Form 3

# Abstract of Thesis

| Name ( JIN YAOAN ) | |
|---|---|
| Title | A study on Compact Elliptic Curve Cryptosystems Resisting Side Channel Attacks<br>（サイドチャネル攻撃に安全な軽量な楕円曲線暗号の研究） |


Today, internet of things (IoT) devices have penetrated into every household. While enjoying the convenience of IoT devices, our interests are also compromised by the security vulnerabilities of IoT devices. The security of IoT devices should be taken seriously. In particular, the development of side channel attacks (SCAs) targeting IoT devices in recent years makes the security of IoT devices more and more important. Therefore, IoT devices with limited computational resources require compact cryptosystems resisting SCAs.

Elliptic curve cryptosystems (ECCs) are typical public key cryptosystems (PKCs) that can ensure equivalent security with considerably shorter keys than Rivest-Shamir-Adleman (RSA). Therefore, compact ECCs are recommended for IoT devices. In ECCs, elliptic curve scalar multiplications (ECSMs) are dominant computations. Therefore, enhancing the security and efficiency of ECSMs is important. In ECSMs, modular inversions are required when affine addition formulae are used. Modular inversions are also critical computations in elliptic curve digital signature algorithms (ECDSAs). Therefore, we also focus on secure and compact modular inversions.

An ECSM consists of a scalar multiplication algorithm and elliptic curve addition formulae. Elliptic curve addition formulae based on affine coordinates are memory-saving and can be efficient according to the ratio of modular inversion cost to modular multiplication cost but weak against SCAs. Elliptic curve complete addition (CA) formulae based on Projective coordinates can achieve secure ECSMs resisting SCAs but are not compact. We focus on secure and efficient ECSMs taking advantages of the compact of affine elliptic curve addition formulae.

Greatest common divisor (GCD) computations or modular inversions are used in RSA key generation, affine elliptic curve addition formulae, and ECDSAs. Therefore, we need focus on them for secure and efficient ECCs. GCD computations and modular inversions are often computed using the binary Euclidean algorithm (BEA) and binary extended Euclidean algorithm (BEEA), respectively. Therefore, the SCA weaknesses of BEA and BEEA become a serious concern. Constant-time GCD (CT-GCD) and constant-time modular inversion (CTMI) algorithms are effective countermeasures in such situations. A modular inversion by Fermat's little theorem (FLT) can work in constant time, but it is not efficient for general inputs. Two CTMI algorithms, named BOS and BY, were proposed by Bos, Bernstein and Yang, respectively. Their algorithms are all based on the concept of BEA. However, one iteration of BOS has complicated computations, and BY requires many iterations. A small number of iterations and simple computations during one iteration are good characteristics of a constant-time algorithm.

In the first part of this thesis, three notions of a secure ECSM, named *generality of k*, *secure generality*, and *executable coordinates*, are proposed. Then, the original affine elliptic curve addition formulae are extended to eliminate some exceptional points. We improve Joye's regular 2-ary RL algorithm and propose new RL ECSMs, which can scan the input scalars from right to left (RL) using (extended) affine coordinates. For the security, we prove that our RL ECSMs satisfy secure generality and (extended) affine coordinates are executable coordinates for them. In the second part of this thesis, new LR ECSMs scanning the input scalars from left to right (LR) are proposed, which are more memory-saving. Our LR ECSM with a memory of 12 field elements uses the least amount of memory. The secure generality of our LR ECSMs and that (extended) affine coordinates are executable coordinates for them are also proved. The efficiency of both LR and RL ECSMs is enhanced by optimizing the number of inversions. Compared with prior works, the efficiency of our ECSMs is analyzed from theoretical and experimental perspectives. In the third part of this thesis, new short-iteration CT-GCD and CTMI algorithms over $F_p$, named SICT-GCD and SICT-MI, respectively, are proposed borrowing a concept from BEA. SICT-GCD and SICT-MI are evaluated from a theoretical perspective. Compared with modular inversions by FLT, BOS, BY, and the improved version of BY, SICT-GCD and SICT-MI are experimentally demonstrated to be faster.

様式 7

# 論文審査の結果の要旨及び担当者

| 氏　名 | （ ＪＩＮ ＹＡＯＡＮ ） | | |
|---|---|---|---|
| | （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 | 三瓶　政一 |
| | 副 査 | 教授 | 井上　恭 |
| | 副 査 | 教授 | 田中　雄一 |
| | 副 査 | 教授 | 鷲尾　隆 |
| | 副 査 | 教授 | 駒谷　和範 |
| | 副 査 | 講師 | 王 イントウ |
| | 副 査 | 教授 | 高島　克幸（早稲田大学教育・総合科学学術院 教育学研究科） |

## 論文審査の結果の要旨

As Internet of things (IoT) devices have become pervasive in every household, we can now enjoy the conveniences of IoT devices. On the other hand, however, our benefits are being undermined by the security vulnerabilities of IoT devices. Therefore, the security of IoT devices needs to be taken seriously. In particular, side-channel attacks (SCAs) targeting IoT devices have become a major threat in recent years. Side-channel attacks are those that use side information such as power consumption, timing, and memory access during data processing. In general, a cryptosystem is built in such a way that it is theoretically impossible to attack in a realistic amount of time, but side-channel attacks use side information instead of theoretical analysis, making it easy to attack cryptosystem that was originally built to be secure. In particular, IoT devices are often used out of sight and out of person, making them vulnerable to various side-channel attacks. Therefore, it is inevitable to realize IoT devices that are secure against side-channel attacks. However, IoT devices have limited computational resources, and compact cryptographic schemes that can withstand SCA are required.

Elliptic curve cryptography (ECC) is a public key cryptography (PKC) that can provide equivalent security with considerably shorter keys than other public key cryptography. Elliptic curve scalar multiplication (ECSM) is the primary calculation in ECC. Therefore, it is important to improve the security and efficiency of ECSM. In this dissertation, compact ECSM with improved security is studied, which consists the following five contributions.

1. Redefining notions of secure scalar multiplication. By defining the relation between coordinate systems and scalar multiplication strictly, the new notion of secure scalar multiplication that works without exception is introduced. This definition allows existing schemes to be evaluated in detail.
2. Extending the affine coordinate that works without exceptional point. The known coordinate system without exceptional points had a large amount of memory and was slow, whereas the coordinate system with exceptional points is newly improved and the zero point of the coordinate system is extended to eliminate the existing exceptional points. This extended secure coordinate allows us to achieve a secure and compact addition formulae.
3. Constructing various lightweight combinations of addition and doubling formulae. By constructing directly computable formulae for which no single formula has existed so far, such as a set of

quadruplication, addition, and doubling, or a set of doublings and additions, etc, a compact direct addition formula can be achieved with the deletion of the inversion. This additive formula is applicable not only to the proposed additive chain but also to various other additive chains, and its effectiveness.

4. Proposing secure and compact left-to-right and right-to-left ECSMs. Using the second through third studies, a secure and compact left-to-right and right-to-left ECSMS are proposed and theoretically proven to satisfy the concepts of the first study.
5. Constructing the new inversion algorithm on which the minimum number of loops that can be proved. An algorithm that computes the inverse with the same number of iterations for any finite field element, and is theoretically proved that the number of iterations is constant. The effectiveness of the proposed algorithm is significant because the inverse algorithm is not only used in the second through fourth studies, but is also used as a basic operation in cryptography.

As described above, in this dissertation, secure and compact elliptic curve cryptosystems are realized by proposing a coordinate system without exception points, direct coordinate formulae, ECSMs without exception points, and the inversion algorithm guaranteed to execute at constant times. The applications of the proposed coordinate system without exception points, direct coordinate formulas, addition chain without exception points, and inverse algorithm guaranteed to work at constant times are not limited to elliptic curve cryptography. These algorithms are fundamental to various cryptographic schemes, such as quantum cryptography, and their effectiveness is very high.

Therefore, this thesis contributes significantly to the development of the field of information security and engineering, and is recognized as a valuable doctoral dissertation.