PSEC 暗号アルゴリズムの詳細評価報告書

平成 13 年 1 月 12 日

1 はじめに 1
2 基本暗号(暗号プリミティブ)に関する安全性評価 1
2.1 安全性の根拠となる問題について 1
2.2 楕円曲線のパラメータの安全性 1
2.3 まとめ 2
3 PSEC 暗号方式 (暗号スキーム) の安全性評価 2
3.1 ランダムオラクルモデル 2
3.2 安全性の分類 3
3.3 PSEC-1 の安全性評価 3
3.3.1 PSEC-1 の概要 3
3.3.2 PSEC-1 の安全性 3
3.4 PSEC-2 の安全性評価 5
3.4.1 PSEC-2 の概要 6
3.4.2 PSEC-2 の安全性 6
3.5 PSEC-3 の安全性評価 8
3.5.1 PSEC-3 の概要 8
3.5.2 PSEC-3 の安全性 8
3.6 まとめ 10
4 おわりに 11
参考文献 11

1 はじめに

本報告書は、PSEC 暗号の安全性評価の結果をまとめたものである。

今回の評価では以下の資料を使用した。

- PSEC 暗号仕様書
- PSEC 暗号自己評価書
- スクリーニング評価結果のコメント

ただし、これらは、IPA から、2000 年 11 月 13 日に送付された CD-R に含まれているものである。

以下では、2 章に基本暗号に関する安全性評価の結果を示し、3 章にスキームに関する安全性評価の結果を示す。

なお、PSEC 暗号の仕様書の 4.1, 6.1, 7.1, 8.1 節の定義「qLen:=¦Fq¦」(Fq の位数)は、qLen が q であることを表しているが、同仕様書の 14 ページに「q のサイズを 160bits」、「qLen=160」と書かれており矛盾している。評価者は、この定義が誤っていると考え、「qLen:=¦q¦」(q のビットサイズ)と認識して、安全性評価を行う。

2 基本暗号(暗号プリミティブ)に関する安全性評価

2.1 安全性の根拠となる問題について

提案者の暗号仕様書によれば、PSEC 暗号の暗号プリミティブは楕円 ElGamal 暗号である。楕円 ElGamal 暗号は、ECDLP を安全性の根拠としている。そのため、評価者は PSEC 暗号の暗号プリミティブも ECDLP を安全性の根拠としていると考えて、安全性評価を行う。

2.2 楕円曲線のパラメータの安全性

ここでは、ECDLP が困難であることを「楕円曲線のパラメータが安全」であると考えて、楕円曲線のパラメータの安全性について評価する。

PSEC 暗号仕様書において、楕円曲線のパラメータは見当たらないので、個々のパラメータに対して安全性評価を行うことができない。楕円曲線の生成方法については、IEEE P1363 の Working Draft の Annex A.12.4～7[IEEE]に従うことが書かれている。以下では、この生成方法について安全性評価を行う。

IEEE P1363 の擬似ランダムな楕円曲線生成アルゴリズムは、ANSI X.9.62-1998(ECDSA)[ANSI]に書かれているもので、擬似的にランダム性をもった楕円曲線(のパラメータ)とそれを検証するための乱数値を出力する。これらの出力を用いて、同じ文献の検証アルゴリズムで(ANSI X.9.62)の生成アルゴリズムを使用して生成していることを検証できる。安全性を達成するための条件判定は、Pollard ρ アルゴリズム[Pol]、Pohlig-Hellman アルゴリズム[Poh]に対して、安全になるための「楕円曲線の位数が almost prime であること」のみである。MOV[MOV], FR[FR] reduction attack に対しての FR(MOV) condition, SSSA

attack[Sma,Sat,Sem]に対しての condition(楕円曲線の位数が q_0 で割り切れない。ただし、q_0 は楕円曲線の定義体の標数)、標数 2 などの拡大体上の楕円曲線の場合の Weil Decent attack[Gal,Gau]に対する判定(拡大次数が素数である)などの判定は行っていない。したがって、これらの攻撃で(多項式時間で)解ける可能性がある。PSEC 暗号仕様書どおり（すなわち、IEEE P1363 のアルゴリズムどおり）に生成すると安全性に問題がある。

なお、文献[NIST]では、上記の攻撃を考慮した推奨パラメータが示されている。

2.3 まとめ

PSEC 暗号のプリミティブは、楕円 ElGamal 暗号である。楕円 ElGamal 暗号は、ECDLP を安全性の根拠としているため、評価者は、楕円曲線パラメータの安全性について評価を行った。その結果、PSEC 暗号仕様書には、楕円曲線のパラメータの記述が見当たらなかった。また、PSEC 暗号仕様書に記載の楕円曲線の生成方法は、安全性に問題があるパラメータを生成する可能性がある。

3 PSEC 暗号方式（暗号スキーム）の安全性評価

PSEC 暗号方式には、PSEC-1、PSEC-2、及び PSEC-3 の 3 つの暗号スキームがある。それぞれについて、暗号プリミティブには安全性に問題はないものとして以下で評価を行う。

まず、安全性の評価を行う前に、PSEC 暗号方式の安全性の議論で用いているランダムオラクルモデルと、安全性の分類について説明する。

3.1 ランダムオラクルモデル

暗号化時や復号時にハッシュ関数を用いる暗号スキームにおいて、そのハッシュ関数が理想的なランダム関数であると仮定する場合、その暗号スキームはランダムオラクルモデルの下で定義される、と言う。

このランダムオラクルモデルの下で、暗号スキームの安全性が理論的に証明できる場合がある。厳密な意味で、理想的なランダム関数であると証明されているハッシュ関数は、現時点では存在しないが、実用的な意味では、例えば SHA-1 のようなハッシュ関数は、理想的なランダム関数としてみなせると信じられている。

従って、このランダムオラクルモデルの概念は、暗号スキームの安全性証明の有効な手法として知られている。

PSEC 暗号方式の提案者は、この概念を用いて、暗号スキームで用いるハッシュ関数が理想的なランダム関数であると仮定して、暗号スキーム全体の安全性を理論的に証明し、実際には、ハッシュ関数として、理想的なランダム関数の代わりに SHA-1 を用いた暗号スキームの実現例を挙げている。

3.2 安全性の分類

攻撃に対する暗号スキームの安全性は、攻撃者の能力、及び達成する暗号スキームの耐性によって分類される（文献[BDPR]参照）。

簡単に説明すると、

攻撃者の能力として、

1. 受動攻撃ができる攻撃者
2. 選択暗号文攻撃ができる攻撃者
3. 適応的選択暗号文攻撃ができる攻撃者

また、達成する暗号スキームの耐性として、多項式時間で、

A) 暗号文から、平文を解読することができない（一方向性）。

B) 暗号文から、平文の部分情報を解読することができない（強秘匿性）。

C) 暗号文から、中の平文を改竄した新たな暗号文を作成できない（頑健性）。

という分類をしたときに、攻撃者の能力と達成する暗号スキームの耐性によって、暗号スキームの安全性を分類することができる。攻撃者の能力は、1 から 3 の順に強力になり、また暗号スキームの耐性は、A から C の順に高くなる。

従って、適応的選択暗号文攻撃ができる最も強力な攻撃者が攻撃を行っても、多項式時間では、中の平文を改竄した新たな暗号文を作成することさえできない、頑健性をもつ暗号スキームが、最も安全な暗号スキームであるということができる。

ここで、適応的選択暗号文攻撃に対し、強秘匿性を有することと頑健性を有することは等価であることが知られているので、暗号スキームが適応的選択暗号文攻撃に対し強秘匿性を有すれば、その暗号スキームは、最も安全であるということができる。

提案者は、PSEC 暗号方式が、適応的選択暗号文攻撃に対し強秘匿性をもつ、すなわち、最強の攻撃者に対しても、最高の耐性をもつ安全な暗号スキームであることを主張している。

そこで、評価者は、提案者の主張が正しいかどうかを検証することにより、提案者の主張通りの安全性を有するかどうかの検討を行い、これを PSEC 暗号方式の安全性の評価とする。

3.3 PSEC-1 の安全性評価

PSEC-1 の安全性の評価を以下に述べる。

3.3.1 PSEC-1 の概要

PSEC-1 は、楕円 ElGamal 暗号を基に、文献[FO1]の手法により設計された暗号方式と捉えられる。

3.3.2 PSEC-1 の安全性

提案者は、PSEC-1 の鍵生成時に、公開鍵パラメータである rLen と hLen については、

mLen+rLen≦qLen,　hLen≦pLen

の条件のみを満たすよう生成しており、安全性の議論においては、さらにパラメータを

rLen≧c_0 pLen (c_0：定数) かつ、hLen=pLen-1　　(1)

と制限した場合の PSEC-1 の安全性について言及している。

そこで、評価者は、パラメータに上記(1)の制限を適用した PSEC-1 の安全性の議論を行う。

その結果、PSEC-1 は、楕円 Diffie-Hellman 部分決定問題が計算困難であれば、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿であると結論付けることができる。

以下でそのことを説明する。

提案者は、文献[FO1]において、以下の定理を示している。

定理 (文献[FO1])

公開鍵 pk と秘密鍵 sk を生成する鍵生成関数 K、暗号化関数 E、及び復号関数 D をもつ公開鍵暗号システム A=(K,E,D)について、暗号化関数 $E_{pk}(M,R)$ (M：平文、R：乱数、pk：公開鍵)、及び復号関数 $D_{sk}(C)$ (C：暗号文、sk：秘密鍵) を

$E:\{0,1\}^{k+k0} \times \{0,1\}^{l} \rightarrow \{0,1\}^{n}$

$D:\{0,1\}^{n} \rightarrow \{0,1\}^{k+k0}$

(ある多項式 ρ と十分大きい k に対し、k_0, n, l ≦ ρ(k) とする。)

とすると、新しい公開鍵暗号システム B=(K',E',D')が以下のように定義できる。

$E':\{0,1\}^{k} \times \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$

$E'_{pk}(m,r) := E_{pk}(m||r, H(m||r))$　($|m|=k$, $|r|=k_0$, H：ハッシュ関数)

$D':\{0,1\}^{n} \rightarrow \{0,1\}^{k}$

$D'_{sk}(c) := D_{sk}(c)$の上位 k ビット ($c=E_{pk}(D_{sk}(c), H(D_{sk}(c)))$ の場合)

もしくは、出力なし (その他の場合)。

いま、ランダムオラクルモデルの下で、公開鍵暗号システム B に、適応的選択暗号文攻撃に対し、確率 ε で強秘匿性を破る攻撃者が存在すれば、公開鍵暗号システム A に、選択平文攻撃に対し、次の確率 ε' で強秘匿性を破る攻撃者が存在する。

$$\varepsilon' = (\varepsilon - q_H \cdot 2^{-(k_0-1)}) \cdot (1-2^{-l_0})^{q_D}$$

ここで、q_H, q_D は、それぞれ攻撃者がハッシュ関数 H、復号オラクルを用いる回数であり、

$$l_0 = \log_2 (\min_{x\in\{0.1\}^{k+k_0}} [\#\{\mathrm{E}_{\mathrm{pk}}(x,r) \mid r \in \{0,1\}^{l}\}])$$

である。

評価者は、時間的制約のため、この定理の正当性を完全に検証することができなかった。従って、この定理が正しいとみなしたときの PSEC-1 の評価を以下に記述する。

PSEC-1 は、楕円 ElGamal 暗号を基に、上記定理の手法により作られる暗号方式であるので、上記確率 ε ’を考えると、乱数成分のビット長は k_0=rLen であり、すなわち確率 ε ’は、

$$\varepsilon' = (\varepsilon - q_H \cdot 2^{-(\mathrm{rLen}-1)}) \cdot (1 - 2^{-l_0})^{q_D}$$

となる。

ここで、rLen≧c_0 pLen=c_0 k であるので、

$$\varepsilon' \geq (\varepsilon - q_H \cdot 2^{-(c_0 k-1)}) \cdot (1 - 2^{-l_0})^{q_D}$$

さらに、l_0 は、PSEC-1 において、平文を固定したときの暗号文のとりうる値の数の最小値のビット数であり、PSEC-1 は楕円 ElGamal 暗号を基にしていることを考えると、hLen=pLen-1=k-1 なので、$l_0 = O(l) = O(\mathrm{hLen}) = O(k)$ となる。

従って、セキュリティパラメータ k を、暗号仕様書に記載の推奨パラメータ程度に大きくすると、確率 ε ’は ε と漸近的に等しくなる。

また、PSEC-1 において、暗号プリミティブである楕円 ElGamal 暗号の乱数に対応するハッシュ関数値 h は、楕円曲線上の点 P のスカラ倍 hP に使われるが、ハッシュ関数値のビット数 hLen は、hLen=pLen-1 なので、ハッシュ関数値は Zp の中から選ばれるようになっており、これは、暗号プリミティブである楕円 ElGamal 暗号の乱数のパラメータ条件を満たす。ただし、楕円 ElGamal 暗号は、乱数は Zp 全体から選ばれるのに対し、PSEC-1 ではハッシュ関数値は Zp 全体から選ばれるわけではない。しかし、現時点でこのことを利用した攻撃法は知られていないので、評価者は、この点については安全性に問題はないと考える。

以上により、PSEC-1 に、適応的選択暗号文攻撃に対し、確率 ε で強秘匿性を破る攻撃者が存在すれば、楕円 ElGamal 暗号に、選択平文攻撃に対し、ε に近い確率 ε ’で強秘匿性を破る攻撃者が存在することになる。

いま、楕円 ElGamal 暗号は、楕円 Diffie-Hellman 決定問題が計算困難であると仮定すると、選択平文攻撃に対して強秘匿であることが知られている（例えば、文献[BG]参照）。また、上記定理による手法は、復号時に楕円離散対数問題の部分問題を解いていることを考えると、楕円 Diffie-Hellman 部分決定問題が計算困難であると仮定すれば、ランダムオラクルモデルの下で、PSEC-1 は適応的選択暗号文攻撃に対し、強秘匿であると評価することができる。

なお、安全性検証のために用いた、楕円 Diffie-Hellman 決定問題の計算困難性の仮定であるが、長い間研究されてきているにも関わらず、現時点では多項式時間アルゴリズムが見つかっていないことから、現時点において、評価者は、これを妥当な仮定であると考える。

3.4 PSEC-2 の安全性評価

PSEC-2 の安全性の評価を以下に述べる。

3.4.1 PSEC-2 の概要

PSEC-2 は、楕円 ElGamal 暗号を基に、文献[FO2]の手法により設計された暗号方式と捉えられる。

3.4.2 PSEC-2 の安全性

提案者は、PSEC-2 の鍵生成時に、公開鍵パラメータである rLen と hLen については、

rLen≦qLen

の条件のみを満たすように生成しており、安全性の議論においては、さらにパラメータを

rLen=qLen-1 かつ、hLen=pLen-1　　(2)

と制限して、共通鍵暗号として受動的攻撃に対し安全であるものを用いた場合の PSEC-2 の安全性について言及している。

そこで、評価者は、パラメータに上記(2)の制限を適用し、かつ用いる共通鍵暗号は受動的攻撃に対し安全であるとしたときの PSEC-2 の安全性の議論を行う。

その結果、PSEC-2 は、楕円 Diffie-Hellman 問題が計算困難であれば、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿であるとは結論付けられなかった。

以下でそのことを説明する。

提案者は、文献[FO2]において、以下の定理を示している。

定理（文献[FO2]）

公開鍵 pk と秘密鍵 sk を生成する鍵生成関数 K、暗号化関数 E、及び復号関数 D をもつ公開鍵暗号システム A=(K,E,D)の、暗号化関数 $E_{pk}(M,R)$（M：平文、R：乱数、pk：公開鍵）、及び復号関数 $D_{sk}(C)$（C：暗号文、sk：秘密鍵）と、暗号化関数 SymE、及び復号関数 SymD をもつ共通鍵暗号システム S=(SymE,SymD)の、暗号化関数 $SymE_K(M)$（M：平文、K：共通鍵）、及び復号関数 $SymD_K(C)$（C：暗号文、K：共通鍵）を用いると、新しい公開鍵暗号システム B=(K',E',D')が以下のように定義できる。

$E'_{pk}(m,r) := E_{pk}(r, H(r||m)) \,||\, SymE_{G(r)}(m)$

$D'_{sk}(c_1||c_2) := SymD_{G(r')}(c_2)$（$c_1=E_{pk}(r', H(r'||m'))$ の場合）

もしくは、出力なし（その他の場合）。

ここで、$r'=D_{sk}(c_1)$、$m'=SymD_{G(r')}(c_2)$。

いま、公開鍵暗号システム A が、受動的攻撃に対し確率 ε_1 で一方向性を有し、共通鍵暗号システム S が、受動的攻撃に対し、確率 ε_2 で安全であれば、ランダムオラクルモデルの下で、公開鍵暗号システム B は、適応的選択暗号文攻撃に対し、以下の確率 ε で強秘匿性を有する。

$$\varepsilon = (2(q_G + q_H)\varepsilon_1 + \varepsilon_2 + 1)(1 - 2\varepsilon_1 - 2\varepsilon_2 - \gamma - 2^{-l})^{-q_D} - 1$$

ここで、q_H, q_G, q_D は、それぞれ攻撃者がハッシュ関数 H、ハッシュ関数 G、復号オラクルを用いる

回数であり、l は、共通鍵暗号で暗号化できる平文のビット数であり、γ は、公開鍵暗号システム A に関し、固定した平文に対し、ランダムに暗号文を選んだときに、それが正しい平文、暗号文対になる確率の最大値を表す。

評価者は、時間的制約のため、この定理の正当性を完全に検証することができなかった。従って、この定理が正しいとみなしたときの PSEC-2 の評価を以下に記述する。

PSEC-2 は、楕円 ElGamal 暗号を基に、上記定理の手法により作られる暗号方式であるので、上記確率 ε を考えると、平文のビット長は l=mLen であり、すなわち確率 ε は、

$$\varepsilon = (2(q_G + q_H)\varepsilon_1 + \varepsilon_2 + 1)(1 - 2\varepsilon_1 - 2\varepsilon_2 - \gamma - 2^{-\mathrm{mLen}})^{-q_D} - 1$$

となる。

ここで、固定した平文に対し、ランダムに暗号文を選んだときに、それが正しい平文、暗号文対になる確率の最大値 γ は、楕円 ElGamal 暗号を暗号プリミティブとしており、$2^{-\mathrm{hLen}}$ であるので、

$$\varepsilon = (2(q_G + q_H)\varepsilon_1 + \varepsilon_2 + 1)(1 - 2\varepsilon_1 - 2\varepsilon_2 - 2^{-\mathrm{hLen}} - 2^{-\mathrm{mLen}})^{-q_D} - 1$$

となる。

また、PSEC-2 において、暗号プリミティブである楕円 ElGamal 暗号の乱数に対応するハッシュ関数値 h は、楕円曲線上の点 P のスカラ倍 hP に使われるが、ハッシュ関数値のビット数 hLen は、hLen=pLen-1 なので、ハッシュ関数値は Zp の中から選ばれるようになっており、また、楕円 ElGamal 暗号の平文に対応する乱数 r は、楕円曲線上の点の X 座標との演算に使われるが、乱数のビット数 rLen は、rLen=qLen-1 なので、乱数は Zq の中から選ばれるようになっていて、これらは、暗号プリミティブである楕円 ElGamal 暗号の乱数と平文の条件を満たす。ただし、楕円 ElGamal 暗号は、乱数及び平文はそれぞれ Zp 全体、Zq 全体から選ばれるのに対し、PSEC-2 ではハッシュ関数値及び乱数はそれぞれ Zp 全体、Zq 全体から選ばれるわけではない。しかし、現時点でこのことを利用した攻撃法は知られていないので、評価者は、この点については安全性に問題はないと考える。

いま、楕円 ElGamal 暗号は、楕円 Diffie-Hellman 問題が計算困難であると仮定すると、受動的攻撃に対して一方向性を有することが知られている（例えば、文献[SS]参照）。なお、安全性保証のために用いる、楕円 Diffie-Helmman 問題の計算困難性の仮定であるが、長い間研究されてきているにも関わらず、現時点では多項式時間アルゴリズムが見つかっていないことから、現時点において、評価者は、これを妥当な仮定であると考える。

また、共通鍵暗号が受動的攻撃に対し安全であるとは、文献[FO2]に定義されているが、簡単に説明すると、平文対 m1,m2 に対して、そのどちらかの暗号文を与えられたとき、共通鍵を知らない攻撃者は、どちらの暗号文であるかを判別することができない、ということである。例えば、1 ビットの平文を暗号化するバーナム暗号は、共通鍵を知らない攻撃者は、暗号文から平文が 0

か 1 かを判別することはできないので、受動的攻撃に対し安全である。

PSEC-2 では、共通鍵暗号はこのような性質をもつ、受動的攻撃に対して安全なものを用いている。

従って、楕円 Diffie-Helmman 問題が計算困難であると仮定すると、ε_1 及び ε_2 は無視できる確率、すなわち全ての定数 c と十分大きいセキュリティパラメータ k に対し、$1/k^c$ よりも小さい確率である。

しかしながら、上記確率 ε を考えると、確率 ε は無視できる確率となるとは限らない。

例えば、共通鍵暗号として 1 ビットの平文を暗号化するバーナム暗号を用いた場合、mLen=1 となり、攻撃者は復号オラクルを多項式回用いることが可能なので、

$$(1-2\varepsilon_1-2\varepsilon_2-2^{-\mathrm{hLen}}-2^{-\mathrm{mLen}})^{-q_D}$$

の値が大きくなり、確率 ε が大きくなる場合がある。

暗号仕様書と暗号自己評価書によれば、パラメータ設定に関し、hLen については hLen=k-1 という制限があるため、セキュリティパラメータ k と関連があるが、平文のビット長 mLen についてはセキュリティパラメータ k との関連が記述されていないため、このような事態が起こりうると考えられる。

従って、Diffie-Hellman 問題が計算困難であると仮定し、PSEC-2 に用いる共通鍵暗号が受動的攻撃に対し安全であるとしても、ε の評価式より、ランダムオラクルモデルの下で、PSEC-2 は適応的選択暗号文攻撃に対し、強秘匿であるとは評価することができなかった。また、適応的選択暗号文攻撃に対し、どの程度の安全性を持つかどうかについて結論付けることはできなかった。

3.5 PSEC-3 の安全性評価

PSEC-3 の安全性の評価を以下に述べる。

3.5.1 PSEC-3 の概要

PSEC-3 は、楕円 ElGamal 暗号を基に、文献[OP]の手法により設計された暗号方式と捉えられる。

3.5.2 PSEC-3 の安全性

提案者は、PSEC-3 の鍵生成時に、公開鍵パラメータである rLen と hLen については、

$$\mathrm{rLen} \leqq \mathrm{qLen}$$

の条件のみを満たすように生成しており、安全性の議論においては、さらにパラメータを

$$\mathrm{rLen}=\mathrm{qLen}-1 \text{ かつ、} \mathrm{hLen}=\mathrm{pLen}-1 \qquad (3)$$

と制限して、共通鍵暗号として受動的攻撃に対し安全であるものを用いた場合の PSEC-3 の安

全性について言及している。

そこで、評価者は、パラメータに上記(3)の制限を適用し、かつ用いる共通鍵暗号は受動的攻撃に対し安全であるとしたときの PSEC-3 の安全性の議論を行う。

その結果、PSEC-3 は、楕円 Gap-Diffie-Hellman 問題が計算困難であれば、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿であると結論付けることができる。

なお、提案者は、PSEC-3 に用いる、受動的攻撃に対し安全な共通鍵暗号として、バーナム暗号を例示している。

以下でそのことを説明する。

提案者は、文献[OP]において、以下の定理を示している。

定理（文献[OP]）

公開鍵 pk と秘密鍵 sk を生成する鍵生成関数 K、暗号化関数 E、及び復号関数 D をもつ公開鍵暗号システム A=(K,E,D)の、暗号化関数 $E_{pk}(M,R)$（M：平文、R：乱数、pk：公開鍵）、及び復号関数 $D_{sk}(C)$（C：暗号文、sk：秘密鍵）と、暗号化関数 SymE、及び復号関数 SymD をもつ共通鍵暗号システム S=(SymE,SymD)の、暗号化関数 $SymE_K(M)$（M：平文、K：共通鍵）、及び復号関数 $SymD_K(C)$（C：暗号文、K：共通鍵）を用いると、新しい公開鍵暗号システム B=(K',E',D')が以下のように定義できる。

$E'_{pk}(m,u) := E_{pk}(u, r) \,||\, SymE_{G(u)}(m) \,||\, H(E_{pk}(u, r), u, m)$

$D'_{sk}(c_1||c_2||c_3) := SymD_{G(u')}(c_2)$ （$c_3 = H(c_1, u', m')$ の場合）

もしくは、出力なし（その他の場合）。

ここで、$u'=D_{sk}(c_1)$、$m'=SymD_{G(u')}(c_2)$。

いま、ランダムオラクルモデルの下で、公開鍵暗号システム B が、適応的選択暗号文攻撃に対し、確率 ε で強秘匿性を破る攻撃者が存在すれば、$0< \nu < \varepsilon$ を満たす全ての ν に対し、

- 公開鍵暗号システム A に、正しい平文、暗号文対であるかどうかを検証することのできる攻撃者に対し、以下の確率φで一方向性を破る攻撃者が存在するか、

$$\varphi = \frac{\varepsilon - \nu}{2} - \frac{q_D}{2^{|H(\cdot)|}}$$

- 共通鍵暗号システム S が、受動的攻撃ができる攻撃者に対し、確率 ν で安全性が破られる。

ここで、q_D は、攻撃者が復号オラクルを用いる回数を表す。

評価者は、時間的制約のため、この定理の正当性を完全に検証することができなかった。従って、この定理が正しいとみなしたときの PSEC-3 の評価を以下に記述する。

PSEC-3 は、楕円 ElGamal 暗号を基に、上記定理の手法により作られる暗号方式であるので、

PSEC-3 に、上記確率 ε の攻撃者が存在すると、それに近い確率で、楕円 ElGamal 暗号に上記の攻撃者が存在するか、もしくは、共通鍵暗号が受動的攻撃に対し安全でないことになる。

いま、楕円 ElGamal 暗号は、正しい平文、暗号文対かどうかを検証できるオラクルを用いても、一方向性を破る攻撃者は存在しない（楕円 Gap-Diffie-Hellman 問題が計算困難である）と仮定すると、受動的攻撃に対し安全な共通鍵暗号を用いれば、PSEC-3 はランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し、強秘匿であると評価することができる。

なお、提案者は、パラメータ rLen の制限をしているが、暗号化時、及び復号時にはこのパラメータは使用されていないため、評価者はその理由が理解できなかった。

また、安全性の保証のために、楕円 Gap-Diffie-Hellman 問題が計算困難であるという仮定をしている。スクリーニング評価結果のコメントにも記載されているが、この問題はやや一般的には知られていない問題と思われる。よって、この問題について知られていることを以下に説明した後、用いた仮定の妥当性について検討する。

楕円 Gap-Diffie-Hellman 問題が計算困難であるとは、楕円 Diffie-Hellman 問題に関する、計算問題と決定問題との難しさの差の存在を仮定したもので、以下のような仮定である。

楕円 Diffie-Hellman（計算）問題は、楕円 Diffie-Hellman 決定問題をオラクルとして用いても、計算困難である。

一般に、決定問題は、計算問題をオラクルとして用いれば多項式時間で解くことができるが、計算問題は、決定問題をオラクルとして用いて多項式時間で解けるとは限らない。しかし、問題の種類によっては多項式時間で計算できる問題が存在する。例えば、グラフ同型問題や充足可能性判定問題については、決定問題をオラクルとして用いて計算問題が多項式時間で計算できることが知られている（文献[KST]参照）。特に、充足可能性判定問題は NP 完全問題であり、Diffie-Hellman 決定問題よりも難しい問題であると信じられている点を考えると、決定問題と計算問題の難しさの差と、決定問題や計算問題の難しさ自身との間には、必ずしも関連性があるとはいえないことになる。

しかしながら、用いた仮定の妥当性を考えると、Diffie-Hellman 決定問題(DDH)と Diffie-Hellman 問題(DH)の間の関係として、DDH≦DH であることは知られているが、現時点では DH≦DDH となる多項式時間アルゴリズムは見つかっていない。従って、現時点において、評価者は、楕円 Gap-Diffie-Hellman 問題の計算困難性の仮定は妥当であると考える。

3.6 まとめ

PSEC 暗号は、PSEC-1、PSEC-2、及び PSEC-3 の 3 つのスキームがあるが、いずれも一般的な楕円 ElGamal 暗号を暗号プリミティブとした暗号スキームであると捉えることができる。

評価者は、これらの安全性について評価を行った結果、提案者による暗号自己評価書に記載

のパラメータ制限を行ったとき、PSEC-1 は、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿性をもち、PSEC-3 は、受動的攻撃に対し安全な共通鍵暗号を用いたとき、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿性をもつと結論付けることができた。しかしながら、現状のパラメータ制限では、PSEC-2 は、適応的選択暗号文攻撃に対し強秘匿性をもつとは結論付けることができなかった。また、PSEC-2 の安全性のレベルがどこまで低下する可能性があるかについては、結論を出すことができなかった。

4 おわりに

本報告書では、PSEC 暗号に関し、暗号プリミティブ及び暗号スキームの両面から安全性の評価を行った。

その結果、PSEC 暗号の暗号プリミティブは楕円 ElGamal 暗号であるが、楕円パラメータの具体的な設定方法の記述が暗号仕様書になく、また、記載されている楕円パラメータ生成アルゴリズムでも、安全性に問題がある楕円パラメータを生成する可能性がある。

また、PSEC 暗号の暗号スキームは、PSEC-1、PSEC-2、及び PSEC-3 の 3 つのスキームがあるが、提案者による暗号自己評価書に記載のパラメータ制限を行ったとき、暗号プリミティブの安全性に問題がないとすると、現時点では、評価者は以下のように評価する。

- PSEC-1
  現時点で妥当と考えられる楕円 Diffie-Hellman 部分決定問題の計算困難性を仮定したとき、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿。
- PSEC-2
  現時点で妥当と考えられる楕円 Diffie-Hellman 問題の計算困難性を仮定したとき、受動的攻撃に対し安全な共通鍵暗号を用いても、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿性をもつという主張には疑問がある。また、達成する安全性のレベルについて結論を出すことはできなかった。
- PSEC-3
  現時点で妥当と考えられる楕円 Gap-Diffie-Hellman 問題の計算困難性を仮定したとき、受動的攻撃に対し安全な共通鍵暗号を用いれば、ランダムオラクルモデルの下で、適応的選択暗号文攻撃に対し強秘匿。

なお、この PSEC 暗号方式は、提案されてから間もなく、今までに第三者による詳細評価が不十分であり、また、今回の評価においても、安全性の証明に提案者が発表した定理を用いているため、安全性について若干の不安は否定できない。

参考文献

[ANSI] ANSI X9.62-1998, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), pp.49—52(1998).

[BDPR] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, “Relations Among Notions of Security for Public-Key Encryption Schemes”, Advances in Cryptology – CRYPTO’98.

[BG] M. Blum, and S. Goldwasser, “An efficient probabilistic public-key encryption scheme which hides all partial information”, Proceeding of Crypto’84, LNCS 196, Springer-Verlag, pp.289—299 (1985).

[FO1] E. Fujisaki, and T. Okamoto, “How to Enhance the Security of Public-Key Encryption at Minimum Cost”, Proceeding of PKC’99, LNCS 1560, Springer-Verlag, pp.53—68 (1999).

[FO2] E. Fujisaki, and T. Okamoto, “Secure Integration of Asymmetric and Symmetric Encryption Schemes”, Proceeding of Crypto’99, LNCS 1666, Springer-Verlag, pp.535—554 (1999).

[FR] G. Frey and H.G. Rück, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, Mathematics of Computation 62, pp. 865—874 (1991).

[Gal] S. Galbraith and N. Smart, “ A Cryptographic Application of Weil Decent”, HP Labs Tech. Report, HPL-1999-70.

[Gau] P. Gaudry, F. Hess and N. Smart, “Constructive and destructive facets of Weil decent on elliptic curves”, HP Labs Tech. Report, HPL-2000-10.

[IEEE] IEEE P1363/D13, Standard Specifications for Public Key Cryptography, pp.143—146, (1999).

[KST] J. Köbler, U. Schöning, and J. Torán, “The Graph Isomorphism Problem – Its Structural Complexity”, Progress in Theoretical Computer Science, Birkhäuser (1993).

[NIST] Recommend Elliptic Curves For Federal Government Use, NIST, (1999)

[MOV] A. Menezes, T. Okamoto and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field”, Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing, pp. 80—89 (1991).

[OP] T. Okamoto, and D. Pointcheval, “OCAC: an Optimal Conversion for Asymmetric Cryptosystems”, manuscript (2000).

[Poh] S.C. Pohlig and M.E. Hellman, “An improved algorithm for computing logarithms over GF(p) and its cryptographic significance”, IEEE Trans. Inf. Theory, IT-24, pp. 106—110 (1978).

[Pol] J. Pollard, “Monte Carlo methods for index computation (mod p)”, Mathematics of Computation 32, pp. 918—924 (1978).

[Sat] T. Satoh and K. Araki, “Fermat quatients and the polynomial time discrete log algorithm for anomalous elliptic curves”, Commetarii Math. Univ. St. Pauli., Vol.

47, pp. 81—92 (1998).

[Sem] I.A. Semaev, “ Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p”, Mathematics of Computation 67, pp. 353—356 (1998).

[Sma] N.P. Smart, “The discrete logarithm problem on elliptic curves of trace one”, J. Cryptology, Vol. 12. No. 3, pp. 193—196 (1999).

[SS] K. Sakurai, and H. Shizuya, “Relationships among the Computational Powers of Breaking Discrete Log Cryptsystems”, Advances in Cryptology – EUROCRYPT'95, LNCS 921, Springer-Verlag, pp.341—355 (1995).