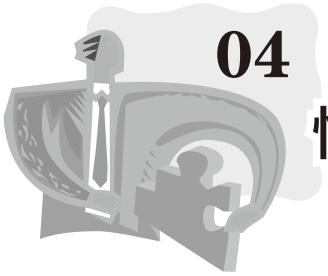

04 情報セキュリティの数学

基

花岡悟一郎（産業技術総合研究所）

証明可能安全性の概念

情報セキュリティ技術は，一見してその性質を理解することが難しく，特に，提示された手法が本当に安全であるか，もしくは，実際には危険であるかを判断することは容易でない．そのため，情報セキュリティの基盤となる暗号理論分野においても，1990 年代末頃から，要求される安全性レベルを厳密に定義し，また，設計した暗号方式がそのような安全性レベルに達しているか否かについて数学的に証明するための研究が活発に行われている．このような枠組みは，「証明可能安全性（provable security）」と呼ばれている．本稿では，暗号理論分野において，どのように安全性の概念が定義され，どのように具体的な暗号方式が設計され，どのように安全性証明がなされているかについて，なるべく平易な説明を試みるものとする．

通常想定される設定

証明可能安全性の枠組みにおいて，通常想定される設定はおおむね以下のとおりである．まず，暗号文の送信者，受信者，さらに，その不正解読を試みる攻撃者は，いずれもチューリング機械上で動作する**確率的多項式時間アルゴリズム**（PPTA）として取り扱われる．この言葉に馴染みがない読者は，単に，「計算機上で現実的に実行可能なソフトウェア」と解釈しておけば，それほど問題はないものと思われる．また，暗号方式を利用する際は，暗号文の背後にある秘匿化された情報（平文）に関する情報が，受信者以外には一切解読できないという安全性が求められる．言い換えれば，安全な暗号の定義の 1 つとして，「受信者が持つ秘密情報（復号鍵）を知らない任意の PPTA を用いても，与えられた暗号文について，それに対応した平文に関する有意な情報を一切得ることができない」場合，安全な暗号とみなすことができる．以下では，公開鍵暗号技術について，このような直観的な定義を，どのように数学的な定義として書き下ろすか，さらに，具体的な暗号方式に関して，そのように定義された安全性レベルの達成がなされているか否かの判定をどのように行うか説明を行う．

❖公開鍵暗号のモデル

公開鍵暗号の安全性を定義するにあたり，そもそも公開鍵暗号とは何を指すのかを定義する必要がある．公開鍵暗号方式 Π は，**鍵生成アルゴリズム** GEN，**暗号化アルゴリズム** ENC，**復号アルゴリズム** DEC の 3 つの PPTA の組として定義される．

GEN：1^kを入力とし，復号鍵と公開鍵のペア(sk, pk)を出力する．ここで，kは復号鍵の長さとする．

ENC：平文 m と公開鍵 pk を入力とし，暗号文 c を出力する．

DEC：暗号文 c と復号鍵 sk を入力とし，平文 m を出力する．

受信者は GEN により鍵ペアを生成し，また，このうち公開鍵を周知にする．送信者は ENC により平文を受信者の公開鍵で暗号化し，受信者に送信する．受信者は DEC により，復号鍵を用いて受信した暗号文の復号を行う．

公開鍵暗号の安全性定義

上記のようにモデル化された公開鍵暗号方式 Π において，復号鍵を持たない任意の PPTA が，与えられた暗号文について，それに対応した平文に関する有

意な情報を一切得ることができないという状態をどのように定義するか述べる．暗号文から有意な情報が一切漏れていないとは，暗号文を観測したとしても，観測しなかった場合に比べて，いかなる平文の部分情報についても，それを言い当てる確率に有意な変化がないとも言い換えることができる．このような安全性の概念は，次のように定義される．まず，あるPPTA $\mathcal{A}$ が，自由に平文候補の集合 X と関数 f を選んだ上で，X からランダムに選ばれた平文 m の暗号文 c を観測し，その上で m を f に代入した値（すなわち，平文 m に関するなんらかの部分情報）$f(m)$ を言い当てられるかを観測する試行 $\mathbf{Exp}^{ss-1}_{\Pi,\mathcal{A}}(k)$ は次のように定式化できる：

$\mathbf{Exp}^{ss-1}_{\Pi,\mathcal{A}}(k)$
　$(sk, pk) \leftarrow \mathrm{GEN}(1^k)$;
　$(X,$ 状態情報 $s) \leftarrow \mathcal{A}($ 選択モード $, pk)$;
　m を X からランダムに選択；
　$\underline{c \leftarrow \mathrm{ENC}(m, pk)}$;
　$(v, f) \leftarrow \mathcal{A}($ 推定モード $, \underline{c}, pk, s)$;
　$v = f(m)$ ならば $d \leftarrow 1$;
　$v \neq f(m)$ ならば $d \leftarrow 0$;
　return d.

なお，下記の試行 $\mathbf{Exp}^{ss-0}_{\Pi,\mathcal{B}}(k)$ との差異が分かるように，該当部分に下線を引いている．試行 $\mathbf{Exp}^{ss-1}_{\Pi,\mathcal{A}}(k)$ では，試行 $\mathbf{Exp}^{ss-0}_{\Pi,\mathcal{B}}(k)$ と異なり，“攻撃者”$\mathcal{A}$ は暗号文 c を観測しながら，$f(m)$ を推定することが許されていることが分かる．したがって，たとえば，$\mathcal{A}$ が c から m を求められるのであれば，「まぐれあたり」よりも有意に高い確率で $f(m)$ の推定に成功することも可能である．一方，上記と同様の操作を，別のPPTA $\mathcal{B}$ が，m の暗号文 c を観測せずに行う試行 $\mathbf{Exp}^{ss-0}_{\Pi,\mathcal{B}}(k)$ は次のように定義できる：

$\mathbf{Exp}^{ss-0}_{\Pi,\mathcal{B}}(k)$
　$(sk, pk) \leftarrow \mathrm{GEN}(1^k)$;
　$(X,$ 状態情報 $s) \leftarrow \mathcal{B}($ 選択モード $, pk)$;
　m を X からランダムに選択；
　$(v, f) \leftarrow \mathcal{B}($ 推定モード $, pk, s)$;
　$v = f(m)$ ならば $d \leftarrow 1$;
　$v \neq f(m)$ ならば $d \leftarrow 0$;
　return d.

ここで，d として値1が出力されれば，“模倣者”$\mathcal{B}$ は m の部分情報の推定に成功したものと考えられるが，そもそも $\mathcal{B}$ は，m の暗号文を観測していないため，仮に無限の計算能力を有していたとしても「まぐれあたり」程度の確率でしか推定に成功することはできない（ただし，X と f を上手に選べば $f(m)$ の取り得る値はいくらでも制限することはできる）．

このとき，任意の“攻撃者”$\mathcal{A}$ に対して，ある“模倣者”$\mathcal{B}$ が存在し，上記の両試行において推定の成功確率に有意な差が生じない場合，公開鍵暗号方式 Π においては，暗号文 c が $f(m)$ の推定にまったく寄与していないということができる．すなわち，そのような場合，c から平文 m に関する一切の部分情報が漏れていないと考えることができる．そのような安全性の概念を**強秘匿性**という．

定義1　任意のPPTA $\mathcal{A}$ に対して，あるPPTA $\mathcal{B}$ が存在し，Π=(GEN, ENC, DEC) が次式を満足するとき，Π は**強秘匿**であるという．

$$\left|\Pr\left[\mathbf{Exp}^{ss-1}_{\Pi,\mathcal{A}}(k)=1\right]-\Pr\left[\mathbf{Exp}^{ss-0}_{\Pi,\mathcal{B}}=1\right]\right|<\epsilon(k)$$

ここで，ϵ は k に対して無視できる値を表す関数とする（直観的には，「ほぼゼロ」と考えておけば特に問題ないものと思われる）．

上記のような暗号方式の安全性の定式化は，GoldwasserとMicaliによって初めてなされ，これを含む一連の成果によって，2012年に両氏は**Turing賞**を受賞している．

強秘匿性は，平文の部分情報の漏洩に関する安全性の要件を分かりやすく表現しているが，その一方で，具体的な公開鍵暗号方式について，それが強秘匿性を満足しているか判定するのがあまり容易でない．そのため，安全性の解析の際は，強秘匿性と等価な概念である**識別不可能性**を用いて議論がなされることがほとんどである．

定義2　任意のPPTA $\mathcal{A}$ に対して，Π=(GEN, ENC, DEC) が次式を満足するとき，Π は**識別不可能**であるという．

$$\left|\Pr\left[\mathbf{Exp}^{ind-1}_{\Pi,\mathcal{A}}(k)=1\right]-\Pr\left[\mathbf{Exp}^{ind-0}_{\Pi,\mathcal{A}}=1\right]\right|<\epsilon(k)$$

ここで，ϵ は上記と同様とし，また，$\mathbf{Exp}^{ind-b}_{\Pi,\mathcal{A}}(k)$ は，

$b \in \{0, 1\}$ に対し，次のように定義される試行とする：

$\mathbf{Exp}^{ind-b}_{\Pi,\mathcal{A}}(k)$

$(sk, pk) \leftarrow \mathrm{GEN}(1^k)$;

$(m_0, m_1,$ 状態情報 $s) \leftarrow \mathcal{A}($ 選択モード$, pk)$;

$c \leftarrow \mathrm{ENC}(m_b, pk)$;

$b' \leftarrow \mathcal{A}($ 推定モード$, c, pk, s)$;

return b'.

識別不可能性とは，“攻撃者”$\mathcal{A}$ に自由に 2 つで 1 組の平文候補 (m_0, m_1) を選ばせた上で，そのどちらかの暗号文を $\mathcal{A}$ に与えたとき，いかなる $\mathcal{A}$ も，暗号化された平文がどちらであったかを 1/2 よりも有意に高い確率で言い当てることができないような安全性を指す．このような安全性の概念の実用上の意味合いは，一見して理解することは困難であるが，上述のとおり，識別不可能性と強秘匿性は等価な概念であることが証明されている．また，識別不可能性は強秘匿性と比べ，安全性の証明を行いやすい定義となっている．そのため，以下においては識別不可能性の定義を用いて説明を進めるものとする．

安全性の証明技法

ここでは，ある与えられた公開鍵暗号方式 Π について，それが上記の安全性の要件を満足することを証明するための技法について説明を行う．ここで，ある特定の攻撃者ではなく，「任意」の攻撃者に対して上記の条件を満たす必要があることに気を付けなければならない．本章では，特に，そのような網羅的な議論をどのように行うのかについて説明を試みる．

上記のとおり，想定し得る最も強力と思われる攻撃者を想定し，その攻撃者をもってしても一切の部分解読を行うことができないことを示したとしても，強秘匿性（＝識別不可能性）を持つことを証明したことにはならない．そのため，背理法を用いることで，もしも公開鍵暗号方式 Π の識別不可能性を破ることができるような攻撃者が存在するとしたら，その攻撃者を用いて，なんらかの矛盾した状況が生じることを示す手法がとられることになる．また，そのような矛盾した状況として，「本来解けないはずの数学的問題が解けてしまう」場合がしばしば採用されている．このような矛盾が確認された際は，背理法により，「Π の識別不可能性を破ることができるような攻撃者が存在する」という仮定が誤っていたものと断定することができる．すなわち，いかなる攻撃者であっても，Π の識別不可能性を破ることができないことを証明したことになる．以下においては，実際にこの技法により，具体的な公開鍵暗号方式について，安全性証明の流れを説明する．

ElGamal 暗号とその安全性証明

安全性証明の説明に用いる具体的な公開鍵暗号として，ここでは ElGamal 暗号を紹介する．ElGamal 暗号はある種の巡回群上において構成される暗号方式であるが，巡回群に馴染みがない読者は，単に，「乗算と除算を定義可能な有限集合」と解釈すればそれほど問題ない．

ElGamal 暗号

GEN：入力 1^k に対し，$\log_2 p \geq k$ となるような素数位数 p を持つ巡回群 G を所定の手続きにより選択する．次に，$g \in G$, $x \in \{1, ..., p\}$ をランダムに選択し，$y = g^x$ を計算する．復号鍵，公開鍵のペアとして次のように (sk, pk) を出力する：

$$sk = x, \quad pk = (y, g)$$

ENC：平文 $m \in G$ および公開鍵 pk に対し，$r \in \{1, ..., p\}$ をランダムに選択し，さらに，次式により暗号文 c を得る：

$$c_1 = g^r$$
$$c_2 = m \cdot y^r$$
$$c = (c_1, c_2)$$

DEC：暗号文 $c(= (c_1, c_2))$ および復号鍵 sk に対し，次式により復号を行う：

$$m = c_2 \cdot {c_1}^{-x}$$

ElGamal 暗号は，巡回群 G を適切に選択することで強秘匿性を満足するものと考えられている．特に，実用上，k=160（もしくは 256）がよく用いられているが，このような典型的なパラメータ設定に関して，下記の Diffie-Hellman 判定問題が困難と考えられている巡回群 G が知られており，それがしばしば利用されている．

定義 3(Diffie-Hellman 判定問題)確率 1/2 で均等に,(i) G からランダムな元 g と,$\{1, ..., p\}$ から 3 つのランダムな値 α, β, γ を選び,$(g_1, g_2, g_3, g_4)=(g, g^{\alpha}, g^{\beta}, g^{\gamma})$ を求める,もしくは,(ii)G からランダムな元 g と,$\{1, ..., p\}$ から 2 つのランダムな値 α, β, を選び,$(g_1, g_2, g_3, g_4)=(g, g^{\alpha}, g^{\beta}, g^{\alpha\beta})$ を求める.この手続きにより,生成された (g_1, g_2, g_3, g_4) が与えられたとき,上記 (i) と (ii) のいずれの処理により生成されたものであるかを判定する問題を G における **Diffie-Hellman 判定問題**という.

Diffie-Hellman 判定問題は,デタラメに推定したとしても 1/2 の確率で正しく解くことができる.しかし,鍵長 k に応じて適切な G を選ぶことで,1/2 よりも有意に高い確率で Diffie-Hellman 判定問題を解く方法が知られていないような G が存在している.そのような G の上で ElGamal 暗号を構成することで,強秘匿性が数学的に証明可能となる.具体的には,次の定理が成立することが知られている.

定理 1　任意の PPTA に関して,G における Diffie-Hellman 判定問題が高々 $1/2+\epsilon(k)$ の確率でしか正解できないとき,ElGamal 暗号は強秘匿性を満たす.

この証明は,上述のとおり,ElGamal 暗号の安全性を破る攻撃者の存在を仮定し,それを用いて Diffie-Hellman 判定問題を 1/2 よりも有意に高い確率で正解するアルゴリズムを構成することで行われる.また,その際,強秘匿性そのものではなく,等価な概念である識別不可能性の定義を用いて証明を行う.より具体的には,ElGamal 暗号の識別不可能性を破るアルゴリズム $\mathcal{A}$ をサブルーチンとして,G における Diffie-Hellman 判定問題を 1/2 よりも有意に高い確率で正解するアルゴリズム $\mathcal{B}^{\mathcal{A}}$ を構成することで証明する.

Diffie-Hellman 判定問題アルゴリズム $\mathcal{B}^{\mathcal{A}}$

入力: (g_1, g_2, g_3, g_4)

出力: $z \in \{(i), (ii)\}$

1. $pk \leftarrow (g_2, g_1)$
2. $(m_0, m_1,$ 状態情報 $s) \leftarrow \mathcal{A}($ 選択モード , $pk)$
3. ランダムビット b を選ぶ
4. $c \leftarrow (g_3, m_b \cdot g_4)$
5. $b' \leftarrow \mathcal{A}($ 推定モード , $c, pk, s)$
6. $z \leftarrow$ "(i)" ($b' \neq b$ のとき) もしくは "(ii)" ($b' = b$ のとき)

ここで,出力値 (i) (もしくは,(ii)) は,(g_1, g_2, g_3, g_4) が (i) の処理によって (もしくは, (ii) の処理によって) 生成されたことを意味する.

次に,アルゴリズム $\mathcal{B}^{\mathcal{A}}$ が 1/2 より有意に高い確率で Diffie-Hellman 判定問題を正解できていることを確認することで証明が完了する.まず,(g_1, g_2, g_3, g_4) が (i) の処理によって生成されていた場合, $c=(g_3, m_b \cdot g_4)$ であり,ランダムな値である g_4 が m_b を完全に隠匿しているため, $\mathcal{A}$ の視点からは b に関する情報が情報理論的に消失してしまっていることが分かる.したがって, $\mathcal{B}^{\mathcal{A}}$ は均等に 1/2 の確率で (i) もしくは (ii) を出力することになる.一方,(g_1, g_2, g_3, g_4) が (ii) の処理によって生成されていた場合, $\mathcal{A}$ の視点からは,ElGamal 暗号における識別不可能性を破る際とまったく同一の入力が与えられているので,1/2 より有意に高い確率で b の正しい推定に成功する.すなわち, $\mathcal{B}^{\mathcal{A}}$ は 1/2 よりも有意に高い確率で (ii) を出力する.これらの議論を整理すると,次のことが言える.

- (g_1, g_2, g_3, g_4) が (i) の処理によって生成されていた場合,$\mathcal{B}^{\mathcal{A}}$ は 1/2 の確率で正解する.
- (g_1, g_2, g_3, g_4) が (ii) の処理によって生成されていた場合,$\mathcal{B}^{\mathcal{A}}$ は 1/2 より有意に高い確率で正解する.

したがって,全体として $\mathcal{B}^{\mathcal{A}}$ は 1/2 よりも有意に高い確率で Diffie-Hellman 判定問題に正解できていることが分かる.これは,「任意の PPTA に関して, G における Diffie-Hellman 判定問題が高々 $1/2+\epsilon(k)$ の確率でしか正解できない」という前提と矛盾しており,よって,「ElGamal 暗号の識別不可能性を破るアルゴリズム $\mathcal{A}$ が存在する」という仮定が誤りであったと言え,上記定理が真であると証明できる.

(2015 年 2 月 28 日受付)

花岡悟一郎 ■ hanaoka-goichiro@aist.go.jp

1997 年東京大学工学部卒業,2002 年同大学院工学系研究科電子情報工学専攻博士課程修了 (博士 (工学)).現在,産総研次世代暗号研究グループ長.英国計算機学会 The Wilkes Award (2007 年),電子情報通信学会論文賞 (2008 年) 等受賞.