# 詳細評価報告書 ECAES

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

本報告で詳細評価する対象暗号 (ECAES) では，鍵共有，暗号化，データ認証の各プリミティブを組み上げて公開鍵暗号スキームが構築されている．データの暗号化及び認証の部分は，それぞれ共通鍵暗号プリミティブとメッセージ認証子プリミティブを直接用いており，それぞれの安全性に依存している．そこで，本報告では，鍵共有に関わる Diffie-Hellman 鍵共有とハッシュ関数に関する部分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，暗号として最も重要である適応的選択暗号文攻撃に対して強秘匿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，詳細な記述がなされていないため，これら安全性の解析については，適宜，自己評価書における引用文献 [1] (“DHAES”) により内容を補完して行なった．

## 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.4** に，以下の記述が存在する．

- 選択平文攻撃と選択暗号分攻撃についての耐性

  Diffie-Hellman 仮定の変種に安全性を帰着している．

- 楕円曲線上の離散対数問題及び Diffie-Hellman 問題に対する攻撃

  仮定が破れた場合には共有情報が入手可能となる．

- 鍵生成に対する攻撃

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

- 共通鍵暗号に対する攻撃

  安全でないプリミティブを用いた場合は，平文情報が漏洩する危険を指摘している．

- メッセージ認証子に対する攻撃

  安全でないプリミティブを用いた場合は，選択暗号文攻撃が可能となってしまう．

- 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．

- 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の関連について述べられている．

### 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十分に網羅されており，その選択の理由について問題は見い出せない．

但し，暗号学的なもの関しては，その安全性の根拠 (数学的な証明) を引用文献 [1] に依存しているために，その正当性をこの自己評価書からのみ判定することは困難である．

## 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

暗号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暗号文攻撃に対して頑強性を有することが求められる．しかしながら，適応的選択暗号文攻撃下では，頑強性は強秘匿性と一致することが知られているので，本報告では考察の容易な強秘匿性を中心に詳細評価を行なうものとする．

以下，一般的な攻撃とプリミティブ固有の攻撃に分けて考える．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，共通鍵暗号に対する攻撃，メッセージ認証子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及び Diffie-Hellman 問題に対する攻撃と適応的攻撃時の耐性が問題となる．

まず，共通鍵暗号プリミティブとメッセージ認証子プリミティブは，それぞれ，適応的攻撃に対して耐性を有することが求められている．対象スキームで用いられるこれらプリミティブは一般的なものであり，これらの条件は十分に合理的なものである．

次に，鍵共有プリミティブは Diffie-Hellman 鍵共有プリミティブとハッシュ関数に依存している．鍵共有プリミティブとしての安全性は自己評価書には陽に記述されていないが，引用文献 [1] に述べられているハッシュ Diffie-Hellman 仮定がそれに相当している．このハッシュ Diffie-Hellman 仮定は，通常知られている計算 Diffie-Hellman 仮定と決定 Diffie-Hellman 仮定の中間に位置するものであり，計算 Diffie-Hellman 仮定よりは強い仮定であるが，決定 Diffie-Hellman 仮定よりは弱い．

### 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 (“SEC 2”)．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

プリミティブの安全性判定の項でも述べたように，適応的選択暗号文攻撃の元で暗号として最高の安全性を提供するには，強秘匿性を検証すれば十分である．

よって，ここでは適応的選択暗号文攻撃に対する耐性を検証する．また，補足として，選択平文攻撃と非適応的選択暗号文攻撃に対する耐性についても述べる．

### 4.2　設定した攻撃法に対する安全性の判定

対象スキームは，以下の三つの仮定

- ハッシュ Diffie-Hellman 仮定
- 非適応的ハッシュ Diffie-Hellman 独立仮定
- 適応的ハッシュ Diffie-Hellman 独立仮定

を用いており，それぞれ，

- 選択平文攻撃
- 非適応的選択暗号文攻撃
- 適応的選択暗号文攻撃

に対する強秘匿性と関係している．

より正確には，選択平文攻撃に対する安全性は，ハッシュ Diffie-Hellman 仮定と共通鍵暗号プリミティブの安全性に依存している．即ち，対象スキームを選択平文攻撃の元で強秘匿性を破ることができたならば，ハッシュ Diffie-Hellman 仮定か共通鍵暗号プリミティブの安全性を破ることができることが証明されている (引用文献 [1] を参照のこと)．同様に，非適応的選択暗号文攻撃に対する安全性は，非適応的ハッシュ Diffie-Hellman 独立仮定と共通鍵暗号プリミティブの安全性に依存しており，適応的選択暗号文攻撃に対する安全性は，適応的ハッシュ Diffie-Hellman 独立仮定と共通鍵暗号プ

リミティブの安全性とメッセージ認証子プリミティブの安全性に依存している (引用文献 [1] を参照のこと).

また，鍵が共有された状況下で，共通鍵暗号プリミティブとメッセージ認証子プリミティブから構築された共通鍵暗号スキームの安全性に関しては， Bellare と Namprempre により考察されている (Bellare, Namprempre: “Authenticated Encryption”, Asiacrypt ’00) が，これにより対象スキームの構成法が強秘匿性と完全性を満たすことが示される.

以上のことから，対象スキームの安全性の証明は十分に信頼に足るものであると結論付けることができる.

プリミティブの安全性の項で述べたように，ハッシュ Diffie-Hellman 仮定は，計算 Diffie-Hellman 仮定と決定 Diffie-Hellman 仮定の中間に位置している (計算 Diffie-Hellman 仮定よりは強い仮定であるが，決定 Diffie-Hellman 仮定よりは弱い). そのため，対象スキームの選択平文攻撃下での安全性は，信頼することができる.

しかしながら，非適応的ハッシュ Diffie-Hellman 独立仮定と適応的ハッシュ Diffie-Hellman 独立仮定については，既存の仮定の相関関係は不明であり，現時点で，既存の仮定と同等に扱うには注意が必要である. よって，非適応的 / 適応的選択暗号文攻撃における対象スキームの安全性は条件付きで保証されているものと考えるべきである.

特に，オラクル (oracle) を導入しても問題の難しさが変化しないという仮定を導入する手法は，最近のものであるために，従来からの定式化との整合性を十分に検討する必要があるものと考えられる. 現時点では，その信頼性を損なうほどの疑問がある仮定ではないが，定式化されて間もない仮定であるために今後の研究動向を注意すべきである.

### 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，対象スキームで示されている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

自己評価書で記述されている攻撃法は，暗号学的なものから非暗号学的なものまで十分に網羅されており，その選択の理由については問題を見い出せない．

対象スキームは，以下の三つの仮定

- ハッシュ Diffie-Hellman 仮定
- 非適応的ハッシュ Diffie-Hellman 独立仮定
- 適応的ハッシュ Diffie-Hellman 独立仮定

を用いており，それぞれ，

- 選択平文攻撃
- 非適応的選択暗号文攻撃
- 適応的選択暗号文攻撃

に対する耐性と関係している．

ハッシュ Diffie-Hellman 仮定は，計算 Diffie-Hellman 仮定と決定 Diffie-Hellman 仮定の中間に位置している (計算 Diffie-Hellman 仮定よりは強い仮定であるが，決定 Diffie-Hellman 仮定よりは弱い)．そのため，対象スキームの選択平文攻撃下での安全性は，信頼するに足るものであると結論付けることができる．

しかしながら，非適応的ハッシュ Diffie-Hellman 独立仮定と適応的ハッシュ Diffie-Hellman 独立仮定については，既存の仮定の相関関係は不明であり，現時点で，既存の仮定と同等に扱うには注意が必要である．よって，非適応的 / 適応的選択暗号文攻撃における対象スキームの安全性は条件付きで保証されているものと考えるべきである．

### 5.1 補足

対象スキームにおける暗号化の手順 (**5.1.3**) において，送信者は楕円曲線 'standard' Diffie-Hellman プリミティブと楕円曲線 cofactor Diffie-Hellman プリミティブのどちらか選択して利用している (**Actions:** 3) が，この選択に関する識別子が受信者に対して送られていないため，正しく復号できないおそれがある (**5.1.4**, **Actions:** 3)．これは仕様の不備であり，選択したプリミティブに関する識別子を送信するように仕様を変更すべきである．

# A　全体概要

## A.1　日本語

自己評価書で記述されている攻撃法は，暗号学的なものから非暗号学的なものまで十分に網羅されており，その選択の理由については問題を見い出せない．また，パラメータ設定指針や具体的パラメータも適切に示されている．

また，本詳細評価では，適応的選択暗号文攻撃に対する強秘匿性を中心に検証している．これは，暗号として最高の安全性を提供するためには，適応的選択暗号文攻撃に対する耐性を検証すれば十分だからである (適応的選択暗号文攻撃の元では強秘匿性と頑強性が同値となる)．

対象スキームは，三つの仮定: ハッシュ Diffie-Hellman 仮定，非適応的ハッシュ Diffie-Hellman 独立仮定，適応的ハッシュ Diffie-Hellman 独立仮定を用いており，それぞれ，選択平文攻撃，非適応的選択暗号文攻撃，適応的選択暗号文攻撃に対する耐性と関係している．

ハッシュ Diffie-Hellman 仮定は，計算 Diffie-Hellman 仮定と決定 Diffie-Hellman 仮定の中間に位置している (計算 Diffie-Hellman 仮定よりは強い仮定であるが，決定 Diffie-Hellman 仮定よりは弱い)．そのため，対象スキームの選択平文攻撃下での安全性は，信頼するに足るものであると結論付けることができる．

しかしながら，非適応的ハッシュ Diffie-Hellman 独立仮定と適応的ハッシュ Diffie-Hellman 独立仮定については，既存の仮定の相関関係は不明であり，現時点で，既存の仮定と同等に扱うには注意が必要である．よって，非適応的 / 適応的選択暗号文攻撃における対象スキームの安全性は条件付きで保証されているものと考えるべきである．

## A.2　英語

The self evaluation report mentions several cryptographic and non-cryptographic attacks, and it can be concluded that the described criteria in it are fair. In addition, an appropriate policy for parameter selection and concrete parameters are provided.

This detail evaluation report concentrates the indistinguishability against adaptive chosen ciphertext attacks as the encryption scheme must have the non-malleability to ensure the strongest security and the non-malleability coincides the indistinguishability under the attack.

This scheme is based on the following three assumptions: Hash Diffie-Hellman assumption, non-adaptive Hash Diffie-Hellman independence assumption, and adaptive Hash Diffie-Hellman independence assumption, and each assumptions are related to the security against chosen plaintext attacks, non-adaptive chosen cipher-

text attacks, and adaptive chosen ciphertext attacks, respectively.

In the complexity theory, the Hash Diffie-Hellman assumption is located between the computational Diffie-Hellman assumption and the decisional Diffie-Hellman assumption, i.e. it is stronger than the computational Diffie-Hellman assumption but weaker than the decisional Diffie-Hellman assumption. So this scheme has reasonable security under chosen plaintext attacks.

However, there is no research regarding relations among the non-adaptive Hash Diffie-Hellman independence assumption, the adaptive Hash Diffie-Hellman independence assumption, and other well-known assumptions. So the scheme has, in some sense, conditional security against non-adaptive/adaptive chosen ciphertext attacks.