ＥＣＤＳＡ 評 価 報 告 書

2002 年 11 月 5 日

日本電信電話株式会社

岡本 龍明

ECDSA 評価報告書

2002 年 11 月 5 日

1 はじめに

本評価報告書では、ECDSA の最近報告された攻撃法を中心にして、ECDSA の安全性評価を示す。また、ECIES に対する攻撃法との比較／関連についても述べる。

なお、ECDSA 仕様記述や既存の攻撃法に対する安全性評価については既に CRYPTREC Report などで報告されているため、本報告書では記述しない。本報告書で用いる記号等は CRYPTREC Report 2001 [1] に準拠することとする。

2 Stern-Pointcheval-MalonLee-Smart による ECDSA の攻撃法

文献 [2] には、ECDSA の 2 種類の攻撃法が報告されている。以下、それらの概要について解説する。

2.1 攻撃法 1（重複署名）

この攻撃法は、重複署名 (duplicate signature) と呼ばれており、署名者が 2 つの異なる文書 M_1, M_2 に対して共通の署名 (r, s) を作ることができるという攻撃である。このことは、署名者が署名の否認をすることに悪用され得る。つまり、署名者はある相手に 文書 M_1 （例えば、借用書）への署名として (r, s) を渡しておき、後にその文書 M_1 に対する責務を果たす必要が生じた段階で、文書 M_2 を提示して、署名 (r, s) は文書 M_2 に対する署名であり文書 M_1 に対して署名を付けた事実は無いと主張することで、文書 M_1 に対する責務を回避しようする攻撃である（つまり、否認不可性 (non-repudiation) に対する攻撃である。）

以下 ECDSA に対して重複署名攻撃が可能なことを示すが、幸いなことに、署名者が $M_1, M_2, (r, s)$ の全てを開示した段階でその署名者の秘密鍵が露見する。従って、この ECDSA に対する重複署名攻撃は、実際的な意味で有効な攻撃とはなり得ない。

この攻撃法の発見の意義は、もしこのような重複署名攻撃法が有効であったとしても従来の安全性の観点（適応的選択文書攻撃に対して存在的偽造不可など「不正者による署名偽造」の観点）では、安全であるとされることである。つまり、重複署名攻撃法は従来考慮されていなかった新しい観点（「署名者による署名否認」の観点）での攻撃法であり、ECDSA に対する重複署名攻撃はその最初に発見された具体的攻撃法である。

それでは、ECDSA に対する重複署名攻撃法を示そう。まず、2 つの文書 M_1, M_2 に対して重複署名攻撃を行おうとする署名者は、鍵生成手順において以下のように秘密鍵 d, 公開鍵 Q を生成し、さらに 2 つの文書に対する重複署名を作成する。

1. $k \in [1, n-1]$ をランダムに選ぶ。
2. $kG = (x_1, y_1)$ を計算し、$r = x_1 bmodn$ とする。
3. $d = -(H(M_1) + H(M_2))/(2r) \bmod n$, $Q = dG$ とし、公開鍵 Q を公開する。
4. $s = k^{-1}(H(M_1) + dr) \bmod n$ を計算し、文書 M_1 と M_2 に対する重複署名を (r, s) とする。

ECDSA の署名作成手順から、明らかに (r, s) は、文書 M_1 の正しい署名となっている。そこで、(r, s) が同時に M_2 の署名にもなっていることを示そう。まず、$dr = -(H(M_1)+H(M_2))/2 \bmod n$, $s = 2k^{-1}((H(M_1) - H(M_2)) \bmod n$ である。文書 M_2、署名 (r, s) の署名検証手順において、

$$R' = (H(M_2)/s)G + (r/s)Q = ((H(M_2) + rd)/s)G$$

$$= k(-H(M_1) + H(M_2))/(H(M_1) - H(M_2))G$$

$$= -kG = (x_1, -y_1) = (r, -y_1).$$

従って、R' の x-座標は r に一致することより、署名 (r, s) は文書 M_2 に対する署名検証にも合格する。つまり、(r, s) は文書 M_1 および M_2 の重複署名となっている。

2.2 攻撃法 2（脆弱性）

この攻撃法は、脆弱性 (malleability) と呼ばれており、文書 M に対する正しい署名 (r, s) を得ると、署名偽造者が同じ文書 M に対する別の署名 (r', s') を偽造できるという攻撃である。

この攻撃法は、以下のように行われる。

ECDSA では、r を kG の x-座標の表現とするため、署名検証では、r が $R' = (H(M)/s)G + (r/s)Q$ の x-座標の表現と一致するかどうかをチェックする。このとき、s の代わりに $s' = n - s$ を用いると、$R'' = (H(M)/s')G + (r/s')Q = -(H(M)/s)G - (r/s)Q = -R'$ となり、R' と R'' の x-座標は同一であるため、結局 r は R'' の x-座標の表現と一致する。従って、文書 M に対する正しい署名 (r, s) があると、$s' = n - s$ としたとき、(r, s') も同じ文書 M に対する正しい署名となる。この攻撃法の本質は、署名検証において、楕円曲線上の点の x-座標の情報のみを用いるため、x-座標が同じ別の点（x-軸に対称な点）に関する署名も署名検証に合格することによる。なお、このことは、上で述べた攻撃法 1（重複署名）や以下で述べる ECIES の攻撃法でも利用される。

さて、以下ではこの攻撃法（脆弱性）の位置づけについて考察する。

通常の偽造においては、署名偽造とは、それまでに得た正しい署名 (r, s) 付き文書 M と異なる文書 M' に対する署名を偽造することであると考えられてきた。このことは、同じ文書 M に対して複数の署名が存在しても実効上の攻撃にはならないという考えに基づいている。しかし、文書 M を額面の金額（例えば、1 万円）としてその署名 (r, s) を電子マネーと考えると、同じ M に対して別の署名 (r', s') を偽造することは、電子マネーの偽造と考えることも可能である。従って、同じ文書に対しての署名偽造が望ましくない応用分野もあり得ることに注意されたい。

一方、署名方式の望ましい安全性は、「適応的選択文書攻撃に対して存在的偽造不可」と考えられているが、これについては、2 つのモデルが考えられる。1 つは、同じ文書 M に対して複数の署名が存在しても実効上の攻撃にはならないという考えに基づくモデル（異文書攻撃モデル）で、選択文書攻撃により k 対の署名文書 $(M_1, (r_1, s_1)), \ldots, (M_k, (r_k, s_k))$ を得て、最終的に偽造者は偽造署名文書対 $(M^*, (r^*, s^*))$ を $M^* \neq M_i$ $(i = 1, \ldots, k)$ という条件で出力するモデルである。もう 1 つのモデル（同一文書攻撃モデル）は、以下の点を除いて上で述べたモデルと同じであるが、異なる点は、偽造署名文書対の条件が $(M^*, (r^*, s^*)) \neq (M_i, (r_i, s_i))$ $(i = 1, \ldots, k)$ となる点である。つまり、異文書攻撃モデルでは、署名を偽造する対象となる文書 M^* は選択文書攻撃で利用した文書 $M_1, \ldots, M_k$ と異なっている必要があるが、同一文書攻撃モデルでは、仮に $M^* = M_i$ であっても、$(r^*, s^*) \neq (r_i, s_i)$ であればよい。

この 2 つのモデルの観点で、ECDSA が署名に通常要求される安全性のレベルである「適応的選択文書攻撃に対して存在的偽造不可」を満足するかどうかを考えると、異文書攻撃モデルでは特にこの観点で具体的な

攻撃方法が知られているわけではないが、同一文書攻撃モデルでは、ここで述べる「脆弱性」が「適応的選択文書攻撃に対して存在的偽造」となる。つまり、同一文書攻撃モデルでは ECDSA は「適応的選択文書攻撃に対して存在的偽造不可」を満足しないことになる。

なお、ECDSA は Generic Model により「適応的選択文書攻撃に対して存在的偽造不可」であるという証明が報告されているが、今回の攻撃法の発見により、このような Generic Model では、上で述べた同一文書攻撃モデルにおける安全性が考慮されていないことが明らかとなり、Generic Model による安全性証明の限界が示されたことになる。

3 Shoup による ECIES の攻撃法

Shoup により 2 種類の攻撃法が報告されている [3]。1 つ目の攻撃法は、ECIES の構成要素として共通鍵暗号に XOR 暗号（one-time padding）を用いた場合の攻撃法である（ECIES は、ハイブリッド暗号であり、共通鍵暗号およびメッセージ認証と組み合わせて利用される。このとき用いる共通鍵暗号の一典型例が XOR 暗号である）。もう 1 つは、上で述べた ECDSA の攻撃法 2（脆弱性）と同様の攻撃法であり、やはり脆弱性 (malleability) と呼ばれる。

3.1 攻撃法 1（XOR 暗号利用方式への攻撃法）

ECIES の構成要素として、共通鍵暗号として XOR 暗号を用いるものとする。このとき、選択暗号文攻撃に対して攻撃可能である（強秘匿でない）。つまり、公開鍵暗号として求められる安全性である「適応的選択暗号文攻撃に対して強秘匿 (IND-CCA2)」を満足しないことになる。

共通鍵暗号として XOR 暗号を用いたときは、$K = EK \| MK$ を kQ から鍵生成関数 KDF で生成された値とし、平文の長さに応じて EK の長さが可変となり、さらにそのプレフィックスは同じである（つまり、K のサイズが L ビットのときと L' ビットのとき、$L > L'$ ならば K の L' ビットのプレフィックスはいずれの場合も同一となる）。このとき、平文 M に対する暗号文 C は、

$$C = kQ \| EM \| MAC(MK, EM), \quad EM = EK \oplus M$$

となる。

そこで、次のような「強秘匿性に対する適応的選択暗号文攻撃」を考える。まず、敵は 2 つの平文 M_0, M_1 ($M_0 = m_0||m', M_1 = m_1||m', |m_0| = |m_1| = l, |m'| = |MK|$) を暗号オラクルに送る。暗号オラクルは、そのいずれかの平文 M_b ($b \in \{0, 1\}$) をランダムに選びその暗号文 C を敵に送る。このとき、

$$C = kQ||EM||MAC(MK, EM), \quad EM = EK \oplus M_b$$

ここで $[x]_L$ を x の L ビットのサフィックスとすると、敵は、$MK' = [EK]_{|MK|} = [C]_{|MK|} \oplus m'$ を得る。そこで敵は、$[C]^l$ を C の l ビットのプレフィックスとしたとき、$C' = kQ||[C]^l||MAC(MK', [C]^l)$ を作成し、選択暗号文攻撃として C' を復号オラクルに送る。暗号文のサイズが l ビットであるため、MAC の鍵は $MK' = [EK]_{|MK|}$ となり、C' の MAC による検証は合格となるため、復号オラクルは $[C]^l$ の復号結果である $M_b = [C]^l \oplus [EK]^l$ を敵に送る。これにより、敵は正しい b の値を得ることができる。つまり、適応的選択暗号文攻撃により強秘匿性を破ることになる。

3.2 攻撃法 2（脆弱性）

ECDSA の場合と同様に、ECIES においてデータ暗号やメッセージ認証に用いられる鍵 K は、楕円曲線上の点 kQ の x-座標のみが用いられる。従って、$-kQ$ が kQ と同じ x-座標の値を持つことより、正しい暗号文

$$C = kQ||EM||MAC(MK, EM), \quad EM = EK \oplus M_b$$

を得た敵は、別の正しい暗号文

$$C' = -kQ||EM||MAC(MK, EM), \quad EM = EK \oplus M_b$$

を作ることが可能となる。つまり、ECIES は脆弱 (malleable) であり、頑強性 (non-malleability) を満足しない。従って、公開鍵暗号に求められる安全性「適応的選択暗号文攻撃に対して強秘匿 (IND-CCA2)」を満足しないことになる。

4 その他

上で述べた特定の攻撃に関する ECDSA の安全性の観点以外で、ECDSA の安全性に関する問題として、ECDSA の仕様のバリエーションと楕円

曲線パラメータの安全性評価について述べる。

4.1 SEC1 仕様と ANSI X.9.62 仕様の差異について

ECDSA の仕様には、CRYPTREC に提案されている SEC1 仕様と、米国で標準化されている ANSI X.9.62 仕様が存在する。

CRYPTREC Report 2001 では、両者の違いは

- 推奨する楕円曲線パラメータ
- 擬似乱数生成器を指定しているか

の 2 点ということになっているが、それ以外に、以下の点が異なっていると思われる。

- ハッシュ関数 (ANSI では SHA-1 のみに限定されている。)
- 楕円曲線の位数 n のサイズがハッシュの出力サイズより小さい場合の規定が異なる。ANSI では、$e = H(M) \bmod n$ を行うのに対して、SEC1 では、$e = (H(M)$ の先頭 $|n|$ ビット) $\bmod n$ とする。

特に後者の相違点により、SEC2 で推奨している楕円曲線パラメータリストのうち 160 ビット未満のもの (例えば、128bit のものなど) では、ANSI と SEC1 で互換性がないと思われる。一方、楕円曲線のパラメータサイズが 160 ビット以上で、ハッシュ関数として SHA-1 を使う場合は、実効上は互換性があると考えられる。

4.2 安全性評価の階層について

暗号の評価では、様々な階層／レベルにおいてそれぞれの階層固有の安全性評価を行なう必要がある。例えば、ECDSA の場合では、基本的なレベル（下層）の安全性として基本問題（つまり楕円曲線上の離散対数問題）の安全性があり、その上位層の安全性としてスキーム（ECDSA）の安全性がある。

ここで、基本問題の安全性評価とスキームの安全性評価は独立の問題であり、また基本問題の安全性は上位のすべてのスキームに共通であることは明確に意識されるべきであろう。

たとえば、SEC1, SEC2 においては、どのような楕円曲線の（安全な）パラメータを選ぶべきかどうかは、全てのスキーム（ECDSA, ECDH,

ECIES）の共通の事項として記述されており、このことは明らかに ECDSA, ECDH, ECIES に限らずその他のすべての楕円曲線上のスキームにおいても共通である。

従って、CRYPTREC としては、いくつかの基本的な問題（素因数分解問題、離散対数問題、楕円曲線離散対数問題）については、各スキーム固有のパラメータとは独立に、スキーム間共通のパラメータ選定基準、推奨パラメータ等を規定すべきであると考える。たとえば、楕円曲線のパラメータについては、SEC1, SEC2 のパラメータは、各スキームに付属する推奨パラメータとして扱われているが、楕円曲線暗号系スキームに共通の規定として、安全な楕円曲線離散対数問題を構成するための推奨パラメータという扱いにすべきである。

一方、SEC1 で記述されているような広く認知されている選定基準を条件とすることは望ましいが、特定のパラメータ設計方針に偏るべきでないと考える。また、利用可能な有限体の規定も素体や 2 の拡大体といった特定の体に限定する必然性は無いと考える。例えば、IEEE P1363 では、本文でスキームの規定を行い、楕円曲線パラメータは、スキーム共通のパラメータとしてそのデータ表現も含めて Appendix で扱われており、また、一般の有限体の利用が可能となる表現方式、パラメータ設計基準が示されている。

さらに、鍵長についても、CRYPTREC としての見解を明確に提示すべきと思われる。SEC2 では、鍵長が 160 ビット未満のパラメータも推奨パラメータに含まれているが、CRYPTREC としては、このようなパラメータを推奨しないことを明示するべきと考える。実際、CRYPTREC Report 2001 では、2.2.2.3 ならびに 2.3.3 では、160 ビット以上が安全であるという記述があるにもかかわらず、2.4 では SEC2 の推奨パラメータを容認しているように思われることより、112 ビットや 128 ビット鍵が利用される余地を残している。（さらに、上で述べたように、160 ビット未満のパラメータを用いた場合は、ANSI 仕様と SEC1 仕様で互換性が保証されない。）

5 まとめ

最近発見された ECDSA の 2 つの攻撃法を中心に安全性の評価を行った。また、ECIES に対する同様の攻撃法についても、ECDSA との比較検討を行う観点より、評価を行った。

結論から述べると、ECDSA の 1 つ目の攻撃法（重複署名）は、従来の

安全性の概念に無い新しいタイプの攻撃法であるが、今回示された攻撃法は実効的な意味が無く、特に考慮する必要は無いと考える。また、もう 1 つの攻撃法（脆弱性：malleability）は、従来知られている安全性（適応的選択文書攻撃に対して存在的偽造不可）の観点で、強いモデル（同一文書攻撃モデル）において、この安全性を破るものである（つまり、偽造が可能となる）。しかし、同じ x-座標の点を用いた署名が複数ある場合はそれらを同一視するなどの運用上のルールを追加することで、この攻撃を回避することは比較的容易である。従って、実用上の問題としてはこの攻撃は深刻ではないが、運用上はこれらの攻撃が存在することを留意して対処すべきであろう。

但し、ECDSA の他の外部評価者も述べているように、もし可能であるならば安全性の証明が可能となる方式に仕様変更をすることが望ましいと考える。

一方、ECIES への攻撃は、ECDSA への攻撃法と比べると、実効上意味のある攻撃になっており、より深刻である。特に、XOR 暗号を用いた場合は、固定文書長に限定するなどの仕様変更を行う必要があり、現仕様のままでは利用を推奨できない。一方、脆弱性の問題は、ECIES が IND-CCA2 レベルの安全性を満足しないことを意味しているが、ECDSA の脆弱性の問題と同様に運用レベルで対処可能である。

なお、本文では記述しなかったが、x-座標のみを利用することによる脆弱性の問題は、CRYPTREC 最終リスト候補になっている ECDH in SEC1 にも存在することを指摘しておく。（つまり、ECDH は、DH 方式が一般的に持つ「man-in-the-middle 攻撃」に対する脆弱性のみならず、ECDH 固有の脆弱性 (malleability) を持つことになる。）

さらに、CRYPTREC の推奨暗号リスト（およびそのサポートドキュメント）においては、鍵サイズを含めた楕円曲線暗号パラメータを全ての楕円曲線暗号系スキームに共通の推奨規定として明確に規定するべきであると考える（現状では、個々のスキーム固有のパラメータと共通的パラメータの規定が混同されている）。その際、IEEE P1363 の Appendix で規定されているような広く認知されている選定基準とし、特定のパラメータ設計方針や特定の有限体に限定すべきでないと考える。

参考文献

[1] 暗号技術評価報告書（2001 年度版） CRYPTREC Report 2001, IPA and TAO (2002 年 3 月)

[2] Stern, J., Pointcheval, D., Malone-Lee, J. and Smart, N.P.: Flaws in Applying Proof Methodologies to Signature Schemes, Proc. of Crypto'02, LNCS 2442, Springer-Verlag, pp.93–110 (2002).

[3] Shoup, V.: A Proposal for an ISO Standard for Public Key Encryption, available at http://shoup.net/papers/ (2001 December).