Towards Practical Inner Product Functional Encryption(Abstract_要旨)

AUTHOR(S):

Tomida, Junichi

CITATION:

Tomida, Junichi. Towards Practical Inner Product Functional Encryption. 京都大学, 2021, 博士(情報学)

ISSUE DATE:

2021-05-24

URL:

https://doi.org/10.14989/doctor.r13425

（ 続紙 1 ）

京都大学	博士（情報学）	氏名	富田 潤一
論文題目	Towards Practical Inner Product Functional Encryption （実用的な内積関数型暗号に向けて）		

（論文内容の要旨）

本論文は、内積関数型暗号とよばれる機能性の高い暗号を実用的にすることを目的とした研究に関するものである。従来の暗号は暗号文を復号すると元データが出力されるが、関数型暗号は元データに所望の関数を適用した関数値のみを復号できる次世代の暗号技術である。信頼できないクラウドサーバーへの安全な計算委託など様々な応用が期待されており、暗号理論および暗号応用研究の中心的研究課題の一つとなっている。内積関数型暗号は、適用できる関数が内積（一次関数）に限定された関数型暗号の一クラスである。関数が限定される一方、高速な方式が構成できることが知られており、実用の可能性が高い関数型暗号の一つである。

本論文は七つの章から構成されている。

第一章では、現代暗号の基本的な概念を概説した後に、関数型暗号の研究の発展について説明している。関数型暗号の研究はIDベース暗号や属性ベース暗号といった復号条件を制御できる暗号に始まり、それらの概念をより一般化することで定式化されたものである。関数型暗号という概念が提唱された後には、一般的な関数型暗号の実現方法や、様々な安全性や性質を持つ関数型暗号について、識別不可能性難読化との関係など非常に多岐にわたる研究がなされている。

第二章では、本論文の主題である内積関数型暗号について既存研究を紹介し、それらに対する本研究の位置づけ及び貢献内容が述べられている。特に本論文では、従来の内積関数型暗号と比べて、効率・機能・安全性の面で優れた方式について研究するものであり、その研究意義と具体的な技術的課題が示されている。

第三章では、第四章以降で必要な記法、暗号学における基礎的な要素技術や関数型暗号などの厳密な定義を与えている。

第四章では、関数秘匿と呼ばれる性質を持つ内積関数型暗号の効率的な構成方法を提案している。関数秘匿は、ある関数を計算して復号するための秘密鍵を与えられた復号者に、その関数自体を知られないようにすることができるという性質である。例えば、内積関数型暗号の有力な応用である生体認証では、計算する関数の表現自体が認証する個人の生体情報を含むため、認証サーバから個人のプライバシーを守るために関数秘匿が必要となる。本章では、従来技術と比較して計算量や使用メモリ量が半分程度となる方式が提案されており、その構成のアイディアは第五章、第六章の結果にも影響を与えている。

第五章では、データサイズに制限のない内積関数型暗号の構成方法が与えられている。従来の内積関数型暗号では、暗号システムの利用開始時にデータサイズを固定する必要があり、以降暗号化できるデータはその固定したサイズのものに限定されるという制限があった。この性質は、様々なサイズのデータを扱うシステムにおいては非効率的な性質であり、どのようなサイズのデータであってもその長さに合わせて暗号化できることが望ましい。本章では、そのような制限がなく任意のサイズのデータを暗号化できる内積関数型暗号の構成方法を提案している。特に、第四章で説明した関数秘匿と呼ばれる性質を持つ方式と、公開鍵方式と呼ばれる暗号化のための鍵を公開することができる方式について構成を示している。

第六章では、緊密安全な種々の内積関数型暗号を得る方法に関する結果が与えられている。暗号方式が緊密安全であるとは、暗号システムを破ろうとする攻撃者が多数の暗号文を入手できる状況であっても、その入手した数に応じて暗号方式の安全性が低下しないことが理論的に証明されていることを指す。撃者は複数の暗号文を入手できると考えるのが現実的なため、実用的な暗号方式は緊密安全であることが望ましいが、従来の内積関数型暗号はいずれも緊密安全性が示されていない。本章では、主に二つの技術を提案している。一つは緊密安全性を持つ内積関数型暗号の構成方法とその安全性証明方法であり、もう一つは緊密安全な内積関数型暗号を関数秘匿性を持つ（多入力）内積関数型暗号へ緊密安全性を維持したまま変換する方法である。1つ目の結果により緊密安全な内積関数型暗号が得られること、2つ目の結果を1つ目の結果に応用することで、緊密安全で関数秘匿な（多入力）内積関数型暗号が構成できる。

第七章では、本論文のまとめと内積関数型暗号における今後の課題や未解決問題が述べられている。本論文では、実用的な内積関数型暗号の実現に向けて、効率性の向上、入力サイズ制限の除去、緊密安全性の獲得方法の3点について、それぞれ新しい技術を提案した。効率の向上技術は残りの2つの結果にも組み込まれているが、入力サイズ制限の除去と緊密安全性を獲得する技術は同時には利用できない。これらはいずれも実用上重要な性質であり、その両立は今後の課題である。また、内積計算だけでは実現できない応用に供するため、より高度な関数を効率的に計算できる関数型暗号の実現が重要な課題である。

（続紙 ２ ）

（論文審査の結果の要旨）
関数型暗号は暗号文を復号すると元データを入力とした関数値のみが得られる暗号方式である。開示できない個人情報に対する委託計算などの重要な応用があり、その実用的な構成は近年における暗号研究の中心的テーマの一つである。任意の関数を扱える関数型暗号は理論的には構成可能であるが、膨大な計算が必要であり実用には遠い状況である。本論文は、関数型暗号の一種である内積関数型暗号について、高効率化・高機能化・安全性向上を図る手法について述べたものであり、得られた成果は以下のとおりである。

（１）関数型暗号の性質の一つである関数秘匿は、計算した関数が復号者に知られないようにする技術である。内積関数型暗号においては、内積計算における一方の入力値を隠蔽することで関数秘匿を達成できるが、安全に隠蔽できることを保証するには大きなパラメータを必要とし、計算効率が低い方法しか知られていなかった。本論文では、安全性証明で用いるハイブリッド論法のステップを効率化する手法を開発し、より小さなパラメータで同等の安全性を保障できることを示した。これによって、半分のメモリ量で倍の計算効率を達成する関数秘匿内積関数型暗号の構成が可能となった。この証明技法は以下の高機能化・安全性向上の技術においても効率を向上するために利用されている。

（２）従来の関数型暗号では、関数の入力サイズは予め固定されており、動的にサイズの変化するデータを扱うことができないという機能上の制約があった。これは、例えば、膨大な塩基配列の部分的な近似度の計算において部分的な入力を許さず、データの最大長に合わせた設定が必要なことを意味し、暗号化・復号の効率が著しく低下するという問題を生じる。本論文では、一つの主鍵対から任意個の副鍵対を生成する手法を開発し、入力に制限がない、すなわち入力サイズが可変で部分的な復号も可能な内積関数型暗号を構成した。

（３）暗号の実利用において攻撃者が複数の暗号文を観測できることは極めて自然な状況であり、観測された暗号文の個数が増大しても安全性が損なわれない方式が望ましいが、そのような方式の構成方法は知られていなかった。本論文では、同一の公開鍵で生成された複数の暗号文とそれらに対する復号結果を攻撃者が入手できる場合であっても安全性が損なわれない、緊密安全性を有する内積関数型暗号を構成した。ここでは、関数秘匿内積関数型暗号から複数の暗号文を入力として関数を計算する入力関数秘匿内積関数型暗号への安全な変換方法も開発した。

以上、本論文では実用的な内積関数型暗号を構成するために必要な効率化、高機能化、安全性向上の研究課題に取り組み、関数秘匿においてメモリ・計算効率を倍増する構成、入力サイズに制限のない機能的な構成、および実利用環境に即した緊密安全性を有する構成を示した。いずれの構成も新規性、有用性の高い手法によるものであり、当該分野の発展のために十分な寄与をしている。よって、本論文は博士（情報学）の学位論文として価値あるものと認める。また、令和３年３月２９日、論文内容とそれに関連した事項について試問を行った結果、合格と認めた。また、本論文のインターネットでの全文公表についても支障がないことを確認した。

要旨公開可能日：　　年　　月　　日以降