各ページ内での各項目の記入スペースの配分は応募者の任意とする	受付番号	

暗号技術概要説明書

１．暗号名：PSEC 暗号（ピーセック暗号）

分類： (1.)公開鍵暗号　　2．共通鍵暗号　　3．ハッシュ関数　　4．疑似乱数生成

詳細分類	公開鍵暗号	(1). 守秘　　2．認証　　3．署名　　4．鍵共有
	共通鍵暗号	1．ストリーム暗号　2．６４ｂｉｔブロック暗号　3．１２８ｂｉｔブロック暗号

２．暗号の概要

２．１ 設計方針：

PSEC 暗号は以下のような要求条件に答えるために作られた秘匿目的の公開鍵暗号方式である。

（１）最強の意味の安全性（適応的選択暗号文攻撃に対して強秘匿／頑健）を保証する理論的証明があること（適当な仮定の下で）。

（２）楕円ElGamal暗号などの楕円離散対数問題に基づく代表的な公開鍵暗号と同等の実用性を有すること。

（３）適当な共通鍵暗号と併用した場合、そのハイブリッドな暗号方式の安全性が最強の意味で理論的に保証されていること（通常、公開鍵暗号は共通鍵暗号と併用され、ハイブリッドな暗号として利用されることに注意）。

そのような最強の意味の安全性を持った実用的な暗号を設計するために我々がとった方針は、Bellare, Rogaway の OAEP の提案以来標準的なアプローチとなった（実用的なハッシュ関数を理想的なランダム関数とみなして安全性を証明する）ランダムオラクルモデルである[1]。PSEC 暗号の基本暗号（暗号プリミティブ）は、その基本的な安全性が 楕円 Diffie-Hellman 問題の困難性と等価である楕円 ElGamal 暗号関数を用いている。また、ランダムオラクルモデル（ハッシュ関数）に基づく変換方式としては、３種類の方法（FO-1 法, FO-2 法, OP 法）[2,3,4]を用いる。それぞれの変換方式に応じて３つの暗号方式（暗号スキーム）が構成でき、それらをそれぞれ PSEC-1, PSEC-2, PSEC-3 と呼ぶ。このように変換された暗号方式は、そこで用いられたハッシュ関数が理想的なランダム関数と仮定し（ランダムオラクルモデル）、かつ楕円 ElGamal 暗号関数の基本的な安全性を仮定し、さらに併用される共通鍵暗号の基本的な安全性を仮定すれば、最強の意味での安全性（適応的選択暗号文攻撃に対して強秘匿／頑健であること）が証明できる。また、SHA のような実用的なハッシュ関数を用いれば、基本暗号および共通鍵暗号と同等の実用性を保持する。

２．２ 想定するアプリケーション：

PSEC-1, PSEC-2, PSEC-3 それぞれが以下のようなアプリケーションを持つ。

（１）PSEC-1：
- 共通鍵暗号の鍵（高々 128 ビット）の配送。
- 短いデータ（高々 256 ビット）の秘匿通信。

（２）PSEC-2：
- 任意の長さの共通鍵暗号鍵の配送。
- 適当な共通鍵暗号と併用することによる長い平文の秘匿通信、特にカプセル的な利用方法（つまり、鍵配送とデータ配送が同期しているような利用形態）

（３）PSEC-3：
- 任意の長さの共通鍵暗号鍵の配送。
- 適当な共通鍵暗号と併用することによる長い平文の秘匿通信、特にカプセル的な利用方法（つまり、鍵配送とデータ配送が同期しているような利用形態）
- 適当な共通鍵暗号と併用することによる長い平文の秘匿通信、特にセッション的利用方法（つまり、セッション開設時における鍵配送とそれ以降の該セッション開設中の複数回の共通鍵暗号によるデータ暗号化）

各ページ内での各項目の記入スペースの配分は応募者の任意とする	受付番号	

２．３ ベースとして用いる理論、技術：

（１）基本暗号関数(暗号プリミティブ)としては､その基本的な安全性(一方向性)が楕円 Diffie-Hellman 問題の困難性と等価である ElGamal 暗号関数を利用した。

（２）ランダムオラクルモデルを用いて、最強の意味での安全性（適応的選択暗号文攻撃に対して強秘匿／頑健）を持つ方式に変換する独自の方式[2,3,4]を開発し、その変換方式を用いて PSEC-1, PSEC-2, PSEC-3 を設計した。特に、PSEC-2, PSEC-3 で用いた変換方式は、公開鍵暗号の最も代表的な利用方法である共通鍵暗号との併用（ハイブリッドな利用法）における（ランダムオラクルモデルにおける）理論的な（最強の意味での）安全性を証明した世界初の変換方式である[3,4]。

（３）PSEC-3 で用いた変換方式は、単にハイブリッドな利用方法に理論的安全性の根拠を与えるだけでなく、ハイブリッドな利用方法の中でも、セッション的利用方法（つまり、セッション開設時に公開鍵暗号機能を用いて鍵配送を行い、それ以降の該セッション開設中に配送済みの鍵を用いて複数回の共通鍵暗号によるデータ暗号通信を行うという利用方法）においてもセッション開設中の暗号通信全体の安全性を理論的に（ランダムオラクルモデルで）保証することができる。また、効率的なハッシュ関数を用いた場合、PSEC-3 の効率性は、そこで用いた基本暗号関数と共通鍵暗号の効率とほぼ同様である（つまり、効率的にほぼ極限まで達成した方式であり、PSEC-3 の処理速度は、楕円 ElGamal 暗号と共通鍵暗号の処理速度とほぼ同じである）。

利用実績・参考文献等：

利用実績：なし

主要な参考文献：

[1] Bellare, M. and Rogaway, P. : Optimal Asymmetric Encryption, Proc. of Eurocrypt'94, LNCS 950, Springer-Verlag, pp.92-111 (1995).

[2] Fujisaki, E. and Okamoto, T.: How to Enhance the Security of Public-Key Encryption at Minimum Cost, Proc. of PKC'99, Springer-Verlag, LNCS 1560, pp. 53--68 (1999).

[3] Fujisaki, E. and Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes, Proc. of Crypto'99, Springer-Verlag, LNCS 1666, pp. 535--554 (1999).

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