椭圆曲线加密算法在身份认证及软件注册中的实现

李美满[1]，朱文球[1]，易德成[1]，彭喜艳[2]

（1.湖南工业大学 计算机与通信学院，湖南 株洲 412008；2.株洲市中等职业学校，湖南 株洲 412000）

摘 要：在简要介绍了椭圆曲线及椭圆曲线密码体制的基础上，重点讨论了通过椭圆曲线数字签名来实现身份认证，分析了身份认证的关键算法，实现了利用$E_p(a,b)$椭圆曲线进行软件注册，同时给出了FPGA硬件实现的方案，提出了椭圆曲线加密算法将逐步取代RSA算法并成为未来密码技术发展的方向。

关键词：椭圆曲线；加密；有限域；身份认证；软件注册

中图分类号：TP309.7 **文献标识码**：A **文章编号**：1673-9833(2009)01-0043-03

Implementation of Elliptic Curve Cryptography Algorithm in Identity Authentication and Software Register

Li Meiman[1]，Zhu Wenqiu[1]，Yi Decheng[1]，Peng Xiyan[2]

(1.School of computer and communication，Hunan University of Technology，Zhuzhou Hunan 412007，China；
2. Zhuzhou Secondary Vocational School，Zhuzhou Hunan 412000，China)

Abstract：Based on the simple introduction of elliptic curve encryption system, implementation of identity authentication by using elliptic curve digital signature is disscussed, and the key algorithms of identity authentication are analyzed. By making use of $E_p(a,b)$ elliptic curve, software register is realized, meanwhile the scheme of FPGA hardware implementation is given out, and elliptic curve encryption algorithm will replace RSA algorithm gradually and it will become direction of cipher technology development in the future.

Key words：elliptic curve; encryption; finite field; identity authentication; software register

身份认证机制是数据库加密系统安全性的第一道防线，一旦被攻破，系统的所有安全措施将形同虚设。在传统情况下，一般采用RSA算法解决数据的安全问题，但RSA存在密钥过长，运算速度慢等问题，与RSA密码体制相比，椭圆曲线密码体制具有安全性高、密钥量小和灵活性好等显著优点[1,2]。

1 椭圆曲线公钥密码体制

椭圆曲线加密法（ECC）是一种公钥加密技术，它以椭圆曲线理论为基础，利用椭圆曲线等式的性质来产生密钥。普通的椭圆曲线是连续的，并不适合用于加密；必须把椭圆曲线变成离散的点才能用于加密。把椭圆曲线拓展到任意域上，特别是特定的有限域上(有限个元素组成的域)，则椭圆曲线在有限域上变成离散的点。将椭圆曲线中的加法运算与离散对数中的模乘运算相对应，将椭圆曲线中的乘法运算与离散对数中的模幂运算相对应，就可以建立基于椭圆曲线的对应的密码体制。

1.1 有限域上F_q的椭圆曲线

F_q表示q个元素的有限域，令$q>3$是1个素数，$a,b \in F_q$，满足$4a^3+27b^2 \neq 0$，由参数a，b定义F_q上一个椭圆曲线方程$y^2=x^3+ax+b(\mathrm{mod}\ q)$，定义曲线参数

$T=(q,a,b,G,n,h)$，

收稿日期：2008-07-01

基金项目：湖南省教育厅青年骨干教师资助项目(湘教通[2007]256号)

作者简介：李美满(1971-)，男，湖南醴陵人，湖南工业大学讲师，硕士，主要研究方向为数据库技术，网络与信息安全，
E-mail：lmm567@163.com

其中：$qt \neq 1 (\mathrm{mod}\ n)$，$1 \leq t < 20$；

G 为基点；

n 为基点 G 的阶，n 为素数；

h 是椭圆曲线上所有点的个数 m 与 n 相除的整数部分，$h \leq 4$；

$q \neq n \times h$。

椭圆曲线方程的所有正整数解（x，y）连同1个称为无穷远的点（记为 O）所组成的集合记为 $E(F_q)$，设 $P \in E(F_q)$，若 P 周期很大，即 $P+P+\cdots+P=O$（共有 n 个 P 相加）成立的最小正整数 n，若 n 不存在，则 P 是无限阶的。事实上，在有限域上定义的椭圆曲线上所有点的阶 n 都是存在的，并且 $O \in E(F_q)$，一定有某个正整数 m，使得 $Q=mp=P+P+\cdots+P$（共有 m 个 P 相加），可以转换为 $m=\log_p Q$。

$E(F_q)$ 对点的“+”运算形成1个Abel群，相关它的离散对数问题是很难处理的，即 $Q=mp$（或 $m=\log_p Q$），其中 Q，p 为椭圆曲线在 $E(F_q)$ 上的点，m 小于点 P 的阶。不难发现，给定 m 和 P，根据加法法则计算 Q 很容易；但给定 Q 和 P，求 m 相对困难。这是椭圆曲线加密算法采用的难题，也即它的离散对数问题[3-5]。

1.2 椭圆曲线加密算法优点及加密流程

椭圆曲线加密算法的最大优点是不存在计算椭圆曲线有理点群的离散对数问题的指数算法，这就意味着在同等安全的前提下，椭圆曲线密码体制可以选择更小的参数。例如160位椭圆曲线密钥就相当于1 024位RSA密钥，而224位ECC则与2 048位RSA、DSA具有相同的安全强度，同时ECC把实数域上的乘法运算、指数运算等映射成椭圆曲线上的加法运算，无论是用硬件实现还是软件实现，椭圆曲线加密算法都比其它公钥密码体系计算量小、处理速度快、占用的存储空间小、加密后的数据包小、带宽要求低、实现成本更低。因而，ECC在身份认证及软件注册中将会有广泛的应用前景。椭圆曲线加密流程如图1所示。

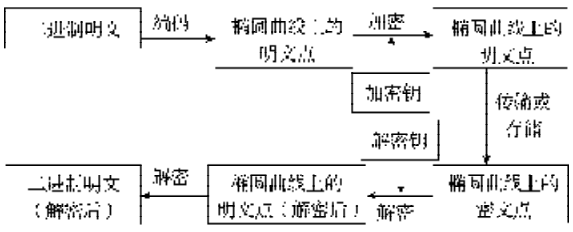

图1 椭圆曲线加密流程图

Fig. 1 Flow chart of elliptic curve encryption

2 基于椭圆曲线密码体制的系统身份认证技术

2.1 认证前期准备工作

1）用户 U 向认证机构CA申请1张数字证书，并根据椭圆曲线的参数 $T_u=(q,a,b,G,n,h)$ 建立1个密钥对（d_u，R_u），其中 $R_u=d_u \cdot G_u$，将 R_u 公开；

2）U 建立1个Hash函数 H_u，一般采用SHA（Secure Hash Algorithm，安全散列算法），函数值的长度为 $hashlen$ 个字节，通过CA的验证后将其公开；

3）U 建立1个 KDF_u（key derivation function）用于从共享秘密数据中提取出对称加密所需的密钥，一般利用第2）步的Hash函数，通过CA验证将其公开；

4）U 建立1个对称加密机制 ENC_u，密钥定义为 $enckey$，长度为 $enckeylen$ 个字节，一般采用3DES或DES，通过CA验证将其公开；

5）U 建立密钥协商机制（key agreement scheme，KAS），一般采用标准Diffie-Hellman机制或带因子的Diffie-Hellman机制，并将其公开；

6）按照上述步骤，用户 V 也建立属于自己的相关信息，除私有密钥 d_u 外，其余全部公开。

2.2 加密及签名过程

假设用户 U 需要将明文信息 M 加密并签名后传输到用户 V，则具体过程如下：

1）U 获取 V 所有公开的信息，并通过CA验证其合法性；

2）根据 V 的椭圆曲线参数 T_u，建立1个临时密钥对（k_1，R_1），其中 $R_1=k_1 \cdot G_v$，$k_1 \in F_q$；

3）根据KAS计算共享点 R。若KAS为SDHP，则 $R=k_1 \cdot R_v$；若KAS为CDHP则 $R=h_v \cdot k_1 \cdot R_v$，这是椭圆曲线上的点（$R_x$，$R_y$）。取 R_x 作为共享秘密数据 skd；

4）根据 V 的 KDF_v 和 $enckeylen$ 从 skd 中计算出对称密钥 $enckey$；

5）根据 V 的 ENC_v，用 $enckey$ 将欲发送的明文信息 M 加密成 EM；

6）根据 U 本身的椭圆曲线参数 T_u，建立另一个临时密钥对（k_2，R_2），其中 $R_2=K_2 \cdot G_u$，这是椭圆曲线上的点（R_{2x}，R_{2y}）；

7）计算 $r=R_{2x} (\mathrm{mod}\ n)$。注意：若 $r=0$，则返回步骤6）重新取1个（k_2，R_2）；

8）根据 U 本身建立的Hash函数 H_u，计算 $H=\mathrm{Hash}(R||EM)$，若 $[\log_2 n] \geq 8(hashlen)$，则令 $e=h$；否则取 H 的左边 $[\log_2 n]$ 位 H'，令 $e=H'$；

9）计算 $S=k_2^{-1}(e+r \cdot d_u) (\mathrm{mod}\ n)$，若 $S=0$，则返回步骤6）；

10）输出 $W=(r, s)\ ||R_1||EM$ 到 V。

2.3 解密及验证过程

V 收到 W 后先验证是否是由 U 发送，检查数据的完整性，再根据 U 的参数将 EM 还原成明文 M，具体过程如下：

1）V 获取 U 的所有公开信息，并通过CA验证其合法性；

2）按照2.2中步骤7）、8）的方法，计算出 e；

3）计算 $U_1=e\cdot s^{-1}(\mathrm{mod}\ n)$，$U_2=r\cdot s^{-1}(\mathrm{mod}\ n)$；

4）计算 $R_3=(R_{3x}, R_{3y})=U_1G_u+U_2R_u$。由 2.2 中步骤 9) $S=k_2^{-1}(e+r\cdot d_u)(\mathrm{mod}\ n)$可知: $S^{-1}=k_2(e+r\cdot d_u)^{-1}(\mathrm{mod}\ n)$。若 W 在传输过程中保持完整，则

$$R_3=U_1G_u+U_2R_u=e\cdot s^{-1}\cdot G_u+r\cdot s^{-1}\cdot d_u\cdot G_u=$$
$$s^{-1}(e+r\cdot d_u)G_u=K_2G_u=R_2;$$

5）计算 $r'=R_{3x}(\mathrm{mod}\ n)$。若有 $r'=r$，则说明 W 是由 U 发送的，且在传输过程中保持了数据的完整性；

6）V 根据自己建立的 KAS 和私有密钥 d_v 计算 $R'=d_v\cdot R_1$。若 KAS 为 SDHP，$R_1=k_1\cdot G_v$，故而 $R'=d_v\cdot k_1\cdot G_v=k_1\cdot R_v=R$；若 KAS 为 CDHP，$R_1=h_v\cdot k_1\cdot R_v$，故而 $R'=d_v\cdot h_v\cdot k_1\cdot G_v=h_v\cdot k_1\cdot R_v=R$；

7）以 R'_x 为共享秘密数据，根据 V 自己建立的 KDF 函数计算出对称加密的密钥 $enckey$；

8）根据 ENC 和对应的 $enckey$，将密文 EM 还原成明文 M。

3　椭圆曲线在软件注册中的实现

将公开密钥算法作为软件注册算法的好处是 Cracker 很难通过跟踪验证算法得到注册机。下面，将简介一种利用 $E_p(a,b)$ 椭圆曲线进行软件注册的方法。

3.1　制作注册机

1）选择 1 条椭圆曲线 $E_p(a,b)$ 和基点 G；

2）选择私有密钥 k（$k<n$，n 为 G 的阶），利用基点 G 计算公开密钥 $K=kG$；

3）产生 1 个随机整数 r（$r<n$），计算点 $R(x, y)=rG$；

4）将用户名和点 R 的坐标值 x,y 作为参数，计算 SHA 值，即 $Hash=\mathrm{SHA}(username, x, y)$；

5）计算 $sn\equiv r-Hash*k(\mathrm{mod}\ n)$；

6）将 sn 和 $Hash$ 作为用户名 $username$ 的序列号。

3.2　软件验证过程

1）从用户输入的序列号中提取 sn 以及 $Hash$；

2）计算点 $R\equiv sn*G+Hash*K(\mathrm{mod}\ p)$，如果 sn、$Hash$ 正确，其值等于软件作者签名过程中点 $R(x,y)$ 的坐标；

3）将用户名和点 R 的坐标值 x,y 作为参数，计算 $H=\mathrm{SHA}(username, x, y)$；

4）如果 $H=Hash$ 则注册成功，如果 $H\neq Hash$ 则注册失败。

4　FPGA 硬件实现

ECC 的实现有软件和硬件 2 种方式。软件化的实现方法开发时间短，但是其加密速度比较慢，妨碍了椭圆曲线加密的实用性。FPGA 硬件实现方法综合了软件的灵活性和硬件的安全性，提供了比软件化方法优越的速度，与传统的 ASIC 实现相比，可编程器件由于其高度的灵活性，更适合于密码学的应用。

FPGA 在软件模型的基础上针对 FPGA 硬件的特性对模型进行了优化。根据椭圆曲线加密算法的要求，对加密系统进行模块化设计，每个模块独立完成其各自功能，模块之间进行相互数据交换以及时序控制，达到加密功能。由于 168 位的椭圆曲线加密算法的计算量比较大，所以在 FPGA 实现的时候，布线是个值得考虑的因素。对于 FPGA 器件的选择应考虑到布线资源，Virtex 系列提供的布线资源比较丰富。

使用 Modelsim 6.0 进行仿真后得到性能指标为：在 40 MHz 时钟驱动下第一次加密或者解密时需要初始的建立时间，明文或者密文的输出需要 2 ms 左右，其后的明文或者密文的输出大约为 25 Mbps。可以看出，这是一个比较高的速率，可以应用于很多场合。

5　结语

椭圆曲线加密算法加密技术比起传统加密技术在解密时使用的公钥较小，因而能获得更高的资源利用率和更快的计算速度。ECC 算法将逐步取代 RSA 算法，成为公开钥密码系统加密算法的首选，随着 Internet、移动办公、移动商务应用的日益广泛，ECC 将具有更加广阔的市场前景和实用价值。

参考文献：

[1] David Salomon. Data Privacy and Security[M]. Beijing: Tsinghua University Press，2005：145-173.

[2] 王　刚，朱艳琴. 基于椭圆曲线的安全传输模型[J]. 计算机应用与软件，2005，22(9)：121-122.
Wang Gang，Zhu Yanqin. A Secure Transmission Model Based on ECC[J]. Computer Applications and Software，2005，22(9)：121-122.

[3] 周玉洁，冯登国. 公开密钥密码算法及其快速实现[M]. 北京：国防工业出版社，2002：9.
Zhou Yujie，Feng Dengguo. Public Key Cryptogaphic Algorithms and Its Fast Implementation[M]. Beijing: Defense Industry Press，2002：9.

[4] 华大芳，刘声雷. 椭圆曲线加密算法与FPGA硬件实现[J]. 合肥工业大学学报：自然科学版，2007，30(1)：39-40.
Hua Dafang，Liu Shenglei. Algorithm of Elliptic Curve Cryptography and Hardware Implementation with FPGA[J]. Journal of Hefei University of Technology: Natural Science Edition，2007，30(1)：39-40.

[5] Menezes A J，Vanstone S. The Elliptic Curve Digital Signature Algorithm(ECDSA)[J]. International Journal on Information Security，2001(1)：40-56.

（责任编辑：罗立宇）