第44卷 第12期 西 安 交 通 大 学 学 报 Vol.44 №12
2010年12月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Dec. 2010

采用异或算子和椭圆曲线的混合加密机制

甘新标，沈立，王志英
（国防科学技术大学计算机学院，410073，长沙）

摘要：针对椭圆曲线加密系统处理由多个零碎文件组成的较大量数据信息时，其安全强度高而实时性较差的问题，提出了一种基于异或算子和椭圆曲线加密的多组混合加密方法(XORECC).该方法利用不同的密钥矢量与明文中零碎的文件异或得到密文，然后将其与零碎文件异或的密角矢量集合存放于锁盒子里，利用椭圆曲线加密机制对锁盒子进行加密以保证XORECC机制的安全性.通过引入异或(XOR)操作，使XORECC机制有效避免了椭圆曲线系统直接对大量数据进行加密，在保证密文高安全性的同时提高了系统的整体性能.

关键词：椭圆曲线加密；密钥矢量；异或算子；锁盒
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2010)12-0028-04

A Method for Encryption Based on Elliptic Curve Cryptography with Exclusive OR Operation

GAN Xinbiao, SHEN Li, WANG Zhiying
(School of Computer, National University of Defense, Changsha 410073, China)

Abstract: Elliptic curve cryptography(ECC) has high security, but is weak in real-time for large volume of data composed of fragmentary files to be encoded. One hierarchical encryption method termed XORECC is proposed, in which XOR operation is applied to each of fragmentary files with different secret vectors (SVs) for generating ciphertext, and then the different SVs are placed into a lock-box. Finally, the lock-box is encrypted using ECC to ensure high security of entire systems. Accordingly, XORECC avoids the direct encryption of ECC to large volume of data and improves encrypting speed. Hence, XORECC would enhance the performance of encryption systems.

Keywords: elliptic curve crylography; secret vector; exclusive or operation; lock-box

随着IT基础架构由计算中心到数据中心的转变，数据安全也变得越来越重要，而数据加密技术正是保证信息安全的最重要的手段，因而成为学术界和工业界研究的热点.

基于椭圆曲线离散对数难题的椭圆曲线加密系统被公认为是安全强度高、执行速度快的加密方法[1-2].但是，软件方法实现的椭圆曲线加密系统的速度还是不能满足用户需求，从而出现了许多基于硬件平台(如VLSI、FPGA)定制的椭圆曲线加密芯片和协处理器[3-4].然而，基于硬件的椭圆曲线加密系统实现成本较高，并且灵活性差[5]，不利于软硬件升级.因此，本文基于纯软件的思想，提出了基于异或算子和椭圆曲线加密(XORECC)的两级加密机制.XORECC利用密钥矢量与明文异或得到密文，然后利用椭圆曲线加密系统对密钥矩阵加密.通过引入XOR操作，XORECC机制有效避免了椭圆曲线系统直接对大量数据进行加密，提高了系统的整体性能.

1 XOR编码

将待加密文件F看成一系列字节的集合，如下

收稿日期：2010-03-05. 作者简介：甘新标(1982—)，男，博士生；王志英(联系人)，男，教授，博士生导师. 基金项目：国家重点基础研究发展规划资助项目(2007CB310901)；国家自然科学基金资助项目(60803041)；国防科技大学优秀研究生创新资助项目(B0906603).

$$F = B_1 B_2 \cdots B_i \cdots B_{n-1} B_n \tag{1}$$

式中:n 为文件的总字节数.

将 F 划分为长度为 m 个字节的一系列分块,不足的可以在末尾补 0,则式(1)可记为

$$F = S_1 S_2 \cdots S_k \cdots S_{\lceil \frac{n}{m} \rceil} \tag{2}$$

式中:

$$S_k = B_{(k-1)*m+1} B_{(k-1)*m+2} \cdots B_{(k-1)*m+m}.$$

定义 1(矩阵异或)　设 $\boldsymbol{A}$ 为 $m \times n$ 的矩阵,$\boldsymbol{B}$ 为 $\boldsymbol{A}$ 的同型矩阵,则 $\boldsymbol{A}$ 异或 $\boldsymbol{B}$ 定义为

$$\boldsymbol{C} = \boldsymbol{A} \oplus \boldsymbol{B} \tag{3}$$

其中

$$c_{ij} = a_{ij} \oplus b_{ij}$$
$$(i = 1,2,\cdots,m; j = 1,2,\cdots,m)$$

任意选择 m 个 m 维向量组成密钥矩阵,记为

$$\boldsymbol{A} = (\boldsymbol{a}_1 \boldsymbol{a}_2 \cdots \boldsymbol{a}_i \cdots \boldsymbol{a}_m)^{\mathrm{T}} \tag{4}$$

式中:$\boldsymbol{a}_i = (a_{i1} a_{i2} \cdots a_{in})$称为密钥矢量.

XOR 编码的过程为,任意选择密钥矢量 $\boldsymbol{a}_i$ 与 F 的每一个分块 S_k 异或. 设文件 F 加密后对应的密文为 F_{mi},则整个文件的 XOR 编码如下

$$F_{mi} = \boldsymbol{a}_i \oplus F \tag{5}$$

则解码对应为

$$\boldsymbol{a}_i \oplus F_{mi} = \boldsymbol{a}_i \oplus \boldsymbol{a}_i \oplus F = F \tag{6}$$

下面证明 XOR 编解码过程的正确性.

由定义 1 可知

$$\boldsymbol{a}_i \oplus \boldsymbol{a}_i \oplus F = \begin{pmatrix} \boldsymbol{a}_i \oplus \boldsymbol{a}_i \oplus S_1 \\ \boldsymbol{a}_i \oplus \boldsymbol{a}_i \oplus S_2 \\ \vdots \\ \boldsymbol{a}_i \oplus \boldsymbol{a}_i \oplus S_{\lceil \frac{n}{m} \rceil} \end{pmatrix} \tag{7}$$

由于

$$\boldsymbol{a}_i \oplus \boldsymbol{a}_i = 0;\ 0 \oplus S_k = S_k$$

所以

$$\boldsymbol{a}_i \oplus \boldsymbol{a}_i \oplus F = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_{\lceil \frac{n}{m} \rceil} \end{bmatrix} = F \tag{8}$$

即明文经过异或算子编解码后可恢复原文件.

2　XORECC 机制

上面的过程证明了 XOR 编码加密的正确性. 为了保证加密系统的高安全性,只要保证密钥矩阵的安全性即可. 椭圆曲线加密(Elliptic Curve Cryptograph, ECC)被公认为安全强度高,因此,XORECC 机制中采用椭圆曲线加密算法对密钥矢量加密[1-2].

2.1　XORECC 基本结构

XORECC 机制是一个两级加密方案,待加密明文先与密钥矩阵异或得到密文,然后由椭圆曲线加密算法对密钥矩阵进行加密处理以保证整个机制的安全性,其基本结构如图 1 所示.

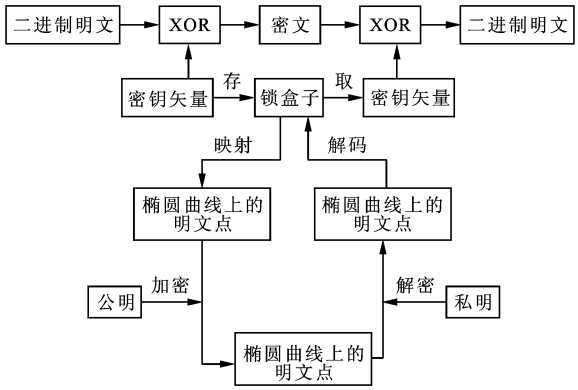

图 1　XORECC 结构

2.2　椭圆曲线相关定义与定理

定义 2　韦尔斯特拉斯(Weierstrass)方程

$$y^2 + axy + by = cx^3 + dx + e \tag{9}$$

所确定的平面曲线为椭圆曲线,记为 E,其中,$a,b,c,d,e \in F$,F 为有限域. 满足式(9)的(x,y)称为 F 域上的点. 此外,椭圆曲线还定义了一个特殊的无穷远点⊙. 在 ECC 系统中,定义在素数有限域上 $H(p)$的椭圆曲线方程如下

$$y^2 = x^3 + ax + b(a,b \in F) \tag{10}$$

式中:p 是大于 3 的素数;a 和 b 为两个小于 p 的非负整数,满足以下条件

$$\Delta(E) = 4a^3 + 27b^2 \bmod p \neq 0 \tag{11}$$

用 $E_p(a,b)$表示模 p 椭圆曲线,其上的点包括满足式(10)的小于 p 的非负整数对(x,y)以及无穷远点⊙.

定义 3　E 上定义"+"运算(点加运算),$P+Q=R$,R 是过 P、Q 点的直线与曲线的另一点关于 X 轴的对称点,如图 2 所示.

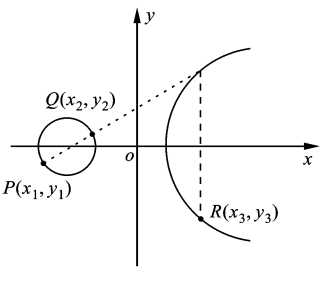

图 2　椭圆曲线上的点加

定理 1　设 P、Q 为 $E_p(a,b)$上的任意两点,L 为 P、Q

的连线，L 与 $E_p(a,b)$ 相交于另一点 R，则：

(1) $P+\odot=P$；

(2) $P+Q+R=\odot$；

(3) $P+Q=Q+P$；

(4) $(P+Q)+R=P+(Q+R)$；

(5) 若 $P+Q=\odot$，则 Q 称为 P 的负点，记为 $Q=-P$.

定义 4 k 个 P 点的点加称为 k 与 P 的点积，记为

$$kP=\underbrace{P+P+\cdots+P}_{k\text{个}P} \tag{12}$$

定义 5 给定素数 p 和椭圆曲线 E 及其上的两点 P、Q，求整数 m，使其满足 $Q=mP$，如果这样的整数 m 存在，它就是椭圆曲线的离散对数.

可以证明，求解椭圆曲线的离散对数在计算上是不可行的[6]，这也是构造 ECC 加密系统的数学基础.

2.3 ECC 加密通讯协议

椭圆曲线加解密通讯协议如图 3 所示，其过程如下.

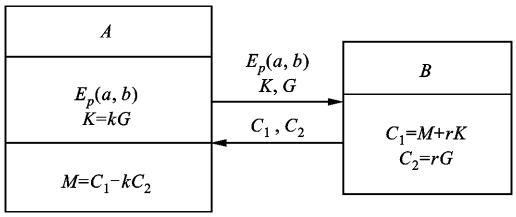

图 3 ECC 通讯协议

步骤 1 用户 A 选定一条椭圆曲线 $E_p(a,b)$，并取椭圆曲线上一点作为基点 G.

步骤 2 用户 A 选择一个私有密钥 k，并生成公开密钥 $K=kG$.

步骤 3 用户 A 将 $E_p(a,b)$ 和点 K、G 传给用户 B.

步骤 4 用户 B 接到信息后，将待传输的明文 F 编码到 $E_p(a,b)$ 上一点 M，并产生一个随机整数 $r(r<n)$.

步骤 5 用户 B 计算点 $C_1=M+rK$；$C_2=rG$.

步骤 6 用户 B 将 C_1、C_2 传给用户 A.

步骤 7 用户 A 接到信息后，计算 C_1-kC_2，结果得到点 M

$$C_1-kC_2=M+rK-k(rG)=$$
$$M+rK-r(kG)=M$$

如何将明文信息嵌入到椭圆曲线上也是椭圆曲线加密的关键. 椭圆曲线上的点由 x 坐标和 y 坐标组成，并且 x、y 都要在椭圆曲线的有限域上. 本文采用如下方法进行明文编码：取一段二进制形式的明文作为椭圆曲线上点的 x 坐标，然后将按照椭圆曲线方程计算得到的 y 值作为 y 坐标的值.

2.4 XORECC 的安全性

XORECC 的安全性由 XOR 编码和 ECC 加密两级加密机制来保证. ECC 的安全性由椭圆曲线离散对数求解难题来保证，同时，任意选择的密钥矢量 $\boldsymbol{a}_i$ 与明文 F 异或，密钥矢量 $\boldsymbol{a}_i$ 置于锁盒之中，攻击者通过对照明密文获取整个锁盒中的密钥矢量几乎不可能，因此，XORECC 机制是安全可靠的.

3 实验测试及性能分析

为了验证 XORECC 方法的有效性，实验环境配置如下.

(1) Intel Core2 Quad 2.33 GHz，4 GB 内存，Microsoft Visual Studio 2005 with SP1.

(2) 为了保证椭圆曲线加密的安全性，椭圆曲线参数的选择至关重要. 通常，有限域 $H(p)$ 上的素数 p 越大就越安全，但是计算速度也会越慢；p 为 200 b 时可以满足一般的安全要求. 本实验设置素数 p 为 200 b.

(3) LibTomMath 库是一个计算高精度整数的开源软件[7]，用标准 C 语言实现了几乎所有标准的密码算法模块.

为了说明椭圆曲线加密系统的局限性，本文对 .txt、.doc、.jpg 等格式的文件进行加解密测试，结果如表 1 所示.

表 1 ECC 性能测试

测试集	大小/B	运行时间/ms
test.txt	10	28 303.892 578
test.doc	20 992	77 663.046 875
test.jpg	1 268 333	4 081 300.250 000

从表 1 可以看出，针对少量的加密数据，ECC 的处理速度还是可以接受的，例如，加密 10 B 的文件，约 28.3 s 可以完成，但是，对于较大量的加密数据，其处理速度是不能接受的，如加密一个大小只有 1.2 MB(1 268 333 B)的文件，耗时高达4 081 300 ms(一个多小时)，这是用户所不能接受的. 因此，XORECC 机制通过引入 XOR 编码避免了 ECC 直接对大量数据信息的加密，其性能比较如表 2 所示，由于只是验

表 2 XORECC 与 ECC 的性能比较($m=30$)

测试集	大小/B	运行时间/ms		
		ECC	XORECC	
			XOR	ECC
test.jpg	12 683 33	4 081 300.25	3.496 922	23 620.265 625

证性实验,所以本实验中较大数据量的明文只包含了一个文件,故锁盒子里面只有一个密钥矢量.

XORECC 与 ECC 相比,性能加速比为

$$\frac{4\ 081\ 300.25}{3.496\ 922+23\ 620.265\ 625}=172.8 \quad (13)$$

由表 2 可知,如果取 $m=30$,即待加密文件 F 被分割为大小 30 个字符的一系列分块,则需要的额外存储空间为包含若干组 30 个字符的密钥矢量所占的空间大小即可,然而,获得的性能加速比却是显著的.因此,使用 XORECC 机制来加密由多个零碎文件构成的大文件或是含有较大量数据信息的文件是有效的.

4　结　语

数据加密技术研究极富挑战性.本文探索了多级混合加密的方法,提出了 XORECC 机制.该机制避免了 ECC 直接对大量数据信息的加密,同时保持了 ECC 高安全性的优点.在实际的应用场景下,较大量的明文极可能包含大量零碎的小文件,所以锁盒子中可能是许多密钥矢量的集合,如何管理和存储密钥矢量和锁盒子将会成为作者下一步的研究内容.

参考文献:

[1] 陈晓峰,王育民. 公钥密码体制研究与进展[J]. 通信学报,2004, 25(8):109-118.
CHEN Xiaofeng, WANG Yuming. A survey of public key cryptography [J]. Journal of Communications, 2004, 25(8): 109-118.

[2] 张险峰,秦志光,刘锦德. 椭圆曲线加密系统的性能分析[J]. 电子科技大学学报, 2001,30(2):144-146.
ZHANG Xianfeng, QIN Zhiguang, LIU Jinde. Analysis of security and efficiency on elliptic curves cryptosystems [J]. Journal of University of Electronic Science and Technology of China, 2001, 30(2):144-146.

[3] 陈超,曾晓洋,章倩苓. 一种新型硬件可配置公钥制密码协处理器的 VLSI 实现[J]. 通信学报,2005,26(1):6-11.
CHEN Chao, ZENG Xiaoyang, ZHANG Qianling. A new hardware-reconfigurable public-key cryptographic coprocessor [J]. Journal on Communications, 2005,26(1):6-11.

[4] 陈婧, 蒋俊洁, 王石, 等. 基于 FPGA 的高速椭圆曲线标量乘法结构[J]. 计算机研究与发展,2008,45(11):1947-1954.
CHEN Qian, JIANG Junjie, WANG Shi, et al. High performance architecture for elliptic curve scalar multiplication based on FPGA [J]. Journal of Computer Research and Development, 2008,45(11):1947-1954.

[5] 丁群, 彭喜元, 扬自恒. 基于神经网络算法的组合序列密码芯片[J]. 电子学报,2006, 34 (3):409-412.
DING Qun, PENG Xiyuan, YANG Ziheng. The cipher chip of combining stream based on the neural network algorithm [J]. Acta Electronica Sinica, 2006, 34 (3):409-412.

[6] 王思叶. 椭圆曲线密码算法的研究和设计[D]. 上海:上海交通大学信息安全学院,2006.

[7] DENIS T S, RASMUSSEN M, ROSE G, et al. Implementing multiple precision arithmetic [M]. Ontario, Canada: Open Communications Security, 2004:9-33.

(编辑　武红江)