＜解説：楕円曲線暗号の原理と国際規格について＞

SC 27/WG 2小委員会
委員　宮地 充子（北陸先端科学技術大学院大学）

1. はじめに

ISO/IEC JTC 1/SC 27/WG 2では，情報セキュリティのアルゴリズム及びプロトコルに関する国際規格の策定を進めている．その中の1つのプロジェクトである15946はcryptographic techniques based on elliptic curves（楕円曲線に基づく暗号手法）に関する国際規格を定める．15946は4つの技術から構成される．この度，著者がプロジェクトエディタを務める15946-4の国際規格が完成し，15946の全4技術の国際規格が発行されることになった．本稿においては，楕円曲線暗号の原理について解説すると共に，国際規格となった15946-4を含む15946に関して解説する．楕円曲線暗号及び暗号全般に関して，詳しく知りたい読者は参考文献 1)を，また楕円曲線について興味を持たれた読者は，2)を読まれることをお薦めする．

2. 楕円曲線暗号

楕円曲線暗号とは，1985年に発表された楕円曲線上の離散対数問題（ECDLP）の難しさを安全性の根拠にする暗号である．一般に楕円曲線暗号とは，ECDLP に基づく公開鍵暗号の総称であり，メッセージの秘匿を実現する暗号，完全性を実現するディジタル署名，鍵共有法等の機能が実現できる．エルガマル暗号やDSA署名などの既存の有限体上の離散対数問題（DLP）を用いる暗号系は，すべて楕円曲線暗号に変換できる．ECDLPはDLPに対する強力な解法である指数計算法が直接適用できないことから，同じ安全性を高速かつコンパクトに実現できるとして，有望な公開鍵暗号系として盛んに研究されるようになった．

2.1 楕円曲線暗号と有限体上の暗号の違い

楕円曲線暗号と有限体上の暗号にはプロトコル自体の大きな違いはない．基本的に有限体の元を楕円曲線の元に，有限体の乗法を楕円曲線の加法に対応させて，双方のプロトコルが実現できる．両者の大きな違いは，その安全性であるECDLPとDLP上の既存攻撃にある．DLPに対する攻撃である指数計算法やその改良は，全てのDLPに準指数時間の攻撃を与える．このため，10^{12}MIPS年の安全性を確保するには1,024ビット程の大きさの有限体が必要になる．一方ECDLPには，任意の楕円曲線に対して適用可能な準指数時間攻撃は提案されていない．この結果，指数時間攻撃しか存在しない楕円曲線が構成でき，現時点では160ビット程の大きさで同じ安全性が実現できる．

2.2 楕円曲線

暗号で利用する楕円曲線について簡単に述べる．

楕円曲線とは，有限体F_p ($p \geqq 5$ の素数)の元a，bに対して，

$$E: y^2 = x^3 + ax + b \quad (D = 4a^3 + 27b^2 \neq 0) \quad (1)$$

で定まる曲線である．ここで$D = 4a^3 + 27b^2$ は判別式と呼ばれる．楕円曲線は(1)を満たす点の集合であるが，$x \to \infty$のとき$y \to \infty$と考えて，無限遠点$O=(\infty, \infty)$もEの点になる．特に，楕円曲線のF_p-有理点の集合を，

$$E(F_p) = \{ (x,y) \in F_p^2 \mid y^2 = x^3 + ax + b \} \cup \{O\}$$

で定める．楕円曲線のパラメータa，bを含む体 F_p を楕円曲線Eの定義体と呼ぶ．楕円曲線には O が零元になるような加法が定義でき，高々数回の定義体上の演算で実現できる．この加法により$E(F_p)$は有限可換群になり，暗号系が構成できることになる．

2.3 楕円曲線暗号の例

具体的な楕円曲線暗号として楕円ディッフィ・ヘルマン鍵共有法について紹介する．楕円曲線暗号の安全性は，有限体F_p上の楕円曲線E/F_p上の離散対数問題（ECDLP）に基づく．ここで，ECDLPについて定義する．

定義[ECDLP]
有限体 Fp 上の楕円曲線E/F_p，E(Fp) $\ni$ G，Y に対して，

$$Y = xG = G + \cdots + G \quad (\text{Gのx回の和})$$

となる x が存在するなら，そのxを求めよ．　■

ECDLPにおいて楕円曲線とその加法の代わりに有限体とその乗法を用いる問題，すなわち$y=g^x \pmod p$よりxを求める問題がDLPである．

以下E/F_pを楕円曲線とし，$G \in E(F_p)$を位数（$lG=O$となる最小の正整数 l）が大きな素数 lの元とする．$E(F_p)$及びGはシステム内で共通に利用されるデータで，システムパラメータと呼ばれる．

ユーザAの鍵生成
1．乱数 $x_A \in \{1, \cdots, l-1\}$を選ぶ．
2．$P_A = x_A G$を計算する．
3．x_Aを秘密鍵，P_Aを公開鍵として出力する．
ユーザBも同様に鍵 (x_B, P_B)を生成する．

鍵共有
AとBが通信なしに，それぞれの公開鍵P_A，P_Bを利用して，鍵を共有する場合を考える．

1．Aは公開ファイルからBの公開鍵P_Bを入手し，

$$K_{A,B}=x_AP_B = x_A\ x_BG$$

を計算する．

2．Bは公開ファイルからAの公開鍵P_Aを入手し，

$$K_{B,A} = x_BP_A=x_Bx_AG$$

を計算する．

3．AとBはE(K)の元$K_{A,B}=K_{B,A}$を鍵として共有する．

3．国際規格15946（楕円曲線に基づく暗号手法）について

楕円曲線に基づく暗号手法の国際規格を定める15946は，General（楕円曲線全般）の規格（15946-1），Digital signatures（添付型署名）の規格(15946-2)，Key establishment（鍵確立）の規格(15946-3)，Digital signatures giving message recovery（メッセージ回復型署名）の規格（15946-4）の4つから構成される．15946-1，2，3の各パートは1998年から審議が始まり2002年に国際規格に，15946-4 は2000 年から審議が始まり，2004 年に国際規格となった，

15946-1 は楕円曲線暗号を実現する際に必要になる要素，楕円曲線のパラメータの生成方法やその検証方法，楕円曲線の元を整数に変換する方法等の規格である．付属書として，楕円曲線の各種加算公式も記載されている．15946-2 は楕円曲線を用いたディジタル署名の規格である．具体的な方式として，EC-GDSA（ドイツ），EC-DSA（米国），EC-KCDSA（韓国）の各方式が規格化されている．15946-3 は楕円曲線を用いた鍵共有法の規格である．Key establishmentの技術はKey agreement（鍵共有）とKey transport（鍵輸送）からなる．Key agreementにおいては，鍵共有を行うエンティティはそれぞれ対等であり，どのエンティティも共有鍵の値を予め決定できない．Key transportにおいては，一方が共有する鍵を決定し他方に輸送することで鍵確立を行う．15946-3では，これら2種類のKey establishmentとして，全10方式が規格化されている．15946-4は楕円曲線を用いたメッセージ回復型署名の規格である．15946-2ではメッセージの全てが署名検証の入力に必要な署名方式を取り扱うのに対し，15946-4ではメッセージの一部が署名検証の入力に必要になる，あるいはメッセージの入力を必要としない署名方式を取り扱う．本規格においてはメッセージ回復型署名具体的な方式として，ECNR（フィンランド），ECMR（日本，松下電器），ECAO（日本，NTT），ECPV（米国），ECKNR（韓国）の各方式が規格化されている．

4．おわりに

楕円曲線暗号は必要な安全性を小さな鍵サイズで実現できるため，有限体上の暗号より高速かつコンパクトに実現できる．今後，携帯電話などの携帯端末の高機能化に伴い，暗号機能の装備は必須となるだろう．このとき楕円曲線暗号のはたすべき役割は非常に大きい．また楕円曲線暗号の研究開発分野における日本の技術水準は非常に高い．本国際規格が楕円曲線暗号の普及への布石となり，高セキュリティ機能を掲載した端末が普及することを願う．

参考文献

1) 宮地充子，菊池浩明 共編：情報セキュリティ，オーム社（2003）．
2) 山本芳彦：現代数学への入門 -- 数論入門 2 --，岩波書店（1996）．