**Lecture Notes in Computer Science** **10726**

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7410

Xiaofeng Chen · Dongdai Lin
Moti Yung (Eds.)

# Information Security and Cryptology

13th International Conference, Inscrypt 2017
Xi'an, China, November 3–5, 2017
Revised Selected Papers

Springer

*Editors*
Xiaofeng Chen
Xidian University
Xi'an
China

Moti Yung
Columbia University
New York, NY
USA

Dongdai Lin
SKLOIS, Institute of Information Engineering
Chinese Academy of Sciences
Beijing
China

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-75159-7 ISBN 978-3-319-75160-3 (eBook)
https://doi.org/10.1007/978-3-319-75160-3

Library of Congress Control Number: 2018931889

LNCS Sublibrary: SL4 – Security and Cryptology



Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The 13th International Conference on Information Security and Cryptology (Inscrypt 2017) was held during November 3–5, 2017, in Xi'an, China. This volume contains the papers presented at Inscrypt 2017. The Program Committee also invited five distinguished researchers to deliver keynote talks. The keynote speakers were Elisa Bertino from Purdue University, USA; Yang Xiang from Swinburne University of Technology, Australia; Mirosław Kutyłowski from Wroclaw University of Technology, Poland; Yunlei Zhao from Fudan University, China; and Kui Ren from University at Buffalo, USA. Inscrypt is a well-recognized annual international forum for security researchers and cryptographers to exchange ideas and present their work, and is held every year in China.

The conference received 80 submissions. Each submission was reviewed by at least three Program Committee members. The committee accepted 27 papers to be included in the conference program. The proceedings contain revised versions of the accepted papers. While revisions are expected to take the reviewers' comments into account, this was not enforced and the authors bear full responsibility for the content of their papers.

Inscrypt 2017 was held in cooperation with the International Association for Cryptologic Research (IACR), and was co-organized by the School of Cyber Engineering, Xidian University, the State Key Laboratory of Information Security (SKLOIS) of the Institute of Information Engineering of Chinese Academy of Science, and the Chinese Association for Cryptologic Research (CACR). Furthermore, Inscrypt 2017 was sponsored by the State Key Laboratory of Integrated Services Networks (ISN) and National 111 Center of Mobile Internet Security (111 project No. B16037), Xidian University. The conference would not have been a success without the support of these organizations, and we sincerely thank them for their continued assistance and support.

We would also like to thank the authors who submitted their papers to Inscrypt 2017, and the conference attendees for their interest and support. We thank the Organizing Committee for their time and effort dedicated to arranging the conference. This allowed us to focus on selecting papers and dealing with the scientific program. We thank the Program Committee members and the external reviewers for their hard work in reviewing the submissions; the conference would not have been possible without their expert reviews. Finally, we thank the EasyChair system and its operators, for making the entire process of managing the conference convenient.

November 2017

Xiaofeng Chen
Dongdai Lin
Moti Yung

# Inscrypt 2017

## 13th International Conference on Information Security and Cryptology

## Xi'an, China November 3–5, 2017

*Sponsored and organized by*

State Key Laboratory of Integrated Services Networks (ISN)
National 111 Project for Mobile Internet Security (Xidian University)
State Key Laboratory of Information Security
(Chinese Academy of Sciences)
Chinese Association for Cryptologic Research

**in cooperation with**

International Association for Cryptologic Research

## Honorary Chairs

| | |
|---|---|
| Xinbo Gao | Xidian University, China |
| Dongdai Lin | Chinese Academy of Sciences, China |

## Steering Committee

| | |
|---|---|
| Feng Bao | Huawei International, Singapore |
| Kefei Chen | Hangzhou Normal University, China |
| Dawu Gu | Shanghai Jiao Tong University, China |
| Xinyi Huang | Fujian Normal University, China |
| Hui Li | Xidian University, China |
| Dongdai Lin | Chinese Academy of Sciences, China |
| Peng Liu | Pennsylvania State University, USA |
| Wenfeng Qi | National Digital Switching System Engineering and Technological Research Center, China |
| Meiqin Wang | Shandong University, China |
| Xiaofeng Wang | Indiana University at Bloomington, USA |
| Xiaoyun Wang | Tsinghua University, China |
| Jian Weng | Jinan University, China |

| | |
|---|---|
| Moti Yung | Snapchat Inc. and Columbia University, USA |
| Fangguo Zhang | Sun Yat-Sen University, China |
| Huanguo Zhang | Wuhan University, China |

## Technical Program Committee

| | |
|---|---|
| Erman Ayday | Bilkent University, USA |
| Ioana Boureanu | University of Surrey, UK |
| Donghoon Chang | NIST, USA |
| Kai Chen | Chinese Academy of Sciences, China |
| Kefei Chen | Hangzhou Normal University, China |
| Xiaofeng Chen | Xidian University, China |
| Cunsheng Ding | Hong Kong University of Science and Technology, Hong Kong, SAR China |
| Jintai Ding | University of Cincinnati, USA |
| Karim Eldefrawy | SRI International, USA |
| Chun-I Fan | National Sun Yat-sen University, Taiwan, China |
| Debin Gao | Singapore Management University, Singapore |
| Dawu Gu | Shanghai Jiao Tong University, China |
| Huaqun Guo | Institute for Infocomm Research, Singapore |
| Jian Guo | Nanyang Technological University, Singapore |
| Weili Han | Fudan University, China |
| Lucjan Hanzlik | Wrocław University of Technology, Poland |
| Lei Hu | Institute of Information Engineering of CAS, China |
| Xinyi Huang | Fujian Normal University, China |
| Miroslaw Kutylowski | Wroclaw University of Technology, Poland |
| Kwangsu Lee | Sejong University, South Korea |
| Tieyan Li | Huawei International, Singapore |
| Yingjiu Li | Singapore Management University, Singapore |
| Dongdai Lin | Chinese Academy of Sciences, China |
| Zhe Liu | University of Waterloo, Canada |
| Florian Mendel | TU Graz, Austria |
| Mridul Nandi | Indian Statistical Institute, India |
| Josef Pieprzyk | Queensland University of Technology, Australia |
| Kouichi Sakurai | Kyushu University, Japan |
| Willy Susilo | University of Wollongong, Australia |
| Qiang Tang | Cornell University, USA |
| Qian Wang | Wuhan University, China |
| Wenling Wu | Chinese Academy of Science, China |
| Shouhuai Xu | University of Texas at San Antonio, USA |
| Yu Yu | Shanghai Jiao Tong University, China |
| Moti Yung | Columbia University, USA |
| Fangguo Zhang | Sun Yat-sen University, China |
| Xianfeng Zhao | Chinese Academy of Sciences, China |
| Yongjun Zhao | The Chinese University of Hong Kong, Hong Kong, SAR China |
| Cliff Zou | University of Central Florida, USA |

## Additional Reviewers

Agrawal, Megha
Alkadri, Nabil
Anada, Hiroaki
Bao, Zhenzhen
Blaskiewicz, Przemyslaw
Chen, Huashan
Chen, Yi
Chow, Sherman S. M.
Cui, Tingting
Dai, Ting
Ding, Ning
Dobraunig, Christoph
Fang, Chengfang
Feng, Yaokai
Gao, Xinwei
Garcia Lebron, Richard
Garg, Surabhi
Guo, Jiale
Guo, Qian
Huang, Yan
Jia, Haoyang
Jiang, Linzhi
Kim, Hyoseung
Kim, Jonghyun
Kumar Chauhan, Amit
Kumar, Abhishek
Larangeira, Mario
Lee, Youngkyung
Li, Huige
Li, Lingchen
Li, Sisi
Li, Xiangxue
Li, Zengpeng
Lin, Hsiao Ying
Liu, Guozhen
Liu, Jianghua
Liu, Ximing
Liu, Zhen
Long, Yu
Lu, Yuan
Mishra, Sweta
Nakano, Yuto
Nogami, Yasuyuki
Pan, Yanbin
Ruj, Sushmita
Rv, Sara
Seo, Minhye
Shahandashti, Siamak
Song, Ling
Sui, Han
Sun, Siwei
Tian, Yangguang
Unterluggauer, Thomas
Wang, Daibin
Wang, Fuqun
Wang, Haoyang
Wang, Huige
Wang, Lei
Wang, Liangliang
Wang, Weijia
Wang, Yuntao
Xie, Shaohao
Xu, Jiayun
Xu, Lingling
Yang, Anjia
Yang, Shao-Jun
Yu, Yong
Yuen, Tsz Hon
Zha, Mingming
Zhang, Huang
Zheng, Yafei
Zhong, Chen
Zong, Peiyuan

# Keynote Speeches

# AI-Driven Cyber Security

Yang Xiang

Swinburne University of Technology, Hawthorn VIC 3122, Australia
yxiang@swin.edu.au

Today we have evidenced massive cyber-attacks, such as WannaCry ransomware, having hit millions of people in more than 150 countries with billions of dollars lose. Cyber security has become one of the top priorities globally in the research and development agenda [1].

Recent years, Artificial Intelligence (AI) [2] has been widely used in numerous fields and industries, including finance, healthcare, education, and transportation, support-ed by a diversity of datasets from a huge number of sources in different domains [3, 4]. These datasets consist of multiple modalities, each of which has a different representation, distribution, scale, and density [5–8].

In addition, with the increase of AI based software like digital services and products, software vulnerability detection [8] that certify the security of using the AI-based Software has become an important research area in both academia and industries [9]. The number of vulnerabilities has been reported to be positively correlated to the volume of the software copies. For example, in 2010, there were about only 4500 vulnerabilities registered in the well-known CVE (Common Vulnerabilities and Expo-sures) database [10], however, this number increased to 17265 in 2017. In another example, more than 43000 software vulnerabilities have been reported via NVD (National Vulnerability Database) since 1997 [11]. These vulnerabilities affected more than 17000 software services and caused about 266 billion dollars losses a year [12]. The trend seems to be increasing with the increase of AI-based software services.

People have recognized that AI technologies are some of the most effective defenses against cyber intrusions [13]. Cyber security companies are increasingly looking to AI to improve defense systems and create the next generation of cyber protection. In this respect, machine learning-based software vulnerable detection techniques are becoming an important research area with the increasingly rich of vulnerability related data. A few important questions have been asked, such as:

- How AI models learn and understand what is normal and what is abnormal on a system?
- How AI that uses machine learning and other technologies can differentiate benign or harmful binary or source codes?
- How can hackers bypass AI-driven security solutions?

Although AI has been talked as one of the game-changing technologies for cyber security, many doubts still persist. New methods and tools, consequently, must follow up in order to adapt to this emerging security paradigm. In this talk, we will discuss the concept of AI-Driven Cyber Security and how data analytics can be used to ad-dress the security and privacy problems in cyberspace. We will outline how deep learning

can learn high-level representations based on the source code we collected and labelled. Deep learning is in part due to an ability to learn feature representations and complex non-linear structure in datasets. Deep learning has achieved particular successes in data domains such as vision, speech and natural language, which each exhibit hierarchies of patterns at fine to coarse scales. Software vulnerability detection is ready for similar success owing to its complex, hierarchical, non-linear detection tasks. For example, in one of our research that using deep learning for software vulnerability detection on cross-project scenario. We first collected datasets from three open-source projects: Libtiff, LibPNG and FFmpeg [8]. Then, the raw features are extracted from the Abstract Syntax Trees (ASTs) of functions. Afterwards, a stacked LSTM network is designed and a proxy for learning ASTs representations of functions is introduced. Finally, classification models are built based on the feature representation learned from the LSTM network.

## References

1. Lee, K.-C., Hsieh, C.-H., Wei, L.-J., Mao, C.-H., Dai, J.-H., Kuang, Y.-T.: Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and time-line event annotation. Soft. Comput. **21**(11), 2883–2896 (2017)
2. Nilsson, N.J.: Principles of Artificial Intelligence. Morgan Kaufmann (2014)
3. Zhang, J., Xiang, Y., Wang, Y., Zhou, W., Xiang, Y., Guan, Y.: Network traffic classification using correlation information. IEEE Trans. Parallel Distrib. Syst. **24**(1), 104–117 (2013)
4. Chen, C., Wang, Y., Zhang J., Xiang, Y., Zhou, W., Min, G.: Statistical features-based real-time detection of drifted twitter spam. IEEE Trans. Inf. Forensics Secur. **12**(4), 914–925 (2017)
5. Wen, S., Zhou, W., Xiang, Y., Zhou, W.: CAFS: a novel lightweight cache-based scheme for large-scale intrusion alert fusion. Concurrency Comput. Pract. Experience **24**(10), 1137–1153 (2012)
6. Liu, S., Zhang, J., Xiang, Y., Zhou, W.: Fuzzy-based information decomposition for incomplete and imbalanced data learning. IEEE Trans. Fuzzy Syst. **25**(6), 1476–1490 (2017)
7. Ghaffarian, S.M., Shahriari, H.R.: Software vulnerability analysis and discovery using machine-learning and data-mining techniques: a survey. ACM Comput. Surv. (CSUR) **50**(4), 56 (2017)
8. Lin, G., Zhang, J., Luo, W., Pan, L., Xiang, Y.: Poster: vulnerability discovery with function representation learning from unlabeled projects. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 2539–2541. ACM (2017)
9. Zhang, Z.-K., Cho, M.C.Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., Shieh, S.: IoT security: ongoing challenges and research opportunities. In: IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA), pp. 230–234. IEEE (2014)
10. Perl, H., et al.: Vccfinder: finding potential vulnerabilities in open-source projects to assist code audits. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 426–437. ACM (2015)
11. Zhang, S., Ou, X., Caragea, D.: Predicting cyber risks through national vulnerability database. Inf. Secur. J. Global Perspect. **24**(4–6), 194–206 (2015)

12. Alves, H., Fonseca, B., Antunes, N.: Experimenting machine learning techniques to predict vulnerabilities. In: Seventh Latin-American Symposium on Dependable Computing (LADC), pp. 151–156. IEEE (2016)
13. Yampolskiy, R.V., Spellchecker, M.: Artificial intelligence safety and cybersecurity: a timeline of AI failures (2016). arXiv preprint, arXiv:1610.07997

# Generic and Efficient Lattice-Based Key Exchange from Key Consensus with Noise

Yunlei Zhao

School of Computer Science, Fudan University, Shanghai, China

Lattice-based cryptography is promising in the post-quantum era. For cryptographic usage, compared with the classic hard lattice problems such as SVP and CVP, the learning with errors (LWE) problem and its variants are proven to be much more versatile. Based upon them, a large number of impressive works are developed in recent years, with key exchange (KE) as the focus of this work.

For KE and public-key encryption (PKE) schemes from LWE and its variants, a key ingredient is the key reconciliation mechanisms. However, they were only previously used and analyzed in a *non-black-box* way. This means, for new KE or PKE schemes developed in the future, we need to analyze from scratch. Also, for the various parameters involved in key reconciliation, the bounds on what could or couldn't be achieved are unclear.

In this work, we abstract and study this key ingredient. Specifically, we formalize the building tool, referred to as key consensus (KC) and its asymmetric variant AKC. KC and AKC allow two communicating parties to reach consensus from close values obtained by some secure information exchange (such as exchanging LWE samples). KC and AKC are fundamental to lattice based cryptography, in the sense that a list of cryptographic primitives based on LWE and its variants can be constructed from them *in a modular and black-box way*. As a conceptual contribution, this much simplifies the design and analysis of these cryptosystems in the future.

Abstracting KC and AKC also allows us to study and prove the inherent upper-bounds among the parameters. In particular, we discover the upper-bounds on parameters for any KC and AKC. This allows us to understand what can or cannot be achieved with any KC and AKC, and guides our actual protocol design. These upper-bounds also guide parameter choosing for various trade-offs, and are insightful in performance comparison.

Guided by, and motivated for reaching, these proved upper-bounds, we then design and analyze both general and highly practical KC and AKC schemes, which are referred to as OKCN and AKCN respectively for presentation simplicity. Both OKCN and AKCN almost meet the proved upper-bounds in general, and can be instantiated to tightly match these upper-bounds. Moreover, they are the first multi-bit reconciliation

---

Extended abstract of the work joint with Zhengzhong Jin, which originally appeared at arXiv: https://arxiv.org/abs/1611.06150. This research was supported in part by NSFC (Grant Nos. 61472084 and U1536205), National Key R&D Program of China (No.2017YFB0802000), Shanghai innovation action project No. 16DZ1100200, and Shanghai science and technology development funds No.16JC1400801.

mechanisms, to the best of our knowledge. We note that OKCN and AKCN have already been influential, and are used in some concurrent subsequent works. For example, some versions of AKCN were used in the schemes of Lizard (Cryptology ePrint Archive, 2016/1126) and Kyber (Cryptology ePrint Archive, 2017/634).

Based on KC and AKC, we present generic constructions of key exchange from LWE and its variants: LWR, RLWE and MLWE, with delicate analysis of error probabilities. Then, for the instantiations of these generic constructions with our OKCN and AKCN schemes, we elaborate on evaluating and choosing the concrete parameters in order to achieve a well-balanced performance among security, computational efficiency, bandwidth efficiency, error rate, and operation simplicity. At a high level, OKCN-based KE corresponds to Diffie-Hellman in the lattice world, while AKCN-based KE is not. Specifically, with AKCN, the responder can predetermine and set the shared-key at its wish. But AKCN-based KE can be directly used for CPA-secure PKE. We suggest that OKCN-based KE is more versatile, and is more appropriate for incorporating into the existing standards like IKE and TLS.

We propose the first construction of key exchange *merely* based on the LWR problem with concrete analysis and evaluation, to the best of our knowledge. In particular, we provide a delicate approach to calculating its error rate. Specifically, for the LWR-based KE protocol, the main difficulty here is the error probability analysis: the rounding operation in LWR brings new noises, yet these noises are *deterministic*, because they are completely determined by the public matrix and the secret vector. In the formula calculating the error probability, the deterministic noises will multiply the secret vector. However, they are correlated. This correlation prevents us from calculating the error probability efficiently. This is a new difficulty we encounter in LWR-based KE. Our contribution is to provide an analysis breaking the correlation, and design an algorithm to calculate the error probability numerically. When applied to LWE-based cryptosystems, OKCN can directly result in more practical or well-balanced schemes of key exchange. The comparisons between OKCN-based KE and Frodo, proposed by Bos et al. at ACMCCS2016, are briefly summarized in Table 1.

**Table 1.** Brief comparison between OKCN-LWE/LWR and Frodo. $|\mathbf{K}|$ refers to the size in bits of the shared key; "bw.(kB)" refers to bandwidth in kilo bytes; "err." refers to the error rate, and "pq-sec" refers to the best known quantum attack against the underlying lattice problem.

| | $\|\mathbf{K}\|$ | bw.(kB) | err. | pq-sec |
|---|---|---|---|---|
| OKCN-LWR | 256 | 16.19 | $2^{-30}$ | 130 |
| OKCN-LWE | 256 | 18.58 | $2^{-39}$ | 134 |
| Frodo | 256 | 22.57 | $2^{-38.9}$ | 130 |

When applying OKCN/AKCN to MLWE-based KE, they result in the (up-to-date) most efficient lattice-based key exchange protocols for 256-bit shared-key. MLWE is a variant between LWE and RLWE. On the one hand, MLWE-based protocols are more efficient than LWE-based; And on the other hand, they are more secure than RLWE-based, as the MLWE problem has fewer algebraic structures than RLWE.

**Table 2.** Brief comparison between OKCN/AKCN-MLWE and Kyber.

| | $\|\mathbf{K}\|$ | bw.(B) | err. | pq-sec |
|---|---|---|---|---|
| OKCN-MLWE-KE | 256 | 1856 | $2^{-50.1}$ | 183 |
| OKCN-MLWE-PKE | 256 | 2048 | $2^{-166.4}$ | 171 |
| AKCN-MLWE-PKE (Kyber) | 256 | 2272 | $2^{-142.7}$ | 171 |

The comparisons between OKCN/AKCN-MLWE and CPA-secure Kyber are briefly summarized in Table 2.

When applied to RLWE-based cryptosystems, AKCN can lead to the most efficient KE protocols with shared-key of size of at least 512 bits, which may be prudent for ensuring 256-bit post-quantum security in reality. For RLWE-based KE, we develop new approaches to lowering the error probability. Firstly, we make a key observation on RLWE-based key exchange, by proving that the errors in different positions in the shared-key are almost independent. This can play a fundamental basis for the approach to lowering error rate of RLWE-based KE with error-correction codes. Then, based upon this observation, we present a super simple and fast code, referred to as *single-error correction* (SEC) code, to correct at least one bit error. By equipping OKCN/AKCN with the SEC code, we achieve the simplest (up to now) RLWE-based KE for much longer shared-key size with error rate that can be viewed as negligible in practice. To further improve the bandwidth, error rate and post-quantum security simultaneously, we develop new lattice code in $E_8$. Note that sphere packing is optimal with the lattice $E_8$. The comparisons with NewHope, proposed by Alkim et al at USENIX Security 2016, are briefly summarized in Table 3.

**Table 3.** Brief comparison between OKCN/AKCN-RLWE and NewHope.

| | $\|\mathbf{K}\|$ | bw.(B) | err. | pq-sec |
|---|---|---|---|---|
| OKCN-RLWE-SEC | 765 | 3392 | $2^{-61}$ | 258 |
| NewHope | 256 | 3872 | $2^{-61}$ | 255 |
| AKCN-RLWE-SEC | 765 | 3520 | $2^{-61}$ | 258 |
| AKCN-RLWE-E8 | 512 | 3360 | $2^{-63.3}$ | 262 |
| NewHope-Simple | 256 | 4000 | $2^{-61}$ | 255 |

# Contents

**Encryption**



**Cryptanalysis and Attack**