数理解析研究所講究録
1093巻 1999年 162-167



# Unpredictability of Pseudorandom Number Generators on Public Key Cryptosystems with Random Inputs

通信・放送機構／横浜リサーチセンター　小柴 健史 (Takeshi Koshiba)

## 1 はじめに

現在のセキュリティ技術において乱数はごく自然なものとして利用されている．とくに，暗号系や署名系の中には乱数は不可欠な部品となっているものもある．公開鍵暗号系では，例えば，ElGamal 暗号 [8] は暗号化のときにランダム入力を利用している．乱数を用いる場合，暗号などの安全性を測るのに乱数生成法をも含めた安全性をも考慮するのは当然である．ElGamal 自身，同じ数を (短期間で) 生成するような乱数生成法を好ましくないとしている．しかしながら，多くの研究者は暗号の安全性を証明するのに際して乱数は理想的であるという仮定を置いている．暗号系が計算機上で動作する限りにおいては乱数生成法もアルゴリズム的であり，暗号系の安全性の評価は乱数生成法をも合わせてなされるべきであろう．

擬似乱数の性質と暗号の安全性は密接な関係にはがあるが，本稿において，乱数の予測困難性と暗号の安全性の関係を明らかにする．線形合同法については，[10, 4] の結果からその暗号学安全性が疑問視されている．が，それは共通暗号鍵などのスケジューリングやストリーム暗号に対してである．一方，公開鍵暗号系に対する結果としては，[1] において DSS 署名が線形合同法との組合せで安全でないことが示されている．著者の知る限りにおいて，その他の場合については証明がされてはいない．

さて現在，乱数と呼ばれているものをおおまかに分類すると，

1. モンテカルロシミュレーションなどに利用するもの，
2. 共通鍵暗号などの鍵生成などに利用する統計的にランダムとされているもの，
3. (一方向関数などを利用して) 乱数の種の計算問題を計算量的に困難であると評価したもの，

のようになる．1 の例としては線形合同法がある．線形合同法の利点としては最大周期を得るための性質などがよく分かっていることが挙げられる．例えば $Z_p$ 上の乱数が欲しい場合，線形合同法を用いると同一の数が出てくるまでの期間を最大周期 にすることが可能である．この性質は ElGamal 暗号には大変好ましいものである．2 の例はいろいろあるが，理論的な保証を与えないので本稿では考察の対象外とする．3 の例としては Shamir の手法 [16]，あるいは Blum-Micali[3], Blum-Blum-Shub[2], Patel[13] などの乱数ビット生成器がある。ただし，ランダムな数ではなくランダムなビットの生成器では効率面で問題がある．同様に，Yao の意味での擬似乱数生成器 [17] も効率面で問題がある．また，線形合同法のときのような最大周期性に関しては保証を与えることが難しい．本稿では，ランダムな入力を要求するような公開鍵暗号系にはどのような乱数がよいのかを議論する．

公開鍵暗号系のスキームについて復習してみる．今 $k_p$ を公開鍵，$k_s$ を秘密鍵，$r$ をランダム入力，$m$ を平文，$c$ を暗号文とすると，暗号化関数 $E$ と復号関数 $D$ は以下のように書き下せる．

$$c = E(k_p, m, r) \quad \text{and} \quad m = D(k_p, k_s, c).$$

これらの式から以下の関係式が成立する．

$$m = D(k_p, k_s, E(k_p, m, r)).$$

ここまでは公開鍵暗号系一般について言えることだが，ここで $k_s$ の役割を $k_p, k_s, r$ の関数 $R(k_p, k_s, r)$ が担えるとしよう．この $R$ のことをランダムトラップドア関数と呼ぶことにする．書き下すと

$$m = D'(k_p, E(k_p, m, r), R(k_p, k_s, r))$$

となる．この式が意味するのは，秘密情報 $k_s$ そのものが分からなくてもランダムトラップドア関数 $R$ の値が分かれば ($D'$ の計算も容易であるという条件の元で) 復号ができることを意味している．

今考える状況として $r$ の系列は理想的なランダム列ではなく，ある計算法によって生成されているとしよう．このとき，公開鍵暗号系において

$$(m_1, c_1, R(\cdot,\cdot,r_1)),\ (m_2, c_2, R(\cdot,\cdot,r_2)),\ \ldots,\ (m_i, c_i, R(\cdot,\cdot,r_i)) \text{ および } c_{i+1}$$

から $m_{i+1}$ を推測する，つまり $R(\cdot,\cdot,r_{i+1})$ を推測することが容易ならば安全とは言えないだろう．なお，$R$ の値が予測困難性は必ずしも暗号の安全性を保証しない．

少くとも言えることは，公開鍵暗号系において，その復号がランダムトラップドア関数 $R$ を用いて効率的に計算できるならば，$R$ の予測問題は困難である必要がある．

以下では，$r$ の系列が $r_{i+1}=f(r_i)$ のように帰納的関数 $f$ で表現できるとする．$f$ が $r_i$ から必ずしも効率的に計算できる必要はないが，$\{r_i\}$ そのものは効率よく計算できる必要がある．

本稿では，ランダムトラップドア関数で記述できる公開鍵暗号系において $f$ に関して安全であるための条件を与える．また，適用例として，ElGamal 暗号において，いくつかの乱数生成法に適用し，その生成法に関して安全でなくなってしまうことを示す．具体的には，乱数が線形合同法の場合，一方向関数的である離散対数問題を利用した場合など，について乱数生成法が原因となって解読されることを示す．また，ElGamal 暗号 において $R$ の予測問題を困難にする，つまり，乱数生成法に関して ElGamal 暗号が安全になるような生成法を提案する．

## 2 乱数生成

今，数列 $\{r_i\}$ において，帰納的関数 $f$ (以下，単に乱数関数と呼ぶ) によって $r_{i+1}=f(r_i)$ なる関係を満たすものとする．本稿を通じてこの仮定を置くものとする．$f$ は必ずしも多項式時間計算可能である必要がないが $\{r_i\}$ を効率的に生成する手法は存在するものとする．

## 3 公開鍵暗号系とランダムトラップドア関数

暗号の安全性はいくつかの平文 $m$ と暗号文 $c$ のペアが分かっているときに未知の暗号文に対応する平文を求めるのが困難か容易かによって測られる．ランダムトラップドア関数 $R$ で表記可能という条件の元では，$r$ そのものの値は分からないが $(m,c)$ から $R(r)$ が容易に計算されてしまうという前提に立った安全性を考えた方がよい．(ここで $R(r)$ という表記は $R(k_p,k_s,r)$ の略記であるが，本稿を通じて $k_p$ および $k_s$ を固定して考える)．

ランダムトラップドア関数 $R$ で表記可能な公開鍵暗号系として ElGamal 暗号を考えよう．まず ElGamal 暗号 [8] について簡単に説明する．

**鍵生成**：素数 $p$，生成元 $g\in Z_p^*$，$x\in Z_{p-1}$ を選択し，$y=g^x \bmod p$ とする．公開鍵は $\langle p,g,y\rangle$ で秘密鍵は $x$ である．

**暗号化**：まず，$r\in Z_{p-1}$ を一様ランダムに選択する．メッセージ $m$ に対して暗号化関数

$$E(\langle p,g,y\rangle,m,r)=(g^r \bmod p,\ y^r m \bmod p)$$

で暗号化する．

**復号**：受け取った暗号文 $(c_m,c_r)$ に対して復号関数

$$D(\langle p,g,y\rangle,x,c_m,c_r)=c_m/(c_r)^x \bmod p$$

で復号する．

ここで $g,p,g^x \bmod p$ から $x$ を求める問題は離散対数問題と呼ばれ，現在のところ効率的な計算法は知られていない．

ElGamal 暗号において $R(\langle p,g,y\rangle,x,r)=g^{rx}$ とすると，復号関数 $D()=c_m/R()$ という関係にあることが容易に確認できる．よって，ElGamal 暗号はランダムトラップドア関数で表記可能と言える．また，ElGamal 暗号の場合，一組の $(m,c)$ から $R(r)$ が容易に計算できる．

ElGamal 暗号の他にもランダムトラップドア関数で表記可能な暗号は存在する．楕円曲線を用いた暗号系はいくつかあるが，そのうち楕円 ElGamal 暗号と呼ばれるものや，従来の枠組では最も強い安全性の概念とされている non-malleability [7] や適応的選択暗号文攻撃 [14] に対する保証がある Cramer-Shoup 暗号 [5] もランダムトラップドア関数で表記可能である．また離散対数問題をベースにしない暗号系では，McEliece 暗号系 [11] がランダムトラップドア関数で表記可能である．

**Theorem 1** $(E,D)$ を公開鍵暗号系とし，$D$ がランダムトラップドア関数 $R$ で表記可能であるとする．今，乱数関数を $f$ とする．このとき $R\circ f\circ R^{-1}$ が効率的に計算可能ならば，公開鍵暗号系 $(E,D)$ は安全でない．

このことから言えることであるが，$f$ が一般に計算が困難だからといって $R\circ f\circ R^{-1}$ の計算が困難とは限らない．以下の章でいくつかの適用例を見ていくことする．

## 4 適用例

### 4.1 線形合同法

一般に広く用いられている乱数生成法として線形合同法がある．線形合同法は $r_i = ar_{i-1}+b \bmod m$ の形の数列 $\{r_i\}$ を生成する．ただし，$m$ は正整数で $a,b,s_0 \in Z_m$ とする．ここでは，最大周期性の条件など，線形合同法の様々な性質については言及しない．線形合同法の詳細については [9, 12] などの教科書を参照のこと．

線形合同法において，乱数関数 $f$ は $f(r_i) = ar_i + b \bmod n$ と書ける．ただし $n$ は生成元 $g$ の位数とする．ここで $R\circ f\circ R^{-1}(s) = s^a y^b$ なる関係がある．よって

**Corollary 2** *ElGamal* 暗号において乱数生成法が *(*法が $g$ の位数の*)* 線形合同法であるとする．パラメータが既知の場合は，次以降の暗号文の解読が容易である．

では，パラメータが未知の場合ではどうであろうか．このことを考えるのに幾つかの準備をする．

問題 DL は入力 $(g,p,y)$ に対して $\bmod p$ で $y = g^x$ なる $x$ を計算する問題，つまり離散対数問題．また，問題 DLLC は入力 $(g,p,y_1,y_2,y_3)$ に対して $\bmod p$ で $y_1 = g^r$，$y_2 = g^{ar+b}$，$y_3 = g^{a(ar+b)+b}$ なる $(a,b)$ を計算する問題．ただし，等号は $\bmod p$ での元での等号である．

ここで，いくつかの定義をする．関数 $f$ が関数 $f'$ に多項式時間関数的多対一帰着可能であるとは多項式時間計算可能関数 $h_1,h_2$ が存在して，任意の入力 $x$ について，$f(x) = h_2(f'(h_1(x)))$ が成立するときを言う．$\leq_m^{\mathrm{FP}}$ で多項式時間関数的多対一帰着を表す．また $f \leq_m^{\mathrm{FP}} f'$ かつ $f' \leq_m^{\mathrm{FP}} f$ のときは $f \equiv_m^{\mathrm{FP}} f'$ と表記する．

**Proposition 3** $\mathrm{DL} \equiv_m^{\mathrm{FP}} \mathrm{DLLC}$.

**Proof.** $\mathrm{DLLC} \leq_m^{\mathrm{FP}} \mathrm{DL}$ は明らか．$\mathrm{DL} \leq_m^{\mathrm{FP}} \mathrm{DLLC}$ を示そう．DLLC を解くアルゴリズムを $B(g,p,y_1,y_2,y_3)$ として，DL を解くアルゴリズム $A(g,p,y)$ を構成すればいい．$A$ の入力 $g,p,y$ に対して $B(g,p,y,y^3,y^7)$ を呼ぶ．その解を $(a,b)$ とする．$b$ を $A$ の出力とする．このアルゴリズムの正当性を検証しよう．$y = g^r$ とする．と，$ar+b = 3r$，$3ar+b = 7r$ が成立する．この連立方程式を解くと $a = 2, b = r$ が解であることが容易に分かり，$A$ は DL を解くアルゴリズムとなっている．□

この Proposition が意味することを考えてみよう．$R\circ f\circ R^{-1}(s) = s^a y^b = (g^x)^{ar+b}$ なので，今，仮に $g^x$ が $Z_p^*$ の生成元になったとき，連続する $R(r_i)$ と $R(r_{i+1})$ から乱数関数 (線形合同法) $f$ のパラメータを計算するのは離散対数問題を解くのと同じくらい難しいと言っている．もちろん，パラメータの計算を無くして $R(r_{i+1})$ の計算は可能かもしれないが，パラメータが未知にする場合は ElGamal 暗号に線形合同法を用いても急務の対策が必要な危険性はないかもしれない．

### 4.2 線形合同法で法が異なる場合

先の例において ElGamal 暗号における法を $p$ とし，また，乱数生成法の法を $p-1$ と仮定した．ElGamal 暗号は $Z_{p-1}$ 上の一様乱数を要求しているので，$p-1$ を法とする線形合同法を用いることは一つの簡単な実装ではある．ここではこの条件を緩和することを考える．今 $q > p-1$ と仮定し，乱数関数 $f$ が $f(r_i) = ar_i + b \bmod q$ と書けるとする．$Z_{p-1}$ 範囲の乱数が必要であるので，

$$t_i = \lfloor s_i(p-1)/q \rfloor$$

として計算する．この場合一様ではなくなるが，実際的にはほぼ一様なので問題はないとして利用している．ここで

$$\frac{q}{p-1}t_i \le r_i < \frac{q}{p-1}(t_i+1)$$

であり，$r_i$ は整数値なので $r_i$ の候補を $S_i$ とすると $S_i$ の要素数は高々 $q/(p-1)$ である．これらの各要素は

$$\frac{q}{p-1}t_i + c_j, \qquad j = 1, \ldots, |S_i|$$

と表現できる．よって $t_{i+1}$ の値は

$$\left\lfloor \left( (\frac{aq}{p-1}t_i + ac_j + b) \bmod q \right) \frac{p-1}{q} \right\rfloor, \qquad j = 1, \ldots, |S_i|$$

の中の一つである．これを $t(j)$ と置く．この値を計算すると

$$t(j) = at_i + \lfloor (ac_j + b)(p-1)/q \rfloor \bmod (p-1)$$

となる．また $c_j$ の値を正確に表現すると，

$$c_j = j - \frac{qt_i \bmod (p-1)}{p-1}, \qquad j = 1, \ldots, |S_i|$$

と書ける．これを代入すると，

$$t(j) = at_i + \left\lfloor \frac{1}{q} \Big( (aj+b)(p-1) - qt_i \bmod (p-1) \Big) \right\rfloor$$

と書ける．$p-1 < q$ を仮定しているので

$$t(j) = at_i + \lfloor (aj+b)(p-1)/q \rfloor \quad \text{or} \quad at_i + \lfloor (aj+b)(p-1)/q \rfloor - 1$$

が言える．よって，すべての $j$ について

$$g^{t_{i+1}} = g^{at_i + \lfloor (aj+b)(p-1)/q \rfloor} \quad \text{or} \quad g^{at_i + \lfloor (aj+b)(p-1)/q \rfloor - 1}$$

をチェックすることにより正しい $j$ と補正値 (指数の 0 または 1 のこと) を計算できる．

**Corollary 4** *ElGamal* 暗号において乱数生成法が *(*法が $q$ の位数の*)* 線形合同法であるとする．もし $q/p = O(poly(n))$ でパラメータが既知の場合は，次以降の暗号文の解読が容易である．

### 4.3 非線形な乱数関数

線形合同法の数列は線形であったが，ここでは非線形な例を考える．Blum-Micali[3] や Patel[13] において $s_{i+1} = g^{s_i}$ なる生成系を用いて，$s_i$ からあるビットを選ぶことにより擬似ランダムビット生成器を構成している．非線形な例として $r_{i+1} = g^{r_i}$ を考えたいが，簡単のために多少変形して $f(r_i) = (g^x)^{r_i}$ とする．このとき $R \circ f \circ R^{-1}(s) = (g^x)^s$ となる．

**Corollary 5** *ElGamal* 暗号において乱数関数が $f(r_i) = (g^x)^{r_i}$ であるとする．このとき，次以降の暗号文の解読が容易である．

## 5 乱数生成法の提案

ElGamal 暗号は離散対数問題をベースにした暗号系なので，離散対数問題をベースにした乱数生成法を考える．また ElGamal 暗号では $Z_{p-1}$ の乱数で同じ数が現れるまでの長さが極力大きいことが望まれる．その実現として $p-1$ を法とする線形合同法を直接利用する替りに以下のように間接的に利用することを考える．

---

Procedure GEN_RND
$s_i := as_{i-1} + b \bmod (p-1)$;
$r_i := (g^{s_i} \bmod p) - 1$;
output $r_i$;

---

GEN_RND で得られる数列 $\{r_i\}$ は $Z_{p-1}$ 上の乱数でなるべく周期が大きくなるようパラメータの調整をすることができる．このときの $R \circ f \circ R^{-1}$ の次の値の予測問題を考える．

まず，$\mathsf{EG}(p,g,Y,C_1,C_1)$ を，素数 $p$ と $g,Y,C_1,C_2 \in Z_p^*$ を入力として，$Y = g^x$ かつ $C_1 = g^r$，$C_2 = mg^{xr}$ を見たす $(m,x,r)$ が存在するならば，$m \in Z_p^*$ を計算する問題とする．この問題は ElGamal 暗号を直接解くことに対応している．$\mathsf{DH}(p,g,X,Y)$ を，素数 $p$ と $g,X,Y \in Z_p^*$ を入力として，$X = g^x$ かつ $Y = g^y$ を満たす $(x,y)$ が存在するならば $g^{xy}$ を計算する問題とする．この問題は Diffie-Hellman 問題 [6] と呼ばれている．$\mathsf{DHE}(p,g,X,Y)$ を，素数 $p$ と $g,X,Y \in Z_p^*$ を入力として，$X = g^x$ かつ $Y = g^y$ を満たす $(x,y)$ が存在するならば，$g^{x^y}$ を計算する問題とする．$\mathsf{DHE}^\star(p,g,X,Y)$ を，素数 $p$ と $g,X,Y \in Z_p^*$ を入力として，$X = g^x$ かつ $Y = g^y$ を満たす $(x,y)$ が存在するならば，$g^{x^y}$ を計算する，存在しなければ，特別な記号 "$\perp$" を出力する問題とする．$\mathsf{NXTR}(p,g,R,A,B)$ を，素数 $p$ と $g,R,A,B \in Z_p^*$ を入力として，$R = g^{g^r}$ かつ $A = g^a$，$B = g^b$ を満たす $(r,a,b)$ が存在するならば，$g^{g^{ar+b}}$ を計算する問題とする．この問題は ElGamal 暗号と乱数生成に GEN_RND を用いて，かつ，内部状態の更新に利用している線形合同法のパラメータが既知の場合の $R \circ f \circ R^{-1}$ の次の値の計算問題に対応している．

**Theorem 6** $\mathsf{EG} \equiv_m^{\mathrm{FP}} \mathsf{DH} \leq_m^{\mathrm{FP}} \mathsf{DHE}^\star$ かつ $\mathsf{DHE} \equiv_m^{\mathrm{FP}} \mathsf{NXTR} \leq_m^{\mathrm{FP}} \mathsf{DL}$.

**Proof.** まず $\mathsf{DH} \leq_m^{\mathrm{FP}} \mathsf{DHE}^\star$ を示す．$B(p,g,X,Y)$ を $\mathsf{DHE}^\star$ を解くアルゴリズムとする．このとき，DH を解くアルゴリズム $A(p,g,X,Y)$ を構成すればよい．アルゴリズム $A$ は以下のようになる．

---

Algorithm $A(p,g,X,Y)$ to solve DH
$z_1 := B(p,g^2,X,g^4)$;
$z_2 := B(p,g^2,Y,g^4)$;
**if** $z_1 \neq \perp$ and $z_2 \neq \perp$ **then** output $B(p,g^2,XY,g^4)/z_1z_2$ and halt;
**if** $z_1 = \perp$ and $z_2 \neq \perp$ **then** output $B(p,g^2,XYg,g^4)/B(p,g^2,Xg,g^4)z_2Y$ and halt;
**if** $z_1 \neq \perp$ and $z_2 = \perp$ **then** output $B(p,g^2,XYg,g^4)/B(p,g^2,Yg,g^4)z_1X$ and halt;
**if** $z_1 = \perp$ and $z_2 = \perp$ **then** output $B(p,g^2,XYg^2,g^4)/B(p,g^2,Xg,g^4)B(p,g^2,Yg,g^4)XYg$ and halt.

---

$p$ が偶素数のときは $z_1$ も $z_2$ も $\perp$ とはならない．このとき $z_1 = g^{x^2/2}$ かつ $z_2 = g^{y^2/2}$，$B(p,g^2,XY,g^4) = g^{(x+y)^2/2}$ なので，アルゴリズム $A$ は $g^{xy}$ を出力するので，$A$ は DH を正しく解いている．$p$ が奇素数のときは $g^2$ は $Z_p^*$ の生成元でないかもしれない．ここで 部分群 $G = \{g^i : i \text{ is even in } Z_{p-1}\}$ を考える．このとき $g^2$ は $G$ の生成元にはなる．アルゴリズム $A$ がアルゴリズム $B$ を呼ぶときに，アルゴリズム $A$ は 3 つめの引数が $G$ に属するように調整を加えている．場合分けは 4 通りになるが，$z_1 = \perp$ かつ $z_2 \neq \perp$ の場合だけを考えよう．他の場合も同様な議論ができる．ここで，$B(p,g^2,XYg,g^4) = g^{((x+1)+y)^2/2}$ かつ $B(p,g^2,Xg,g^4) = g^{(x+1)^2/2}$ が成立していることは容易に確かめられる．いずれの場合にしろ，アルゴリズム $A$ は $g^{xy}$ を出力するので，DH を解いていることになる．

次に $\mathsf{DHE} \leq_m^{\mathrm{FP}} \mathsf{NXTR}$ を示そう．$C(p,g,R,A,B)$ を NXTR を解くアルゴリズムとしよう．DHE を解くアルゴリズム $B(p,g,X,Y)$ を構成しさえすればよい．アルゴリズム $B$ は，まず $C(p,g,X,Y,1)$ を呼び，答えとして $w$ を得る．アルゴリズム $B$ は $w$ をそのまま $B$ の出力とする．ここで，$x = g^z$ を仮定しよう．このとき $w = g^{g^{zy}} = g^{(g^z)^y} = g^{x^y}$ であり，アルゴリズム $B$ は DHE を解いている．

最後に $\mathsf{NXTR} \leq_m^{\mathrm{FP}} \mathsf{DHE}$ を示そう．$B(p,g,X,Y)$ を DHE を解くアルゴリズムとする．NXTR を解くアルゴリズム $C(p,g,R,A,B)$ を構成すればよい．アルゴリズム $C$ はアルゴリズム $B(p,g,R,A)$ を呼び，答えとして $w$ を得る．さらに，$\mathsf{DH} \leq_m^{\mathrm{FP}} \mathsf{DHE}$ であるからアルゴリズム $C$ は $\mathsf{DH}(p,g,w,g^B)$ を解き，答えとして $w'$ を得ることができる．$w = g^{(g^r)^a} = g^{g^{ra}}$ および $w' = g^{g^{ra}g^b} = g^{g^{ra+b}}$ が成立することは容易に確認で

きる．このことからアルゴリズム $C$ は NXTR を解いている．

NXTR $\leq_m^{\mathrm{FP}}$ DL については明らかである．[15] で，EG $\equiv_m^{\mathrm{FP}}$ DH が証明されているので，これで証明は完了する．□

この定理から，ElGamal 暗号において GEN_RND を乱数生成法 (線形合同法のパラメータが既知でもよい) 利用すれば，乱数部分を切っ掛けにして解かれることはないと思われる．

## References


[1] M. Bellare, S. Goldwasser, and D. Micciancio. Pseudo-random number generation within cryptographic algorithms: The DSS case. In *Lecture Notes in Computer Science (CRYPTO'97)*, Vol. 1294, pp. 277–291. Springer-Verlag, 1997.

[2] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on Computing*, 15(2):364–383, 1986.

[3] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850–864, 1984.

[4] J. Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of the Association for Computing Machinery*, 36(1):129–141, 1989.

[5] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Lecture Notes in Computer Science (CRYPTO'98)*, Vol. 1462, pp. 13–25. Springer-Verlag, 1998.

[6] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[7] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pp. 542–552. ACM Press, 1991.

[8] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4):469–472, 1985.

[9] D. E. Knuth. *The Art of Computer Programing*, Vol. 2. Seminumerical Algorithms. Addison-Wesley, 3rd edition, 1998.

[10] H. Krawczyk. How to predict congruential generators. *Journal of Algorithms*, 13(4):527–545, 1992.

[11] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report 42-44, pp. 114–116, Jet Propulsion Laboratory, 1978.

[12] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*, Vol. 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. SIAM, 1992.

[13] S. Patel and G. S. Sundaram. An efficient discrete log pseudo random generator. In *Lecture Notes in Computer Science (CRYPTO'98)*, Vol. 1462, pp. 304–317. Springer-Verlag, 1998.

[14] C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Lecture Notes in Computer Science (CRYPTO'91)*, Vol. 576, pp. 433–444. Springer-Verlag, 1992.

[15] K. Sakurai and H. Shizuya. A structural comparison of the computational difficulty of breaking discrete log cryptosystems. *Journal of Cryptology*, 11(1):29–43, 1998.

[16] A. Shamir. On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, 1(1):38–44, 1983.

[17] A. C. Yao. Theory and applications of trapdoor functions. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pp. 80–91. IEEE Computer Society Press, 1982.