

电力系统集团加密通信与集团签署—认证

史开泉¹, 陈泽雄²

(1. 山东大学数学与系统科学学院, 山东省济南市 250100; 2. 大叶大学资讯工程系, 台湾彰化 515)

摘要: 设在电力系统中有两个集团, 各集团成员分别具有共同的经济—技术利益和法律责任。文中提出具有这些特征的电力系统集团加密通信与集团签署—认证系统, 给出了集团加密通信系统的数学结构, 加密—解密算法和集团秘密钥匙、集团公开钥匙的生成方法; 给出了集团签署与集团认证算法。所给出的电力系统集团加密通信和集团签署—认证具有工程应用的一般性。

关键词: 电力系统; 椭圆曲线; 集团加密与解密; 集团秘密钥匙; 集团公开钥匙; 集团签署; 认证定理

中图分类号: TM73; TP309

0 引言

自从 1987 年 N. koblitz 提出 Elliptic Curve Cryptosystems^[1], 椭圆曲线加密理论与技术引起了人们的重视。椭圆曲线加密理论与加密技术在不同工程系统中的信息安全研究中得到了应用^[2~8]。将信息加密理论、电力系统两个彼此独立的学科进行相互交叉、相互渗透、互补共享的研究将成为电力系统通信的一个新的研究方向, 该超前性研究方向或许正在引起人们的注意和重视。例如核电技术是国家的核心机密之一, 在核能生产中不可避免地要进行核电技术交流、核电事故诊断, 这些活动一般都在因特网上完成; 又如, 电力系统市场化之后, 发电集团的竞价信息、电力调度的实时信息和非实时信息也要通过因特网完成传输。因此, 电力系统信息的安全性及数据的加密与认证的研究已迫在眉睫。

本文提出满足下列特征的电力系统集团加密通信与集团签署—认证问题:

设 A, B 是电力系统中两个进行核电技术合作或进行数据信息交换的集团, $A = \{A_1, A_2, \dots, A_r\}$, $B = \{B_1, B_2, \dots, B_t\}$; A 上的成员 A_1, A_2, \dots, A_r 具有共同的经济—技术利益和法律责任; B 上的成员 B_1, B_2, \dots, B_t 具有共同的经济—技术利益和法律责任。对 A 中的任意一个成员 A_j , A_j 的利益和责任必须得到保护, 拒绝 $A_1, A_2, \dots, A_{j-1}, A_{j+1}, \dots, A_r$ 对 A_j 的利益和责任的侵犯和强加; 与此相似, 对 B 中的任意一个成员 B_i , B_i 的利益和责任必须得到保护, 拒绝 $B_1, B_2, \dots, B_{i-1}, B_{i+1}, \dots, B_t$ 对 B_i 的利益和责任的侵犯

和强加。简而言之, $\{A_1, A_2, \dots, A_r\}$ 在利益、责任的限定下共同把核电技术明文(或数据信息明文) P_m 加密成核电技术密文(或数据信息密文) C_m , 把 C_m 送至 $\{B_1, B_2, \dots, B_t\}$ 。在对 P_m 加密成 C_m 的过程中, A_1, A_2, \dots, A_r 一个都不能缺席, 若 A_j 缺席, 将发生 $r - 1$ 个 A_j 集体篡改 P_m , 用篡改后的 P_m 对 A_j 进行集体欺诈。 $\{B_1, B_2, \dots, B_t\}$ 接收到 $\{A_1, A_2, \dots, A_r\}$ 送来的密文 C_m , 在对 C_m 解密的过程中, B_1, B_2, \dots, B_t 也一个都不能缺席, 若 B_i 缺席, 将发生 $t - 1$ 个 B_i 集体篡改、伪造 C_m , 以篡改、伪造的 C_m 对 B_i 进行集体欺诈。

本文给出了满足上述特性的集团 $A = \{A_1, A_2, \dots, A_r\}$ 与集团 $B = \{B_1, B_2, \dots, B_t\}$ 之间的核电技术(或数据信息)的加密通信系统, 并给出了集团签署—集团认证。

1 椭圆曲线及其特征

定义 1 由 Weierstrass 方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

确定的满足 $D \neq 0$ 的曲线 $E(K)$ 称为椭圆曲线。

$$E(K) = \{(x, y) | x, y \in K, P(x, y) = 0\} \cup \{O\} \quad (2)$$

式中: $\forall a_i \in \mathbb{N}^+$; K 是一个数域; $P(x, y)$ 是 $E(K)$ 上的点; O 称为无穷远点。

应用中, 一般取式(1)的简化形式:

$$y^2 = x^3 + ax + b \quad (3)$$

式(3)记为 $E_m(a, b)$, m 是一个选择的质数。

定义 2 称 D 是椭圆曲线 $E_m(a, b)$ 的判别式, 如果

$$D = (4a^3 + 27b^2) \bmod m \neq 0 \quad (4)$$

定义 3 称 \oplus 是定义在 $E_m(a, b)$ 上的点加运算,

如果 $\forall P, Q, R \in E_m(a, b)$ 满足：

$$\begin{cases} P \oplus Q \oplus R = O \\ P \oplus Q = Q \oplus P \\ P \oplus (-P) = O \\ (P \oplus Q) \oplus R = P \oplus (Q \oplus R) \\ P \oplus O = P \end{cases} \quad (5)$$

因此，容易得到下面的重要结论：

- a. $E_m(a, b)$ 上的点 P 关于 \oplus 运算构成 Abel 群；
- b. 任取基点 $G \in E_m(a, b)$, G 生成一个闭环 T_G ；
- c. T_G 上的任意一个起点 G' 与终点 G° 满足 $G' = G^\circ$ 。

定义 4 设 $E_m(a, b)$ 是方程(3)确定的椭圆曲线 ($D \neq 0$); $P(x_1, y_1), Q(x_2, y_2)$ 是 $E_m(a, b)$ 上的两点; 称 $R(x_3, y_3)$ 是 $E_m(a, b)$ 上 $(P(x_1, y_1) \oplus Q(x_2, y_2))$ 的生成点, 如果:

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod m \quad (6)$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod m \quad (7)$$

式中: m 是一个选择的质数; λ 满足:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad P(x_1, y_1) \neq Q(x_2, y_2) \quad (8)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad P(x_1, y_1) = Q(x_2, y_2) \quad (9)$$

定义 3、定义 4 分别是椭圆曲线的特性和求取 $E_m(a, b)$ 上点的依据。

利用上面的概念, 我们给出下面的讨论。

2 对称集团加密通信与加密-解密算法

约定 $A = \{A_1, A_2, \dots, A_r\}$, $B = \{B_1, B_2, \dots, B_t\}$ 是秘密通信的两个集团; P_m 是核电技术明文, C_m 是 P_m 的密文; $\{A_1, A_2, \dots, A_r\}$ 是 P_m 的加密者、密文 C_m 的发送者; $\{B_1, B_2, \dots, B_t\}$ 是 C_m 的接收者、 C_m 的解密者。

A 对于 P_m 的加密准则和 B 对于 C_m 的解密准则如下: 若 $|A| < r$, A 把 P_m 加密成 C_m 是非法的; 若 $|A| = r$, A 把 P_m 加密成 C_m 是合法的; 若 $|B| < t$, B 把 C_m 解密成 P_m 是非法的; 若 $|B| = t$, B 把 C_m 解密成 P_m 是合法的。

A 与 B 共同做出的准备如下:

选取椭圆曲线 $E_m(a, b)$:

$$y^2 = x^3 + ax + b \quad (10)$$

且 $D = (4a^3 + 27b^2) \bmod m \neq 0 \quad (11)$
式中: m 是一个质数; $a, b \in \mathbb{N}^+$; D 是椭圆曲线判别式。

满足式(10)的点 $G = (x_i, y_i)$ 构成点集:

$$E_m(a, b) = \{(x_1, y_1), (x_2, y_2), \dots, (x_a, y_a)\} \quad (12)$$

$\{A_1, A_2, \dots, A_r\}, \{B_1, B_2, \dots, B_t\}$ 共同选择基点 $G \in E_m(x_j, y_j)$; A, B 分别给出:

$$n^A = P_A(0) \quad (13)$$

$$P^A = P_A(0)G \quad (14)$$

$$n^B = P_B(0) \quad (15)$$

$$P^B = P_B(0)G \quad (16)$$

式中: n^A, P^A 分别为集团 A 的秘密钥匙、公开钥匙; n^B, P^B 分别为集团 B 的秘密钥匙、公开钥匙。

- a. 集团 $\{A_1, A_2, \dots, A_r\}$ 关于 P_m 的加密与加密算法

集团 $\{A_1, A_2, \dots, A_r\}$ 把 P_m 加密成密文 C_m , 将 C_m 送给集团 $\{B_1, B_2, \dots, B_t\}$, 即 $\{A_1, A_2, \dots, A_r\}$ 取正整数 k , 基点 $G \in E_m(a, b)$, 明文 P_m 和集团 $\{B_1, B_2, \dots, B_t\}$ 的公开钥匙 $P^B, \{A_1, A_2, \dots, A_r\}$ 给出:

$$C_m = \{kG, P_m + kP^B\} = \{kG, P_m + k(P_B(0)G)\} \quad (17)$$

然后, $\{A_1, A_2, \dots, A_r\}$ 送 C_m 给 $\{B_1, B_2, \dots, B_t\}$ 。

- b. 集团 $\{B_1, B_2, \dots, B_t\}$ 关于 C_m 的解密与解密算法

集团 $\{B_1, B_2, \dots, B_t\}$ 接收 C_m , 把 C_m 解密成 P_m , 即 $\{B_1, B_2, \dots, B_t\}$ 取 C_m 中的第 2 项 $C_{m,2} = P_m + kP^B$; 取 C_m 中的第 1 项 $C_{m,1} = kG$ 与集团 $\{B_1, B_2, \dots, B_t\}$ 的秘密钥匙 n^B 之积, $\{B_1, B_2, \dots, B_t\}$ 得到:

$$\begin{aligned} C_{m,2} - C_{m,1} &= P_m + kP^B - n^B(kG) = \\ &P_m + kP^B - k(n^B G) = \\ &P_m + k(P_B(0)G) - \\ &k(P_B(0)G) = P_m \end{aligned} \quad (18)$$

然后, $\{B_1, B_2, \dots, B_t\}$ 获取 P_m 。

对 a, b 的研究, 得出讨论:

若 $A = \{A_1, A_2, \dots, A_r\}$ 闭缩成 $A = \{A_0\}$, $\{A_0\}$ 是只具有一个成员的集团, $\{B_1, B_2, \dots, B_t\}$ 不变。集团 A 的秘密钥匙选为 $n^A = \eta \in \mathbb{N}^+$, 公开钥匙 $P^A = \eta G$; 集团 $B = \{B_1, B_2, \dots, B_t\}$ 的秘密钥匙 n^B , 公开钥匙 P^B , 仍然利用式(15)、式(16), 而且 $n^B = P_B(0)$, $P^B = P_B(0)G$; 则得到非对称集团的椭圆曲线加密通信系统与加密-解密算法。所谓非对称集团是指满足条件: $|A| \ll |B|$; 因此得到:

- c. 集团 $\{A_0\}$ 把 P_m 加密成 C_m , 送 C_m 给 $\{B_1, B_2, \dots, B_t\}$

$\{A_0\}$ 选择正整数 k , 基点 $G \in E_m(a, b)$, 明文 P_m 和集团 $\{B_1, B_2, \dots, B_t\}$ 的公开钥匙 $P^B, \{A_0\}$ 给出:

$$C_m = \{kG, P_m + kP^B\} = \{kG, P_m + k(P_B(0)G)\} \quad (19)$$

然后, $\{A_0\}$ 送 C_m 给 $\{B_1, B_2, \dots, B_t\}$ 。

d. 集团 $\{B_1, B_2, \dots, B_t\}$ 接收 C_m , 把 C_m 解密成 P_m

$\{B_1, B_2, \dots, B_t\}$ 取 C_m 中的第 2 项 $C_{m,2} = P_m + kP^B$, 取 C_m 中的第 1 项 $C_{m,1} = kG$ 与集团 $\{B_1, B_2, \dots, B_t\}$ 的秘密钥匙 n^B 之积, $\{B_1, B_2, \dots, B_t\}$ 得到:

$$\begin{aligned} C_{m,2} - C_{m,1} &= P_m + kP^B - n^B(kG) = \\ &P_m + kP^B - kP^B = \\ &P_m + k(P_B(0)G) - \\ &k(P_B(0)G) = P_m \end{aligned} \quad (20)$$

然后, $\{B_1, B_2, \dots, B_t\}$ 获取 P_m 。

对 c, d 的研究再给出的讨论:

若 $A = \{A_1, A_2, \dots, A_r\}$ 闭缩成 $A = \{A_0\}$, $B = \{B_1, B_2, \dots, B_t\}$ 闭缩成 $B = \{B_0\}$; $\{A_0\}, \{B_0\}$ 分别是只有一个成员的集团。 $n^A = \eta, P^A = \eta G$ 是集团 A 的秘密钥匙和公开钥匙; $n^B = \varphi, P^B = \varphi G$ 是集团的 B 的秘密钥匙和公开钥匙; $\eta, \varphi \in \mathbb{N}^+, G \in E_m(a, b)$, 则得到:

e. 集团 $\{A_0\}$ 把 P_m 加密成 C_m, C_m 送给 $\{B_0\}$

$\{A_0\}$ 选择正整数 k , 基点 $G \in E_m(a, b)$, 明文 P_m 和集团 $\{B_0\}$ 的公开钥匙 $P^B, \{A_0\}$ 给出:

$$C_m = \{kG, P_m + kP^B\} \quad (21)$$

然后, $\{A_0\}$ 送 C_m 给 $\{B_0\}$ 。

f. 集团 $\{B_0\}$ 接收 C_m , 把 C_m 解密成 P_m

$\{B_0\}$ 取 C_m 中的第 2 项 $C_{m,2} = P_m + kP^B$, 取 C_m 中的第 1 项 $C_{m,1} = kG$ 与集团 $\{B_0\}$ 的秘密钥匙 n^B 之积, $\{B_0\}$ 得到:

$$\begin{aligned} C_{m,2} - C_{m,1} &= P_m + kP^B - n^B(kG) = \\ &P_m + kP^B - k(n^B G) = \\ &P_m + kP^B - kP^B = P_m \end{aligned} \quad (22)$$

然后, $\{B_0\}$ 获取 P_m 。

显然, 式(21)、式(22)是我们在一般的椭圆曲线加密系统中经常看到的。

这里指出: 若 $B = \{B_1, B_2, \dots, B_t\}$ 是 P_m 的加密者, C_m 的发送者; $A = \{A_1, A_2, \dots, A_r\}$ 是 C_m 的接收者, C_m 的解密者, 可以得到与 a~f 类似的结果。

3 对称集团秘密钥匙与公开钥匙的数学结构与生成

下面, 仅给出集团 $\{A_1, A_2, \dots, A_r\}$ 的秘密钥匙 n^A 、公开钥匙 P^A 的数学结构与生成; 集团 $\{B_1, B_2, \dots, B_t\}$ 的秘密钥匙 n^B 、公开钥匙 P^B 的数学结构和生成与 n^A, P^A 相似。

设 $n^{A_1}, n^{A_2}, \dots, n^{A_r}$ 分别是集团 A 的成员 A_1, A_2, \dots, A_r 的秘密钥匙, $\forall n^{A_j} \in \mathbb{N}^+, j=1, 2, \dots, r$; a 是 A_1, A_2, \dots, A_r 共同选择的一个原根, $a \in \mathbb{N}^+$; p 是 A_1, A_2, \dots, A_r 共同选择的一个质数。

3.1 集团秘密钥匙、公开钥匙的多项式生成

利用 $a, n^{A_i}, p, i=1, 2, \dots, r$; 得到 A_1, A_2, \dots, A_r 的特征值 y_1, y_2, \dots, y_r , 且

$$\begin{cases} y_1 = a^{n^{A_1}} \bmod p \\ y_2 = a^{n^{A_2}} \bmod p \\ \vdots \\ y_r = a^{n^{A_r}} \bmod p \end{cases} \quad (23)$$

由式(23)得到二元序列:

$$(1, y_1), (2, y_2), \dots, (r, y_r) \quad (24)$$

由式(24)得到集团 A 的特征多项式 $P_A(x)$:

$$\begin{aligned} P_A(x) &= \sum_{j=1}^r y_j \prod_{\substack{i=1 \\ i \neq j}}^r \frac{x - x_i}{x_j - x_i} \bmod p = \\ &a_{r-1}x^{r-1} + a_{r-2}x^{r-2} + \dots + a_1x + a_0 \bmod p \end{aligned} \quad (25)$$

令 $x=0$, 得到集团 $\{A_1, A_2, \dots, A_r\}$ 的秘密钥匙 n^A 、公开钥匙 P^A , 且

$$n^A = P_A(0) \quad (26)$$

$$P^A = P_A(0)G \quad (27)$$

式中: G 是第 2 节中 $\{A_1, A_2, \dots, A_r\}, \{B_1, B_2, \dots, B_t\}$ 共同选择的基点, $G \in E_m(a, b)$ 。

这里需要指出: 集团秘密钥匙 $n^A = P_A(0)$ 选择的优点是: 从式(23)中可以看到, 若 n^{A_j} 是 A_j 的秘密钥匙, $A_j \in A$; 显然 n^{A_j} 不会被 $\{A_1, A_2, \dots, A_{j-1}, A_{j+1}, \dots, A_r\}$ 获取, 不会被不法之徒盗取和篡改; 这是因为从

$$y_j = a^{n^{A_j}} \bmod p \quad (28)$$

求取 n^A 是一个求解离散对数问题, 求解离散对数到目前为止不存在有效算法, 从式(28)中求 n^{A_j} 是困难的。

3.2 集团秘密钥匙与公开钥匙的乘积生成

A 的成员 A_1, A_2, \dots, A_r 共同选择质数 $p; n^{A_1}, n^{A_2}, \dots, n^{A_r}$ 分别是 A_1, A_2, \dots, A_r 的秘密钥匙; a 是 A_1, A_2, \dots, A_r 共同选择的原根^[9]; $\forall n^{A_j} \in \mathbb{N}^+, j=1, 2, \dots, r; a \in \mathbb{N}^+$ 。 n^A 是集团 $\{A_1, A_2, \dots, A_r\}$ 的秘密钥匙, P^A 是集团 $\{A_1, A_2, \dots, A_r\}$ 的公开钥匙, 且

$$n_A = a^{n^{A_1}} a^{n^{A_2}} \cdots a^{n^{A_r}} \bmod p = \prod_{i=1}^r a^{n^{A_i}} \bmod p \quad (29)$$

$$P^A = n^A G = \left(\prod_{i=1}^r a^{n^{A_i}} \bmod p \right) G \quad (30)$$

B 的成员 B_1, B_2, \dots, B_t 共同选择质数 $q; n^{B_1}, n^{B_2}, \dots, n^{B_t}$ 分别是 B_1, B_2, \dots, B_t 的秘密钥匙; b 是 B_1, B_2, \dots, B_t 共同选择的原根; $n^{B_i} \in \mathbb{N}^+, i=1, 2, \dots, t; b \in \mathbb{N}^+$ 。 n^B 是集团 $\{B_1, B_2, \dots, B_t\}$ 的秘密钥匙, P^B 是集团 $\{B_1, B_2, \dots, B_t\}$ 的公开钥匙。 n^B, P^B 的形式与

式(29)、式(30)类似,此处从略。

4 对称集团签署-集团认证与算法

约定: $A=\{A_1, A_2, \dots, A_r\}$, $B=\{B_1, B_2, \dots, B_t\}$ 是秘密通信集团; $1 \ll r, t; m$ 是签署明文; $h(\cdot)$ 是 $\{A_1, A_2, \dots, A_r\}$ 与 $\{B_1, B_2, \dots, B_t\}$ 共同选择的 hash 函数, $h(m)$ 是 m 的 hash 函数值; $h(m) \in \mathbb{N}^+$ 。

集团 $\{A_1, A_2, \dots, A_r\}$ 与集团 $\{B_1, B_2, \dots, B_t\}$ 双方共同给出的准备如下:

选取椭圆曲线 $E_n(a, b)$, 质数 n :

$$y^2 = x^3 + ax + b \quad (31)$$

$$D = 4a^3 + 27b^2 \bmod n \neq 0 \quad (32)$$

满足式(31)的点集:

$$E_n(a, b) = \{(x_1, y_1), (x_2, y_2), \dots, (x_a, y_a)\} \quad (33)$$

选择基点 $P; P \in E_n(a, b); a, b \in \mathbb{N}^+$ 。

集团 $\{A_1, A_2, \dots, A_r\}$ 的秘密钥匙 n^A 选为式(26)、式(27)给出的形式。

令 $d=n^A=P_A(0), P_A(0) \in [1, n-1]$; 且

$$Q = P_A(0)P \quad (34)$$

(E, P, Q, n) 公开。

4.1 $\{A_1, A_2, \dots, A_r\}$ 给出 m 的签署 (r, s) , 送 (r, s) 给 $\{B_1, B_2, \dots, B_t\}$

a. $\{A_1, A_2, \dots, A_r\}$ 取 $t=P_A(0), t \in [1, n-1]; t$ 是会话钥匙, 计算:

$$R = (x_R, y_R) = tP \quad (35)$$

$$r = x_R \bmod n \quad (36)$$

$$s = t(h(m) + dr)^{-1} \bmod n \quad (37)$$

式中: $h(\cdot)$ 是 hash 函数; $r, s \neq 0$ 。

b. $\{A_1, A_2, \dots, A_r\}$ 送 m 的签署 (r, s) 给 $\{B_1, B_2, \dots, B_t\}$ 。

4.2 $\{B_1, B_2, \dots, B_t\}$ 接收签署 (r, s) , 对 (r, s) 给予认证

a. $\{B_1, B_2, \dots, B_t\}$ 给出计算:

$$u_1 = h(m)s \bmod n \quad (38)$$

$$u_2 = sr \bmod n \quad (39)$$

$$R' = (x_{R'}, y_{R'}) = u_1P + u_2Q \quad (40)$$

$$r' = x_{R'} \bmod n$$

b. $\{B_1, B_2, \dots, B_t\}$ 对于 (r, s) 的认证, 若

$$r = x_R \bmod n = x_{R'} \bmod n = r' \quad (41)$$

则 (r, s) 是 $\{A_1, A_2, \dots, A_r\}$ 给出的签署, 是合法签署, $\{B_1, B_2, \dots, B_t\}$ 予以确认; 否则, $\{B_1, B_2, \dots, B_t\}$ 给予拒绝。

由式(35)、式(41)的讨论, 我们给出:

定理(集团通信签署-认证定理) 设 R 是 E

(k) 上的任意一点, $\alpha, \beta \in \mathbb{N}^+, n$ 是一个质数, 则惟一存在一点 $R' = \alpha P + \beta Q, R' \in E(k)$ 满足:

$$x_R \bmod n = x_{R'} \bmod n \quad (42)$$

证明: 由式(37), 得

$$s = t(h(m) + dr)^{-1} \bmod n \quad (43)$$

则有:

$$s(h(m) + dr) \bmod n = t \quad (44)$$

将式(44)两边同乘点 P :

$$tP = Ps(h(m) + dr) \bmod n \quad (45)$$

由式(35)、式(45), 得:

$$R = (x_R, y_R) = tP = Ps(h(m) + dr) \bmod n = psh(m) \bmod n + Psdr \bmod n \quad (46)$$

因为: $u_1 = h(m)s \bmod n, u_2 = sr \bmod n$, 代入式(46), 则有:

$$R = (x_R, y_R) = tP = Pu_1 + Pdu_2 \quad (47)$$

因为 $Q = dP$, 所以式(47)成为:

$$R = (x_R, y_R) = u_1P + u_2Q \quad (48)$$

又因为 $R' = (x_{R'}, y_{R'}) = u_1P + u_2Q$, 代入式(48)中, 则式(48)成为:

$$R = (x_R, y_R) = (x_{R'}, y_{R'}) = R'$$

因此,

$$x_R = x_{R'} \quad (49)$$

$$r = x_R \bmod n = x_{R'} \bmod n = r' \quad (50)$$

这里指出: 本文给出的对称集团签署-认证同样适用于非对称集团签署-认证。非对称集团是对称集团的特例。非对称集团是指: $|A| < |B|$ 或 $|B| < |A|$ 。

5 电力系统集团加密通信与集团签署-认证的应用

这里只给出对称集团加密通信系统与集团秘密钥匙-公开钥匙多项式生成的应用示例。而对称集团加密通信系统与集团秘密钥匙-公开钥匙乘积生成的应用示例、非对称集团加密通信系统与集团秘密钥匙-公开钥匙生成的应用示例、集团签署-认证的应用示例从略, 事实上这些例子也很容易得到。

设集团 A 有 3 个成员, $A=\{A_1, A_2, A_3\}$, 集团 B 有 3 个成员, $B=\{B_1, B_2, B_3\}$; A 是明文 P_m (P_m 是核电设计与运行参数报告) 的加密者、密文 C_m 的发送者; B 是密文 C_m 的接收者、密文 C_m 的解密者; $n^{A_1}=2, n^{A_2}=3, n^{A_3}=5$ 分别是 A_1, A_2, A_3 的秘密钥匙; $n^{B_1}=11, n^{B_2}=13, n^{B_3}=17$ 分别是 B_1, B_2, B_3 的秘密钥匙; $n^A=P_A(0)$ 是集团 A 的秘密钥匙; $P^A=P_A(0)G$ 是集团 A 的公开钥匙; $n^B=P_B(0)$ 是集团 B 的秘密钥匙; $P^B=P_B(0)G$ 是集团 B 的公开钥匙。

$E_{23}(1,1)$: $y^2 = x^3 + x + 1 \pmod{23}$ 是集团 A 与集团 B 共同选择的椭圆曲线; $a=2, b=7$ 是 A, B 分别选择的原根^[9], $p=11$ 是 A, B 选择的模。对 $E_{23}(1,1)$ 求模并得到 $E_{23}(1,1)$ 上的点, 则有:

$$y^2 = x^3 + x + 1 \pmod{23}$$

令 $x=0$, 得到:

$$y^2 = 1 \pmod{23}$$

$$y = \begin{cases} 1 \pmod{23} = 1 \pmod{23} \\ -1 \pmod{23} = 22 \pmod{23} \end{cases}$$

因此有点: $(0,1), (0,22)$ 。以此类推, 满足 $E_{23}(1,1)$ 的点是: $(0,1), (0,22), (1,7), (1,16), (3,10), (3,13), (4,0), (5,4), (5,19), (6,4), (6,19), (7,11), (7,12), (9,7), (9,16), (11,3), (11,20), (12,4), (12,19), (13,7), (13,16), (17,3), (17,20), (18,3), (18,20), (19,5), (19,18)$; $E_{23}(1,1)$ 的点的序 $n=27$; $(n+1)=(27+1)=28G=O$, O 是椭圆曲线 $E_{23}(1,1)$ 的无穷远点。

A, B 在 $E_{23}(1,1)$ 选择基点 $G=(5,4)$, 明文 $P_m=(9,7) \in E_{23}(1,1)$ 。这里: 真实的 P_m 明文已经利用数据压缩技术把 P_m 压缩到 $E_m(a,b)$ 中的一个点。

由式(23)~式(27), 集团 A 的秘密钥匙 n^A , 公开钥匙 P^A 分别是(计算过程从略): $n^A=9, P^A(0)=n^A G=72G=56G \oplus 16G=16G=(11,3)$ 。

由式(23)~式(27), 集团 B 的秘密钥匙 n^B , 公开钥匙 P^B 分别是 $n^B=10, P^B(0)=n^B G=24G=(18,3)$ 。

a. $\{A_1, A_2, A_3\}$ 把 P_m 加密成 C_m, C_m 送 B, 即 $\{A_1, A_2, A_3\}$ 取正整数 $k=3$, 基点 $G=(5,4)$, 明文 $P_m=(9,7)$, $\{B_1, B_2, B_3\}$ 的公开钥匙 $P^B(0)=24G=(18,3)$, $\{A_1, A_2, A_3\}$ 给出:

$$\begin{aligned} C_m &= \{kG, P_m + kP^B\} = \{3G, 14G + 3 \times 24G\} = \\ &\quad \{3 \times 8G, 14G + 72G\} = \{24G, 86G\} = \\ &\quad \{24G, 2G\} = \{(18,3), (0,22)\} \end{aligned}$$

然后, $\{A_1, A_2, A_3\}$ 送 $C_m=\{(18,3), (0,22)\}$ 给 $\{B_1, B_2, B_3\}$ 。

b. $\{B_1, B_2, B_3\}$ 接收 C_m , $\{B_1, B_2, B_3\}$ 把 C_m 解密成 P_m , 即 $\{B_1, B_2, B_3\}$ 取 C_m 中的第 2 项 $C_{m,2}=P_m+kP^B$, $\{B_1, B_2, B_3\}$ 取 C_m 中第 1 项 $C_{m,1}=kG$ 与集团 $\{B_1, B_2, B_3\}$ 的秘密钥匙 n^B 之积, $\{B_1, B_2, B_3\}$ 给出:

$$\begin{aligned} C_{m,2} - C_{m,1} &= P_m + kP^B - n^B(kG) = \\ &2G - 10(24G) = 2G - (240G) = \\ &2G - (16G) = 2G + (-16G) = \\ &2G + 12G = 14G = (9,7) = P_m \end{aligned}$$

6 结语

本文给出的研究是把椭圆曲线加密理论、加密技术与电力系统通信相互嫁接而得到的。椭圆曲线的加密技术比其他加密技术具有更多的优点。例如, 在相同的安全性的条件下, 椭圆曲线 160 位元的密钥长度相当于 RSA^[5] 1 024 位元的密钥长度, 因此椭圆曲线具有更快的加密-解密过程。椭圆曲线的安全性、可靠性已经得到确认^[10]。

本文给出的电力系统集团加密通信, 集团签署-认证, 具有工程应用的一般性, 所给出的研究扩展到电力系统其他应用领域的研究具有可行性。电力系统加密通信与通信认证将成为电力系统研究热点之一。

参 考 文 献

- Koblitz N. Elliptic Curve Cryptosystems. Mathematics of Computation, 1987, 48(17): 203~209
- Menezes A J, Vanstone S A. Elliptic Curve Cryptosystem and Their Implementation. Journal of Cryptology, 1993, 6(4): 209~224
- Jurisic A, Menzes A J. Elliptic Curve and Cryptography. Dr-Dobb's Journal, 1997, (22): 26~35
- Caelli W, Dawson E, Rea S. PKI, Elliptic Curve Cryptography and Digital Signatures. Elsevier Computer and Security, 1999, 18(1): 47~66
- Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. Communications of the Association for Computing Machinery, 1978, 21(2): 120~126
- Elgamal T. A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans on Information Theory, 1985, 31(4): 469~472
- Harn L. Group-oriented (t, n) Threshold Digital Signature Scheme and Digital Multisignature. IEE Proceedings—Computer and Digital Techniques, 1994, 141(5): 307~313
- Harn L, Lin H Y, Yang S. Threshold Cryptosystem with Multiple Secret Sharing Policies. IEE Proceedings—Computer and Digital Techniques, 1994, 141(2): 142~144
- 闵嗣鹤, 严士健(Min Sihe, Yan shijian). 初等数论(Primary Number Theory). 北京: 北京人民教育出版社(Beijing: People Education Press), 1983. 106~114
- Horton M. Cryptography and Network Security Principles and Practice. New Jersey. 1999. 193~206

史开泉(1945—), 男, 教授, 博士生导师, 主要研究方向为电力系统信息识别、电力系统加密通信理论与技术。
E-mail: fsxmar@sdu.edu.cn

陈泽雄(1963—), 男, 教授, 博士, 主要研究方向为系统加密理论与技术及系统分析。

(下转第 61 页 continued on page 61)

(上接第 57 页 continued from page 57)

GROUP ENCRYPTION COMMUNICATION AND GROUP SIGNATURE-AUTHENTICATION OF POWER SYSTEM

Shi Kaiquan¹, T. S. Chen²

(1. Shandong University, Jinan 250100, China)

(2. Da-Yeh University, Taiwan, China)

Abstract: We assume two groups in power systems and that members of each group all have common economic-technology interest and legal liability. The group encryption communication and group signature-authentication of power system with above characteristics are put forward. The mathematical structure of group encryption communication system, encrypt-decrypt algorithm and the generation methods of group secret key, group public key are given. The algorithm of group signature and group authentication is presented out. The proposed group encryption communication and group signature-authentication of power system has the universality of engineering application.

Key words: power systems; elliptic curve; group encryption-decryption; group secret key; group public key; group signature; authentication theorem