数理解析研究所講究録
第381巻 1980年 52-72

52

公開鍵暗号系の安全性保証の難しさ

大阪大 基礎工 情報 嵩 忠雄
神戸商船大 輸送科学 山村 三朗

あらまし
1. でランダム多項式時間計算可能な関数のクラスと、他のクラスとの関係を整理した。2. では公開鍵方式の暗号系とディジタル署名に共通な枠組として、公開鍵系を導入し、安全性の上界を議論した。3. では公開鍵系によるディジタル署名の方法を示し、4. では公開鍵系を用いた暗号系を示し、そのために公開鍵系が満たすべき条件を与えた。5. では、これらの適用における安全性の下界問題を定式化し、1. と2. の結果を利用して、安全性保証の難しさを示した。これらは、異る文脈で述べられていたいくつかの事柄を定式化し、整理統合し、一部を拡張したものである。

1. ランダム多項式時間計算可能な関数のクラス

Σを記号T, Fを含む有限な記号集合, Σ^*を空系列Λを含むΣの上のすべての有限長系列の集合とし、系列xの長さを

$|x|$と書く。Σ^*からΣ^*への関数のクラスP^*, NP^*を文献(2)に従って、それぞれ次の条件を満たすような関数f全体の集合として定義する。

P^*：決定性テューリング機械と多項式tがあって、任意の入力$x \in \Sigma^*$に対して、$t(|x|)$以下のステップ数で$f(x)$を出力して停止する。

NP^*：非決定性テューリング機械Mと多項式tとがあって、Mは任意の入力$x \in \Sigma^*$に対して、ステップ数$t(|x|)$以下で$f(x)$を出力し、停止するような計算パスが少くとも一つある。

以下、テューリング機械の入力はΣ^*の元、出力はΣ^*の元か特殊記号ϕ（$\phi \notin \Sigma$）とする。非決定性テューリング機械の有限長の計算パスに、次のように'確率'を割当てる。与えられた入力に対し、一つの状態においてm個の動作が可能なとき、各動作をとる'確率'はそれ以前の状態とは独立に$1/m$とする。停止して出力yを残すすべての計算パスの確率和を、テューリング機械がyを出力する確率と呼ぶ。出力ϕは計算が失敗したことを示すと解釈し、ϕを出力する確率を問題の入力に関する失敗率と呼ぶ。

$D \subseteq \Sigma^*$, fを$\Sigma^* \to \Sigma^*$の関数とする。非決定性テューリング機械Mが、任意の入力$x \in D$に対して、(1)入力長$|x|$のあ

る多項式オーダのステップ数以内で必ず停止し、(2) $f(x)$ を出力する確率が ρ 以上であり、(3) ϕ を出力する確率が φ 以下であり、(4) ϕ でも $f(x)$ でもない系列を出力する確率が ε 以下であるとき、MはDの上で f を多項式時間内に、正解率 ρ 以上、失敗率 φ 以下，誤り率 ε 以下で計算するという。

ここで、Σ^* から Σ^* への関数のクラス RP^*, $PP^*(\rho)$（ただし、$1/2 < \rho \leq 1$）をそれぞれ次の条件を満たすような関数 f 全体のクラスとして定義する。

RP^*：ある $0 \leq \varphi < 1$ と非決定性テューリング機械Mがあって、Mは f を Σ^* の上で多項式時間内に、失敗率 φ 以下、誤り率0（従って、正解 $1-\varphi$ 以上）で計算する。

注意1：r を多項式とし、上のMにおいて、ϕ を出力して停止する代りに、$r(|x|)$ 回数までは、初期状態にもどって再計算するように変更することによって、失敗率を $\varphi^{r(|x|)}$ 以下に下げ、正解率を $1-\varphi^{r(|x|)}$ 以上に上げることができる。

$PP^*(\rho)$：f を Σ^* の上で多項式時間内に正解率 ρ 以上で計算する非決定性テューリング機械が存在する†。

---

† 文献(14)の *polynomial bounded probabilistic Turing machines with bounded error probability* によって計算される関数のクラスと一致する。

定義から、

$$P^* \subseteq RP^* \subseteq NP^* \qquad (1)$$

また $1/2 < \varepsilon < \varepsilon' \leq 1$ なら $PP^*(\varepsilon) \subseteq PP^*(\varepsilon')$ であり、注意1から、任意の $1/2 < \varepsilon < 1$ に対して

$$RP^* \subseteq PP^*(\varepsilon) \qquad (2)$$

なお、Σ^* の部分集合Dから Σ^* への関数 f に対しても、f を含むある全域関数が上述のクラスに属するとき、f 自身もそのクラスに属するという。

Σ^* の部分集合のクラスP、NP、co-NPを通常通り定義する(1)。また、Σ^* の部分集合のクラスRP、co-RPを文献(3)の'randomly decidable sets' Rの定義を若干変更して†、それぞれ次の条件RP、co-RPを満たすような部分集合L全体の集合として定義する。

RP：非決定性チューリング機械Mと多項式 t と数 φ（ただし、$0 \leq \varphi < 1$）があって、Mは任意の x に対して、必ずステップ数 $t(|x|)$ 以下で停止し、$x \in L$ のとき、ϕ または T を出力し、失敗率は φ 以下であり、$x \notin L$ のときは ϕ を出力する。

co-RP：$\Sigma^* - L \in RP$、

定義から、

$$RP \subseteq NP,\ co\text{-}RP \subseteq co\text{-}NP \qquad (3)$$

---

† 文献(3)では、出力 ϕ の代りに停止しないとしている。

$$P \subseteq RP \cap co\text{-}RP \qquad (4)$$

例1[3]：すべての素数からなる集合 $\in co\text{-}RP \cap NP$。

$D \subseteq \Sigma^*$ に対し、Σ^* の上の述語 $g_0(x) \triangleq x \in D$ を考え†便宜上、上記の部分集合のクラスを $\Sigma^* \to \{T, F\}$ の関数のクラスともみなす。このとき、定義から、

$$RP \cap co\text{-}RP \subseteq RP^*, NP \cap co\text{-}NP \subseteq NP^* \qquad (5)$$

(5)の逆がある意味で成立する。関数 f_1 が関数 f_2 に 'polynomical time Turing reducible'[1] であるとき、$f_1 \propto_T f_2$ と書く。$f_1 \propto_T f_2$ かつ $f_2 \in Q$（Q は関数のクラス）であるとき、f_1 は<u>Q-容易</u>であるという。[1] クラス Q_1 のすべての関数が Q_2-容易であるとき、$Q_1 \leq_T Q_2$ と書く。次の関係が知られている。[2]

$$NP^* \leq_T NP \cap co\text{-}NP \qquad (6)$$

(6)に対応して、次の命題が示される。

<u>命題1</u>：$RP^* \leq_T RP \cap co\text{-}RP$

（略証）式(6)に対する文献[2]の証明同様、2分法を利用する。Σ^* の系列間にアルファベット順 $\leq_A$（長さが短い方がより小さいとする）を導入する。$f \in RP^*$ に対し、$(\Sigma^*)^2$ の上の述語 $g_f(x, y) \triangleq f(x) <_A y$ を考える。適当に符号化し、$(\Sigma^*)^2$ の元を Σ^* の元で表わすと、$g_f \in RP \cap co\text{-}RP$.

† $\triangleq$ は、左辺を右辺に等しいとして定義することを表わす。

$f(x)$ の計算を2分法で g_f を使って行うには、最悪 $|x|$ に比例する個数の異る y に対し、'oracle' テューリング機械(1)で 'g_f の計算ルーチン' を呼ぶ必要がある。一回の g_f の計算での失敗率を $c_1/|x|$ (c_1 は適当な定数) 以下にする必要があるが、入力長 $|x|$ に対し、注意1で述べた繰り返し回数を、例えば $|x|$ に比例するように選べばよい。

命題2：$f_1 \propto_T f_2$, $f_2 \in RP \cup co\text{-}RP$ ならば、任意の $1/2 < \gamma < 1$ に対して、

$$f_1 \in PP^*(\gamma)$$

系2：任意の $1/2 < \gamma < 1$ に対し、

$$RP \cup co\text{-}RP \subseteq PP^*(\gamma)$$

(系の略証) $f_2 \in RP$ ($co\text{-}RP$ でも同様) とする。RP の定義における非決定性テューリング機械Mについて、注意1で述べた変更を行い、失敗率を $1-\gamma$ 以下にした後、出力 ϕ を出力Tで置き換えると、$f_2(x)=T$ である入力 x に対する正解率は γ 以上、また $f_2(x)=F$ である入力に対しては正解率1。

(命題2の略証) f_1 を計算する 'oracle' テューリング機械において、$f_2(x)$ を計算するルーチンが呼ばれる回数は、$|x|$ の多項式オーダである。従って命題1の略証で述べたと同様に、$f_2(x)$ を計算するルーチンの失敗率を注意1に従

って変更すればよい。

例2(12)：例1と系2から、任意の$1/2<\gamma<1$に対して、素数か否かの判定問題$\in PP^*(\gamma)$。

2．公開鍵系

有限な記号集号Σの上の公開鍵系を次のような関数の3字組(p, g, f)と定義する。

(1) $P: (\Sigma^*)^2 \to \{T, F\}$

(2) $g: K \times (\Sigma^*)^2 \to \{T, F\}$

ただし、$K \triangleq \{k \mid \exists h [p(k, h) = T]\}$

(3) $f: \{(k, h, x) \mid k \in K, h \in H(k), x \in X(k)\} \to \Sigma^*$

ただし、$k \in \Sigma^*$に対して

$H(k) \triangleq \{h \mid p(k, h) = T\}$

$X(k) \triangleq \{x \mid \exists y [g(k, x, y) = T]\}$

(4) すべての$k \in K$に対して、$X(k)$は空でない。

(5) すべての$k \in K$, $h \in H(k)$, $x \in X(k)$に対して、

$g(k, x, f(k, h, x)) = T$

Kの元を公開鍵，$H(k)$の元をkに関連する秘密鍵と呼ぶ。次の問題を公開鍵系(p, g, f)の解読問題と呼ぶ。

解読問題：任意に与えられた$k \in K$, $x \in X(k)$に対して、$g(k, x, y) = T$を満たすyを一つ求めよ。

任意の$k \in K$, $x \in X(k)$に対して、

$$f(k, x, f(k,x)) = T \qquad (7)$$

を満たす関数 f を解読関数という。公開鍵系は解読問題がより複雑である程、より安全であるという。また、任意の $k \in K$ に対し、$x \in H(k)$ を一つ求める問題を秘密鍵を求める問題という。以下、これらの問題の複雑さ†を考える。次の命題の後半は文献(11)の結果を若干整理拡張したものである。

命題3：r を $(\Sigma^*)^2$ の上の述語とし、$x \in \Sigma^*$ に対し、$Y(x) \triangleq \{y \mid r(x,y)=T\}$, $X \triangleq \{x \mid Y(x) \neq$ 空集合$\}$ とおく。もし、

(1) $r \in NP$、

(2) ある多項式 l があって、任意の $x \in X$ に対し、集合 $Y_l(x) \triangleq \{y \mid y \in Y, |y| \leq l(|x|)\}$ は空でない、

ならば、$\Sigma^* \to \Sigma^*$ の関数 f で、任意の $x \in X$ に対し、

$$r(x, f(x)) = T \qquad (8)$$

を満たし、NP－容易である関数 f が存在する。

さらに、

(3) ある多項式 m があって、任意の $x \in \Sigma^*$ に対して、$|Y_l(x)| \leq m(|x|)$, かつ

---

† NP, NP*, ・・・などを、記号集合 $\Sigma \cup \{',', '\}$ の上で考えるか、適当な符号変換を行って、二つ以上の記号を含む記号集合の上で考える。

(4) 任意の $0 \leq n \leq m(|x|)$ に対して、述語 $\#(x,n) \triangleq |Y_\ell(x)| > n$ が co-NP に属する$^+$

とき、上の式(8)を満たす NP ∩ co-NP − 容易な関数 g が存在する。

(略証) $x \notin X$ に対して $g(x) = \Lambda$, $x \in X$ に対して、$g(x)$ は $Y(x)$ のアルファベットと長さ順 $\leq_A$ での最小系列とする。$(\Sigma^*)^2$ の上の述語 $b(x,z) \triangleq \exists y \in Y(x)[y <_A z]$ を考えると、条件(2)と2分法で、$g \propto_T b$。条件(1)が成立すれば、$b \in NP$。さらに、条件(3), (4)が成立すれば、$b \in NP^*$ であることが、下記のような非決定性チューリング機械Mが存在することにより示され、$\propto_T$ の推移律と式(6)から後半が成立する。Mの作り方の方針：$z = \Lambda$ なら、$b(x,z) = F$。$x \in \Sigma^*$, $z \in \Sigma^* - \{\Lambda\}$ に対し、1) $\#(x,0) = F$ なら、停止して F を出力し、それとは平行に 2) $Y_\ell(x)$ の元を探す。そのような元 y_1 が一つ求まれば、$y_1 <_A z$ なら停止して、T を出力する。$y_1 \geq_A z$ であるとき、2.1) $\#(x,1) = F$ なら、停止して F を出力する。2.1) とは平行に、2.2) $Y_\ell(x) - \{y_1\}$ の元を探す。このようなことを

$^+$ 有限集合 A に対して、$|A|$ は A の元の個数を表わす。また、非負数 n は長さ $\ell(|x|)$ 以下の Σ の系列として表わされるとする。

繰り返すと、高々$m(|x|)$回の繰り返しで、停止してTまたはFを出力する計算パスが存在する。

この命題から直ちに次の系が得られる。

系3：(p, g, f)を公開鍵系とし、$k, x \in \Sigma^*$に対し、$Y(k,x) \triangleq \{y \mid g(k,x,y) = T\}$, $KX \triangleq \{(k,x) \mid Y(k,x) \neq$ 空集合$\}$とおく。もし

(1) $g \in NP$,

(2) ある多項式l_Yが求まって、任意の$(k,x) \in KX$に対し、$|y| \leq l_Y(|k|+|x|)$であるような$y \in Y(k,x)$が存在する、

ならば、NP-容易な解読関数が求まる[†]。さらに、

(3) 任意の$(k,x) \in KX$に対し、$Y(k,x)$は一つの元のみからなる、

(4) $KX \in co\text{-}NP$,

も成立すれば、$NP \cap co\text{-}NP$-容易な解読関数が求まる。

また、次の命題も成立する。

命題4：公開鍵系(p, g, f)において、もし

(1) $p \in NP$

(2) ある多項式l_Hが求まって、任意の$k \in K$に対して、

---

† 求まるとは、それを実現する'oracle'チューリング機械が構成できるの意味

$|h| \leq l_H(|k|)$であるような$h \in H(k)$が存在する

ならば、任意の公開鍵$k \in K$に対して、関連する秘密鍵を与えるNP-容易な関数が求まる。さらに、

(3) fがNP-容易

ならば、NP-容易な解読関数が求まる。

さらに、上の条件(3)の代りに

(3') $f \in NP^*$

が成立し、

(4) 任意の$k \in K$, $h, h' \in H(k)$, $x \in X(k)$に対して、
$f(k, h, x) = f(k, h', x)$

(5) $K \in$ co-NP、

も成立すれば、NP∩co-NP-容易な解読関数が求まる。

(略証)前半は命題3の系である。条件(1),(2),(3'),(4),(5)が成立するとする。条件(1),(2),(5)から、$(k, x) \in (\Sigma^*)^2$を入力とし、$|k|$の多項式オーダのステップ数をもって$k \notin K$なら、少くとも一つの計算パスで$\Sigma \cup \{\phi\}$に含まれない特殊記号ωを出力し、$k \in K$なら一つ以上の計算パスで$|h| \leq l_H(|k|)$かつ$h \in H(k)$であるようなhを出力する非決定性チューリング機械M_1が作れる。条件(3')から、k, xとM_1の出力zを入力とし、$|k|+|x|+|z|$の多項式オーダのステップ数をもって、$z = \phi$ならϕを、$z = \omega$なら

入を、それ以外は$f(k, \Sigma, \chi)$を出力する非決定性チューリング機械M_2を作ることができる。M_1とM_2を縦続接続したものは、条件(4)から与えられた入力に対し、ϕ以外の出力は同一であり、一つの解読関数を実現している。

3. 公開鍵系によるディジタル署名

公開鍵系(p, g, f)と、正整数$\underline{n} \leq \bar{n}$について、

(K) 無作為に$p(k, e) = T$, $\underline{n} \leq |k| \leq \bar{n}$であるような$k, e$を求める実用的手続き†$AK$

と、$k \in K_{\underline{n}}^{\bar{n}}$について($K_{\underline{n}}^{\bar{n}} \triangleq \{k \mid \underline{n} \leq |k| \leq \bar{n}, k \in K\}$)、

(Q) gを計算する実用的手続きAQ、

(F) fを計算する実用的手続きAF、

が与えられ、一方、

(CA) 解読問題を解くことは、ほとんど全ての$k \in K_{\underline{n}}^{\bar{n}}$、$\chi \in X(k)$に対して、計算量が過大で実際上不可能であるとする。

通信文はΣの上の系列とする。各$k \in K_{\underline{n}}^{\bar{n}}$に対して、$\Sigma$の上の系列を適当な長さで区切り、発信人の識別子、日付け、通し番号、必要なら乱数系列などを付け加え、$X(k)$の元に変換する実用的な方法が与えられているとする。ただし、こ

† 以下、'手続き'は一般に乱数発生の機能を持つ計算機のプログラムとして表されるものを意味している。

の変換は単射であるとする。全射でなくてもよいが、$X(k)$の上へほぼ'均等'に(解読問題が易しいような部分集合に集中しないように)写像されるとする。以下この変換を省略し、$X(k)$の元を平文と呼ぶ。

ディジタル署名の方法

(S1) 手続きAKで無作為に(k, κ)を選び、公開鍵kを、例えば公開ファイルに自己の識別子と共に登録し、κは秘密に保持する。

(S2) 発信者は送るべき平文mに対して、

$$(m, f(k, \kappa, m))$$

を送る。

(S3) ディジタル署名つき平文(m, s)が、偽造か否かの判定法は、mから発信者の識別子を知り、公開ファイルからその公開鍵kを求め、手続きAQを用い

$g(k, m, s) = T$なら、認証し、

$g(k, m, s) = F$なら、偽造

と判定する。

上の判定で偽造なら、明らかに偽造である(伝送上の誤りとか公開ファイルの管理上の手落ちは考えていない)。偽造でない方の判定は、もし問題の発信者が、問題の時点で発生し得る意味のある平文のなかに、解読問題の易しいものが含

まれる可能性を無視できるなら、正しい。

安全性

公開鍵 k と偽造したい平文 x に対して秘密鍵を知らずに、ディジタル署名を求めることは、公開鍵系 (p, g, f) の解読問題そのものである。条件 (K), (Q), (F) から、当然系3の条件 (1), (2) および命題4の条件 (1), (2), (3), (3′) が成立するとしてよい。

4. 公開鍵方式の暗号系

今までに提案されている公開鍵方式の暗号系[4~10]は次のような定式化に含まれる。

次の条件

(D) 任意の $k \in K$, $x \in X(k)$ に対して、$g(k, x, y) = T$ を満たす y がちょうど一つある、

を満たす公開鍵系 (p, g, f) と正整数 $n \leq r$ について、条件 (K), (F), (A) が成立し、(Q) の代りに

(E) 任意の $k \in K$ と $y \in Y(k)$ が与えられたとき、$g(k, x, y) = T$ を満たす x を一つ求める実用的手続きAE

が与えられるとする。

ディジタル署名と異り、$X(k)$ の代りに $Y(k) \equiv \{y \mid \exists x\ (g(k, x, y) = T\}$ の元を平文として（通信文から平文へ

の変換については同様）用いる。鍵の選択、登録については（S1）と同様。

暗号化法

受信者の公開鍵k_eを知り、暗号化すべき平文mに対して、手続きAEによって

$$g(k_e, c, m) = T$$

を満たす$c \in X(k_e)$を求める。cを暗号文と呼ぶ。

復号化法

公開鍵k_e，秘密鍵k_dをもつ受信者が暗号文cを受信したとき、手続きAFにより

$$m = f(k_d, k_e, c)$$

のように平文mが求まる（公開鍵の条件(5)と前述の条件(D)から上式が成立する）。

暗号の安全性

暗号解読（ここでは、盗聴した暗号文cと公開情報のみからもとの平文を求める問題，'ciphertext only attack'(*)を考える）の問題は、公開鍵系(p, g, f)の解読問題そのものである。系3と補題4はその複雑さの上界を与える。系3の条件(3)および命題4の条件(4)は、暗号系の条件(D)から自動的に成立する。また条件(K)，(F)，(E)から、系3の条件(1)，(2)，および命題4の条件(1)，(2)，(3)，(3')が成

立するとしてよい。問題なのは、系3の条件(4)と命題4の条件(5)である。Rivest-Shamir-Adleman[6]やRabin[8]の公開鍵系では、これらは成立しているが、Merkle-Hellman[5], Graham-Shamir[7]の公開鍵系では、成立しているか否か現在不明である。

暗号系へ適用できる公開鍵系は、条件(D)が要求されるので、一般的にいって、公開鍵系によるディジタル署名に比べて安全な系を求めるのがより困難であり、また安全の保証を与えることもそうである。

5. 安全性保証の難しさ

ディジタル署名とか暗号について、許容計算時間内に、例えば可能な入力のうちの1%に対して、正解率0.51以上で解読する手続きがあれば、普通安全とはいえない。従って、複雑さの尺度として最大複雑度とか平均複雑度は、適切ではない。

次に定義する百分位数複雑度は、文献(7)で導入されたものを、失敗率と誤り率を考慮して拡張したものである。fを$\Sigma^* \to \Sigma^*$の関数とする。

$0<\rho\leq 1$, $1/2<\gamma\leq 1$に対して、非決定性チューリング機械$M_{\rho,\gamma}$が存在して、各正整数nについて、長さnの入力系列のうち少くとも$100\times\rho\%$の入力系列に対して、必ずγ

ステップ数 $G(n, \rho, \gamma)$ 以下で停止して、確率 γ 以上で $f(x)$ を出力するとき、関数 f は百分位数複雑度 $G(n, \rho, \gamma)$ をもつという。このような百分位数複雑度については、合成数を法とする平方根を求める問題(8)以外ほとんどわかっていない。

安全性の問題を漸近的な性質のみで議論するために、

クラスI：どのように小さい $0 < \rho \leq 1$ と $1/2$ に近い $1/2 < \gamma \leq 1$ に対しても、入力系列長 n に関して多項式オーダであるような百分位数複雑度 $G(n, \rho, \gamma)$ を持たない $\Sigma^* \to \Sigma^*$ の関数からなるクラス

を導入する。定義から、任意の $1/2 < \gamma \leq 1$ について、$PP^*(\gamma)$, 従って RP^*, RP, co-RP と I とは共通元を持たない。

ディジタル署名あるいは暗号系に対する安全性の条件(CA)を

安全性の条件(CA')：すべての解読関数はクラスIに含まれる。

と定式化するのが自然であろう。また前述したように、ディジタル署名での条件(K), (Q), (F)を満たす最低限の漸近的条件として、系3の条件(1), (2)および命題4の条件(1), (2), (3')が成立するとしてよく、暗号系での条件(K), (F), (E), (D)を満たす最低限の漸近的条件として、系3の

条件(1), (2), (3) および命題4の条件(1), (2), (3'), (4) が成立するとしてよい。いずれにしても、解読関数はNP-容易であるから、このような公開鍵系のなかに、安全性の条件(CA')を満たすものが存在すれば、任意の $1/4 < \varepsilon \leq 1$ について、$PP^*(\varepsilon)$ と I が共通元をもたないこと、命題2および式(3)から、

$$P \subseteq RP \cup (co\text{-}RP \cap NP) \subsetneq NP \qquad (9)$$

が成立しなければならない。さらに、系3の条件(4)あるいは命題4の条件(5)と安全性の条件(CA')を満たす公開鍵系が存在すれば、その解読関数は、$NP \cap co\text{-}NP$-容易であるから、命題2と式(3)を用いて、

$$(RP \cap co\text{-}NP) \cup (co\text{-}RP \cap NP) \subsetneq NP \cap co\text{-}NP \qquad (10)$$

が成立し、また式(2), (5)から

$$RP^* \subsetneq NP^* \qquad (11)$$

も成立する。従って、安全性の保証は、(9)、(10)、(11)を証明すること(複雑さに関する理論の難問中の難問である)より易しくはない。

以上から、'相対的な'保証で満足すべきであろう。$\Sigma^* \to \Sigma^*$ の関数 f_1, f_2 について、$f_2 \notin I$ と仮定すれば、$f_1 \notin I$ が帰結されるとき、$f_1 \propto_I f_2$ と書くことにする。定義から、推移律を満たす。f_1 が f_2 に 'polynomial time transformable'(1)

なら、もちろん $f_1 \propto_I f_2$ であるが、$f_1 \propto_T f_2$ の場合はわからない。計算が複雑と考えられている典型的な関数 f_d を一つ選び（例えば、素因数分解$\in NP^*$[12]）、条件(CA')の代りに

安全性の相対的条件(CA'')：任意の解読関数 g について、

$f_d \propto_I g$

を考えるのが妥当であろう。Rabin[8]とWilliams[13]の公開鍵系について、f_d を素因数分解と選んだときの条件(CA'')が示されているが、それ以外公開鍵系では与えられていない。

本稿では、解読問題を一つのディジタル署名文あるいは、平文に対する問題として考えてきた。もし同一の鍵を制限なく繰返し使った場合、暗号文の十分長い系列から、平文系列を求める問題では、漸近的に線形時間で可能となり、漸近的な立場から議論するのは無意味である[14]。

謝辞

原稿について御助言いただいた、谷口健一助教授に感謝いたします。

参考文献

(1) Garey, M.R. and Johnson, D.S.:"Computers and intractability —— a guide to the theory of NP-completeness", W.H. Freeman & Co. (1979).

(2) Miller, G.E.:"Riemann's hypothesis and tests for primality", J. Comput. & Syst. Sci., 13, 3, p.300 (Dec. 1976).

(3) Adleman, L. and Manders, K.:"Reducibility, randomness, and intractability", Proc. The 9th Ann. ACM Symp. on Theory of Computing, p.151 (1977).

(4) Diffie, W. and Hellman, M.E.:"New directions in cryptography" IEEE Trans. Inf. Theory, 22, 6, p.644 (Nov. 1976).

(5) Hellman, M.E.:"The mathematics of public-Key cryptography", Scientific American, p.130 (Aug. 1979).

(6) Rivest, R.L., Shamir, A. and Adleman, L.:"A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM, 21, 2, p.120 (Feb. 1978).

(7) Shamir, A.:"On the cryptocomplexity of knapsack system", Proc. The 11th Ann. ACM Symp. on Theory of Computing, P.118 (1979).

(8) Rabin, M.O.:"Digitalized signatures and public-key functions as intractable as factorization", Tech. Rep. MIT/LCS/TR-212, MIT Lab. Comp. Sci., Cambridge, Mass. (Jan. 1979).

(9) Lempel, A.:"Cryptology in transition", Computing Surveys, 11, 4, p.285 (Dec. 1979).

(10) Simmons, J.S.:"Symmetric and asymmetric encryption", Computing Surveys, 11, 4, p.305 (Dec. 1979).

(11) Brassard, G.:"A note on the complexity of cryptograhpy", IEEE Trans. Inf. Theory, 25, p.232 (March 1979).

(12) Rabin, M.O.:"Probabilistic algorithms", Algorithms and Complexity, Recent Results and New Directions, edited by J.F. Traub, Academic Press, New York, p.21 (1976).

(13) Williams, H.C.:"A modification of the RSA public-key encryption procedure", Scientific Report #92, Dep. of Comp. Sci., Univ. of Manitoba, Winnipeg, Manitoba, Canada (July 1979).

(14) Brassard, G.:"Relativized cryptogram", Proc. The 20th Ann. Symp. on Foundations of Comp. Sci., p.383 (Oct. 1979).