博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　多変数公開鍵暗号の安全性に関する研究
申請者　：　藤田　亮
審査委員会　：　主査　教授　辻井重男
副査　教授　板倉征男
副査　教授　有田正剛
副査　教授　笠原正雄
副査　教授　松尾和人

Ⅰ．論文内容の要旨

博士後期課程学生、藤田亮君の博士請求論文は「多変数公開鍵暗号の安全性に関する研究」と題し、７章からなっている。

第１章　「緒言」では、本論文の研究が次のような背景の下に始められたことを述べている。１９７０年代に発明された公開鍵暗号の中で、電子社会の基盤として広く実用化されているのは、ＲＳＡ暗号と楕円暗号である。ＲＳＡの安全性は素因数分解問題の困難性に、楕円暗号の安全性は離散対数問題の困難性にそれぞれ依拠している。しかし、これらの困難性は、研究者の間で信頼性を得てはいるが、証明されているわけではない。また、両者とも暗号化・復号処理時間が共通鍵暗号に比べて桁違いに大きいという欠点も有している。そこで、これらの方式の万一のアルゴリズム的危殆化に備えるため、また、両方式より高速性の点で優れた公開鍵暗号の探求が、早くから始められている。

多変数公開鍵暗号はその中の一つであり、１９８０年代、横浜国立大学の今井研究室（当時)、及び東京工業大学の辻井研究室（当時）において始められた日本生まれの公開鍵暗号である。１９９４年、素因数分解問題、及び離散対数問題は、量子コンピュータによって現実的時間で解かれることが明らかにされたが、多変数公開鍵暗号が依拠する多変数方程式の求解困難性はＮＰ完全であり、量子コンピュータによっても解けないため、２０００年前後から、海外においても多くの方式が発表されて今日に至っている。しかし、どの方式も落とし戸構造に基づく脆弱性を内包しており、安全性向上が重要な課題となっており、本研究の目的が、多様な多変数公開鍵暗号の安全性向上させる方式を探求することにあると述べている。

第２章「多変数公開鍵暗号の安全性に関する従来研究」では、多変数公開鍵暗号の概要について説明した後、多変数公開鍵暗号に対する多様な攻撃法とそれらに対する安全性強化について、従来の研究成果を体系的に説明している。

第３章「線形持駒行列方式」では、多くの乱数、及びランダム多項式を付加することにより、多様な多変数公開鍵暗号の安全性を強化する方式を提案し、多様な攻撃法に対するに対する安全性について検討している。特にグレブナ基底計算攻撃に対しては、これまで提案された方式に比べて、解読計算時間が、著しく増大することを計算機シミュレーションによって示している。

第４章「非線形持駒行列方式」においては、線形持駒方式の安全性をより強化するため、送信側から送られてきた補助情報を用いて、持駒行列の要素に平分変数を含む非線形持駒行列方式を提案し、グレブナー基底計算攻撃に対する計算量が、線形持駒行列より増大することを計算機シミュレーションによって示している。

第５章「非線形持駒摂動ベクトル方式」では、第４章で提案した非線形持駒行列方式が４層式非線形持駒方式と見做せることに着目して、情報伝送効率（平文対暗号文の比率）を高めつつ、グレブナ基底計算攻撃に対する耐性をより向上できることに着目して、３層式非線形持駒方式を提案して、そのことを計算機シミュレーションンによって実証し、更にランク攻撃に対する安全性、差分攻撃に対する安全性について検討し、これらの攻撃に対し安全であることを確認している。

第６章「２層式非線形持駒方式」では、第５章で提案した非線形持駒行列方式におけるランダム多項式部を２つの多変数１次多項式の積に置き換えることにより、差分攻撃に対する攻撃を回避し、より情報伝送効率を高める方式を提案し、グレブナ基底計算攻撃に対する耐性が大きいこと、及び、ランク攻撃、差分攻撃に対する安全性を確認している。

第７章「結論」では、以上の成果を要約し、今後の課題として、第３章、第４章、第５章、第６章に提案した諸方式を特徴の比較と適用領域の明確化が今後の課題であると述べている。

Ⅱ. 論文審査結果の要旨

以上を要するに、本論文は、量子コンピュータが実用化された将来においても、電子社会の基盤が崩壊するのを避けるべく、RSA 暗号や楕円暗号に代わる公開鍵暗号の有力候補と見做されている多変数公開鍵暗号の安全性を可能な限り汎用的に強化する持駒方式を提案し、その安全性について、代数攻撃（グレブナ基底計算攻撃)、ランク攻撃、差分攻撃等、想定される全ての攻撃に対する安全性を検討して、その有効性を示したものであって、情報学並びに情報社会の発展に貢献するところが大きい。よって、我々は、本論文が、博士（情報学）の学位論文として十分価値あるものと認める。

Ⅲ. 審査経過

本審査委員会は、2008 年 1 月 28 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。