論文の内容の要旨

論文題目　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）

氏　　名　小暮　淳

1　背景

今日の情報通信社会において情報セキュリティ技術が果たす役割は非常に重要であり、暗号技術はその中核をなす技術の一つであるため、本論文では暗号技術に焦点を当てる。暗号アルゴリズムは共通鍵暗号と公開鍵暗号との 2 種類がある。公開鍵暗号は整数論を直接利用しており、攻撃法も多様なアプローチが考えられるため、本論文では公開鍵暗号の安全性解析を目的とする。

現在の暗号の安全性は解読アルゴリズムの計算量に基づいている。解読アルゴリズムを高速に改良するアプローチはここ数十年大きな進展はないが、それ以外にもサイドチャネル攻撃や量子計算機攻撃などの大きな脅威がある。前者はデバイスの物理的挙動を観察することにより秘密情報を引き出すものであり、後者は能力の高い計算機モデルを利用するものである。本論文では、これらのアプローチに対する対策を考える上で必要な安全性解析に関して貢献することを目指す。

2　既存暗号の安全性解析
－ランダム鍵ビット漏洩攻撃に対する安全性解析

サイドチャネル攻撃は 1990 年代後半から盛んに研究されており、暗号研究の大きな流れの一つとなっている。公開鍵暗号で最もよく使われている RSA 暗号[5]に関しては、秘密鍵の一部の漏洩を仮定し秘密鍵全体を求める研究が広範囲に行われていた。2009 年に Heninger と Shacham[1]は、RSA

暗号秘密鍵のランダムな部分情報が漏れたと仮定して秘密鍵全体を求める新しい手法を示した。彼らの方法は以下の 4 段階からなる。

1. 秘密鍵の各ビットを変数として、その間に成り立つ関係式を求める。
2. 最下位ビットから始めて、上位ビットの解候補値を順に求める。
3. 漏洩情報と解候補の値を比較し、一致しないものは候補から外す。
4. 残った候補が秘密鍵が満たすべき関係式を満たすかどうかを確認する。

彼らの方法はランダム情報が漏れると仮定する点で新しく、ある状況で実現可能でもあるため重要であるが、彼らの安全性解析は RSA 暗号の場合のみであった。本論文の貢献は以下の 2 点である。

1. 本攻撃に対する安全性解析を一般の場合に拡張した。
2. 安全性解析を他の幾つかの具体的な暗号に適用した。

効果としては、以下の 2 点であると考える。

1. 他の暗号の本攻撃に対する安全性解析が容易かつ統一的になった。
2. 本攻撃に対する暗号のセキュリティパラメーター設定が容易かつ統一的になった。

攻撃を他の暗号に適用した場合、第 1 段階において得られる関係式は RSA 暗号と異なり、安全性解析も異なる。この関係式が一般の形の線型連立方程式の場合に、解候補数の期待値の上界は以下の 4 つの要素により明に記述できる。

1. 秘密鍵の各ビットが漏洩する確率 δ
2. 変数の数 r
3. 一つ前までのビットの値からは一意に決まらない変数の数 l
4. 一意に決まらない変数の方程式系の自由度 w

一つ前のビットまでの解の割り当てが正しい場合に生成される誤った解候補数の期待値を $\mathrm{E}Z_g$、割り当てが誤っている場合に生成される誤った解候補数の期待値を $\mathrm{E}W_b$ と書くと、

$$\mathrm{E}Z_g = \sum_{j=0}^{w-1} \delta^j (1-\delta)^{l-j} \binom{l}{j} (2^{w-j} - 1)$$

および

$$\mathrm{E}W_b = \frac{(2-\delta)^r}{2^{r-w}}$$

となる。誤った解候補数の期待値の総計は

$$\frac{\mathrm{E}Z_g}{1-\mathrm{E}W_b}$$

に秘密鍵のビット長を掛けた数で上から抑えられる。

本結果を Paillier 暗号[4]および高木による RSA 暗号の変形[6]に適用した。Paillier 暗号は、データを暗号化したまま加算が可能であり、クラウドサービス環境において近年期待が大きい技術である。Paillier 暗号の本攻撃に対する安全性は、RSA 秘密鍵のうち 3 変数の情報が漏洩する場合とほぼ同等であることが判明した。高木による RSA 暗号の変形は、暗号鍵の法の形が RSA の場合は pq であるものを、$p^v q$ という形に変形することにより復号性能を向上させたものである。この形の法は他の標準暗号でも用いられることがあり、安全性を検討しておくことは重要である。RSA 暗号と比較すると、$v = 2$ のときのみトータルの解候補数は高木の変形の方が大きくなることが判明した。ただし高木の

変形の場合、事前計算により得られる情報が少なく、トータルの攻撃計算量は RSA に比べて公開鍵指数を e とすると $O(e^2)$ 倍となり、本攻撃に対しては、より安全であると言える。

3　将来に備えた暗号の安全性解析
－異なる区間からの部分和問題の困難性

量子計算機の実現等により現在の暗号が効率的に解かれる場合に備え、異なる問題の困難性に安全性を依拠する暗号を準備しておく必要がある。候補として幾つかの問題が提案されているが、本論文では格子理論に関連した問題、特に部分和問題と最短ベクトル問題(SVP：Shortest Vector Problem)とに焦点を当てる。格子理論に関連した問題に基づく暗号が、現時点では実用に最も近いと考えるからである。

部分和問題とは、n 個の正の整数(重み) $a_1,...,a_n$ およびその部分和 s が与えられたときに、その部分和を与える部分集合を求める問題である。即ち

$$s = \sum_{i=1}^{n} m_i a_i$$

となるような、$m = (m_i) \in \{0,1\}^n$ を求める問題である。ナップサック型暗号では、重み $a_1,...,a_n$ を公開鍵とし、平文 m に対して暗号文を s とするため、暗号文と公開鍵とから平文を求める問題は正に部分和問題となる。Lagarias と Odlyzko[2]は、すべての重みが、ある同一区間 $[1, A]$ から一様ランダムに選択されたと仮定し、部分和問題の密度 d を

$$d = \frac{n}{\log_2 A}$$

と定義し、密度がある閾値 $d_0 = 0.6463...$ より小さい場合には部分和問題を SVP に帰着する方法(LO アルゴリズム)を提示した。更に最短ベクトルを LLL アルゴリズム[3]などの近似アルゴリズムにより求め、それが真の最短ベクトルである場合には元の部分和問題を解くことができる。このことから密度 d は、部分和問題の困難性の指標と見ることができる。

これまでの研究は、すべての重みが同一区間から一様ランダムに選択されるという仮定に基づいていた。しかしながらナップサック型暗号の改良を考える上で、上記仮定は必ずしも満たされるとは限らない。例えば公開鍵のサイズを削減する方法として、各重み a_i のビット長を i によって変える方法が考えられるが、そのような場合には上記仮定は満たされない。そこで本論文では、上記仮定が満たされない場合の部分和問題の困難性について考察する。本論文の貢献は以下の 2 点である。

1. 各重みが異なる区間から選択されたと仮定した場合の部分和問題の困難性を解析した。
2. そのような場合に新しい密度の定義を導入し、その有効性を示した。

これらの結果の効果は、鍵生成などにおいて、より柔軟な暗号の設計が可能となることであると考える。

各 a_i が、それぞれ異なる区間 $[1, A_i]$（A_i は正の整数)から一様ランダムに選択されたと仮定し、密度 d の代わりに新たな密度 d_H を

$$d_H = \frac{n}{\log_2 \mathrm{HM}(A_1,...,A_n)}$$

により定義すると、d_H が閾値 d_0 より小さい場合には LO アルゴリズムが有効に働くことを示した。

ただし $\mathrm{HM}(A_1,...,A_n)$ は、$A_1,...,A_n$ の調和平均

$$\mathrm{HM}(A_1,...,A_n)=\frac{1}{\frac{\frac{1}{A_1}+...+\frac{1}{A_n}}{n}}$$

を表す。また、各重みが異なるビット長の場合に解読実験を行い、その困難性を示す指標として d よりも d_H の方が適切であることを示した。

参考文献

[1] Heninger, N. and Shacham, H.: Reconstructing RSA Private Keys from Random Key Bits. In: Proceedings of CRYPTO 2009, LNCS 5677, pp.1--17, Springer, Heidelberg (2009)

[2] Lagarias, J. C. and Odlyzko, A. M.: Solving low-density subset sum problems. In: J. ACM, 32(1), pp. 229--246, 1985

[3] Lenstra, A. K., Lenstra Jr., H. W., and Lovász, L.: Factoring polynomials with rational coefficients. In: Mathematische Annalen, 261, pp.515--534, 1982

[4] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Proceedings of EUROCRYPT 1999. LNCS 1592, pp.223--238, Springer, Heidelberg (1999)

[5] Rivest, R.L., Shamir, A., and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. In: Comm. of the ACM, Vol. 21(2), pp.120--126, 1978

[6] Takagi, T.: Fast RSA-type Cryptosystem Modulo $p^k q$. In: Proceedings of CRYPTO 1998, LNCS 1462, pp.318--326, Springer, Heidelberg (1998)