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)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		楠本啓太郎	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	尾形わかは	教授	審査員	田中圭介	教授
	審査員	植松友彦	教授		安永憲司	准教授
		山田功	教授			
		松本隆太郎	教授			

論文審査の要旨（2000 字程度）

本論文は、“Construction and Analysis of Post-Quantum Key Exchange Protocols for Secure Messaging (セキュアメッセージングに向けた耐量子計算機安全な鍵交換プロトコルの研究)”と題し、英文６章より構成されている。

第１章“Introduction (はじめに)”では、まず、利用者が増加しているメッセージングアプリケーションにおいて、やり取りされるコンテンツや利用者間の関係性といったプライバシー情報を保護することの要求が高まっていることを述べた上で、プライベートなメッセージングを実現する上で重要なセキュアメッセージングと、その核となる暗号技術である鍵交換の説明をしている。次に、２者間向けセキュアメッセージングとグループ向けセキュアメッセージングについて、既存の方式を概説し、大規模な量子計算機の実用化によりこれらの既存のセキュアメッセージングが危殆化することを述べている。そのような背景から、量子計算機に対しても安全な鍵交換プロトコルの実現を本研究の課題として設定し、耐量子計算機安全な２者間およびグループ内の鍵交換プロトコル、耐量子計算機安全かつメタデータの秘匿性も保証するグループ内鍵交換プロトコルを新たに構築していることを述べている。

第２章“Preliminaries (準備)”では、本論文を通じて参照される記法及び、鍵カプセル化メカニズムや電子署名方式などの暗号プリミティブの定義を概説している。

第３章“Post-Quantum Authenticated Key Exchange for Signal Protocol (Signalプロトコルでの利用に適した耐量子計算機安全な認証鍵交換)”では、現在世界で最も利用されているセキュアメッセージングプロトコルであるSignalプロトコルに組み込むことのできる、耐量子計算機安全な２者間鍵交換プロトコルを提案している。提案方式は、標準的な安全性を満たす任意の鍵カプセル化メカニズム、署名方式、及び共通鍵暗号技術から構成され、Signalプロトコルで用いられているX3DH方式より高い安全性を持つ。また、提案方式をNIST耐量子計算機暗号標準化候補の暗号方式で実装して通信コストと計算コストを測ることにより、提案方式が実環境で動作可能であることを確認している。

第４章“Continuous Group Key Agreement via Post-Quantum Multi-Recipient PKEs (耐量子計算機安全な複数受信者公開鍵暗号に基づく継続的グループ鍵交換)”では、まず、グループ内セキュアメッセージングを実現するための要素技術である継続的グループ鍵交換を、複数の受信者に同一のメッセージを効率的に送信できるmulti-recipient PKEとよばれる公開鍵暗号技術を用いて構成している。特に、committing multi-recipient PKEと呼ばれる新しい暗号技

術を導入することで、鍵更新時にグループの各メンバーが受信するデータサイズをグループメンバー数に依存しない定数とすることに成功している。加えて、格子問題に基づく新しいmulti-recipient PKEを開発することで、既存の継続的グループ鍵交換方式であるTreeKEMよりも小さな鍵更新コストを達成している。

第5章“MetaData-Hiding Continuous Group Key Agreement（メタデータを秘匿する継続的グループ鍵交換)”では、まず、4章で用いた継続的グループ鍵交換の安全性定義を、メタデータの秘匿性を包含するように拡張している。拡張された安全性モデルは、利用者とサーバ間でやり取りされるデータから漏洩するメタデータに加えて、各ユーザがサーバへアクセスする際のアクセスパターンから漏洩するメタデータも考慮している初めての安全性定義である。次に、既存の継続的グループ鍵交換方式を、電子署名方式のみを用いて、メタデータを秘匿する方式に変換する手法を与えている。具体的な実現例として、4章で提案したmulti-recipient PKEに基づく継続的グループ鍵交換方式に変更を加えたうえで、この変換手法を適用することにより、メタデータを秘匿する耐量子計算機安全な継続的グループ鍵交換方式が得られることを示している。

第6章“Conclusion（まとめ)”では、本論文の成果を要約するとともに、今後の課題について言及している。

以上を要約すると、本論文は、量子計算機に対して安全なセキュアメッセージングを実現するために有用な耐量子計算機安全な鍵交換プロトコルを提案するものである。本論文で提案された方式はインターネット上での安全なコミュニケーションを実現するために極めて重要であり、工学上貢献するところが大きい。よって我々は、本論文が博士(工学)の学位論文として十分価値があるものと認める。