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

Fuzzy 鍵を用いたグループ署名技術
Group Signature with Fuzzy Key

川名のん* 長沼健* 中村渉* 本宮志江*
Non Kawana Ken Naganuma Wataru Nakamura Yukie Motomiya

羽渕峻行* 高橋健太*
Takayuki Habuchi Kenta Takahashi

キーワード 生体認証、電子署名

あらまし

グループ署名は、署名生成者が誰であるかを秘匿しつつ、グループのメンバである事を証明する電子署名技術である。本稿では、生体情報などの Fuzzy な秘密鍵情報からグループ署名を生成する Fuzzy グループ署名方式について提案する。

本提案方式の特徴は、Fuzzy な秘密鍵で署名を生成する事に加え、署名生成者と匿名化実行者を分ける事が可能な点である。具体的には、グループに所属する署名者が通常の個人型の Fuzzy 署名方式で電子署名を生成し、グループの代表である匿名化実行者が匿名化処理を行う。この際、匿名化実行者は署名者の秘密鍵などの機密情報を必要とせず、グループの公開鍵のみで匿名化処理を行う。

参考文献

[1] K. Takahashi, T. Matsuda, T. Murakami, G. Hanaoka, M. Nishigaki, “Signature schemes with a fuzzy private key,” International Journal of Informatics Society 2019, 18:581–617.

[2] D. Boneh, X. Boyen, H. Shacham, “Short Group Signatures,” in CRYPTO, 2004, vol. 3152 of Lecture Notes in Computer Science, pp. 41–55, Springer, Berlin, Germany, 2004.

* 株式会社日立製作所 研究開発グループ, 神奈川県横浜市戸塚区吉田町２９２,
Hitachi, Ltd. R&D group, 292, Yoshida-cho, Totsuka-ku