

椭圆曲线加密算法及其在 PKI 中应用模型的研究

陈翔, 庄毅, 吴学成

(南京航空航天大学 信息科学与技术学院, 江苏 南京 210016)

摘 要:对公钥基础设施(PKI)的关键技术进行了研究与分析,提出了一个基于椭圆曲线密码体制(ECC)的 PKI 模型,讨论了椭圆曲线加密算法的核心算法,并对算法提出了改进。比较了新旧两种算法的效率,得出了新算法更有效的结论,从而验证了这个 PKI 模型的可行性。

关键词:椭圆曲线加密系统; 数据加密算法; 公钥基础设施

中图分类号: TP301.6

文献标识码: A

文章编号: 1005-3751(2006)03-0129-03

Research on ECC and Application Model of ECC to PKI

CHEN Xiang, ZHUANG Yi, WU Xue-cheng

(College of Computer Sci. and Techn., Nanjing Univ. of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: The key technique of public key infrastructure(PKI) is analyzed. A model of PKI based on elliptic curves cryptosystems(ECC) is proposed. The most important arithmetic of ECC is analyzed. And the amelioration is put on the arithmetic. Comparison is done on efficiency of the older and the newer, the newer arithmetic is more efficient, so, the feasibility of the model is validated.

Key words: elliptic curves cryptosystems; data cryptology arithmetic; public key infrastructure

1 PKI 的关键性问题

随着 Internet 技术的发展, Internet 服务、电子商务、网络银行等成为近年来的几大热点, 信息安全问题成为这些技术全面应用的关键问题之一。而公开密钥基础设施(PKI, Public Key Infrastructure)是主要的信息安全解决方案。PKI 的安全技术主要包括公钥加密技术、数字签名和验证技术。其中密钥交换和身份验证的安全性依赖于它所使用的公开密钥算法、对称加密算法和摘要算法, 而这些加密算法的载体是 PKI 的核心——CA (Certification Authority), 即认证机构, CA 就是通信双方相互依赖的第三方。CA 通过加密算法来保证信息安全, 加密算法包括对称加密算法和非对称加密算法。常用的对称加密算法有美国数据加密标准(DES); 而常用的非对称加密算法有: 基于大整数的分解问题困难性的 RSA, 基于离散对数问题困难性的 DSA, 以及基于椭圆曲线离散对数(ECDLP)问题困难性的 ECC。

在实际的 PKI 方案中, 所采用的加密算法是对称加密算法和非对称加密算法的混合, 例如用非对称密钥体制传递会话密钥, 用对称密码体制传输消息, 主要因为对称

密码体制加解密速度快, 但是密钥管理不方便, 而非对称密码体制加解密速度相对较慢, 但密钥管理方便。现今 RSA 加密算法已在 PKI 中得到广泛的应用, 而椭圆曲线加密算法相比于 RSA、DSA 等算法, 具有密钥短、加密强度大等特点, 现在正成为研究热点^[1]。文中提出一种基于 ECC 的 PKI 模型, 并对椭圆曲线的核心算法进行一些研究。

2 一个基于 ECC 的 PKI 模型

2.1 PKI 模型的通信过程

这个过程主要分为两大部分: 初始化过程; 用户之间进行通信的过程。下面以用户 A 向用户 B, 通过 ECC 加密发送明文 M 为例进行说明。

2.1.1 初始化过程

2.1.1.1 椭圆曲线的选取

椭圆曲线的选取过程^[2]由 CA 来完成。CA 选取有限域 $GF(p)$ 上的椭圆曲线 $E: y^2 = x^3 + ax + b$, 即给出一组椭圆曲线参数 (p, a, b, G) 。整数 p 表示有限域 $GF(p)$ 的特征; $a, b \in GF(p)$ 定义了一条椭圆曲线; G 表示一个基点。对各参数有如下要求:

要选择一条足够安全的椭圆曲线, 其 p 要大于 2^{160} , a, b 由 CA 随机选取, 但要保证 $a, b \in GF(p)$ 及 $4a^3 + 27b^2 \neq 0 \pmod{p}$; 基点 $G(G.x, G.y)$ 也是由 CA 选取的椭圆曲线 $E: y^2 = x^3 + ax + b$ 上的点。这些参数被写入椭圆曲线参数文件, 可以被任何用户所访问。

收稿日期: 2005-06-03

基金项目: 航空基金资助项目(04c52009); 国家“十五”预研项目(41801150201)

作者简介: 陈翔(1981—), 男, 江苏南通人, 硕士研究生, 研究方向为网络安全; 庄毅, 副教授, 主要从事网络安全和分布式计算的研究。

2.1.1.2 用户密钥的选取和证书生成

(1) 用户 A 随机选取一个整数 K_A , 作为自己的私钥, 保存在只有自己可以读取的参数文件中, 计算 $G_A = K_A \cdot G$ (点积运算), G_A 为自己的公钥。同理, 用户 B 随机选取一个整数 K_B , 作为自己的私钥, 计算 $G_B = K_B \cdot G$ (点积运算) 作为自己的公钥。

(2) 用户用自己的公开密钥 R (即 G_A 和 G_B) 向 CA 申请证书, CA 对 R 产生数字签名, 记为 $Dd(R)$, 再产生证书 $C = \{R, Dd(R)\}$ 返回给用户。持有证书的用户之间可以进行安全的数据通信。

2.1.2 用户之间进行通信的过程

(1) 编码。用户首先对信息 M 进行分组 (为方便, 以一个字符为一个分组), 使其成为有限域上的明文信息块 m 。然后将 m 经编码嵌入到椭圆曲线上的点 p_m 。这种“编码”不同于加密, 任何一个合法用户都可以解码恢复明文。记分组数为 num , 约定 $0 \leq num < [p/256] - 1$, 要找到这样的 x , 使之满足 $256m \leq x < 256(m+1)$, 且 $f(x) = x^3 + ax + b \pmod{p}$ 为 $GF(p)$ 上的平方剩余。若找到这样的 x , 就完成了明文信息的编码阶段。

(2) 发送密文。用户 A 对经过分组与编码的信息进行加密计算, 并发送如下点对给用户 B。

$$\{G_A, p_m \cdot x + (K_A \cdot G_B) \cdot x\} \\ = \{K_A \cdot G, p_m \cdot x + (K_A \cdot (K_B \cdot G)) \cdot x\}$$

(3) 接受密文并解密。用户 B 接受到密文, 可使用 K_B 作如下解密运算, 恢复出 $p_m \cdot x$ 。由点积运算的性质, 可得

$$K_A \cdot (K_B \cdot G) = K_B \cdot (K_A \cdot G)$$

$$p_m \cdot x + (K_A \cdot (K_B \cdot G)) \cdot x = (K_B \cdot (K_A \cdot G)) \cdot x \\ = p_m \cdot x$$

(4) 解码。得到 p_m 后, 去掉点 p_m 的 x 坐标的最低一个字节, 即将 $p_m \cdot x$ 除以 256 后取整, 即可得到明文分组 m 。也即: $m = [P_m \cdot x / 256]$ 。

2.2 PKI 模型的设计

文献[3]中提出的模型, 只用了一重 ECC, 即只是完成了用对方公钥进行加密的工作, 并没有进行签名的设计, 这不能满足信息的不可否认性等要求。在此提出一些改进。在系统设计过程中, 通常是非对称加密算法加密会话密钥, 而用对称加密算法加密所需传送的明文, 这里所采用的非对称加密算法是 ECC, 对称加密算法是 3DES, 哈希函数是 MD5。

模型先进行上述的初始化工作。在数据传送之前, CA 对用户进行身份认证。只有合法的用户之间才能进行安全的数据通信, 用户 A 向用户 B 发送数据流程模型, 如图 1 和图 2 所示。

(1) A 随机产生会话密钥 (简称密钥, 模型中是 3DES 密钥), 用它对数据明文加密得到数据密文, 同时用 ECC 加密这个密钥 (用 B 的公钥), 得到密钥密文。

(2) A 对数据明文用哈希函数进行运算, 得到该明文的数据摘要, 接着也用 ECC 加密这个数据摘要, 记为 x

(用 B 的公钥), 得到加密摘要; 并再对密钥密文和加密摘要进行数字签名 (用 A 的私钥)。

(3) B 接收到经 A 签名后的密钥密文和加密摘要以及数据密文。

(4) B 对密钥密文和加密摘要验证签名 (用 A 的公钥); 并还原出密钥和数据摘要 x (用 B 的私钥); 用密钥对数据密文进行解密得到数据明文。

(5) B 对解密后得到的数据明文用哈希函数进行运算, 得到一个新的数据摘要, 把它与之前的数据摘要 x 进行比较, 若一致, 则数据完整性得到保证, 说明接收到的数据信息是有效的。

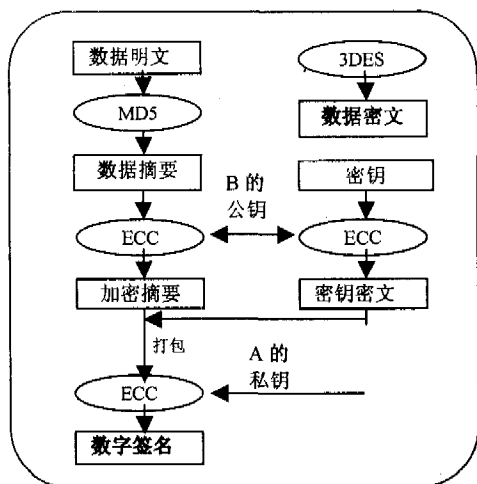


图 1 发送方 A

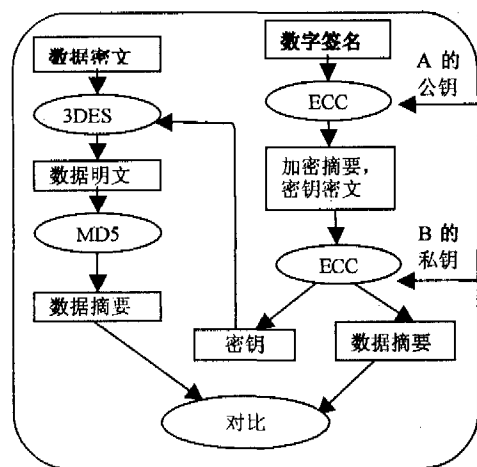


图 2 接收方 B

3 PKI 模型实现的核心算法

如上文所述, PKI 系统确保通信安全所依赖的是加密算法, 尤其是其中的非对称加密算法。所以, 这个模型的核心就是 ECC。模型实现的关键问题就是如何高效快速地实现 ECC 算法。而寻求 ECC 的快速算法也一直是椭圆曲线密码研究中的一个重要问题。文中在这方面进行一些探索和尝试。

在给定的一条有限域 $GF(q)$ 上的椭圆曲线中, 设 P 和 Q 是其上两点, n 是一正整数, 设 $Q = nP$, 从 n, P 求 Q

存在有效的算法,而从 P, Q 求 n 没有有效的算法,这个问题就是椭圆曲线离散对数问题。椭圆曲线密码体制就是基于这一特性,仿照 ElGamal 类加密体制和签名方案、Diffie-Hellman 密钥交换方案构造的。

在椭圆曲线密码体制中,从 n, P 求 Q ,称为椭圆曲线的点积运算,它是密码体制实现中的核心步骤。目前从 n, P 求 Q 一般通用的算法是 Binary Algorithm, Sliding Window Method 等。在这些算法中,从 P 计算 $2^s P, s \neq 1$ 是核心步骤,通常的算法中 s 取8。这个运算称为倍点运算,它是上述点积的基础,也是加密过程中最常用的运算。下面对这个运算进行研究。

3.1 旧的算法分析

根据椭圆曲线倍点公式,在有限域 $GF(q)$ 上,设 $P = (x, y), 2P = (x_1, y_1)$

其中: $x_1 = (x + \frac{y}{x})^2 + (x + \frac{y}{x}) + a$

$$y_1 = x^2 + (x + \frac{y}{x})x_1 + x_1$$

在计算的过程中一般要用到 $2^k P, k \geq 1$,可以直接一步步地计算 $2P, 2^2 P, 2^3 P \dots$,但是这样效率非常低。文献[4]中提出可以直接计算 $4P, 8P, 16P$ 来计算 $2mP, m \geq 1$,而不是一步步计算 $2P, 2^2 P, 2^3 P \dots$ 。文献[4]中算出 $4P = (x_2, y_2)$, 其中 $x_2 = \frac{\xi^2 + (\delta\gamma)\xi}{(\delta\gamma)^2} + a, y_2 = \frac{\xi(\delta\gamma)x_2 + (\delta^2)^2}{(\delta\gamma)^2} + x_2, \gamma = x^2, \eta = \gamma + y, \delta = \eta^2 + \eta x + a\gamma, \xi = \eta x + \gamma, \zeta = \delta(\delta + \xi) + \gamma^2$,从这些表达式中可以看到,虽然直接计算 $4P$ 与先算 $2P$ 再算 $2 \cdot 2P$ 相比需要多计算9次乘法,但是可以少一次求逆运算。由于一次求逆运算的时间通常多于9次乘法的时间,所以这样能有效地减少运算时间。

3.2 一种改进的快速算法

文献[5]在上面的基础上进行推广,给出直接计算 $2^s P, 1 \leq s \leq m$ 的公式,可以进一步减少计算量。先推导出 $2^s P, 1 \leq s \leq m$ 的表达式,记 $2^k P = (x_k, y_k)$,则:

$$x_k = (x_{k-1} + \frac{y_{k-1}}{x_{k-1}})^2 + (x_{k-1} + \frac{y_{k-1}}{x_{k-1}}) + a;$$

$$y_k^2 = x_{k-1}^2 + (x_{k-1} + \frac{y_{k-1}}{x_{k-1}})x_k + x_k$$

这里是要把 (x_k, y_k) 直接表示成 $x_k = \frac{a_k}{c_k} + a, y_k = \frac{b_k}{c_k} + x_k$ 的形式。其中 a_k, b_k, c_k ,都是关于 x, y 的整式,这样就实现了用乘法来减少求逆的目的。将上两式代入递推式,就得到 a_k, b_k, c_k 的递推式:

$$c_k = \delta^2, a_k = \gamma^2 + \delta\gamma$$

$$b_k = a_{k-1}^4 + \delta\gamma x_k, \text{其中 } \delta = a_{k-1}c_{k-1}$$

$$\gamma = a_{k-1}^2 + b_{k-1}c_{k-1}, \text{而 } a_0 = x, b_0 = y, c_0 = 1$$

3.3 算法的分析比较

由上面的递推公式,可以来估计改进过的方法的计算

量。在改进的方法中计算 $2^s P, 1 \leq s \leq m$ 的运算量为 $4s$ 次乘法、 $4s$ 次平方、 $4s$ 次求逆、1次求逆,而逐步计算则需要 $2s$ 次乘法、 $2s$ 次平方、 s 次求逆。由于加法计算次数两种方法相差不大,忽略不计。前面几种运算都以176位为例,各自的时间如表1所示。

表1 各种运算计算时间

运算类型	计算时间(总时间/ μs)
176位平方	4.23
176位 \times 176位乘法	38.56
176位求逆	158.73

下面利用表1,通过计算总的运算量来比较改进后的方法和逐步计算。具体数据见表2。

表2 两种方法计算量的比较

	4P		8P		16P		2 ^s P	
	改进算法	逐步计算	改进算法	逐步计算	改进算法	逐步计算	改进算法	逐步计算
乘法	8	4	12	6	16	8	4s	2s
平方	8	4	12	6	16	8	4s	2s
求逆	1	2	1	3	1	4	1	s
总时间(μs)	501.05	488.62	710.77	720.24	920.49	977.24	169.16s + 158.73	243.31s
节省率			1.3%		5.8%		30.5%	

通过表2中的比较可以看出,改进的算法与文献[4]中算法的区别在于将费时的域中求逆运算替换为比较快的平方或者乘法运算,这样减少了计算量,加快了运算速度。改进的算法性能随着指数 s 的增大而提高,在极限情况下性能可比文献[4]的算法提高30%,所以这个算法更具有实用价值。将这个改进的算法应用到上述的PKI模型中,可以提高实现效率,进而提高整个PKI系统的性能。

4 总结

文中改进了一个基于ECC的PKI实用模型,并对其实现中最重要的倍点运算进行研究,介绍了它的高效算法,进而可以得出这个PKI模型比较具有实用价值的结论。

参考文献:

- [1] Schneier B. 应用密码学[M]. 吴世忠,祝世雄,张文政译. 北京:机械工业出版社,2000.2-4.
- [2] 卢开澄. 计算机密码学[M]. 北京:清华大学出版社,2003.282-297.
- [3] 周国祥,张庆胜. ECC应用于PKI之研究[J]. 合肥工业大学学报(自然科学版),2003,26(6):101-107.
- [4] Guajardo J, Paar C. Efficient algorithms for elliptic curve cryptosystems[A]. Advances in Cryptology, Proceedings of Eurocrypt'97[C]. [s.l.]:Springer-Verlag,1997.342-356.
- [5] 李湛. 一种改进的椭圆曲线密码实现算法[J]. 电子科技,2004(7):31-33.