論文審査の結果の要旨

氏名　小暮　淳

本論文は「Security Analysis against Random Key Bits Leakage Attack and Hardness of Subset Sum Problem from Different Intervals（ランダム鍵ビット漏洩攻撃に対する安全性解析と異なる区間からの部分和問題の困難性）と題し、5 章から構成されている。情報の安全性を守るために暗号技術が広く使われているが、計算量的な安全性に基づく暗号では、素因数分解, 離散対数問題, ナップザック問題などを解くのに非常に多くの時間がかかるという計算量的な安全性に根拠が置かれている．しかし，サイドチャンネル攻撃（デバイスの物理的挙動を観測することなどにより秘密情報の一部を得る攻撃）による安全性の脅威や、将来量子コンピュータが実用化したときに、素因数分解や離散対数問題が多項式時間で解けるという脅威が存在することが知られている。本論文では、このような背景の下で、前者の脅威に対する評価として素因数分解の困難さに根拠を置く暗号系に対するランダム鍵ビット漏洩攻撃に対する安全性解析を行い、後者の脅威に対しては、量子コンピュータを用いても多項式時間の解法が知られていないナップザック問題に対して安全性評価を行なっている。

第 1 章「Introduction」では、研究の背景を述べると共に、本研究の目的および従来研究に対する本研究の位置付けを述べている。

第 2 章「Preliminaries and Notation」では、本研究で対象とする公開鍵暗号である RSA 暗号、Paillier 暗号、Takagi 暗号、Okamoto-Tanaka-Uchiyama 暗号の暗号化および復号化の手続きを紹介すると共に、本論文で使用する表記法を示している。

第 3 章「Security Analysis against Random Key Bits Leakage Attack」では、RSA 暗号の秘密鍵のランダムな部分情報が漏洩したと仮定して秘密鍵全体を求める Heninger と Shacham の攻撃手法の安全性解析を、特定の暗号に拠らない一般の場合に拡張している。また、その一般的な解析手法を、Pailler 暗号, RSA 暗号の素数の積 pq を p^tq に拡張した Takagi 暗号に適用している。その結果、本攻撃に対して Pailler 暗号は RSA 暗号とほぼ同等の安全性を有し、Takagi 暗号は、$t = 2$ のときのみ Takagi 暗号が RSA 暗号より安全となることを明らかにしている。

第 4 章「Hardness of Subset Sum Problem from Different Interval」では、部分和問題の困難さに基づくナップサック型暗号を取り上げている。将来、量子コンピュータが実現すると素因数分解が多項式時間で解かれるため、第 3 章で取り上げたような暗号は安全でなくなるため、他の暗号を準備しておく必要があるが、部分和問題に基づくナップサック型暗号が有力な候補の 1 つと考えられている。部分和問題は、格子理論に基づく最短ベクトル問題と密接に関係しており、部分和の各重みがある一定の区間から一様

に取られている場合、その区間幅の対数値の逆数で決まるように定義された密度が、ある閾値 d_0 以下であれば部分和問題が解けることを Lagarias と Odlyzko が格子理論に基づき示している。これに対して、本研究では、各重みがそれぞれ異なる区間から一様に取られる場合に対して、Lagorias と Odlyzko の解析手法を拡張することにより、安全性解析を行なっている。その結果、密度を各区間幅の調和平均の対数値の逆数で決まるように定義すると、その密度が同じ閾値 d_0 以下のときに、部分和問題が解けるという、より一般的な結果を理論的に証明している。本研究の成果は、秘密鍵サイズをよりフレキシブルに変化させるようなナップサック型暗号を検討するときに重要となる。

最後に、第 5 章「Conclusion」で本研究の結果と貢献をまとめている。

なお、本論文の第 3 章と第 4 章の成果は、山本博資および國廣昇との共同研究であるが、論文提出者が主体となって新しい解析手法の提案、理論解析、数値実験を行なったものであり、論文提出者の寄与が十分であると判断する。

したがって、博士（科学）の学位を授与できると認める。

以上 1783 字