Structure-Preserving Cryptography

Masayuki Abe

NTT Secure Platform Laboratories, NTT Corporation, Japan
abe.masayuki@lab.ntt.co.jp

Bilinear groups has been a common ground for building cryptographic schemes since its introduction in seminal works [5, 6, 3]. Not just being useful for directly designing schemes for their rich mathematical structure, they aim to modular construction of complex schemes from simpler building blocks that work over the same bilienar groups. Namely, given a description of blinear groups, several building blocks exchange group elements each other, and the security of the resulting scheme is proven based on the security of the underlying building blocks. Unfortunately, things are not that easy in reality. Building blocks often require grues that bridge incompatible interfaces or they have to be modified to work together and the security has to be re-proved.

Structure-preserving cryptography [2] is a paradigm for designing cryptographic schemes over bilinear groups. A cryptographic scheme is called structure preserving if its all public inputs and outputs consist of group elements of bilinear groups and the functional correctness can be verified only by computing group operations, testing group membership and evaluating pairing product equations. Due to the regulated interface, structure-preserving schemes are highly inter-operable as desired in modular constructions. In particular, combination of structure-preserving signatures and non-interactive proof system of [4] yields numerous applications that protect signers' or receivers' privacy. The required properties on the other hand make some important primitives such as pseudo-random functions and collision resistant shrinking commitments unavailable in the world of structure-preserving cryptography. Interestingly, however, the constraints on the verification of correctness aim to argue non-trivial lower bounds in some aspects of efficiency such as signature size in the structure-preserving signature schemes.

Since the first use of the term "structure-preserving" in [1] in 2010, intensive research has been done for the area. In this talk, we overview state of the art on several structure-preserving schemes including commitments and signatures with a careful look about underlying assumptions, known bounds, and impossibility results. We also show open questions and discuss promising directions for further research.

References

1. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, pages 209–236, 2010.
2. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. *Journal of Cryptology*, 2015. DOI: http://dx.doi.org/10.1007/s00145-014-9196-7.

3. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, pages 223–238, 2004.
4. Jens Groth and Amit Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012.
5. Alfred Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.
6. Ryuichi Sakai and Masao Kasahara. ID based cryptosystems with pairing on elliptic curve. *IACR Cryptology ePrint Archive*, 2003:54, 2003.