\mathscr{A}$ who may obtain the plaintext of Users with the following abilities: (i) $\mathscr{A}$ may corrupt any subset of Users to obtain all plaintexts belonging to Users; (ii) $\mathscr{A}$ may corrupt $\mathscr{C}_0$ (or $\mathscr{C}_1$) to achieve plaintext of all outsourced data from the Users.

4 Privacy-preserving Machine Learning

Assume that Users is a set of n mutually distrusting users $\mathsf{U}_1, \mathsf{U}_2, \cdots, \mathsf{U}_n$, where each user U_i has its privacy data m_i and public/private key $(\mathtt{pk}_i, \mathtt{sk}_i)$, $i = 1, 2, \cdots, n$. To get some "knowledge " from the jointed data of Users and protect each user's data privacy, our solution can be divided into two phases:

Set up phase: 1) Initially, KGC sets up BCP cryptosystem and generates $(\mathtt{pp}, \mathtt{msk})$ and $(\mathtt{sk}, \mathtt{pk})$ by running ParaGen and KeyGen, respectively. For the private key $\mathtt{sk}$, KGC divides it into n pieces $\mathtt{sk} = \mathtt{sk}_1 + \cdots \mathtt{sk}_n$, where $\mathtt{sk}_i$ $(i \in [1, n])$ is chosen uniformly at random from the key space of BCP cryptosystem. KGC computes $\mathtt{pk}_i = g^{\mathtt{sk}_i} \bmod N$ and distributes $(\mathtt{pp}, (\mathtt{pk}_i, \mathtt{sk}_i))$ $(i \in [1, n])$ to U_i. At the same time, KGC sends $(\mathtt{pp}, \mathtt{msk})$ and pp to cloud $\mathscr{C}_0$ and $\mathscr{C}_1$, respectively. 2) After receiving pp and $(\mathtt{pk}_i, \mathtt{sk}_i)$, each user U_i uses PRG generates a pseudorandom number R_i, let $m_{i0} = R_i$ and $m_{i1} = m_i - R_i$. Then, U_i uploads $c_{i0} = \mathsf{Enc}_{(\mathtt{pp}, \mathtt{pk}_i)}(m_{i0})$ and $c_{i1} = \mathsf{Enc}_{(\mathtt{pp}, \mathtt{pk}_i)}(m_{i1})$ to the cloud $\mathscr{C}_0$ and $\mathscr{C}_1$, respectively, where $m_i = m_{i0} + m_{i1}, i = 1, 2, \cdots, n$.

After the set up phase, $\mathscr{C}_0$ and $\mathscr{C}_1$ have collected a part of outsourced data from different users respectively. Right now, $\mathscr{C}_0$ and $\mathscr{C}_1$ can jointly perform some cryptographic interactive protocols such that the data encrypted under different public keys transformed into data encrypted under the unified public key. This is due to the fact that MPC only works for encryptions under the same public key. After executing the transformation protocol, $\mathscr{C}_0$ and $\mathscr{C}_1$ can learn/train machine learning by some cryptographic interactive protocols in the training phase.

Training phase: The key operation in this phase is the computation of the activation functions. Since the BCP cryptosystem is additive homomorphic encryption, we need the activation functions only including the operation of addition and multiplication, so they can be computed over the ciphertext domain.

In the existing literatures, lots of works use polynomial approximation to compute the activation function, such as [13, 14] applied a low-degree polynomial function to approximate the sigmoid function. However, the low-degree (3 or 5) polynomial approximation is still high to be used with HE schemes, since the computational complexity and accuracy is depend on this degree.

In this work, we take rectified linear unit (ReLU) function $g(z) = max\{0, z\}$ [7, 12] as activation function, since the ReLU function is nearly linear. We only need to compare the size of 0 and z over the ciphertext domain.

After all computations are done, each user retrieves the encrypted output of the $\mathscr{C}_1$ and decrypts jointly with its respective private key.

4.1 Security analysis

The security analysis is considered in the semi-honest model, meaning that every protocol parties are honestly follow the protocol but try their best to analyze or infer the data flow to learn additional information about other parties' inputs, intermediate results and output results by gathering the protocols transcripts. Recall that some cryptographic interactive protocols between $\mathscr{C}_0$ and $\mathscr{C}_1$ are executed depending on the "blinding-the-message" techniques.

We require the adversary $\mathscr{A}$ has the polynomial bounded of computing power, since the BCP cryptosystem guarantees the semantic security in the semi-honest model. $\mathscr{A}$ may corrupt any subset of Users to obtain their ciphertext, however, $\mathscr{A}$ will not be able to decrypt the ciphertext without knowing the corrupted Users' private key due to the semantic security of the BCP cryptosystem. $\mathscr{A}$ may compromise $\mathscr{C}_0$ (or $\mathscr{C}_1$) to achieve the ciphertext and private data of Users. However, $\mathscr{A}$ is unable to recover the Users's private key to decrypt the ciphertext, because the message is pre-processed by splitting into two pieces, where one piece is a pesudorandom number and another price is the message reduce a pesudorandom number. $\mathscr{C}_0$ holds the master key and only obtains a pesudorandom number after decrypting; $\mathscr{C}_1$ only gets a blinded message (the message reduce a pesudorandom number) without leaking the message information.

5 Conclusion and Further Work

In this paper, we have proposed a scheme for securely training machine learning model while supporting that uses inputs data are learned by the accessed servers. In our

scheme, users split their data into two parts and encrypt each split data with different pubic keys and outsource the ciphertexts to two servers. The servers can transform the data encrypted under different public keys into data encrypted under the same public key. Based one the transformed data, servers can perform a secure machine learning algorithm without leaning any private information. Our scheme can be applied in real-word collaborated learning, and we expect to improve the efficiency and give a comprehensive application in further work.

References

1. Abadi, M., Goodfellow, I., Goodfellow, I., Mcmahan, H.B., Mironov, I., Talwar, K., Zhang, L.: Deep learning with differential privacy. In: ACM Sigsac Conference on Computer and Communications Security. pp. 308–318 (2016)
2. Aono, Y., Hayashi, T., Wang, L., Moriai, S.: Privacy-preserving deep learning via additively homomorphic encryption. IEEE Transactions on Information Forensics & Security **13**(5), 1333–1345 (2018)
3. Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudo-random bits. In: Foundations of Computer Science, 1982. Sfcs '08. Symposium on. pp. 112–117 (2008)
4. Bresson, E., Catalano, D., Pointcheval, D.: A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications pp. 37–54 (2003)
5. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., Wernsing, J.: Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In: International Conference on Machine Learning. pp. 201–210 (2016)
6. Graepel, T., Lauter, K., Naehrig, M.: Ml confidential: Machine learning on encrypted data. In: International Conference on Information Security and Cryptology. pp. 1–21. Springer (2012)
7. Hesamifard, E., Takabi, H., Ghasemi, M.: Cryptodl: Deep neural networks over encrypted data. arXiv preprint arXiv:1711.05189 (2017)
8. Li, P., Li, J., Huang, Z., Gao, C.Z., Chen, W.B., Chen, K.: Privacy-preserving outsourced classification in cloud computing. Cluster Computing **21**(1), 1–10 (2017)
9. Li, P., Li, J., Huang, Z., Li, T., Gao, C.Z., Yiu, S.M., Chen, K.: Multi-key privacy-preserving deep learning in cloud computing. Future Generation Computer Systems **74**, 76–85 (2017)
10. Li, T., Huang, Z., Li, P., Liu, Z., Jia, C.: Outsourced privacy-preserving classification service over encrypted data. Journal of Network & Computer Applications **106**, 100–110 (2018)
11. Li, T., Li, J., Liu, Z., Li, P., Jia, C.: Differentially private naive bayes learning over multiple data sources. Information Sciences **444**, 89–104 (2018)
12. Mohassel, P., Zhang, Y.: Secureml: A system for scalable privacy-preserving machine learning. In: In 2017 38th IEEE Symposium on Security and Privacy. pp. 19–38 (2017)
13. Yuan, J., Yu, S.: Privacy preserving back-propagation neural network learning made practical with cloud computing. IEEE Transactions on Parallel and Distributed Systems **25**(1), 212–221 (2014)
14. Zhang, Q., Yang, L.T., Chen, Z.: Privacy preserving deep computation model on cloud for big data feature learning. IEEE Transactions on Computers **65**(5), 1351–1362 (2016)

Lattice-Based Simulatable VRFs: Challenges and Future Directions

Carlo Brunetta, Bei Liang, and Aikaterini Mitrokotsa

Chalmers University of Technology, Gothenburg, Sweden
{brunetta,lbei,aikmitr}@chalmers.se

Abstract Lattice-based cryptography is evolving rapidly and is often employed to design cryptographic primitives that hold a great promise for being post-quantum resistant and can be employed in multiple applications such as: e-cash, unique digital signatures, non-interactive lottery and others. In such application scenarios, a user is often required to prove non-interactively the correct computation of a pseudo-random function $F_k(x)$ without revealing the secret key k used. Commitment schemes are also useful in such application settings to commit to a chosen value, while keeping it hidden to others but being able to reveal the committed value later. In this short paper, we provide our insights on constructing a *lattice-based simulatable verifiable random function (sVRF)* and point out the main challenges that need to be addressed in order to achieve it.

Keywords: Dual-Mode Commitment Scheme, Lattice-based Cryptography, Non Interactive Zero Knowledge Arguments, Pseudo Random Functions, Verifiable Random Functions

1 Introduction

Zero-knowledge (ZK) proofs [14] are employed to prove the knowledge of secret information while preserving provers privacy with respect to a NP language. Depending on whether the zero-knowledge proof is performed interactively or not, we may have *interactive* or *non-interactive* protocols; while the latter are more efficient regarding communication costs.

Pseudo-random functions (PRFs) [10] are a very useful cryptographic primitive that is often employed in combination with *zero-knowledge* proofs in multiple application scenarios. Let us consider a general scenario: a prover $\mathcal{P}$ wants to prove to a verifier $\mathcal{V}$ the knowledge of a secret $\boldsymbol{w}$ and the correct computation of a PRF $F_{\boldsymbol{w}}$ on the input x, *i.e.,* $F_{\boldsymbol{w}}(x)$. A rather important question is:

How may $\mathcal{P}$ prove to $\mathcal{V}$ the correct evaluation of the PRF $F_{\boldsymbol{w}}(x)$ without leaking any information about $\boldsymbol{w}$, just by providing a proof π?

We consider the case where the communication between $\mathcal{P}$ and $\mathcal{V}$ should be **non**-interactive, *i.e.,* $\mathcal{P}$ needs to provide $\mathcal{V}$ all the necessary information to verify the correct computations in a single step.

The above stated question can be solved by employing a *verifiable random function* (VRF) [16]. A VRF is a PRF with two additional algorithms; one

algorithm that is able to generate a proof π of the correct computation of the PRF $F_{\boldsymbol{w}}(x)$ as well as a *verification* algorithm.

Recent papers [11,8] use the VRF into a *blockchain* context in order to either define a *fair and verifiable lottery* in which the winner will publish the next block, or as a way to generate a *"common and shared random string"* which can be seen as an equivalent of the CRS model.

Finding these study cases is extremely important to motivate the community to research and further develop primitives that allows scenarios where *verification* or *providing a proof* is a mandatory step.

Although algebraic pseudo-random functions and ZK proofs are well studied primitives, they have received limited attention in lattice settings; furthermore, to the best of our knowledge, *building lattice-based VRFs is an open problem.*

Lattice-based cryptographic primitives [1,18], mainly rely on the *learning with errors* (LWE) and the *short integer solution* (SIS) problems; they are quite promising for providing post-quantum resistance guarantees, while also offering simpler arithmetic operations and thus, important efficiency guarantees.

Designing a lattice-based VRF is a challenging and currently open problem since it requires a non-interactive proof in the standard model. As a step towards this direction, in this short paper, we provide our insights on designing a lattice-based *simulatable VRF* (sVRF), originally introduced by Chase and Lysyanskaya [6]. Informally, an sVRF is a VRF defined in a public parameter model, such as the *common random string* (CRS) model, which implies the existence of honest common parameters on the top of the standard VRF system. More precisely, besides the usual algorithms in a VRF there is an additional parameter generation algorithm which takes as input the security parameters and output the public parametrs pp. Both the input domain and output range of the sVRF depend on pp. Meanwhile, pp is included in the inputs for all the algorithms KeyGen, Eval, Prove and Verify. Moreover, except of the uniqueness and pseudorandomness properties, sVRFs should also satisfy *simulatability* which is a novel property making them different from VRFs. Simulatability states that there exists a simulator that is able to simulate the common parameters such that, corresponding to a verification key, for any x, y, it is possible to produce a proof π that $F(sk, x) = y$. The simulated transcription is required to be indistinguishable from the values computed from the parameters that are generated honestly. In this paper, we describe our insights on constructing an sVRF when relying on Libert *et al.*'s [14] method to prove zero-knowledge arguments for lattice-based PRFs. Furthermore, we describe the main challenges that need to be addressed in order to construct a lattice-based sVRF using this method.

1.1 A Roadmap to Lattice-based sVRFs

Chase and Lysyanskaya's [6] provided a general construction of sVRFs from a perfectly binding computational hiding non-interactive commitment scheme and an unconditionally-sound multi-theorem NIZK for NP. Their main idea is to use a multi-theorem NIZK to generate the proof for a statement that the public verification key is a commitment of the secret key and the function

value is the correct result on the input applied to the secret-keyed PRF, *i.e.*, $\mathsf{pk} = \mathsf{Com}(\mathsf{sk}; r) \wedge y = F(\mathsf{sk}, x)$. However, such solution is based on a general assumption, in order to come up with a lattice-based sVRF, we should specify a lattice-based PRF scheme.

Fortunately, thanks to the very recent significant results of Boneh *et al.* [4] who proposed a LWE-based key homomorphic PRFs as well as Libert *et al.*'s [14] three round zero-knowledge arguments of correct evaluation for the LWE-based PRF Boneh *et al.* [4] w.r.t committed keys and inputs, it is possible to obtain a non-interactive solution of $y = F(\mathsf{sk}, x)$ as the correct evaluation of a PRF for a secret input x and a committed key sk, and yielding a sVRF furthermore.

Libert *et al.* have significant contributions [14,12,13] in the area of designing efficient zero-knowledge proofs for lattice-related language. For instance, Libert *et al.* [12] considered how to construct zero-knowledge arguments of knowledge of a secret matrix X and vectors $\boldsymbol{s}, \boldsymbol{e}$ such that for a public vector $\boldsymbol{b}$ it holds $\boldsymbol{b} = \boldsymbol{X} \cdot \boldsymbol{s} + \boldsymbol{e} \bmod q$. Libert *et al.* [13] also investigated in the lattice setting how to design zero-knowledge arguments for the statement that c_x, c_y and c_z are the commitments to the polynomial-size bit-strings x, y and z which are the binary representations of large integers X, Y, Z satisfying certain algebraic relations such as $Z = X + Y$ and $Z = X \cdot Y$.

In order to obtain zero-knowledge arguments for the correct evaluation of key-homomorphic PRF [1] of Boneh *et al.* [4] , Libert *et al.* [14] presented an useful abstraction of Stern's protocol [19] and they modified the Boneh *et al.*'s lattice PRF [4] in order to efficiently prove the correct computation of the PRF interactively, while providing zero-knowledge guarantees.

As stated in their paper, it is possible to obtain the first non-interactive lattice-based zero-knowledge protocol by directly applying the Fiat-Shamir transformation [9]. The main issue with this choice is that the Fiat-Shamir transformation is secure in the *Random Oracle Model* (ROM) which is against the original sVRF definition [6].

Thus, our main research objective is to find an appropriate transformation from ZK to NIZK, defined over lattices, not relying on the ROM. In Figure 1, we depict two different strategies in order to obtain a lattice-based sVRF: either by directly transforming Libert *et al.*'s ZK argument or by providing a different lattice-based ZK PRF proof system and applying a ZK to NIZK transformation and then the Chase-Lysyanskaya's transformation from NIZK to sVRF.

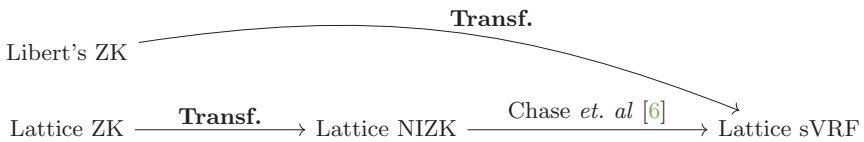


Figure 1. Roadmap to lattice-based sVRF. In **bold**, this paper's main research focus.

[1] Namely demonstrating knowledge of a committed secret key $\boldsymbol{k}$, a secret input $\boldsymbol{J}$ and an output $\boldsymbol{y}$ satisfying $\boldsymbol{y} = F_{\boldsymbol{k}}(\boldsymbol{J})$

2 Applying Lindell's Tranformation

In this section we provide our finding when defining a sVRF based on Libert's ZK argument and the Lindell's transformation [15]. We explain our discoveries and challenges.

We considered Lindell's transformation [15] from any sigma-protocol into a corresponding NIZK protocol. In contrast to Fiat-Shamir's transformation [9], Lindell's transformation does not require the random oracle model; more precisely, in Lindell's transformation the *zero-knowledge* property holds in the *common reference string* (CRS) model, while in order to achieve *soundness*, the used hash function is modeled as a *non-programmable* random oracle [17].

In order to adopt Lindell's transformation an important requirement is that of a *dual-mode* commitment scheme.

The main concept of a commitment scheme is that it is possible to secretly fix some message m that it is used in a protocol and in a second phase, open the commitment and therefore prove the correct knowledge or possession of the specific message m. Designing lattice-based commitment schemes has already received some attention in the literature [3,2].

The *dual-mode* represents the possibility to sample a statement in a language L via a bit b and use the commitment scheme in a *binding* way, *i.e.*, a commitment c can be decommitted in a *unique* message m, or in a *"trapdoor"* way, *i.e.,* that with some secret witness $\boldsymbol{w}$, it is possible to decommit c to any message m'.

Therefore, the main property required for a dual-mode commitment scheme is that it is impossible to distinguish how the bit b is selected and therefore impossible to know if we are decommitting to the original message or we are using the trapdoor to decommit to an arbitrary message.

A *dual-mode commitment scheme* represents a specific type of commitment schemes that are equivalently defined by Catalano and Visconti as *hybrid commitment schemes* [5].

As described in [15], in order to define a dual-mode commitment scheme, Lindell requires a *membership-hard efficient-sampling language* defined as:

Definition 1 (Membership-hard with Efficient Sampling [15]). *Let L be a language. L is* membership-hard with efficient sampling *(MHES) if there exists a probabilistic polynomial-time sampler S_L such that for every probabilistic polynomial-time distinguisher D there exists a negligible function $\mu(\cdot)$ such that:*

$$|\mathsf{Pr}(D(S_L^x(0,1^n),1^n)=1) - \mathsf{Pr}(D(S_L(1,1^n),1^n)=1)| \leq \mu(n)$$

where $S_L(b,\cdot)$ is a sampler that returns an instance in the language L if $b=0$ and an instance not in the language L if $b=1$. S_L^x denotes only the instance without the witness.

In a nutshell, the MHES language L is a language in which it is hard to distinguish if an efficient sampling algorithm S_L sampled the statement x in the

language L or not: it is hard to decide the membership of $x \in L$ but it is easy to sample x in the language (or not).

In summary, in order to build an sVRF while employing the Lindell's transformation, the main building blocks required are depicted in Figure 2.

Figure 2. Roadmap to Lindell's transformation.

By assuming the hardness of the *inhomogeneous short integer solution* (ISIS) problem, if we follow the idea and structure of the DDH language construction proposed by Lindell [15] in order to define the language L_{IS} of Eq. (1), the result is unfortunately not MHES for common lattice security parameters.

$$L_{\mathsf{IS}} \coloneqq \{(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{u}, \boldsymbol{v}) \mid \boldsymbol{A}, \boldsymbol{B} \in {\mathbb{Z}_p}^{n \times m}, \tilde{\boldsymbol{w}} \in \{0,1\}^m, \boldsymbol{u} = \boldsymbol{A}\tilde{\boldsymbol{w}}, \boldsymbol{v} = \boldsymbol{B}\tilde{\boldsymbol{w}}\}. \quad (1)$$

This is the case since whenever we provide a statement not in the language $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{u}, \boldsymbol{v}) \notin L_{\mathsf{IS}}$, it exists in fact a statement $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}\tilde{\boldsymbol{w}}', \boldsymbol{A}\tilde{\boldsymbol{w}}') \in L_{\mathsf{IS}}$ in the language for some $\tilde{\boldsymbol{w}}'$. Therefore it cannot be used to define a dual-mode commitment scheme mainly because the commitment scheme will not be perfectly binding, which is a necessary condition in order to use Lindell's transformation.

3 Challenges and Future Directions

In this section we will briefly discuss and collect our conjectures and/or our future research directions by dividing them into into two major classes: a first class of questions related to *transformations* from ZK to NIZK and a second class of challenges regarding *lattice languages*.

3.1 ZK Transformations

Choosing Lindell's transformation is not optimal for the final goal of constructing an sVRF since the transformation is defined in the non-programmable ROM.

Ciampi *et al.* [7] modified and improved Lindell's transformation: the transformation does not require the non-programmable random oracle *nor* a perfectly binding commitment scheme at the cost of a more specific language. By using Ciampi *et al.*'s transformation, it might be possible to obtain a ZK to NIZK transformation not based on the ROM.

Challenge 1 *Is it possible to use Ciampi* et al. *transformation in our sVRF construction-idea? The main challenge of this approach is to check if any lattice-based language can be defined in order to fulfil the transformation hypothesis and requirement.*

With the same spirit, we find an additional challenge of more general interest: a ZK to NIZK transformation that is not defined in the random oracle model (or any similar ones). Therefore, we state as a general challenge for future investigation:

Challenge 2 *Are there any other transformations in the literature that can be used for our construction-idea? Are they efficient? How do they compare among themselves or with respect to the Fiat-Shamir's transformation?*

3.2 Lattice Languages

When considering the Lindell's transformation, the language L_{ls} is ill-defined and therefore cannot be used in order to build a dual-mode commitment scheme. Furthermore, the language challenge of defining a membership-hard language can be seen as of perpendicular interest.

Challenge 3 *Is there a way to define a lattice-based membership-hard efficient sampling language L that can be used to define a dual-mode commitment scheme?*

Generally speaking and quite informally, the main obstacle is finding *"good"*-languages that have a *"unique-witness"*. This means that it would be incredibly useful to find a lattice-language L in which the witness of a statement $x \in L$ is unique. Solving this problem will open new direction in lattice based cryptography.

Challenge 4 *Find a lattice-based language L in which every statement $x \in L$ has a unique witness w.*

As a different but related problem, if we consider a different ZK PRF proof system, the ZK language used for our construction-idea requires an additional property in order to be used by the Chase-Lysyanskaya's transformation. The ZK system has to be able to prove the correct computation of the PRF **and** the correctness of an additional commitment. It has to be defined over lattices **and**, after transforming it with the best ZK to NIZK transformation possible, the obtained NIZK has to be multi-theorem.

Challenge 5 *Given the best ZK transformation, find a ZK PRF argument/proof system that can be used for the Chase-Lysyanskaya's transformation.*

Acknowledgement. We really thank the anonymous reviewers for their insightful comments, suggestions, discussions and the new literature-direction that we can now explore. This work was supported by the the Swedish Research Council (Vetenskapsrådet) through the grant PRECIS (621-2014-4845).

References

1. Ajtai, M.: Generating Hard Instances of Lattice Problems (Extended Abstract). In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. pp. 99–108. STOC '96, ACM, New York, NY, USA (1996), http://doi.acm.org/10.1145/237814.237838
2. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More Efficient Commitments from Structured Lattice Assumptions. Tech. Rep. 997 (2016), https://eprint.iacr.org/2016/997
3. Benhamouda, F., Krenn, S., Lyubashevsky, V., Pietrzak, K.: Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings. In: Proceedings, Part I, of the 20th European Symposium on Computer Security – ESORICS 2015 - Volume 9326. pp. 305–325. Springer-Verlag New York, Inc., New York, NY, USA (2015), http://dx.doi.org/10.1007/978-3-319-24174-6_16
4. Boneh, D., Lewi, K., Montgomery, H., Raghunathan, A.: Key Homomorphic PRFs and Their Applications. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013. pp. 410–428. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
5. Catalano, D., Visconti, I.: Hybrid Commitments and Their Applications to Zero-knowledge Proof Systems. Theor. Comput. Sci. 374(1-3), 229–260 (Apr 2007), http://dx.doi.org/10.1016/j.tcs.2007.01.007
6. Chase, M., Lysyanskaya, A.: Simulatable VRFs with Applications to Multi-theorem NIZK. In: Advances in Cryptology - CRYPTO 2007. pp. 303–322. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (Aug 2007), https://link.springer.com/chapter/10.1007/978-3-540-74143-5_17
7. Ciampi, M., Persiano, G., Siniscalchi, L., Visconti, I.: A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography. pp. 83–111. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
8. David, B., Gaži, P., Kiayias, A., Russell, A.: Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018. pp. 66–98. Lecture Notes in Computer Science, Springer International Publishing (2018)
9. Fiat, A., Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology — CRYPTO' 86, vol. 263, pp. 186–194. Springer Berlin Heidelberg, Berlin, Heidelberg (2006), http://link.springer.com/10.1007/3-540-47721-7_12
10. Goldreich, O., Goldwasser, S., Micali, S.: How to Construct Random Functions. J. ACM 33(4), 792–807 (Aug 1986), http://doi.acm.org/10.1145/6490.6503
11. Li, W., Andreina, S., Bohli, J.M., Karame, G.: Securing Proof-of-Stake Blockchain Protocols. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology, vol. 10436, pp. 297–315. Springer International Publishing, Cham (2017), http://link.springer.com/10.1007/978-3-319-67816-0_17
12. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 101–131. Springer (2016)
13. Libert, B., Ling, S., Nguyen, K., Wang, H.: Lattice-based zero-knowledge arguments for integer relations. In: Annual International Cryptology Conference. pp. 700–732. Springer (2018)

14. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash. In: Asiacrypt 2017. LNCS, Springer, Hong Kong, China (Dec 2017), https://hal.inria.fr/hal-01621027
15. Lindell, Y.: An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle. In: Dodis, Y., Nielsen, J.B. (eds.) Theory of Cryptography, vol. 9014, pp. 93–109. Springer Berlin Heidelberg, Berlin, Heidelberg (2015), http://link.springer.com/10.1007/978-3-662-46494-6_5
16. Micali, S., Rabin, M., Vadhan, S.: Verifiable random functions. In: 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039). pp. 120–130 (1999)
17. Nielsen, J.B.: Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. In: Goos, G., Hartmanis, J., van Leeuwen, J., Yung, M. (eds.) Advances in Cryptology — CRYPTO 2002, vol. 2442, pp. 111–126. Springer Berlin Heidelberg, Berlin, Heidelberg (2002), http://link.springer.com/10.1007/3-540-45708-9_8
18. Peikert, C.: A Decade of Lattice Cryptography. Foundations and Trends® in Theoretical Computer Science 10(4), 283–424 (2016), http://www.nowpublishers.com/article/Details/TCS-074
19. Stern, J.: A new paradigm for public key identification. IEEE Transactions on Information Theory 42(6), 1757–1768 (Nov 1996)

An SDN-based Secure Mobility Model for UAV-Ground Communications

Rajesh Kumar[1]*, Mohd. Abuzar Sayeed[1], Vishal Sharma[2], Ilsun You[2]

[1]CSED, TIET, Patiala, Punjab, India-147004,
[2]Information Security Engineering, Soonchunhyang University, South Korea-31538,
rakumar@thapar.edu, abuzar.sayeed@gmail.com,
vishal_sharma2012@hotmail.com, ilsunu@gmail.com

Abstract. Multi-UAV collaborative networks provide with the opportunity to exploit civil, chemical, biological, radiological, nuclear and geographical reconnaissance, survey, management, and control. For the collaborative network formation, coverage is of prime paramountcy. Alongside coverage, possession of information and communication security is withal a major challenge. The coverage quandary can be resolved by a perspicacious selection of UAV waypoints. But the security paradigm which can be an effect of faulty node, intrusion or even choice of erroneous communication channels needs to be taken care of through efficacious strategies. Consequently, both a specialized UAV mobility model and a security mechanism are required in order to establish prosperous collaborative networks. In this article, an SDN-based secure mobility model is proposed which takes into account the topological density and restricts the UAV and ground node (Wireless Sensor Networks (WSNs)) transmissions to authenticity. Significant gains are observed for throughput, coverage, and latency by establishing a simulated network between multiple UAVs and WSN motes.

Keywords: UAVs · Mobility Model · SDN · Security · WSNs.

1 Introduction

Unmanned Aerial Vehicles (UAVs) are autonomous flying nodes which are either pre-programmed or controlled via a ground station. UAVs have found application in scientific, research, civilian and military applications as a result of the flexibility and ease of deployment. UAVs have taken the cooperative networks to a new level. The cooperation between ground and aerial nodes has resulted in significant gains in data dissemination, monitoring, and control over strategic locations [1]. UAVs also prove significant when it comes to data gathering from inaccessible locations. One such case is autonomous networking where UAVs help uplifting the problem of coverage, failures, limiting guidance and dead nodes by acting as supervisors [2–7]. Efficient and intelligent surveying is one of the key aspects of UAV networks. Nature-based algorithms like Hill Myna and Desert Sparrow optimizations (HMADSO) performs cooperative rendezvous and efficient task allocation [8]. Cooperative ground and air surveillance mechanisms

utilize UAVs for a broad coverage and ground nodes for a detailed zoom in picture of the area surveillance as studied in [9] [10] [11]. In [12], the multi-hop characteristics of WSN data transmission were replaced by direct communication between UAV and sensor nodes where UAVs served as sinks. Efficient deployment of available resources can help improve the coverage and reduce the number of hops for boosting the overall throughput [13], [14].

Wireless Sensor Networks (WSNs) are spatially dispersed energy concentric dedicated sensor nodes largely deployed in inaccessible locations [15]. WSNs are energy sensitive devices and suffer from a constant depletion. Together with path selection, the multi-hopping produces un-necessary traffic, delays and packet drops. With a general deployment in sensitive areas the transmission carried to or from UAV is of prime importance for UAVs-WSNs communications. These collaborative networks involve threats in the form of UAVs communicating with non-authentic ground nodes. Such a problem becomes gross when ground and aerial nodes are allowed to communicate without coordination and authentication. Another scenario involves UAVs communicating with a faulty aerial node. These types of issues can be resolved through efficient mobility model.

Mobility model defines a movement scheme which mimics the real world movements, traffic and response scenarios. One key characteristic of a good mobility model is its ability to adapt to the dynamically changing network behavior [16]. The coordination between WSN and UAV nodes is characterized by the erratic and dynamic behavior of the networks. Vehicular models like Synthetic, Survey and Simulation-based approaches don't suffice as the inherent inconsistencies of the erratic network behavior hinder the overall mathematical formulation of the scenario as well as the survey and simulation of every single scenario is not feasible. Trace-based models don't suffice under disaster condition, military applications, unforeseen events and even under extreme security requirements [17] [18].

In this paper, a Software Defined Network (SDN) [19] controller based mobility model for communication between Multi-UAV and WSNs is introduced. SDN is effectively a new paradigm in the field of computer networks which separates data forwarding from the control logic thus facilitating better flexibility, scalability, and dynamic adaptability. The SDN controller provides with the opportunity to update flows on the move, thus, adapting to the dynamic topology, and also updates the legal moves as well as node authentication by means of pre-installed flow tables [19]. Mobility model for multi-UAV WSN networks is proposed which takes into account the attraction factor for setting up the waypoints for UAV movements. The authentication is performed on the basis of pre-installed flows. The pre-installed flow table of the UAV is constantly updated with the changing topology. The controller-generated dynamic waypoints prevent UAV from erratic movements as well as any unidentified transmission is discarded based on the flow action rules. The proposed approach is compared against the traditional Clustered Hierarchical WSN layout [20] with UAVs as sinks and against a technique where UAV maneuvers are statically fixed before the flight.

2 Proposed Approach

This article presents a secure SDN-based mobility model for Multi-UAV coordinated WSN networks. The complete geography is divided into a matrix. The WSN nodes falling into a particular sector (block of the matrix) are default considered into the same cluster. In the given model, the selection of controller and cluster head is done as

$$\min(D_m) \text{ and } \max(\mathcal{L}), \forall \mathcal{N}, \tag{1}$$

s.t.

$$\begin{aligned} \mathcal{L}_A &> 0, \\ \tau_s &\geq Mean(\tau_{\mathcal{N}}), \end{aligned} \tag{2}$$

where $\mathcal{L}$ refers to the set containing the total connections for nodes, $\mathcal{L}_A$ is the number of connections active on a node, τ_s is the mean life time of the selected node, and $\tau_{\mathcal{N}}$ refers to the mean life time of $|\mathcal{N}|$ nodes, D_m is the average one hop distance for nodes represented with a set $\mathcal{N}$, which is given as the distance metric, such that,

$$D_{m_i} = \frac{\sum_{i=1}^{S_n} \mathcal{H}}{S_n}, S_n \leq |\mathcal{N}|, \tag{3}$$

D_{m_i} is the node under consideration, $\mathcal{H}$ is one hop distances from the node under consideration with S_n being the active nodes, given that the node coordinates lie within the same sector as that of the base station. For the model to proceed further,

$$0 \leq D_{m_i} \leq \frac{S_n\,(S_n - 1)}{2\mathcal{N}}, \tag{4}$$

where the extreme values are expressed as:

$$D_{m_i} = \begin{cases} 0, D_m^{(selected)} = \text{ infinite}, \mathcal{L} = \min, \tau_s = \max, \text{ Isolated } = True \\ \frac{S_n(S_n-1)}{2\mathcal{N}}, D_m^{(selected)} = \max, \mathcal{L} = \max, \tau_s = \min, \text{ Isolated } = False \\ \text{Otherwise, Select.} \end{cases} \tag{5}$$

The controller suggested in the paper has six major components namely; Mission control, UAV topology map, active topology, Density Function for Route Establishment (DFRE), flow Table, and logs.

Mission control component of the UAV Controller keeps track of the overall mission statistics and conceptual layout of the system. The information includes cell structure, information about the geography. The main function is to provide preliminary information to the UAV topology map. Active topology component stores the current UAV movement statistics and functions which dictate the overall movement criterion and geometric characteristics of the flight path. Active topology also forwards the overall sensed statistics of the geographical area to the UAV topology map. The UAV topology map component serves as data storage for mission control and active topology components.

DFRE works on the stored statistics to find an efficient and viable route for the UAVs. Once the complete area is surveyed, the component starts with calculating the density component of respective areas. Fig. 1 presents the block diagram of the SDN controller used by the proposed model for coordinating UAVs with WSNs over a defined geographical area.

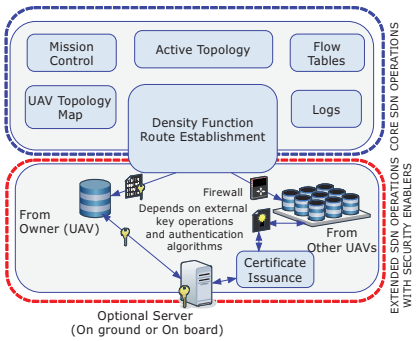


Fig. 1: A component diagram of the considered SDN Controller for UAV-WSN coordinations.

The transfer between UAV and sensor nodes always happens through the cluster-head. When UAV is in range of the cluster head the Head Swap are performed for inter-changing the cluster heads. UAV becomes the cluster head of the sector to facilitate transfer not only from the designated cluster head but also allows the cluster members to send data directly towards the UAV. The UAV waypoints are set in a way that it moves from head of one densely populated cluster towards the head of another densely populated cluster. UAV waypoints are decided on the basis of topological density and distance. The transmissions are facilitated by coordination function, which is calculated by means of topological density as follows:

$$A_f = \frac{S_a}{\mathcal{A}} \times \frac{S_n}{\mathcal{N}} \left(\sqrt{\frac{1}{|\mathcal{N}|} \left(T_{psys} - \overline{T_{psys}} \right)^2} - \sqrt{\frac{1}{S_n} \left(T_p - \overline{T_p} \right)^2} \right) \tag{6}$$

where T_p is the number of transmissions per unit time in a sector, S_a denotes the sector area, and $T_{p_{sys}}$ is the number of transmissions per unit time in the entire system.

Similarly, this model can be extended to calculate the coordination of each sector as well as the entire zone while fixating the number of transmissions permissible to each node, each sector and each area under the control of a single base station.

After estimating the coordination function of each region, the DFRE further prioritizes the areas of interest as dense and scarce. The inequality in (7) iden-

tifies the densely populated clusters from the scares ones based on the average hop distances of the area, such that,

$$1 \leq \mathcal{A}_{range} \leq \frac{\mathcal{N}(\mathcal{N}-1)}{2}, \tag{7}$$

which can be evaluated as:

$$Area = \begin{cases} \text{Dense, if,} \left(\frac{\min(S_n)-mean(S_n)}{2}\right) < \mathcal{A}_{range} \leq \frac{\mathcal{N}(\mathcal{N}-1)}{2} \\ \text{Sparse, if,} 1 \leq \mathcal{A}_{range} \leq \left(\frac{\min(S_n)-mean(S_n)}{2}\right) \\ \text{Normal, Otherwise.} \end{cases} \tag{8}$$

With all the areas mapped, the DFRE component now performs the weight assignment in order to proceed with the shortest route selection procedure. The model uses a network graph for coordination in which the edge weights between the nodes are given by:

$$E_w = \frac{T_{psys}\eta_1 + |\mathcal{N}|\eta_2}{\eta_1\eta_2} - \frac{T_p\eta_3 + S_n\eta_4}{\eta_3\eta_4}, \tag{9}$$

where η_1, η_2, η_3, and η_4 are the balancing constants for T_{psys}, $\mathcal{N}$, T_p, and S_n, respectively, such that $\eta_1 + \eta_2 = 1$ and $\eta_3 + \eta_4 = 1$ with $\eta_1 \neq 0$, $\eta_2 \neq 0$, $\eta_3 \neq 0$, and $\eta_4 \neq 0$.

The densely populated sectors are serviced by UAV maneuvers directly along with the sectors which fall in line to two consecutive UAVs. The scarce sectors which don't fall in the path of UAV are the designated as isolated zones. These isolated zones fixate on sensors, which send hello packets towards nearby dense regions and the base station when the network is initialized. The purpose of the hello packets is to determine the number of active nodes in the region and number of hops required to reach the dense sector and the base station.

The proposed model considers that the Flow table component of the controller is pre-installed with the specific information of the available sensor nodes. The data transmission is controlled by the flow table match action rules. The DFRE component keeps tracks of the overall topology and updates the flow tables accordingly. In addition, it interacts with the security module to authenticate the waypoints and maintain the legitimacy of incoming connections. Further, to verify the connectivity between the UAVs and the WSNs, DFRE checks for previously calculated waypoints and matches with the next possible waypoints. In such a way, the movement of UAVs is authenticated and verified before transmissions[1]. The details of security considerations and requirements are provided below:

– The system maintains the check on the certificates generated by the controller for other UAVs in the form a centralized corpus on the controller. It also maintains the details of keys to be used for securing the communications.

[1]The detailed procedure for authentication and verification will be presented in our future reports.

- The channel security is based on the network architecture and depends on the initial phases of mutual authentication, which are not covered at the moment and is marked as an assumption.
- The keys for securing the location as well as the system conditions are generated by the owner UAV, which can relay with an optional server to check for freshness and prevent any replay attacks.
- Once the keys are initiated, the DFRE module improvises the availability of waypoints and allocate it to the topology generator, which helps to fixate the points for maneuverability. Any violation in the waypoints is tracked through crypto-mechanisms based on keys generated in the initial phase.
- The certificate issuance helps to re-verify the UAVs and the waypoints and avoids overheads associated with re-verification. However, the requirement of verification of waypoints depends on the type of network layout and the environment in which the UAVs are deployed.

3 Performance Evaluations

The proposed technique relies on exploits the movement characteristics of UAV in order to achieve significant gains over the already existing models. The evaluation and testing of the approach are done on a model consisting of the base station, WSN motes and the UAVs serving as relays by using NS-3 and Matlab^{TM}. The testing is performed on a $1200 \times 1200m^2$ area. The number of UAVs is varied between 1 and 10 with WSN nodes equaling 100. The average packet size is varied between 512 bytes to 1024 bytes and the value of balancing constants (η) are kept fixed at 0.5. The connections are generated through the modeling without overlapping and the proposed approach is compared with hierarchical WSN layout and Statically Maneuvered UAV approaches.

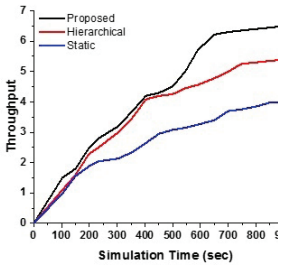


Fig. 2: Throughput vs. Simulation time.

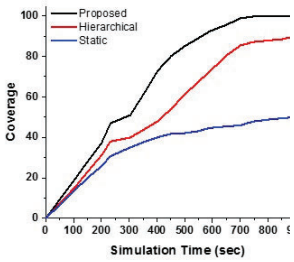


Fig. 3: Coverage vs. Simulation time.

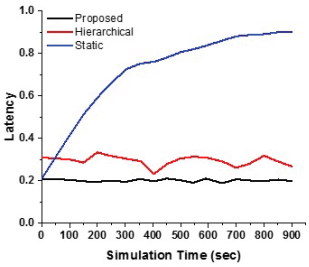


Fig. 4: Latency vs. Simulation time.

The proposed approach performs at the maximum throughput level of 95.7% as compared to 77.1% and 57.1% throughput levels of hierarchical WSN approach and static deployment of UAVs respectively. Fig. 2 gives the throughput

compassion of the considered approaches against the proposed approach. Initially, three approaches have comparable throughput but with time the static approach starts degrading. The traditional hierarchical approach initially performs in close proximity to the proposed approach but cannot match the steep ascent as the proposed approach performs uniformly throughout the simulation tests. The proposed approach provides the maximum coverage of around 99% in comparison to 84% and 49% coverage of hierarchical and static deployment. The approach also provides a faster and efficient coverage against the other two solutions. Fig. 3 gives the coverage relationship between the existing and the proposed approaches. The latency of the proposed approach is approximately constant at 20% gains. The hierarchical approach works with a varying latency between 19% and 34%. The latency levels always stay in close proximity to the proposed approach but with consistent fluctuation. The static UAV approach possesses inconsistent latency measures with a maximum of 84% and average latency of around 65%, as shown in Fig. 4.

4 Conclusion

In this article, a novel mobility scheme based on the transmission density of the WSN nodes is proposed which is capable of including waypoint-security of UAVs. The UAVs perform successive shifts towards dense regions thus resulting in high coverage and throughput. The proposed approach incorporates a simple flow based technique through SDN controller for authentication and coordination of WSN as well as aerial nodes. Significant gains are observed for metrics like throughput, coverage, and latency. The details on authentication procedures and verification mechanisms will be presented in our future reports.

Acknowledgement

This paper was presented at the Workshop associated with the 12th International Conference on Provable Security, 25-28 October, 2018, Jeju, Rep. of Korea.

References

1. V. Sharma and R. Kumar, "A cooperative network framework for multi-uav guided ground ad hoc networks," *Journal of Intelligent & Robotic Systems*, vol. 77, no. 3-4, pp. 629–652, 2015.
2. W. Wang, X. Guan, B. Wang, and Y. Wang, "A novel mobility model based on semi-random circular movement in mobile ad hoc networks," *Information Sciences*, vol. 180, no. 3, pp. 399–413, 2010.
3. J. Zhao, F. Gao, L. Kuang, Q. Wu, and W. Jia, "Channel tracking with flight control system for uav mmwave mimo communications," *IEEE Communications Letters*, 2018.
4. L. Liu, S. Zhang, and R. Zhang, "Comp in the sky: Uav placement and movement optimization for multi-user communications," *arXiv preprint arXiv:1802.10371*, 2018.

5. D. Yang, Q. Wu, Y. Zeng, and R. Zhang, "Energy trade-off in ground-to-uav communication via trajectory design," *IEEE Transactions on Vehicular Technology*, 2018.
6. V. Sharma, I. You, R. Kumar, and V. Chauhan, "Offrp: optimised fruit fly based routing protocol with congestion control for uavs guided ad hoc networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 27, no. 4, pp. 233–255, 2018.
7. V. Sharma, M. Bennis, and R. Kumar, "Uav-assisted heterogeneous networks for capacity enhancement," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1207–1210, 2016.
8. V. Sharma, D. Reina, and R. Kumar, "Hmadso: a novel hill myna and desert sparrow optimization algorithm for cooperative rendezvous and task allocation in fanets," *Soft Computing*, pp. 1–24, 2017.
9. B. Grocholsky, J. Keller, V. Kumar, and G. Pappas, "Cooperative air and ground surveillance," *IEEE Robotics & Automation Magazine*, vol. 13, no. 3, pp. 16–25, 2006.
10. R.-I. Ciobanu, D. Reina, C. Dobre, S. Toral, and P. Johnson, "Jder: A history-based forwarding scheme for delay tolerant networks using jaccard distance and encountered ration," *Journal of Network and Computer Applications*, vol. 40, pp. 279–291, 2014.
11. P. Chandhar, D. Danev, and E. G. Larsson, "Massive mimo as enabler for communications with drone swarms," in *Unmanned Aircraft Systems (ICUAS), 2016 International Conference on*, pp. 347–354, IEEE, 2016.
12. D.-T. Ho and S. Shimamoto, "Highly reliable communication protocol for wsn-uav system employing tdma and pfs scheme," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 1320–1324, IEEE, 2011.
13. Z. Han, A. L. Swindlehurst, and K. R. Liu, "Optimization of manet connectivity via smart deployment/movement of unmanned air vehicles," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3533–3546, 2009.
14. Z. Han, A. L. Swindlehurst, and K. R. Liu, "Smart deployment/movement of unmanned air vehicle to improve connectivity in manet," in *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, vol. 1, pp. 252–257, IEEE, 2006.
15. E. Taqieddin, F. Awad, and H. Ahmad, "Location-aware and mobility-based performance optimization for wireless sensor networks.," *JoWUA*, vol. 8, no. 4, pp. 37–59, 2017.
16. J. Harri, F. Filali, and C. Bonnet, "Mobility models for vehicular ad hoc networks: a survey and taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, 2009.
17. F. Valenza, T. Su, S. Spinoso, A. Lioy, R. Sisto, and M. Vallini, "A formal approach for network security policy validation," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 8, no. 1, pp. 79–100, 2017.
18. B. K. Bhargava, A. M. Johnson, G. I. Munyengabe, and P. Angin, "A systematic approach for attack analysis and mitigation in v2v networks.," *JoWUA*, vol. 7, no. 1, pp. 79–96, 2016.
19. G. Secinti, P. B. Darian, B. Canberk, and K. R. Chowdhury, "Sdns in the sky: Robust end-to-end connectivity for aerial vehicular networks," *IEEE Communications Magazine*, vol. 56, pp. 16–21, Jan 2018.
20. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

Expressive Ciphertext-Policy Attribute-Based Encryption with Fast Decryption*

Hikaru Tsuchida[1] **, Takashi Nishide[2], and Eiji Okamoto[2]

[1] NEC Corporation, 1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666, Japan. h-tsuchida@bk.jp.nec.com
[2] Faculty of Engineering, Information and Systems, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan.
{nishide,okamoto}@risk.tsukuba.ac.jp

Abstract. Attribute-Based Encryption (ABE) is a cryptosystem which supplies access control for an encrypted data in a cloud storage and has been actively studied. However, in the ABE system, a receiver needs much time to decrypt an encrypted data. It is because the cost of pairing operations for decryption becomes heavy linearly with the size of an access structure specified for ciphertexts. Due to this, the construction of ABE is required to reduce the number of pairing operations and achieve expressiveness of an access structure simultaneously.
In this paper, we propose a new construction of ciphertext-policy ABE supporting general predicates with a constant number of pairing operations for decryption. We also prove that our construction achieves new security notion which we introduce, restricted-selectively payload-hiding security under the q-type decisional bilinear Deiffie-Hellman assumption.

Keywords: Public Key Encryption · Access Control · Attribute-Based Encryption · Non-monotone Access Structure · Fast Decryption

1 Introduction

1.1 Background

Attribute-Based Encryption (ABE) [14, 7, 6, 13, 5, 17, 8, 9] is considered as one of the best methods for access control of data which is stored in the cloud storage server. ABE is the public key cryptosystem which supplies data security and access control without needing to trust the cloud and it enables to specify access policies and associated attributes among encrypted data and users' private keys. ABE is roughly divided into two types: Key-Policy ABE (KP-ABE) [7] (which specifies access policies to users' private keys and associated attributes to ciphertexts) and Ciphertext-Policy ABE (CP-ABE) [6] (which specifies access

* This work was supported in part by JSPS KAKENHI Grant Number 17K00178 and the Telecommunications Advancement Foundation.
** The major part of this work was completed while the author was a graduate student at University of Tsukuba.

policies to ciphertexts and associated attributes to users' private keys). Also ABE is already mature enough to be deployed in applications to IoT devices [4, 11, 3, 15].

Most existing ABE constructions are pairing-based ones [14, 7, 6, 13, 5, 17, 8, 9, 12]. Especially, there exists previous works with constant number of pairing operations for decryption [9, 10, 2, 17], but these scheme can support monotone access structure only.

For a device which has only low computation resources, many pairing operations lead to a very heavy task. Therefore, the CP-ABE scheme supporting expressive access structures (as [12]) with a constant number of pairing operations for decryption (as [9, 10, 17, 2]) is more desirable.

1.2 Our Results

We propose a new CP-ABE scheme supporting non-monotone access structures with inner-product relations with three pairing operations for decryption. There is no CP-ABE scheme that supports non-monotone access structures with constant pairing operations except our proposal as far as we know. We also introduce a new security model, restricted-selectively payload-hiding (r-PH) security against the chosen plaintext attacks that is weaker than selectively payload-hiding security against the chosen plaintext attacks in [16]. We prove that our construction achieves r-PH security under the q-type decisional bilinear Diffie-Hellman assumption.

1.3 Key Techniques

The proposed scheme is composed by conjunction of the Functional Encryption for Inner-Product functionality (FEIP) proposed by Abdalla et al. [1] and the selectively secure CP-ABE supporting monotone access structures with constant pairing operations for decryption proposed by Hohenberger and Waters [9]. Our design of the access structure is based on [12] proposed by Okamoto and Takashima. In [12], the access structure is a non-monotone access structure with inner-product relations which is realized by combining monotone span programs and inner-product predicates. The scheme [12] uses the property of Dual Pairing Vector Spaces (DPVS) to express the inner-product predicate, but we use a modified FEIP to specify the inner-product predicates. We also employ the selectively secure CP-ABE with fast decryption [9] for realizing monotone span programs. In this way, our proposed scheme realizes the same access control as [12] (which is more expressive than [9]) and a constant number of pairing operations.

2 Preliminaries

2.1 Notations

We follow the notations in [12].

Let A be a set, and then $a \xleftarrow{\mathsf{U}} A$ denotes that a is uniformly selected from A. When B is a random variable or distribution, $b \xleftarrow{\mathsf{R}} B$ denotes that b is randomly selected from B according to its distribution. We define $\mathbb{Z}_p := \{0, 1, \ldots, p-1\}$ and $\mathbb{Z}_p^\times := \mathbb{Z}_p \backslash \{0\}$. A vector symbol denotes a vector representation over $\mathbb{Z}_p$, e.g., $\boldsymbol{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$. For two vectors $\boldsymbol{s} = (s_1, \ldots, s_n) \in \mathbb{Z}_p^n$ and $\boldsymbol{t} = (t_1, \ldots, t_n) \in \mathbb{Z}_p^n$, $\boldsymbol{s} \cdot \boldsymbol{t}$ denotes the inner-product $\sum_{i=1}^n s_i t_i \bmod p$. We let $\mathbf{0}$ be abused as the zero vector in $\mathbb{Z}_q^n$ for any n.

2.2 General Predicates: Non-Monotone Access Structures with Inner-Product Relations

We follow the definitions in [12]. However, the target vector is $(1, 0, \ldots, 0)$ as in [16] rather than $(1, 1, \ldots, 1)$ as in [12].

2.3 Symmetric bilinear pairing groups

Definition 1 (Symmetric bilinear pairing groups). *"Symmetric bilinear pairing groups" $(p, \mathbb{G}, \mathbb{G}_T, g, \boldsymbol{e})$ are a tuple of a prime p, cyclic multiplicative group $\mathbb{G}$, $\mathbb{G}_T$ of order p, $g \neq 1 \in \mathbb{G}$, and a polynomial-time computable nondegenerate bilinear pairing $\boldsymbol{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ i.e., $\boldsymbol{e}(g^s, g^t) = \boldsymbol{e}(g, g)^{st}$ and $\boldsymbol{e}(g, g) \neq 1$. Let $\mathcal{G}_{\mathsf{bpg}}$ be an algorithm that takes input 1^λ and outputs a description of bilinear pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, \boldsymbol{e})$ with security parameter λ.*

2.4 Security Assumption

We employ the the q-DBDHE assumption similarly to [16, Section 5].

Definition 2 (q-DBDHE: q-Decisional Bilinear Diffie-Hellman Exponent Assumption). *The q-DBDHE problem is to guess $\tilde{b} \in \{0, 1\}$, given $(\mathsf{param}_{\mathbb{G}}, \boldsymbol{y}, T_{\tilde{b}}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\tilde{b}}^{\mathsf{q\text{-}DBDHE}}(1^\lambda)$, where*

$$
\begin{aligned}
&\mathcal{G}_{\tilde{b}}^{\mathsf{q\text{-}DBDHE}}(1^\lambda) : \\
&\mathsf{param}_{\mathbb{G}} := (p, \mathbb{G}, \mathbb{G}_T, g, \boldsymbol{e}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \\
&a, s \xleftarrow{\mathsf{U}} \mathbb{Z}_p,\ \boldsymbol{y} := (g^a, \ldots, g^{(a^q)}, g^{(a^{q+2})}, \ldots, g^{(a^{2q})}, g^s), \\
&T_0 := \boldsymbol{e}(g, g)^{(a^{q+1})s}, T_1 := R \xleftarrow{\mathsf{U}} \mathbb{G}_T, \\
&\textit{return } (\mathsf{param}_{\mathbb{G}},\ \boldsymbol{y},\ T_{\tilde{b}}),
\end{aligned}
$$

for $\tilde{b} \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic machine $\mathcal{B}$, we define the advantage of $\mathcal{B}$ for the q-DBDHE problem as:
$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{q\text{-}DBDHE}}(\lambda) :=$
$|\Pr[\mathcal{B}(1^\lambda, \varrho) \to 0 \mid \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{q\text{-}DBDHE}}(1^\lambda)] - \Pr[\mathcal{B}(1^\lambda, \varrho) \to 0 \mid \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{q\text{-}DBDHE}}(1^\lambda)]|$.

The q-DBDHE assumption is: For any probabilistic polynomial-time adversary $\mathcal{B}$, the advantage $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{q\text{-}DBDHE}}(\lambda)$ is negligible in λ.

3 Expressive Attribute-Based Encryption with Fast Decryption (EABEFD)

3.1 Definitions of EABEFD

Definition 3 (Expressive Attribute-Based Encryption with Fast Decryption). *An expressive attribute-based encryption with fast decryption (EABEFD) scheme consists of the following algorithms. These are randomized algorithms except for* Dec.

1. $\mathsf{Setup}(1^\lambda, \boldsymbol{n})$
   Setup *algorithm takes as input a security parameter* λ *and format* $\boldsymbol{n} := (n_1, \ldots, n_d)$. *It outputs a pair of public parameter and master secret key* (PK, MSK).
2. $\mathsf{KeyGen}(PK, MSK, \Gamma)$
   KeyGen *takes as input a public key* PK, *master secret key* MSK *and a set of attributes* $\Gamma := \{(t, \boldsymbol{x}_t) \mid \boldsymbol{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{Z}_p^{n_t} \setminus \{\boldsymbol{0}\};\ t \in \{1, \ldots, d\}\ ; x_{t,1} = 1\}$. *It outputs a user private key* sk_Γ.
3. $\mathsf{Enc}(PK, m, \mathbb{A})$
   Enc *takes as inputs a public key* PK, *a plaintext* m *and an access structure* $\mathbb{A} := (M, \rho)$. *It outputs a ciphertext* $CT_\mathbb{A}$.
4. $\mathsf{Dec}(PK, sk_\Gamma, CT_\mathbb{A})$
   Dec *takes as inputs a public key* PK, *a user secret key* sk_Γ *and a ciphertext* $CT_\mathbb{A}$. *It outputs a message* m *or a special symbol* $\perp$.

An EABEFD scheme should have the following correctness property: for all security parameter λ, all attribute sets $\Gamma := \{(t, \boldsymbol{x}_{A,t})\}$, all messages m and all access structures $\mathbb{A}$, it holds that $m = \mathsf{Dec}(PK, sk_\Gamma, CT_\mathbb{A})$ with overwhelming probability, if $\mathbb{A}$ accepts Γ where

$$
\begin{aligned}
&(PK, MSK) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, \boldsymbol{n} := (n_1, \ldots, n_d)),\\
&sk_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(PK, MSK, \Gamma),\\
&CT_\mathbb{A} \xleftarrow{\mathsf{R}} \mathsf{Enc}(PK, m, \mathbb{A})
\end{aligned}
$$

Definition 4 (Restricted-selectively Payload-hiding Secure against the Chosen Plaintext Attack). *For an adversary* $\mathcal{A}$, *we define* $\mathsf{Adv}_\mathcal{A}^{\mathsf{EABEFD,r\text{-}PH}}(\lambda) := |\Pr[\mu' = \mu] - 1/2|$ *to be the advantage of an adversary in the following experiment for any security parameter* λ. *An EABEFD scheme is restricted-selectively payload-hiding secure against the chosen plaintext attack if the advantage of any polynomial-time adversary is negligible:*

Init
The adversary $\mathcal{A}$ *gives the challenge access structure* $\mathbb{A}^* := (M^*, \rho^*)$ *to the challenger* $\mathcal{C}$. *Here, the number of rows of* M^* *is* ℓ^*.

Setup
Given 1^λ, $\mathcal{C}$ *runs* $\mathsf{Setup}(1^\lambda, \boldsymbol{n} := (n_1, \ldots, n_d))$ *and gives* PK *to* $\mathcal{A}$.

Phase 1

Let $\tilde{\rho}^* : \{1,\ldots,\ell^*\} \to \{1,\ldots,d\}$ *by* $\tilde{\rho}(i)^* := t$ *if* $\rho^*(i) = (t, \boldsymbol{v})$ *or* $\rho^*(i) = \neg(t, \boldsymbol{v})$*, where* ρ^* *is given in challenge access structure* $\mathbb{A}^*$*.* $\mathcal{A}$ *is allowed to issue a polynomial number of key queries for some attribute sets* $\Gamma_i := \{(t, \boldsymbol{x}_t)\}(i = 1,\ldots,q_1)$ *to* $\mathcal{C}$*. Then,* $\mathcal{C}$ *runs* $\mathsf{KeyGen}(PK, MSK, \Gamma_i)$ *for* $i = 1,\ldots,q_1$ *to generate attribute secret key* sk_{Γ_i} *and gives it to* $\mathcal{A}$*. Here, for any* Γ_i *where* $i = 1,\ldots,q_1$*, the following must hold:* $\boldsymbol{T} \notin \mathsf{span}\langle (M^*_{i'})_{i' \in I'} \rangle$ *where* $M^*_{i'}$ *is the* i'*-th row of* M^* *and* I' *is defined as* $\{i' \mid 1 \le i' \le \ell^*$ *and* $\exists (t, \boldsymbol{x}_t) \in \Gamma_i, \tilde{\rho}^*(i') = t\}$*.*

Challenge

$\mathcal{A}$ *gives two challenge plaintexts* m^*_0, m^*_1 *to* $\mathcal{C}$*.* $\mathcal{C}$ *flips a random coin* $\mu \xleftarrow{\mathsf{U}} \{0,1\}$*, and computes* $CT_{\mathbb{A}^*} \xleftarrow{R} \mathsf{Enc}(PK, m^*_\mu, \mathbb{A}^*)$*. Then,* $\mathcal{C}$ *gives* $CT_{\mathbb{A}^*}$ *to* $\mathcal{A}$*.*

Phase 2

$\mathcal{A}$ *is allowed to issue a polynomial number of key queries for some attribute sets* $\Gamma_i (i = q_1{+}1,\ldots,\nu)$ *to* $\mathcal{C}$ *as in* **Phase1***. Then,* $\mathcal{C}$ *runs* $\mathsf{KeyGen}(PK, MSK, \Gamma_i)$ *for* $i = q_1 + 1,\ldots,\nu$ *to generate attribute secret key* sk_{Γ_i} *and gives it to* $\mathcal{A}$*. Here, for any* Γ_i *where* $i = 1,\ldots,q_1, q_1+1,\ldots,\nu$*, the following must hold:* $\boldsymbol{T} \notin \mathsf{span}\langle (M^*_{i'})_{i' \in I'} \rangle$ *where* $M^*_{i'}$ *is the* i'*-th row of* M^* *and* I' *is defined as* $\{i' \mid 1 \le i' \le \ell^*$ *and* $\exists (t, \boldsymbol{x}_t) \in \Gamma_i, \tilde{\rho}^*(i') = t\}$*.*

Guess

$\mathcal{A}$ *outputs a guess* μ' *of* μ*. If* $\mu' = \mu$*, then* $\mathcal{A}$ *wins.*

We note that the r-PH security is weaker than selectively payload-hiding security against the chosen plaintext attacks, but actually both are the same if an attribute category has only one attribute value and an access structure is monotone as in [16].

3.2 Construction

Let us define $\tilde{\rho} : \{1,\ldots,\ell\} \to \{1,\ldots,d\}$ by $\tilde{\rho}(i) := t$ if $\rho(i) = (t, \boldsymbol{v})$ or $\rho(i) = \neg(t, \boldsymbol{v})$, where ρ is given in access structure $\mathbb{A} := (M, \rho)$. We note that our proposal works with the restriction that an attribute can only be used in at most one row in the access matrix M as well as the scheme [16]. That is, the $\tilde{\rho}$ function is injective. As in [12], we assume that input vector $\boldsymbol{x}_t := (x_{t,1},\ldots,x_{t,n_t})$ is normalized such that $x_{t,1} := 1$. We also assume that $x_{t,1}$ is non-zero. If $\boldsymbol{x}_t$ is not normalized, we can change it to a normalized one by $(1/x_{t,1}) \cdot \boldsymbol{x}_t$.

1. $\mathsf{Setup}(1^\lambda, \boldsymbol{n} := (d, n_1,\ldots,n_d))$:

$\mathsf{param}_{\mathbb{G}} := (p, \mathbb{G}, \mathbb{G}_T, g, \boldsymbol{e}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\ \alpha, \beta, a \xleftarrow{\mathsf{U}} \mathbb{Z}_p^\times,$

$\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, \boldsymbol{e}(g,g)^\alpha, g^a, g^\beta),$

$h_t \xleftarrow{\mathsf{U}} \mathbb{G}$ for $t = 1,\ldots,d,\ s_{t,j} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^\times$ for $t = 1,\ldots,d; j = 1,\ldots,n_t,$

$PK := (\mathsf{gparam},\ \{h_t\}_{t=1}^d,\ \{g^{s_{t,j}}\}_{t=1;j=1}^{d;n_t}),$

$MSK := (\{\boldsymbol{s}_t := (s_{t,1},\ldots,s_{t,n_t})\}_{t=1}^d, g^\alpha, \beta),$

return (PK, MSK).

2. $\mathsf{KeyGen}(PK, MSK, \Gamma = \{(t, \boldsymbol{x}_t) \mid \boldsymbol{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{Z}_p^{n_t} \setminus \{\boldsymbol{0}\};$
$1 \leq t \leq d; x_{t,1} = 1\})$:
$z \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{\times},\ K := g^{\alpha} g^{az},\ L := g^{z},\ K_t := h_t^{z}$ for t s.t. $(t, \boldsymbol{x}_t) \in \Gamma$,
for $(t, \boldsymbol{x}_t) \in \Gamma$,

$$\tau_{(t,\boldsymbol{x}_t)} \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{\times},\ k_{(t,\boldsymbol{x}_t)} := \tau_{(t,\boldsymbol{x}_t)}(\sum_{j=1}^{n_t} x_{t,j} s_{t,j}) = \tau_{(t,\boldsymbol{x}_t)} \boldsymbol{x}_t \cdot \boldsymbol{s}_t,$$

$$\tilde{k}_{(t,\boldsymbol{x}_t)} := g^{z(1-\tau_{(t,\boldsymbol{x}_t)})(\sum_{j=1}^{n_t} x_{t,j} s_{t,j})/\beta} = g^{z(1-\tau_{(t,\boldsymbol{x}_t)})\boldsymbol{x}_t \cdot \boldsymbol{s}_t/\beta},$$

return $sk_{\Gamma} := (\Gamma, K, L, \{K_t\}_{t \text{ s.t. } (t,\boldsymbol{x}_t)\in\Gamma}, \{k_{(t,\boldsymbol{x}_t)}, \tilde{k}_{(t,\boldsymbol{x}_t)}\}_{(t,\boldsymbol{x}_t)\in\Gamma})$.

Remark: We explain how to modify FEIP [1] briefly. We use two parameters $\tau_{(t,\boldsymbol{x}_t)}$ and β. $\tau_{(t,\boldsymbol{x}_t)}$ is the value to prevent users from colluding and getting $\boldsymbol{s}_t$ by using $k_{(t,\boldsymbol{x}_t)}$ and solving simultuneous equations. β is the value to connect CP-ABE [9] and FEIP [1].

3. $\mathsf{Enc}(PK, m, \mathbb{A} = (M, \rho))$:
$\boldsymbol{f} := (s, y_2, \ldots, y_r),\ \boldsymbol{\lambda} := (\lambda_1, \ldots, \lambda_\ell)^T = M \cdot \boldsymbol{f}^T,\ r' \xleftarrow{\mathsf{U}} \mathbb{Z}_p^{\times}$,
$C := m\boldsymbol{e}(g,g)^{\alpha s},\ C' := g^{s},\ c := g^{r'},\ \tilde{c} := g^{\beta r'}$,
for $i = 1, \ldots, \ell$,
$\theta_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p$,
if $\rho(i) = (t, \boldsymbol{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{Z}_p^{n_t} \setminus \{\boldsymbol{0}\})$,

$$c_{i,1} := g^{r' s_{t,1}} (g^{a\lambda_i} h_t^{-s}) g^{\theta_i v_{i,1}},$$
$$c_{i,2} := g^{r' s_{t,2}} g^{\theta_i v_{i,2}},$$
$$\vdots$$
$$c_{i,n_t} := g^{r' s_{t,n_t}} g^{\theta_i v_{i,n_t}},$$

if $\rho(i) = \neg(t, \boldsymbol{v}_i)$,

$$c_{i,1} := g^{r' s_{t,1}} (g^{a\lambda_i} h_t^{-s})^{v_{i,1}},$$
$$c_{i,2} := g^{r' s_{t,2}} (g^{a\lambda_i} h_t^{-s})^{v_{i,2}},$$
$$\vdots$$
$$c_{i,n_t} := g^{r' s_{t,n_t}} (g^{a\lambda_i} h_t^{-s})^{v_{i,n_t}},$$

return $CT_{\mathbb{A}} := (\mathbb{A}, C, C', c, \tilde{c}, \{c_{i,j}\}_{i=1;j=1}^{\ell;n_{\tilde{\rho}(i)}})$.

4. $\mathsf{Dec}(PK, sk_{\Gamma}, CT_{\mathbb{A}})$:
If $\mathbb{A} := (M, \rho)$ accepts $\Gamma := \{(t, \boldsymbol{x}_t)\}$, then compute I and $\{\omega_i\}_{i\in I}$ s.t.
$\boldsymbol{T} = \sum_{i\in I} \omega_i M_i$, where M_i is the i-th row of M, and

$$I \subseteq \{i \in \{1,\dots,\ell\} \mid [\rho(i) = (t, \boldsymbol{v}_i) \ \wedge \ (t, \boldsymbol{x}_t) \in \Gamma \ \wedge \ \boldsymbol{v}_i \cdot \boldsymbol{x}_t = 0] \vee [\rho(i) = \neg(t, \boldsymbol{v}_i) \ \wedge \ (t, \boldsymbol{x}_t) \in \Gamma \ \wedge \ \boldsymbol{v}_i \cdot \boldsymbol{x}_t \neq 0]\},$$

for $i \in I$,

$$K'_i := (\prod_{j=1}^{n_t} (c_{i,j})^{x_{t,j}})/c^{k_{(t,\boldsymbol{x}_t)}},$$

$$K' := \boldsymbol{e}(\prod_{i \in I \wedge \rho(i)=(t,\boldsymbol{v}_i)} {K'_i}^{-\omega_i} \prod_{i \in I \wedge \rho(i)=\neg(t,\boldsymbol{v}_i)} {K'_i}^{-\omega_i/(\boldsymbol{v}_i \cdot \boldsymbol{x}_t)}, \ L) \cdot \boldsymbol{e}(\tilde{c}, \prod_{i \in I \wedge \rho(i)=(t,\boldsymbol{v}_i)} \tilde{k}_{(t,\boldsymbol{x}_t)}^{\omega_i} \prod_{i \in I \wedge \rho(i)=\neg(t,\boldsymbol{v}_i)} \tilde{k}_{(t,\boldsymbol{x}_t)}^{\omega_i/(\boldsymbol{v}_i \cdot \boldsymbol{x}_t)}) \cdot \boldsymbol{e}(C', \ K \prod_{i \in I} {K_{\tilde{\rho}(i)}}^{\omega_i})$$

return C/K'.

The security proof of our construction is similar to [16, Section 5].

4 Conclusion

In this paper, we proposed the new CP-ABE scheme supporting non-monotone access structures with inner-product relations, which needs only three pairing operations for decryption. We also proved that our construction achieves r-PH security (which we introduced) under the q-DBDHE assumption. Extending our scheme such that $\tilde{\rho}$ does not need to be injective and proving that our scheme achieves selective security are left as future work.

References

1. Abdalla, M., Bourse, F., Caro, A.D., Pointcheval, D.: Simple functional encryption schemes for inner products. In: Public Key Cryptography. Lecture Notes in Computer Science, vol. 9020, pp. 733–751. Springer (2015)
2. Agrawal, S., Chase, M.: FAME: fast attribute-based message encryption. In: CCS. pp. 665–682. ACM (2017)
3. Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S.R., Rahmani, A., Liljeberg, P.: On the feasibility of attribute-based encryption on internet of things devices. IEEE Micro **36**(6), 25–35 (2016)
4. Ambrosin, M., Conti, M., Dargahi, T.: On the feasibility of attribute-based encryption on smartphone devices. In: IoT-Sys@MobiSys. pp. 49–54. ACM (2015)
5. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Public Key Cryptography. Lecture Notes in Computer Science, vol. 6571, pp. 90–108. Springer (2011)
6. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy. pp. 321–334. IEEE Computer Society (2007)

7. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security. pp. 89–98. ACM (2006)
8. Green, M., Hohenberger, S., Waters, B.: Outsourcing the decryption of ABE ciphertexts. In: USENIX Security Symposium. USENIX Association (2011)
9. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Public Key Cryptography. Lecture Notes in Computer Science, vol. 7778, pp. 162–179. Springer (2013)
10. Malluhi, Q.M., Shikfa, A., Trinh, V.C.: A ciphertext-policy attribute-based encryption scheme with optimized ciphertext size and fast decryption. In: AsiaCCS. pp. 230–240. ACM (2017)
11. Moffat, S., Hammoudeh, M., Hegarty, R.: A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot. In: Proceedings of the International Conference on Future Networks and Distributed Systems. ICFNDS '17, ACM, New York, NY, USA (2017). https://doi.org/10.1145/3102304.3102338, http://doi.acm.org/10.1145/3102304.3102338
12. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: CRYPTO. Lecture Notes in Computer Science, vol. 6223, pp. 191–208. Springer (2010)
13. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM Conference on Computer and Communications Security. pp. 195–203. ACM (2007)
14. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 3494, pp. 457–473. Springer (2005)
15. Touati, L., Challal, Y.: Efficient CP-ABE attribute/key management for iot applications. In: CIT/IUCC/DASC/PICom. pp. 343–350. IEEE (2015)
16. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography. Lecture Notes in Computer Science, vol. 6571, pp. 53–70. Springer (2011)
17. Zhang, Y., Zheng, D., Chen, X., Li, J., Li, H.: Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts. In: ProvSec. Lecture Notes in Computer Science, vol. 8782, pp. 259–273. Springer (2014)

Achieving Strong Security and Member Registration for Lattice-based Group Signature Scheme with Verifier-local Revocation

Maharage Nisansala Sevwandi Perera[1] and Takeshi Koshiba[2]

[1] Graduate School of Science and Engineering
Saitama University, Saitama, Japan
perera.m.n.s.119@ms.saitama-u.ac.jp,
[2] Faculty of Education and Integrated Arts and Sciences
Waseda University, Tokyo, Japan
tkoshiba@waseda.jp

Abstract. A fully dynamic group signature scheme with member registration and member revocation with strong security is desirable when using group signatures in real life. Langlois, Ling, Nguyen, and Wang (PKC 2014) presented the first lattice-based group signature scheme with member revocation. Even though their scheme employs the most flexible revocation approach called Verifier-local revocation, their scheme relied on a weaker security notion and was unable to provide a member registration mechanism. This work obtains a fully dynamic group signature scheme by proposing a group joining protocol to their scheme.

Keywords: lattice-based group signatures, verifier-local revocation, member registration, dynamical-almost-full anonymity

1 Introduction

Group signature schemes introduced by Chaum and van Heyst [10] allow the group members to issue signatures on behalf of the group while being anonymous and allow the group manager to trace the signer. Both member registration and revocation are required when applying group signature schemes in practice. Among the several revocation approaches Verifier-local Revocation (VLR) which was proposed by Brickell [5] and formalized by Boneh et al. [4] is known as the most suitable method for member revocation in group signature schemes. In VLR group signature schemes every member of the group has a token other than their secret signing key and when a member is revoked, the group manager sets the revoking member's token to a list called *Revocation List* (*RL*) and passes RL to the verifiers. Thus the verifiers can validate the signer other than validating the signature at the signature verification. Since VLR requires to send the revocation information only to the verifiers who are less in number than members VLR seems to be the most suitable approach for any size of groups. However, most of the existing VLR group signature schemes operate in the

bilinear map setting which will be insecure when the quantum computers become a reality. In recent years, lattice-based cryptography considered as the most promising candidate against quantum computers. The first lattice-based group signature scheme that supports member revocation was suggested by Langlois et al. [14] in 2014. The scheme in [14] manages member revocation using VLR mechanism. Their scheme operates within the structure of a *Bonsai tree* of hard random lattices [9]. However, the noticeable disadvantage of this scheme is that it satisfies a weaker security notion of *selfless-anonymity*. On the other hand, since the scheme [14] facilitates only member revocation it cannot consider as a fully dynamic group signature scheme. To be a fully dynamic group signature scheme it should also satisfy member registration. Libert et al. [15] proposed a scheme based on lattices with member registration with a new tool where new users can join anonymously by contacting the group manager with their public keys. However, the scheme in [15] does not facilitate member revocation. Recently, Ling et al. [17] presented a fully dynamic group signature scheme based on lattices using accumulators, which seems to be less efficient than VLR in a larger group.

This paper aims to achieve full dynamicity for the existing VLR group signature scheme [14].

1.1 Our Contribution

This paper delivers a new scheme by adding a member registration facility to the VLR scheme in [14]. In the scheme in [14] all the keys are generated and fixed at the beginning because they have only considered member revocation. However, since our scheme consists of member registration, we propose a joining-protocol that allows members to join the group with their own secret signing keys. Moreover, the previous VLR scheme [14] was relied on a weaker security notion, the selfless-anonymity. To increase the level of the security, in our scheme we employ the security notion, *dynamical-almost-full anonymity* provided in [20] which was proposed for VLR schemes with member registration and revocation. Moreover, we use explicit tracing algorithm for identifying the signers in our scheme.

2 Preliminaries

2.1 Notations

For any integer $k \geq 1$, we denote the set of integers $\{1, \ldots, k\}$ by $[k]$. We denote matrices by bold upper-case letters such as $\mathbf{A}$, and vectors by bold lower-case letters, such as $\mathbf{x}$. We assume that all vectors are in column form. The concatenation of matrices $\mathbf{A} \in \mathbb{R}^{n \times m}$ and $\mathbf{B} \in \mathbb{R}^{n \times k}$, is denoted by $[\mathbf{A}|\mathbf{B}] \in \mathbb{R}^{n \times (m+k)}$. The concatenation of vectors $\mathbf{x} \in \mathbb{R}^m$ and $\mathbf{y} \in \mathbb{R}^k$ is denoted by $(\mathbf{x}\|\mathbf{y}) \in \mathbb{R}^{m+k}$. If S is a finite set, $b \xleftarrow{\$} S$ means that b is chosen uniformly at random from S.

Throughout this paper we present security parameter as n and maximum number of members in a group as $N = 2^\ell \in \mathsf{poly}(n)$. The norm bound for

LWE noises is b such that $q/b = \ell\tilde{\mathcal{O}}(n)$. Let χ be a b-bounded distribution over $\mathbb{Z}$. Let $k_1 := m + \ell$ and $k_2 := n + m + \ell$. We choose other parameters as in scheme [14]. Let prime modulus q be $\omega(n^2 \log n)$ and dimension m be $\geq 2n \log q$. Gaussian parameter σ be $\omega(\sqrt{n \log q \log n})$, integer norm bound β be $\lceil \sigma \cdot \log m \rceil$ s.t. $(4\beta + 1)^2 \leq q$, and the number of decomposition p be $\lfloor \log \beta \rfloor + 1$. Sequence of integers $\beta_1, \beta_2, \beta_3, \ldots, \beta_p$ be $\beta_1 = \lceil \beta/2 \rceil; \beta_2 = \lceil (\beta - \beta_1)/2 \rceil$ $\beta_3 = \lceil (\beta - \beta_1 - \beta_2)/2 \rceil; \ldots; \beta_p = 1$. Number of protocol repetitions t be $\omega(\log n)$.

Let $\mathcal{H}_1$: $\{0,1\}^* \to \mathbb{Z}_q^{n \times \ell}$, $\mathcal{H}_2$: $\{0,1\}^* \to \{1,2,3\}^t$, and $\mathcal{G}$: $\{0,1\}^* \to \mathbb{Z}_q^{n \times m}$ be hash functions, modeled as a random oracle. Select one-time signature scheme $\mathcal{OTS} = (\mathsf{OGen}, \mathsf{OSign}, \mathsf{OVer})$, where OGen is the key generation algorithm of $\mathcal{OTS}$ key pair (**ovk**, **osk**), OSign is signature generation and OVer is signature verification functions.

2.2 Lattices

Let q, n, m be integers and $\mathbf{B} = [\mathbf{b}_1 | \cdots | \mathbf{b}_m] \in \mathbb{Z}_q^{r \times m}$ be linearly independent vectors in $\mathbb{Z}_q^r$. The r-dimensional lattice $\Lambda(\mathbf{B})$ for $\mathbf{B}$ is defined as

$$\Lambda(\mathbf{B}) = \{\mathbf{y} \in \mathbb{Z}^r \mid \mathbf{y} \equiv \mathbf{B}\mathbf{x} \bmod q \text{ for some } \mathbf{x} \in \mathbb{Z}_q^m\},$$

which is the set of all linear combinations of columns of $\mathbf{B}$.

2.3 Lattice-Related Properties

Learning With Errors (LWE)

Definition 1 ([19]). *LWE is parametrized by $n, m \geq 1, q \geq 2$, and χ. For $\boldsymbol{s} \in \mathbb{Z}_q^n$, the distribution $\mathrm{A}_{\boldsymbol{s},\chi}$ is obtained by sampling $\boldsymbol{a} \in \mathbb{Z}_q^n$ uniformly at random and $\mathrm{e} \leftarrow \chi$, and outputting the pair $(\boldsymbol{a}, \boldsymbol{a}^T \cdot \boldsymbol{s} + \mathrm{e})$.*

There are two version of LWE problem. *Search-LWE* is to find the secret $\mathbf{s}$ and *Decision-LWE* is to distinguish LWE samples and samples chosen according to the uniformly distribution. We use the hardness of Decision-LWE problem.

For a prime power q, $b \geq \sqrt{n}\omega(\log n)$, and distribution χ, solving $LWE_{n,q,\chi}$ problem is at least as hard as solving $SIVP_\gamma$ (*Shortest Independent Vector Problem*), where $\gamma = \tilde{O}(nq/b)$ [21].

Short Integer Solution ($\mathbf{SIS}_{n,m,q,\beta}$)

Definition 2 ([19, 21]). *Given m uniformly random vectors $\boldsymbol{a}_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, find a nonzero vector $\boldsymbol{x} \in \Lambda^\perp(\boldsymbol{A})$ such that $||\boldsymbol{x}|| \leq \beta$ and $\boldsymbol{A}\boldsymbol{x} = 0 \mod q$.*

Inhomogeneous Short Integer Solution ($\mathbf{ISIS}_{n,m,q,\beta}$)

Definition 3 ([14]). *Given m uniformly random vectors $\boldsymbol{a}_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, find a vector $\boldsymbol{x} \in \Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$ such that $||\boldsymbol{x}|| \leq \beta$.*

For any m, $\beta = \mathsf{poly}(n)$, and for any $q \geq \beta \cdot \omega(\sqrt{n \log n})$, solving $SIS_{n,m,q,\beta}$ problem or $ISIS_{n,m,q,\beta}$ problem with non-negligible probability is at least as hard as solving $SIVP_{\gamma}$ problem, for some $\gamma = \tilde{O}(\beta\sqrt{n})$ [11].

2.4 Lattice-Related Trapdoor generation and the preimage sampling algorithms

We use trapdoor and preimage sampling algorithms discussed below.

- $\mathsf{SampleD}(\mathbf{R}, \mathbf{A}, \mathbf{u}, \sigma)$ outputs $\mathbf{x} \in \mathbb{Z}^m$ sampled from the distribution $D_{\mathbb{Z}^m,\sigma}$ for any vector $\mathbf{u}$ in the image of $\mathbf{A}$, a trapdoor $\mathbf{R}$ and $\sigma = \omega(\sqrt{n \log q \log n})$. The output $\mathbf{x}$ should satisfy the condition $\mathbf{A} \cdot \mathbf{x} = \mathbf{u} \bmod q$.
- $\mathsf{GenTrap}(n, m, q)$ is an efficient randomized algorithm that outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a trapdoor matrix $\mathbf{R}$ for given any integers $n \geq 1$, $q \geq 2$, and sufficiently large $m = 2n \log q$. The distribution of the output $\mathbf{A}$ is $\mathrm{negl}(n)$-far from the uniform distribution.
- $\mathsf{SamplePre}(\mathbf{A}, \mathbf{R}, \mathbf{u}, \sigma)$ outputs a sample $\mathbf{e} \in \mathbb{Z}^m$ from a distribution that is within negligible statistical distance of $D_{\Lambda_q^{\mathbf{u}}(A),\sigma}$, on input a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, a trapdoor basis $\mathbf{R}$, a target image $\mathbf{u} \in \mathbb{Z}_q^n$, and the standard deviation $\sigma \geq \omega(\sqrt{\log m})$.

3 New VLR group signature scheme with member registration

In this section, we first describe our new lattice-based VLR group signature scheme with member registration and revocation. Then we present the underlying interactive protocol in brief.

3.1 Description of the Scheme

Our scheme consists of two extra algorithms Join and Open than the algorithms given in [14].

Key Generation: This randomized algorithm $\mathsf{KeyGen}(n, N)$ creates a group public key **gpk**, the group manager key **ik**, and the tracing manager key **ok**.

1. Run $\mathsf{GenTrap}(n, m, q)$ to get $\mathbf{A}_0 \in \mathbb{Z}_q^{n \times m}$ and a trapdoor $\mathbf{T}_{\mathbf{A}}$.
2. Sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$.
3. Sample $\mathbf{A}_i^b \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ for each $b \in \{0, 1\}$ and $i \in [\ell]$.

4. Set the matrix $\mathbf{A} = [\mathbf{A}_0|\mathbf{A}_1^0|\mathbf{A}_1^1|\ldots|\mathbf{A}_\ell^0|\mathbf{A}_\ell^1] \in \mathbb{Z}_q^{n\times(2\ell+1)m}$.
5. Run $\mathsf{GenTrap}(n,m,q)$ to obtain $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{T_B}$.
6. Select an additional random matrix $\mathbf{F} \hookleftarrow U(\mathbb{Z}_q^{4n\times 4m})$.

Finally we obtain, $\mathbf{gpk} = (\mathbf{A}, \mathbf{B}, \mathbf{F}, \mathbf{u})$, $\mathbf{ik} = \mathbf{T_A}$, $\mathbf{ok} = \mathbf{T_B}$.

Join: A new user i, who has a personal public and private key pair ($\mathbf{upk}[i]$, $\mathbf{usk}[i]$) interacts with the group manager GM (issuer) to join the group, through the joining protocol.

1. User i samples a vector $\mathbf{w}_i \leftarrow D_{\mathbb{Z}^{4m},\sigma}$, and computes $\mathbf{y}_i \leftarrow \mathbf{F}\cdot\mathbf{w}_i \in \mathbb{Z}_q^{4n}$. Then he generates an ordinary digital signature $sig_i \leftarrow \mathsf{Sign}(\mathbf{usk}[i], \mathbf{y}_i)$ and sends both sig_i and $\mathbf{y}_i$, whose binary representation $\mathsf{bin}(\mathbf{y}_i)$ consists of $4n\lceil\log q\rceil = 2m$ bits to the group manager GM.
2. GM confirms $\mathbf{y}_i$ was not previously used by any member and verifies sig_i is a valid signature generated on $\mathbf{y}_i$, using $\mathsf{Vf}(\mathbf{upk}[i], \mathbf{y}_i, sig_i)$. GM aborts if any condition fails. Otherwise, GM creates a certificate for the key $cert_k = \mathsf{Sign}(\mathbf{ik}, \mathbf{y}_i)$ and proceeds as follows.
   (a) Select a fresh ℓ-bit string as the index d and let $d = d[1]\ldots d[\ell] \in \{0,1\}^\ell$ be the binary representation of d.
   (b) Sample vectors $\mathbf{x}_1^{d[1]}\ldots\mathbf{x}_\ell^{d[\ell]} \leftarrow D_{\mathbb{Z}^m,\sigma}$.
   (c) Compute $\mathbf{z} = \sum_{i=1}^{\ell}\mathbf{A}_i^{d[i]}\cdot\mathbf{x}_i^{d[i]} \bmod q$.
   (d) Get $\mathbf{x}_0 \in \mathbb{Z}^m \leftarrow \mathsf{SampleD}(\mathbf{T_A}, \mathbf{A}_0, \mathbf{u}-\mathbf{z}, \sigma)$.
   (e) Let $\mathbf{x}_1^{1-d[1]}\ldots\mathbf{x}_\ell^{1-d[\ell]}$ be zero vectors 0^m.
   (f) Define $\mathbf{x} = (\mathbf{x}_0||\mathbf{x}_1^0||\mathbf{x}_1^1||\ldots||\mathbf{x}_\ell^0||\mathbf{x}_\ell^1) \in \Sigma^{(2\ell+1)m}$. If $||\mathbf{x}||_\infty \le \beta$ then proceed else abort.
   (g) Let the revocation token of the new user i be $\mathbf{grt}[i] = \mathbf{A}_0\cdot\mathbf{x_0}$.
   Finally, GM saves the new member's details $(d, \mathbf{y}_i, \mathbf{usk}[i], sig_i, \mathbf{x}, \mathbf{grt}[i], 1)$ in reg and sends the member certificate $cert_i = (cert_k, d, \mathbf{x})$

Signing : The randomized algorithm $\mathsf{Sign}(\mathbf{gpk}, \mathbf{gsk}[i], cert_i, M)$ generates Σ on a message M, where the user i secret signing key $\mathbf{gsk}[i]$=$\mathbf{w}_i$.

1. Run $\mathsf{OGen}(1^n)$ to obtain a key pair (**ovk, osk**).
2. Encrypt the index d as follows. Let $\mathbf{G} = \mathcal{H}_1(\mathbf{ovk})$. Sample $\mathbf{s} \leftarrow \chi^n$, $\mathbf{e}_1 \leftarrow \chi^m$ and $\mathbf{e}_2 \leftarrow \chi^\ell$, and compute the ciphertext ($\mathbf{c}_1 = \mathbf{B}^T\mathbf{s} + \mathbf{e}_1$, $\mathbf{c}_2 = \mathbf{G}^T\mathbf{s} + \mathbf{e}_2 + \lfloor q/2\rfloor d$).
3. Sample $\rho \xleftarrow{\$} \{0,1\}^n$, let $\mathbf{V} = \mathcal{G}(\mathbf{A}, \mathbf{u}, \mathbf{B}, M, \rho) \in \mathbb{Z}_q^{m\times n}$.
4. Compute $\mathbf{v} = \mathbf{V}\cdot(\mathbf{A}_0\cdot\mathbf{x_0}) + \mathbf{e}_1 \mod q$ ($||\mathbf{e}_1||_\infty \le \beta$ with overwhelming probability and $\mathbf{A}_0\cdot\mathbf{x_0}$ is the revocation token $\mathbf{grt}$ of user i).
5. Confirm that $cert_k$ is generated on $\mathbf{y}_i$ by executing $\mathsf{Verify}(\mathbf{A}, \mathbf{y}_i, cert_k)$. Then form

$$\mathbf{P} = \left(\begin{array}{c|c} \mathbf{B}^T & \\ \mathbf{G}^T & \mathbf{I}_{m+\ell} \end{array}\right) \in \mathbb{Z}_q^{k_1\times k_2}; \mathbf{c} = \begin{pmatrix}\mathbf{c}_1\\ \mathbf{c}_2\end{pmatrix} \in \mathbb{Z}^{k_1}; \mathbf{e} = \begin{pmatrix}\mathbf{s}\\ \mathbf{e}_1\\ \mathbf{e}_2\end{pmatrix} \in \mathbb{Z}^{k_2} \qquad (1)$$

and repeat the zero knowledge interactive protocol of the commitment described in Section 3.2 $t = \omega(\log n)$ times with the public parameter ($\mathbf{A}$, $\mathbf{F}$, $\mathbf{u}$, $\mathbf{V}$, $\mathbf{v}$, $\mathbf{P}$, $\mathbf{c}$) and prover's witness $(\mathbf{x}, \mathbf{e}_1, \mathbf{e})$ to make the soundness error negligible and prove that user is certified. Then make it non-interactive using the Fiat-Shamir heuristic as a triple, $\Pi = (\{CMT^{(k)}\}_{k=1}^{t}, CH, \{RSP^{(k)}\}_{k=1}^{t})$, where CH = $(\{Ch^{(k)}\}_{k=1}^{t}) = \mathcal{H}_2(M, \{CMT^{(k)}\}_{k=1}^{t}, \mathbf{c}_1, \mathbf{c}_2)$.
6. Compute $\mathcal{OTS}$; $sig = \mathsf{OSig}(\mathbf{osk}, (\mathbf{c}_1, \mathbf{c}_2, \Pi))$.
7. Output signature $\Sigma = (\mathbf{ovk}, (\mathbf{c}_1, \mathbf{c}_2), \Pi, sig, \mathbf{v}, \rho)$.

Verification : $\mathsf{Verify}(\mathbf{gpk}, M, \Sigma, RL = \{\{\mathbf{u}_i\}_i\})$ checks whether the given Σ is valid on the given M and signer is a valid member as follows.

1. Parse Σ as $(\mathbf{ovk}, (\mathbf{c}_1, \mathbf{c}_2), \Pi, sig, \mathbf{v}, \rho)$, and get $\mathbf{V} = \mathcal{G}(\mathbf{A}, \mathbf{u}, \mathbf{B}, M, \rho) \in \mathbb{Z}_q^{m \times n}$.
2. If $\mathsf{OVer}(\mathbf{ovk}, (\mathbf{c}_1, \mathbf{c}_2), \Pi, sig) = 0$ then return 0.
3. Parse Π as $(\{CMT^{(k)}\}_{k=1}^{t}, \{Ch^{(k)}\}_{k=1}^{t}, \{RSP^{(k)}\}_{k=1}^{t})$.
4. If $(Ch^{(1)}, \ldots, Ch^{(t)}) \neq \mathcal{H}_2(M, \{CMT^{(k)}\}_{k=1}^{t}, \mathbf{c}_1, \mathbf{c}_2)$ return 0 else proceed.
5. Form $\mathbf{P}$, $\mathbf{c}$ as in (1) and for $k = 1$ to t run the verification steps of the commitment scheme to validate $RSP^{(k)}$ with respect to $CMT^{(k)}$ and $Ch^{(k)}$. If any of the conditions fails then output invalid and hold.
6. For each $\mathbf{u}_i \in RL$ compute $\mathbf{e}_i^{'} = \mathbf{v} - \mathbf{V} \cdot \mathbf{u}_i \mod q$ to check whether there exists an index i such that $||\mathbf{e}_i^{'}||_\infty \leq \beta$. If so return invalid.
7. Return valid.

Open : $\mathsf{Open}(\mathbf{ok}, M, \Sigma, reg)$ functions as follows, where $\mathbf{ok} = \mathbf{T_B}$.

1. Let $\mathbf{G} = \mathcal{H}_1(\mathbf{ovk})$.
2. Then for $i \in [\ell]$, sample $\mathbf{y}_i \leftarrow \mathsf{SamplePre}(\mathbf{T_B}, \mathbf{B}, \mathbf{g}_i, \sigma)$.
3. Let $\mathbf{Y} = [\mathbf{y}_1 | \ldots | \mathbf{y}_\ell] \in \mathbb{Z}^{m \times \ell}$, where $\mathbf{B} \cdot \mathbf{Y} = \mathbf{G}$.
4. Compute $d' = (d'_1, \ldots, d'_\ell) = \mathbf{c}_2 - \mathbf{Y}^T \cdot \mathbf{c}_1 \in \mathbb{Z}_q^\ell$.
5. For each $i \in [\ell]$, if d'_1 is closer to 0 than to $\lfloor q/2 \rfloor$ modulos q, then let $d_i = 0$. Otherwise, let $d_i = 1$.
6. Create $d = (d'_1, \ldots, d_\ell) \in \{0,1\}^\ell$ and return d.

3.2 The Underlying ZKAoK for the Group Signature Scheme

The Stern-like [22] interactive system allows the signer to convince the verifier, he is a certified and valid group member who followed the signature generation correctly. The public parameters consists of matrices $\mathbf{A} = [\mathbf{A}_0 | \mathbf{A}_1^0 | \mathbf{A}_1^1 | \ldots | \mathbf{A}_\ell^0 | \mathbf{A}_\ell^1] \in \mathbb{Z}_q^{n \times (2\ell+1)m}$, $\mathbf{F} \in \mathbb{Z}_q^{4n \times 4m}$, $\mathbf{V} \in \mathbb{Z}_q^{m \times n}$, and $\mathbf{P} \in \mathbb{Z}_q^{k_1 \times k_2}$, and vectors $\mathbf{u} \in \mathbb{Z}_q^n$, $\mathbf{v} \in \mathbb{Z}_q^n$, $\mathbf{c} \in \mathbb{Z}^{k_2}$. The prover's inputs are the vectors $\mathbf{x} = (\mathbf{x}_0 || \mathbf{x}_1^0 || \mathbf{x}_1^1 || \ldots || \mathbf{x}_\ell^0 || \mathbf{x}_\ell^1) \in \mathbb{Z}^{(2\ell+1)m}$, $\mathbf{e}_1 \leftarrow \chi^m$, $\mathbf{w} \in [-\beta, \beta]^{4m}$, $\mathbf{y} \in \{0,1\}^{2m}$, and $\mathbf{e} \in \mathbb{Z}^{k_2}$. The prover's goal is to convince the verifier the following four statements.
1. $\mathbf{A} \cdot \mathbf{x} = \mathbf{u} \mod q$ and $\mathbf{x} \in \mathsf{Secret}_\beta(d)$.
2. $||\mathbf{e}_1||_\infty \leq \beta$ and $\mathbf{V} \cdot (\mathbf{A}_0 \cdot \mathbf{x}_0) + \mathbf{e}_1 = \mathbf{v} \mod q$.

3. $\mathbf{F} \cdot \mathbf{w} = \mathbf{H}_{4n \times 2m} \cdot \mathbf{y} \mod q$.
4. $\mathbf{Pe} + (0^{k_1 - \ell} || \lfloor q/2 \rfloor d) = \mathbf{c} \mod q$.

To prove the goal 1 and 2 we can directly use the interactive protocol given in [14]. We can use the proof provided in [15] for the goal 3 and the proof given in [16] for the goal 4. We can combined all the proofs together and use as the interactive protocol for our scheme.

4 Correctness and Security Analysis of the Scheme

Correctness

For all $\mathbf{gpk}$, $\mathbf{gsk}$, and $\mathbf{grt}$, $\mathsf{Verify}(\mathbf{gpk}, M, \mathsf{Sign}(\mathbf{gpk}, \mathbf{gsk}[i], cert_i, M), RL) = \mathsf{Valid}$ and $\mathbf{grt}[i] \notin RL$ and $\mathsf{Open}(\mathbf{gpk}, \mathbf{ok}, M, \mathsf{Sign}(\mathbf{gpk}, \mathbf{gsk}[i], cert_i, M), reg) = i$

Security

Theorem 1. *In the random oracle model, the proposed scheme is dynamical-almost-full anonymous based on the hardness of $LWE_{n,q,\chi}$.*

Theorem 2. *Based on the hardness of SIS problem, the proposed scheme is traceable, in the random oracle model.*

Theorem 3. *Based on the hardness of SIS problem, the proposed scheme is non-frameable, in the random oracle model.*

5 Conclusion

This work focuses on facilitating member registration mechanism for the scheme given in [14]. Thus we suggested a joining protocol to the existing VLR lattice-based scheme [14]. Moreover, we made the new scheme stronger in security than the scheme in [14].

References

1. Agrawal, S., Boyen, X., Vaikuntanathan, V., Voulgaris, P., Wee, H.: Functional encryption for threshold functions (or fuzzy ibe) from lattices. In: PKC 2012, LNCS. vol. 7293, pp. 280–297. Springer Berlin Heidelberg (2012)
2. Ateniese, G., Song, D., Tsudik, G.: Quasi-efficient revocation of group signatures. In: Proceedings of Financial Cryptography 2002, LNCS. pp. 183–197. Springer (2002)
3. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: EUROCRYPT 2003, LNCS. vol. 2656, pp. 614–629. Springer Berlin Heidelberg (2003)
4. Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In: ACM-CCS 2004. pp. 168–177. ACM (2004)

5. Brickell, E.: An efficient protocol for anonymously providing assurance of the container of the private key. *Submitted to the Trusted Comp. Group (April 2003)* (2003)
6. Brickell, E., Pointcheval, D., Vaudenay, S., Yung, M.: Design validations for discrete logarithm based signature schemes. In: PKC 2000, LNCS. vol. 1751, pp. 276–292. Springer Berlin Heidelberg (2000)
7. Camenisch, J., Lysyanskaya, A.: Dynamic accumulators and application to efficient revocation of anonymous credentials. In: CRYPTO 2002, LNCS. vol. 2442, pp. 61–76. Springer Berlin Heidelberg (2002)
8. Camenisch, J., Neven, G., Rückert, M.: Fully anonymous attribute tokens from lattices. In: SCN 2012, LNCS. vol. 12, pp. 57–75. Springer Berlin Heidelberg (2012)
9. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. EUROCRYPT 2010 6110 of *LNCS*, pages 523–552 (2010)
10. Chaum, D., Van Heyst, E.: Group signatures. In: EUROCRYPT 1991, LNCS. vol. 547, pp. 257–265. Springer Berlin Heidelberg (1991)
11. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: ACM 2008. pp. 197–206. ACM (2008)
12. Gordon, S.D., Katz, J., Vaikuntanathan, V.: A group signature scheme from lattice assumptions. In: ASIACRYPT 2010, LNCS. vol. 6477, pp. 395–412. Springer Berlin Heidelberg (2010)
13. Laguillaumie, F., Langlois, A., Libert, B., Stehlé, D.: Lattice-based group signatures with logarithmic signature size. In: ASIACRYPT 2013, LNCS. vol. 8270, pp. 41–61. Springer Berlin Heidelberg (2013)
14. Langlois, A., Ling, S., Nguyen, K., Wang, H.: Lattice-based group signature scheme with verifier-local revocation. In: PKC 2014, LNCS. vol. 8383, pp. 345–361. Springer Berlin Heidelberg (2014)
15. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In: ASIACRYPT 2016, LNCS. vol. 10032, pp. 373–403. Springer Berlin Heidelberg (2016)
16. Ling, S., Nguyen, K., Wang, H.: Group signatures from lattices: simpler, tighter, shorter, ring-based. In: PKC 2015, LNCS. vol. 9020, pp. 427–449. Springer Berlin Heidelberg (2015)
17. Ling, S., Nguyen, K., Wang, H., Xu, Y.: Lattice-based group signatures: Achieving full dynamicity with ease. In: ACNS 2017, LNCS. vol. 10355, pp. 293–312. Springer International Publishing, Cham (2017)
18. Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller. In: EUROCRYPT 2012. vol. 7237, pp. 700–718. Springer Berlin Heidelberg (2012)
19. Peikert, C.: A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science 10(4), 283–424 (2016), https://doi.org/10.1561/0400000074
20. Perera, M.N.S., Koshiba, T.: Achieving almost-full security for lattice-based fully dynamic group signatures with verifier-local revocation. In: ISPEC 2018, LNCS (to appear)
21. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005. pp. 84–93. ACM Press (2005)
22. Stern, J.: A new paradigm for public key identification. IEEE Transactions on Information Theory 42(6), 1757–1768 (1996)

A Type-based Formal Specification for Cryptographic Protocols

Paventhan Vivekanandan

Indiana University, Bloomington, Indiana, USA
pvivekan@umail.iu.edu

Abstract. This paper investigates a preliminary application of homotopy type theory in cryptography. It discusses specifying a cryptographic protocol using homotopy type theory which adds higher inductive type and univalence to Martin-Löf's intensional type theory. A higher inductive type specification can act as a front-end mapped to a concrete cryptographic implementation in the universe. By having a higher inductive type front-end, we can encode domain-specific laws of the cryptographic implementation as higher-dimensional paths. The higher inductive type gives us a graphical computational model and can be used to extract functions from underlying concrete implementation. Using this model we can extend types to act as formal certificates guaranteeing on correctness properties of a cryptographic implementation.

1 Introduction

Formal verification of cryptographic protocols has become a significant research focus over recent years [4] [7]. Some widely used cryptographic implementations were found to be flawed after their deployment becoming vulnerable to various attacks. For example, the Heartbleed attack (CVE- 2014-0160) is a consequence of a simple coding error [6]. Even with skilled designers, developers and testers it is highly difficult to implement a cryptographic protocol without errors [5].

In this paper, we examine a new approach to formally specify and verify the correctness properties of a cryptographic construction based on type theory, a foundational language of mathematics alternative to set theory. We use an extension of type theory, namely the homotopy type theory, to specify cryptographic constructions. Homotopy type theory extends type theory by adding higher inductive type and univalence axiom. We discuss specifying cryptographic scheme using a higher inductive type in homotopy type theory, implemented in Agda, and how to map the abstract type to a concrete implementation in the universe. We also discuss designing a higher inductive type for a database model with multi-layered encryptions in the style of cryptDB [3].

Designing cryptographic constructions as a higher inductive type has the following benefits.

– In type theory all functions are functorial. Therefore, the functional correctness and domain-specific properties of a cryptographic construction can be

specified as paths or homotopies in a higher inductive type, and the functions will preserve the path structures in the mapping of the type to the universe.
- By specifying cryptographic properties as paths, we achieve guarantee on the correctness of the underlying concrete implementation with respect to the encoded properties.
- We can have a graphical representation of a cryptographic construction in a topological space, and we map it to a concrete implementation in the universe.
- By modeling a cryptographic construction as a higher inductive type, we get the groupoid structure and the relevant coherence laws for free.
- We get elimination rules corresponding to the higher inductive type.

2 Background

Homotopy type theory extends Martin-Löf's intensional type theory by adding univalence axiom and higher inductive types. It introduces the notion of viewing type as a topological space in homotopy theory or a higher-dimensional groupoid in category theory. Because of this correspondence, we can observe an element of the identity type $x =_A y$ for $a, b : A$ as a path in a topological space or a morphism in a groupoid.

Higher inductive types are a general schema for defining new types in homotopy type theory. It extends an ordinary inductive type by providing constructors for generating paths and higher paths. A higher inductive type can be specified in Agda using `{-# REWRITE , ...#-}` mechanism.

Because of the correspondence of types to a topological space or a higher-dimensional groupoid, we can map the elements of an identity type, which are paths in homotopy type theory, to equivalences between types in a universe. Equivalence can be relaxed to a bijection when types behave like sets. The mapping of a path to equivalence is made possible by the univalence axiom which describes that we may identify equivalent types A and B in the following sense.

$$ua : (A \simeq B) \to (A =_U B) \tag{1}$$

In (1), the type U is the *universe* or the *type of types*. The univalence axiom states that when we have a proof of type $A \simeq B$, we can obtain a path between A and B. In homotopy type theory, the following definitions give an equivalence between type A and type B.

$$A \simeq B :\equiv \sum_{f:A\to B} isequiv(f) \tag{2}$$

$$isequiv(f) :\equiv \Big(\sum_{g:B\to A} (f \circ g \sim id_B) \Big) \times \Big(\sum_{h:B\to A} (h \circ f \sim id_A) \Big) \tag{3}$$

A homotopy between non-dependent functions $f_1, f_2 : A_1 \to A_2$ is given as follows.

$$f_1 \sim f_2 :\equiv \prod_{x:A_1} (f_1(x) =_{A_2} f_2(x)) \tag{4}$$

In (3), the composite $f \circ g$ is homotopic to the identity function id_B, and the composite $h \circ f$ is homotopic to the identity function id_A. There is also a reduced notion of equivalence called *quasi-inverse*. A quasi-inverse for a function $f : A \to B$ is given by

$$qinv(f) :\equiv \sum_{g:B\to A} \Big((f \circ g \sim id_B) \times (g \circ f \sim id_A) \Big) \tag{5}$$

Also, we have a function that maps an element of quasi-inverse $qinv(f)$ to $isequiv(f)$ for $f : A \to B$ [1].

$$mkqinv : qinv(f) \to isequiv(f) \tag{6}$$

For examples described in this paper, we will use $mkqinv$ to obtain a proof of equivalence from quasi-inverse. For a path $p : A =_U B$, we have a function *coe* [2] that coerces along p. The following declaration gives the type of *coe*.

$$coe : (A =_U B) \to (A \to B) \tag{7}$$

In the presence of univalence, we also have a computation rule for *coe* [2] defined as follows.

$$coe\,(ua\,(f\,,\,isequiv(f)))\,x = f(x) \tag{8}$$

where $x : A$, $f : A \to B$ and $(f\,,\,isequiv(f)) : A \simeq B$.

Also, in homotopy type theory the functions behave functorially on paths. It means that a function $f : A \to B$ respects equality and it preserves the path structure in the mapping from type A to type B. Now we can give the type of ap_f which defines the action of non-dependent functions on paths as follows.

$$ap_f : (x =_A y) \to (f(x) =_A f(y)) \tag{9}$$

The following declaration gives the action of dependent functions of type $f : \prod_{(x:A)} B(x)$ on paths.

$$apd_f : \prod_{p:x=y} (p_*(f(x)) =_{B(y)} f(y)) \tag{10}$$

In (10), $p_*(f(x))$ lying in space $B(y)$ can be thought of as an endpoint of a path obtained by lifting p from f(x) to a path in the total space $\sum_{(x:A)} B(x) \to A$ [1]. The following declaration gives the type of $p*$ also known as *transport*.

$$transport^B_p : B(x) \to B(y) \tag{11}$$

where $p : x = y$ for $x, y : A$.

3 Higher Inductive Type front-end for OTP

In this section, we will discuss an encoding of the one-time pad using a higher inductive type with a path constructor to specify the encryption function. We will construct a proof for an equivalence which reflects the encryption path of the higher inductive type in the universe. The functional correctness property, which states that decryption inverts encryption, will be part of the construction of the proof for the equivalence. We will then map this higher inductive type, with the encryption path, to a concrete implementation of the one-time pad, with the equivalence reflecting the encryption path, in the universe. The encryption and the decryption functions are then projected from the concrete implementation in the universe using the higher inductive type which acts as a front-end.

3.1 One-time Pad

The following Agda code gives the higher inductive type encoding of the one-time pad.

```
data OTP (n : Nat) : Set where
    -- point constructors
    message : OTP n
    cipher  : OTP n
    -- path constructors
    otp-encrypt : {n : Nat} → (key : Vec Bit n) →
      message {n} ≡ cipher {n}
```

The higher inductive type `OTP` has two point constructors `message` and `cipher` representing the plain-text and the cipher-text respectively. The path constructor `otp-encrypt` represents the encryption function of the one-time pad. We parameterize the type `OTP` with the length n of the data. `otp-encrypt` uses the same length parameter `n` to specify the length of the key which encodes another restriction, namely the length of the key for the one-time pad should be equal to the length of the message, which is crucial for the security of the one-time pad.

The following code gives the recursion principle and its action on constructors or the computation rules for the type `OTP`.

```
otp-rec : {n : Nat} →
    (B : Set) → (b-msg : B) → (b-cipher : B) →
    (b-encrypt : (key : Vec Bit n) → b-msg ≡ b-cipher) →
    OTP n → B
otp-rec B b-msg b-cipher b-encrypt message = b-msg
otp-rec B b-msg b-cipher b-encrypt cipher = b-cipher

postulate
  β-otp-rec : {n : Nat} →
      (B : Set) → (b-msg : B) → (b-cipher : B) →
      (b-encrypt : (key : Vec Bit n) → b-msg ≡ b-cipher) →
      {key : Vec Bit n} →
      ap (otp-rec B b-msg b-cipher b-encrypt)
         (otp-encrypt key) ≡ (b-encrypt key)
```

The recursion principle `otp-rec` states that when given a type `B` with point constructors `b-msg` and `b-cipher` and path constructor `b-encrypt`, there exists a function of type `OTP n → B`. `otp-rec` maps `message` and `cipher` to `b-msg` and `b-cipher` respectively. `β-otp-rec` gives the action of `otp-rec` on the path `(otp-encrypt key)` which maps it to the path `(b-encrypt key)`. Equation (9) gives the type of `ap`.

3.2 Implementation of one-time pad in the universe

The encryption function for the one-time pad is straightforward, and it is implemented using `xor`. The encryption of one-time pad is defined using the following function.

```
OTP-encrypt : {n : Nat} → (key : Vec Bit n) → (message : Vec Bit n) → Vec Bit n
OTP-encrypt {n} key message = message xorBits key
```

where `xorBits` perform `xor` on two vectors of equal length.

Similar to keys, we have chosen to use the type `Vec Bit n` to represent the point constructors `message` and `cipher` of the higher inductive type `OTP` in the

universe. Therefore, the path `otp-encrypt` should be mapped to an equivalence formed by `OTP-encrypt` between types `Vec Bit n` and `Vec Bit n`. To create an equivalence for the function `OTP-encrypt`, we need a proof element of type given by equation (5). To construct a proof element of (5), we need a function `g : Vec Bit n → Vec Bit n`, a proof element of `f∘g ∼ id`, and a proof element of `g∘f ∼ id`. For the one-time pad, the encryption function is also its inverse. So both `f` and `g` are represented by `OTP-encrypt` in this case. Therefore, the types `f∘g ∼ id` and `g∘f ∼ id` are definitionally the same. The equivalence formed by `OTP-encrypt` is defined as follows.

```
OTP-equiv : {n : Nat} → (key : Vec Bit n) → Vec Bit n ≃ Vec Bit n
OTP-equiv key = ((OTP-encrypt key) ,
                 equiv₁ (mkqinv (OTP-encrypt key) (α-OTP key) (α-OTP key)))

(α-OTP key) : (OTP-encrypt key (OTP-encrypt key msg)) ≡ msg
```

In the above code, `(OTP-equiv key)` is of the type given by equation (2). $\texttt{equiv}_1$ forms a proof element of the type given by equation (3). The type of `mkqinv` is given by equation (6) which takes an element of (5) as input and gives an element of (3) as output.

3.3 Mapping OTP into the universe

The higher inductive type `OTP` defined in section 3.1 can now be mapped into the universe using univalence. The equivalence `(OTP-equiv key)` respects the path structure specified by the constructor `otp-encrypt`. Because of this, a path formed by univalence given by `(ua (OTP-equiv key))` represents the path structure of `otp-encrypt` in the universe. This correspondence allows us to define a mapping `I-OTP` which maps the points `message`, `cipher` of `OTP` to type `Vec Bit n` and a mapping `I-OTP-path` which maps the path `(otp-encrypt key)` to `(ua (OTP-equiv key))`.

```
I-OTP : {n : Nat} → OTP n → Set
I-OTP {n} bits = otp-rec Set (Vec Bit n) (Vec Bit n)
                   (λ key → ua (OTP-equiv key)) bits

I-OTP-path : {n : Nat} → (key : Vec Bit n) →
             ap I-OTP (otp-encrypt {n} key) ≡ ua (OTP-equiv key)
I-OTP-path {n} key = β-otp-rec Set (Vec Bit n) (Vec Bit n)
                       (λ k → ua (OTP-equiv k))
```

`I-OTP` is defined using the recursion principle `otp-rec` of the higher inductive type `OTP`. It maps the points of `OTP` to the type `Vec Bit n` in the universe represented by `Set`. `I-OTP-path` maps the path `(otp-encrypt key)` to `(ua (OTP-equiv key))` using `β-otp-rec`. Now we can define an interpreter function `ITP` using `coe` given by equation (7) as follows.

```
ITP : {n : Nat} → {a b : OTP n} → (p : a ≡ b) → (I-OTP a) → (I-OTP b)
ITP {n} {a} {b} p = coe (ap I-OTP p)
```

When we give the path `otp-encrypt` as input, the interpreter `ITP` returns the encryption function `OTP-encrypt`. In the case of `OTP`, the functional correctness property is part of the equivalence `(OTP-equiv key)` given by `(α-OTP key)`, and the path `otp-encrypt` will reflect this through the mapping specified by `I-OTP-path`. Consider the following example.

```
pf : (ITP (otp-encrypt (1b :: (0b :: []))) (1b :: (1b :: []))) ≡ (0b :: (1b :: []))
```

In the above code, `ITP` takes `otp-encrypt` as input with key `(1b :: (0b :: []))` and plain-text `(1b :: (1b :: []))` and returns the cipher-text `(0b :: (1b ::[]))` as output.

4 Encoding Properties as Higher Dimensional Paths

The path `otp-encrypt` described in the previous section is one-dimensional. We can also encode domain-specific cryptographic properties as higher dimensional paths. In this section, we will design properties of a database model with multi-layered encryptions in the style of cryptDB [3] as higher dimensional paths. CryptDB has different layers of encryption known as *onion layers* of encryption. The idea of cryptDB is to allow computation on top of encrypted data without the need to decrypt them. Consider the following higher inductive type specification for cryptDB[1].

```
data encDB : Set where
  -- point constructors
  tab : encDB
  tabDET : encDB
  tabHOM : encDB
  tabOPE : encDB

  -- one-dimensional paths
  hom-enc : tab ≡ tabHOM
  det-enc : tab ≡ tabDET
  ope-enc : tab ≡ tabOPE
```

4.1 Homomorphic Encryption

In cryptDB, homomorphic encryption is implemented using paillier cryptosystem. According to the homomorphic property of paillier cryptosystem, the addition of two plain-texts will be equal to the multiplication of their corresponding cipher-text. This can be expressed as a two-dimensional path (Fig 1).

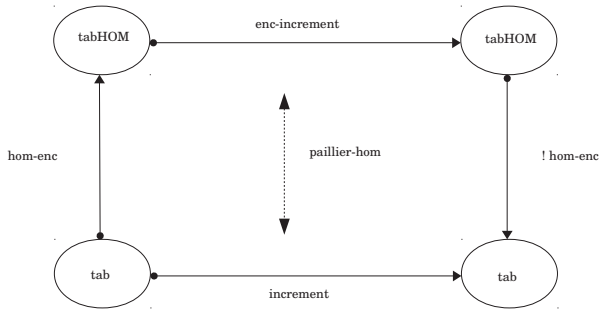


Fig. 1: Homotopy representing the homomorphic property of paillier cryptosystem. `hom-enc` concatenated with `enc-increment` and `(! hom-enc)` is the same as `increment`.

[1] We have simplified the higher inductive type `encDB` for ease of understanding. A detailed implementation can be found at `https://github.com/pavenvivek/ProvSec-2018`.

4.2 Deterministic Encryption

Deterministic encryption generates the same cipher-text on multiple encryptions of the same plain-text. In cryptDB, a deterministic encryption scheme is used to perform equality comparisons on encrypted data. The correctness property of deterministic encryption requires $DET(m1) \equiv DET(m2)$ when $m1 \equiv m2$. We can specify this property as a heterogenous path over a path of type $m1 \equiv m2$.

```
det-correctness : (p : m1 ≡ m2) →
   transport (λ x → tab {x} ≡ tabDET) p (det-enc {m1}) ≡ (det-enc {m2})
```

`det-correctness` says that the path `(det-enc {m1}) ≡ (det-enc {m2})` lies over `p : m1 ≡ m2`.

4.3 Order-Preserving Encryption

Order-preserving encryption (OPE) [9] allows inequality comparisons on encrypted data without the need to decrypt them. Order-preserving encryption requires, for plain-texts x and y, if $(x < y)$ then $OPE(x) < OPE(y)$. We cannot specify this property in the style of `det-correctness` because inequality relation does not form paths. However, we can use a different approach to model this restriction in a higher inductive type. For example, consider a function `bigE (m1, m2)` which returns the biggest of two elements. When there exists a path `p' : bigE(m1, m2) ≡ bigE(c1, c2)`, where c1 and c2 are the OPE cipher values of m1 and m2 respectively, lying in the space `encDB`, we can design a two-dimensional path saying `ope-encrypt` is the same path as `p'`. This holds only when OPE respects the inequality relation between the plain-texts.

5 Limitations and Future Work

A limitation of homotopy type theory is that the univalence can be added only as an axiom. We would like to develop the framework described in this paper using *cubical type theory* [8] in which the univalence computes.

Another limitation is that the mapping of higher inductive type into the universe requires the functions represented by paths to be bijective. We cannot specify all functions as bijections. One way to work around this problem is to encode functions as mappings between singleton types in the universe [2]. Future work in this direction would be to characterize mapping of partial bijections to paths using the tools of homotopy theory.

Also, it might not be possible to map probabilistic encryptions to singleton types in the universe because they compute to different values during each execution and does not uniquely identify the contents of a singleton type. Another limitation is the difficulty involved in deriving proofs for bijections.

6 Related Work

The work discussed in this paper takes the first step towards formal specification of cryptographic protocols based on types. There are other works which support formal specification of cryptographic constructions using different settings. For example, the Foundational Cryptography Framework [4] implements a probabilistic programming language embedded inside Coq proof assistant that enables

the specification of cryptographic schemes, security definitions, and hard problems. ProVerif [11], a cryptographic protocol verifier, allows for the automated reasoning of security properties based on Dolev-Yao model. EasyCrypt [10] enables machine-checked construction and verification of cryptographic schemes.

7 Conclusion

We have shown how to implement a cryptographic scheme using the tools of homotopy type theory. The limitations of homotopy type theory, namely having univalence only as an axiom and the requirement for functions to have inverses has restricted us to only a subset of cryptographic schemes to be benefitted by the model described in this paper. Nevertheless, there is a lot of work going on to improve type theory to allow for univalence to compute and mapping of non-bijective functions into the universe which can reduce the restrictions and enable us to encode more interesting cryptographic constructions.

References

1. The Univalent Foundations Program, Institute for Advanced Study. Homotopy Type Theory: Univalent Foundations Of Mathematics (2013).
2. Anguili, C., Morehouse, E., Licata, D., Harper, R.: Homotopical Patch Theory. In: International Conference on Functional Programming (ICFP), Sweden (2014)
3. Popa, R.A., Redfield, C.M.S, Zeldovich, N., Hari Balakrishnan, H. : CryptDB: Protecting Confidentiality with Encrypted Query Processing. In: Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP), Portugal (2011)
4. Petcher, A., Morrisett, G.: The Foundational Cryptography Framework. In: Focardi R., Myers A. (eds) Principles of Security and Trust (POST). Lecture Notes in Computer Science, vol 9036. Springer, Berlin, Heidelberg (2015)
5. Lazar, D., Chen, H., Wang, X., Zeldovich, N.: Why does cryptographic software fail?: a case study and open problems. In: Proceedings of 5th Asia-Pacific Workshop on Systems (APSys). Beijing, China (2014)
6. Durumeric, Z., Kasten, J., Adrian, D., Halderman, J.A., Bailey, M., Li, F., Weaver, N., Amann, J., Beekman, J., Payer, M., Paxson, V.: The Matter of Heartbleed. In: Proceedings of the 2014 Conference on Internet Measurement Conference. Vancouver, BC, Canada (2014)
7. Berg, M.: Formal Verification of Cryptographic Security Proofs. Ph.D. thesis, Saarland University (2013), `http://www.infsec.cs.uni-saarland.de/~berg/publications/thesis-berg.pdf`
8. Cohen, C., Coquand, T., Huber, S., Mörtberg, A.: Cubical Type Theory: a constructive interpretation of the univalence axiom. In: Leibniz International Proceedings in Informatics (LIBIcs). pp. 1–33. Germany (2015)
9. Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y.: Order preserving encryption for numeric data. In Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data. Paris, France (2004).
10. Gilles, B., Grégoire, B., Heraud, S., and Béguelin, S.Z.: Computer-aided security proofs for the working cryptographer. In: Advances in Cryptology - CRYPTO 2011. Lecture Notes in Computer Science, vol. 6841, pp. 71–90 (2011).
11. Blanchet, B.: Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif. In: Foundations and Trends in Privacy and Security. vol. 1, num. 1-2, pp.1–135 (2016).

A Novel Non-Interactive Multi-party Key Exchange from Homomorphic Encryption

Rakyong Choi and Kwangjo Kim

School of Computing, KAIST
{thepride,kkj}@kaist.ac.kr

Abstract. In this paper, we consider the problem of key exchange among n parties. There are several multi-party key exchange schemes like group key exchange protocols. But, most of them are interactive key exchange protocols with more overhead.
Thus, we give a new generic approach to construct a non-interactive multi-party key exchange protocol without trusted third party. For that, we use the concept of homomorphic encryption scheme and generate a Boolean circuit to generate the ephemeral common key for n parties. We can achieve quantum-resistance with the lattice-based homomorphic encryption scheme from the literature.

Keywords: Non-interactive Key Exchange · Homomorphic Encryption · Group Key Exchange

1 Introduction

Since the seminal work by Diffie and Hellman [11], the need for a key exchange protocol over an insecure channel becomes essential to prevent unauthorized access or accidental disclosure of the information while transmission process between entities over an insecure network. Communicating between two entities on a public network needs to be secure to prevent any attacks to read transmitted messages. Secure transmission means encrypting the message with an encryption key and then sending it from one entity to another. The problem is how to share the key between two entities securely. For that, we use key exchange protocols which identifies each entity to another, create and distribute the key among them securely.

Homomorphic encryption supports any computation on encrypted data without decryption key. After Gentry's paper [15] in 2009, there are a number of research on homomorphic encryption based on ideal lattices, (ring-)LWE problem, and Approximate GCD problem [6, 7, 16, 24]. Homomorphic encryption is applicable to various areas using outsourcing computation like machine learning methods for encrypted data [9, 17, 18] or two-party key exchange protocol [21].

In this paper, we suggest a generic approach to construct a non-interactive multi-party key exchange protocol from rich cryptographic ingredients like homomorphic encryption scheme.

1.1 Outline of the Paper

The rest of this paper is structured as follows. We review the history of group key exchange protocol and homomorphic encryption scheme briefly in Chapter 2. We give the definition of non-interactive key exchange, homomorphic encryption, and homomorphic encryption scheme in Chapter 3. Then, we propose a new methodology to construct a non-interactive multi-party key exchange protocols without trusted third party in Chapter 4 and compare it with previous protocols in Chapter 5. Finally, we give a conclusion with future work in Chapter 6.

2 Previous Work

2.1 Group Key Exchange

A group key exchange (GKE) protocol is a multi-party key exchange protocol in which a shared secret is derived from n parties as a function of the information contributed by each of these. In GKE protocol, every group member has to interact in order to compute the group key and no entity can predetermine the resulting value. GKE protocol does not require the existence of secure channels between its participants since no secure transfer takes place during the processing.

Tree-based GKE is one method to obtain a common session key by some tree structure. For example, in Kim *et al.*'s paper [20], all user is considered as a leaf node of the tree and thus, no parties have higher authority.

In the paradigm of provable security, Bresson *et al.* [8] suggested the first security model for GKE protocols with two major security notions. The first notion is authenticated key exchange (AKE) security which requires the indistinguishability of computed group keys from random keys and the second notion is mutual authentication (MA) security which means that two parties authenticate mutually.

For quantum-resistant multi-party key exchange protocols, Ding *et al.* [12] constructed the lattice-based interactive multi-party GKE protocol and recently, Boneh *et al.* [4] proposed the non-interactive key exchange protocols from isogenies on elliptic curves.

2.2 Homomorphic Encryption

Since Rivest *et al.* [23] questioned whether there exist any encryption schemes that are homomorphic under any group/ring/field operations, which allows to perform arbitrary computation on the input data, it had been remained as an interesting open problem in cryptography for decades.

After Gentry's breakthrough paper [15] in 2009, many attempts are dedicated to make more efficient homomorphic encryption schemes based on LWE, Ring-LWE, and approximate GCD problems [5–7, 14, 16, 24].

For key agreement protocol, Krendelev and Kuzmin [21] recently proposed two-party key exchange protocol based on homomorphic encryption but their protocol misses the security proof and it considers two parties only.

3 Preliminaries

In this chapter, we review the definition of non-interactive key exchange protocol and homomorphic encryption scheme.

Definition 1. (non-interactive key exchange) A key exchange protocol is *non-interactive* when the protocol enables two parties who know each other's public key to agree on a shared common key without requiring any interaction and a multi-party key exchange protocol is *non-interactive* when there is no interaction between n parties.

Definition 2. (homomorphic encryption) A homomorphic encryption scheme $\mathcal{HE}$ is a tuple of PPT algorithms $\mathcal{HE} = (\mathsf{HE.Gen}, \mathsf{HE.Enc}, \mathsf{HE.Eval}, \mathsf{HE.Dec})$ with the following functionality:

$\mathsf{HE.Gen}(n, \alpha)$:
Given the security parameter n and an auxiliary input α, this algorithm outputs a key triple (pk, sk, evk), where pk is the key used for encryption, sk is the key used for decryption and evk is the key used for evaluation.

$\mathsf{HE.Enc}(pk, m)$:
Given a public key pk and a message m, this algorithm outputs a ciphertext c of the message m.

$\mathsf{HE.Eval}(evk, C, c_1, \cdots, c_n)$:
Given an evaluation key evk, a Boolean circuit C, and pairs $\{c_i\}_{i=1}^{n}$ where c_i is either a ciphertext or previous evaluation results, this algorithm produces an evaluation output.

$\mathsf{HE.Dec}(sk, c)$:
Given a secret key sk and a ciphertext or an evaluation output c, this algorithm outputs a message m.

4 Our Approach

In this chapter, we propose how to construct multi-party key exchange protocol with rich ingredients. Our construction can be considered as quantum-resistant protocol if we use lattice-based key exchange protocol and lattice-based homomorphic encryption scheme as underlying cryptographic protocols.

4.1 Security Model

In the following methods, we assume that the server is honest but curious so that the server should not be able to gain any information on the value of that session key during the protocol. Also, we assume that all parties are fully trusted so that no one can reveal the other's ephemeral key.

We assume that the adversary $\mathcal{A}$ can make queries to any instance as the former security modelling of key exchange protocols [1–3]. $\mathcal{A}$ can send messages

to some party, run the protocol to get the appropriate session key, and reveal the some session key but $\mathcal{A}$ cannot corrupt a party for any insider attacks.

To check the security of our multi-party key exchange protocol, we have to prove the following security requirements:

1. **Session key security**
   If uncorrupted parties in the proposed protocol complete matching sessions, they have the same key and the probability that the adversary guesses whether the key is from the protocol or from random is negligible. This can be interpreted as AKE security from Bresson *et al.*'s paper about the security model of GKE protocols [8].
2. **Known key security**
   Even after an adversary $\mathcal{A}$ has acquired one particular session key, other session keys are still secure.
3. **Key privacy**
   In the proposed protocol, the server should not be able to gain any information on the value of the session key, even though the server's help is mandatory to establish a session key between n parties in the protocol.
4. **Resistance to other various attacks**
   The protocol should withstand well-known network attacks such as user impersonation and modification attacks as well as man-in-the-middle attacks.

With these security requirements, we will check the validity of our multi-party key exchange protocol under the security of the given homomorphic encryption scheme.

Compared to Bresson *et al.*'s security requirement, we miss the security notion of mutual authentication since the underlying homomorphic encryption guarantees that the protocol outputs a valid output only if each party behaves honestly.

4.2 Construction with Homomorphic Encryption

In Fig. 1, we give a generic construction of non-interactive multi-party key exchange protocols from homomorphic encryption. As tree-based group key exchange protocol by Kim *et al.* [20], we restrict the parties to be located in the leaf node of the given graph (or a given circuit). Red rectangle box shows the area that remains hidden from outsiders and every party pre-shares the same key sk from $\mathsf{HE.Gen}$ algorithm of homomorphic encryption scheme $\mathcal{HE}$, like password-authenticated key exchange protocols. Note that a circuit C can be public in our protocol.

Under this condition, our protocol runs as follows.

Step 1. Make the Boolean circuit C with n inputs.

Step 2. Each party makes ephemeral session key k_i and encrypt it with public key pk, $c_i = \mathsf{HE.Enc}(pk, k_i)$.

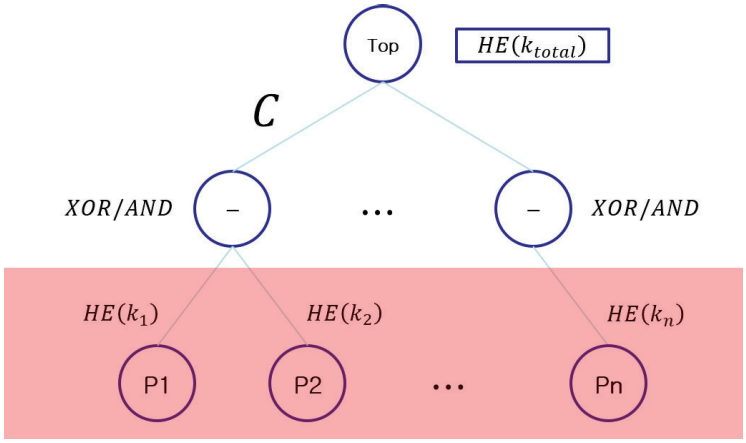


Fig. 1: Multi-party Key Exchange Protocol from Homomorphic Encryption

Step 3. Run evaluation algorithm $c = \mathsf{HE.Eval}(evk, C, c_1, \cdots, c_n)$ given the Boolean circuit C.

Step 4. Each party decrypts the evaluation value c and get the session group key $k = \mathsf{HE.Dec}(sk, c)$.

Theorem 1. *If underlying homomorphic encryption scheme $\mathcal{HE}$ is secure, our non-interactive multi-party key exchange protocol is also secure, i.e., it satisfies session key security, known key security, and key privacy.*

Proof. (sketch)

1. **Session key security**
   Since $\mathcal{HE}$ is secure, each ciphertext and evaluation value are distinguishable from random. Thus, all ciphertext c_i of the ephemeral session key k_i from party i are indistinguishable from random and so does the ciphertext c of the session group key k, evaluation value of all the ciphertext $c_i's$. Hence, our construction guarantees session key security.
2. **Known key security**
   Each session group key does not reveal the ephemeral session key k_i since the evaluation value k does not leak the information of the values in the circuit C. Even more, the party chooses different ephemeral session key k_i for each session. Hence, we cannot guess the previous session group key from one particular session group key. *i.e.*, we can guarantee known key security for our protocol.
3. **Key privacy**
   Since the server doesn't have the information of the pre-shared secret key sk, the server is not possible to know the session group key k but the evaluation value of it. As we stated in the session key security proof, evaluation value is

distinguishable from random when $\mathcal{HE}$ is secure and thus, our construction provides key privacy.

5 Comparison with Other Method

In Table 1, we compare our construction with other previous approaches like Kim *et al.*'s tree-based GKE protocol [20] and lattice-based multi-party key exchange protocols by Ding *et al.* [12].

Since Ding *et al.*'s protocol interacts one to each other, its complexity is $O(n^2)$, where n is the number of group members for group key agreement protocol. Meanwhile, our method can be achieved in $O(n)$ complexity with natural tree structure in the design.

Compared to other two methods, our method is non-interactive and does not need any fully-trusted third party in the protocol. We only need a server which is honest but curious. Also, our method can become a quantum-resistant group key agreement protocol if we adopt lattice-based homomorphic encryption scheme from the literature, like [16], for example.

Table 1: Comparison of group key agreement protocols

Method	Tree-based GKE [20]	DXL12 [12]	Ours
Communication Complexity[a]	$O(n)$	$O(n^2)$	$O(n)$
Non-interactivity[b]	X	X	**O**
Trusted Third Party[c]	O	**X**	**X**
Quantum Resistance[d]	X	**O**	△ [e]

[a] n is the number of group members for group key agreement protocol.
[b] O: protocol is non-interactive, O: protocol is interactive
[c] O: protocol needs the trusted third party, X: protocol doesn't need any trusted third party
[d] O: quantum-resistant, X: vulnerable to quantum computing attacks
[e] △: our design is quantum-resistant if the underlying homomorphic encryption scheme was designed to be quantum-resistant.

6 Concluding Remark

In this paper, we construct a novel method to design non-interactive multi-party key exchange protocol using homomorphic encryption scheme and compare this method with other protocols like tree-based group key exchange by Kim *et al.* [20] and lattice-based multi-party key exchange protocol by Ding *et al.* [12]

Our construction is a kind of group key exchange protocol and shares some properties that tree-based group key exchange and password-authenticated key exchange protocols.

As future work, first among several directions, we will adopt our generic construction to Gentry *et al.*'s well-known lattice-based homomorphic encryption scheme paper in CRYPTO 2013 [16]. Then, we will give the more concrete security proof including forward secrecy, where forward secrecy states that even if a party's long-term key is leaked to the adversary, the adversary is not able to acquire previous session keys, even though the adversary actively interfered, or tried to act as a man-in-the-middle attack. We will check security proof in both classical and quantum adversaries.

We also consider implementation of our quantum-resistant multi-party non-interactive key exchange protocol using some lattice-based libraries with homomorphic encryption tools like HElib and FHEW [13, 19].

Besides that, we leave the followings as challenging issues:

1) When each party has the different secret key. (We may use a multi-key variant of homomorphic encryption scheme [10, 22] instead of vanilla homomorphic encryption.)
2) When dynamic group settings are considered instead of static group setting so that the tree structure becomes updated.

Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00555, Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World).

References

1. Bellare, M., Pointcheval, D., and Rogaway, P. Authenticated key exchange secure against dictionary attacks. In *Advances in Cryptology–EUROCRYPT 2000* (2000), Springer, pp. 139–155.
2. Bellare, M., and Rogaway, P. Entity authentication and key distribution. In *Advances in Cryptology–CRYPTO'93* (1993), Springer, pp. 232–249.
3. Bellare, M., and Rogaway, P. Provably secure session key distribution: the three party case. In *Annual ACM symposium on Theory of computing* (1995), ACM, pp. 57–66.
4. Boneh, D., Glass, D., Krashen, D., Lauter, K., Sharif, S., Silverberg, A., Tibouchi, M., and Zhandry, M. Multiparty non-interactive key exchange and more from isogenies on elliptic curves. *arXiv preprint arXiv:1807.03038* (2018).
5. Brakerski, Z., Gentry, C., and Vaikuntanathan, V. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT) 6*, 3 (2014), 13.
6. Brakerski, Z., and Vaikuntanathan, V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Advances in Cryptology–CRYPTO 2011*. Springer, 2011, pp. 505–524.
7. Brakerski, Z., and Vaikuntanathan, V. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing 43*, 2 (2014), 831–871.

8. Bresson, E., Chevassut, O., Pointcheval, D., and Quisquater, J.-J. Provably authenticated group diffie-hellman key exchange. In *Proceedings of the 8th ACM conference on Computer and Communications Security* (2001), ACM, pp. 255–264.
9. Cheon, J. H., Kim, M., and Lauter, K. Homomorphic computation of edit distance. In *International Conference on Financial Cryptography and Data Security* (2015), Springer, pp. 194–212.
10. Clear, M., and McGoldrick, C. Multi-identity and multi-key leveled fhe from learning with errors. In *Annual Cryptology Conference* (2015), Springer, pp. 630–656.
11. Diffie, W., and Hellman, M. New directions in cryptography. *IEEE transactions on Information Theory 22*, 6 (1976), 644–654.
12. Ding, J., Xie, X., and Lin, X. A simple provably secure key exchange scheme based on the learning with errors problem. *IACR Cryptology ePrint Archive 2012/688* (2012).
13. Ducas, L., and Micciancio, D. Fhew: bootstrapping homomorphic encryption in less than a second. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2015), Springer, pp. 617–640.
14. Fan, J., and Vercauteren, F. Somewhat practical fully homomorphic encryption. *IACR Cryptology ePrint Archive 2012* (2012), 144.
15. Gentry, C. Fully homomorphic encryption using ideal lattices. In *Annual ACM on Symposium on Theory of Computing* (2009), ACM, pp. 169–178.
16. Gentry, C., Sahai, A., and Waters, B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology–CRYPTO 2013*. Springer, 2013, pp. 75–92.
17. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., and Wernsing, J. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In *International Conference on Machine Learning* (2016), pp. 201–210.
18. Graepel, T., Lauter, K., and Naehrig, M. Ml confidential: Machine learning on encrypted data. In *International Conference on Information Security and Cryptology* (2012), Springer, pp. 1–21.
19. Halevi, S., and Shoup, V. Algorithms in helib. In *International Cryptology Conference* (2014), Springer, pp. 554–571.
20. Kim, Y., Perrig, A., and Tsudik, G. Tree-based group key agreement. *ACM Transactions on Information and System Security (TISSEC) 7*, 1 (2004), 60–96.
21. Krendelev, S., and Kuzmin, I. Key exchange algorithm based on homomorphic encryption. In *Computer Science and Information Systems (FedCSIS), 2017 Federated Conference on* (2017), IEEE, pp. 793–795.
22. López-Alt, A., Tromer, E., and Vaikuntanathan, V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing* (2012), ACM, pp. 1219–1234.
23. Rivest, R. L., Adleman, L., and Dertouzos, M. L. On data banks and privacy homomorphisms. In *Foundations of secure computation 4.11* (1978), pp. 169–180.
24. Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. Fully homomorphic encryption over the integers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2010), Springer, pp. 24–43.