7-5 Structure Preserving Cryptography

Miyako OHKUBO

Cryptography is an essential technology for building secure information systems. Its practical use in secure system design requires specialized knowledge about cryptography while information security is of a common concern in our society as illustrated by privacy issues caused by services using IoT devices.

We propose a new concept called "Structure-Preserving Cryptography" in designing cryptographic applications and present concrete instantiations of structure-preserving cryptographic building blocks such as digital signatures, commitments, and so on. Structure-preserving building blocks have regulated data structure for their input and output so that they can be easily connected each other. Such high interoperability makes the task of developing secure systems easier. Besides, it reduces the cost of development and risk of having flaws due to the use of delicate cryptographic building blocks. Having a regulated data structure prohibits the use of classical mathematical properties. We overcome the difficulty by developing a novel use of mathematical properties over bilinear groups.

Since the first publication of our result in CRYPTO 2010, structure-preserving cryptography has been an active research area. Several structure-preserving schemes have been studied as an interesting target of research, and they are used in number of constructions of cryptographic applications in the literature presented in top-notch international conferences.

1 Introduction

Cryptography is an integral part of information systems, and designing secure and efficient systems requires sophisticated expert knowledge on cryptography. With the increasing proliferation of the Internet of Things, underlying privacy issues have become more apparent, resulting in growing needs for cryptographic applications. As such, maintenance of security has become a serious social challenge. This study proposes a new design concept —"Structure-preserving (SP) Cryptography" [2][11] — that enables simple and secure development of sophisticated cryptographic applications by interconnecting several cryptographic schemes through a specific interface with a unified data format. To move the novel concept into practice, several concrete cryptographic schemes have been developed including SP digital signatures [1][2][5][8]-[12], SP commitments [1][4][11], and others [6][7][10] and the lower bounds of the sizes have been shown [2]-[4].

Provision of easily and efficiently interoperable cryptographic schemes facilitates modular construction of secure systems — like Lego® blocks — as well as reducing cost and risks in development. A classical approach for constructing a cryptographic scheme essentially exploits the differences in data formats from the perspective of mathematical structure. In this study of structure-preserving cryptography, we propose a specific unified data format over a mathematical structure called pairing groups so that useful cryptographic schemes can be built on the same mathematical structure. Since the first efficient SP digital signature scheme[1] was presented in a top-notch international conference, CRYPTO'10, structure-preserving cryptography has become increasingly widespread among the research community. A number of research results in the area of structure-preserving cryptography have been presented in major conferences and journals. Structure-preserving cryptography established an active area in the fundamental research on cryptography.

2 Targeted challenge

Information is a great source of business values and it plays an essential role in social systems. On the flip side,

we are witnessing serious incidents of leaks of essential information such as passwords and "My Number" (Social Security and Tax Number System). Privacy violation while using IoT presents another serious concern. All this stresses the importance of cryptographic technology that contributes to the construction of secure information systems. Advanced applications — such as cloud access control and cryptocurrency represented by Bitcoin — usually interconnect various cryptographic tools: e.g. a message is encrypted using a public-key encryption scheme and the ciphertext is signed using a digital signature scheme. It will be followed by a zero-knowledge proof that the encrypted data is in a legitimate form. Each cryptographic tool is designed so that it guarantees the desired security by itself and the mathematical form of input/output data is conveniently determined according to the security it offers. Such discordance among the interfaces makes it very difficult for the cryptographic schemes to be seamlessly connected, resulting in such inexpediences as larger design cost, use of unrealistic security assumptions, and unexpected vulnerabilities.

To address this challenge, the author has pursued new cryptographic schemes that enable simple and direct interoperation, whose key feature is a unified interface with a specific data format over pairing groups. In typical constructions of cryptographic schemes, the discrepancy in mathematical forms between the input and output contributes to the security of the scheme. For example, in a digital signature scheme, it is a common practice to assign one data form to the target document and another to the signature in order to prevent forgery. This standard approach will no longer be valid if the input and output data are unified into a single mathematical form. Thus, offering interoperability among cryptographic schemes is not just an issue of modifying the interface on the surface but raises an intrinsically-new research challenge.

3 Techniques

Efficient pairing groups used in cryptography have three data forms: scalar values, source group elements, and target group elements. Structure-preserving cryptography is a characterization of cryptographic schemes over pairing groups with the following properties:

- Input and output consist solely of source group elements
- Correctness of particular functions can be verified solely with group operations and pairing operations

It also represents a design concept in which these cryptographic schemes are seamlessly connected for constructing secure applications. The former property enables direct connection between the cryptographic schemes, and the latter enables to show the validity of input-output relations in an efficient manner. While these provisions in terms of data format and operations guarantee the high level of interconnectivity and convenience inherent to structure-preserving cryptography, they present a technical hurdle when it comes to constructing new structure-preserving schemes in concrete terms. Because the available data format is limited only to source group elements, direct use of standard one-way structures over pairing groups — from a scalar value to a source group element, or from a source group element to a target group element — is no longer possible. Our idea to overcome the difficulty is to use the standard source-to-target group one-way structure only within the functions so that no target group elements are contained in the output data. For example, we propose an SP digital signature scheme whose security is based on the hardness of merging two pairs of random source group elements, (X1, Y1) and (X2, Y2), into one pair, (X3, Y3), whose pairing yields a target group element that equals the product of pairings of the given two pairs. Forging a signature by combining two or more signatures is as hard as finding a solution for the merging problem. The hardness is based on one-wayness from the source group to target group, while the construction evades using target group elements in the output by using pairing operations only in the process of verifying signatures.

4 Framework of structure-preserving cryptography

Because the data format of the input/output interface in structure-preserving cryptography is unified to a source group element of pairing groups, connected use of multiple cryptographic schemes should easily be achieved without converting input/output formats. The specific interface brings huge merit because it eliminates the need to consider format conversions for every application design. As there are numerous possible combinations of dissimilar cryptographic schemes, smooth interconnectivity will be a considerable benefit in terms of reducing design cost and risk of vulnerability inherently associated with the new design.

Let us elaborate the point with an example of connecting two cryptographic tools. Suppose that one of them

outputs a scalar value, and the other proves that the value satisfies a specific relation. Currently available techniques to prove such a statement in a non-interactive manner require the value to be represented by source group elements. Thus, there must be a process for format conversion from each bit of the scalar value to a source group element. It however suffers serious expansion of the input size and results in a proof consisting of a prohibitively large number of source group elements. This sharply contrasts to the case of proving one's knowledge about a value represented by a single source group element where the proof consists of a handful of source group elements.

Cryptography over pairing groups has already been practically implemented in a variety of ways, and its processing requires a relatively small amount of computation even executable on smartphones. It is true also in SP digital signatures and SP commitments, whose specific constructions are shown in this research. In SP digital signature schemes, both signatures and public keys consist of several source group elements, and the process of signature generation and signature verification requires only a small amount of computation — typically several group operations for the former and several pairing computations for the latter. The practical performance and usability of SP digital signatures in realistic applications have been demonstrated. (http://www.atmarkit.co.jp/ait/articles/1312 /05 / news103.html)

5 Comparison to conventional technologies

The security of applications constructed following the concept of structure-preserving cryptography can be guaranteed through some mathematical hardness assumptions on pairing groups. This approach is easily realizable within a reasonable amount of computation, and has little risk of introducing vulnerability associated with connection. In the following, we give a high-level comparison between structure-preserving cryptography and some conventional technologies.

【Classical technology 1: Based on random oracles】

Centered in the years from the 1990s to the early 2000s, many cryptographic technologies were carried out based on the Random Oracle Hypothesis, or idealization of the hash function. Many of the currently used cryptographic technologies are proposed in this model. It can provide relatively easy interconnection between cryptographic tools preserving reasonable efficiency. However, as real-world implementation of an idealized hash function is impossible, it is generally considered that the promised guarantee of security sometimes fails to meet expectations. Structure-preserving cryptography is theoretically based on mathematical hardness assumptions, which, just as with the commonly used elliptic curve discrete logarithm problems, is known to have a high level of plausibility.

【Classical technology 2: Based on general complexity assumptions】

Constructions based on general assumptions, such as the existence of one-way functions, is often plagued by poor performance even though the validity of the assumptions is well expected. They also suffer from the absence of interconnectivity in general. For example, to guarantee correctness about a computation, the computation will be translated into a logical circuit followed by validation of the circuit's input/output relations by means of zero-knowledge proof. This approach requires a complex set of format conversions, often resulting in the emergence of vulnerability risks and significant loss of efficiency. Constructions in this category are mostly considered as feasibility results. Structure-preserving cryptography offers interconnectivity and efficiency in each constituting cryptographic schemes.

【Classical technology 3: Construction using pairing groups】

Classical cryptographic techniques that make use of pairing groups for construction generally offer good performance but pay less attention to interconnectivity. For instance, secret keys are typically represented in scalar values in ordinary digital signature schemes. Showing one's possession of a correct secret key in a non-interactive zero-knowledge manner then suffers from the same inefficiency as described in Section **4**. In the same situation, the use of a fully SP digital signature scheme can reduce the number of source group elements down to the level of dozens, thanks to the fact that the secret key solely consists of source group elements which enables the use, through direct connection, of a highly efficient structure-preserving non-interactive proof system[13] available in the literature.

6 Applications

Structure-preserving cryptography contributes to building secure and efficient information systems by modularly connecting cryptographic tools. We illustrate an anonymous electronic voting system as an example. In an anonymous voting system, it is required that voters are

strictly authenticated to prevent double voting, but at the same time it should be infeasible to identify the voters. Both of these seemingly inconsistent requirements are essential for anonymous voting. A physical solution for the problem would be to use an envelope and stamp: each voter puts a vote in an envelope and gets a stamp on it from an authority who verifies the voter's identity. Then the envelope will be posted to the aggregator who receives the vote, verifies the stamp, opens the envelope, and counts the ballot. With cryptography, the voter encrypts his/her ballot and asks for a digital signature on the ciphertext from the authority, and then sends, from a public terminal, the ballot to the aggregator with proof that the ballot has been once encrypted and signed by the authority without revealing the ciphertext nor the signature from the authority. Such a magical procedure is possible with cryptography in theory but structure-preserving cryptography makes it easy in practice. Since the encryption scheme, the signature scheme and the proof system are all interoperable in structure-preserving cryptography, the high-level idea itself is already a solution in reality.

Besides being a powerful tool for building privacy-protecting information systems in practice (e.g., an anonymous credential system[14]), structure-preserving cryptography contributes to advancing other areas of research that include symbolic security analysis and computer aided system design[15]-[17].

7 Future perspective

Since the first publication of the efficient SP digital signature scheme, many techniques and applications have been developed based on the concept of structure-preserving cryptography. Exemplary applications include: verifiable encryption for establishing fair contracts, oblivious transfer with access control, and group signature that enables anonymous authority delegation.

In computer science, it is often hard to analyze a lower bound and this applies to the performance analysis in cryptography as well. In structure-preserving cryptography, it is sometimes possible to show a concrete lower bound for some particular efficiency measure due to the simplicity of the computation model. So far, the lower bounds for the size of structure-preserving signatures and commitments have been shown. Matching optimal constructions are presented in [2]-[4].

The usefulness of structure-preserving cryptography has penetrated into the community and spread beyond the bounds of its initially envisaged intent. It is causing the emergence of new technologies and functions such as homomorphic signatures and equivalent class signatures that yield higher-level applications. For example, due to the limitation on the available types of computation, it is demonstrated that an exhaustive search for all possible constructions of a specific type of digital signature scheme with security guarantee is possible in realistic time with standard computational resources. The approach has had an impact on the field of automated design and verification.

A variety of applications have been realized by developing basic cryptographic tools — digital signature, commitment, and public-key cryptography — under the concept of structure-preserving cryptography. Further extension of this comes into view by finding still missing SP cryptographic tools such as ID-based encryption and signatures.

As mentioned above, the concept of structure-preserving cryptography has prompted the emergence of outside-the-box cryptography technologies beyond conventional boundaries. In the future, the concept is expected to play the role of a cradle to branch cryptography technology into new areas.

The pairing group, the current basis supporting structure-preserving cryptography, is one of the standard mathematical bases most frequently used in modern cryptography, on which much research is currently underway in view of implementing it on a variety of platforms and speeding up execution. Progress in these technologies will further enhance the practicality of structure-preserving cryptography. Another future prospective includes evolution from pairing to multilinear mapping, which will provide the potential to develop more sophisticated encryption technology under the concept of structure-preserving cryptography.

References

1 Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, "Structure-Preserving Signatures and Commitments to Group Elements," CRYPTO 2010, pp.209–236, LNCS 6223, Springer, 2010.

2 Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, "Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups," CRYPTO 2011, pp.649–666, LNCS 6841, Springer, 2011.

3 Masayuki Abe, Jens Groth, and Miyako Ohkubo, "Separating Short Structure-Preserving Signatures from Non-interactive Assumptions," ASIACRYPT 2011, pp.628–646, LNCS 7073, Springer, 2011.

4 Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo, "Group to Group Commitments Do Not Shrink," EUROCRYPT 2012, pp.301–317, LNCS 7237, Springer, 2012.

5 Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss,

Ryo Nishimaki, and Miyako Ohkubo, "Constant-Size Structure-Preserving Signatures," Generic Constructions and Simple Assumptions. ASIACRYPT 2012, pp.4–24, LNCS 7658, Springer, 2012.

6 Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo: Tagged One-Time Signatures, "Tight Security and Optimal Tag Size," Public Key Cryptography 2013, pp. 312–331, LNCS 7778, Springer, 2013.

7 Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo, "Double-trapdoor anonymous tags for traceable signatures," Int. J. Inf. Sec. 12(1), pp.19–31, 2013

8 Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi, "Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures," TCC 2014, pp.688–712, LNCS 8347, Springer, 2014.

9 Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi, "Structure-Preserving Signatures from Type II Pairings," CRYPTO (1) 2014, pp.390–407, LNCS 8616, Springer, 2014.

10 Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi, "Fully Structure-Preserving Signatures and Shrinking Commitments," EUROCRYPT 2015, pp.35–65, LNCS 9057, Springer, 2015.

11 Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo, "Structure-Preserving Signatures and Commitments to Group Elements," Journal of Cryptology, volume 29, issue 2, pp.363–421, April 2016.

12 Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo, "Constant-Size Structure-Preserving Signatures," Generic Constructions and Simple Assumptions. Journal of Cryptology, volume 29, issue 4, pp.833–878, October 2016.

13 Jens Groth and Amit Sahai, "Efficient Noninteractive Proof Systems for Bilinear Groups. SIAM J. Comput. 41(5), pp.1193–1232, 2012.

14 Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, and Markulf Kohlweiss, "Composable and Modular Anonymous Credentials," Definitions and Practical Constructions. ASIACRYPT (2) 2015, pp.262–288, LNCS 9453, Springer, 2015.

15 Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi, "Strongly-Optimal Structure Preserving Signatures from Type II Pairings," Synthesis and Lower Bounds. Public Key Cryptography 2015, pp.355–376, LNCS 9020, Springer, 2015.

16 Gilles Barthe, Benjamin Grégoire, and Benedikt Schmidt, "Automated Proofs of Pairing-Based Cryptography," ACM Conference on Computer and Communications Security 2015, pp.1156–1168, ACM, 2015.

17 Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt, "Automated Unbounded Analysis of Cryptographic Constructions in the Generic Group Model," EUROCRYPT (2) 2016, pp.822–851, LNCS 9666, Springer, 2016.

Miyako OHKUBO, Ph.D.

Senior Researcher, Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography, Cryptographic Protocol