一种基于ECC的消息安全交换方案

杨世平[1,2]，李 祥[1]

(1. 贵州大学计算机软件与理论研究所 贵阳 550025; 2. 贵州大学明德学院 贵阳 550004)

【摘要】提出一种基于ECC的消息安全交换方案，实现建立在ECC之上的消息安全交换的数字签名和加密消息的会话密钥交换。利用有限域上椭圆曲线点群中的离散对数问题的难解性来增强协议的安全性。通信的各方产生自己的私钥和公钥对，用户的证书由CA签发后交给用户保存，交换的消息和签名等信息采用压缩加密传输，避免了消息在传输的过程中被第三者窃取或篡改，保证了数据的机密性、完整性和不可否认性。

关 键 词 数字签名; 椭圆曲线密码体制; 消息交换; 安全协议
中图分类号 TN301.6 文献标识码 A

Scheme of Secure Message Interchange Based on ECC

YANG Shi-ping[1,2], LI Xiang[1]

(1. Institute of Computer Software and Theory, Guizhou University Guiyang 550025; 2. Mingde College, Guizhou University Guiyang 550004)

Abstract A scheme of secure message interchange based on Elliptic Curves Cryptosystem (ECC) is proposed in this paper. The digital signature and symmetric key exchange in the scheme both are established on ECC. The computational intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP) over a finite field enhances security of the scheme. Each end user in a network generates its own private key and public key. Users' certificates are signed by CA and then sent to each user to keep respectively. The message and its digital signature are encrypted to transmit in the network without disclosure. The scheme proposed here provides mutual authentication between the sender and the recipient and ensures confidentiality, integrity and nonrepudiation of the interchanged messages.

Key words digital signature; elliptic curves cryptosystem; message interchange; secure protocol

消息交换(电子文档、电子邮件等)是网络中的主要应用功能之一。网络中未经安全处理的消息容易被未授权地复制、修改甚至伪造，参与消息交换的双方事后对交换的消息予以否认等。因此，如果没有安全的消息交换协议保障，通过网络交换平台传输的消息就很难保证在传输的过程中未受篡改或伪造，即未经安全处理的消息其保密性、完整性和不可否认性等往往得不到保证。

目前国内外在网络信息交换应用研究方面的一个重要成果是Pretty Good Privacy (PGP)[1]，它是公钥密码体制[2]和对称密钥体制相结合的一个典型应用，广泛应用于签名和加密重要文件及发送、接收加密的电子邮件，以保证它们在网络上的安全传输。PGP采用一种RSA或DSS和传统加密的IDEA杂合算法，对电子邮件进行签名和压缩加密。PGP设计的基本思想是对待发送的电子邮件进行签名，然后随机生成一个密钥(每次加密不同)，用IDEA算法对邮件和签名加密，随机密钥用RSA算法加密。接收方同样用RSA解密出该随机密钥，再用IDEA解密邮件和签名。这样的链式加密做到了既有RSA体系的保密性，又有IDEA算法的快捷性。本文借鉴该设计思想，用ECC实现收发两方的双向认证、消息的数字签名和验证、公钥证书的分发和随机加密密钥的交换等，提出了一个有效、安全的消息交换方案。

1 椭圆曲线密码体制的概念[3-5]

将椭圆曲线(Elliptic Curve)用于密码的算法，是利用有限域上椭圆曲线的点构成的群实现离散对数密码算法。满足椭圆曲线方程的一个有序对偶称为一个点，常用P、Q表示。P的坐标为$P=(x,y)$，x、y属于该有限域；P的x、y坐标分别表示为$P.x$和$P.y$。

椭圆曲线上的点乘运算是椭圆曲线密码系统的

收稿日期：2006 – 09 – 08
基金项目：贵州省科学技术基金资助项目(黔科合J字[2007]2204号)
作者简介：杨世平(1955 –)，男，教授，主要从事网络与信息安全方面的研究.

核心运算之一。椭圆曲线上的点乘运算定义如下：给定一条椭圆曲线E和曲线上的一点P，曲线E上的P点的点乘xP为点P与自身相加x次之和，即$xP=P+P+\cdots+P$，共x个P相加。

若E为GF(p)上的椭圆曲线，P为E上的一点，则E上关于P的椭圆曲线离散对数问题为：给定一点$N\in E$，求解整数$x\in \mathrm{GF}(p)$，使$xP=N$。

1.1 椭圆曲线数字签名算法[5-7]

设系统参数为(GF (p), E, P, n, H)，其中，GF(p)为有限域；E为GF(p)上的椭圆曲线；P为基点，其阶为大素数n；$(k,Q_k=kP)$为私、公密钥对；m为待签名的消息；$H(\cdot)$为一个Hash函数。ECDSA算法如下：

1) 签名算法：

(1) 选取随机整数$t\in[2,n-2]$，计算：$Q=tP=(x,y)$，$r=Q.x \bmod n$。

(2) 计算：$e=H(m)$，$s=t^{-1}(e+kr)\bmod n$。

(3) 消息m的签名为(r, s)。

2) 验证算法：

(1) 计算：$e=H(m)$，$u_1=s^{-1}e\bmod n$，$u_2=s^{-1}r\bmod n$。

(2) 计算：$R=u_1P+u_2Q_k=(x,y)$，$v=R.x \bmod n$。

(3) 当且仅当$v=r$，接受签名。

验证算法的正确性如下：如果$e=ts-rk \bmod n$，则$u_1+u_2k=es^{-1}+rs^{-1}k=t-rs^{-1}k+rs^{-1}k=t \bmod n$，并且$nP=O$，所以$u_1P+u_2Q_k=u_1P+u_2kP=(u_1+u_2k)P=tP$。

1.2 椭圆曲线**Diffie-Hellman**密钥交换算法[5-7]

椭圆曲线Diffie-Hellman密钥交换算法的目的是使两个用户能够安全地交换一个密钥，以此用于后继的消息加密，算法本身只用于密钥的交换。Diffie-Hellman密钥交换算法的安全性是基于有限域上离散对数难解问题，而椭圆曲线Diffie-Hellman密钥交换算法有更好的安全性。

用户A和B选择一个共同定义在有限域上的椭圆曲线E和一个阶为大素数n的基点P，密钥交换算法如下：

(1) 用户A选择一个整数d_a，满足$d_a\in[2,n-2]$。A计算其公开密钥$Q_a=d_aP$，发送给B，d_a作为A的私有密钥被秘密保存。

(2) 用户B选择一个整数d_b，满足$d_b\in[2,n-2]$，保存为自己的私钥，并计算其公开密钥$Q_b=d_bP$，发送给A。

(3) A产生秘密密钥$K=d_aQ_b$，B产生秘密密钥$K=d_bQ_a$。因$K=d_aQ_b=d_a(d_bP)=d_b(d_aP)=d_bQ_a$，故产生的密钥是相同的。

2 消息安全交换方案

消息安全交换方案要解决如参与消息交换的各方的认证、消息的机密性、完整性和各方事后的不可否认等问题。

设系统参数为(GF(p), E, P, n, H)并公开，其中，GF(p)为有限域；E为GF(p)上的椭圆曲线；P为基点；大素数n为基点的阶；d_a、Q_a、d_b、Q_b分别为网络中通信方A和B的私钥和公钥对；d_{CA}、Q_{CA}为CA中心的私钥和公钥对。在方案中，CA中心根据用户的请求，负责网络中所有用户的证书发放。私钥d_a、d_b分别由用户A和B持有并保密，公钥Q_a、Q_b则公开，由CA进行认证。t_a、t_b为证书的有效期，待发送的消息为m，$H(\cdot)$输入为不超过2^{64} b长的任意消息，输出为一个160 b长的消息摘要的Hash函数，如SHA-1($\cdot$)。

消息安全交换方案是实现用户A发送自己签名并加密的消息m给用户B，用户B解密收到的信息并进行签名验证：

1) A从CA处取得自己的证书并保存，证书用CA的私钥签名。

(1) A选择随机整数$d_a\in[2,n-2]$，计算：$Q_a=d_aP$，$A\rightarrow \mathrm{CA}:\mathrm{ID}_a,Q_a$。

(2) CA选择随机整数$k_a\in[2,n-2]$，计算：$R_a=k_aP$，$q_a=Q_a.x \bmod n$，$r_a=R_a.x \bmod n$，$s_a=k_a^{-1}\times(H(q_a,\mathrm{ID}_a,t_a)+d_{\mathrm{CA}}r_a)$，$\mathrm{CA}\rightarrow A:Q_{\mathrm{CA}},\mathrm{ID}_a,(r_a,s_a),t_a$。

(3) A计算：$e_a=H(q_a,\mathrm{ID}_a,t_a)$；保存：$Q_a,Q_{\mathrm{CA}},\mathrm{ID}_a,(r_a,s_a),e_a,t_a$。

2) B从CA处取得自己的证书并保存，证书用CA的私钥签名。

(1) B选择随机整数$d_b\in[2,n-2]$，计算：$Q_b=d_bP$，$B\rightarrow \mathrm{CA}:\mathrm{ID}_b,Q_b$。

(2) CA选择随机整数$k_b\in[2,n-2]$，计算：$R_b=k_bP$，$q_b=Q_b.x \bmod n$，$r_b=R_b.x \bmod n$，$s_b=k_b^{-1}\times(H(q_b,\mathrm{ID}_b,t_b)+d_{\mathrm{CA}}r_b)$，$\mathrm{CA}\rightarrow B:Q_{\mathrm{CA}},\mathrm{ID}_b,(r_b,s_b),t_b$。

(3) B计算：$e_b=H(q_b,\mathrm{ID}_b,t_b)$；保存：$Q_b,Q_{\mathrm{CA}},\mathrm{ID}_b,(r_b,s_b),e_b,t_b$。

3) A与B分别获取对方的证书，并验证CA的签名，计算数据加密密钥。

(1) $A\rightarrow B:\mathrm{ID}_a,Q_a$。

(2) B计算：$Q_k=d_bQ_a=(d_bd_a)P$。选取点Q_k的x坐标$q_k=Q_k.x \bmod n$为会话密钥，产生一个随机数g。

(3) $B\rightarrow A:\mathrm{ID}_b,Q_b,E_{q_k}(e_b,(r_b,s_b),t_b,g)$。

(4) A计算：$Q_k = d_a Q_b = (d_a d_b)P$。选取点$Q_k$的$x$坐标$q_k = Q_k.x \bmod n$为会话密钥；$D_{q_k}(E_{q_k}(e_b,(r_b, s_b),t_b,g))$解密得到：$e_b,(r_b,s_b),t_b,g$。

A验证CA的签名：$c = s_b^{-1}$，$u_1 = ce_b \bmod n$，$u_2 = cr_b \bmod n$，$R = u_1 P + u_2 Q_{\mathrm{CA}}$，$v = R.x \bmod n$；当且仅当$v = r_b$，签名正确。

计算数据加密密钥：$k_m = (Q_k.x + g) \bmod n$。

(5) $A \to B: E_{q_k}(e_a,(r_a,s_a),t_a,g)$。

(6) $D_{q_k}(E_{q_k}(e_a,(r_a,s_a),t_a,g))$。

B解密得到$e_a,(r_a,s_a),t_a,g$。B验证CA的签名：$c = s_a^{-1}$，$u_1 = ce_a \bmod n$，$u_2 = cr_a \bmod n$，$R = u_1 P + u_2 Q_{\mathrm{CA}}$，$v = R.x \bmod n$；当且仅当$v = r_a$，签名正确。

计算数据加密密钥：$k_m = (Q_k.x + g) \bmod n$。

4) A对发送的消息签名并加密传输。

(1) A选择随机整数$t \in [2, n-2]$，计算：$Q = tP$，$r = Q.x \bmod n$，$s = t^{-1}(H(m) + d_a r) \bmod n$，$M_{\mathrm{zip}} = \mathrm{ZIP}(m,(r,s))$；将签名$(r, s)$附于消息$m$之后并压缩。

(2) $A \to B: E_{k_m}(M_{\mathrm{zip}})$；$A$将压缩的数据加密发送给$B$。

5) B对收到的消息解密并验证。

(1) $M_{\mathrm{zip}} = D_{k_m}(E_{k_m}(M_{\mathrm{zip}}))$。

(2) $(m,(r,s)) = \mathrm{UNZIP}(M_{\mathrm{zip}})$，解压缩$M_{\mathrm{zip}}$后分离出$m$、$r$、$s$。

(3) 验证签名。$e = H(m)$，$c = s^{-1}$，$u_1 = ce \bmod n$，$u_2 = cr \bmod n$。计算：$R = u_1 P + u_2 Q_a$，$v = R.x \bmod n$；当且仅当$v = r$，签名正确，保证了消息的m完整性。

至此完成了一次完整的消息交换。

在方案运行开始之前，用户自己生成公、私钥对，并通过秘密通道传送给CA，CA生成其证书，并且签名传输给用户保存，证书的有效期为$t_i (i = a,b,\cdots)$。当证书到期以后，再以同样的方式申请新的证书。当用户A准备向B发送一个消息m时，进行如下处理：消息m由用户A使用消息摘要算法压缩成为128 b或160 b的消息摘要e，再通过ECC签名算法，用私钥d_a对消息摘要e进行签名运算得到s，(r, s)即为A对公文m的签名。消息m、r与s拼接在一起压缩生成报文M_{zip}，并发送给B。用户B解压缩并分离出消息m、r、s，然后验证签名的正确性，检查消息的合法性和完整性。

3　消息交换方案的安全性分析

在上述消息交换方案中采用椭圆曲线密码体制来完成数字签名和密钥交换，其安全性依赖于椭圆曲线E上的离散对数的难解性，给定P、kP条件下计算k的难度。在实现相同安全性能条件下，椭圆曲线密码所需要的密钥长度小于RSA、DSA等基于有限域素数分解或者离散对数问题的公钥密码系统。

方案中的消息摘要函数可以选用SHA-1来产生“摘要”，它是美国联邦安全压缩标准(Secure Hash Standard，SHS)规定的算法，其输入为不超过2^{64} b长的任意消息，输出为一个160 b长的消息摘要。

消息交换中可选用IDEA算法来对消息和签名进行加密传送。IDEA是一个迭代分组密码，分组长度为64 b，密钥长度为128 b。IDEA密码中使用了三种不同的运算：⊕为逐位异或运算；田为模2^{16}加运算；⊙为模2^{16}+1乘运算(0与2^{16}对应)。IDEA算法由8轮和随后的一个输出变换组成。该算法所需要的混淆可通过对两个16位子块连续使用三个“不相容”的群运算来获得，并且选择使用的MA-结构(乘法和加法结构)可提供必要的扩散。IDEA密码能够抵抗穷举攻击分析、差分攻击分析和线性分析，其存在的弱密钥也不能证明它对IDEA是不安全的。IDEA是一种安全性较好、效率高的分组密码算法。

4　结 束 语

消息交换的应用非常广泛，它是电子政务、电子商务应用中的重要功能。消息在交换的过程中随时都有失密、篡改或伪造等被攻击的可能，因此，应具备一个安全的消息交换方案。本文正是从这样一个角度出发，提出一种利用有限域上椭圆曲线密码体制来实现消息的安全交换，解决消息交换的认证、机密性、完整性和不可否认的问题。

参 考 文 献

[1] BENZ J J. PGP: a hybrid solution[EB/OL]. http://www.sans.org/rr/whitepapers/vpns/717, 2004-04-05.

[2] CAELLI W J, DAWSON E P, REA S A. PKI, elliptic curve cryptography and digital signatures[J]. Computers and Security, 1999, 18(1): 47-66.

[3] KOBLIZ N. Elliptic curve cryptography[J]. Math. Computation, 1987,48(177): 203-209.

[4] MILLER V S. Use of elliptic curve in cryptography[C]// Advances in Cryptology, Proceedings of CRYPTO'85, Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1986, 218: 417-426.

[5] AYDOS M, SAVAS E, KOC C K. Implementing network security protocols based on elliptic curve cryptography[C]// Proceedings of the Fourth Symposium on Computer Networks. Istanbul, Turkey: [s. n.], 1999.

(下转第947页)

因此，如果复合膜的电阻以串联结构为主，则主要表现高电阻相的电阻特性；若以并联结构为主，则主要表现低电阻相的电阻特性。实验所制的复合膜的负电阻温度系数特性可能是由于在复合膜的等效电阻网络中，串联电阻状态占据重要地位，从而表现出高电阻相VO_2的阻温特性。

研究表明经过掺杂的VO_2虽然降低了相变温度，但由于杂质能级的引入严重降低了半导体相的电阻率，而对金属相的电阻率影响不大，从而大大降低了转换温度处电阻率的变化[9]；再加上复合膜中的聚合物导电相的影响，导致复合膜电阻的相变数量级与纳米VO_2粉体的相比，有一定程度的降低。

4　结　论

本文制备的纳米VO_2和PEDT的复合膜在30℃～40℃温区表现出明显的负电阻温度系数特性。通过计算简化模型的电阻表明当复合膜的电阻为串联结构时，则主要表现高电阻相的电阻特性。由于掺杂和导电聚合物相的作用，复合膜的电阻突变量比VO_2的有一定程度地降低。

本文制备的复合膜不仅具有VO_2的相变特性，其相变区域更接近室温状态，而且由于PEDT突出的导电聚合物特性，使其具有非常广阔的应用前景。

参　考　文　献

[1] GUINNETON F, SAUQUESB L, VALMALETTE J C, et al. Comparative study between nanocrystalline powder and thin film of vanadium dioxide VO_2: electrical and infrared properties[J]. J Phys. Chem. of Solids, 2001, 62: 1229-1238.
[2] KIVAISI R T, SAMIJI M. Optical and electrical properties of vanadium dioxide films prepared under optimized RF sputtering conditions[J]. Sol Ene. Mat & Sol Cel, 1999, 57: 141-152.
[3] GUINNETON F, VALMALETTE J C, GAVARRI J R. Nanocrystalline vanadium dioxide:synthesis and mid-infrared properties[J]. Opt Mater, 2000, 15: 111-114.
[4] 黄维刚, 林　华, 涂铭旌. 纳米VO_2粉体的制备及性能和应用[J]. 表面技术, 2004, 33(1): 67-69.
[5] GOODENOUGH J B. The two components of the Crystallographic Transition in VO_2[J]. Solid State Chem., 1971, 3: 450-490.
[6] 易　捷, 谢原寿, 苏国钧. 聚(3,4-乙撑二氧噻吩)的合成与应用[J]. 电子元件与材料, 2003, 22(8): 41-44.
[7] 陈湘宁. 导电聚合物BAYTRONR及其在固体电解电容器上的应用[J]. 电子元件与材料, 2000, 19(3): 35-36.
[8] BOUGUETTAYA M, VEDIE N, CHEVROL C. New conductive adhesive based on Poly(3, 4-ethylene dioxythiophene)[J]. Synthetic Metals, 1999, 102: 1428-1431.
[9] 袁宁一, 李金华, 林成鲁. 氧化钒薄膜的结构、性能及制备技术的相关性[J]. 功能材料, 2001, 32(6): 572-575.

编　辑　漆　蓉

(上接第823页)

[6] MENEZES A J, VANSTONE S A. Elliptic curve cryptosystems and their implementations[J]. Journal of Cryptology, 1993, 6(4): 209-224.
[7] AYDOS M, SAVAS E, KOC C K. An elliptic curve cryptography based authentication and key agreement protocol for wireless communication[C]//2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Dallas, Texas: [s.n], 1998.
[8] 秦志光, 张险峰, 周世杰, 等. 基于ECC的门限数字签名方案及其安全性[J]. 电子科技大学学报, 2005, 34(1): 109-112.
[9] 徐秋亮. 改进门限RSA数字签名体制[J]. 计算机学报, 2000, 23(5): 449-453.
[10] 刘木兰, 周展飞, 陈小明. 密钥共享体制[J]. 科学通报, 2000, 45(9): 897-898.

编　辑　黄　莘