詳細評価報告書 ECDSA

岡本 龍明　　藤岡 淳

NTT 情報流通プラットフォーム研究所

1　はじめに

本スキーム (ECDSA) は，楕円曲線上の署名関数ならびにハッシュ関数の各プリミティブを組み上げてスキームが構築されている．本報告では、プリミティブ並びにスキームの安全性を中心に評価を行なうものとする．

また，その評価については，署名スキームとして最も重要である「適応的選択文書攻撃に対して存在的偽造不可性」を有するか否かを中心に，適宜，その他の攻撃法に対する安全性を検討することとする．

但し，提出された自己評価書 (“SEC 1”) には，その点に関する詳細な記述がなされていないため，独自の評価を行っている．

2　妥当性検証

2.1　自己評価書の記述内容の解説

自己評価書の **B.3** に，以下の記述が存在する．

- 楕円曲線上の離散対数問題に対する攻撃

  仮定が破れた場合には公開鍵より秘密鍵の計算が容易となり、偽造が可能となる．

- 鍵生成に対する攻撃

  安全でない乱数生成の利用により，通常の署名システムにおける攻撃が適用可能となる．

- 鍵導出関数に対する攻撃

  いくつかの性質を満たさなければならないことを指摘している．

- 不適切な領域変数の利用に基づく攻撃

  不適切な領域変数を利用すると Pohlig-Hellman 攻撃などが可能となる．

- ハッシュ関数に対する攻撃安全でないハッシュ関数（一方向でないもしくは衝突不可能でない）を用いた場合は、ある署名文書対から別の署名文書対を偽造することが可能となる
- 不適切な公開鍵の利用に基づく攻撃

  不適切な公開鍵の利用により small subgroup 攻撃が可能となる．
- 実装攻撃

  故障依存攻撃，電力解析攻撃，タイミング解析攻撃が適用不可能なように実装すべきであることを指摘している．
- 各種変数の選択

  各種変数を選択することにより変化する効率性と安全性について述べている．

2.2 評価すべき攻撃法の設定と選択の理由

評価すべき攻撃法は，暗号学的なものから非暗号学的なものまで列挙されているが，署名スキームの安全性に関して最も重要な「適応的選択文書攻撃に対する存在的偽造不可性」については記述がほとんど無い。

3 プリミティブの安全性判定

3.1 各攻撃法に対するプリミティブの安全性判定

ここでは，プリミティブ固有の攻撃について考える．

鍵生成に対する攻撃，不適切な領域変数の利用に基づく攻撃，不適切な公開鍵の利用に基づく攻撃，実装攻撃などが一般的な攻撃にあたりこれについては，自己評価書で記述されている以外のことはここでは考慮しない．

一方，プリミティブ固有の攻撃としては，鍵導出関数に対する攻撃，ハッシュ関数に対する攻撃などがあり，特に，楕円曲線上の離散対数問題に対する攻撃などが問題となる．

まず，署名関数プリミティブとハッシュ関数プリミティブに求められている安全性の条件は一般的なものであり，十分に合理的なものである．

また，楕円曲線上の離散対数問題に関しては当然のことながら (パラメータの設定に依存する部分は存在するものの) 問題はないと考えられる．

3.2 パラメータの設定に関する判定

楕円曲線のパラメータ設定について適切なガイドライン (安全と思われる曲線のパラメータの生成法の指針) が示されている．さらに，素体上で，体のサイズが 112 ビッ

ト， 128 ビット， 160 ビット， 192 ビット， 224 ビット， 256 ビット， 384 ビット， 521 ビットのパラメータが示されている．また，同様に標数が 2 の拡大体上では，体のサイズが 113 ビット， 131 ビット， 163 ビット， 193 ビット， 233 ビット， 239 ビット， 283 ビット， 409 ビット， 571 ビットのパラメータが示されている．

これらのパラメータは，それぞれのサイズに応じて，想定される安全度が示されている．従って，利用者は望ましい安全度と処理速度や鍵長などの性能面での特質を考慮して，それぞれの利用環境に適したパラメータを選ぶことができる．例えば，素体で 160 ビットのパラメータは，安全度が 80 ビットの総当たり (80 ビットの鍵の共通鍵暗号) に対応し， 1024 ビットの素因数分解 (1024 ビットの RSA 法) や 1024 ビットの有限体上の離散対数問題 (1024 ビットの ElGamal 法) に対応する．

さらに，これらパラメータは大きく，ランダムに選択した曲線と Koblitz 曲線と呼ばれる特殊な曲線に大別される．従来の楕円曲線法への攻撃は，特殊な曲線に対して行なわれているため，ランダムな曲線は，将来起こり得る攻撃法を考慮して導入されている．一方， Koblitz 曲線は，暗号 / 復号処理を行なう際に，より高速な処理が可能となるため導入されている．

いずれのパラメータも， Shanks の BSGS 法，超特異曲線などに対する MOV 攻撃， FR 攻撃， Anomalous 曲線に対する SSSA 攻撃など現在知られている全ての攻撃法に対して安全であるように考慮されている．

なお，ここで示されたパラメータは，提案されたプリミティブやスキームに特化されたものではなく，どのような楕円曲線上の暗号 / 鍵配送 / 署名 / 認証スキーム / プリミティブで用いることが出来る．従って，ここで提案されたパラメータは，この部分単独でも各種方式に共用される情報を提供するものとして有用であろう．

4　スキームの安全性判定

4.1　組み合わせに対する攻撃法の設定とその理由

署名として最高の安全性を提供するためには，スキームとして適応的選択文書攻撃に対して存在的偽造不可性を有することが求められる．

4.2　設定した攻撃法に対する安全性の判定

ハッシュ関数を理想的なランダム関数と仮定することで、「適応的選択文書攻撃に対する存在的偽造不可性」を証明することが期待される。

しかしながら、本方式はそのような証明ができる可能性はかなり低いと言わざるを得ない。このことについては、明確な理論的な根拠がある訳ではないが、既に証明がついている類似の方式との比較から得られた結論である。

一方、本方式は既に利用実績が十分にあるにもかかわらず、「適応的選択文書攻撃に

対する存在的偽造不可性」であることを否定するような攻撃法は一切報告されていないことより、この意味での安全上の問題は無いように思われる。

4.3 パラメータの設定に関する判定

楕円曲線上の暗号方式の安全性は，最も基本的なレベルとして，楕円曲線上の離散対数問題 (ECDLP) に基づいている．一般に ECDLP は，そのベースポイントの位数の平方根のオーダーの攻撃 (Shanks の BSGS 法など) が最も効率が良いものされてきたため，大雑把に言うと，例えば，160 ビットの素体上の ECDLP の最も効率的な攻撃は，80 ビットの総当たり (つまり，80 ビットの鍵の共通鍵暗号の攻撃) ならびに，1024 ビットの素因数分解 (1024 ビットの RSA 法) や 1024 ビットの有限体上の離散対数問題 (1024 ビットの ElGamal 法) を解くことに相当すると考えられている．

しかし，特殊な曲線に対してはより効率の良い攻撃が知られている．現在，知られている攻撃は，大きく 2 つあり，有限体上の乗法群の離散対数問題に帰着させる方法と有限体上の加法群の離散対数問題 (つまり，単なる割算) に帰着させる方法である．前者は，超特異曲線などに対する MOV 攻撃や FR 攻撃が該当し，後者は Anomalous 曲線に対する SSSA 攻撃が該当する．従って，楕円曲線のパラメータを選択する場合は，これら攻撃法が適用できないような曲線を選ぶ必要がある．幸い，曲線をランダムに選べば，圧倒的な確率でこれらの攻撃に対して安全な曲線となる．

現在知られている攻撃法の観点で，本提案で示された楕円曲線のパラメータ設定のガイドラインは適切であると思われる．さらに，具体的に示された一連のパラメータの具体的データは適切に選択されていると思われる．これらパラメータは，利用者が希望する各種安全度に対応して，素体上で，体のサイズが 112 ビット，128 ビット，160 ビット，192 ビット，224 ビット，256 ビット，384 ビット，521 ビットのパラメータが示されている．また，同様に標数が 2 の拡大体上では，体のサイズが 113 ビット，131 ビット，163 ビット，193 ビット，233 ビット，239 ビット，283 ビット，409 ビット，571 ビットのパラメータが示されている．これらの鍵サイズの選択およびパラメータの種類は適切に選択されていると思われる．

さらに，これらパラメータは大きく，ランダムに選択した曲線と Koblitz 曲線と呼ばれる特殊な曲線に大別される．現在での高速実現を考慮すれば，Koblitz 曲線を利用する実用的意義が認められ，また将来への安全性を重視するならばランダム曲線の意義は十分にあり，いずれのタイプの曲線もそれぞれ実用的な意義が認められる．従って，利用者の使う環境や目的に応じて両タイプの曲線パラメータを提供することは適切であると考える．

ランダムに選ばれた曲線は，恣意的に選ばれた曲線でないことを示すため，乱数の種となるシード情報からハッシュ関数で変換して得られた値を用いて曲線のパラメータを定めるようにしている．このような工夫は，曲線がランダムに選ばれたことを示す上で

有効であると思われる．

なお，ここで示されたパラメータは，提案されたプリミティブやスキームに特化されたものではなく，どのような楕円曲線上の暗号 / 鍵配送 / 署名 / 認証スキーム / プリミティブで用いることが出来る．従って，ここで提案されたパラメータは，この部分単独でも各種方式に共用される情報を提供するものとして有用であると思われる．

5　まとめ

本方式は、何らかの妥当な仮定の下で「適応的選択文書攻撃に対する存在的偽造不可性」である理論的な保証は示されていない。しかしながら、既に利用実績が十分にあるにもかかわらず、「適応的選択文書攻撃に対する存在的偽造不可性」であることを否定するような攻撃法は現在までに報告されていないことより、スキームとしての安全上の問題は無いように思われる。

A　全体概要

A.1　日本語

本自己評価書には、提案方式 (ECDSA) が何らかの妥当な仮定の下で「適応的選択文書攻撃に対する存在的偽造不可性」であるような理論的な保証は示されていない。しかしながら、既に利用実績が十分にあるにもかかわらず、「適応的選択文書攻撃に対する存在的偽造不可性」であることを否定するような攻撃法は現在までに報告されていない。従って、本方式はスキームとしての安全上の問題は無いように思われる。

一方、基本的な仮定（楕円離散対数問題の困難性）を保証するためのパラメータ設定指針や具体的パラメータが適切に示されている。

A.2　英語

The self evaluation report does not show that the proposed scheme (ECDSA) is “existentially unforgeable against adaptive chosen message attacks”. However, no effective attacks have been reported although it has been used very widely. Thus, there seems no problem in security of this scheme.

On the other hand, in order to guarantee the security of the underlying primitive problem (intractability of the elliptic curve discrete logarithm), an appropriate policy for parameter selection and concrete parameters are provided.