論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Construction and Analysis of Post-Quantum Key Exchange Protocols for Secure Messaging
著者(和文)	橋本啓太郎
Author(English)	Keitarou Hashimoto
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第12390号, 授与年月日:2023年3月26日, 学位の種別:課程博士, 審査員:尾形 わかは,植松 友彦,山田 功,松本 隆太郎,田中 圭介,安永 憲司
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第12390号, Conferred date:2023/3/26, 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	情報通信 系 情報通信 コース	申請学位（専攻分野）： Academic Degree Requested	博士 （ 工学 ） Doctor of
学生氏名： Student's Name	楾本啓太郎	指導教員（主）： Academic Supervisor(main)	尾形わかは
		指導教員（副）： Academic Supervisor(sub)	

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

Messaging applications such as WhatsApp, LINE, Slack, are widely used for both private and business communications. On the other hand, some service providers of such applications and governments are trying to collect information about application users (e.g., messages and social graphs). Such activities threaten users' privacy; thus people have become hesitant to use such messaging applications that do not protect their privacy. To ensure the privacy of users, some messaging apps implement secure group messaging (SGM) and SGM becomes popular around the world. SGM ensures the confidentiality of messages by encrypting messages with the shared secret key among conversation partners. That is, third parties other than conversation partners cannot access messages. In addition, SGM has strong post-compromise and forward secrecy (PCFS) security, which guarantees the confidentiality of past and future messages even if the key at a certain period is compromised. The most famous SGM protocol is Signal, which has been implemented in other SGM apps such as WhatsApp and Facebook Messenger and is currently used by over 2 billion people. However, since its efficiency deteriorates as the number of group members increases, it limits the number of group members to 1,000. To solve this problem, industries such as Google and Meta and academia such as universities and research institutes are collaborating to develop and standardize Message Layer Security (MLS) protocol. It can operate efficiently even in large groups of 50,000 members. In addition, from the other perspective, it is necessary to develop a new SGM secure against quantum computers since currently used cryptographic protocols are known to be broken by large-scale quantum computers. Thus, the National Institute of Standards and Technology (NIST) is working on the standardization of post-quantum cryptography. To ensure the privacy of conversations in the future, we need to start developing post-quantum secure group messaging protocols.

The objective of this work is to realize post-quantum secure group messaging. The contributions of this work are the following.

The first contribution of this work is developing a post-quantum authenticated key exchange protocol for Signal's initial key agreement. We formalize the security model for Signal's initial key agreement and propose a new generic construction based on key encapsulation mechanisms and signature schemes. That is, the proposed protocol can be instantiated from various well-studied post-quantum assumptions. Also, we implement the proposed protocol with the NIST PQC candidates and evaluate the communication and computation costs of each instantiation. This experimental result confirms that the proposed protocol works efficiently in a real-world environment. Moreover, we construct a deniable authenticated key exchange protocol from ring signatures and non-interactive zero-knowledge arguments. This allows users to deny the fact that they have exchanged session keys with another user.

The second contribution of this work is designing a new post-quantum continuous group key agreement protocol from multi-recipient public key encryptions. The proposed protocol achieves the most efficient total communication costs for each user when all group members update their key materials. We also formulate a new Universal Composability (UC) security model suitable for the proposed protocol and prove the security of the proposed protocol. In addition, we propose a new lattice-based multi-recipient public key encryption that contributes to reducing the uploading costs of the proposed protocol. Moreover, the

experimental result confirms that the proposed protocol works efficiently even for a group of 1000 members.

The third contribution of this work is proposing a metadata-hiding continuous group key agreement protocol. To do so, we formulate a UC security model for metadata-hiding secure group messaging, and a simple and generic wrapper protocol that converts any non-metadata-hiding continuous group key agreement into metadata-hiding one with minimum overhead. Then, we rigorously prove that the modified version of the protocol proposed in the second contribution plus our new wrapper protocol satisfies the desired metadata-hiding properties. This is the first provably-secure metadata-hiding SGM protocol. In contrast to existing secure group messaging that only ensures the confidentiality of messages, our protocol additionally hides the relationship between users. Thus, our protocol enhances users' privacy.