非可換群を用いた完全準同型暗号

縫田　光司（ぬいだ　こうじ）

産業技術総合研究所

k.nuida@aist.go.jp

2014 年 5 月 22 日

概 要

現在知られている暗号技術は、そのほぼ全てが可換な代数的構造（可換群など）を基盤として構成されている。本発表では、非可換群を用いることで完全準同型暗号という公開鍵暗号技術の構成を簡略化する話者の最近の研究について解説し、この研究で直面している数学的問題の紹介を行った。

1　公開鍵暗号

「公開鍵暗号」とは、誰もが入手できる公開情報（「公開鍵」）を用いて通信したいメッセージを暗号文に変換する暗号化アルゴリズムと、受信者だけが知っている秘密情報（「秘密鍵」）を用いて暗号文をもとのメッセージへ戻す復号アルゴリズムを備えた暗号技術のことである。暗号化と復号のアルゴリズムを適切に設計することで、攻撃者が公開鍵と暗号文のペアを入手したとしても、もとのメッセージの情報が得られないようにすることが目標である。

より詳しくは、公開鍵暗号の**暗号化アルゴリズム** Enc は、公開鍵 pk と、メッセージ集合 $\mathcal{M}$ から取ったメッセージ $m \in \mathcal{M}$ を入力とし、**暗号文** $c \in \mathcal{C}$（$\mathcal{C}$ は暗号文全体の集合）を出力する確率的アルゴリズムである。一方、**復号アルゴリズム** Dec は、秘密鍵 sk と暗号文 $c \in \mathcal{C}$ を入力とし、メッセージ $m \in \mathcal{M}$ もしくは「復号失敗」を表す記号 $\perp$ を出力する（何らかのメッセージに正しく対応しない暗号文が入力に与えられる可能性も考慮している）。厳密な定式化では、この他に公開鍵と秘密鍵を生成する**鍵生成アルゴリズム**も導入するが、簡略化のため本稿では割愛する。この状況で、公開鍵暗号が**完全**である（「完全準同型暗号」の「完全」とは無関係なので注意されたい）ということを、$\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) = m$ となる確率が「ほぼ 1 である」ことと定める（注意 1 を参照）。つまり、「暗号化して復号すると（充分小さい確率を除いて）ちゃんと元のメッセージに戻る」ということである。

注意 1. 実際には、公開鍵暗号の構成の背後には、暗号の安全性強度を定める何らかの正整数パラメータ（セキュリティパラメータと呼ばれる）が定まっている。例えば RSA 暗号の場合、素数二つの積 $N = pq$ を用いて暗号が構成されるが、この場合素数 p と q もしくは合成数 N のビット長（二進数表示の桁数）がセキュリティパラメータとされることが多い。そのため、上述の確率 $\Pr[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) = m]$ も、本来はセキュリティパラメータの関数として捉えられるべきものである。このようなセキュリティパラメータ λ の関数 $\varepsilon = \varepsilon(\lambda)$ が**無視できるくらい小さい**ということを、$\varepsilon = \lambda^{-\omega(1)}$、つまり $-\log \varepsilon / \log \lambda$ が定数オーダーより真に大きいことと定義する（例えば、指数関数的に減少する関数など）。そして、$\varepsilon \in [0, 1]$ が**ほぼ 1 である**ということを、$1 - \varepsilon$ が無視できるくらい小さいことと定義する。

以下、公開鍵暗号の具体例を紹介する。

例 2 (ElGamal 暗号（ElGamal, 1985 [1]）)**.** 有限（乗法）巡回群 $G = \langle g \rangle$ とその生成元 g、および G の元 $h := g^s$ を公開鍵 pk とし、指数 $s \in \mathbb{Z}$ を秘密鍵 sk とする。メッセージ集合は $\mathcal{M} = G$、暗号文集合は $\mathcal{C} = G \times G$ である。

$\mathsf{Enc}(\mathsf{pk}, m)$（$m \in G$）暗号化アルゴリズムは、まず整数 r をランダムに選び、$c_1 := g^r$、$c_2 := mh^r$ として暗号文 $c := (c_1, c_2)$ を出力する。

$\mathsf{Dec}(\mathsf{sk}, c)$（$c = (c_1, c_2) \in G \times G$）復号アルゴリズムは、秘密鍵 s を用いて $m := c_2 {c_1}^{-s}$ を計算して出力する。

このとき、復号アルゴリズムに入力した暗号文 c が正しい形 $c = (g^r, mh^r)$ であったとすると、$h = g^s$ であることからその出力は $mg^{sr}g^{-rs} = m$ となる。よってこの公開鍵暗号は完全性を持つ。

なお、公開鍵暗号の安全性を数学的に定式化することもできるが、専門的になりすぎるので本稿では割愛する。直感的には、本稿で扱う公開鍵暗号が「安全」であるとは、暗号文と公開鍵のペア（これは誰でも入手可能）を入手したとしても、対応するメッセージの情報を何も得ることができないということを意味する。例 2 の ElGamal 暗号の場合、この暗号が安全であるための必要条件は、生成元 g と元 $h = g^s$ をもとに指数 s（正確にはそれを g の位数で割った余り）を求めること（この問題は「離散対数問題」と呼ばれる）が計算量的に困難なことである。位数が等しい巡回群は抽象群として互いに同型であるが、一般に離散対数問題の困難さは巡回群の具体的な表示の仕方に強く依存し、例えば同じ位数の巡回群であっても $\mathbb{Z}/(q-1)\mathbb{Z}$ と ${\mathbb{F}_q}^\times$ ではその上の離散対数問題の困難さは大きく異なる（前者の方がとても簡単である）。

2　準同型暗号と完全準同型暗号

近年の暗号分野では、単にメッセージを守るだけに留まらない様々な追加機能を備えた公開鍵暗号技術が研究されている。暗号文に対してある特殊な操作を施すことで、もとのメッセージの演算結果に対応した新たな暗号文を得ることができる「**準同型暗号**」もそうした高機能暗号技術の一つである。

例 3. 例 2 の ElGamal 暗号について、メッセージ集合 $\mathcal{M} = G$ には群 G の乗法演算が定まっている。一方、暗号文の集合 $\mathcal{C} = G \times G$ に対する操作として、直積群としての乗法演算を考える。すると、メッセージ m と m' に対応する暗号文 $c = (g^r, mh^r)$ と $c' = (g^{r'}, m'h^{r'})$ について、暗号文たちに操作を施した結果 $(g^{r+r'}, mm'h^{r+r'})$ は、メッセージの積 mm' に対応する暗号文となっている。このように、メッセージの乗法に対応する暗号文の演算が定まっているという意味で、ElGamal 暗号は**乗法準同型暗号**である、もしくは**乗法準同型性**を持つ、などと言われる。

初期の準同型暗号は、乗法準同型暗号や加法準同型暗号など一種類のメッセージ演算のみに対応したものであったが、対応できる演算の種類を拡大する研究が進められ、2009 年に Gentry によって任意のメッセージ演算に対応可能な「**完全準同型暗号**」が初めて実現された [2]。この方式（に限らず、その後の既存方式全て）はメッセージ集合を $\mathcal{M} = \{0, 1\}$ としているが、この場合、メッセージに対する演算として例えばビットの AND 演算 $b_1 \wedge b_2$、OR 演算 $b_1 \vee b_2$、NOT 演算 $\neg b$ の三種に対応する暗号文の演算が定まれば、他の演算は全てこれらの組合せで表せるので充分である（実際には、AND と OR はいずれか一方でよい）。

なお、完全準同型暗号に限らず既存の暗号技術は、ほぼ全てその構成基盤として巡回群などの可換な数理構造を用いている。そこで話者の最近の研究では、これまでとは異なり非可換群を用いた完全準同型暗号の新たな構成を試みている [3]。以下ではその内容を紹介する。

3　話者の研究

以下、話者による完全準同型暗号の構成のアイデアについて述べる。そのために、メッセージ集合 $\mathcal{M} = \{0, 1\}$ 上の AND 演算 $\wedge$ と NOT 演算 $\neg$ に対応する、非可換（有限）群 G 上の演算の構成を目指す。

AND 演算に対応する G 上の演算では、交換子演算 $(g, h) \mapsto [g, h] := ghg^{-1}h^{-1}$ が肝となる。より詳しくは、その入力の片方をランダムな共役元で置き換えた確率的演算 $(x_1, x_2) \mapsto [gx_1g^{-1}, x_2]$（ここで g は

群 G の一様ランダムな元）を AND 演算に対応する G 上の演算として用いたい。その際、G の単位元 1 を $0 \in \mathcal{M}$ に対応する元とし、一方で $X \subset G \setminus \{1\}$ を $1 \in \mathcal{M}$ に対応する元の空でない集合とする。まず、入力の少なくとも一つが 0 に対応する元（単位元）であれば、上記の演算結果 $[gx_1g^{-1}, x_2]$ は g の選び方によらず常に 0 に対応する元（単位元）となる。これは AND 演算の性質 $0 \wedge b = b \wedge 0 = 0$ と正しく対応している。次に入力が両方とも 1 に対応する元（X の元）である場合、AND 演算の性質 $1 \wedge 1 = 1$ と対応させるためには演算結果 $[gx_1g^{-1}, x_2]$ がまた 1 に対応する元（X の元）になることが望ましいが、実際には演算結果の挙動は G や X の選び方に大きく依存する。例えば、G が可換群であるとすると演算結果 $[gx_1g^{-1}, x_2]$ は常に単位元、つまり 0 に対応する元となるので AND 演算の性質とは決して対応しない（換言すると、本構成において G の非可換性が本質的に必要である）。そこで、所望の性質が成り立つための条件として以下の定義を導入する。

定義 4. 群 G が**交換子に関して分離的**であるとは、部分集合 $X \subset G \setminus \{1\}$ であって以下の二つの条件を満たすものが存在することと定義する。すなわち、

1. 比 $|G \setminus X|/|G|$ は（注意 1 の意味で）無視できるくらい小さい。
2. 以下を満たす（注意 1 の意味で）無視できるくらい小さな ε が存在する：任意の $x_1, x_2 \in X$ について、一様ランダムな $g \in G$ に対して $[gx_1g^{-1}, x_2] \notin X$ となる確率は ε 以下である。

二つめの条件が成り立つと、入力が両方とも 1 に対応しているとき（注意 1 の意味で）ほぼ 1 の確率で演算結果 $[gx_1g^{-1}, x_2]$ がまた 1 に対応する元となり、（無視できるくらい小さな確率を除いて）AND 演算の性質 $1 \wedge 1 = 1$ との対応が取れている。なお、一つめの条件は、実際の構成において部分集合 X が何であるかを気にすることなく X 上ほぼ一様分布する元を選べることを保障するものである。実際、この条件があると G の元はほぼ全て X の元であり、G 上の一様分布は統計距離の意味で X 上の一様分布の充分精度のよい近似となっている。

次に NOT 演算に対応する群上の演算を考えるが、そのために以下では群 G の代わりに直積群 $G \times G$ を取り扱う。そして、部分集合 $X \subset G \setminus \{1\}$ を上記のようにとるとき、

- $(x, y) \in G \times G$ が $0 \in \mathcal{M}$ に対応 $\overset{\text{def}}{\iff} y \in X$ かつ $x = 1$
- $(x, y) \in G \times G$ が $1 \in \mathcal{M}$ に対応 $\overset{\text{def}}{\iff} y \in X$ かつ $x = y$

と定める。以上の状況で、$G \times G$ 上の演算

$$\neg(x, y) := (x^{-1}y, y)$$

を考えると、これは 0 に対応する (x, y) と 1 に対応する (x, y) とを交換することがわかる。つまりこの演算は $\mathcal{M}$ 上の NOT 演算と正しく対応している。なお、群 G を直積群 $G \times G$ に取り替えた影響で、上述した AND 演算に対応する演算にも一工夫必要である。直感的には、各成分ごとに上記の演算を施すのであるが、その際ランダムな $g \in G$ の選び方を両方の成分で同期させる必要がある。すなわち、新しい演算を以下のように定める。

$$(x_1, y_1) \wedge (x_2, y_2) := ([gx_1g^{-1}, x_2], [gy_1g^{-1}, y_2]) \quad (g \in G \text{ は一様ランダムな元})$$

すると、G と X が定義 4 の条件を満たしていれば、この演算は無視できるくらい小さい確率を除いて $\mathcal{M}$ 上の AND 演算と正しく対応することがわかる。

以上のように $G \times G$ 上に AND 演算および NOT 演算と対応する演算を定義できたが、これまでの議論では安全性について全く考慮していないことに注意されたい。実際、上記のようにメッセージ $0 \in \mathcal{M}$ および $1 \in \mathcal{M}$ と $G \times G$ の元との対応を定めると、$(x, y) \in G \times G$ が 0 に対応するか 1 に対応するかは $x = 1$ であるかどうかを調べるだけで特定できるが、これは全くもって困難ではないので安全な暗号であるとは

いえない。そこで、群 G を生のまま用いる代わりに、別の群 $G^\dagger$ とその正規部分群 $H^\dagger$ で $G^\dagger/H^\dagger \simeq G$ を満たすものを用意しておき、復号以外の全ての操作を G の代わりに $G^\dagger$ 上で行うこととする。このアイデアが正しく働くためには、$G^\dagger$ の元について剰余群 G への標準的射影の値の計算が、ある秘密の情報（これが秘密鍵となる）があれば簡単であるけれども秘密の情報がないと困難であるようになればよい。しかし、この条件を満たす $G^\dagger$ と $H^\dagger$ の具体的構成にはまだ成功していないため、この具体的構成が今後解決すべき問題の一つである。

なお、定義 4 を満たす群 G の具体例としては、充分大きな素数冪 q（より正確には、$1/q$ が無視できるくらい小さいもの）に対する 2 次特殊線型群 $SL_2(\mathbb{F}_q)$ がある（部分集合 X は $X = SL_2(\mathbb{F}_q) \setminus \{\pm I\}$ で与えられる）。これは以下の二つの補題を合わせることで示される（証明は [3] を参照されたい）。

補題 5. 任意の有限群 G と部分集合 $X \subset G$、任意の元 $x, y \in G$ について、$g \in G$ を一様ランダムに選ぶとき、

$$\Pr[[gxg^{-1}, y] \notin X] \leq \frac{|G \setminus X| \cdot |Z_G(x)| \cdot |Z_G(y)|}{|G|}$$

が成り立つ。ここで $Z_G(x)$ は x の G における中心化群を表す。

補題 6. $A \in SL_2(\mathbb{F}_q)$、$A \neq \pm I$ のとき $|Z_{SL_2(\mathbb{F}_q)}(A)| \leq 2q$ が成り立つ。

上記の $G^\dagger$ および $H^\dagger$ の具体的構成を探す上で、剰余群 G の候補も多く手にしておいた方が好都合なのであるが、これまで $SL_2(\mathbb{F}_q)$ 以外の具体例を見つけていない。例えば対称群 S_n が定義 4 を満たすかどうか考えてみたが、S_n においては中心化群の濃度が比較的大きな元が多いため、補題 5 を単に適用するだけでは所望の性質を示すことはできなさそうである。もし S_n が実際に定義 4 を満たすとしても、証明には別の手法が必要となる。S_n が定義 4 を満たすかどうかも本研究に関連して解決したい問題の一つである。

参考文献

[1] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in: Proceedings of CRYPTO 1984, Lecture Notes in Computer Science 196, Springer, 1985, pp.10–18

[2] C. Gentry, Fully homomorphic encryption using ideal lattices, in: Proceedings of STOC 2009, ACM, 2009, pp.169–178

[3] K. Nuida, A simple framework for noise-free construction of fully homomorphic encryption from a special class of non-commutative groups, preprint, IACR Cryptology ePrint Archive 2014/097, 2014, http://eprint.iacr.org/2014/097