PSEC-KEM の安全性評価

2002 年 11 月 8 日

1. はじめに

本報告書では、PSEC-KEM の安全性を検証し、その評価に関する意見を述べる。

2. PSEC-KEM

PSEC-KEM は鍵共有方式である。ここでは、本報告書の理解を容易にするための参考として概略を示す。正式な記述は[1]を参照のこと。

大文字は楕円曲線上の点、小文字は整数を表す。G および H は鍵導出関数で、安全性証明ではランダムオラクルとみなされる。

暗号化鍵: (P, W)

復号鍵: s

[関係式: $W = sP$]

暗号化

乱数 r 生成

$\alpha \| k = G(r)$

$C_1 = \alpha P$

$Q = \alpha W$

$c_2 = r \oplus H(C_1, Q)$

暗号文: (C_1, c_2) → 送信

k → 鍵として出力

復号化

$Q' = sC_1$

$r' = c_2 \oplus H(C_1, Q')$

$\alpha' \| k' = G(r')$

$C_1 \underset{?}{=} \alpha' P$

もし等しければ、k' を鍵として出力、それ以外は invalid を出力

3. PSEC-KEM の安全性

結論として、安全性に問題はないと考えられる。その理由を以下に順次示す。

3.1 IND-CCA2 性

自己評価書[2]により、

・楕円曲線上の Diffie-Hellman 計算困難性

・G および H のランダムオラクル性

の条件下で、IND-CCA2 の意味で安全性が証明されている。IND-CCA2 の意味は次の通りである。

攻撃モデル: 適応的選択暗号文攻撃 CCA2

安全性: 強秘匿(識別不可能性) IND

この定式化は[8]と同一である。

この枠組みにおける証明自体は信頼できると見られる。なお、ISO 提案[8]にはゲームベースの異なった証明があることを付け加えておく。

3.2 ハイブリッド暗号の NM-CCA2 性

暗号において、現在与えられている最も強い安全性の定義は、適応的選択暗号文攻撃 CCA2 に対して NM (Non-Malleable)という NM-CCA2 である。仕様書[1]では PSEC-KEM の安全性の証明として、IND-CCA2 で十分な理由に[10]の次の定理をあげている。

定理 IND-CCA2 な KEM と IND-CCA2 な DEM(Data Encapsulation Mechanism)を組み合わせたハイブリッド暗号は IND-CCA2 である。

一方、公開鍵暗号では IND-CCA2 と NM-CCA2 は等価であり、このハイブリッド暗号も公開鍵暗号なので、IND-CCA2 な KEM と IND-CCA2 な DEM を組み合わせたハイブリッド暗号は NM-CCA2 なる。

NESSIE の Web Page で公開されている[11]において、DEM 側の証明の不備が指摘されたが、[10]では訂正されている。これは、DEM の安全性証明に際し、攻撃者が KEM の鍵導出関数へアクセスしても DEM が安全であるという証明が必要という指摘である。鍵導出関数をランダムオラクルでモデル化しているので、結果として定理は成立する。

結局、ランダムオラクルモデルのもとで、PSEC-KEM が IND-CCA2 であることを示せば十分であると言う主張は、暗号鍵共有という面では、筋が通っている。

3.3 ランダムオラクルモデルの妥当性

PSEC-KEM の安全性証明は、鍵導出関数をランダムオラクルとみなして、楕円曲線上の Diffie-Hellman 計算困難性に帰着している。

ランダムオラクルの本質は、ある出力が他の出力と無相関であるということで、全く推測できないということにある。これを実際に実現する方法として、[1]ではハッシュ関数 SHA-1 を用いた方法を推奨している。これは、一般的にとられている方法のひとつで[8]にも示されており、ランダムオラクルとみなせると言う主張に実際上問題があるとは思えない。

3.4 楕円曲線上の Diffie-Hellman 計算困難性

現時点で、楕円曲線上の Diffie-Hellman 計算困難性は広く信じられており、これを仮定することに実際上の問題があるとは思えない。

4. PSEC-KEM 方式と他の方式との比較

KEM として知られている他の方法、楕円 Cramer-Shoup、ECIES-KEM および楕円 ElGamal と、安全性および処理量に関して比較する。

安全性については、まず、楕円 ElGamal は攻撃法が知られているので、PSEC-KEM はこれに対する優位性を持つ。他の方式に対しては

楕円 Cramer-Shoup: 楕円 DDH、汎用一方向性ハッシュ関数
ECIES-KEM: 楕円 GDH、ランダム
PSEC-KEM: 楕円 CDH、ランダム

となり、枠で囲ったところが優位点となっている。

処理量に関して言えば、楕円乗算の回数を基準に、

楕円 Cramer-Shoup: 暗号化 5、復号化 3
ECIES-KEM: 暗号化 2、復号化 1
PSEC-KEM: 暗号化 2、復号化 2

となる。

総合すると、特に PSEC-KEM が他方式に完全に劣っていると言うことはない。

5. PSEC-KEM の電子政府システムにおける利用方法とその安全性について

最強の意味で安全であることをある意味で証明されている使い方は、IND-CCA2 である DEM (Data Encapsulation Mechanism)と組み合わせたハイブリッド暗号である。したがって、この使い方をするなら問題ない。

他の使い方については KEM の安全性の定義の妥当性にかかっている。IND-CCA2 であることは示されているので、適応的選択暗号文攻撃に対しては識別不可能である。これなら、電子政府での利用に、実際上問題はないと思われる。

なお、絶対的な評価として、IND-CCA2 が KEM で十分かどうかをみればよいのであって、定義が最強な安全性であることを証明する必要性までは認められない。公開鍵暗号系でも最強な安全性定義であることが証明されているものはない。

6. PSEC-KEM の推奨パラメータや補助関数の選択

PSEC-KEM の利用に際しては、いくつかのパラメータや補助関数を決める必要がある。これらは[1]の付録に推奨値が示されている。

パラメータに関しては、楕円曲線上の Diffie-Hellman 計算困難性を満たす値として、現在一般に使われている値をもとに得られたもので、問題はないと思われる。

鍵導出関数としては、ハッシュ関数 SHA-1 を用いた方法を推奨している。これは、一般的にとられている方法のひとつで、ランダムオラクルとみなせると言う主張に実際上問題があるとは思えない。

楕円曲線の選択に関しては、http://www.secg.org などを参照せよ、と記述されているのみである。利用者からすると、選択法も記述されていたほうが望ましいと言える。これについては最後に議論する。

7. 公開鍵暗号評価小委員会の評価について

評価用に渡された資料の日付は、

・公開鍵暗号評価小委員会評価報告書: 2001 年 12 月 14 日

・PSEC-KEM 仕様書: 2002 年 5 月 14 日

である。したがって、公開鍵暗号評価小委員会評価報告書は、正確には、今年 5 月 14 日付の PSEC-KEM 仕様書に対する報告書ではない。

7.1 公開鍵暗号評価小委員会評価報告書(2001 年 12 月 14 日)

公開鍵暗号評価小委員会評価報告書の結論は、

「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、新たにみつからなかった。したがって、注意深く実装すれば、あるいは更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。」

であった。これに基づいて出された改訂版が今年 5 月 14 日付 PSEC-KEM 仕様書であると考えられる。

改訂版では、楕円曲線の選択以外は、述べられている。楕円曲線の選択は後でまとめて議論する。

なお、暗号技術評価報告書(2002 年 3 月)が一般に公開されているが、これは暗号技術評価委員会の報告書である。参考のために関連部分を載せておく。

「スクリーニング評価の結果、次の点が確認された。

(1) 鍵カプセル化メカニズムにおける証明可能安全性の定義は[8]によるものであり、妥当と認める。ただし、鍵カプセル化メカニズムの安全性の定義は、[12]における公開鍵暗号の安全性定義とは異なっており、IND-CCA2 の強度が最強かどうかが示されていな

い。

(2) 自己評価書における、IND-CCA2 の証明に問題は見当たらない。

(3) 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段として広く知られており、妥当と考えられる。」

7.2 公開鍵暗号の詳細評価結果の概要

これは、渡された資料以外であり、暗号評価委員会資料に含まれている公開鍵暗号評価小委員会の一応の結論である。非常に重要なので、これについて触れる。

これによると、PSEC-KEM を不採用にした理由は以下の 3 点である。

(1) 一般に鍵共有法が満たすべき安全性は、その使用目的や使用環境により異なると考えられる。ハイブリッド暗号の一構成要素としての安全性は達成されているが、鍵共有法を含め、それ以外の応用についての安全性概念や利用方法は現在まだ研究段階にあり、明確になっているとはいえない。また、応募書類でもそのような明確な記述はない。

(2) KEM 技術の応用については今後更なる進展があることが予想されるので、不適切な利用方法がなされないよう、十分にその意義や安全性を確認した上で電子政府に採用しても遅くはない。実際、ISO 標準化の段階(NP, WD, CD, FCD, DIS, IS)のうち、現状はまだ WD であり、次のステップとして MAC, SKE, さらに KEM で知られる KDF 選定があげられており、IS 化へ到達するにはまだ時間がかかると考えられる。したがって、KEM を用いた技術については、これからの動向を注視し、仕様や推奨技術等の確定を待ってからシステムへの導入を検討すべきである。

(3) PSEC-KEM はその楕円曲線ドメインパラメータの選択方法について、SECG などを参照せよ、と言及するにとどまっており、安全性についての配慮が十分に説明されているとは言いがたい。

まず、(1) については、応募された PSEC-KEM が、ハイブリッド暗号で NM-CCA2 を達成できること、単独で、適応的選択暗号文攻撃に対して識別不可能性が示されていることを、どう評価するかである。実用上、十分な安全性を持つと考える。

なお、評価委員会は、応募暗号自体が安全で今後 10 年間使えるかどうかを評価すればいいのであって、それをクリアしているなら、落とす理由はない。もし、研究段階とか今後の動きが明確でないという理由で落すなら、公募の時点で、それを明記しておくべきである。

次の(2)も同様の論理から、落す理由にはならない。

結局、残った問題は、(3)の、楕円曲線の選択に関しては SECG などを参照せよ、と記述されているのみで、具体的に述べていないと言う点である。楕円曲線の選択については、確かに、提案書の不備といえなくもない。また、利用者からすると、選択法も記述されて

いたほうが望ましいと言える。

しかし、利用者に情報がなくて全く決められないというならともかく、一応広く知られている参照先が示してあり、しかも、この参照先は広く知られていて、実装する際によく参照されている。これを参照して安全性の低いパラメータを選択する可能性は低い。他方式との比較から見て優位な点もあることも考え合わせると、参照先を示してあるのに具体的な選択方法に触れていないということが、落す理由の一つになるほどではないと思われる。

8. 結論

以上、結論としては、PSEC-KEM を落とすに足る理由は見当たらない。

参考文献

[1] 日本電信電話株式会社、PSEC-KEM 仕様書、2002 年 5 月 14 日

[2] 日本電信電話株式会社、PSEC-KEM 自己評価書

[3] 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

[4] 公開鍵暗号評価小委員会資料

[5] R. Cramer and V. Shoup, “A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack”, Proc. of CRYPTO'98, pp.13-25, Spriger-Verlag, 1998

[6] J. Jonsson and B. Kaliski, “On the Security of RSA Encryption in TLS”, Advances in Cryptology, CRYPTO2002, LNCS 3442, pp.12y-145

[7] B. Kaliski, “Key Encapsulation: An Emerging Paradigm for Public-Key Cryptography”, RSA-Conference-2002-Japan (May/29-30/2002), Conference Note, 2002

[8] V. Shoup, “A Proposal for an ISO Standards for Public Key Encryption (version 2.1)” December 20, 2001.
Available at http://shoup.net/papers/
Also at ePrint Archive http://eprint.iacr.org/2001/112

[9] NESSIE security report (version 1.0), NES/DOC/ENS/WP5/D20/1, 2002/10/21
Available at https://www.cosic.esat.kuleuven.ac.be/nessie/

[10] R. Cramer and V. Shoup, “Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack, http://shoup.net/papers/2001/12/17

[11] L. Granboulan, “RSA Hybrid Encryption Schemes”, http://eprint.iacr.org/2001/110

[12] M. Bellare, A. Desai, D. Pintcheval and P. Rogaway, “Relations Among Notions of

Security for Public-Key Encryption Schemes", Advances in Cryptology, CRYPTO'98, Springer-Verlag, LNCS 1462, pp.26-45, 1998