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： HDEF-ECDH

(Higher Degree Extension Field - Elliptic Curve Diffie-Hellman Key-Agreement)

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：

既存の解読アルゴリズムに対して安全であり，かつユーザ毎に容易に楕円曲線を生成できる，ワンタイムパスワード的な使い捨て楕円曲線を可能にした汎用楕円曲線Diffie-Hellman鍵共有法(汎用ECDH鍵共有法)を設計する．

具体的な設計方針は以下の通りである．

1. 楕円曲線上の離散対数問題（ECDLP）に対する exhaustive 攻撃に相当する Pohlig-Hellman, Pollard-ρ 法に対する耐攻撃性を高めるため、素数位数の楕円曲線 E / F_q とする．
2. 近年の Weil decent の攻撃可能性を削減するため、素体上の楕円曲線 E / F_q とする．
3. SSSA に対する耐攻撃性を確保するため、$\#E(F_q) \neq q$ とする．
4. FR-帰着に対する計算量的耐性（i.e. 帰着拡大次数 $k > \log q$ ）を保証する．
5. 楕円曲線がシステマティックに容易に構成できる．
6. 楕円曲線 Diffie-Hellman 鍵共有法(ECDH 鍵共有法)を拡張し，ユーザ毎に利用する楕円曲線が異なっていても鍵共有が可能であり，同じ楕円曲線を利用している場合は，ECDH 鍵共有法により鍵共有が可能になるスキームを実現する．

FR-帰着法に対する明確な条件に関する研究を 99 年度より行ってきたが，今回，初めて FR-帰着法に対する安全性が保証できる条件を導き出した．本条件により，以上の設計方針を満足する楕円曲線を用いることを特徴とした汎用 ECDH 鍵共有法を提案する．(詳細な証明は自己評価書に記載)

2．2 想定するアプリケーション：

本提案暗号技術は，FR-帰着法に対する安全性の保障された楕円曲線をシステマティックに容易にコンパクトな実装で構成できることを特徴に持つ．本提案暗号技術で用いている ECDLP プリミティブは，DLP に基づく任意のスキームに対して利用可能であるが，最も有効な利用が望める ECDH 鍵共有法をスキームとし，特に安全性を強化したい場合のアプリケーションでの利用を想定する．

ECDH 鍵共有法の場合，通常楕円曲線はシステムで共通に利用されることが多い．しかし近年の傾向として，特定の楕円曲線に対して ECDLP が解読されることからも，特定の楕円曲線を複数のユーザが利用するシステムは安全上好ましくない．本提案 汎用 ECDH 鍵共有法では，容易でコンパクトな楕円生成を有し，例えばスマートカードなどでワンタイムパスワード的に楕円曲線を生成し，生成した楕円曲線を用いて鍵共有を実現することが可能となる．本提案汎用 ECDH 鍵共有法は，ユーザが同じ楕円曲線を用いる場合は，従来の IEEE1363 等で標準化されている公開鍵付 ECDH 鍵共有法と一致する．また，ユーザ間で異なる楕円曲線を利用する場合でも，それぞれの ECDH の安全性に帰着する ECDH 鍵共有法を与える．またこの際に，それぞれが鍵共有の度に楕円曲線を生成したい場合は，非常にコンパクトでかつ高速な楕円曲線生成アルゴリズムを可能にする．言うまでもないが，従来どおりの固定した楕円曲線を想定し，それにより ECDH 鍵共有法を実現することも可能である汎用的な方式である．

２．３ ベースとして用いる理論、技術：

前項で述べた設計方針を満足するために我々が導いた結果を示す。
（詳細な証明は自己評価書に記載）

定理１ E/F_q を F_q 上定義された楕円曲線，t を E/F_q のトレースとする。FR-帰着によって，E/F_q 上のECDLPが $F_{q^k}^*$ 上のDLPに帰着できるとする。この時，$t \geq 3$ に対して，拡大次数 k は次を満たす。

$$k > \frac{\log q}{\log(t-1)}$$

系１ E/F_q を F_q 上定義された楕円曲線，E/F_q を $t=3$ とする。FR-帰着によって，E/F_q 上のECDLPが $F_{q^k}^*$ 上のDLPに帰着する時，拡大次数 k は次を満たす。

$$k > \log q$$

上の系1.の結果から，t=3の時，FR-帰着によって帰着されるDLPは，拡大次数が十分大きいため，現在提案されている最高速の解読を用いても指数時間が要求されることが保証できる.

利用実績・参考文献等：

1. A. Miyaji and H. Shizuya, "Integration of DLP-based cryptosystems", ICICE Japan Tech. Rep., ISEC99-48, (1999-9), 73-80
2. 高野俊三, 宮地充子, "Some explicit conditions for FR-reduction", *第３回「代数幾何・数論及び符号・暗号」*,(2000), 74-85
3. A. Miyaji M. Nakabayashi and S. Takano, "New relation between FR-reduction and elliptic curve traces", ISEC2000-9 発表予定