暗号アルゴリズム評価報告書
PSEC-2 および PSEC-KEM

2001 年 12 月 14 日

産業技術総合研究所

渡辺 創

暗号アルゴリズム評価報告書
PSEC-2 および PSEC-KEM

2001 年 12 月 14 日

1　まえがき

本報告書は, CRYPTREC2000 応募暗号である PSEC-2 と, その改訂版として CRYPTREC2001 に応募された暗号である PSEC-KEM について, その安全性評価を行なったものである. 以下 2 章では, まず CRYPTREC2000 において PSEC-2 を評価した報告書 (CRYPTREC2000 詳細評価報告書#2[3], 以下 #2) で問題があると指摘されていた点を示す. 次に指摘された点それぞれについて, その主張の有効性について論じる. 3 章では, CRYPTREC2001 に応募された暗号である PSEC-KEM の仕様と自己評価について, 2 章で指摘された問題点のうち, 有効であると判断されたものが改訂の後でも有効であるかどうかを論じる. 最後に 4 章で本評価の結論を述べる.

2　PSEC-2 CRYPTREC2000 詳細評価報告書 #2

2.1　指摘された問題点

まず PSEC-2 に関して, #2[3] で指摘されていた点を以下に挙げる.

2.1.1　PSEC-2 で用いられているプリミティブに関する指摘

1. PSEC-2 の仕様記述において, 標数 3 の体を利用しないことが明示的に述べられていない, 暗黙のうちに排除して議論が行なわれている, と指摘されている.
2. PSEC-2 の仕様記述において, 記法の誤りが多く存在するため, さらなる校正が必要である, と指摘されている. 具体的には以下のような例が挙げられている (指摘された点が多いため, ここでは全てを挙げない).
   - q_0 と書かれるべきところに p と記述されている.
   - h が文脈とは関係のないところで出てくる.
3. PSEC-2 の仕様記述において, 鍵を生成するアルゴリズムが曖昧である, IEEE 標準の文献が挙げられているだけである, と指摘されている. 具体的には例として, 以下のような問題点が挙げられている (この他にも必要である).

- どのように楕円曲線を生成するのか, が書かれていない.
- どのようなチェックが楕円曲線を生成する際に必要か, が書かれていない.

4. PSEC-2 で用いるプリミティブ関数である ElGamal スキームのバージョンについて文献が引用されていない, と指摘されている. より具体的には以下の事実について懸念を表している.
   - メッセージ空間が DH 関数 (#2 を参照) の計算可能な部分群に一致しない場合に, ElGamal 暗号化関数は欠陥持っている.
5. PSEC-2 で用いるパラメータに関して,

$$\frac{p}{2^{l_r}}, \frac{2^{l_m}}{2^{|q|}}$$

   は小さくなければならない, そうでなければプリミティブ関数の逆関数計算の困難性 (逆 ElGamal 仮定) と, ECCDH の等価性が証明できない, と指摘されている.
   また, 仕様書 [1] には記述されていないが, 自己評価書 [2] ではそれが成り立つことを前提としている, とも指摘されている.
6. PSEC-2 のプリミティブ関数で, 楕円曲線上要素の第 1 座標をマスクとして用いることは, 強秘匿性 (semantic security) を損なう可能性があるのではないか, と指摘されている.

2.1.2 PSEC-2 のスキームに関する指摘

1. PSEC-2 が最強の安全性を満たすためには $l_h \simeq k$ である必要がある, しかし仕様では $l_h \leq k$ であることのみが条件として挙げられている, これでは $l_h << k-1$ であっても構わないことになるため, 結果として安全性が証明できてない, と指摘されている. ただし, 自己評価書 [2] では $l_h = k-1$ と設定され, 安全性の議論がなされている, とも指摘されている.
2. PSEC-2 が最強の安全性を満たすためには $l_r \simeq |q|$ とするべきである, しかし仕様では $l_r \leq |q|$ であることのみが条件として挙げられている, これでは $l_r << |q|$ であっても構わないことになるため, 結果として安全性が証明できてない, と指摘されている. ただし, 自己評価書 [2] では $l_r = |q|-1$ と設定され, 安全性の議論がなされている, とも指摘されている (#2 では $l_h = |q|-1$ となっているが, l_h は l_r の誤植であろう).

2.2 指摘された問題点に対する考察

2.2.1 PSEC-2 で用いられているプリミティブに関する指摘

1. #2 で指摘された通り, 曖昧さを排除するためには, 記述を加える方が望ましいと思われる.
2. #2 で指摘された通り, 今一度校正が必要である.
3. #2 で指摘された通り, このような記述では適当でない曲線や値が使用されてしまう可能性がある. その結果, EPOC-2 が簡単に破られてしまう危険がある. 暗号学的に

は当然満たすべき条件ではあるが, 実装者がそのような知識を持っている保証はない. したがって #2 の指摘は妥当であり, 記述を加える必要があると思われる.

4. #2 で指摘された通り, 欠陥を防ぐためにも記述を加える必要があると思われる.
5. #2 で指摘された通り, 記述を加える必要があると思われる.
6. 詳しい考察は行なっていないが, #2 で指摘されたように, 楕円曲線上要素の第 1 座標を用いることで, 強秘匿性を損なう可能性があると思われる. ただし PSEC-2(スキーム) ではメッセージとして乱数が用いられ, それとマスクを取るため, 問題は起きないと考えられる.

2.2.2 PSEC-2 のスキームに関する指摘

1. #2 で指摘された通り, PSEC-2 が最強の安全性を満たすためには $l_h \simeq k$ である必要があると思われる. $l_h << k-1$ では, 明らかに安全性が証明できない. 仕様の記述は指摘されたように, あるいは自己評価書 [2] の記述 ($l_h = k-1$) のように修正されるべきである.
2. #2 で指摘された通り, PSEC-2 が最強の安全性を満たすためには $l_r \simeq |q|$ とするべきである. $l_r << |q|$ では, 明らかに安全性が証明できない. 仕様の記述は指摘されたように, あるいは自己評価書 [2] の記述 ($l_r = |q| - 1$) のように修正されるべきである.

3 PSEC-KEM CRYPTREC2001 応募仕様書および自己評価書

本章では, CRYPTREC2001 に応募された PSEC-2 の改訂版 (PSEC-KEM) の応募資料, 仕様書および自己評価書に基づき, #2 で指摘された点についてその有効性を議論する.

3.1 PSEC-2 で用いられているプリミティブに関する指摘

1. #2 で指摘された点についての記述が, PSEC-KEM の仕様書 [4] では存在する. したがって問題は解決されている. る.
2. PSEC-KEM の仕様書 [4] では, 内容を含めて大きく仕様の記述が変更されている. 記号の不整合については特に認められなかった.
3. #2 で指摘された点についての記述が, PSEC-KEM の仕様書 [4] でも依然欠落している. 同様に記述を加える必要があると思われる.
4. #2 で指摘された点についての記述が, PSEC-KEM の仕様書 [4] でも依然欠落している. 欠陥を防ぐためにも記述を加える必要があると思われる.
5. #2 で指摘された点についての記述が, PSEC-KEM の仕様書 [4] でも依然欠落している. 同様に記述を加える必要があると思われる.
6. PSEC-KEM ではプリミティブ関数が変更されており, #2 で指摘された部分については, その問題点は解決している. これは楕円曲線上要素の第 1 座標を, プリミティブ関数で用いなくなったためである.

3.2 PSEC-2 のスキームに関する指摘

1. PSEC-KEM の仕様書 [4], 自己評価書 [5] ではセキュリティパラメータ k を用いた議論はなされていない. また, プリミティブ関数が変更されている. もし同様の議論を行なった場合には, やはり #2 で指摘されたような条件の付加が必要であるように思われる. これは,

   $k = pLen$ と考える. 推奨パラメータとして, $pLen \leq 160$, $hLen \leq 128$($hLen$ は #2 中の l_h に対応する) のみ書かれており, この場合には $l_h << k - 1 = pLen - 1$ となる可能性が残っている.

   ためである.
2. プリミティブ関数が変更されているため, l_r は用いられない. よって特に問題は起こらない.

4 結論

以上述べたように, 仕様記述の不備に起因する問題点がほとんどであった. またその他の有効な攻撃については, 新たに見つからなかった. したがって, 注意深く実装すれば, あるいはさらなる改訂版を出しそれに基づいた実装をすることにより, 安全な暗号を用いることが可能であると考えられる.

参考文献

[1] Specification of PSEC, CRYPTREC2000 応募書類.

[2] Self Evaluation of PSEC, CRYPTREC2000 応募書類.

[3] Evaluation Report on the PSEC Cryptsystem,
CRYPTREC2000 詳細評価報告書 #2

[4] Specification of PSEC-KEM, CRYPTREC2001 応募書類.

[5] Self Evaluation of PSEC-KEM, CRYPTREC2001 応募書類.