ＥＣＤＳＡ 評 価 報 告 書

2001 年 12 月

株式会社 東芝

新保　　淳
丹羽 朗人
岡田 光司

ECDSA 評価報告書

平成 13 年 12 月

1　はじめに

本文では、ECDSA の安全性評価の結果についてまとめる。本文の構成は、2 章で SEC1[40] および SEC2[41] により提案されている ECDSA の仕様について概要をまとめ、3 章で ECDSA に対する既存の攻撃を挙げる。以下、4 章では、ECDSA の適応的選択平文攻撃に対する安全性の証明について検証し、その正当性および妥当性を考察する。5 章では、SEC2 において推奨されている Koblitz 曲線固有の攻撃に対する安全性について考察する。

2　ECDSA 仕様

本章では、SEC1[40] および SEC2[41] に記述されている ECDSA のアルゴリズムおよび設計基準についての概要を説明し、その妥当性に関する考察を行う。

2.1　ECDSA アルゴリズム

署名方式は、署名者 U と検証者 V の 2 者により実行される。まず、署名者 U が平文 M に対しする署名 S を生成し、平文 M と署名 S を検証者 V へ送る。すると、検証者 V は受け取った署名 S が真に平文 M に対する署名者 U の署名であるかどうかを検証することができる[1] 。

SEC1 に提案されている ECDSA は、署名者 U により実行される署名生成アルゴリズム、検証者 V により実行される署名検証アルゴリズムと、これらを実現するためのセットアップ、および鍵生成の手続きからなる。以下に、各アルゴリズムの詳細を示す。

[1] 署名者が平文 M を署名と一緒に送らなくても、署名からメッセージを復元可能なメッセージ復元型署名方式も知られている。ECDSA ではメッセージ復元型署名ではないため詳細は省略する。

セットアップ: 署名者 U と検証者 V は、ECDSA を実行する事前準備として以下を行う。

1. 署名者 U は、署名アルゴリズムで使用するハッシュ関数 H を選択する。(現在 SEC1 でサポートしているハッシュ関数は SHA-1 のみ。)
2. 署名者 U は、楕円曲線のドメインパラメータ $T = (p, a, b, G, n, h)$ または $(m, f(x), a, b, G, n, h)$ (2.2 項参照) を選択する。
3. 検証者 V は、署名者 U の選択したハッシュ関数 H および楕円曲線パラメータ T を、検証可能な方法で取得する。

鍵生成: 署名者 U および検証者 V は、以下により鍵を生成する。

1. 署名者 U は、楕円曲線ドメインパラメータ T を用いて、秘密鍵 $d \in [1, n-1]$ を (疑似) ランダムに選び、公開鍵 $Q = dG$ を生成する。
2. 検証者 V は、署名者 U が生成した公開鍵 Q を、検証可能な方法で取得する。

署名生成: 署名者 U は、セットアップおよび鍵生成手続きにより生成した鍵 (d, Q)、楕円曲線パラメータ T、ハッシュ関数 H を用いて、以下の署名生成アルゴリズムを実行する。

入力: 平文 M

出力: 平文 M に対する署名 $S = (r, s)$ または invalid。

アルゴリズム:

1. $k \in [1, n-1]$ を (疑似) ランダムに選ぶ。
2. $kG = (x_1, y_1)$ を計算し、x_1 を整数表現 x_1' に変換する。
3. $r = x_1' \bmod n$ を計算する。$r = 0$ の場合 step 1 へ戻る。
4. $H(M)$ を計算し、出力をビット列 m に変換する。ハッシュ関数 H の出力が invalid の場合、invalid を出力して終了する。
5. $k^{-1} \bmod n$ を計算する。
6. $s = k^{-1}(m + dr) \bmod n$ を計算する。 $s = 0$ の場合 step 1 へ戻る。
7. 署名 $S = (r, s)$ を出力する。

署名検証: 検証者 V は、セットアップおよび鍵生成手続きにより生成した鍵 Q、楕円曲線ドメインパラメータ T、ハッシュ関数 H を用いて、以下の検証アルゴリズムを実行する。

入力: 平文 M、および署名者 U の平文 M に対する署名 $S = (r, s)$。

出力: valid または invalid。

アルゴリズム:

1. r, s がともに $[1, n-1]$ の整数であることを確認する。
2. $H(M)$ を計算し、出力をビット列 m に変換する。
3. $u_1 = ms^{-1} \bmod n$, $u_2 = rs^{-1} \bmod n$ を計算する。
4. $R = (x_r, y_r) = u_1 G - u_2 Q$ を計算する。$R = O$ ならば invalid を出力。
5. x_r を整数表現 x'_r へ変換し $v = x'_r \bmod n$ を計算する。
6. $v = r$ ならば valid、$v \neq r$ ならば invalid を出力する。

これらアルゴリズムの定義は、基本的に ANSI X9.62[1]、 FIPS 186-2[7]、および IEEE Std 1363-2000[18] により定義されているアルゴリズムと違いはない。

2.2 ECDSA 設計基準

ECDSA が既存の攻撃に耐え得るため、現在では暗号に使用できる楕円曲線に制限が加えられている。具体的にはパラメータ選択に制限を設けることになる。本章ではその制限によるパラメータ生成について SEC1 に従って説明する。

2.2.1 素体上の楕円曲線の場合

楕円曲線のドメインパラメータの定義

素体 F_p 上の楕円曲線 E の Weierstrass 標準形を

$$y^2 = x^3 + ax + b$$

とする。またベースポイントを $G = (x_G, y_G)$ とし、その位数を n、$h = \#E(F_p)/n$ とおく。このとき F_p 上の楕円曲線のドメインパラメータを、$T = (p, a, b, G, n, h)$ と定義する。

ドメインパラメータの妥当条件

外部からドメインパラメータを与えられた場合にそれがパラメータとして妥当かを判断する手順を以下に挙げる。

Input: セキュリティレベルに応じて整数 t を集合 $\{56, 64, 80, 96, 112, 128, 192, 256\}$ より選ぶ。

$Output:$ F_p 上の楕円曲線ドメインパラメータ $T = (p, a, b, G, n, h)$

次の条件を満たしているかどうかをチェックし、全て満たしていれば妥当、そうでなければ妥当でないとする。

1. p は $t \neq 256$ なら $\lceil log_2 p \rceil = 2t$、$t = 256$ なら $\lceil log_2 p \rceil = 521$ となる奇素数か。
2. a, b, x_G, y_G は $[0, p-1]$ の範囲の整数か。
3. $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ となっているか。
4. ${y_G}^2 \equiv {x_G}^3 + ax_G + b$ となっているか。
5. n は素数か。
6. $h \leq 4, h = \lfloor (\sqrt{p}+1)^2/n \rfloor$ か。
7. $nG = O$ か。
8. $1 \leq B < 20$ なる B に対し、$p^B \not\equiv 1 \pmod{n}$ でしかも $nh \neq p$ か。

ドメインパラメータの生成においては、SEC1 では実質的には上記の条件を満たすようにパラメータ選定することのみが指定されており、具体的な生成アルゴリズムを指定するような記述は存在していないが、それは確かに不要であろう。ここで、上記条件の妥当性について考察する。

1. まず、最後の条件について SEC1 の 3.1.1.2.1 では $q^B \not\equiv 1 \pmod{n}$ となっているが、この q は p の誤植であると思われる。
2. 条件のうち、1,2,3,4,7 は a, b によって決まる曲線が素体上の非特異 3 次曲線 (即ち楕円曲線) で、ベースポイント G がその上にあることを確認するということで楕円曲線暗号として成立するために当然必要なチェックである。
3. 条件 5,6,8 は楕円曲線暗号の根拠となる楕円離散対数問題に対する攻撃に対して弱い楕円曲線を選定していないかどうかのチェックである。どの条件がどのような具体的な攻撃に対するチェックであるかの詳細については、3.2 に説明を譲る。

結論としては、これら妥当性判定条件は ECDSA 設計基準として必要な条件である、と言える。

2.2.2　2 の拡大体上の楕円曲線の場合

楕円曲線のドメインパラメータの定義

2 の拡大体 F_{2^m} 上での楕円曲線の Weierstrass 標準形を

$$y^2 + xy = x^3 + ax^2 + b$$

とする。また F_{2^m} の元を F_2 上の多項式基底で表すために用いる最小多項式を $f(x)$ とする。更にベースポイントを $G = (x_G, y_G)$ とし、その位数を n、$h = \#E(F_{2^m})/n$ とおく。このとき F_{2^m} 上の楕円曲線のドメインパラメータを、$T = (m, f(x), a, b, G, n, h)$ と定義する。

ドメインパラメータの妥当条件

外部からドメインパラメータを与えられた場合にそれがパラメータとして妥当かを判断する手順を以下に挙げる。

Input： セキュリティレベルに応じて整数 t を集合 $\{56, 64, 80, 96, 112, 128, 192, 256\}$ より選ぶ。

Output： F_p 上の楕円曲線ドメインパラメータ $T = (m, f(x), a, b, G, n, h)$

次の条件を満たしているかどうかをチェックし、全て満たしていれば妥当、そうでなければ妥当でないとする。

1. t' を $\{64, 80, 96, 112, 128, 192, 256, 512\}$ に属する t より小さい最大整数とするとき、m は、$2t < m < 2t'$ を満たし、$\{113.131.163.193, 233, 239, 283, 409, 571\}$ に属するか。
2. $f(x)$ は SEC1 の 2.1.2. の Table1（ここでは省略）にある次数 m の既約バイナリ多項式か。
3. a, b, x_G, y_G は次数 $m-1$ 以下のバイナリ多項式か。
4. F_{2^m} で $b \neq 0$ となっているか。
5. F_{2^m} で ${y_G}^2 + x_G y_G \equiv {x_G}^3 + a{x_G}^2 + b$ となっているか。
6. n は素数か。
7. $h \leq 4, h = \lfloor(\sqrt{2^m} + 1)^2/n\rfloor$ か。
8. $nG = O$ か。
9. $1 \leq B < 20$ なる B に対し、$2^{mB} \not\equiv 1 \pmod{n}$ でしかも $nh \neq 2^m$ か。

ドメインパラメータの生成においては、SEC1 では実質的には上記の条件を満たすようにパラメータ選定することのみが指定されており、具体的な生成アルゴリズムを指定するような記述は存在していない点については同様である。

ここで、上記条件の妥当性について考察する。

1. 条件のうち、1,2,3,6 は a, b によって決まる曲線が 2 の拡大体上の非特異 3 次曲線 (即ち楕円曲線) で、ベースポイント G がその上にあることを確認するということで楕円曲線暗号として成立するために当然必要なチェックである。

2. 条件 4,5,7 は楕円曲線暗号の根拠となる楕円離散対数問題に対する攻撃に対して弱い楕円曲線を選定していないかどうかのチェックである。どの条件がどのような具体的な攻撃に対するチェックであるかの詳細については、3.2 に説明を譲る。

結論としては、これら妥当性判定条件は ECDSA 設計基準として必要な条件である、と言える。

3 既存の攻撃

本章では、ECDSA アルゴリズムおよびプリミティブに対する既存の攻撃をまとめるとともに、安全性のモデル化を行う。

3.1 アルゴリズムに対する攻撃

3.1.1 攻撃の種類と安全性の定義

署名方式に対する攻撃の種類、および署名方式の安全性については Goldwasser ら [15] によりモデル化され定義されている。この定義は各署名方式の安全性証明に広く用いられており [3, 32, 5, 27, 28, 4]、現時点で一般的な安全性の定義と言える。本項ではこのモデルと定義について解説する。

署名方式の安全性は 2 つの観点から考えられる。一つはどのような偽造かという観点であり、もう一つは攻撃者 (敵) にどのような攻撃を許すかという観点である。まず、偽造のレベルについては以下が考えられる。

1. 全面的解読 (total break)：署名者の秘密鍵を計算できる。

2. 一般的偽造 (universal forgery)：署名アルゴリズムと機能的に等価なアルゴリズムを効率的に見つけられる。

3. 選択的偽造 (selective forgery)：ある決められた平文に対して署名が偽造できる。

4. 存在的偽造 (existential forgery)：少なくとも一つの平文に対して署名が偽造できる。平文はランダムな意味のない平文でもよい。

これら偽造のレベルとしては、順番が後の偽造の方がより容易な偽造であることがわかる。つまり、全面的解読が可能ならばそれ以外の偽造も可能といえる。よって署名方式の安全性を考える場合、最も容易な存在的偽造さえも不可能であることを証明できれば、全ての偽造に対して安全な署名方式といえる。一方、敵の攻撃として以下の種類が知られている。

1. 受動的攻撃 (passive attack,key-only attack, no-message attack)：署名者の公開鍵だけを用いて署名を偽造する。

2. 既知平文攻撃 (known message attack)：敵は平文の集合 $M_1, \ldots, M_k$ に対する署名を知っており、この情報を用いて署名を偽造する。ただし、平文は敵が選ぶことはできない。

3. 一般選択平文攻撃 (generic chosen message attack)：敵は、前もって選んだ平文の集合 $M_1, \ldots, M_k$ に対して真の署名者が生成した署名を得られる。これらの平文と署名の組から得られる情報を用いて、前に選んだ平文とは異なる平文に対する署名を偽造する。この攻撃では、平文の選択は署名者の公開鍵に依存しないという意味で一般的 (generic) である。また、署名を得る前に全ての平文 $M_1, \ldots, M_k$ を選択しておくため非適応的 (nonadaptive) である。

4. 指向的選択平文攻撃 (directed chosen message attack)：敵は署名者の公開鍵に依存した平文を選び、それに対する署名が得られる。この点以外は一般選択平文攻撃と同じである。

5. 適応的選択平文攻撃 (adaptive chosen message attack)：敵が毎回適応的に選んだ平文に対して真の署名者が署名を生成し、最後にそれらの平文とは異なる平文に対する署名を偽造する。つまり、敵は以前に得られた署名の情報を利用して新たに平文を選択し、この平文に対する署名を得ることができる。言い換えると、敵が真の署名者をオラクルとして用いることが許されている状況での攻撃である。

こちらは順番が後の攻撃の方がより強力な攻撃であることがわかる。よって、最も強力な攻撃である適応的選択平文攻撃に対して安全であることが証明できれば、全ての攻撃に対して安全といえる。

以上より、署名方式の安全性について「適応的選択平文攻撃に対して存在的偽造が不可能」であることが証明可能ならば、現時点で最高の安全性を有する署名方式であるといえる。本文では、このような署名方式を「安全な」署名方式と呼ぶ。

3.1.2 安全性の証明手法と既存の結果

本項では、これまでに知られている安全性の証明手法と ECDSA 方式の安全性に関する結果についてまとめる。

まず署名方式の安全性を証明する場合、署名を偽造する問題を数学的に計算困難と広く信じられている問題、例えば適当な群上の離散対数問題や素因数分解問題などに還元する方法が一般的である。これにより、その数学的な問題が計算困難であると仮定すれば、その署名方式が安全と言える。

これまで、Goldwasser ら [15] により、素因数分解問題は困難という仮定のもとで安全な署名方式が提案されている。さらに、Rompel[30] により、一方向性関数の存在のみを仮定した安全な署名方式も提案されている。しかし、これらの方式は署名が平文に比べ大きい、計算が煩雑といった欠点があり、実用的とは言い難い。

これに対し Bellare-Rogaway[2] は、署名方式で用いるハッシュ関数を理想的なランダム関数と仮定した Random Oracle Model を提案し、この Random Oracle Model のもとでより実用的な署名方式の安全性を証明している [3]。Random Oracle Model の妥当性については、理想的なランダム関数と実装時に用いられるハッシュ関数 (例えば SHA-1) の間のギャップなど疑問視する声もあるが、現在は Random Oracle Model における安全性を証明することが、署名方式の安全性を示す一指標として定着しつつある。

ECDSA については、これまで Random Oracle Model のもとでの安全性は証明されていない。Pointcheval-Stern[28] および Brickell ら [4] は、DSA または ECDSA を変形した署名方式について Random Oracle Model のもとでの安全性を証明しているが、残念ながらこれらの証明手法は ECDSA そのものには適用できない。

最近、Brown[5] により、Generic Model における ECDSA (正確には Generic Model 上で定義した DSA：Generic DSA) の安全性が、ハッシュ関数の衝突困難性 (collision-registant) に還元可能であることが証明された。つまり、ハッシュ関数の衝突困難性のみを仮定すれば Generic Model における ECDSA は安全である、と主張している。Generic Model とは、ある位数の群の要素の表現 (バイナリ表現) がランダムに与えられると仮定したモデルであり、群の表現が攻撃に役立たないことを仮定している。本文ではこの結果に注目し、その正当性と妥当性について考察する。詳細は 4 章を参照されたい。

一方、Schnorr-Jacobsson[32] は、Random Oracle Model と Generic Model

を組み合わせたモデルを定義し、このモデルの下で Schnorr 署名方式の安全性を、他の問題への還元ではなく、絶対的な計算量を導出することにより証明している。

3.2 プリミティブに対する攻撃

ECDSA の根拠となる楕円離散対数問題（ECDLP）に対する攻撃として現在考えられている一般的なアルゴリズムを以下に列挙する。

1. Pohlig-Hellman 法 [26]
   ECDLP を中国剰余定理を用いて法の各素因子の ECDLP に帰着させる。

2. baby-step-giant-step 法
   Shanks により考案された離散対数問題の求解アルゴリズムでその計算のオーダーはおおよそ $O(\sqrt{n})$ になる。

3. Pollard の ρ 法、λ 法 [29]
   ECDLP の対象となる 2 点の線型結合をランダムウォークさせ、それらの点の衝突 (collision) によって ECDLP を解く。必要な step 数は、$\sqrt{\pi n/2}$ であるが、Oorschot-Wiener[25] によって並列計算ができるようになり、M 個のプロセッサを用いれば、必要な step 数は、$(\sqrt{\pi n/2})/M$ になる。

4. MOV 帰着 [22]、あるいはそれを含む FR 帰着 [10]
   Weil pairing,Tate pairing と呼ばれるものを用いて ECDLP を有限体上の離散対数問題に帰着させる。supersingular 曲線等小さい有限体上の離散対数問題に帰着するような楕円曲線に対して有効になる。

5. SSSA 攻撃 [37][33][31]
   楕円曲線の位数が法と一致する場合に多項式時間で ECDLP を解く方法を与える。

なお、有限体上の乗法群の離散対数問題では、Index calculus 法という攻撃方法があるが、楕円曲線上の離散対数問題には適用できないことが Miller[23]、Silverman-Suzuki[36] にて議論されている。またこれに類する方法で Silverman[35] により提案された Xedni calculus 法があるが現在のところ、実用には至っていないようである。2.2 での設計基準の一部については 2.2(3) でも述べたように、これら攻撃に対する耐性を持つように妥当性判定条件が挙げられており、ここではこれについて解説する。

1. baby-step-step-giant-step 法、Pohlig-Hellman 法、Pollard の ρ 法、λ 法については、楕円曲線の位数が almost prime であれば回避できること

が知られている。これは素体の場合、妥当性条件の条件 5,6、2 の拡大体の場合、妥当性条件の条件 4,5 によって保証される。

2. MOV/FR 帰着については、素体の場合、妥当性条件の条件 8 の前半 ($p^B \neq 1$)、2 の拡大体の場合、妥当性条件の条件 9 の前半 ($2^{mB} \neq 1$) によって保証される。

3. SSSA 攻撃については、素体の場合、妥当性条件の条件 8 の後半 ($nh \neq p$)、2 の拡大体の場合、妥当性条件の条件 9 の後半 ($nh \neq 2^m$) によって保証される。

これら以外に Koblitz 曲線固有の攻撃が考えられるが、それについては、5 章にて説明する。

4 アルゴリズムの安全性証明に関する評価

最近、Brown[5] により、Generic Model における ECDSA の選択平文攻撃に対する存在的偽造不可能性が証明された。これは、Generic Model における ECDSA の安全性がハッシュ関数の衝突困難性 (collision-resistant) に還元可能であることを示している。本章では、この証明について解説し、その正当性および妥当性について考察する。

まず、4.1 項で Generic Model の背景と解説を行う。次に、4.2 項で Brown[5] の証明について解説する。最後に、4.3 項で Brown の証明の正当性および Generic Model の妥当性について考察する。

4.1 Generic Model

4.1.1 Generic Model とは

Generic Model とは、群の要素表現 (バイナリ表現) がランダムに与えられると仮定したモデルである。特に [5] では、位数が素数 n の加法群 $\mathbb{Z}_n$ と同型な、要素数 n のビット列集合 S (群要素の表現集合：Generic Group) を考え、$\mathbb{Z}_n$ から S への全単射 $\sigma : \mathbb{Z}_n \to S \subset \{0,1\}^*$ がランダムに与えられると仮定している。そして、Generic Group 上の演算は全てオラクルへの問い合わせ (query) により行われる。特に [5] では、$(X, Y) \in S^2$ をオラクルへ入力することにより、それらの要素を減算した結果 $Z = X - Y \in S$ を得ると仮定している (全ての演算は減算を用いて計算可能である)。

例えば ECDSA の場合、楕円曲線上の位数 n の加法群がランダムに与えられ (楕円曲線自体は変わってよいが、群の位数は一定)、その楕円曲線上の演算は全てオラクルへの問い合わせにより行うモデル、と考えることができる。

この Generic Model において安全性の検証を行うことは、群の要素表現に依存しない攻撃のみを仮定した上での安全性を検証している、と考えられる。逆に、群の要素表現に依存した攻撃は考慮せず、純粋にアルゴリズムに対する攻撃のみを仮定したモデルと言っても良い。

4.1.2 Generic Model における従来の結果

Nechaev[24] は、ランダムな群における離散対数問題の計算困難性を証明している。その後、Shoup[34] はこのモデルを Generic Model と定義し、Generic Model における離散対数問題、Diffie-Hellman 問題 (DH 問題) の計算量の下界を導出している。さらに Maurer-Wolf[21] は、Generic Model における離散対数問題と DH 問題の等価性 (還元にかかる計算量の下界) について検討している。

近年、Schnorr-Jacobsson[32] は、Random Oracle Model と Generic Model を組み合わせたモデルを定義し、このモデルの下で Schnorr 署名方式の安全性を、他の問題への還元ではなく、絶対的な計算量の下界を導出することにより証明している。さらに、次項で述べるように、Brown[5] により Generic Model における ECDSA の安全性がハッシュ関数の衝突困難性 (collision-resistant) に還元可能であることが証明されている。

署名方式を含む暗号学的な方式の安全性の証明に Generic Model を用いた例は上記の 2 例 [32, 5] のみである。よって、この安全性の証明手法が一般的とは言い難い。また、これらの妥当性について記述されたレポートは発表されていない。

4.2 Brown[5] による安全性の証明

4.2.1 Generic DSA

Brown[5] は、ECDSA そのものの安全性を証明するのではなく、DSA/ECDSA をサブクラスとして含む署名方式 – Generic DSA を定義し、Generic Model におけるこの方式の安全性を証明している。Generic DSA の定義は以下の通りである。

定義 1 (Generic DSA) 位数が素数 n である加法群のベースポイント (原始元) を G とする。また、還元関数 $f : \langle G \rangle \to [0, n-1]$、ハッシュ関数 $h : 0, 1^* \to [0, n-1]$ を定義する。

鍵生成: 秘密鍵 $d \in [0, n-1]$ をランダムに選択し、$Q = dG$ を公開鍵とする。

署名生成: 平文 M に対する署名生成を以下の手順で行う。

1 ランダムな整数 $k \in [0, n-1]$ を選択。

2 $R = kG$ を計算。

3 $r = f(R)$ を計算。

4 $e = h(M)$ を計算。

5 $s = k^{-1}(e + dr) \bmod n$ を計算。

6 (r, s) を平文 M の署名とする。

署名検証: 平文 M、署名 (r, s)、公開鍵 Q により下式が成り立つことを検証する。

$$r = f(s^{-1}h(M)G + s^{-1}rQ)。$$

DSA/ECDSA は Generic DSA のサブクラスに含まれると考えられる。DSA は、ハッシュ関数 h として SHA-1 の出力の modulo n を、ベースポイント G として $\mathbb{Z}_p^*$(p は素数) のうち位数が $n|p-1$ を満たす要素を、還元関数 f を $f(R) = R \bmod n$ と定義したものに一致する。また ECDSA は、ハッシュ関数 h として SHA-1 の出力の modulo n を、ベースポイント G として有限体上の楕円曲線における位数 n のベースポイントを、還元関数 f を $f(R) = x_R \bmod n$(ただし x_R は楕円曲線上の点 R の x 座標) と定義したものに一致する。

確かに DSA と ECDSA とは、ベースポイント G により決定される加法群の要素表現以外のアルゴリズムに差異はなく、この要素表現がランダムに与えられると仮定される Generic Model では同じアルゴリズムと考えて良い。その意味で Generic DSA の定義は妥当なものと思われる。

以降、Generic DSA で用いるハッシュ関数 h は、一方向性および衝突困難性 (collision-resistant:$h(x) = h(x')$ を満たす x, x' を見つけることは困難) を有することを仮定し、証明を行っている[2] 。

4.2.2 主な結果と証明の概要

Brown[5] は、$\mathbb{Z}_n$ と同型な Generic Group $S \subset \{0,1\}^*$ を考え、この Generic Model 上での Generic DSA について以下の 2 つの結果を導出している。定理 2 は受動的攻撃に対する安全性、定理 3 は適応的選択平文攻撃に対する安全性を示している。

[2] その他、ハッシュ関数 h が一様 (出力 $h(x)$ が一様分布と区別不可能となるような入力分布が存在する) であること、還元関数 f が almost invertible(高い確率で逆写像を求められ、かつ逆写像が一様分布) であることを仮定している。

定理 2 受動的攻撃により、敵 F_h が実行時間 τ 以下、確率 ϵ 以上で存在的偽造に成功すると仮定すると、実行時間 τ' 以下、確率 ϵ' 以上でハッシュ関数 h の逆写像を求めるアルゴリズム I_h が存在する。ただし、τ',ϵ' は以下の通り*:*

$$\epsilon' = \frac{\epsilon - 3\left(\begin{array}{c}\tau' \\ 2\end{array}\right)/n}{\tau'}, \quad \tau' \leq 2\tau$$

定理 3 適応的選択平文攻撃 *(*選択平文数を q とする*)* により、敵 F_h が、実行時間 τ 以下、確率 ϵ 以上で存在的偽造に成功すると仮定すると、実行時間 τ' 以下、確率 ϵ' 以上でハッシュ関数 h の *collision* を求めるアルゴリズム C_h が存在する。ただし、τ',ϵ' は以下の通り*:*

$$\epsilon' = \epsilon - 3\left(\begin{array}{c}\tau' \\ 2\end{array}\right)/n, \quad \tau' \leq 2\log n(\tau + q).$$

以下、定理 2 の証明の概要を述べる。証明方法は、敵 F_h をサブルーチンとして用いた I_h を構成し、その成功確率 ϵ' と実行時間 τ' を見積もっている。

I_h への入力を $e \in_R [0, n-1]$、出力を $h(M) = e$ を満たす平文 M とする。まず、Generic Group S のベースポイント G および公開鍵 Q を選び F_h へ入力する。次に、F_h からの query に対して、S の演算を行うオラクルをシミュレートする。オラクルの出力が $xG + yQ$ を満たすような query の 1 つに対して

$$Z = f^{-1}(yx^{-1}e \bmod n)$$

を出力し、それ以外は S の要素をランダムに出力する。ただし $x, y \in \mathbb{Z}_n$ は、それ以前の query により得られた値である。e のランダム性から Z も S 上でランダムであり、F_h からは本当のオラクルと区別がつかない。最終的に F_h が平文 M と署名 (r, s) を出力し、I_h はこの平文 M をそのまま出力する。

もし F_h が偽造に成功していたとすると $V = s^{-1}h(M)G + s^{-1}rQ$ に対して $r = f(V)$ が成立している。また、F_h の query の中で、必ずオラクルが $s^{-1}h(M)G + s^{-1}rQ$ を出力するような query が存在するはずである。その出力がたまたま Z に一致した場合、以下の式が成り立つ:

$$r = f(V) = f(Z) = yx^{-1}e = (s^{-1}h(M)))^{-1}(s^{-1}r)e = rh(M)^{-1}e \bmod n.$$

これより $h(M) = e$ が成り立つ。

以上のアルゴリズムの実行時間と成功確率を見積もると、定理 2 の値に等しい。よって、証明に誤りはないと考えられる。

定理 3 については証明の記述はほとんどなく、その正当性を検証することはできなかった。

4.3 証明の正当性およびモデルの妥当性について

まず、Brown[5] の証明の正当性について考察する。前項で説明した通り、安全性の証明は ECDSA そのものではなく Generic DSA について行われている。Generic Model のもとでの Generic DSA の安全性という意味では、定理 2 の受動的攻撃に対する安全性の証明は正しいと判断できる。一方、定理 3 の適応的選択平文攻撃に対する安全性の証明についての記述はほとんどなく、その正当性を検証するまでに至らなかった。[5] は単なる Technical Report であり、その後、学会・論文誌などで発表されていないため、今後 Full Paper が公表されるのを待つしかない。最近、Brown により論文 [6] が書かれたようだが、公表はされていないため入手できなかった。以降は定理 2 のみが正しいとして考察を行う。

では、Generic Model のもとでの Generic DSA の安全性の証明が、DSA または ECDSA の安全性の証明と言えるであろうか[3] 。確かに ECDSA は Generic DSA のサブクラスに含まれるが、それがすなわち ECDSA の安全性が証明されたと言うには語弊があると思われる。それを検証するには、証明の前提である Generic Model の妥当性について考察する必要がある。

まず Generic Model では、$\mathbb{Z}_n$ から S への全ての全単射 σ がランダム選ばれると仮定している。よって全単射の数は $n!$ 個存在する。しかし ECDSA では、楕円曲線上の点の部分集合である群は巡回群であり、たとえベースポイント B をランダムに選んだとしても高々n 個の全単射しか実現できない。全ての全単射を実現するためには楕円曲線を変更し、かつ上記の点集合を含む位数 n の部分群を探さなければならず、事実上実現不可能である。これは、単純に楕円曲線をランダムに選ぶという手続きとは異なっている点に注意されたい。上記の全ての全単射がランダムに選ばれる事象と楕円曲線をランダムに選ぶという事象の間にどの程度の差があるのかは知られていない。これに関する考察は今後必要になるであろう。しかし、たとえ楕円曲線をランダムに選ぶことにより Generic Model を実現していると証明されたとしても、楕円曲線をランダムに選ぶという実装には大きな問題がある。

実装を考えた場合、Random Oracle Model において理想的なランダム関数をハッシュ関数で実装したときに起こる問題と同じ問題が生じる。Random Oracle Model では、実装したハッシュ関数、例えば SHA-1 に致命的な欠陥が生じた場合、別の安全なハッシュ関数に置き換えることにより全体の安全性が保たれると広く信じられている。Generic Model でも、同じように実装に用いた群に致命的な欠陥が見つかった場合、別の安全な群に置き換えることは可能であろうか。ベースポイント B の変更や楕円曲線そのものを置き換え

[3] [5] では、この証明 ECDSA に適用できるが DSA には適用不可能かもしれない、という記述がある。しかし、その理由は明記されていない。今回検証した限りでは、定理 2 は Generic Model のもとで DSA にも適用可能と思われる。

ることはパラメータの変更だけで実現可能なため、ハッシュ関数の実装そのものを変更する場合よりも一見容易に実現可能と考えられる。しかし、ベースポイント B や楕円曲線を変更することにより、各ユーザの秘密鍵/公開鍵を全て更新しなけれならないという、運用上の問題が生じる。よって、ベースポイントや楕円曲線の変更が、ハッシュ関数の変更と比較してメリットがあるとは言い難い。

しかし、現在知られている ECDLP などの離散対数問題を解くアルゴリズム、例えば Pohlig-Hellman 法 [26] や Pollard の ρ 法 [29] などは全て群上の演算をブラックボックスとして用いる Generic Model 型のアルゴリズムと言える (Index-calculus 法は Generic Model 型ではない)。これらの攻撃に対する安全性を考える場合、Generic Model における安全性の証明は、署名方式を含む暗号学的方式の安全性を示す一指標といえるであろう。

以上を結論づけると、[5] の証明について受動的攻撃に対する結果については正当性があると判断できるが、適応的選択平文攻撃に対する結果についてはその証明が明記されておらず、正当な結果かどうかを判断するには至らなかった。また、Generic Model のもとでの ECDSA 安全性の証明は、安全性を示す一指標にはなると思われるが、Random Oracle Model と比較すると成熟したモデルではないため一般的な考察が不足しており、今後の議論に注目する必要がある。また Generic Model に従った実装を考えた場合、鍵の変更が伴うなど、実用上問題があると考えられる。

5 Koblitz 曲線の安全性に関する評価

5.1 Koblitz 曲線の定義と特徴

Koblitz 曲線とは Koblitz[20]、Solinas[39] で導入された 2 の拡大体上の曲線で次式によって定義されるもので、anomalous binary curve(ABC 曲線) とも呼ばれている：

$$u^2 + uv = v^3 + av + 1 \ (a = 0, 1)$$

但し、この曲線は定義体が F_{2^m} である F_2 上の曲線とする（F_2 係数 $u.v$ は F_2 の元になる）この曲線の特徴として Frobenius 写像を用いることによって点のスカラー倍演算を高速に計算できることがあげられる。

その要点は、通常のスカラー倍演算はスカラーを 2 進展開して点の加算と、それより計算量の少ない点の 2 倍算の実行回数を最小にすることによって行われるのに対して、Koblitz 曲線では、2 倍算より計算量が少ない Frobenius 写像 φ を用いてスカラーを φ 進展開することによってスカラー倍演算を行うことができるということである。具体的には次の通り。Frobenius 写像とは次

のような自己準同型写像である：

$$\varphi : (x, y) \to (x^2, y^2)$$

この演算の計算量については、F_{2^m} の F_2 上の基底として、正規基底を用いた場合は、基底の係数の入れ替えのみで行うことができ、多項式基底を用いた場合でも通常の点の加算や倍数演算に比べると無視できる程少ない。

この Frobenius 写像 φ は次の関係式を満たしている：

$$\varphi^2 - t\varphi + 2 = 0$$

ここで φ の積は写像の合成を表し、t は楕円曲線のトレースと呼ばれる量で Koblitz 曲線の場合には、$t = (-1)^{1-a}$ になる。この式を変形して

$$2 = t\varphi - \varphi^2$$

として用い、2 進展開における倍数演算を上記右辺に置き換えることにより、スカラーの φ 進展開が可能になる。Koblitz 曲線の場合には t による係数増加がないため、φ 進展開の係数増加を抑えることができる。

[39] では更なる工夫として、φ 進 NAF 展開が導入されている。ここで NAF 展開について簡単に説明すると、スカラーの符号付き展開であって、各位の値が確率 2/3 で 0 になるような展開であり、0 が多いことによってスカラー倍の計算コストを抑えることができる。

この曲線は近年、次のような拡張がなされている。

(1) Koblitz 曲線の種数 2 の超楕円曲線への拡張

Gunther-Lange-Stein[16] は次のような式で定義される 2 の拡大体上の超楕円曲線について、Frobenius 写像 φ による divisor のスカラー倍演算の高速化を検討した：

$$u^2 + uv = v^5 + av^2 + 1 \ (a = 0, 1)$$

但し、この曲線は定義体が F_{2^m} である F_2 上の曲線とする。この場合も Koblitz 曲線と同様にスカラー倍演算を φ 進 NAF 展開によって行うことが可能であり、それによって divisor のスカラー倍演算が高速化できることが示されている。

(2) 標数 p の拡大体（OEF 等）上の曲線への拡張

Kobayashi-Morita-Kobayashi-Hoshino[19] は 2 以外の標数 p の拡大体 F_{p^m} においても標数 2 の場合と全く同様に F_p 上楕円曲線の点のスカラー倍演算を Frobenius 写像によって高速化できることが示されている。但しこの場合 φ 進 NAF 展開等は考えられていない。

(3) 素体 F_p 上で Frobenius 写像以外の自己準同型写像を用いる拡張

Gallant-Lambert-Vanstone [12] は素体 F_p 上で上記の手法を Frobenius 写像以外の自己準同型写像に拡張する方法を提案している。有限体上の楕円曲線は（標数 0 の体上の楕円曲線の場合と異なり）必ずCM（虚数乗法）を持つ、即ちスカラー倍以外の自己準同型写像は必ず存在する。しかしながら、それらが Frobenius 写像と同じようにスカラー倍を効率化できるためには、自己準同型写像の計算量が少なくとも点の倍数演算より高速である必要があるが、一般には必ずしもそうなるとは限らない。

SEC2 では、(3) で自己準同型写像が高速にできる曲線を一般化された「Koblitz 曲線」として、その推奨パラメータを挙げている。

5.2 Koblitz 曲線固有の攻撃とその対策

3.2 にて一般的な楕円離散対数問題（ECDLP）に対する種々の攻撃を挙げた。Koblitz 曲線に対しては、これらの他にその性質を利用した攻撃が見出されている。本項では、これら攻撃とその対策について説明する。Koblitz 曲線固有の攻撃を以下に列挙する：

(1) 並列 Pollard λ 法、ρ 法の高速化

3.2 で ECDLP に対する攻撃として並列 Pollard λ 法、ρ 法を挙げた。これらについて、Gallant-Lambert-Vanstone[13] は、Koblitz 曲線に対して並列 Pollard λ 法が $\sqrt{2m}$ 倍に高速化できることを示した。Wiener-Zuccherato[42] は、同様に Koblitz 曲線に対して並列 Pollard ρ 法が $\sqrt{2m}$ 倍に高速化できることを示した。

これら攻撃に対する対策としては、鍵長を調整して安全性を保つということになると考えられる。SEC1 では、p.59 の B.1 にてこの攻撃についても触れているが、このために鍵長の調整 をすることについての記述はない。この程度の攻撃高速化は問題にしていないものと思われるが、それについての明示的な記述はない。SEC2 でも Koblitz 曲線と他の曲線を安全性において同等に扱っており（p.5 の Table1、p.22 の Table4 で同じ強度に扱っている）、これにはやや問題があると思われる。

(2) Weil descent による攻撃

楕円曲線の定義体が標数 p の拡大体で拡大次数が合成数 nm の場合に、Frey[8, 9] のアイデアに基づき、Galbraith-Smart[11] は Weil descent という代数幾何学的手法により、$F_{p^{mn}}$ 上の ECDLP を F_{p^m} 上の超楕円曲線上の離散対数問題に帰着させる攻撃の構想を発表し、Gaudry-Hess-Smart[14] は実際に、2 の拡大体の場合に Pollard ρ 法より高速に攻撃することができることを示した。GHS の方法は、Weil descent による攻

撃を実現する手法の一つであり、他の実現手法もあると考えられる。また、GHS の方法は、そのままでは Koblitz 曲線に適用することはできなかった。ところが Smart[38] によると Frey とその学生は Koblitz 曲線に適用できるように GHS の方法を拡張したとのことである。この攻撃に対する対策としては、Hess-Seroussi-Smart[17] でも述べられているように定義体の拡大次数を素数とすることが挙げられる。

SEC1 では、p.59 の B.1 にてこの攻撃についても触れており、FR 帰着の適用可能な曲線と合わせて、これらの弱い曲線を暗号向けに使用しない旨が述べられている。SEC1 では、設計基準のパラメータ妥当性条件の 1 により拡大次数を素数から選んでいる。これは Koblitz 曲線の場合、曲線の位数が almost prime であるために必要な条件であるが、同時に Weil descent による攻撃に対して弱いパラメータ設定を回避することになっている。

以上の総括として、

1. SEC1 でのパラメータ設定により Koblitz 曲線に対する安全性は確保されている。

2. しかし SEC2 では、同じ鍵長の Koblitz 曲線と他の曲線の安全性・強度を同等に扱っており、この考え方にはやや問題があると思われる。

6 まとめ

本文では、ECDSA の安全性評価の結果についてまとめている。

特に、Brown[5] により証明された Generic Model における ECDSA の選択平文攻撃に対する存在的偽造不可能性について考察を行った。しかし、証明が明記されておらず、正当な結果かどうかを判断するには至らなかった (受動的攻撃に対する存在的偽造不可能性の証明については正当な結果であると思われる)。また、証明の前提である Generic Model の妥当性について考察を行った。Generic Model のもとで ECDSA の安全性を証明することは、安全性を示す一指標になると思われる。しかし、Random Oracle Model と比較すると成熟したモデルではないため一般的な考察が不足しており、今後の議論に注目する必要があると考えられる。また Generic Model に従った実装を考えた場合、鍵の変更が伴うなど、実用上問題があると考えられる。

また、Koblitz 曲線固有の攻撃に対する安全性について考察を行った。Koblitz 曲線は、点のスカラー倍演算を高速に行うことができ、その結果 ECDSA の署名生成／検証を高速に行うことが可能である。しかしながら、一般に高速に演算できる暗号については高速に攻撃できる可能性が高いと言われており、

Koblitz 曲線もその例外でなく、Koblitz 曲線に対して Pollard の λ 法／ ρ 法の高速化が可能であった。従って通常の曲線に比べて鍵長の設定については注意が必要である。また Koblitz 曲線に対してはその特徴により Weil descent 攻撃が可能である。これに対しては SEC1 では拡大次数を素数にすることによって回避できており、問題はない。

References

[1] ANSI X9.62, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digial Signature Algorithm (ECDSA)", American National Standard for Financial Services, 1998.

[2] M.Bellare and P.Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", First ACM Conference on Computer and Communications Security, ACM, 1993.

[3] M.Bellare and P.Rogaway, "The exact security of digital signatures – how to sign with RSA and Rabin", Advanced in Cryptology – EUROCRYPT'96, Lecture Notes in Computer Science **1070**, Springer-Verlag, pp.399–416, 1996.

[4] E.Brickell, D.Pointcheval, S.Vaudenay and M.Yung, "Design validations for discrete logarithm based signature schemes", Proceedings of Third International Workshop on Theory in Public Key Cryptosystems, PKC 2000, Lecture Notes in Computer Science **1880**, Springer-Verlag, pp.276–292, 2000.

[5] D.Brown, "The exact security of ECDSA", Technical Report CORR 200-34, Dept. of C&O, University of Waterloo, 2000. Available at http://www.cacr.math.uwaterloo.ca.

[6] D.Brown, "Concrete lower bounds on the security of ECDSA in the generic group model", Preprint.

[7] FIPS PUB 186-2, "Digital Signature Standard", National Institute of Standards and Technology, January 2000.

[8] G.Frey, "Weil descent", Talk at Waterloo workshop on the ECDLP, 1998,
http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html

[9] G.Frey, "Applications of Arithmetical Geometry to Cryptographic Constructions", http://www.exp-math.uni-essen.de/preprints/index00.html

[10] G.Frey and H.G.Rück,"A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves", Mathematics of Computation, **62**, pp.865–874, 1994.

[11] S.D.Galbraith,N.P.Smart, "A cryptpgraphic application of Weil descent",Proceeding Cryptography and Coding, Springer-Verlag, Lecture Notes in Computer Science **1746**, pp.191–200, 1999.

[12] R.Gallant, R.Lambert and S.Vanstone, "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms", Advances in Cryptology – CRYPTO'2001, Lecture Notes in Computer Science **2139**, Springer-Verlag, pp.190–200, 2001.

[13] R.Gallant,R.Lambert,S.Vanstone,"Improving the Parallelized Pollard Lambda Serch on Binary Anomalous Curves", Mathematics of Computation, **69**, pp.1699–1705, 2000.

[14] P.Gaudry, F.Hess and N.P.Smart, "Constructive and Destructive fasets of Weil descent on ellptic curves", http://www.cs.bris.ac.uk/Tools/Reports/Ps/2000-gaudry.ps.gz

[15] S.Goldwasser, S.Micali and R.Rivest, "A digital signature scheme secure against adaptive chose message attacks", SIAM Journal of Computing **17**, No.2, pp.281–308, 1988.

[16] C.Günther, T.Lange and A.Stein, "Speeding up the Arithmetic on Koblitz Curves of Genus Two", preprint http://www.exp-math.uni-essen.de/ lange/main.ps

[17] F.Hess, G.Seroussi and N.P.Smart, "Two topics in hyperelliptic cryptography", http://www.cs.bris.ac.uk/Tools/Reports/Ps/2000-hess.ps.gz

[18] IEEE Std 1363-2000, "Standard specifications for public key cryptography", Institute of Electrical and Electronics Engineers, Inc., August 2000.

[19] T. Kobayashi, H. Morita, K. Kobayashi and F. Hoshino, "Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic ", Advances in Cryptology – EUROCRYPT'99, Lectur Notes in Computer Science **1592**, Springer-Verlag, pp.176–189, 1999.

[20] N.Koblitz,"CM-Curves with Good Cryptographic Properties", Advances in Cryptology – CRYPTO'91, Lecture Notes in Computer Science **576**, Springer-Verlag, pp.279–287, 1997.

[21] U.Maurer and S.Wolf, "Lower bounds on generic algorithm in groups", Advanced in Cryptology – EUROCRYPT'98, Lecture Notes in Computer Science **1403**, Springer-Verlag, pp.72–84, 1998.

[22] A.J.Menezes, T.Okamoto and S.A.Vanstone, "Reducing elliptic curve logarithms to a finite field", IEEE Transactions on Information Theory, **39**, pp.1639–1946, 1993.

[23] V.Miller,"Use of elliptic curves in cryptography", Advances in Cryptology – CRYPTO'85, Lecture Notes in Computer Science **218**, Springer-Verlag, pp.417–426, 1986.

[24] V.I.Nechaev, "Complexity of a determinate algorithm for the discrete logarithm", Math. NOtes 55, pp.165–172, 1994.

[25] P.van Oorschot and M.Wiener,"Parallel collision serch with cryptanalytic applications",Journal of Cryptology, **12**,pp.1–28, 1999

[26] S.Pohlig and M.Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", IEEE Transactions on Information Theory, **24**, pp.106–110, 1978.

[27] D.Poincheval and J.Stern, "Security proofs for signature schemes", Advanced in Cryptology–EUROCRYPT'96, Lecture Notes in Computer Science **1070**, Springer-Verlag, pp.387–398, 1996.

[28] D.Pointcheval and J.Stern, "Security agruments for digital signatures and blind signautures", Journal of Cryptology **13**, No.3, pp.361–396, 2000.

[29] J.Pollard, "Monte Carlo methods for index computation mod p", Mathematics of Computation, **32**, pp.918–924, 1978.

[30] J.Rompel, "One-way functions are necessary and sufficient for secure signature", Proceedings of the 22nd annual ACM symposium on Theory of Computing – STOC'90, pp.387–394, 1990.

[31] T.Satoh and K.Araki,"Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves,Commentarii Math.Univ.St.Pauli, 47, pp.81–92, 1998, MR98e:11093

[32] C.P.Schnorr and M.Jakobsson, "Security of discrete log cryptosystems in random oracle + generic model", Conference on the

Mathematics of Public-Key Cryptography, The Fields Institute, Tronto, Canada, 2000. Available at http://www.mi.informatik.uni-frankfurt.de/research/papers.html.

[33] I.A.Semaev,"Evaluation of discrete logarithms on some elliptic curves",Mathematics of Computation, **67**, pp.353–356, 1998.

[34] V.Shoup, "Lower bounds for discrete logarithms and related problems", Advanced in Cryptology – EUROCRYPT'97, Lecture Notes in Computer Science **1233**, Springer-Verlag, pp.256–266, 1997.

[35] J.H.Silvermann,"The Xedni calculus and the elliptic curve discrete logarithm problem", Designs, Codes and Cryptography, **20**, pp.5–40, 2000

[36] J.H.Silvermann and J.Suzuki,"Elliptic curve discrete logarithms and the index calculus",Advances in Cryptology – ASIACRYPT'98, Lecture Notes in Computer Science **1514**, Springer-Verlag, pp.110–125, 1998.

[37] N.P.Smart,"The discrete logarithm problem on elliptic curves of trace one",Journal of Crytology, **12**(3),pp.193–196, 1999

[38] N.P.Smart,"Weil descent Page", http://www.cs.bris.ac.uk/ niegel/Weil-descent.html

[39] J. A. Solinas "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves",Advances in Cryptology – CRYPTO'97, Lecture Notes in Computer Science **1294**, Springer-Verlag, pp.357–371,1997.

[40] Standards for Efficient Cryptography, "SEC1:Elliptic Curve Cryptography", Certicom Research, Ver.1.0, September 2000.

[41] Standards for Efficient Cryptography, "SEC2:Recommended Elliptic Curve Domain Parameters", Certicom Research, Ver.1.0, September 2000.

[42] M.Wiener, R.Zuccherato,"Faster attacks on elliptic curve cryptosystems", Selected Areas in Cryptography, Lecture Notes in Computer Science **1556**, pp.190–200, 1999.