基于椭圆曲线的单轮零知识证明方案

孟 彦，侯整风，昂东宇，周 循
（合肥工业大学 计算机与信息学院，安徽 合肥 230009）

摘 要：零知识证明在信息安全领域有着很广泛的应用前景。然而传统的零知识证明方案为了保证方案的正确性需要多轮的迭代，大大增加了交互双方的通信量，使得方案往往不适合实际应用。提出了一种单轮零知识证明的方案，在保证方案正确性、完全性和零知识性的同时将方案运行的迭代次数降低到1，最大程度地减少了方案的通信量。同时将零知识证明扩展到了椭圆曲线上的离散对数问题，提高了方案的安全性。最后给出了构造单轮零知识方案的一个必要条件。

关键词：零知识证明；椭圆曲线；单轮零知识方案；交互式证明
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673-629X(2007)12-0147-04

One-Round Zero-Knowledge Proofs Protocol Based on Elliptic Curve

MENG Yan, HOU Zheng-feng, ANG Dong-yu, ZHOU Xun
(Department of Computer Science and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: A zero-knowledge proof (ZKP) is a powerful tool which can be used and already be used for many cryptographic applications. But for the completeness property and the soundness property the existing zero-knowledge proofs are iterative in nature. The multiple communication rounds makes ZKPs unsuitable in practice. In this thesis, propose a new ZKP protocol which runs in one-round while ensure the completeness property and the soundness property. On the other hand, extend ZKPs to elliptic curves. At last, proposed a necessary condition which was needed by constructing a one-round zero-knowledge proofs protocol.

Key words: zero-knowledge proofs; elliptic curves; one-round ZKP protocol; interactive proof

0 引 言

零知识证明(ZKP)是1989年由Goldwasser, Micali和Rackoff提出的一种交互式证明方案[1]，即示证者(Prover)向验证者(Verifier)证明他知道一个秘密(Secret)，但是验证者在验证后并不知道秘密是什么。随后1989年Uriel Feige, Amos Fiat和Adi Shamir又提出了基于零知识证明的身份认证方案[2]，首次将零知识证明应用在了信息安全领域。随后的十几年零知识证明在密码学领域有了很大的发展，被应用到了信息安全的很多领域，如：电子现金系统的构造[3]、匿名通信[4]、电子投票选举[5]、数字水印[6~8]、智能卡[9]等。但是现有的大多数零知识证明方案为了达到一定的安全强度都是需要多轮迭代运行的，这一特性很大程度上抑制了零知识证明方案的应用。近年来许多学者在降低零知识证明迭代次数上进行了大量的研究，提出了许多非交互式的方案[10,11]和常数轮的方案[12,13]。

零知识证明的适用范围是非常广泛的，Goldreich, Micali和Wigderson证明了任何NP问题都可以被零知识证明[14]，例如二次剩余问题、汉密尔顿图问题、离散对数问题等。在离散对数问题当中，建立在椭圆曲线域上的离散对数问题因为其计算上的复杂性得到了很多密码学研究者的重视，椭圆曲线加密系统也是近年来的研究热点。研究资料表明：椭圆曲线加密系统中只要160位的密钥长度就可以达到RSA加密系统中1024位密钥长度的安全性。相对于RSA和离散对数而言，在相同的安全强度下，椭圆曲线加密系统在实现具有加解密速度快、运行时系统功耗少，以及对通信带宽要求低等许多优点。正因为如此，椭圆曲线加密系统被应用在智能卡、移动通信加密、电子商务等诸多方面。1991年Neal Koblitz提出了基于椭圆曲线域上离散对数问题的零知识证明方案[15]，通过椭圆曲线上离散对数问题提高了方案的安全性，随后有研究者将这一方案应用在电子商务中[16]，但是该方案仍然是多轮迭代的。

收稿日期：2007-02-07
作者简介：孟 彦(1981-)，男，安徽合肥人，硕士研究生，研究方向为网络与信息安全；侯整风，教授，硕士生导师，研究方向为计算机网络与信息安全、数据库。

文中结合了以上两点提出了一种基于椭圆曲线离散对数问题的单轮零知识证明方案。方案利用了椭圆曲线上离散对数问题加强了方案的安全性,另一方面利用离散对数函数的自身特点、经过对多轮方案的修改,将方案证明所需的迭代轮数降低到了一次。

1 零知识证明

零知识证明的形式化定义已在文献[1,2]中给出,这里首先给出一个基本的基于离散对数的零知识证明方案[16]。

1.1 离散对数零知识证明

方案双方为示证者 Prover(P)、验证者 Verifier(V),其中 V 为计算上多项式有界的。示证者(P)向验证者(V)零知识地证明他知道一个给定数的离散对数。给定一个大素数 p,以及群 Z_p 的一个本原元 g 和 $m \in Z_p$。P 向 V 证明他知道 $g^s = m$ 中的 s。方案如下:

方案初始状态:P,V 共享 g,m,p;

1) P 随机选取 $r \in Z_p$,计算 Commit $= g^r$,发送 Commit 给 V;

2) V 选取并发送 Challenge $\in \{0,1\}$ 给 P;

3) P 计算

$$\text{Response} = \begin{cases} r & \text{如果 Challenge} = 0 \\ r + s & \text{如果 Challenge} = 1 \end{cases}$$

发送 Response 给 V;

4) V 检验

$$g^{\text{Response}} \stackrel{?}{=} \begin{cases} \text{Commit} & \text{如果 Challenge} = 0 \\ \text{Commit} \cdot m & \text{如果 Challenge} = 1 \end{cases}$$

如果检验显示错误,他拒绝 P 并且中止方案;否则 V 接收证明。

重复以上步骤 t 次。

从以上方案中可以很容易地看出在每一轮验证中,P 成功欺骗 V 的概率为 1/2,执行 t 轮迭代验证之后 P 成功欺骗 V 相信其证明的概率为 2^{-t},所以当 t 足够大的时候 2^{-t} 就可以达到一个足够小的量,那么 V 就可以充分相信 P 不会欺骗成功。方案的完全性、合理性以及零知识性已经得到证明[16]。

1.2 方案的分析

对于以上的一个基本的零知识证明模型需要确定迭代次数 t 达到多少对于 V 来说模型才是安全的,不会被 P 所欺骗。已经被证明在每一轮的欺骗概率为常量(1/2)的情况下,为了使差错概率降到一个可以忽略的小量,即对所有的常数 c,降为以 $1/(\log_2 p)^c$ 为界的一个量,方案就必须重复 $\log p$ 轮[17]。所以以上的方案就至少要运行 $\log p$ 轮。这对于实际应用来说是一个很大的弊端,P、V 双方的交互通信代价将很大。

2 基于椭圆曲线的单轮零知识方案

2.1 方案的提出

由上节的分析可以看出零知识证明最大的弊端在于为了保证方案最后的正确性,即零知识方案的完全性和合理性,必须将方案迭代运行多轮,以达到安全的差错概率下界。而在实际应用中,多轮迭代意味着示证者 P 和验证者 V 之间的多次通信。这大大地耗费了网络资源,也大大增加了方案运行的时间。为了克服这一弊端,一种单轮的零知识证明方案应运而生。另一方面,由于椭圆曲线上离散对数问题的计算复杂性,提高了方案的安全性,所以文中的单轮零知识方案也将基于椭圆曲线上的离散对数问题。下面简单给出方案:

给定有限域 F_p,并给定 F_p 上的一条椭圆曲线 E,E 的阶为 order(E)。对于给定椭圆曲线 E 上的一个基点 G,示证者 P 向验证者 V 证明他知道一个椭圆曲线上离散对数问题的解,即他知道 $s \cdot G = M(\text{mod}p)$ 中的 s。

初始条件:P,V 共享 p,G,M

1) V 随机选取 $r \in F_p$,计算 $B = r \cdot G$,发送 B 给 P;

2) P 计算 $K = s \cdot B$,发送 K 给 V;

3) V 检验 $K \stackrel{?}{=} r \cdot M$,如果等于则接收证明,如果不等于则不接收证明。

2.2 方案的证明

零知识方案的证明,即证明方案的完全性、正确性和零知识性。这三个性质的形式化定义已经在多篇文章中给出[2,16,17],在这里简单地给出方案的证明。

(1)完全性:直接由方案可以很容易地看出,如果 P 确实知道 S,并且遵守方案指令完成方案,那么 V 总是接收 P 的证明的。则方案是完全的。

(2)正确性:首先假设不诚实示证者 $\tilde{P}$ 不知道 s,但是他企图欺骗 V。因为方案是基于椭圆曲线上离散对数问题的,那么在步骤 1 中 $\tilde{P}$ 是无法解出 r 来构造欺骗的。如果他在步骤 2 中使用假的 s 构造 $K = \tilde{s} \cdot B$ 发送给 V,那么 V 在步骤 3 中必然由于检验失败而拒绝接收 $\tilde{P}$ 的证明。如果 $\tilde{P}$ 在步骤 2 中猜测 s 的值,那么猜中的几率为 $1/p$,这也正是方案的差错率。所以 V 将以 $1/p$ 的概率接收 $\tilde{P}$ 的证明,即 V 将以 $1 - 1/p$ 的概率拒绝 $\tilde{P}$ 的欺骗证明。

(3)零知识性:构造模拟器 $\varepsilon\sigma$,初始化 $\varepsilon\sigma$ 输出 OUTPUT 为空串。$\varepsilon\sigma$ 选取 $r \in F_p$,计算 $B = r \cdot G$;$\varepsilon\sigma$ 计算 $K = r \cdot M$,则模拟器 $\varepsilon\sigma$ 的输出为:B,K,r。对于

模拟器的输出,由于 r 是随机均匀选取的,所以 r, B, K 明显是与参数独立且与(P, V)的证明副本同分布的。证明完毕。

2.3 方案的分析

在 1.1 节的离散对数零知识证明方案中运行一遍方案分为"承诺"(Commit)、"挑战"(Challenge)、"应答"(Response)三个步骤,称这三个步骤为一轮。那么在 1.1 节方案中每一轮的差错概率为 1/2。P 欺骗 V 的方法是:$\tilde{P}$ 在发送 Commit = r 之前首先猜测 V 给出的 Challenge,当猜测 Challenge = 0 时发送 Commit = r 给 V,当猜测 Challenge = 1 时,由于在步骤 3 中发送的是 Response = $r + s$ 给 V,所以 $\tilde{P}$ 可以发送 Commit = f(Response)/m 给 V。这样 $\tilde{P}$ 有 1/2 的概率猜中 V 发出的 Challenge,成功完成欺骗。

在 2.1 节提出的新方案中,步骤2发送 $K = s \cdot B$,这样就阻止了 $\tilde{P}$ 计算 f(Response)/m,从而阻止了 $\tilde{P}$ 有 1/2 的概率欺骗 V,$\tilde{P}$ 要想欺骗 V 就只能猜测 s 的值,而在椭圆曲线域上猜测 s 的值的概率为 $1/p$,故给出方案的单轮差错概率为 $1/p$。如果在 1.1 节方案中,那么需要迭代运行 160 次才能够达到 $1/2^{160}$ 的差错概率;而在新的方案中,如果选择的大素数 p 为 160 位,则运行一次方案就可以达到 $1/2^{160}$ 的差错概率。这样大大地降低迭代的次数,减少了交互证明双方 P、V 的通信次数。

另一方面新的方案是建立在椭圆曲线离散对数问题之上的,我们知道现在解决 F_p 上的基本离散对数问题已知最好的算法是亚指数时间的,其时间杂度为 $\mathrm{Exp}(O((\log p)^{1/3}(\log\log p)^{2/3}))$;而解决椭圆曲线域 E/F_p 上已知最好的算法是指数时间的,其时间复杂度为 $\mathrm{Exp}(O(\log p))$[18],所以建立在椭圆曲线离散对数问题上的零知识证明方案具有更高的安全性[16]。此外,由于椭圆曲线算法的特殊性,方案很适合应用于智能卡等功耗和内存受限制的应用环境,拓展了方案的应用范围。

2.4 单轮零知识证明方案的构造条件

通过以上对方案的分析可以看出单轮的零知识证明方案与多轮迭代的零知识方案相比在应用上是具有很大优势的。但是单轮零知识证明方案的构造是有条件的,下面说明构造单轮零知识方案的一个必要条件。

定义 1　对于一个二元函数 $f(x, y)$,若等式 $f(x_1, f(x_2, y)) = f(x_2, f(x_1, y))$ 成立,则二元函数 f 关于变量 y 可交换。

定理 1　单轮零知识证明方案的证明问题满足的两个必要条件:单向同态函数;函数经过常量替换后为关于替换变量的可交换函数。

证明:条件 1 证明在文献[14]中已经给出;对于条件 2 证明有:设函数 $f(x)$ 经过常量替换后的函数为 $f(x, y)$,x 的一个值 x_s 为 P 向 V 证明他所拥有的秘密;V 随即选取的参数值为 x_r,为了在第三步验证 P 拥有秘密并且 P 不泄漏秘密 x_s,则必有等式 $f(x_r, f(x_s, y)) = f(x_s, f(x_r, y))$ 成立。证明完毕。

根据以上定义和定理,将方案 2.1 的函数 $f(x) = g^x$ 中的 g 替换为变量 y,则对于函数 $f(x, y) = y^x$ 有 $f(x_1, f(x_2, y)) = f(x_2, f(x_1, y))$,所以函数 y^x 是关于变量 y 可交换的。也正是这一性质使得在方案 2.1 中的第二步可以将秘密 s 通过离散对数问题进行包装,最后验证者 V 通过函数关于 y 可交换的性质来验证示证者 P 拥有 s,同时 V 无法得到 s。

另一个结论是:由于经典的二次剩余问题并不具备以上的性质,故不能应用在文中提出的方案中构成单轮的零知识方案。

3 结束语

提出了一种基于椭圆曲线离散对数问题的单轮零知识证明方案。方案避免了以往零知识证明方案中的多轮迭代,大大减少了交互证明双方的通信,同时方案基于椭圆曲线离散对数问题,提高了方案的安全强度,并且为智能卡,PDA 等内存和功耗限制设备上的应用提供了便利。此外还讨论了单轮零知识证明方案的构造条件,揭示了构造单轮零知识证明方案的一个必要条件。

参考文献:

[1] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems[C]// Proceedings of the 17th Annual ACM Symposium on Theory of Computing. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 1985:291-304.

[2] Feige U, Fiat A, Shamir A. Zero Knowledge Proofs of Identity[J]. Journal of Cryptology, 1988,1:77-94.

[3] Franklin M, Yung M. Secure and efficient off-line digital money[C]// Proceedings of the 20th International Colloquium on Automata, Languages and Programming (ICALP '93), Lecture Notes in Computer Science 700. Lund, Sweden: Springer-Verlag,1993:265-276.

[4] Ahn L, Bortz A, Hopper N. K-Anonymous Message Transmission[C]// Proceedings of the 10th ACM conference on computer and communication security. New York, NY, USA: SVM Press,2003:122-130.

[5] Baudron O, Pierre-Alain F, Pointcheval D, et al. Practical multi-candidate election system[C]// In PODC '01: Proceedings of the twentieth annual ACM symposium on Princi-

ples of distributed computing. New York, NY, USA: ACM Press, 2001: 274 - 283.

[6] Craver S. Zero - knowledge Watermark Detection[C]// Proceedings of the Third International Workshop on Information Hiding, Lecture Notes in Computer Science 1768. Berlin: Springer - Verlag, 2000: 101 - 116.

[7] Zou X X, Dai Q, Huang C, et al. Zero - Knowledge watermark verification protocols [J/OL]. Journal of Software, 2003, 14(9): 1645 - 1651. http://www.jos.org.cn/1000 - 9825/14/1645.pdf.

[8] HE Yong - Zhong, WU Chuan - Kun, FENG Deng - Guo. Publicly Verifiable Zero - Knowledge Watermark Detection[J/OL]. Journal of Software, 2005, 16(9): 1607 - 1616. http://www.jos.org.cn/1000 - 9825/14/1606.pdf.

[9] Beth T. Efficient zero - knowledge identification scheme for smart cards[C]// Advances in Cryptology: Proceedings of Euro - crypt'88. New York, USA: Springer - Verlag, 1988: 77 - 84.

[10] Blum M, Feldman P, Micali S. Non - interactive zero - knowledge and its applications (extended abstract)[C]// In Proceedings of the 20th Annual ACM Symposium on Theory of Computing. [s.l.]: ACM, 1988: 103 - 112.

[11] De Santis A, Persiano G. Zero - knowledge proofs of knowledge without interaction[C]// In 33rd Annual Symposium on Foundations of Computer Science. Pittsburgh, Pennsylvania: IEEE, 1992: 427 - 436.

[12] Bellare M, Micali S, Ostrovsky R. Perfect zero - knowledge in constant rounds[C]// In Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing. Baltimore, Maryland: [s.n.], 1990: 482 - 493.

[13] Brassard C, Crepeau C, Yung M. Constant - Round Perfect Zero - Knowledge Computationally Convincing Protocols[J]. Theoretical Computer Science, 1991, 84: 23 - 52.

[14] Goldreich O, Micali S, Wigderson A. Proofs that yield nothing but their validity or all languages in NP have zero - knowledge proof systems[J]. J. ACM, 1991, 38(3): 690 - 728.

[15] Koblitz N. Elliptic curve implementation of zero - knowledge blobs[J]. Journal of Cryptology, 1991, 4: 207 - 213.

[16] Almuhammadi S, Sui N T, McLeod D. Better Privacy and Security in E - Commerce: Using Elliptic Curve - Based Zero - Knowledge Proofs[C]// 2004 IEEE International Conference on E - Commerce Technology (CEC'04). Washington, DC, USA: IEEE Computer Society, 2004: 299 - 302.

[17] Mao Wenbo. Modern Cryptography: Theory and Practice[M]. Beijing: Publishing House of Electronics Industry, 2004.

[18] Balasubramanian R, Koblitz N. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone Algorithm[J]. Journal of Cryptology, 1998, 11(2): 141 - 145.

(上接第146页)

围,并代理与认证服务器的通信。并且在各个应用中加入filter,使得当用户在认证服务器验证,被转移到应用之后,应用系统能够根据自身原有的授权机制,授予用户特定的权限。这样就将授权的功能分布于各个应用之中。

4.3 认证服务端模块的实现

认证服务端主要处理统一的用户认证、用户代理访问、代理访问验证以及用户请求服务的验证;含两个认证子模块,分别用于处理基于密码的身份验证和基于服务的身份认证。原有系统中只需要改进子模块基于密码的身份验证。将身份的验证通过与数据库中的用户数据做比较,判断是否合法。

5 结束语

文中提出的基于CAS的SSO系统的设计与实现,完成了统一的身份认证,实现企业门户系统的单点登录,提高了用户使用系统的效率,减轻了系统管理员的工作负担,并且使得认证和授权分离,克服了原有系统的缺点,系统的分工以及层次清晰,在实际运行过程中,实现了三个应用之间的单点登录,稳定性好,能够快速反应,对于今后企业门户系统实现单点登录有较强的参考价值。

参考文献:

[1] 谭立球,费耀平,李建华.企业信息门户单点登录系统的实现[J].计算机工程,2005,31(17):102 - 104.

[2] The Open Group. Single Sign - On[EB/OL]. 2005. http://www.opengroup.org/security/sso, 1995 - 2005.

[3] JA - SIG Central Authentication Service[EB/OL]. 2006. http://www.ja - sig.org/products/cas/, 2005 - 2006.

[4] 邱 航,杜向辉.单点登录原型系统KSSO的设计与实现[J].计算机工程与设计,2006,27(9):1645 - 1648.

[5] Zhao Gang, Zheng Dong, Chen Kefei. Design of single sign - on[C]// E - Commerce Technology for Dynamic E - Business, 2004. IEEE International Conference. Beijing, China: [s.n.], 2004: 253 - 256.

[6] 金 辉. Single sign - on[EB/OL]. 2002 - 10. http://www - 900. ibm. com/developerWorks/cn/security/se - sso/index.shtml.