SCIENCE CHINA
Information Sciences

• INSIGHT •
Special Focus on Advanced Technology of Software
May 2016, Vol. 59 050106:1–050106:3
doi: 10.1007/s11432-016-5558-0

New trends of information security —how to change people's life style?

Zhenfu CAO

Department of Cryptography and Network Security, School of Computer Science and Software Engineering, East China Normal University, Shanghai 200062*, China*

Received December 28, 2015; accepted January 16, 2016; published online April 12, 2016

Citation Cao Z F. New trends of information security—how to change people's life style? Sci China Inf Sci, 2016, 59(5): 050106, doi: 10.1007/s11432-016-5558-0

Ciphertext refers to encrypted data. During the years of 2007 and 2008, we proposed and solved two problems in information security, namely ciphertext access control and biometric feature matching without storing any biometric features. In 2008, we completed the development of encrypted data sharing mobile devices and then in 2011, we further studied the techniques to address these two problems and embedded them into chips. We believe that the wide adoption of the techniques can essentially change people's life style, since it not only contributes to relieving the bottleneck in cloud computing and big data, but avoids the additional storage and communication overhead brought up by traditional biometric feature matching techniques, therefore adapts better to the scenario of the realtime and efficiency requirements in biometric feature authentication.

With the development in recent years, we suggest three new trends of information security in both theoretical and industrial aspects: "communication channel security plus" model, big data processing in the ciphertext domain and the new method of realizing multiple data security by exploiting the public key encryption only once.

(1) "Communication channel security plus" model. From the publication of "Mathematical Principles in Communication" and "Communication under Noise" respectively in 1948 and 1949 to the emergence of Diffie-Hellman public key cryptosystem and even the attribute-based encryption (ABE) against chosen plaintext attack and adaptive chosen ciphertext attack, only communication channel security model is considered. However, can ABE in this security model well address the issue of ciphertext access control? Definitely not. Let us consider the example of encrypted TV programs. First of all, it is probable for the authorized user to sell or rent the secret key to unauthorized ones, without affecting his own deciphering ability. It results in that each user of the group can successfully watch more TV programs by launching this kind of secret key sharing attack. To effectively resist the security threat, it is required to adopt the security model of traceability to reveal the source of secret key leakage. Moreover, it is also required to exploit the security model of revocability to invalidate the illegally obtained Set-Top boxes duplicating from the leaked secret keys. To integrate the security model of traceability and revocability to the traditional communication channel security model has become a new trend of information security.

(2) Big data processing in the ciphertext domain. Undoubtedly, another trend of information security is big data processing technique, the characteristic of which is effectiveness in the ideal model but ineffectiveness when adversaries exist.

Email: zfcao@sei.ecnu.edu.cn

The reason is that the adversary can store or distribute the manipulated data to lead the errors in computational or statistic results and seriously affect people's life. Therefore, we have suggested the following two solutions: the first one is the UC technique to prove the proposed constructions for big data are computationally indistinguishable between ideal environment and real environment; the other is the technique of big data processing in ciphertext to realize fine-grained access control, keyword searching, pattern matching and statistics from multiple dimensions on encrypted data. Though the results related to the UC technique were not published, it has definitely become one of the most important techniques in the direction of big data processing in the ciphertext domain.

(3) The new method of realizing multiple data security by exploiting the public key encryption only once. It is believed that public key cryptosytems have to be adopted to solve many security issues. For instance, fully homomorphic encryption (FHE) is widely adopted to address the issues of secure outsourced computation and big data in ciphertext. However, can FHE essentially solve these two problems? Absolutely not. The reason is that despite great effort on designing lightweight FHE, its high computational cost still makes it unable to well adapt to the resource-constrained mobile devices. More seriously, directly applying public FHE on data deviates the principle of hybrid encryption that public key encryption is used to encrypt symmetric keys which is further to encrypt the data. Therefore, we proposed the new method for efficient outsourced computation and big data processing in ciphertext domain by reducing the usage times of public key encryption (only once in the optimal case).

With respect to the three trends presented above, we have carried out abundant work of great significance. In 2012, I was invited to publish the first book in the field of multiparty cryptography titled "New Directions of Modern Cryptography" [1], which introduced a series of important results [2–6] on the new trends outlined above. It contributes greatly to a series of basic problems including "communication channel security plus" model, cloud computing and privacy preservation. Since 3 years ago, my team focused on outsourced signal processing security and outsourced data processing security, explored an absolutely new theory in cryptography, and tries to become a theory practitioner from the requirements in reality [7].

In the aspect of "communication channel security plus" model, we have achieved a series of important results. The first is the "communication channel security plus white-box traceability" model. White-box traceability refers to given a secret key, to find its leakage source. The fact that in ciphertext policy ABE (CP-ABE), the deciphering ability of a secret key is shared by all users possessing the same attributes, rather than the secret key holder himself, has brought great difficulties in studying white-box traceability. The existing work tried to solve the problem by scarifying the expressiveness of ciphertext policy (supporting only AND relations). We gave the first white-box traceable CP-ABE supporting any monotonic policies [8], which has the same security and efficiency as the most optimized CP-ABE without traceability. Recently, we further deleted the list in the construction to achieve dynamic scalability [9]. Black-box traceability refers to given a deciphering device without accessing the encapsulated deciphering algorithm and secret key, the algorithm of black-box traceability enables to trace at least one malicious user participating in generating the deciphering device by exploiting it as a deciphering oracle (i.e. providing ciphertext to the device and getting the corresponding plaintexts). We proposed a black-box traceable CP-ABE in a regular paper [10] of ACM CCS 2013. It achieved both the adaptive security (the highest level) and high expressiveness (permitting any monotonic access structure as the policy) with the optimized efficiency to realize black-box traceability, namely adding $O(\sqrt{K})$ elements in ciphertext and public key (K is the number of users in the system) [11]. Revocable ABE mainly comprises two scenarios, namely the authorized case and the unauthorized case. The authorized Scenario refers to the user authorizes a proxy server to re-encrypt a ciphertext with access policy π_1 to another ciphertext with access policy π_2. We proposed the attribute-based proxy re-encryption scheme [12] in ASIACCS 2009, and proved its chosen plaintext/structure security and master key security in the standard model. In the unauthorized Scenario, Dong et al. [13] proposed the first revocation scheme by restricting the set of accessible users. Waters et al. [14] further studied this scenario in CRYPTO 2012 by deleting the revocation list.

In the aspect of big data processing in the ciphertext domain, the existing work focused on achieving efficient outsourced computation by designing lightweight FHE. Following the idea of how to reduce the usage times of public key encryption when it cannot be avoided to achieve privacy preservation, my team proposed the first efficient privacy preserving data aggregation [15,16] by exploiting any one-way trapdoor function (OWTF) without adopting FHE. It realized secure data ag-

gregation on n data by performing the OWTF only once.

In 2008, my team completed the first platform-based encrypted data sharing mobile device with independent intellectual property rights, together with a series of anti-counterfeiting products. In 2011, the first encrypted data sharing chip was successfully devised also with independent intellectual property rights. It filled the gaps in the world by simultaneously addressing the problems of ciphertext access control and biometric feature matching without storing any biometric features.

In the latest 5 years, my team has published more than 180 papers including [17–23] in top cryptography and security conferences and IEEE journal/transaction series, among which there exist 20 papers of CCF A rank, 64 papers of CCF B rank and 53 papers of CCF C rank. Two of my Ph. D. students were awarded as outstanding doctoral dissertation of Shanghai.

References

1 Cao Z F. New Directions of Modern Cryptography. Boca Raton: CRC Press Inc., 2012. 1–400
2 Shao J, Cao Z F, Wang L C, et al. Proxy re-signature schemes without random oracles. In: Proceedings of 8th International Conference on Cryptology in India, Chennai, 2007. 197–209
3 Shao J, Cao Z F. CCA-secure proxy re-encryption without pairings. In: Proceedings of 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, 2009. 357–376
4 Liu Z, Cao Z F, Huang Q, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles. In: Proceedings of 16th European Symposium on Research in Computer Security, Leuven, 2011. 278–297
5 Liang X H, Cao Z F, Lin H, et al. Provably secure and efficient bounded ciphertext policy attribute based encryption. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, 2009. 343–352
6 Lin H, Cao Z F, Liang X H, et al. How to construct interval encryption from binary tree encryption. In: Proceedings of 8th International Conference on Applied Cryptography and Network Security, Beijing, 2010. 19–34
7 Cao Z F. New development of cryptography (in Chinese). J Sichuan Univ Eng Sci Ed, 2015, 47: 1–12
8 Liu Z, Cao Z F, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Trans Inf Forensics Secur, 2013, 8: 76–88
9 Ning J T, Dong X L, Cao Z F, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Trans Inf Forensics Secur, 2015, 10: 1274–1288
10 Liu Z, Cao Z F, Wong D S. Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, 2013. 475–486
11 Liu Z, Cao Z F, Wong D S. Traceable CP-ABE: How to trace decryption devices found in the wild. IEEE Trans Inf Forensics Secur, 2015, 10: 55–68
12 Liang X H, Cao Z F, Lin H, et al. Attribute based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, 2009. 276–286
13 Qian J L, Dong X L. Fully secure revocable attribute-based encryption. J Shanghai Jiaotong Univ Sci Ed, 2011, 16: 490–496
14 Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption. In: Proceedings of 32nd Annual Cryptology Conference, Santa Barbara, 2012. 199–217
15 Zhou J, Dong X L, Cao Z F, et al. Secure and privacy preserving protocol for cloud-based vehicular DTNs. IEEE Trans Inf Forensics Secur, 2015, 10: 1299–1314
16 Zhou J, Cao Z F, Dong X L, et al. Security and privacy in cloud-assisted wireless wearable communications: challenges, solutions and future directions. IEEE Wirel Commun, 2015, 22: 136–144
17 Zhang Z Y, Cao Z F, Ding N, et al. Non-malleable statistically hiding commitment from any one-way function. In: Proceedings of 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, 2009. 303–318
18 Cao Z F, Visconti I, Zhang Z Y. Constant-round concurrent non-malleable statistically binding commitments and decommitments. In: Proceedings of 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, 2010. 193–208
19 Cao Z F, Visconti I, Zhang Z Y. On constant-round concurrent non-malleable proof systems. Inf Process Lett, 2011, 111: 883–890
20 Dong X L, Wei L F, Zhu H J, et al. EP2DF: an efficient privacy preserving data forwarding scheme for service-oriented vehicular ad hoc networks. IEEE Trans Veh Technol, 2011, 60: 580–591
21 Lin H, Zhu X Y, Fang Y G, et al. Efficient trust based information sharing schemes over distributed collaborative network. IEEE J Sel Areas Commun, 2013, 31: 279–290
22 Zhu H J, Du S G, Gao Z Y, et al. A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks. IEEE Trans Parall Distr Syst, 2014, 25: 22–32
23 Zhou J, Lin X D, Dong X L, et al. PSMPA: patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system. IEEE Trans Parall Distr Syst, 2015, 26: 1693–1703