論文 / 著書情報
Article / Book Information

題目(和文)	集約署名の研究
Title(English)	Studies on Aggregate Signature
著者(和文)	手塚真徹
Author(English)	Masayuki Tezuka
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第11711号, 授与年月日:2022年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第11711号, Conferred date:2022/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学 系 数理・計算科学 コース	申請学位（専攻分野）： Academic Degree Requested	博士 （ 理学 ） Doctor of
学生氏名： Student's Name	手塚 真徹	指導教員（主）： Academic Supervisor(main)	田中 圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 800 語程度）
Thesis Summary (approx.800 English Words)

This thesis consists of the following two studies which are related to aggregate signature.
At first, we study for the Camenisch-Lysyanskaya (CL) signature based synchronized aggregate signature scheme. Next, we study an extension of redactable signature scheme.

A Study on the CL Signature Based Synchronized Aggregate Signature:
Digital signature is a fundamental cryptographic primitive which allows us to verify the authenticity of a message. In this scheme, a signer generates a message and computes its signature. Then sender sends the message and its signature to a verifier, The verifier checks the validity of the message by verifying the signature. If the signature is valid, we can guarantee that the message is legitimately generated by the signer and is not changed.
In the Internet of Things (IoT) era, a huge number of devices are connected to the Internet, and it is necessary to guarantee authenticity for a large amount of data output by these devices. If we use digital signature for an IoT system, this will yield a significant number of signatures and consumes the signature storage for a database.
Aggregate signature proposed by Boneh, Gentry, Lynn, and Shacham allows anyone us to convert many different signatures into an aggregate signature whose size is much smaller than a concatenation of the individual signatures. Thanks to this feature, we can reduce the leads storage space. However, the aggregate signature schemes proposed so far have two drawbacks. The first is the difficulty of constructing a provable secure aggregate signature scheme without the random oracle model (ROM). Currently, only two constructions (an indistinguishability obfuscation (iO) based scheme and a multilinear map based scheme) are known.
The second is inefficient verification. In the pairing based aggregate signature scheme by Boneh, Gentry, Lynn, and Shacham, the number of pairing evaluations for an aggregate signature is linear in the number of signatures that are aggregated.
To circumvent these problems, various restricted aggregate signatures have been proposed. Synchronized aggregate signature is one of them. In this scheme, all of the signers have a synchronized time period and each signer can sign a message. A set of signatures that are all generated for the same period can be aggregated into a short signature.
The efficient synchronized aggregate signature scheme was proposed by Lee, Lee, and Yung. This scheme is based on the CL signature scheme and the security of this scheme is proven under the Lysyanskaya-Rivest-Sahai-Wolf (LRSW) assumption in the ROM. The LRSW assumption is an interactive assumption. However, security analysis for interactive assumptions is questionable. It is desirable to avoid using interactive assumptions.
In this thesis, we revisit the synchronized aggregate signature scheme by Lee et al. We give a new security proof for this synchronized aggregate scheme under the modified 1-strong Diffie-Hellman-2 (1-MSDH-2) assumption which is a non-interactive assumption and the ROM.

A Study on the Extension of Redactable Signature Scheme:
Currently, the need to prove the validity of digital documents issued by governments and enterprises is increasing. When disclosing documents, governments or enterprises must remove private information concerning individuals. However, in the use of digital signature, if we removed a part of a signed document, a signature will be invalid. A trivial solution for this problem is to resign a modified document. However, if the original signer is not reachable anymore or refuses to resign, it is not convenient.
Redactable signature allows anyone to remove parts of a signed message without invalidating the signature. A verifier still verifies the validity of the signature on a message some part is removed. However, current redactable signature schemes have a drawback for the signature size and redaction rights.

The feature of redactable signature that anyone can remove parts of a signed message may seem useful at first glance, but the ability for anyone to remove part of a message has a drawback. If governments or enterprises use a redactable signature scheme, anyone can remove the necessary information which should be disclosed. That is, an officer in governments or enterprises can intentionally hide a fact that is an inconvenient truth.

To make up for this weakness, we introduce a notion of t-out-of-n redactable signature. This scheme has a signer, n redactors, a combiner, and a verifier. The signer designates n redactors and a combiner in advance and generates a signature of a message. Each redactor decides parts that he or she wants to remove from the message and generates a piece of redaction information. The combiner collects pieces of redaction information from all redactors, extracts parts of the message that more than t redactors want to remove, and generates a redacted message. By using a t-out-of-n redactable signature scheme, we can decentralize redaction rights.

Then, we give a provable secure t-out-of-n redactable signature scheme. Our scheme is constructed by using the idea of the redactable signature scheme by Miyazaki, Hanaoka, and Imai which is based on the aggregate signature by Boneh, Gentry, Lynn, and Shacham. Our scheme can be proven under the co-computational Diffie-Hellman (co-CDH) assumption in the ROM.