ECC 与 AES 混合加密算法在射频 CPU 卡安全机制中的应用①

潘峥嵘, 朱丽丽

(兰州理工大学 电气工程与信息工程学院, 兰州 730050)

摘 要: 针对无线射频 CPU 卡自身及其在射频识别(RFID)的过程中存在的安全隐患问题, 提出了一种将椭圆曲线加密算法(ECC)与高级加密标准(AES)相结合的混合加密算法. 该方法用高密钥效率的 ECC 算法加密射频 CPU 卡中的重要信息, 再用 AES 算法加密射频 CPU 卡与读写器之间的通讯信息, 在通讯的过程中重要的信息经过了 ECC 和 AES 双重加密, 攻击者即使得到射频卡或者截获信息, 也不能很快就得到有用的信息. 实验结果表明, 该方法有效地提高了射频 CPU 卡自身及其在通信过程中的安全性及抵御攻击的可能性, 充分发挥了混合加密算法的优势.

关键词: 射频 CPU 卡; ECC; AES; 混合加密算法

Application of ECC and AES Algorithm to Security of CPU Card

PAN Zheng-Rong, ZHU Li-Li

(College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China)

Abstract: In order to deal with the safety problem of privacy in CPU card and Radio Frequency Identification (RFID) process, this paper proposes an encryption algorithm that combines the Elliptic Curve Crypto-system (ECC) with the Advanced Encryption Standard (AES). This method firstly uses the high efficiency secret-key to encrypt important information, and then use the AES to encrypt the communication information between CPU card and the reader and writer. Thus the important information will be encrypted double in the process of communication, even though attackers get the Radio Frequency CPU card or intercept the communication information, they can't obtain useful information as quickly as they need. The experimental results show that the method improves the safety of the CPU card and against the attacks during the communication. The proposed mixed encryption algorithm plays an important role in the safety problem of privacy.

Key words: CPU card; ECC; AES; mixed encryption algorithm

无线射频识别(Radio Frequency Identification, 简称 RFID)技术是利用无线射频方式进行非接触双向通信并交换数据, 有效实现物品的无接触自动识别与动态管理, 具有提高社会管理、生产流通的效率和精准控制能力. 虽然射频 IC 卡的应用越来越广泛, 但应用过程中产生的用户隐私泄露等安全问题也日益凸显出来. 同时, 通过穷举攻击和中途拦截等攻击途径攫取卡中的信息、非法复制和篡改卡中内容等犯罪现象也随之出现. 尤其是 2009 年 M1 卡 "破解门"事件的爆发, 更是引起全球的恐慌. 因此, 对射频 IC 卡安全功能进行升级, 提高加密水平迫在眉睫.

近几年, 很多学者在 RFID 系统安全方面进行了大量的研究, 提出了一些不同的加密方法. 文献[1]运用的是对导出密钥运用 AES 加密的方法, 该方法体现了分级密钥优越性, 安全性有了一定的提高, 但是, 安全性要提高就要不断增加密钥的长度, 这在实现上

① 基金项目:甘肃省科技支撑计划(1011NKCA071)
收稿时间:2011-12-14;收到修改稿时间:2012-01-16

有一定的困难; 文献[2]把 DES 算法运用到 RFID 射频识别中, DES 和 3DES 算法已有破解的方法安全性不高; 文献[3]运用动态改写用户密钥的方法提高射频通信中的信息的安全性, 但是, 和文献[1]存在同样的问题, 要以增加密钥的长度来提高安全性.

通过对文献的分析发现, 影响安全级别的因素一是算法破解难易程度, 二是密钥的长短问题. 针对这一情况, 本文提出了一种将椭圆曲线密码体制(ECC)与已经取代 DES 标准的高级数据加密标准(AES)相结合的加密算法, 该算法结合了 AES 算法运算速度快、对内存要求低、算法可靠、能够有效抵抗查分分析和现行分析攻击的优点, 和 ECC 算法能够提供最高比特强的公钥密码, 用较短的密钥加密, 得到较高的安全级别密文的优势.

1 ECC算法原理

ECC(Elliptic Curve Crypto-system, 椭圆曲线密码体制)是一种能够提供最高比特强的公钥密码体制, 其安全性是建立在椭圆曲线离散对数的难解性的基础上的, 目前已正式列入了 IEEE Pl363 标准[4].

椭圆曲线是指威尔斯特拉(Weierstrass)方程:

$$E: y^2 + axy + by = x^2 + cx^2 + dx + e \tag{1}$$

密码学中的椭圆曲线的系数都在有限域中, 常用表达式为:

$$E_p(a,b): y^2 \equiv x^2 + ax + b(\mathrm{mod}\ p) \tag{2}$$

P 为一个大素数, a 、 b 、 x 和 y 均在有限域 $GF(P)$ 中, 即从 $\{0,1,L,P-1\}$ 上取值, 且满足:

$$4a^2 + 27b^2(\mathrm{mod}\ P) \neq 0 \tag{3}$$

椭圆曲线 E 上点集 $E_p(a,b)$ 关于“+”法构成 Abel 群. “+”法定义为任意取椭圆曲线上两点 P 、 Q 作直线(若 P 、 Q 两点重合, 则作过 P 点的切线)交于椭圆曲线的另一点 P', 过 P' 作 y 轴的平行线交于 R [5].

规定: $P+Q=R$, 定义:

$$kP = P + L + P \tag{5}$$

对于椭圆曲线上的一个基点 $P(x_{P,}y_P)$, 给定一个整数 d, 计算 $dP=Q$ 是容易的. 但是, 要是从 Q 点及 P 点推导出整数 d, 则是非常困难的[6]. 在 $E_p(a,b)$ 中挑选生成元点 $G=(x_{G,}y_G)$, G 应使得满足 $nG=0$ 的最小的 n 是一个非常大的素数(N 表示椭圆群 $E_p(a,b)$ 的元素个数, n 是 N 的素因子). 选择一个小于 n 的整数 n_S 作为其私钥, 然后生成公钥 $P_B=n_BG$, 则 B 的公钥为 (E,n,G,P), 私钥为 n_S.

加密过程:

1)A 将明文信息编码成一个数 $m<P$, 并在椭圆群 $E_p(a,b)$ 中选择一点 $P_t=(x_t,y_t)$;

2)在区间 $[1,n-1]$ 内, A 选取一个随机数 k, 计算点 $P_1: P_1=(x_1,y_1)=kG$;

3) 依据接收方 B 的公钥 P_B, A 计算点 $P_2=(x_2,y_2)=kP_B$;

4)A 计算密文 $C=mx_t+y_t$;

5)A 传送加密数据 $C_m=\{kG, P_t+kP_B, C\}$ 给接收方 B.

解密过程:

1)接收方 B 收到加密数据 $C_m=\{kG, P_t+kP_B, C\}$

2)接收方 B 使用自己的私钥 n_S 作如下计算:

$P_t+kP_S-n_s(kG)=P_t+k(n,G)-n_s(kG)=P_t$;

3)B 计算 $m=(C-y_t)/x_t$, 得明文 m.

2 AES算法原理

AES(Advanced Encryption Standard 高级数据加密标准)又称 Rijndael 加密法, 是一种对称密钥的分组迭代加密算法, 分组长度固定为 128 bits, 使用的密钥可以分为 128 bits, 192 bits 或 256 bits 三种不同的长度[7]. AES 算法将明文数据块看成是字节的二维矩阵(称为状态矩阵), 它有 4 行, N_b 列(N_b 等于数据块长除以 32), 在标准 AES 里 $N_b=4$. 密钥也同样表示为二维字节数组, 4 行, N_k 列(N_k 等于密钥块长除以 32). 算法转换的轮数 N_r 由 N_r 决定, 对应于 128 位, 192 位和 256 位不同的密钥长度, 运算的轮数分别为 10 轮, 12 轮和 14 轮. AES 对数据的加密是通过把输入的明文和密钥由轮函数经 N_r+1 轮迭代来实现的, 初始轮和结尾轮与中间的 N_r-1 轮不同[8]. 整个加密算法机制如图 1 所示.

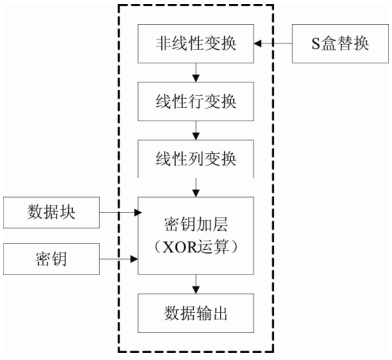
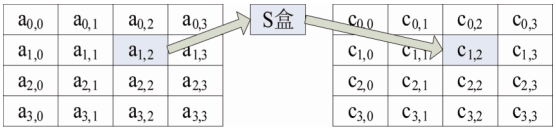


图 1 AES 算法加密机制结构框图

初始轮只对明文和密钥进行异或操作：中间 N_r-1轮依次对状态矩阵进行 SubbBytes、ShiftRows、MixColumns 和 AddRoundKey 变换；结尾轮不进行 Mix Columns 变换.

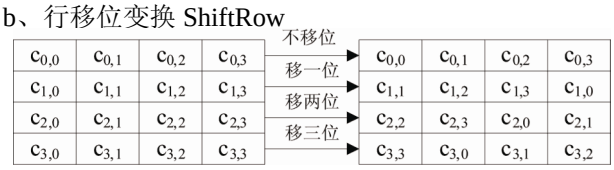
加密过程为:

a、S-盒变换 SubbByte



(其中, s 盒内的元素用 a_{ij} 来表示)

b、行移位变换 ShiftRow



c、列混淆变换 MixColumn

把经过行移位后的状态矩阵C与固定的矩阵E相乘，得到混合后的状态矩阵C'．其中固定矩阵E为

$$E=\begin{pmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{pmatrix}$$

d、圈密钥加变换 AddRoundKey

经过列混淆变换得到的状态矩阵C'经过与下面的矩阵进行异或变换，得到新的变换矩阵C.

w[4i]	w[4i+1]	w[4i+2]	w[4i+3]

依次循环进行变换，直到最后一轮不做列混淆变换 MixColumn，即可得到密文，存入共享扇区.

解密密文:

首先，对接收到的密文进行分组(128 位)，得 4∗4矩阵，然后对此矩阵进行 9 轮的圈密钥加变换、反列变换、反行变换和反 S 盒变换；接着进行 1 轮的圈密钥加变换、反行变换、反 S 盒变换，输出明文数据.

3　加密结构及实验验证

实验选用 Microchip 公司的一款通用小型 PIC 单片机-PIC16F883，内有 128 字节的数据 EEPROM，可用于存储可变数据，频率选择范围从 1KHZ 到 8MHZ，支持在线调试.

目前市场上现有的 CPU 卡内部携带的大多是 DES 或 3DES 协处理器，极少数的如龙杰 ACOS5 密钥智能卡内部采用 AES-128bits 或 RSA-2048bits 的加密，而采用 ECC 加密协处理器的 CPU 卡则还没有见到过. 因此实验采用虚拟 CPU 卡实现对 ECC 加密算法的模拟. 设计混合加密结构如下图 2 所示.

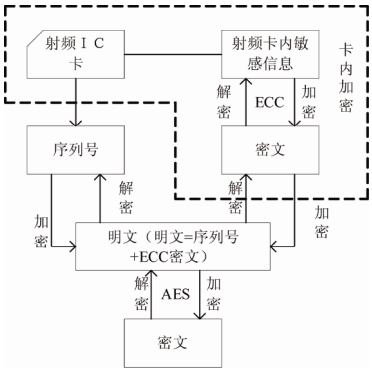


图 2　混合加密结构框图

由于 CPU 卡内部自带有微处理器，可以在卡内部实现对信息的加密，因此，我们在 CPU 内部设计 ECC 加密协处理器对内部信息进行加密. 从混合加密结构图可以很清楚地看出在 CPU 卡的内部我们进行 ECC 加密处理，对卡内的不需要经常被读取或进行通讯的重要信息进行加密；对于外部通讯信息和 ECC 加密密钥进行 AES 加密，这样相当于对内部重要信息进行了两次加密，从而提高了卡内存储信息的安全性.

实验以 ECC 加密卡内明文信息, AES 加密 128 位通信随机数据信息为例给出相应的实验结果:

椭圆曲线的参数如下(以十六进制显示):

有限域 P 是:f2a391

曲线参数 a 是:9db27

曲线参数 b 是:b5f8f

曲线 G 点坐标是:(a9cd7, 2cc80)

私钥 K 是:77364b4ec144c

公钥坐标是:(2c77e53, 2c77e53)

取随机数$k=c, P_t=(b,1)$

明文信息为:112244779955886600

加密数据结果为:1122825c00c99e59

AES 加密:161122825c00c99e59

AES 密钥:000102030405060708090A0B0C0D0E

0F

加 密 密 文 :BE1180C587FC0BE4A4379224F995DA92

解密:161122825C00C99E5900000000000000(位数不够用 0 补足)

ECC 解密得明文:112244779955886600

本实验的测试结果与其他实验相关结果对比如下表 1.

表 1 实验加解密速度对比表

算法	加密时间	解密时间
动态密钥TEA[3]	加解密速度21.3kb/s	
AES[9]	64.69kb/s	52.11kb/s
优化AES[10]	64Mb/s	43Mb/s
ECC和AES混合	65.2Mbits/s	42.8Mbits/s

从实验结果对比表格中我们可以看出, 混合加密算法的加解密速度相对还是比较快的, 能够满足射频 CPU 卡对加密的要求, 另外, 双重的加密效果增加了存储信息的安全级别, 使这种混合加密算法具有更广泛的应用性.

4 结论

在实际应用中, 公钥密码算法通常被用来加密关键性的、核心的机密数据(如本论文中的 CPU 卡内的重要敏感信息), 而对称密码算法通常被用来加密大量的数据(如明文数据). 将 AES 算法和 ECC 算法相结合, 充分体现了两种算法存储空间小、带宽需求低、用更短密钥加密信息等优点, 同时又具有很强的抗攻击性, 大大提高了 RFID 系统信息的安全性, 发挥了混合加密的整体优势, 也将会在保密数据的传输领域得到广泛应用.

参考文献

1 Feldhofer M, Dominikuc S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. Cryptographic Hardware and Embedded Systems. Cambridge, MA. Springer, 2004. 357–370.

2 徐志.基于 DES 加密算法的射频识别系统的设计.电工电气, 2009(4):6–9.

3 谢高生,易灵芝,王根平.动态密钥在 Mifare 射频 IC 卡识别系统中的应用.计算机测量与控制,2009,17(4):725–726,737.

4 Miller V. Uses of Elliptic Curves in Cryptography. Advances in Cryptology-CRYPTO, 85, LNCS21. Santa Barbara, Calif: Springer-Verlag,1986. 417–426.

5 俞经善,王晶,杨川龙.基于 ECC 和 AES 相结合的加密系统的实现.信息技术,2006,2:44–46.

6 Koblitz N. Elliptic Curve Cryptosystems. Mathematics of Computation,1987,48(177):203–209.

7 Lucc T. Integrated design of AES(Advanced En- cryption Standard) encrypter and decrypter. IEEE Transactions on Information Theory, 1991,37(5):1241–1260.

8 Sucp L, Huang CT, et al. A high through put low-cost AES Processor. Communications Magazine, IEEE, 2003,41(12): 86–91.

9 曾少林,易灵芝,王根平,赵吉清.高级加密标准算法在 RFID 数据安全中的应用.计算机测量与控制,2007,1(6):792–793, 797.

10 张红南,刘晓巍,邓蓉,张卫青,胡锦,赵欢.IC 卡的优化设计及 FPGA 仿真.湖南大学学报(自然科学版),2006,33(2): 66–69.

(上接第 174 页)

9 陈勇,马纯永,陈戈.基于 VC/OpenGL 的虚拟海大校园导航系统.计算机辅助设计与图形学学报,2007,19:263–266.

10 唐琏,谷士文,费耀平,等.全方位全景图像的一种映射方式.计算机工程,2000,26(8):95–97.

11 王娟,师军.一种柱面全景图像自动拼接算法.计算机仿真, 2008,25(7):213–215.

12 Lowe, DG. Distinctive image features from scale-invariant keypoints. International Journal of Computer Vision, 2004, 60 (2):91–110.