氏名	阪本光星
学位の種類	博士（応用情報科学）
学位記番号	博情第７１号
学位授与年月日	令和５年　３月２４日
学位授与の要件	学位規則第４条第１項該当（課程博士）
論文題目	Design of Efficient Symmetric-Key Cryptographic Algorithms

論文審査委員　（主査）准教授　五十部孝典
（副査）教授　中本幸一
（副査）准教授　栗原淳

学位論文の要旨

Cryptography plays a crucial role in the modern internet communication system. Especially, thanks to the development of communication technology, we can see variety of its applications everywhere, and the importance of cryptography is getting more and more enhanced. The main role of cryptography, especially symmetric-key cryptography which is treated in this thesis, is to provide data confidentiality and integrity by a block cipher, stream cipher, hash function, message authenticated codes and authenticated encryption scheme. With the rapid development of communication technology for a latest few decades, such symmetric-key cryptographic algorithms need to meet not only the security requirement but also implementation requirement on resource-constrained devices such as RFIDs and medical devices. Studying on such resource-constrained algorithms is called lightweight cryptography, and have get the most attention in the field of symmetric-key cryptography for the latest decade. Another area of interest is designing ultra-high throughput cryptographic algorithms for the rapid advancement of mobile communication systems like 5G and beyond 5G. In these systems, it is necessary to design ultra-high throughput and high-security cryptographic algorithms due to the increasing of the data transmission speed.

This thesis is dedicated to the design of symmetric-key cryptographic algorithms, including a lightweight block cipher, lightweight tweakable block cipher, block cipher-based low-latency pseudo-random function, and ultra-high throughput authenticated encryption with associated data scheme. Specifically, we introduce

four algorithms: a tweakable blockcipher Tweakable TWINE, lightweight block cipher WARP, lightweight PRP Orthros, and an ultra-high throughput AEAD Rocca and investigate how to design them along with the background of why these new algorithms is necessary.

論文審査の結果の要旨

暗号技術は現代のインターネット通信システムにおいて極めて重要な役割を果たしている。特に通信技術の発展により、情報セキュリティの基盤技術である暗号技術の重要性はますます高まっている。さらに、通信技術の急速な発展に伴い、RFID や医療機器などのリソース制限のあるデバイスでの実装要件にも対応する必要がある。また 5G および 6G のモバイル通信システムの急速な進展に伴い、超高速暗号アルゴリズム求められている。

本論文では、これらのニーズに応えるため、軽量暗号、低遅延暗号、超高速暗号アルコリズムの設計手法に関して新たな知見を与えている。この理論をもとに、軽量ブロック暗号 WARP、軽量 Tweakable ブロック暗号 TWINE,低遅延擬似乱数関数 Orthros,超高速暗号 Rocca を提案している。それぞれハードウェアサイズ、クリティカルパスの短さ、ソフトウェアでの処理速度の観点で世界一を達成している。

このように、本研究は共通鍵暗号の設計理論に関して新規性を有しており、また実際の暗号アルゴリズムも設計しており有用性の観点でも優れている。以上より、本研究は博士の学位に値するものと認める。