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

Invisible and Unlinkable Policy-Based Sanitizable Signatures

Masahito Ishizaka * Kazuhide Fukushima * Keisuke Tanaka †

Keywords: Policy-Based Sanitizable Signatures, Range-Based Sanitizable Signatures, Policy-Based Sanitizable Signatures for Turing Machines, Invisibility, Unlinkability.

Abstract

In the ordinary digital signatures, if a signed-message is altered, its signature becomes invalid. In sanitizable signatures (SS) [1], an entity (called sanitizer) chosen by the signer can partially modify the message while retaining validity of the signature. Two security notions of SS hard to simultaneously achieve are invisibility (the modifiable blocks are unknown) and unlinkability (no sanitized signature can be linked to its source). Bultel et al. [2] proposed a generic construction of invisible and unlinkable SS based on non-accountable SS (NASS) and verifiable ring signatures. Ishizaka et al. [3] proposed generic NASS constructions based on trapdoor SS and (labeled) public-key encryption. In this work, we propose a new primitive named policy-based SS (PBSS) as a generalization of SS. In PBSS, each signer chooses a general policy representing a condition whom not only the original message but also any modified message must satisfy. We show that the SS by Bultel et al. and the NASS by Ishizaka et al. can be generalized to policy-based ones. By instantiating the PBSS construction from existing schemes, we obtain some concrete advanced SS schemes, such as range-based SS (each modifiable numerical sub-message msg_i can be modified within a range $[L_i, R_i]$) and PBSS for Turing machines (PBSS for a very general policy class, all (deterministic) Turing machines).

References

[1] G. Ateniese, D.H. Chou, B. De Medeiros, and G. Tsudik. Sanitizable signatures. In *ESORICS 2005*, pp. 159–177. Springer, 2005.

[2] X. Bultel, P. Lafourcade, R. Lai, G. Malavolta, D. Schröder, S. Aravinda, and K. Thyagarajan. Efficient invisible and unlinkable sanitizable signatures. In *PKC 2019*, pp. 159–189. Springer, 2019.

[3] M. Ishizaka, Y. Nakano, S. Kiyomoto, and K. Tanaka. Invisible and unlinkable sanitizable signatures from trapdoor sanitizable signatures. In *SCIS 2021*. IEICE ISEC, 2021.

* KDDI Research, Inc. 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan. {ma-ishizaka, ka-fukushima}@kddi-research.jp

† School of Computing, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama Muguro-ku, Tokyo, 152-8552, Japan. keisuke@is.titech.ac.jp