身份基认证密钥协商协议

路守克,史国川
(解放军陆军军官学院 计算中心,安徽 合肥 230031)

摘 要:为了使得用户间能在公共数据网络进行安全通信,利用椭圆曲线上双线性映射的特性提出了一个身份基认证密钥协商协议,利用双线性对生成会话密钥,为随后的通信提供机密性、完整性保证。该协议实现了通信双方的相互身份认证功能,使通信双方能确认对方的身份,同时还提供了密钥协商的功能。经过分析表明该协议满足较高的安全性,提供了已知密钥安全性、完善前向保密性、密钥泄露安全性、未知密钥共享安全性和密钥控制安全等安全属性,并且新协议在计算效率和安全性方面取得了较好的平衡,更加适合现实网络通信的需要。

关键词:身份基;认证密钥协商;安全属性;双线性对
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)12-0172-03

An Identity-Based Authenticated Key Agreement Protocol

LU Shou-ke, SHI Guo-chuan
(Computing Center, Army Officer Academy of PLA, Hefei 230031, China)

Abstract: Aiming to solve the communication security problems which in a public network, an ID-based mutual authentication and key agreement scheme is proposed in this paper, in which some characteristics of bilinear map are used. The functions implemented by this protocol include authentication, guaranteed the integrity and agree the session key fairly between two communications. Moreover, this protocol provides some security properties such as known key security, perfect forward secrecy, key-compromise impersonation, unknown key-share resilience and key control. This protocol has better security characteristic and keeping with the nice efficience, more suited to realities of the need of internet communications.

Key words: identity-based; authenticated key agreement; security attributes; bilinear pairing

0 引 言

随着信息技术的发展,人们对信息网络的依赖越来越强,电子商务、电子政务、企业信息化等与人们生活息息相关的信息安全问题已经成为全社会关注的焦点。认证密钥协商协议为开放的网络环境下安全通信提供了重要保证,允许通信双方(多方)在身份认证的基础上通过各自提供的信息共同协商一个安全的共享会话密钥,为随后的保密通信建立一个秘密的通道,使得通信参与方安全地传送信息,以此来保证数据的机密性、完整性。

1976年,Diffie和Hellman[1]首次提出了公钥密码学的概念同时给出了第一个密钥协商协议——Diffie-Hellman协议,该协议并没有进行双向认证,因此协议不能抵抗中间人攻击。在密钥协商协议中,参与方能够确定只有意定通信方可以计算相同的会话密钥,则称该协议提供了隐式密钥认证(Implicit Key Authentication, IKA)。认证密钥协商协议(Authenticated Key Agreement, AK)能够提供协议参与方之间双向隐式密钥认证。

身份基(或基于身份的, ID-based)密码系统最早由Shamir[2]在1984年提出。在基于身份的公钥密码系统中,用户的公钥就是用户的信息(电子邮件地址、姓名、电话号码等)或是根据用户信息得到,私钥由可信第三方——私钥生成中心(PKG, Private Key Genenator)生成。自2001年Boneh和Franklin[3]利用双线性对实现了身份基密码体制后,人们相继提出了许多实用的身份基加密体制和密钥协商协议以及改进协议[4~12]。

文中研究了身份基和双线性映射的密钥协商问题,首先回顾了协议需要的背景知识,在此基础上提出了一个新的身份基认证密钥协商协议,最后给出协议性能分析。

1 背景知识

设q为大素数,G_1和G_2分别为阶为q的椭圆曲线

收稿日期:2011-05-20;**修回日期**:2011-08-24
基金项目:安徽省自然科学基金(青年基金)项目(10040606Q63)
作者简介:路守克(1984-),男,硕士研究生,研究方向为网络信息安全;史国川,教授,研究方向为网络信息安全。

上的加法循环群和有限域上乘法循环群。双线性映射 $\hat{e}:G_1\times G_1\to G_2$ 是定义在群 G_1 和 G_2 上的双线性对。它必须满足以下性质:

a)双线性:对任意 $p,q\in G_1,a,b\in Z_q^*$,有 $\hat{e}(ap,bq)=\hat{e}(p,q)^{ab}$。

b)非退化性:$\hat{e}(p,p)\neq 1$。

c)可计算性:对任意 $p,q\in G_1$,存在多项式时间算法能够计算 $\hat{e}(p,q)$。

2 身份基认证密钥协商协议

2.1 身份基公钥基础设施(ID-Based PKI)

2001 年,Bone 和 Franklin 首次提出了实用的身份基公钥基础设施,并给出了一个身份基加密方案,在 ID-Based PKI 中,有一个密钥生成中心 KGC(Key Generation Center)来生成系统需要的参数和根据用户信息生成用户私钥,它包括系统设置算法和私钥抽取算法。

KGC 利用参数生成器 BDH 生成阶为素数 q 的循环群 G_1 和 G_2,一个双线性映射 $\hat{e}:G_1\times G_1\to G_2$,$p$ 是 G_1 的生成元。选择强密码哈希函数 $H_1:\{0,1\}^*\to Z_q^*$。

系统设置:KGC 随机选择 $s\in Z_q^*$ 作为系统主密钥,且 $P_{pub}=sP$,并把 s 作为系统主密钥保存,并公开系统参数 $\{G_1,G_2,q,p,P_{pub},H_1\}$。

私钥抽取:用户将身份标示信息 $ID_i\in Z_q^*$ 提交给 KGC,KGC 计算用户对应的公钥 $Q_{ID}=H_1(ID_i)$,在 KGC 注册私钥 $S_{ID}=S_{KGC}Q_{ID}$。然后把私钥安全的发给用户。

2.2 新协议描述

文中提出一个新的身份基认证密钥协商协议(见表 1),使得通信参与方能够在实现相互认证的同时共享一个会话密钥。假设用户 A 和 B 要进行安全通信,首先要经过 KGC 系统初始化,分别拥有公私钥对 (Q_i,S_i),且知道对方的公钥,其协商过程如下:

表 1　身份基认证密钥协商协议

A		B
$a\leftarrow Z_q^*$		$b\leftarrow Z_q^*$
$T_A=aQ_B$,		$T_B=bQ_B$
$T_{A1}=S_AQ_B$,		$T_{B1}=S_BQ_A$
$U_A=aP_{KGC}$	T_A,T_{A1},U_A →	
	← T_B,T_{B1},U_B	$U_B=bP_{KGC}$

(1)A 随机选择整数 a,计算 $T_A=aQ_B,T_{A1}=S_AQ_B,U_A=aP_{KGC}$,发送 T_A,T_{A1},U_A 给 B。

(2)B 随机选择整数 b,计算 $T_B=bQ_B,T_{B1}=S_BQ_A,U_B=bP_{KGC}$,发送 T_B,T_{B1},U_B 给 A。

(3) 用户 A 计算 $h=H_2(aU_B)$,$K_{AB}=\hat{e}(h(T_B+T_{B1}),S_AQ_B+aQ_B)$;相应的,用户 B 计算 $h=H_2(bU_A)$,$K_{BA}=\hat{e}(h(T_A+T_{A1}),S_BQ_A+bQ_A)$。

3 协议分析与比较

3.1 协议分析

3.1.1 正确性分析

利用双线性对的知识可以得到如下结果:在上述协议中,$K_{AB}=\hat{e}(h(T_B+T_{B1}),S_AQ_B+aQ_B)=\hat{e}(h(b+S_B)Q_A,(S_A+a)Q_B)=e(Q_A,Q_B)^{h(S_A+a)(S_B+b)}=\hat{e}(h(S_A+a)Q_B,(b+S_B)Q_A)=K_{BA}$

协议的正确性很显然是成立的。

3.1.2 安全性分析

下面对文献[13]中 LAW 等人提出的认证密钥协商协议应满足的安全属性进行分析:

(1)隐式密钥认证(Implicit Key Authentication,IKA):在密钥协商协议中,协议参与方 A 确定除了意定通信方 B 外,没有别的任何一方能够计算出相同的会话密钥,参与者 B 无需采取任何行动。

在上述协议中,参与方计算的最终会话密钥都利用了自己私钥参与计算,所以用户不需要单独向通信方证明自己的身份,因此该协议提供了隐式密钥认证。

(2)已知密钥安全(Known-Key Secrecy,K-KS):两个协议参与者一次会话密钥的泄露不会导致其他会话密钥的泄露,也就是攻击者无法根据获得的会话密钥求出其他会话密钥,则称该协议满足已知密钥安全性。

由于最终产生的共享的会话秘密不仅与当前会话中的临时私钥 a,b 有关,而且与 KGC 的主私钥有关,因此当两个协议参与者之间共享的某个会话密钥泄露之后,攻击者无法根据已获得的会话密钥求出其它会话密钥。

(3)前向安全性(Forward Secrecy,FS):如果协议参与者一方长期私钥泄露了,攻击者不能求出旧的会话密钥,则称协议提供了部分前向保密性。如果所有参与方长期私钥泄露,也不会导致旧的会话密钥泄露,则称该协议提供了完美前向安全。

协议中,a,b 由通信双方随机产生,攻击者无法根据破解当前的会话密钥来获取以往的会话密钥。

(4)密钥泄露伪装安全(Key-Compromise Impersonation,K-CI):假设两个协议参与者 A 和 B,如果 A 的长期私钥泄露,那么攻击者可以冒充 A 和别的实体进行密钥协商。然而,我们希望用户 A 私钥泄露不能够使攻击者反过来冒充其他用户与 A 进行密钥协商。密钥泄露伪装攻击指攻击者在得到用户 A 私钥后可以假冒其他用户和 A 进行密钥协商。

假设用户 A 的私钥泄露,攻击者只能冒充用户 A 的身份,协议中利用了主私钥和临时私钥计算会话密

钥,攻击者不能在仅知道 A 的私钥来冒充别的用户和 A 通信,因此,协议提供了密钥泄露伪装安全。

(5)未知密钥共享(Unknown Key-Share,UK-S):未知密钥共享指协议的参与者 A 不会在不知道对方身份的情况下,与其协商一个会话密钥。也就是说 A 不会在不知情的情况下被迫与攻击者共享了一个会话密钥,而自己认为是和自己意定通信方共享的密钥。

在协议中,参与协议的双方公钥都是利用哈希函数和系统主私钥得到,攻击者不能用别的公钥取代。因此,协议提供了未知密钥共享安全性。

(6)密钥控制安全(Key Control,KC):密钥的建立都是由协议所有参与者共同提供信息协商得到,任何参与方或攻击者都不能决定会话密钥或是把密钥的值设定成其预先选定的值。

在协议的执行过程中,不仅用到了参与方的长期私钥和临时公钥,而且也用到了强安全哈希函数来共同计算会话密钥。因此该协议提供了密钥控制安全性。

3.2 协议比较

下面将新协议与现有的几个经典的身份基(基于身份的)认证密钥协商协议[14~17]进行比较,主要包括协议运算过程中的指数运算和乘法运算次数的比较。

表 2 中包括了协议完成所需要的指数运算和乘法运算次数以及点加法运算的比较。从表中可以看出,新协议与 Scott 协议、Chen-Kudla 协议具有完全一样的计算效率。但是通过对协议安全属性比较得知,新协议达到了所有安全属性,而表中其他协议却具有不同的安全缺陷。

表 2 协议计算效率比较

	Smart 协议	Scott 协议	Chen-Kudla 协议	McCullagh-Barreto 协议	新协议
配对运算	2	1	1	0	1
群 G1 上表量点乘运算	2	2	2	1	2
群 G2 上指数运算	0	2	2	1	2
群 G1 上点加法运算	1	1	1	1	1

新协议满足已知所有的安全属性,与经典的身份基认证密钥协商协议在安全属性方面的比较如表 3 所示。

4 结束语

文中提出了一个身份基认证密钥协商协议,经分析表明可以满足等献性、公平性、保密性等基本特性,这也是未来电子商务发展的重要安全保障,具有实际的应用价值。新协议不仅保持了较高的通信和计算效率,还满足现有的所有已知安全属性,通过比较表明新协议在总体性能和安全性上优于现有经典的主要协议,具有较强的实用性,更加适合实际通信运用。

表 3 安全属性比较

安全属性	Smart 协议	Scott 协议	Chen-Kudla 协议	McCullagh-Barreto 协议	新协议
已知密钥安全	满足	满足	满足	满足	满足
前向安全	不满足	满足	不满足	满足	满足
密钥泄露伪装安全	满足	不满足	满足	不满足	满足
未知密钥共享安全	满足	满足	满足	满足	满足
密钥控制安全	满足	满足	满足	满足	满足

参考文献:

[1] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Trans. Inf. Theory, 1976, 22(6): 644-654.

[2] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology: CRYPTO84. Berlin: Springer-Verlag, 1984: 47-53.

[3] Boneh D, Franklin N M. Identity-based encryption from the weil pairing[C]//Advances in Cryptology: CRYPTO 2001. Berlin: Springer, 2001: 213-229.

[4] Wang X, Dong Q, Zhou Y, et al. Improvement of McCullagh-Barreto Key Agreement with KCI-security[J]. The Journal of China Universities of Posts and Telecommunications, 2009 (2): 68-71.

[5] Wang S, Cao Z, Choo R, et al. An Improved Identity-based Key Agreement Protocol and Its Security Proof[J]. Information Sciences, 2009(3): 307-308.

[6] Wang S, Cao Z, Chent Z, et al. Perfect Forward Secure Identity-based Authenticated Key Agreement Protocol in the Escrow Mode[J]. Science in CHINA SER F: Information Sciences, 2009(8): 1358-1370.

[7] 王圣宝,曹珍富,董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报, 2007, 30(10): 1842-1852.

[8] 任勇军,王建东,庄 毅. 标准模型下增强的基于身份认证密钥协商协议[J]. 电子与信息学报, 2009(8): 1990-1995.

[9] 冯新泉,黎忠文. P2P 中基于无证书的认证及密钥协商协议[J]. 计算机技术与发展, 2009, 19(2): 165-168.

[10] 王圣宝,鲁磊纪. 一种适用于军事通信的高效认证密钥协商协议[J]. 炮兵学院学报, 2011(1): 59-61.

[11] 丁 辉,殷新春. 一种新的基于身份的认证密钥协商协议[J]. 计算机工程, 2010(12): 127-129.

[12] 郭 华,张 帆,李舟军,等. 对一个基于身份的密钥协商协议的分析与改进[J]. 计算机科学, 2010(10): 78-81.

(下转第 204 页)

查准率。横坐标轴代表候选服务数量，纵坐标代表查准率。虚线标识综合 SN-QoS 的查准率，实线标识只考虑数值 N-QoS 的查准率。从图 2 中可以得出结论，文中采取的综合 QoS 相似度匹配算法可以更准确的检索出匹配的服务。随着候选服务数量的增加，查准率有所下降。

图 3 比较的是综合 SN-QoS 与数值 N-QoS 匹配的查全率。横坐标轴代表候选服务数量，纵坐标代表查全率。虚线标识综合 SN-QoS 的查全率，实线标识只考虑数值 N-QoS 的查全率。从图 3 中可以得出结论，大致上，文中采取的综合 QoS 相似度匹配算法的查全率却低于只考虑数值的 QoS。这是因为仅仅考虑数值 QoS 的搜索范围更广泛，查全率比较高是合乎情理的。

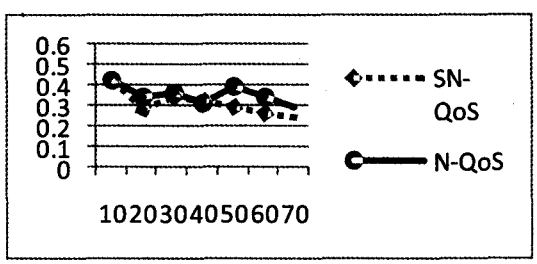

图 3 综合 SN-QoS 与数值 N-QoS 匹配的查全率比较

4 结束语

考虑语义服务质量的 Web 服务发现在信息量急剧膨胀社会中极具探讨价值。文中提出了一个考虑基于 WordNet 的 QoS 语义相似度和支持三种度量方式的 QoS 数值相似度相综合的 QoS 匹配算法。获得更高的查准率。并且考虑领域专家意见，避免用户请求忽略某些 QoS 参数。标准化为多属性决策矩阵，采用传统阈值算法得出符合用户需求的 Top-k 候选服务。构成一个比较完整的 Web 服务 QoS 匹配模型。QoS 参数在实际情况中有很多种形式，文中所采取的区间形式并不能覆盖所有情况，这需要进一步考虑。在实际情况中，用户的个人偏好也是值得提供商探讨考虑的。

参考文献：

[1] Dobson G, Lock R, Sommervile I. QosOnt: an Ontology for QoS in Service-Centric Systems[C]//31st EUROMICRO Conference on Software Engineering and Advanced Applications. Porto, Portugal: [s. n.], 2005.

[2] Zhou C, Chia L T, Lee B S. DAML-QoS Ontology for Web Service[C]//Proceedings of IEEE International Conference on Web Services (ICWS'04). [s. l.]: [s. n.], 2004.

[3] Wang X, Vitvar T, Kerrigan M, et al. A QoS-aware Selection Model for Semantic Web Service[C]//4th International Conference on Service Oriented Computing (ICSOC2006). [s. l.]: [s. n.], 2006: 390-401.

[4] Oldham N, Verma K, Sheth A, et al. Semantic Partner Selection[C]//15th International World Wide Web Conference. Edinburgh, Scotland, UK: [s. n.], 2006.

[5] Yang F C, Su S, Li Z. Hybrid QoS-aware semantic web service composition strategies[J]. Science in China Series F-information Sciences, 2008, 51(11): 1822-1840.

[6] Zeng L Z, Benatallah B, Ngu A H H. QoS-aware middleware for Web services composition[J]. IEEE Transactions on Software Engineering, 2004, 30(5): 311-327.

[7] Ran S. A Model for Web Services Discovery with QoS[J]. ACM Sigecom Exchanges, 2003, 4(1): 1-10.

[8] Al-Masri E, Mahmoud Q H. Discovering the Best Web Service [C]//Proc of the 16th International Conference on World Wide Web. Banff, Alberta, Canada: [s. n.], 2007: 1257-1258.

[9] 蒋哲远，韩江洪，王 钊. 动态的 QoS 感知 Web 服务选择和组合优化模型[J]. 计算机学报，2009，32(5)：1014-1025.

[10] 郭得科，任 彦. 一种 QoS 有保障的 Web 服务分布式发现模型[J]. 软件学报，2006，17(11)：2324-2334.

[11] 张龙昌，邹 华，杨放春. 一种基于多 QoS 注册中心和模型异构的 WEB 服务选择算法[J]. 电子与信息学报，2011，33(1)：168-174.

[12] 王芝虎，葛 声，张力军. 企业级 Java Web 服务的研究与实现[J]. 计算机应用研究，2005，22(1)：128-133.

[13] 王东睿，杨 庚，陈 蕾，等. 基于 WordNet 和 Kernel 方法的 Web 服务发现机制研究[J]. 计算机技术与发展，2010，20(12)：69-76.

[14] 高 洋，黄映辉. 基于三次匹配的语义 Web 服务发现模型[J]. 计算机技术与发展，2009，19(9)：122-124.

(上接第 174 页)

[13] Law L, Menezes A, Qu M, et al. An Efficient Protocol for Authenticated Key Agreement[J]. Designs, Codes and Cryptography, 2003, 28: 119-134.

[14] Smart N P. An Identity-based Authenticated Key Agreement Protocol Based on the Weil Pairing[J]. Electronic Letters, 2002, 38: 630-632.

[15] Scott M. Authenticated ID-based Key Exchange and Remote Log-in with Insecure Token and PIN Number[R/OL]. 2002. http://eprint.iacr.org/2002/164.

[16] Chen L, Kudla C. Identity Based Authenticated Key Agreement Protocols from Pairings[R/OL]. 2002. http://eprint.iacr.org/2002/184.

[17] McCullagh N, Barreto P S L M. A New Two-Party Identity-Based Authenticated Key Agreement[C]//Proceedings of CT-RSA 2005. [s. l.]: Springer-Verlag, 2005: 262-274.