氏名（本籍）	黒川 貴司（東京都）
専攻分野の名称	博士（工学）
学位記番号	工博甲第 267 号
学位授与の日付	令和 5 年 3 月 23 日
学位授与の要件	学位規則第 4 条第 1 項該当
研究科・専攻	工学資源学研究科　電気電子情報システム工学専攻
学位論文題目（英文）	Analysis of algorithms related to multivariate public key cryptosystems and the transport layer protocol
論文審査委員	（主査）教授　山村　明弘 （副査）教授　河上　肇 （副査）教授　小野田　勝 （副査）准教授　田沼　慶忠

論文内容の要旨

近年、量子コンピュータの開発が進んできており、従来から使われてきている RSA 暗号などはショアのアルゴリズムにより、将来危殆化する懸念がある。いつ誤り訂正が可能で大規模な量子コンピュータが登場するかを明らかにすることは難しいが、暗号技術の社会実装には年月が掛かり、もし安全でなかつた場合はさまざまな損失をこうむるおそれがあるため、導入前の段階においてきちんと安全性評価を行うことが必要である。現在、米国の政府機関である NIST が行っている耐量子計算機暗号を選定するプロジェクトには世界中から多くの公開鍵暗号方式が提案されている。2022 年現在このプロジェクトはラウンド 4 まで進んでいて、多変数公開鍵暗号はセレクションには残っていないが、再度、電子署名方式の公募が進められているため、多変数公開鍵暗号が再度登場することが期待される。その中で、多変数多項式の求解問題の困難性に安全性を依拠する公開鍵暗号方式が存在する。それを多変数公開鍵暗号と呼ぶ。多変数公開鍵暗号の安全性を評価するためには、多変数多項式の求解問題に関する安全性の評価が必要になる。多変数多項式の求解問題を解くアルゴリズムには、グレブナー基底計算アルゴリズムとその変形版である F4 アルゴリズムがある。グレブナー基底計算では、2 つの多項式の最高次の単項式を打ち消し合う、リダクションという操作を行う。2 つの多項式と、2 つの多項式の最高次の単項式を打ち消し合うために用い

られる単項式を合わせて、クリティカルペアと呼ぶ。F4 アルゴリズムでは、クリティカルペアからマコーレー行列と呼ばれる行列を構成し、ガウス消去を行うことで、まとめて複数の多項式のリダクションを行うという特徴(メリット)がある。しかしながら、行列のサイズが大きくなるにつれて処理コストが大きくなるというデメリットもある。このようなデメリットへの対策として、クリティカルペアからなる集合を部分集合に分割して、各部分集合ごとにリダクションの処理を行い、マコーレー行列のガウス消去において、 ランクが落ちたら(ゼロ多項式が生成されたら)その他の部分集合を無視して、次の処理(より次数の高いクリティカルペアの処理)に進むことで処理時間を短縮可能であるという既存研究がある。この基本戦略に対して、いくつかの改良版を提案し、計算機実験によりオリジナルの F4 アルゴリズムに比べて処理時間を短縮できること(約 6〜7 分の 1)を示した。また、マコーレー行列のガウス消去において、ランクが落ちた際に残りのクリティカルペアを無視しても失敗する割合が非常に少ないことも、計算機実験により確かめた。さらに、マコーレー行列のランクが落ちるために最低限必要なクリティカルペアの数の害Ⅲ合がほぼ一定という特徴があることも計算機実験により明らかになった。このような特徴の数学的な理由付けを明らかにすることは今後の課題である。

次に、暗号通信プロトコルである SSL/TLS はオンラインションピングなど身近な場所で広く普及しており、通信内容の漏洩を防ぐための暗号化機能の他にも、通信相手を認証するための機能が含まれている。これらの機能に支障をきたしてしまうと、安全に通信サービスを使うことができなくなる。近年、SSL/TLS に対して、CRIME、LUCKY THIRTEEN、POODLE、BEAST 等、多くの攻撃手法が提案され、実際の適用事例が公表されてきている。ここで、BEAST 攻撃は、TLS l.0 における CBC モードと呼ばれるブロック暗号の一種の操作方法に対して適用可能な攻撃方法である。TLS l.0 の CBC モードには 2 点の脆弱性がある。1 つはパディングに関する問題点で、 もう 1 つは初期化ベクトル IV の選択方法に関する問題点である、ウェブブラツザ等にセキュリティバグ等が存在すると、これらの脆弱性を突いて実際に攻撃が可能になってしまう。BEAST 攻撃に対する対策として、1/n-l レコード分害Ⅲと呼ばれるパッチが提案された。これは、送信データを一度にすべて送信するのではなく、送信データを一番はじめの 1 バイトの部分と残りの部分に分けて送信する方法である。このパッチ適用後の CBC モードに関して、選択平文攻撃に対する識別不可能性(IND-CPA)を示すことができる。本来、CBC モードでは、データを暗号化する際に、仕様で決められたいくつかの情報が付加される。つまり、SEQ_NUM というカウンターの役目を果たすデータ等にメッセージ認証コードが施された後、それが付加される、1/n-l レコード分割が対策として有効である理由は、1 バイト目の処理の際に出力される IV が予測不可能になるからだと考えられる。

論文審査結果の要旨

量子コンピュータの開発が進んできており、従来から使われてきている RSA 暗号などは P。Shor のアルゴリズムにより危殆化する懸念がある。誤り訂正が可能な大規模な量子コンピュータが利用可能となる時期を把握することはできないが、暗号技術の安全性を量子計算機の導入を考慮した上で安全性評価が必要である。米国政府標準局 NIST が行なっている耐量子計算機暗号の選定プロジェクトには多くの公開鍵暗号方式が提案されている。その一つとして多変数多項式の求解問題の困難性に安全性を依拠する公開鍵暗号方式（多変数公開鍵暗号）が提案されている。多変数公開鍵暗号の安全性評価には多変数多項式の求解問題に関するアルゴリズムの効率性の解析が必要になる。多変数多項式の求解問題を解くアルゴリズムにはグレブナー基底計算アルゴリズムとその変形版である F4 アルゴリズムが知られている。グレブナー基底計算では二つの多項式の最高次の単項式を打ち消し合うリダクションという操作を行う。二つの多項式と二つの多項式の最高次の単項式を打ち消し合うために用いられる単項式を合わせて、クリティカルペアと呼ぶ。F4 アルゴリズムではクリティカルペアからマコーレー行列と呼ばれる行列を構成しガウス消去を行うことでまとめて複数の多項式のリダクションを行うという特徴があるが、行列のサイズが大きくなるにつれて処理コストが大きくなるというデメリットもある。クリティカルペアからなる集合を部分集合に分割して各部分集合ごとにリダクションの処理を行い次の処理に進むことで処理時間を短縮可能である。この方策を改良して F4 アルゴリズムに比べて処理時間を短縮できることを示した。

暗号通信プロトコルである SSL/TLS に対して CRIME、LUCKY THIRTEEN、Poodle、BEAST 等多くの攻撃手法が提案され、実際に適用事例も公表されてきている。BEAST 攻撃は TLS l.0 における CBC モードと呼ばれるブロック暗号の暗号利用モードに対する適用可能な攻撃方法である。TLS l.0 の CBC モードには 2 点の脆弱性がある。1 つはパディングに関する問題点であり、もう 1 つは初期化ベクトル IV の選択方法に関する問題点である。Web ブラウザにセキュリティバグ等が存在するとこれらの脆弱性を利用して攻撃が可能になる。BEAST 攻撃に対する対策として 1/n-1 レコード分割と呼ばれるパッチが提案された。送信データを一度にすべて送信するのではなく送信データをはじめの 1 バイトの部分と残りの部分に分けて送信する方法である。パッチ適用後の CBC モードには選択平文攻撃に対する識別不可能性（IND-CPA）が存在することを示した。

以上のように、本論文は公開鍵暗号方式に関連するアルゴリズムの効率性や強度評価に関して新たな事項を明らかにし、情報セキュリティの安全性に関連する新たな知見を得た。本論文は博士（工学）の学位論文に値するものである。