基于ECC的自认证代理签密方案

俞惠芳[1] 王彩芬[2] 王之仓[1]
(青海师范大学计算机系 西宁 810008)[1] (西北师范大学数学与信息科学学院 兰州 730070)[2]

摘 要 为了克服代理签密中的证书管理问题和密钥托管问题,提出了一种新的基于椭圆曲线密码体制(ECC)的自认证代理签密方案,其困难性基于椭圆曲线离散对数问题(ECDLP)。与已有文献相比,此方案具有安全性强、密钥长度短、所需要存储空间少、占用带宽小、计算量和通信量低等优点。

关键词 代理签密,自认证代理签密,自认证签密,椭圆曲线离散对数问题
中图法分类号 TP309 **文献标识码** A

Self-certified Proxy Signcryption Scheme Based on Elliptic Curve Cryptography

YU Hui-fang[1] WANG Cai-fen[2] WANG Zhi-cang[1]
(Department of Computer Science, Qinghai Normal University, Xining 810008, China)[1]
(College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China)[2]

Abstract To overcome certificate management problem and key escrow problem in proxy signcryption schemes, a new self-certified proxy signcryption scheme based on elliptic curve cryptography(ECC) was proposed, it hardness relys on elliptic curve discrete logarithm problem(ECDLP). Compared with the existence literatures, the proposed scheme possesses good security and shorter key, less requirement of storage space and less bandwith requirement, lower computational complexity and communication cost.

Keywords Proxy signcryption, Self-certified proxy signcryption, Self-certified signcryption, Elliptic curve discrete logarithm problem

自从1985年Miller和Koblitz各自独立地提出椭圆曲线密码体制之后,人们不断深入研究以椭圆曲线上有理点构成的Abel群构建的椭圆曲线密码体制。椭圆曲线密码体制的安全性依赖于椭圆曲线的有理点群上离散对数问题的难解性。椭圆曲线密码体制具有"密钥短、速度快、安全性高"的突出优点,因此,对椭圆曲线密码体制的各种理论和应用的研究一直是密码学中的一个热点。

文献[1]提出了代理签密的概念和方案,代理签密是代理签名和加密技术的结合。代理签密是指,原始签密人由于某种不可避免的原因不能执行签密时,可以将数字签密的权力委托给代理签密人,让其代替他行使签密权。后来,许多代理签密方案[2-12]被提出。

本文利用椭圆曲线离散对数问题的难解性和自认证签密[13]的优点,设计出了一种新的基于ECC的自认证代理签密方案。

该方案满足代理签密的各种安全特性,不存在基于身份环境中固有的密钥托管问题和由于公钥证书的存在带来的一系列开销问题,而且具有安全性强、速度快、密钥长度短、算法简单易行、便于软硬件实现等特点。

1 复杂性假设

定义1 设G是阶为素数q的循环群,则G上的Elliptic Curve Discrete Logarithm Problem(ECDLP)是:已知P和Q是G中的元素,而且$Q=nP$,求解正整数s。

2 基于ECC的自认证代理签密方案

本节给出一个新的基于ECC的自认证代理签密方案,具体细节如下。

2.1 初始化

$F(q)$:定义的有限域;E:定义在有限域$F(q)$上的安全椭圆曲线;G:E上的一个阶为素数n的公开基点,其中,$G\in E(F(q))$;n:G的阶,是一素数;$h()$:是安全的哈希函数,$(.)_x$:E上点$(.)$的x坐标。

权威机构SA(System Authority)随机选择一个秘密值$s\in[1,n-1]$作为系统主密钥,然后,计算其公钥$y=sG$。

最后,SA公开$(E,q,n,G,h(),y)$,保密s。

2.2 用户密钥提取

(1)原始签密人A(其身份为d_A)随机选择一个秘密值$r_A\in$

到稿日期:2009-08-14 返修日期:2009-11-23 本文受教育部科学技术研究重点项目(208148),甘肃省科技攻关项目(2GS064——AS2-035-03),青海省科技厅软课题项目(2008-Z-620)和青海省重点课程《现代操作系统》建设项目资助。
俞惠芳(1972-),女,硕士,副教授,CCF会员,主要研究方向为信息安全、现代密码学,E-mail:yuhuifang@qhnu.edu.cn;王彩芬(1963-),女,教授,博士生导师,主要研究方向为信息安全、协议的设计以及协议的形式化分析;王之仓(1974-),男,硕士,副教授,主要研究方向为信息安全、神经网络。

$[1,n-1]$，计算 $y_A=r_AG$。然后，原始签密人 A 发送(d_A,y_A)给 SA。

(2)SA 收到(d_A,y_A)以后，计算 $Q_A=h(d_A,y_A)$和 $x_A=sQ_AG$，并将(y_A,x_A)发给原始签密人 A。

(3)原始签密人 A 收到(y_A,x_A)以后，可以通过方程 $x_A+r_AG=yQ_A+y_A$ 验证 x_A 的合法性。如果上式成立，则原始签密人 A 就计算 $S_A=r_A+(x_A)_x \bmod n$，并将其作为自己的私钥，y_A 作为自己的公钥。

(4)采用相似的方法，代理签密人 B 获得自己的公钥和私钥：(y_B,S_B)，接收者 C 获得自己的公钥和私钥：(y_C,S_C)。

2.3 代理密钥提取

原始签密人 A 建立一个授权许可证 m_w 用以明确原始签密人 A 和代理签密人 B 的身份信息、授权关系和授权关系的使用限制等内容。然后，执行以下步骤：

(1)A 计算 $\chi_A=h(m_w)S_A \bmod n$，然后，将(m_w,χ_A)发送给 B。

(2)B 收到(m_w,χ_A)后，检查验证等式 $\chi_AG=h(m_w)(y_A+(yQ_A)_xG)$是否成立。

若成立，则 B 计算代理密钥 $\chi_p=\chi_A+h(m_w)S_B \bmod n$；否则，要求 A 重发。

2.4 代理签密

为了发送消息 m 给接收者 C，代理签密人 B 进行以下协议：

(1)B 选择随机数 $k\in[1,n-1]$，计算 $R=kG$，并将 R 发送给 M。

(2)B 计算 $V=k(y_C+(yQ_C)_xG)$和 $c=m+(V)_x \bmod n$。

(4)B 计算 $S=h(m,R)k^{-1}\chi_p \bmod n$。

(5)B 输出密文(m_w,R,c,S)。

2.5 解签密

接收者 C 收到密文(m_w,R,c,S)以后，执行以下步骤：

(1)计算 $V=RS_C$。

(2)恢复消息 $m=c-(V)_x \bmod n$。

(3)检查以下验证等式是否成立：

$$RS=h(m,R)\cdot h(m_w)\cdot((y_A+(y_AQ_A)_xG)+(y_B+(yQ_B)_xG))$$

若成立，密文(m_w,R,S)以及原始签密人 A 和代理签密人的公钥(y_A,y_B)同时被认证，C 就接受(m_w,R,S)；否则，验证失败，C 认为(m_w,R,S)不合法。

3 正确性分析

3.1 代理密钥提取阶段的正确性

$$\begin{aligned}\chi_AG&=h(m_w)S_AG=h(m_w)(r_A+(x_A)_x)G\\&=h(m_w)(r_AG+(x_A)_xG)\\&=h(m_w)(y_A+(yQ_A)_xG)\end{aligned}$$

3.2 签密提取阶段的正确性

$$\begin{aligned}V&=k(y_C+(yQ_C)_xG)=k(r_CG+(sQ_CG)_xG)\\&=kG(r_C+(x_C)_x)=RS_C\end{aligned}$$

$$\begin{aligned}RS&=kGh(m,R)k^{-1}\chi_p\\&=kGh(m,R)k^{-1}h(m_w)(S_A+S_B)\\&=h(m,R)\cdot h(m_w)\cdot((r_A+(x_A)_x)G+(r_B+(x_B)_x)G)\\&=h(m,R)\cdot h(m_w)\cdot((r_AG+(x_A)_xG)+(r_BG+(x_B)_xG))\\&=h(m,R)\cdot h(m_w)\cdot((y_A+(yQ_A)_xG)+(y_B+(yQ_B)_xG))\end{aligned}$$

4 安全性分析

定理 1 除了代理签密人和接收者外，其他任何人均不能从密文中提取出消息明文。

证明：攻击者可截获在公开信道上传输的代理签密组(m_w,R,c,S)。假设攻击者知道了原始签密人的私钥、代理签密人的私钥和代理签密密钥，那么攻击者为了从密文中恢复出消息明文，就必须要知道会话密钥 V。然而，由于攻击者不知道接收者的私钥 S_C，则不可能通过 $V=RS_C$ 计算出会话密钥 V，因此不可能通过 $m=c-(V)_x \bmod n$ 从密文中提取出消息明文。

那么攻击者为了获得会话密钥 V，只能通过 $V=k(y_C+(yQ_C)_xG)$计算出 V。然而由 $R=kG$ 求出 k，进而计算 $V=k(y_C+(yQ_C)_xG)$是不可行的，因为椭圆曲线离散对数问题是个困难问题。因此，攻击者不可能通过等式 $m=c-(V)_x \bmod n$ 得到关于消息明文的任何有用消息。

可见，攻击者在不知道随机数 k 和接收者私钥 S_C 的情况下，不可能计算出会话密钥 V，因而无法恢复出消息明文，即本文方案满足保密性。

定理 2 代理签密人不能否认他曾经向接收者发送过关于消息明文的有效代理签密。

证明：只有代理签密人才能声称有效的代理签密组(m_w,R,c,S)，任何第三方仲裁者均可以通过验证等式 $RS=h(m,R)h(m_w)((y_A+(yQ_A)_xG)+(y_B+(yQ_B)_xG))$检查$(m_w,R,S)$为代理签密人对消息 m 的有效密文，因为接收者恢复出消息 m 后，上述验证等式中的所有参数都是公开的。因此，接收者在不需要泄露其私钥的情况下，只要公开(m_w,R,m,S)，便可以在实现本文方案的可公开验证性的基础上，实现其强不可否认性。

因此，一旦代理签密人代替原始签密人创建了一个有效的代理签密组，他就无法否认自己的签密行为。

定理 3 本文方案满足强不可伪造性。

证明：因为签名 $S=h(m,R)k^{-1}\chi_p \bmod n$ 中含有系统主密钥 s、原始签密人的私钥 S_A、代理签密人的私钥 S_B 和代理签密人随机选取的 k，通过 $y=sG$ 求解 s 和通过 $R=kG$ 求解 k，相当于求解椭圆曲线离散对数困难问题，是不可行的，所以，除了代理签密人以外，权威机构、原始签密人、密文接收者以及与本文方案无关的任何第三方都不可能伪造关于消息 m 的有效密文，使得 $S=h(m,R)k^{-1}\chi_p \bmod n$ 成立。

再者，由于代理密钥 χ_p 中含有原始签密人的私钥 S_A 以及代理签密人的私钥 S_B，并且在解签密的验证过程中需要用到原始签密人的公钥 y_A 和代理签密人的公钥 y_B，因此每个原始签密人均无法否认其对此代理签密的授权，代理签密人也无法否认其签密。此外，在授权证书中包含了代理签密人的身份，从而攻击者不能冒充代理签密人。

因此，任何攻击者都不能伪造出一个有效的关于消息明文的代理签密。

定理 4 任何第三方都可根据密文确定相应的代理签密

(下转第 101 页)

增加，某个组的吞吐量单调增加。例如，在图5(b)中，当 p_n 从60%增加到90%时，组2的吞吐量从3.294Mbps增加到3.88Mbps。因此，增加的空闲信道可在组间动态分配。注意在图5(b)中，当 $p_n=30\%$ 时，组1的吞吐量为0Mbps。这是因为在该环境下，空闲信道非常少，不足以为每个组分配信道，仅部分投标较高的组能获得。

从以上仿真可以看出，新协议能够保证信道分配的公平性及动态性。

结束语 本文提出了一种新的认知MAC协议。协议的目标是在主用户达到收益最大化的同时最大化频谱的利用率，并且将次用户的带宽要求考虑在内。借用组合拍卖的思想，设计出一种新的拍卖算法，该算法作为协议的核心非常适合在特定场合解决信道分配问题。仿真实验表明，提出的新协议能最大化地利用频谱资源，保证信道分配的公平性及动态性。

参 考 文 献

[1] Federal Communications Commission, Spectrum Policy Task Force[R]. Rep. ET Docket no. 02-135. 2002

[2] Haykin S. Cognitive radio: Brain-empowered wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2005,23(2):201-220

[3] Neel J O. Analysis and Design of Cognitive Radio Networks and Distributed Radio Resource Management Algorithms[D]. Virginia Polytechnic Institute,2006

[4] Jia J, Zhang Q, Shen X. HC-MAC: A Hardware-constrained Cognitive MAC for Efficient Spectrum Management[J]. IEEE Journal on Selected Areas in Communications,2008,26(1):106-117

[5] Shin K G, Hamdaoui B. OS-MAC: An Efficient MAC Protocol For Spectrum-Agile Wireless Networks[J]. IEEE Transactions on Mobile Computing,2008,7(8):915-930

[6] Mishra A. A Multi-channel MAC for Opportunistic Spectrum Sharing in Cognitive Networks[C]// Military Communications Conference. 2006:1-6

[7] Su H, Zhang X. Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2008,26(1):118-129

[8] Mansi T, Ravi P. CSMA-based MAC Protocol for Cognitive Radio Networks[C]// IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2007:1-8

[9] Corderio C, Challapali K, Birru D, et al. IEEE 802.22: an introduction to the first wireless standard based on cognitive radios [J]. Journal of Communications,2006,1(1):38-47

[10] de Vries S, Vohra R V. Combinatorial auctions: A survey[J]. INFORMS Journal on Computing,2003,15(3):284-309

[11] Krishna V. Auction Theory[M]. Academic Press,2002

[12] The network simulator (ns-2)[EB/OL]. http://www.isi.edu/nsnam/ns/

(上接第92页)

人的身份。

证明：完整有效的密文中有原始签密人所建立的授权许可证 m_w，而 m_w 中有代理签密人的身份信息，任何第三方都可以从 m_w 中确定相应代理签密人的身份。

因此，本文方案满足强可识别性。

定理5 代理签密人不能将代理签密密钥用于产生有效密文以外的其它目的。

证明：由于授权许可证 m_w 出现在解签密阶段的验证等式 $RS=h(m,R)h(m_w)((y_A+(yQ_A)_xG)+(y_B+(yQ_B)_xG))$ 中，而且代理签密密钥中包含有原始签密人的授权信息，因此，代理签密人不能签署未经授权的信息，只能用于产生有效的代理签密组，当然他也不能把代理签密权利转给其他人。

因此，本文方案能够有效防止签密权力的滥用。

定理6 本文方案满足可区分性。

证明：授权许可证 m_w 描述了代理签密人的信息、原始签密人和代理签密人之间的约束信息，并会出现在有效的代理签密里。原始签密人的公钥及代理签密人的公钥都会出现在代理签名的验证等式里，而且最重要的是代理签密密钥里也包含代理签密人的私钥。因此本文方案能够很好地满足可区分性。

结束语 本文设计了一个新的基于ECC的自认证代理签密方案，此方案克服了双线性对运算量大以及计算效率低的缺陷，具有安全性强、计算量小、速度快、密钥长度短、便于计算机实现等优点，因而在移动通信、移动代理、电子商务、电子选举、电子拍卖等领域有着很好的应用前景。

参 考 文 献

[1] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy signcryption[C]// Proceedings of 22nd Australasian computer science conference. Berlin: Springer-Verlag,1999:420-431

[2] Chan W K, Wei V K. A threshold proxy signcryption[C]// Proceedings of International Conference on Security and Management. Monte Carlo Resort, Las Vegas, Nevada, USA, 2002:24-27

[3] Chan W K, Wei V K. A threshold proxy signcryption[C]// Proceedings of International Conference on Security and Management. Monte Carlo Resort, Las Vegas, Nevada, USA, 2002:24-27

[4] Wang Q, Cao Z F. Two proxy signcryption schemes from bilinear pairings[C]// Proceedings of CANS 2005, LNCS 3810. Berlin: Springer-Verlag, 2005:161-171

[5] Wang M, Li H, Liu Z J. Efficient identity based proxy-signcryption schemes with forward security and public verifiability[C]// ICCNMC 2005. LNCS3619. Berlin: Springer-verlag, 2005:982-991

[6] Li X X, Chen K F. Identity based proxy-signcryption scheme from pairings[C]// IEEE International Conference on Services Computing. Los Alamitos, California: IEEE Computer Society Press, 2004:494-497

[7] 刘俊宝，肖国镇. 带门限共享解密的多代理签密方案[J]. 计算机工程，2006,32(23):21-23

[8] 胡振鹏，钱海峰，李志斌. 基于身份的多接收者的代理签密方案[J]. 华东师范大学学报：自然科学版，2008(1):83-87

[9] 于刚，黄根勋. 一个前向安全的基于身份的代理签密方案[J]. 计算机工程与应用，2008(2):157-159

[10] 张学军，王育民. 高效的基于身份的代理签密[J]. 计算机工程与应用，2007,43(3):109-111

[11] 王书海，冯志勇，綦朝晖. 权限可控的公开验证代理签密方案[J]. 计算机应用，2008,28(12):3163-3164

[12] 禹勇，杨波，李发根，等. 基于身份的可快速撤销代理权的代理签密方案[J]. 电子与信息学报，2008,30(3):672-675

[13] 俞惠芳，王彩芬. 一个高效的自认证签密方案[J]. 计算机工程，2009,35(16):138-139,142