Form 3

Abstract of Thesis

Name (ALHUSSEIN MUATAZ MEZAAL HUSSEIN)	
Title	Practical quantum key distribution system robust against side-channel attacks (サイドチャネル攻撃耐性のある実用的量子鍵配送システム)

Abstract of Thesis

Quantum mechanics is a theory that brings a new understanding of the world especially around a microscopic scale, in which some phenomena look fundamentally different from our intuitive sense. Applications of this theory have revolutionized technologies that we use in our daily life. These days, one particular field known as quantum information processing is being investigated for its potential to bring tools that can solve some of key questions in science. For example, a quantum system enables distant two parties to generate an identical secret key for a cryptosystem, which is secure against any eavesdropping permitted by physical law. It relied on the fact that measuring any quantum system would change its state, from which eavesdropping is revealed. The scheme to create a secret key as above is called “Quantum Key Distribution” or “QKD” for short.

The security of QKD is mathematically provable, and a system assuming ideal devices has been proved to be unconditionally secured. However, any implementation would have to use some currently available technologies, which have some gaps from the original theoretical model. Then, there is a question if the theoretical security is still hold with such gaps. In other words, can quantum mechanics still provide provable security to actually implemented systems?

The above question opens a new kind of research, where eavesdropping taking advantage of actual devices’ gap from the theoretical model, called side-channel attacks, is searched, and a countermeasure against it is devised, in order to make practically implemented systems secure. This thesis was involved in this kind of study, and proposed some countermeasures against the most powerful side-channel attack, i.e., detector blinding and control attack.

This thesis consists of seven chapters, which is organized as follows:

Chapter 1 is the introduction of the thesis. The history of quantum cryptography was briefly introduced. Then, the purpose of this thesis was described.

Chapter 2 describes the quantum key distribution algorithm in general. We explained in brief the theoretical security of quantum key distribution. Some examples of quantum key distribution systems were also presented.

Chapter 3 introduces side-channel attacks, including operating properties of a single-photon detector. We described loopholes in a single-photon detector and attacks taking advantage of the loopholes. Some previously proposed countermeasures were also introduced with some discussion.

In **Chapter 4**, we proposed a countermeasure using post processing in four-states QKD protocols, which utilizes photon statistics of weak coherent light, monitoring coincident clicks at a measurement system, to detect eavesdropping. We also provided an analysis estimating the number of coincident clicks, and conducted an experiment to confirm the feasibility of this scheme.

In **Chapter 5**, we conducted experiments of four-state QKD systems with the countermeasure proposed in Chapter 4. A novel receiver configuration was also proposed and demonstrated, which enables a simpler setup than conventional QKD receivers.

In **Chapter 6**, we proposed a countermeasure against side-channel attack in differential phase shift QKD. We performed theoretical estimation and simulations to evaluate the system performance of the proposed scheme.

Finally, we concluded the thesis in **Chapter 7**.

様式 7

論文審査の結果の要旨及び担当者

氏　名	（ALHUSSEIN MUATAZ MEZAAL ALHUSSEIN）		
論文審査担当者		(職)	氏　名
	主査	教授	井上 恭
	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	宮地 充子
	副査	教授	鷲尾 隆　(産業科学研究所)
	副査	教授	駒谷 和範　(産業科学研究所)
	副査	准教授	五十嵐 浩司

論文審査の結果の要旨

情報化社会の進展に伴い、暗号通信技術の重要性が増している。現在の暗号システムは解読に要する計算量の膨大さを安全性の根拠としているが、その一方で、量子力学の原理に基づいて究極的に安全な暗号通信を提供する量子暗号（または量子鍵配送 Quantum Key Distribution）の研究が進められている。QKD 研究は、量子計算機により現在の暗号システムが破られる事が示された 1990 年代から活発化し、量子論に基づく安全性の理論研究及び実験的研究が進められ、2010 年前後には大規模な現場実験が行われるに至っている。しかしながら 2010 年代になって、それまでの安全性理論では考慮されていなかった、実際のデバイスの動作特性を利用する盗聴法（サイドチャネル攻撃）が提案・実証され、QKD 研究における大きな課題のひとつとなった。

本論文は QKD システムに対するサイドチャネル攻撃（SCA）対策に関する研究をまとめたものである。これまで SCA 対策がいくつか提案されているが、それらには、システム実装が困難あるいは用いるデバイスの特性に依存、といった課題があった。そこで本論文では、標準的な QKD 方式である BB84 プロトコル及びシステムの簡便さを特長とする DPS-QKD プロトコルについて、実装が容易かつデバイス無依存である SCA 対策を提案し、システムパラメータの最適化、性能評価、さらには実証実験を行っている。具体的な内容は以下の通りである。

(1) BB84 方式において、従来は秘密鍵生成には不要として廃棄していた光子検出事象（基底不一致検出）が、SCA 時には正常時と異なる挙動を示すことに着目し、この検出事象をモニターする SCA 対策を提案し、その実現性を示している。装置構成を変更することなくデータ処理のみで SCA を防ぐことができ、実用性の高い手法である。

(2) 上記提案対策を備えた QKD システム実証実験を行っている。さらにここでは、受信装置において従来は安定動作のためには光子検出器が 4 台必要であったところを 2 台で賄う新規アイデアを導入し、より簡易な構成で SCA 耐性のある BB84 プロトコルが実装できることを示している。

(3) DPS-QKD 方式では、基底不一致という事象は起きないため上記対策を適用することができない。そこでそれに代わる SCA 対策として、受信系の前段に可変減衰器を配置し、無作為に 6dB の減衰を付加することを提案している。減衰時に SCA が実行されると、光子検出が起こらなくなり、このことより SCA が検知される。ただし減衰分だけ QKD 性能が低下する。システムパラメータを最適化し、10%程度の伝送距離性能の低下で SCA を防げることを示している。

以上のように本論文は、量子鍵配送システムへのサイドチャネル攻撃に関し、実装が容易かつデバイス無依存な防御策を提案し、その有効性を検証・実証している。これらの成果は、サイドチャネル攻撃耐性がありかつ実用性の高い量子鍵配送システム構築への道を開くものであり、工学的・学問的な見地から意義深い。よって本論文は博士論文として価値あるものと認める。