SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

指定された追跡可能性を有するグループ署名の双線形群における例示
An Instantiation of Group Signatures with Designated Traceability in Bilinear Groups

穴田 啓晃 * 福光 正幸 † 長谷川 真吾 ‡
Hiroaki Anada Masayuki Fukumitsu Shingo Hasegawa

キーワード グループ署名，匿名性，追跡可能性，開封者，属性ベース，双線形群

あらまし

暗号要素技術において，匿名性と追跡可能性は両立するのが難しい二性質である．この「匿名性と追跡可能性のフェアネス」の先行研究としては，匿名型ディジタル署名では次のようなものがある．即ち,「メッセージ依存開封」,「説明可能追跡」,「説明可能リング署名」そして「二分岐匿名署名」といった先行研究である (出典は本編参照)．これらに対し，CANDAR2021 で導入された「指定された追跡可能性を有するグループ署名」(group signatures with designated traceability，GSdT) [2] は，署名者が追跡者（開封者）をアクセス構造で指定可能なグループ署名スキームである．すなわち，グループ署名を生成する者が主体的に追跡可能性の一部分を制御出来る点を特徴とする．本稿では，双線形群の構造に基づき [2] の GSdT の例を与える．

GSdT の構成要素は euf-cma secure な署名スキーム（Sig），adaptive IND-CPA secure で payload-hiding な ciphertext-policy 属性ベース暗号スキーム（ABE），そして simulation-sound な非対話型ゼロ知識証明系（NIZK）である．[2] の具体例を構成する際に留意すべき点は，ABE の先行研究はそのほとんどが双線形群のターゲット群において “blinding factor” を乗じることで平文を暗号化する設計であるという制約がある点である．この制約を満たそうとすると，Sig はターゲット群において署名を生成することとなり，このためソース群において署名を生成する “structure-preserving signatures (SPS)” 等とは相容れない．そこで，本稿で与える例では，ABE としてペアリングフリーなもの（Herranz[4]）を用いる設計とする．即ち，Sig として SPS を用いることを優先し，ソース群（という単独の群）において属性ベース暗号化する．ただし，[4] の ABE には，ユーザー数の上限が ABE のセットアップ時に固定されなければならないという別の制約がある．この制約は，開封者の数の上限を GSdT のセットアップ時に固定することに相当する．

結果として，本稿で与える例の構成要素としては次の三つを用いる．Sig は，“compact structure-preserving signatures with almost tight security” [1]，ABE は，“pairing-free CP-ABE with limited number of users” [4]，そして NIZK は，“Groth-Sahai NIZK” [3] である．これらの選択に拠り，GSdT の安全性要件である正当性，匿名性，追跡可能性そして陥罪不可能性は，Type-III の双線形群に対する SXDH 仮定に帰着されることとなる．

* 長崎県立大学情報システム学部情報セキュリティ学科，〒 851-2195 長崎県西彼杵郡長与町まなび野 1-1-1; anada@sun.ac.jp
† 北海道情報大学情報メディア学部情報メディア学科，〒 069-8585 北海道江別市西野幌 59-2; fukumitsu@do-johodai.ac.jp
‡ 東北大学データ駆動科学・AI 教育研究センター，〒 980-8576 仙台市青葉区川内 41 マルチメディア教育研究棟; shingo.hasegawa.b7@tohoku.ac.jp

参考文献

[1] M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo, and J. Pan. Compact structure-preserving signatures with almost tight security. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, pages 548–580, 2017.

[2] H. Anada, M. Fukumitsu, and S. Hasegawa. Group signatures with designated traceability. In *Proc. Ninth International Symposium on Computing and Networking, CANDAR 2021, Matsue, Japan, November 23-26, 2021*, 2021.

[3] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *Proceedings of the Theory and Applications of Cryptographic Techniques 27th Annual International Conference on Advances in Cryptology*, EUROCRYPT'08, pages 415–432, Berlin, Heidelberg, 2008. Springer-Verlag.

[4] J. Herranz. Attribute-based versions of schnorr and elgamal. *Appl. Algebra Eng. Commun. Comput.*, 27(1):17–57, 2016.