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：ESIGN 署名（イーサイン署名）

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：

ESIGN 署名は以下のような要求条件に答えるために作られた署名目的の公開鍵暗号方式である。

（１）最強の意味の安全性（適応的選択文書攻撃に対して存在的偽造不可）を保証する理論的証明があること（適当な仮定の下で）。

（２）RSA 署名や楕円 DSS 署名、楕円 Schnorr などの代表的なディジタル署名方式のいずれよりも優れた性能を保持すること。

そのような最強の意味の安全性を持った実用的なディジタル署名方式を設計するために我々がとった方針は、Bellare, Rogaway 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]。ESIGN 署名の基本署名関数（暗号プリミティブ）は、その基本的な安全性が素因数分解の困難性と同等であると予想されている e 乗根近似関数（基本 ESIGN 関数）[2]を用いている。この基本 ESIGN 署名関数をハッシュ関数を用いて変換した署名方式は、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）、かつ基本 ESIGN 署名関数の基本的な安全性（一方向性： e 乗根近似仮定）を仮定すれば、最強の意味での安全性（適応的選択文書攻撃に対して存在的偽造不可であること）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 ESIGN 署名関数と同等の実用性を保持する。基本 ESIGN 署名関数は RSA 署名に比べて署名速度が数十倍高速であるため、提案する ESIGN 署名は RSA 署名に比べて署名速度が数十倍高速であることを特長とする（なお、署名検証速度は RSA 署名とほぼ同等である）。また、楕円 DSS 署名や楕円 ElGamal 署名と比べても数倍以上高速である。

想定するアプリケーション：

（１） 通常の電子署名アプリケーション：ESIGN 署名は、ディジタル署名（電子署名）が適用可能な全てのアプリケーションに適用可能である。 特に ESIGN 署名は高速処理を特長としており、多くの文書に対する署名作成処理を一括処理する必要のある（認証機関などの）署名サーバーや、IC カードや携帯端末などのローエンドの低機能端末における署名処理に適している。

（２） 利用者認証：サーバー等が利用者の正当性を検証するシステムにおいて、事前に利用者の公開鍵をサーバーに登録しておき、利用者の正当性をサーバーが認証するときは、サーバーは利用者に乱数を送り、それに対して利用者が署名をサーバーに返し、その署名の正当性を確認することで利用者の正当性を確認することができる。

２．３ ベースとして用いる理論、技術：

（１）独自の基本署名関数（暗号プリミティブ）である基本 ESIGN 署名関数を 15 年前に開発した[1,2]。この基本 ESIGN 署名関数の基本的安全性（一方向性：e 乗根近似仮定）に関しては、様々な研究が行われてきたが、関数の次数 e が 4 以上の場合については、現在まで有効な攻撃は発見されておらず [3,4,5,6]、提案者らは素因数分解以外に有効な攻撃法が無いと予想している。さらに、ここで用いた法 $n = p^2q$ の素因数分解のアルゴリズムについても研究がされてきたが、特に固有の有効なアルゴリズムは発見されていない [7,8,9]。

（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（適応的選択文書攻撃に対して存在的偽造不可）を持つ方式に変換した [10]。

利用実績・参考文献等：

利用実績：

・IC カード上での電子署名システムや電子マネーシステム、電子公証・認証システム
・ISO/IEC 14888-3 (Digital Signature Algorithms with Appendix) で標準化済
・IEEE P1363a に採用（IEEE P1363a/D4 (Draft Version 4), May 22, 2000 に採用済）

主要な参考文献：

[1] Okamoto, T. and Shiraishi, A.: A Fast Signature Scheme Based on Quadratic Inequalities, Proc. of the ACM Symposium on Security and Privacy, ACM Press (1985).
[2] Okamoto, T.: A Fast Signature Scheme Based on Congruential Polynomial Operations, IEEE Trans. on Inform. Theory, IT-36, 1, pp.47-53 (1990).
[3] Brickell, E. and DeLaurentis, J.:An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.28-32 (1986)
[4] Brickell, E. and Odlyzko: Cryptanalysis: A Survey of Recent Results, Chap.10, Contemporary Cryptology, Simmons (Ed.), IEEE Press, pp.501--540 (1991).
[5] Girault, M., Toffin, P. and Vall{\'e}e, B.: Computation of Approximate L-th Roots Modulo n and Application to Cryptography, Proc. of Crypto'88, LNCS 403, Springer-Verlag, pp.100-117 (1990)
[6] Vall{\'e}e, B., Girault, M. and Toffin, P.: How to Guess L-th Roots Modulo n by Reducing Lattice Bases, Proc. of Conference of ISSAC-88 and AAECC-6 (1988)
[7] Peralta, R.: Bleichenbacher's improvement for factoring numbers of the form $N=PQ^{2}$ (private communication) (1997).
[8] Peralta, R. and Okamoto, E.: Faster Factoring of Integers of a Special Form, IEICE Trans. Fundamentals, E79-A, 4, pp.489-493 (1996).
[9] Pollard, J.L.: Manuscript (1997).
[10] Okamoto, T., Fujisaki, E. and Morita, H.: TSH-ESIGN: Efficient Digital Signature Scheme Using Trisection Size Hash, submission to P1363a (1998).