Form 3

Abstract of Thesis

Name (HOUGAARD HECTOR BJOLJAHN)	
Title	Study on Post-Quantum Group Key Exchanges and Generalization (耐量子グループ鍵共有法と一般化に関する研究)

Abstract of Thesis

The advent of quantum computing has seen many classically secure cryptographic constructions become potentially insecure in the near future. Quantum computers can easily solve problems that most current cryptographic constructions use as building blocks, namely the integer factorization problem, the discrete logarithm problem, and the elliptic curve discrete logarithm problem. This means that we will need to discard those cryptographic constructions or risk having information fall into malicious hands. The nature of cryptographic proofs offers us an alternative: Fix them. By generalizing the constructions and updating the basis for their security, we can preserve these constructions while guarding against any future adversaries, quantum included. So far, quantum-secure, or post-quantum cryptography (PQC) secure, key exchanges, signature schemes, encryption schemes, and more have been proposed but there are still classical constructions that have no PQC alternative and there are many improvements that can be made in security, key size, and speed (complexity).

In this dissertation, we consider the generalization of classical constructions to PQC secure versions and beyond. In particular, we consider group key exchanges (GKEs) and pseudorandom permutations. PQC secure GKEs do exist but they all have linear order complexity so an improvement would be welcome. PQC secure pseudorandom permutations have yet to be constructed but recent PQC secure pseudorandom functions point towards their inevitability.

In Chp. 3, we show that it is possible to define a GKE using the isogeny based PQC primitive, supersingular isogeny Diffie-Hellman (SIDH), to create a logarithmic order complexity GKE. We further give a peer-to-peer/sequential version with similar complexity. We also show that there is a compiler that turns both GKEs into authenticated GKEs, also with logarithmic order complexity.

In Chp. 4, we show that it is also possible to define a GKE using the lattice based PQC primitive, ring-learning-with-errors (R-LWE) to create a logarithmic order complexity GKE. We also give a peer-to-peer/sequential version and show that both can be compiled into logarithmic order complexity authenticated GKEs.

In Chp. 5, we take advantage of the structure of cryptography together with the previous GKEs to generalize the definitions of key exchange (KE) and hard problems and then give generic compilers for GKEs, both a concurrent and sequential version.

In Chp. 6, we generalize the Even and Mansour block cipher construction to using group actions as their underlying operations, giving us a pseudorandom permutation that is secure against an unbounded adversary having polynomially-many classical oracle queries.

Finally, we conclude by summarizing our results, discussing their relation to the wider field of cryptography, and considering future work based on them.

様式 7

論文審査の結果の要旨及び担当者

氏　名	（ HOUGAARD HECTOR BJOLJAHN ）		
	（職）		氏　名
論文審査担当者	主 査	教授	宮地　充子
	副 査	教授	滝根　哲哉
	副 査	教授	丸田　章博
	副 査	教授	馬場口　登
	副 査	教授	三瓶　政一
	副 査	教授	井上　恭
	副 査	教授	鷲尾　隆
	副 査	教授	駒谷　和範
	副 査	Distinguished Researcher	Mehdi　Tibouchi（日本電信電話株式会社）

論文審査の結果の要旨

The advent of quantum computing has seen many classically secure cryptographic constructions become potentially insecure in the near future. Quantum computers can easily solve problems that most current cryptographic constructions use as building blocks, namely the integer factorization problem, the discrete logarithm problem, and the elliptic curve discrete logarithm problem. This means that it is necessary to discard those cryptographic constructions or risk having information fall into malicious hands. The nature of cryptographic proofs offers an alternative: Fix them. By generalizing the constructions and updating the basis for their security, these constructions can be preserved while guarding against any future adversaries, quantum included. So far, quantum-secure, or post-quantum cryptography (PQC) secure, key exchanges, signature schemes, encryption schemes, and more have been proposed but there are still classical constructions that have no PQC alternative and there are many improvements that can be made in security, key size, and speed (complexity).

As consumer-level computational power can be severely limited, efficiency has become a major factor. The uses for cryptography have also changed and the number of parties involved in a single cryptographic protocol too. For example, IoT devices in a home accessed by a family or a group chat in the LINE or WhatsApp communication applications. For a group of parties wishing to communicate securely, a secure two-party key exchange can be repeated for each pair of parties, but this quickly leads to very large numbers of keys being stored and many rounds of exchanges, both of which could be severely reduced. This is the reason for group key exchanges (GKEs) where each party ends up with a single session key shared by all the involved parties. Most cryptographic applications also require a large amount of randomness when altering information best kept secret, however this is often difficult and expensive to acquire. A solution is to instead shuffle the information using a permutation in a way that “looks” random, a so-called pseudorandom permutation (PRP).

In this dissertation, the generalization of classical constructions to PQC secure versions and beyond is considered. In particular, this dissertation considers GKEs and PRPs.

GKEs may be compared using round complexity (the maximum number of times any party must wait for information from other parties in order to proceed), communication complexity (the maximum number of

messages received by any party), and memory complexity (the maximum number of values stored until the session key computation). These complexities are dependent on the number of parties and can be expressed as functions thereof. Intuitively and factually, the slower this function grows, the better the complexity. Although PQC secure GKEs do exist, they all have linear order communication and memory complexity so an improvement to either constant or logarithmic order would be welcome. Furthermore, PQC secure PRPs have yet to be constructed but recent PQC secure pseudorandom functions (PRFs) point towards their inevitability.

In Chp. 3, it is shown that it is possible to define a GKE using the isogeny based PQC primitive, supersingular isogeny Diffie-Hellman (SIDH), to create a logarithmic order communication and memory complexity GKE. Furthermore, a peer-to-peer/sequential version with similar complexity is given. It is also shown that there is a compiler that turns both GKEs into authenticated group key exchanges (AGKEs), also with logarithmic order complexity. These (A)GKEs manage to reduce the communication and memory complexities by an entire order of magnitude (linear to logarithmic) compared to other PQC (A)GKEs based on the same primitive. The structure of these (A)GKE constructions also gives highly flexible (A)GKEs that can be changed according to the needs of the network and individual users.

In Chp. 4, it is shown that it is also possible to define a GKE using the lattice based PQC primitive, ring-learning-with-errors (R-LWE), to create a logarithmic order complexity GKE. A peer-to-peer/ sequential version is also given and it is shown that both can be compiled into logarithmic order complexity AGKEs. On top of having the complexity improvements over other R-LWE based (A)GKEs, these constructions serve as PQC alternatives, each PQC primitive having its own pros and cons.

In Chp. 5, the structure of cryptography is taken advantage of together with the GKEs in Chp. 3 and Chp. 4, and a generalization of the definitions of key exchanges and hard problems, in order to give generic compilers for group key exchange, both a concurrent and sequential version. These constructions allow for new primitives to be turned into GKEs, securing cryptography regardless of what adversaries the future holds.

In Chp. 6, the Even and Mansour block cipher construction is generalized to using group actions as their underlying operations, giving a PRP that is secure against an unbounded adversary having polynomially-many classical oracle queries. Although this does not show quantum security directly, it does show that PQC primitives can potentially be used in classical constructions without a loss in security.

The dissertation is concluded by summarizing the dissertation results, discussing their relation to the wider field of cryptography, and considering future work based on them.

As described above, this dissertation achieves constructions of group key exchange protocols secure against quantum computers. In particular, for the first time, this dissertation proposed group key exchange protocols that achieve logarithmic communication and memory complexity, i.e. computational complexity, with respect to the number of users. The group key exchange protocol is an essential technology to realize secure communication among a large number of devices with the spread of IoT devices. Therefore, the proposed quantum-safe group key exchange protocols with logarithmic efficiency will be especially effective in realizing quantum-safe communication among IoT devices, which are exploding in number.

Therefore, this dissertation is considered to be valuable as a doctoral thesis.