一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
ISEC2016-73,COMP2016-34(2016-12)

［招待講演］整数計画を用いた高速拡張可能双線型型変換

阿部　正幸†,††　星野　文学†,†††　大久保美也子††††

† NTT セキュアプラットフォーム研究所
†††† NICT サイバーセキュリティ研究所
†† 京都大学 大学院情報学研究科
††† 東京工業大学 情報理工学院
E-mail: †{abe.masayuki, hoshino.fumitaka}@lab.ntt.co.jp, ††††m.ohkubo@nict.go.jp

あらまし　本講演では，2016 年 8 月 14 日から 18 日にカリフォルニア大学サンタバーバラ校 (UCSB) にて開催された第 36 回国際暗号学会議 (CRYPTO 2016) で発表された，双線型型変換に関する最近の結果 [1] を紹介する．

キーワード　変換，双線型群，整数計画，Groth-Sahai 証明，ゼロ知識

[Invited Talk] Fast and Scalable Bilinear-Type Conversion Using Integer Programming

Masayuki ABE†,††, Fumitaka HOSHINO†,†††, and Miyako OHKUBO††††

† Secure Platform Laboratories, NTT
†††† Cybersecurity Research Institute, NICT
†† Graduate School of Informatics, Kyoto University
††† School of Computing, Tokyo Institute of Technology
E-mail: †{abe.masayuki, hoshino.fumitaka}@lab.ntt.co.jp, ††††m.ohkubo@nict.go.jp

Abstract　In this talk, we will present recent results on bilinear-type conversion [1], which appeared in the 36th International Cryptology Conference (CRYPTO 2016) held at the University of California, Santa Barbara (UCSB) from August 14 to 18, 2016.

Key words　Conversion, Bilinear groups, Integer programming, Groth-Sahai proofs, Zero-knowledge

1. Introduction

Bilinear type conversion is to convert cryptographic schemes designed over symmetric groups instantiated with imperilled curves into ones that run over more secure and efficient asymmetric groups [2]. In this talk, we introduce a novel type conversion method called IPConv using 0-1 Integer Programming. Instantiated with a widely available IP solver, it instantly converts existing intricate schemes, and can process largescale schemes that involves more than a thousand variables and hundreds of pairings.

Such a quick and scalable method allows a new approach in designing cryptographic schemes over asymmetric bilinear groups. Namely, designers work without taking much care about asymmetry of computation but the converted scheme runs well in the asymmetric setting. We demonstrate the usefulness of conversion-aided design by presenting somewhat counterintuitive examples where converted DLIN-based Groth-Sahai proofs are more compact than manually built SXDH-based proofs.

References

[1] Masayuki Abe, Fumitaka Hoshino, and Miyako Ohkubo. Design in Type-I, Run in Type-III: Fast and Scalable Bilinear-Type Conversion Using Integer Programming. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 387–415. Springer, 2016.

[2] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Takeya Tango. Converting cryptographic schemes from symmetric to asymmetric bilinear groups. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 241–260. Springer, 2014.