PSEC-KEM アルゴリズムの詳細評価報告書

2001 年 12 月 14 日

1 はじめに

本報告書は、PSEC-KEM アルゴリズム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-KEM 仕様書
- PSEC-KEM 自己評価書
- 平成 12 年度詳細評価レポート（PSEC-2）

ただし、これらは、NTT コミュニケーションズ株式会社から、2001 年 11 月 8 日に送付された MO に含まれているものである。

以下では、2 章に暗号プリミティブに関する安全性評価の結果を示し、3 章に暗号スキームである、鍵カプセル化メカニズム（key encapsulation mechanisms, KEM）に関する安全性評価の結果を示す。

なお、PSEC-KEM 仕様書の 7.1.1, 7.1.4 節に記載の関数「BS2IP」は仕様書内で定義されていないため、このままでは実装できない。評価者は、3.1 節に定義されている関数「BS2OSP」と 3.4 節に定義されている関数「OS2ISP」の合成関数を、関数「BS2IP」の定義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

ここでは、PSEC-KEM の暗号プリミティブに関する安全性評価を行う。

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-KEM の暗号プリミティブは PSEC-2 暗号と同様であり、楕円 ElGamal 暗号である。楕円 ElGamal 暗号は、ECDLP(楕円曲線上の離散対数問題)を安全性の根拠としている。そのため、PSEC-KEM 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-KEM 仕様書において、楕円曲線の推奨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。楕円曲線のパラメータに関しては、PSEC-KEM 仕様書で「楕円曲線のパラメータについては、SECG などを参照」のあいまいな記述がされているのみである。したがって、使用する楕円曲線のパラメータによっては、安全性が低くなる可能性がある。以下では、SECG[SECG]の楕円曲線のパラメータについて安全性評価を行う。

SECG には、以下に挙げられる楕円曲線のパラメータが示されている。

(1) 素体上の楕円曲線

(1-1) CM (虚数乗法) を用いて生成された楕円曲線

"secpXXXkY"のように記載されている。ただし、XXX は楕円曲線の定義体の位数(160, 192 など), Y はバージョン番号を示している。SECG では Koblitz curve と呼ばれている。

(1-2) ランダムに生成された楕円曲線

"secpXXXrY"のように記載されている。

(2) 標数 2 の体上の楕円曲線

(2-1) 体の持ち上げにより生成された楕円曲線

"sectXXXkY"のように記載されている。一般に、Koblitz curve と呼ばれている。

(2-2) ランダムに生成された楕円曲線

"sectXXXrY"のように記載されている。

(1), (2)共に、MOV[MOV], FR[FR] reduction attack や SSSA attack[Sma,Sat,Sem]に対して安全になるように選ばれている。また、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」(楕円曲線の位数が大きい素数で割り切れる)条件も満たしている。(2)の標数 2 の体上の楕円曲線については、拡大次数が素数になるように選ばれており、現在知られている Weil Decent attack[Gal,Gau]に対しても安全になるように考慮されている。

これらの SECG に記載されている楕円曲線の一部は、NIST[NIST]にも採用されており、現在の攻撃に対し、十分な安全性を持っている。ただし、楕円曲線の位数 (または、楕円曲線の定義体) のビットサイズは、PSEC-KEM 仕様書の付録 B で書かれている 160bits 以上として評価している。

2.3 まとめ

PSEC-KEM 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、楕円曲線のパラメータの安全性について評価を行った。その結果、PSEC-KEM 仕様書には、楕円曲線の推奨パラメータが見当たらず、「楕円曲線のパラメータについては、SECG などを参照」のようなあいまいな記述がされているのみである。そのため、安全性の低い楕円曲線パラメータを選択する可能性がある。なお、この記述にある SECG の楕円曲線パラメータは、現在の攻撃に対し、十分な安全性を持っているため、SECG の楕円曲線パラメータを使用すればこの問題はなくなる。

3 PSEC-KEM (暗号スキーム) の安全性評価

ここでは、PSEC-KEM の暗号プリミティブには安全性に問題はないものとして、PSEC-KEM の鍵カプセル化メカニズム (key encapsulation mechanisms) の安全性について以下で評価を行う。

本節では、まず、鍵カプセル化メカニズムと、安全性の分類と、ランダムオラクルモデルについ

て説明した後、PSEC-KEM の安全性評価結果について説明し、最後にまとめを述べる。

3.1 鍵カプセル化メカニズム

公開鍵暗号の効率的な利用方法の一つとして、公開鍵暗号を用いてある暗号鍵を通信相手に伝送し、その後、伝送した暗号鍵を用い秘密鍵暗号方式で通信を行うという、公開鍵暗号方式と秘密鍵暗号方式をハイブリッドに用いた利用方法がある。

鍵カプセル化メカニズム (key encapsulation mechanism) とは、公開鍵暗号方式で暗号鍵を通信相手に伝送する方式である。具体的には、鍵生成アルゴリズム K と暗号化アルゴリズム E と復号アルゴリズム D で構成される以下のような暗号方式である (文献[Shoup]参照)。

鍵生成アルゴリズム K: 公開鍵 pk と秘密鍵 sk を生成する
暗号化アルゴリズム E: 公開鍵 pk を入力とし、鍵 Key と暗号文 C の組 (Key, C) を出力する
復号アルゴリズム D: 秘密鍵 sk と暗号文 C を入力とし、鍵 Key を出力する

鍵カプセル化メカニズムは、暗号化アルゴリズム E において平文の入力がない点において一般的な秘匿目的の公開鍵暗号方式とは異なる。

3.2 安全性の分類

公開鍵暗号方式の安全性は、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 (文献[BDPR]参照) 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。

しかし、鍵カプセル化メカニズムは、3.1 節で述べた通り、暗号化アルゴリズム E において平文の入力がないため、鍵カプセル化メカニズムにおける安全性は、上述の公開鍵暗号方式の安全性と定義が異なる（文献[Shoup]参照）。簡単に説明すると、公開鍵暗号方式における強秘匿性の定義は、多項式時間で、

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。

ことであったが、鍵カプセル化メカニズムにおける強秘匿性の定義は、多項式時間で、

B'）暗号文から、鍵の部分情報を解読することができない。

ことである（文献[Shoup]参照）。

評価者は、この定義を妥当であると考える。なお、強秘匿性以外の一方向性、及び頑健性についての定義は、PSEC-KEM 評価書には記載されていなかった。

3.3 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仮定の下で、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。代表的には、RSA-OAEP 暗号（文献[BR2]参照）がそれにあたる。

この仮定の下では、ハッシュ関数はランダムな値を出力する決定的な関数ではなく、ランダムな値を出力する非決定的な関数として扱われる。すなわち、ハッシュ関数の出力値を「実際に入力しなければ、出力値は全く予測不可能」であるランダムな値とみなす。そのため、我々が通常用いる、入力値に対し出力値は決まっている関数とは全く違う考え方(モデル)を用いていることになる。よって、ランダムオラクルモデルの仮定の下で安全性証明が可能でも、実際の環境では、ランダムな値を出力する非決定的な関数は定義できないため、安全性証明は成り立たない。

しかしながら、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、ランダムオラクルモデルの仮定の下での安全性証明は、実際の環境での安全性をある程度保証していると考えることもできる。

従って、このランダムオラクルモデルの概念は、RSA-OAEP 暗号に代表されるように、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-KEM 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ている。この実現例としては、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 から構成される MGF1 マスク生成関数（KDF1 という名前で文献[Shoup]に記載されている）を用いた暗号スキームを挙げている。

3.4 PSEC−KEM の安全性評価結果

PSEC-KEM の安全性の評価結果を以下に述べる。

PSEC-KEM 仕様書付録 F によれば、PSEC-KEM は PSEC-2 を変更した方式である。従って、まず、PSEC-KEM の方式の概要について説明した後、PSEC-2 との方式の差異について述べる。その後、PSEC-KEM の安全性ついて述べる。

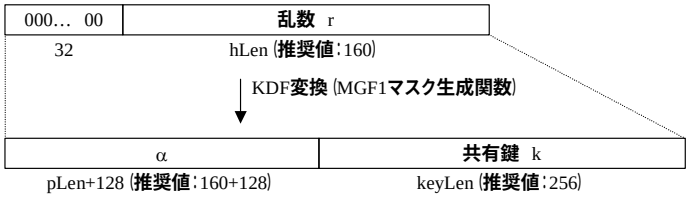
3.4.1 PSEC-KEM の概要

PSEC-KEM は、楕円 ElGamal 暗号を基に、以下の手法により設計された鍵カプセル化メカニズムと捉えられる（PSEC-KEM 仕様書参照）。

なお、以下の説明で、各要素の下に書かれた数値はビット数を表し、括弧内は、PSEC-KEM 仕様書の付録 C に記載のパラメータ推奨値を適用した場合のビット数である。

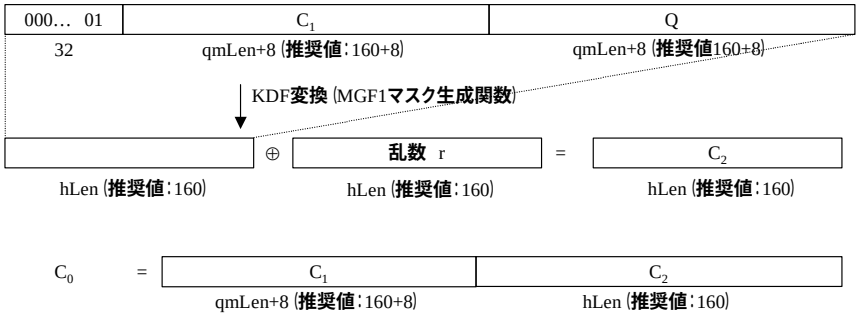
《暗号化》

1. （エンコーディング処理：EME-PSEC-KEM-A）
   ビット長hLenの乱数 r から、楕円ベキ倍係数 α, 共有鍵 k を生成



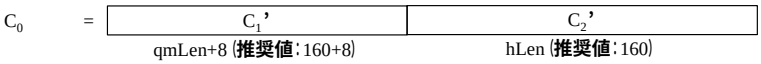
2. （暗号化プリミティブ：EP-PSEC）
   α と、公開鍵である楕円曲線上の点（P, W）から、楕円曲線上の点（Q, C_1）を生成
   ・$Q = \alpha W$
   ・$C_1 = \alpha P$

3. （エンコーディング処理：EME-PSEC-KEM-B）
   暗号文 C_0 を生成



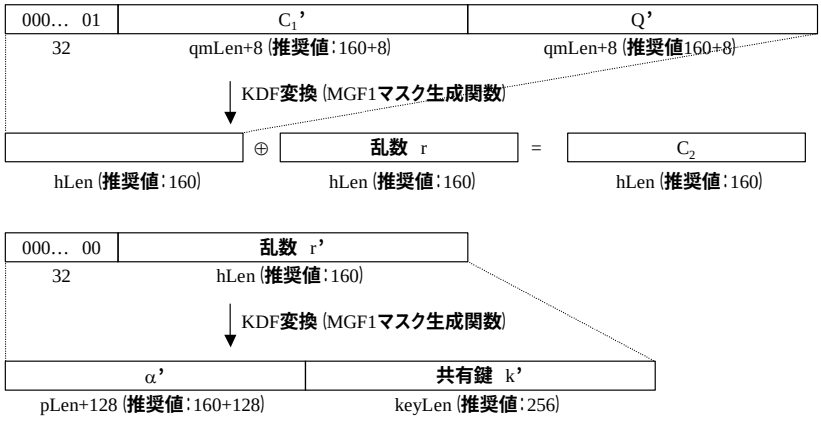
《復号化》

1. (デコーディング処理：EME-PSEC-KEM-C)
   暗号文C_0から、楕円曲線上の点 C_1'と 数値 C_2'を生成



2. (復号化プリミティブ：DP-PSEC)
   楕円曲線上の点 C_1'と秘密鍵 s から、楕円曲線上の点 Q'を生成
   'Q' = sC_1'

3. (デコーディング処理：EME-PSEC-KEM-D)
   楕円曲線上の点 C_1', 数値 C_2', 楕円曲線上の点 Q から、楕円ベキ倍係数α', 共有鍵 k'を生成



もしも、C_1'= α'P ならば、共有鍵 k'を出力／それ以外は invalid を出力

3.4.2 PSEC-2 と PSEC-KEM との差異

PSEC-2 と PSEC-KEM の暗号化方式、及び復号方式の概要は以下の通りである。

[PSEC-2 の暗号化方式 (概要)] (平成 12 年度詳細評価レポート (PSEC-2) 参照)

入力： 公開鍵 pk(=W, P), 平文 m

出力： 暗号文 (C_1, C_2, C_3)

i. Q=h(m||r) W
   C_1=h(m||r) P を計算 (h はハッシュ関数)
ii. C_2=r⊕x[Q] で乱数 r を送信
iii. その後、C_3=g(r)⊕m で平文 m を暗号化して送信 (g はハッシュ関数)

[PSEC-KEM の暗号化方式 (概要)] (PSEC-KEM 仕様書参照)

入力： 公開鍵 pk(=W, P)

出力： 暗号文 (C_1, C_2)

i. Q=G(r) W
   C_1=G(r) P を計算 (G はハッシュ関数)
ii. C_2=r⊕H (C_1, Q)で乱数 r を送信 (H はハッシュ関数)

[PSEC-2 の復号方式 (概要)] (平成 12 年度詳細評価レポート (PSEC-2) 参照)

入力： 公開鍵 pk(=W, P), 秘密鍵 sk(=s), 暗号文 (C_1, C_2, C_3)

出力： 復号文 m', もしくは出力なし

i. $Q'=sC_1$

$r'=C_2 \oplus x[Q']$ を計算

ii. $m'=g(r') \oplus C_3$ を計算 (g はハッシュ関数)

iii. $C_1=h(m' \| r')$ P が成り立てば、m'を復号文として出力する (h はハッシュ関数)

[PSEC-KEM の復号方式 (概要)] (PSEC-KEM 仕様書参照)

入力： 公開鍵 pk(=W, P), 秘密鍵 sk(=s), 暗号文 (C_1, C_2)

出力： 鍵 k, もしくは出力なし

i. $Q'=sC_1$

$r'=C_2 \oplus H(C_1, Q')$ を計算 (H はハッシュ関数)

ii. $C_1=G(r')$ P が成り立てば、G(r')から鍵 k を求めて出力する (G はハッシュ関数)

提案者は、PSEC-2 と PSEC-KEM との差異について、PSEC-KEM 自己評価書の付録 F において、「PSEC-1, PSEC-2, PSEC-3, 及び PSEC-KEM はエンコーディングメソッドが異なるため、スキームとして同一でない。」と言及している。評価者はこのことについて検討した結果、以下の点から、提案者の主張通り PSEC-2 と PSEC-KEM は別のスキームであると結論付ける。

1. PSEC-2 は、秘匿通信目的の公開鍵暗号方式であるが、PSEC-KEM は、鍵カプセル化メカニズムのための公開鍵暗号方式であり、安全性の定義が異なる (文献[BDPR][Shoup]参照)。
2. PSEC-2 の暗号化方式は、平文を入力するが、PSEC-KEM の暗号化方式は、平文を入力できる構造にはなっていない (上述の PSEC-2, PSEC-KEM の暗号化方式 (概要) 参照)。
3. PSEC-2, PSEC-KEM ともに、乱数 r を秘匿して送信し、受信側で乱数 r を復号している点は類似している (上述の PSEC-2, PSEC-KEM の暗号化方式 (概要) , 復号方式 (概要) を参照)。しかし、乱数 r を秘匿するために、PSEC-2 では、平文 m と乱数 r のハッシュ値からαを生成して、公開鍵 W のベキ倍点αW の x 座標を用いるのに対し、PSEC-KEM では、乱数 r のハッシュ値からαを生成し、公開鍵 W のベキ倍点αW と公開鍵 P のベキ倍点αP のハッシュ値を用いている。また、受信側で復号結果が正当かどうかを判断するために、PSEC-2 では、平文 m と乱数 r が必要なのに対し、PSEC-KEM では、乱数 r のみしか必要としない。

3.4.3 PSEC-KEM の安全性

提案者は、PSEC-KEM が、鍵カプセル化メカニズム (key encapsulation mechanism) の安全性定義 (文献[Shoup]参照) において、楕円 Diffie-Hellman 計算問題が計算困難であれば、ランダムオラクルモデルの仮定の下で、適応的選択暗号文攻撃に対し、強秘匿であると主張している。ま

た、提案者は、PSEC-KEM の安全性レベルについて、Cramer-Shoup 暗号（文献[CS]参照）、及び ECIES（文献[ABR]参照）と安全性レベルの比較を行っている。

評価者は、提案者によるこれらの自己評価が正しいかどうかの検討し、その結果をもって PSEC-KEM の安全性評価結果とする。

以下では、まず、提案者による PSEC-KEM の安全性主張を述べ、それらの主張に対する評価者の検討結果を説明する。

3.4.3.1 提案者による PSEC-KEM の安全性主張

ここでは、提案者による PSEC-KEM の安全性主張について述べる。

提案者は、PSEC-KEM 自己評価書 3 節において、以下の定理を示している。

定理 3.1（PSEC-KEM 自己評価書）

A を、復号オラクル、ランダムオラクル G, H にそれぞれ q_D 回, q_G 回, q_H 回の質問をし、アドバンテージが ε で実行時間が t であるような PSEC-KEM（K, E, D）に対する IND-CCA2 における攻撃者とする。このとき、成功確率 ε ’で実行時間が t’の（K に関する）楕円 Diffie-Hellman 問題の回答を含む（qH＋qD）個の値のリストを出力するようなアルゴリズムが存在して、

$$\varepsilon' \geq \frac{\varepsilon}{2(1+2^{-128})} - \frac{(q_G + 3q_D)(1+2^{-128})}{p} - \frac{q_D + q_G}{2^{hLen}}$$

$$t' \leq t + q_H \cdot (T + \mathrm{O}(1))$$

ここで、T は K に関する楕円曲線上の乗算 2 回を行う計算時間である。

この定理で主張していることは、ランダムオラクルモデルの仮定の下で、攻撃者が PSEC-KEM の IND-CCA2 性を破る確率　ε /2 と、楕円 Diffie-Hellman 問題の回答を含むリストを出力できる確率 ε ’の差が無視できるほど小さくなることである。従って、楕円 Diffie-Hellman 問題が計算困難ならば、PSEC-KEM は IND-CCA2 であることを主張している。

また、提案者は、PSEC-KEM 自己評価書 2.1 節において、PSEC-KEM の安全性レベルを Cramer-Shoup 暗号、及び ECIES と、以下のように比較している。

1. Cramer-Shoup 暗号は、PSEC-KEM と同様に最強の意味での安全性証明がついている。安全性証明において、ランダム関数仮定には、汎用一方向性ハッシュ関数を仮定しており、これは PSEC-KEM より妥当な仮定であるが、整数論的仮定には、楕円 DDH 問題を仮定しており、これは PSEC-KEM より強い仮定である。
2. ECIES は、PSEC-KEM と同様に最強の意味での安全性証明がついている。安全性証明において、ランダム関数仮定には、PSEC-KEM と同じ仮定を用いているが、整数論的過程には、楕円 GDH 問題を仮定しており、これは PSEC-KEM より強い仮定である。

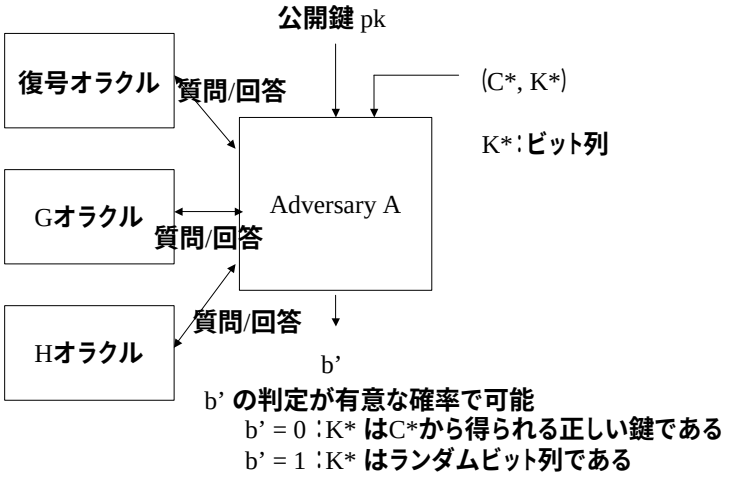
3.4.3.2 評価者の検討結果

ここでは、前節で述べた、提案者による PSEC-KEM の安全性主張に対する評価者の検討結果を説明する。

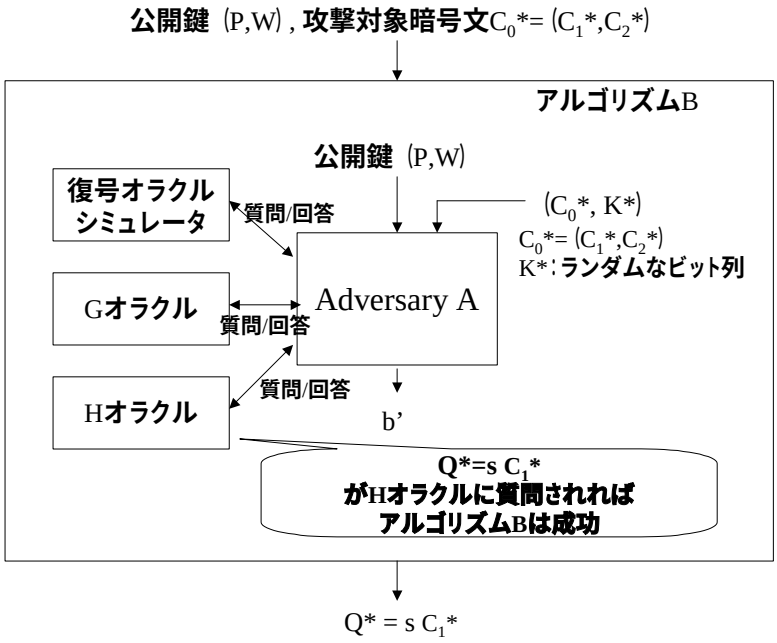
はじめに、PSEC-KEM の安全性証明についての検討結果を述べ、次に、他の暗号方式との安全性レベルの比較についての検討結果を述べる。

[PSEC-KEM の安全性証明]

まず、文献[Shoup]によれば、ランダムオラクルモデルの仮定の下で、PSEC-KEM の IND-CCA2 性を効率良く破る攻撃者 Adversary A は、以下の図のように、公開鍵 pk と、攻撃対象暗号文 C^*と、ビット列 K^*を与えられたとき、復号オラクル、及び G オラクル、H オラクルに質問を行い、有意な確率で、ビット列 K^*がランダムなものか正しい鍵かを判別できる。



今、楕円 Diffie-Hellman 問題を計算するアルゴリズム B を、この攻撃者 Adversary A を用いて、以下の図のように構成する（PSEC-KEM 自己評価書 3.1 節参照）。



なお、アルゴリズム B は秘密鍵が分からないため、復号オラクルへの質問は正しく回答することが完全にはできない。従って、復号オラクルのふるまいをシミュレートする復号オラクルシミュレータを用いる。

以下で、上記のアルゴリズム B に関する、評価者の検討結果を説明する。

アルゴリズム B に用いられる復号オラクルシミュレータは、暗号文 C が質問されたとき、G, H オラクルに過去に質問された質問とその回答である G, H の関数値から、都合良く暗号文 C が構成できれば、そこから逆演算を行い、矛盾しない復号結果を返す。それ以外は reject を返す (PSEC-KEM 自己評価書 3.1.3 節)。

もし、復号オラクルシミュレータが復号オラクルと異なる結果を出力すれば、Adversary A は正しく動くとは保証できないため、アルゴリズム B も正しく動くとは保証できない。

評価者は、復号オラクルシミュレータが復号オラクルと異なる結果を出力する確率について検討した。その結果、ランダムオラクルモデルの仮定の下では、Adversary A は G オラクル, H オラクルに質問しないと、関数 G, H の値は分からないので、復号オラクルシミュレータが復号オラクルと異なる結果を出す確率 Pr[Fail]は結果として非常に低く、PSEC-KEM 自己評価書 3.3.2 に記述されている通り、

$$\Pr[Fail] \le \frac{(q_G + 3q_D)(1 + 2^{-128})}{p} + \frac{q_D}{2^{hLen}}$$

となることが分かった。

一方、このアルゴリズム B が正しく Q^* を出力できる確率は、Adversary A が正しく動いて、かつ

H オラクルに Q^* を質問する確率である。

評価者は、この確率を検討した結果、PSEC-KEM 自己評価書 3.4 節に記述に記述されている通り、

$$\Pr[AskH] \geq \frac{\varepsilon}{2(1+2^{-128})} - \frac{(q_G+3q_D)(1+2^{-128})}{p} - \frac{q_D+q_G}{2^{hLen}}$$

となることが分かった。

これにより、アルゴリズム B が、Q^*を出力できる確率 ε ’は、PSEC-KEM 自己評価書に記載の定理 3.1 の通り、

$$\varepsilon' \geq \frac{\varepsilon}{2(1+2^{-128})} - \frac{(q_G+3q_D)(1+2^{-128})}{p} - \frac{q_D+q_G}{2^{hLen}}$$

となる。

ここで、アルゴリズム B が入力 (P, W=sP, C_1^*) から、$Q^*=sC_1^*$を求めることができれば、アルゴリズム B の入力を (P, sP, tP) とすれば、stP を求めることが可能である。従って、アルゴリズム B は楕円 Diffie-Hellman 問題を解くことが可能である。

今、PSEC-KEM 仕様書の付録 C に記載の推奨パラメータを用いた場合、PSEC-KEM に対する攻撃者が復号オラクル、ランダムオラクルにそれぞれ 2^{40} 回の質問をした場合でも、

$$\left| \frac{\varepsilon}{2(1+2^{-128})} - \varepsilon' \right| \leq \frac{(q_G+3q_D)(1+2^{-128})}{p} + \frac{q_D+q_G}{2^{hLen}} \approx \frac{2^{42}}{2^{160}} + \frac{2^{41}}{2^{160}} \leq 2^{-117}$$

となる。ここで、PSEC-KEM 仕様書の付録 C に記載の推奨パラメータを用いた場合、ε ’は 2^{-80} 程度となる (文献[SECG]参照) ので、攻撃者が PSEC-KEM の IND-CCA2 性を破る確率 ε /2 と楕円 Diffie-Hellman 問題の回答を含むリストを出力できる確率 ε ’との差が 2^{-80} に比べて無視できるぐらい小さくなる。すなわち、ランダムオラクルモデルの仮定の下で、楕円 Diffie-Hellman 問題の回答が計算困難であれば、PSEC-KEM の IND-CCA2 性を破るのは困難であるということができる。

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、これは妥当な仮定である。

[他の暗号方式との安全性レベルの比較]

PSEC-KEM は、鍵カプセル化メカニズム方式であるので、上記の安全性証明で用いている強秘匿の定義は、Cramer-Shoup 暗号、及び ECIES 等の秘匿暗号方式の強秘匿の定義と異なる (文献[BDPR][Shoup]参照) 。また、鍵カプセル化メカニズム方式における、一方向性や頑健性の定義は、PSEC-KEM 自己評価書には記載されていなかった。

従って、PSEC-KEM には、本評価書 3.2 節で述べた安全性の分類を用いることができない。す

なわち、鍵カプセル化メカニズムである PSEC-KEM は、秘匿暗号方式と安全性を直接比較できない。

また、鍵カプセル化メカニズム方式において、IND-CCA2=NM-CCA2（最強の意味で安全）となることが PSEC-KEM 自己評価書に記述されておらず、IND-CCA2 であることをもって最強の意味で安全である根拠が示されていない。

また、提案者によれば、楕円 GDH 仮定は楕円 CDH 仮定よりも強い仮定とのことであるが、その根拠も示されていない。

3.5 まとめ

評価者が、PSEC-KEM の暗号スキームの安全性について検討した結果は、以下の通りである。

1. 鍵カプセル化メカニズムの安全性定義において、楕円 Diffie-Hellman 計算問題が計算困難であれば、ランダムオラクルモデルの仮定の下で、適応的選択暗号文攻撃に対し、強秘匿である。
2. PSEC-KEM 自己評価書では他の秘匿暗号方式との比較結果について記載されているが、秘匿暗号方式と鍵カプセル化メカニズム方式は、強秘匿性の定義が異なることから直接比較できない。
3. PSEC-KEM 自己評価書に記述してある、最強の意味で安全ということについて、PSEC-KEM 自己評価書にはその根拠が示されていない。

4 おわりに

本報告書では、PSEC-KEM 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-KEM の暗号プリミティブは、楕円 ElGamal 暗号であるが、楕円曲線の推奨パラメータが記述されておらず、「楕円曲線のパラメータについては、SECG などを参照」のようなあいまいな記述がされているのみである。そのため、安全性の低い楕円曲線パラメータを選択する可能性がある。

また、PSEC-KEM の暗号スキームは、暗号プリミティブの安全性に問題がなく、提案者による PSEC-KEM 仕様書に記載の推奨パラメータを用いると、現時点では、以下のように評価できる。

- 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、ランダムオラクルモデルの仮定の下で、適応的選択暗号文攻撃に対し強秘匿。
- しかし、このことをもって PSEC-KEM が「最強の安全性」を持つということはいえない。
- また、鍵カプセル化メカニズムと秘匿暗号の安全性レベルは直接比較できない。

また、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広く知られているが、評価者は、この仮定が非常に強力な仮定であると感じている。PSEC-KEM の

安全性証明は、このランダムオラクルモデルの仮定の下での特徴を用いてなされており、実環境の下での安全性は証明されていないので、将来、攻撃法が出現する可能性は残っている。

参考文献

[ABR] M. Abdalla, M.Bellare and P.Rogaway, “DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem”, submission to IEEE P1363a, http://grouper.ieee.org/groups/1363/P1363a/submissions.html, 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, LNCS 1462, Springer-Verlag, pp.26–45, 1998.

[BR] M. Bellare and P. Rogaway, “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”, Proc. of the First ACM Conference on Computer and Communications Security, ACM Press, pp.62–73, 1993.

[BR2] M. Bellare and P. Rogaway, “Optimal Asymmetric Encryption – How to encrypt with RSA”, Advances in Cryptology – Eurocrypt’94, LNCS 950, Springer-Verlag, pp.92–111, 1995.

[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.

[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).

[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).

[SECG] SEC 2: Recommended Elliptic Curve Domain Parameters, SECG ,

http://www.secg.org, (2000)

[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).

[Shoup] V. Shoup, A Proposal for an ISO Standard for Public Key Encryption (v. 2.0), ISO/IEC JTC1/SC27, N2563, http://shoup.net/papers/, 2001.

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