氏　　名	小寺　雄太
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第　　６１９２　　号
学位授与の日付	２０２０年　３月２５日
学位授与の要件	自然科学研究科　　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study of Cryptographic Primitives for Efficient Database Protection （効率的なデータベース保護を実現する暗号方式に関する研究）
論文審査委員	教授　野上　保之　　教授　豊田　啓孝　　准教授　栗林　稔

学位論文内容の要旨

Recently, cloud storage has been widely used in both business use and personal use. However, using a classical ciphering system to protect private information prevents even data owners to edit, search a keyword, or some kind of arithmetic operation to the encrypted data in general. To address this hardness, researchers have devoted much time to studying a cryptosystem allowing operations over the encrypted domain. Such cryptosystems are said to be functional encryptions, and recently, secure database systems have been developed in both academia and industry by well combining several types of functional encryptions.

Searchable encryptions (SEs) are the class of techniques that enables a client to publish various queries for searching a keyword over an encrypted domain to outsource or share private data securely with a little sacrifice of information leakage. Since the information leakage can be covered by using another technique so-called oblivious random machine, SEs have been studied as a useful technique. Therefore, the thesis focuses on a typical construction of SEs using symmetric-key encryption and proposes two types of SEs.

Furthermore, one more construction is proposed, which achieves the location-based search that is a novel concept to search a keyword by considering the location of information in the matrix type storage. More precisely, the location-based search purposes to overcome the hardness of conventional schemes that indicates the hardness of searching a keyword beyond whether it is contained in documents or not. Though such searchability is required for handling the list of human-related data which can be represented by the matrix type format, for example, there is no such construction in the previous researches.

Therefore, the first construction of the location-based search is considered in the thesis. It uses the cyclotomic polynomial over a finite field to embed each entry of information represented in the manner of $m \times n$ matrix. Throughout the security discussion, it is concluded to be secure in the sense it can be an SE scheme allowing the location-based search without leaking any additional information to an adversary except the conventionally accepted leaks.

論文審査結果の要旨

本論文では，近年とくに高機能な情報セキュリティを実現するとして注目をされる検索可能暗号の実現に関する理論的およびアルゴリズム的な研究の成果を報告している。最初に，その実現の鍵として重要となる「機能的かつセキュリティ応用できる擬似乱数生成法」の提案を行っており，とくにセキュリティ観点で重要となるビットおよびビットパターンの分布特性に対して理論的な証明を与えた。また，生成される擬似乱数系列に対して，群構造的な性質を有することを発見し，その理論的な証明を与えるなど，既存の研究とは異なる観点から多くの成果を得ている。その理論的な成果に基づき，その擬似乱数生成法に関してセキュリティ観点からビット分布を均一化する必要性があることを問題提起し，その効率のよい均等化手法を提案し，アルゴリズムにまとめている。

続いて，その擬似乱数生成に関する研究の成果をベースにしながら，検索可能暗号の新たなアプローチを提案している。具体的には，従来では部分一致検索を行うために複数個のトラップドアを生成する必要があったが，本研究では先に述べた擬似乱数生成器を用いることで単一のトラップドアで確率的に部分一致検索を行う仕組みを実現している。また，世界に先駆けてMatrixタイプのデータベースに対する具体的な検索可能暗号方式を提案している。これにより，Matrix形式のデータに対して，行および列を指定するような暗号化キーワード検索を可能としている。そのトラップドアは有限体理論に基づく数学的な困難性も利用しており，組織的なMatrixデータベースの暗号化および暗号化キーワードによる検索トラップドアを構成するアルゴリズムを提案している。

以上のような成果は，申請者を筆頭著者とするジャーナル論文4本，国際会議論文5本にまとめられている。その国際会議論文の内の1つはBest Paper Awardを受賞しており，申請者を共著者とする論文や国際会議発表は10本以上を数え，広く当該分野の研究者に認められているものである。

本博士論文は，そのような複数の研究成果が具体的なパラメータを用いた構成法も交えて詳述されており，博士（工学）の称号を与えるに相応しいものであると判断する。