文章编号:1001-5132（2008）02-0145-05

椭圆曲线加密体制在移动电子商务安全中的应用

周　宇，王晓东，曹小华

（宁波大学 信息科学与工程学院，浙江 宁波 315211）

摘要：重点分析了 ECC 在移动电子商务安全 WPKI 中加密及签名算法方面的改进和应用，并在 ECC 原理与 WPKI 体系结构的基础上，探讨了 ECC 在 WPKI 体系中 WTLS 证书、无线身份识别模块及 WTLS 协议的应用，最后论述了基于 ECC 的身份认证方案.

关键词：ECC；WPKI；移动电子商务；安全

中图分类号：TN918.8^{+}2　　文献标识码：A

随着移动通信技术和互联网技术逐渐发展成为信息产业的两大支柱，作为两者结合产物的移动电子商务(Mobile E-commerce)正日益得到广泛应用. 由于其涉及到移动环境下的资金流动，安全问题就成为整个业务成功的焦点. 在有线通信中，电子商务交易的重要安全保障之一是公钥基础设施(Public Key Infrastructure，PKI). 在保证信息安全、身份证明、信息完整性和不可抵赖性等方面，PKI已得到了普遍的认同[1]，PKI的系统概念、安全操作流程、密钥及证书等方面同样也适用于解决移动电子商务交易的安全问题. 但在应用PKI的同时要考虑到移动通信环境的特点，并据此对PKI技术进行改进，这是开放移动联盟(Open Mobile Alliance，OMA)提出的无线公钥基础设施(Wireless PKI，WPKI)的基本出发点[2].

在加密和签名算法方面，虽然WPKI支持传统的签名算法(如RSA)，但是从执行和资源的角度来看，在无线环境中执行这些算法也不太合适. 椭圆曲线加密体制(Elliptic Curve Cryptography，ECC)于 1985 年由Neal Koblitz和Vieter Miller提出[3]，它的数论基础是有限域上的椭圆曲线离散对数问题，而目前还没有针对这个难题的亚指数时间算法，因而在当今公钥密码体制中，ECC具有每比特最高的安全强度. 它的典型密钥长度比其他如RSA算法小 6 倍，如 163 位密钥的ECC具有 1 024 位密钥RSA及DSA相同的安全强度，这使得密钥存储、证书尺寸、内存使用及数字签名过程更为有效，同时ECC算法易于用软件硬件实现，因此最适合支持无线环境安全需要.

1　ECC 概述

1.1　椭圆曲线的定义

设 K 为域. 域 K 上的 Weierstrass 方程为：

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

其中 $a_i \in K$. 定义变量如下：

$$b_2 = a_1^2 + 4a_2 ,$$

$$b_4 = a_1a_3 + 2a_4 ,$$

收稿日期：2007-11-07.　　宁波大学学报（理工版）网址：http://3xb.nbu.edu.cn
基金项目：浙江省自然科学基金（2006832）.
第一作者：周　宇（1960－），男，江苏扬州人，硕士/副教授，主要研究方向：信息处理技术及信息安全. E-mail: zhouyu@nbu.edu.cn

$b_6 = a_3^2 + 4a_6$

$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$，

$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$.

当 $\Delta \neq 0$，域 K 上点集为：

$$E := \{(x,y) \mid y^2 + a_1 xy + a_3 y = x^3 + a_2 x_2 + a_4 x + a_6\} \cup \{o\}, \quad (2)$$

其中 $a_i \in K$，$\{o\}$ 为无穷远点，称为域 K 上的椭圆曲线.

在实际的密码学应用中，主要研究和应用的椭圆曲线方程有以下 2 种：

(1) 有限域上的椭圆曲线 F_q (表示 q 个元素的有限域)：$y^2 = x^3 + ax + b$，其中 $a, b \in F_q$，满足 $4a^3 + 27b^2 \neq 0$.

(2) 有限域上椭圆曲线 F_2^m ：$y^2 + xy = x^3 + ax^2 + b$，其中 $a, b \in F_2^m$，满足 $b \neq 0$.

1.2 基本运算

在 K 为实数域的时候，从几何角度理解椭圆曲线的加法运算比较直观. 如图 1 即为椭圆曲线上不同两点 $P(x_1, y_1)$ 和 $Q(x_2, y_2)$ 的加法：连接点 P 和 Q 交曲线 E 于另一点，过该点作平行于纵坐标轴的直线与曲线 E 相交于点 $R(x_3, y_3)$，则 R 为 P 和 Q 两点之和，记为 $R = P + Q$.

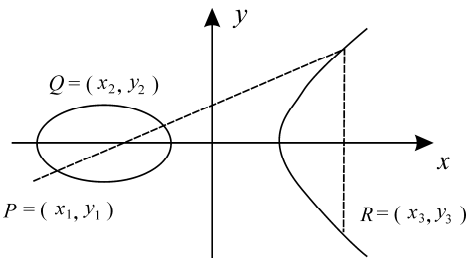

图 1 椭圆曲线的点加运算

特殊情况下，当 P 和 Q 为同一点时，过点 P 作曲线 E 的切线与曲线交于一点，过该点作平行于纵坐标轴的直线与曲线 E 相交于点 $R(x_3, y_3)$，记为：$R = P + P = [2]P$，称为椭圆曲线的倍点运算[4]，如图 2 所示；若切线和纵坐标轴平行即交曲线于无穷远处，则 $P + P = O$，即点 P 是椭圆曲线 E 上阶为 2 的点.

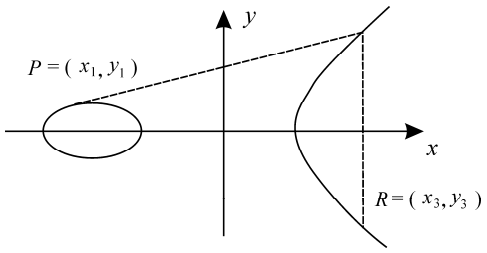

图 2 椭圆曲线的倍点运算

由倍点运算更进一步，可以得到椭圆曲线的标量乘运算定义：$Q = [k]P$，即 k 个点 P 相加得到的结果，该运算是构成椭圆曲线密码体制的基础，也是涉及效率问题的关键步骤.

1.3 典型椭圆曲线密码体制

在椭圆曲线构成的 Abel 群 $Ep(a, b)$ 上考虑方程 $Q = kP$，其中 $P, Q \in Ep(a, b), k < p$，则由 k 和 P 比较容易计算 Q，而对给定的 Q 和 P 计算 k 则是困难的，此为椭圆曲线上的离散对数问题(ECLDP).

EC-Diffie-Hellman 密钥交换协议：选取有限域 K、椭圆曲线 E/K 及基点 $P \in E(K)$. K, E, P 为公开信息. 若 A 与 B 想进行密钥交换，执行的具体步骤如下：

(1) A 产生 1 个 E 上的点 m，B 产生 1 个 E 上的点 n，分别作为自己的私钥.

(2) A 计算 $K_A = mP$，B 计算 $K_B = nP$.

(3) A 把 K_A 传送给 B，同时 B 把 K_B 传送给 A.

(4) A 计算：$K_C = mK_B$；Bob 计算：$K_C = nK_A$，K_C 即为 A 和 B 所商定的密钥.

2 WPKI 体系结构

WPKI的主要组件包括[5]：终端实体应用程序(EE)；PKI门户(PKI Portal)；认证中心(CA)；目录服务(PKI Directory)；WAP网关. 在应用模型中还涉及数据提供服务器等设备，WPKI的体系结构如图 3 所示.

2.1 终端实体 EE

EE 依赖 WMLSCrypt API 实现密钥管理和加

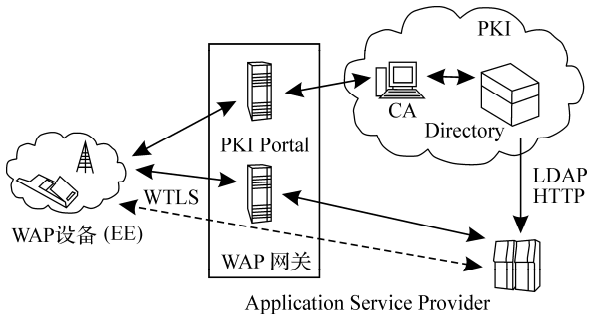

图 3　WPKI 结构

密运算，包括产生、存储并允许访问用户公钥/密钥对；初始证书申请；证书更新请求、证书撤消请求；查询、恢复和撤消证书信息；验证证书和读取证书内容；产生和验证数字签名.

2.2　PKI Portal

理论上功能类似于 PKI 中的 RA 功能，一般作为手机终端和 PKI 之间的连接桥梁，负责将 WAP 客户的需求转换给 PKI 中 RA 和 CA. PKI Portal 内嵌 RA 功能，实现与无线网络中的 WAP 设备和有线网络中的 CA 互相操作.

2.3　WAP 网关

在 WAP1.X 中需要 WAP 网关来处理客户与源服务器之间的协议转换工作. WAP 网关使用 WAP 协议与客户通信，使用标准 Internet 协议与源服务器通信. WAP2.0 标准则有了较大的改进，但仍兼容 1.0 标准. 在 WAP2.0 中客户与源服务器之间可以直接使用 HTTP/1.1 通信，当然，配置 1 个 WAP 代理还可以完成其他一些处理工作，主要则是对移动服务功能的增强.

3　ECC 在 WPKI 中的应用

3.1　WTLS 证书

WPKI 为减小公钥证书存储空间，一种机制是定义新的证书格式——WTLS 证书格式，比 X.509 证书格式尺寸(大小约 2 K，对于仅有 8 k 容量大小的 SIM 卡来而言仍属负担)明显减小. 另一种机制是在证书的储存上引入大于 100 bytes 的 ECC，能用占较小内存的密钥，使得证书总尺寸缩小. 同时，WPKI 对 IETF PKIX 证书格式中的一些字段尺寸做了限制，但由于 WPKI 是 PKIX 的子集，此举可保证这些 PKI 标准互操作的可能性.

3.2　WIM

无线应用协议识别模块(WAP Identity Module，WIM)主要用于储存和处理用于用户识别和身份认证的信息. WIM 主要在无线终端内的智能卡上实现，而智能卡自身硬件的资源极为有限，因此用其实现安全系统面临着存储器容量和计算能力方面受到的限制.

将椭圆曲线密码体制应用于智能卡的具体优点有如下几方面：

3.2.1　卡密钥生成

在使用其他现有的公开密钥体制的应用中，密钥是在安全的环境中装进或注进卡中，而在卡上生成密钥基本上是不可行的. 使用 ECC 生成小密钥对所需的时间很短，因此如果有好的随机数发生器，则可在智能卡上外加一个计算能力非常有限的设备就可以生成密钥对.

3.2.2　不需要协处理器

传统 RSA 等公钥密码体制包含太多的运算，因而需要称为“密码协处理器”的专用硬件设备. 密码协处理器不但占用了宝贵的空间，还增加了大约 20%到 30%的芯片成本. 而使用 ECC 则减少了处理时间，算法且能在可用的 ROM 中实现，因而不需要额外的硬件.

3.2.3　可升级

智能卡应用需要越来越强的安全性(使用更长的密钥)，而 ECC 只需要较少的附加系统资源就可增强安全性，这意味着如使用 ECC，智能卡能够提供更高的安全性而不需要增加另外的成本.

3.3　WTLS 协议

WTLS是用于提供移动设备到WAP网关的通信安全[6]. WTLS协议从TLS1.0 演化而来，并针对无线信道和嵌入式系统的特殊要求作了一些修改.

WTLS 定义了 ECDH 和 ECDSA 作为可选的算法之一. ECDH 用于交换密钥协商信息，而 ECDSA 用于对密钥协商信息进行数字签名. 如客户机在向服务器发送连接请求的同时，提议使用 ECDH-ECDSA 算法进行密钥协商，ClientHello 中算法信息内容就包括椭圆曲线参数，其中还包括曲线方程系数、伽罗瓦域定义参数、生成元 G 和阶 r . 如果服务器同意使用这种算法，ServerHelloM 就会向客户机发送含有 ECDH 公钥和 ECDSA 公钥的服务器证书，然后客户机向服务器发送自己的 DH 公钥，这些信息都经过 ECDSA 算法签名的. 这样双方通过 ECDH 算法可以安全地协商出 1 个秘密值，再通过 1 个伪随机数产生方法，从这个秘密值中产生安全连接所需的全部参数.

4 实现身份认证

4.1 初始化

4.1.1 CA 选择椭圆曲线参数

CA 选取有限域 F_q 上的椭圆曲线 $E: y^2 = x^3 + ax + b$，即给出 1 组椭圆曲线参数 (q, a, b, G) . 整数 q 表示 1 个有限域 F_q ； $a, b \in F_q$ 定义 1 条椭圆曲线； G 表示 1 个基点.

对于以上各参数有如下要求：要选择一条足够安全的椭圆曲线，其 q 要大于 2 160，a, b 由 CA 随机选取，但保证 $a, b \in F_q$ 及 $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, q)$ ；其基点 $G(G.x, G.y)$ 也是由 CA 选取的椭圆曲线 $E: y^2 = x^3 + ax + b$ 上的点. 这些参数都被写入椭圆曲线参数文件，可以被任何用户所访问.

4.1.2 EE 申请证书

(1) EE 在 WIM 中产生公钥、私钥对：用户 S 随机选取整数 k_S 作为其私钥，计算 $G_S = k_S G$ (点积运算)，则 G_S 为用户的公钥.

(2) EE 向 PKI Portal 申请证书：EE 获得根 CA 证书，WTLS 中采用 ECDH-ECDSA 算法建立安全通道，传递用户 S 的公钥 G_S .

(3) PKI Portal 验证通过后，向 CA 转发证书申请.

(4) CA 生成证书：CA 中心对 G_S 产生数字签名，记为 $Ds(G_S)$ ，再产生证书 $C = \{G_S, Ds(G_S)\}$ ，存入 PKI Directory，并取得证书 URL.

(5)颁发证书：CA 通过 RA 将证书 URL 返回 EE.

4.2 身份认证流程

WPKI标准提供了WTLS Class2、WTLS Class3和SignText 3 种功能模式[6]. 在此则采用WTLS Class3 模式：

(1) 用户在客户端签署交易后，并发送交易内容、数字签名和用户证书的 URL 到服务器(逻辑上通过 WAP 网关)；

(2) 服务器根据证书的 URL 向证书数据库验证用户证书(如果用户证书已经在证书数据库中)；

(3) 如果有需要，证书数据库将发送用户证书到服务器；

(4) 服务器签署交易，并发送交易内容、数字签名和服务器证书到 EE(逻辑上通过 WAP 网关)；

EE 利用根 CA 证书对服务器证书验证通过，从而在 EE 和服务器间建立 WTLS 会话. WAP 网关只起路由器的作用，移动终端与应用服务器之间的通信对 WAP 网关是透明的，其流程如图 4 所示.

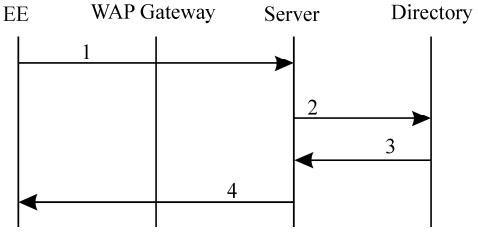

图 4 WTLS Class3 流程

5 结束语

WPKI 作为 PKI 在无线通信环境下的优化，可以有效保证信息安全、身份证明、信息完整性和不可抵赖性，而 WPKI 技术的核心优化则是数据加密

算法. ECC 以其短密钥的特点，具有安全性能更高、计算量小、处理速度快、存储空间占用小及带宽要求低优点，比传统的 RSA 等公钥密码算法更适于无线无线通信环境下的安全应用.

参考文献：

[1] 谢冬青, 冷健. PKI 原理与技术[M]. 北京: 清华大学出版社, 2004.

[2] WAP Forum. WAP public key infrastructure definition [EB/OL]. [2001-08-21]. http://www.wapforum.org.

[3] Certicom Corporation. SEC 1: elliptic curve cryptography [EB/OL]. [2005-06-12]. http://www.secg.org/download/aid-385/sec1_final.pdf.

[4] Darrel Hankerson. 椭圆曲线密码学导论[M]. 张焕国, 译. 北京: 电子工业出版社, 2005.

[5] WAP Forum. WAP 2.0 technical white paper[EB/OL]. [2002-11-09]. http://www.wapforum.org.

[6] WAP Forum. Wireless transport layer security[EB/OL]. [2001-06-07]. http://www.wapforum.org.

[7] 栗红生. 无线公钥体系在无线数据业务中的应用[J]. 计算机工程与设计, 2006, 27(12):2 309-2 310.

Application of Elliptic Curve Cryptography in Security of Mobile E-commerce

ZHOU Yu, WANG Xiao-dong, CAO Xiao-hua

(Faculty of Information Science and Technology, Ningbo University, Ningbo 315211, China)

Abstract: This paper focuses on the improvement of ECC application in encryption algorithm of WPKI for mobile e-commerce. Based on the principium of ECC and architecture of WPKI, the ECC's application in WTLS certification, wireless identification module and WTLS protocol are explored. In the end, an identity authentication solution based on ECC is described.

Key words: ECC; WPKI; mobile e-commerce; security

CLC number: TN918.8^{+}2　　**Document code:** A

（责任编辑　章践立）