基于双线性对的可认证密钥协商协议*)

陈铁明[1,2] 叶敏克[1] 蔡家楣[1]

(浙江工业大学软件学院 杭州 310032)[1]

(北京航空航天大学软件开发环境国家重点实验室 北京 100083)[2]

摘 要 针对 Smart 等人提出的密钥协商方案存在主密钥托管单点失效安全问题,提出两个新的可认证双线性对密钥协商协议:一个通过向可信第三方获取对方注册的公钥,及实体唯一持有的私钥,实现身份认证和密钥协商;另外直接给出一个无第三方的简单密钥协商方案,先利用椭圆曲线上的数乘实现节点安全认证,再通过双线性对生成会话密钥。最后分析两个协议均满足基本的密钥协商安全属性,并给出协议性能的综合分析。

关键词 密钥协商,椭圆曲线,双线性对,密钥托管,认证

Bilinear Pairings-based Authenticated Key Agreement Protocols

CHEN Tie-ming[1,2] YE Min-ke[1] CAI Jia-mei[1]

(College of Software Engineering, Zhejiang University of Technology, Hangzhou 310032, China)[1]

(State Key Lab of Software Development and Environment, Beihang Univeristy, Beijing 100083, China)[2]

Abstract To solve the single point of failure problem as in the master key escow of Smart's identity-based protocol, two novel authenticated key agreement prototocols using pairings were proposed. One is a trust authority based scheme. It conducts entity authentication and key agreement using entity's registerd open key from the trust party and the entity's private key. Another protocol implements a simple but secure key exchange solution without trust authority. Number multiplicative on points over elliptic curves is at first used to guarantee the node authentication, and the bilinear pairing is then combined to exchange the session key. The two proposed protocols satisfy some basic key agreement security attributions, and the respective implementation performance was analyzed at last.

Keywords Key agreement, Elliptic curve, Bilinear pairings, Key escow, Authentication

1 引言

网络通信双方协商密钥的目的在于建立安全通道,即利用协商的会话密钥加密通信数据以防止第三方截获、伪造或篡改。密钥协商的基本方法主要有两类:一类是通信双方的某一个实体单方面产生一个密钥,将密钥安全地发送给对方完成密钥共享;另一种方法是通信双方各自产生私钥和公钥,通过公钥信息交互完成共享密钥的协商。双方实体共同协商密钥具有更好的公平性和安全性[1]。

采用公钥算法的最早密钥协商协议由 Diffie 和 Hellman 提出[2],最初基于简单离散对数难题,随后出现多种扩展方案,形成一系列 Diffe-Hellman 问题[3,4]。同时,Shamir 等人提出的基于身份的加密模型[5],给基于 ID 的高效密钥协商协议提供了现实可行性;2001 年 Boneh 和 Franklin 提出椭圆曲线上的双线性对,实现完整的身份加密系统 IBE[6],因此基于 ID 的双线性对密钥协商协议成为当前的一个研究热点。较有代表性的有 Smart 协议[7]、Chen-Kulda 协议[3]、Yuan-Li 协议[8]、Ryu-Yoon-Yoo 协议[9]、Wang 协议[10]等,另有学者提出基于 ID 的三方协商方案[11,12]等。限于篇幅,不再赘述,Colin Boyd 等人关于密钥协商的专著[13]较系统地介绍了可认证密钥协议的研究现状。

本文将提出新的可认证双线性对密钥协商方案。第二节首先介绍密钥协商的基本安全属性,给出双线性对的数学基础,并简要描述 Smart 密钥协商方案;第三节分别提出可信第三方和无第三方环境下的两个可认证密钥协商协议;最后分析两个协议满足密钥协商的安全需求,并给出协议性能分析及相关结论。

2 背景知识

2.1 协议安全属性

Menenes 等人总结了一个好的安全密钥协商协议应满足以下基本的安全属性[1]:

密钥协商安全(Known-key Security):协议运行时,每次协商的会话密钥具有唯一性,即每次协商密钥的参数随机。

密钥前向安全(Forward Secrecy):攻击者即使破解协议当前协商的密钥,也不能获得通信双方之前协商的共享密钥。

私钥泄漏安全(Key Compromise Impersonation Secrecy):假设攻击者获得通信实体 A 的私钥,可伪造 A 的角色与其它实体通信,但不能扮演其它实体和 A 合法通信。

密钥共享安全(Unknown Key-Share Secrecy):通信实体 A 在没有获取实体 B 的信息前,不能强迫 B 与其共享密钥。

密钥控制安全(No Key Control):会话密钥的协商需要通信双方的共同参与,任何单方不能通过参数的预先设置等方法确定密钥。

*)本文获国家自然科学基金(60673080,60773115),国家 863 技术专题计划项目(2006AA10Z235),浙江省自然科学基金(Y106290),浙江省科技厅计划项目(2007C21008)等资助。**陈铁明** 讲师,在职博士,研究方向为安全协议、信息安全;**叶敏克** 硕士研究生,研究方向为网络信息安全;**蔡家楣** 教授,研究领域为信息安全、软件工程。

密钥托管安全(Key Escrow Security):针对可信第三方密钥托管的密码体制,会话密钥除通信双方尚有第三方实体知道,如 PKI 的 CA 中心或 IBE 系统的 PKG 服务器等;但在某些场景中,通信双方不希望有任何其它实体掌握协商的会话密钥,或推导出会话密钥。

当存在可信第三方时,密钥托管安全等效于完美前向安全(Perfect Forward Secrecy),即攻击者攻破可信第三方的私钥,也无法获得协商的密钥[3]。

2.2 双线性对

令 G_1 为椭圆曲线上的加法群,G_2 为有限域上的乘法群,均为 q 阶循环群(q 为素数)。双线性对是定义在 G_1,G_2 上的双线性映射 $\hat{e}:G_1\times G_1\to G_2$,一个可接受的双线性对应满足以下三条性质:

(1)双线性:$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$,$P,Q\in G_1$,$a,b\in Z_q^*$;

(2)非退化性:若 P 是 G_1 的生成元,则 $\hat{e}(P,P)$ 是 G_2 的生成元;存在 $P\in G_1$,满足 $\hat{e}(P,P)\neq 1$;

(3)可计算性:存在有效的算法,对任一 $P,Q\in G_1$,计算 $\hat{e}(P,Q)$ 可在多项式时间内完成。

2.3 Smart 方案

Smart 等人于 2002 年提出第一个基于 ID 的密钥协商协议[7],具体过程如下:

初始化:PKG 选择 q 阶循环群 G_1,G_2,构建双线性映射 $\hat{e}:G_1\times G_1\to G_2$,哈希函数 $H_1:\{0,1\}^*\to G_1$,G_1 的生成元 P。选择 $s\in Z_q^*$,计算 $P_{pub}=s*P$,公开系统参数 $\langle G_1,G_2,\hat{e},P,P_{pub},H_1,H\rangle$,其中 s 为主密钥,H 为密钥生成函数。

私钥析取:已知通信实体的 ID,计算公钥 $Q_{ID}=H_1(ID)$,私钥 $S_{ID}=sQ_{ID}$

密钥协商过程如下:

(1)A 随机选择 $a\in Z_q^*$,计算 $T_A=aQ_A$,将 T_A,Q_A 发送给 B;

(2)B 随机选择 $b\in Z_q^*$,计算 $T_B=bQ_B$,将 T_B,Q_B 发送给 A;

(3)A 计算 $K_{AB}=\hat{e}(S_A,T_B+Q_B)$,$B$ 计算 $K_{BA}=\hat{e}(S_B,T_A+Q_A)$。

Smart 协议假设通信双方 A 和 B 在 PKG 初始化环境下可安全完成私钥析取。显然,

$K_{AB}=K_{BA}=\hat{e}(Q_A,Q_B)^{s(a+b)}$

通过密钥生成函数 H 即可得到最终的共享会话密钥。

3 新的密钥协商协议

文献[7]给出了 Smart 协议满足密钥协商安全属性(1)-(5)的论断。由于 PKG 拥有主密钥 s,可获得任意通信实体的私钥,从而计算得到通信双方的共享密钥,无法满足密钥的完美前向安全性。鉴于密钥托管安全的考虑,我们将针对是否存在可信第三方的网络环境,提出两个新的隐含认证安全密钥协商协议。

3.1 可信第三方认证协议

初始化:PKG 选择 q 阶循环群 G_1,G_2,构建双线性映射 $\hat{e}:G_1\times G_1\to G_2$,哈希函数 $H_1:\{0,1\}^*\to G_1$,公开系统参数 $\langle G_1,G_2,\hat{e},H_1,H\rangle$,其中 H 为密钥生成函数。

公钥注册:已知通信实体的 ID,选择私钥 $s_{ID}\in Z_q^*$,计算 $Q_{ID}=H_1(ID)$,向 PKG 注册公钥 $K_{ID}=s_{ID}^{-1}Q_{ID}$。

密钥协商过程如下:

(1)A 随机选择 $a\in Z_q^*$,计算 $T_A=aK_B$,将 T_A,Q_A 发送给 B;

(2)B 随机选择 $b\in Z_q^*$,计算 $T_B=bK_A$,将 T_B,Q_B 发送给 A;

(3)A 计算 $S_A=s_AT_B$,$K_{AB}=\hat{e}(S_A,aQ_B)$;B 计算 $S_B=s_BT_A$,$K_{BA}=\hat{e}(S_B,bQ_A)$。

经验证 $K_{AB}=\hat{e}(s_Abs_A^{-1}Q_A,aQ_B)=\hat{e}(bQ_A,aQ_B)=\hat{e}(Q_A,Q_B)^{ab}$,

$K_{BA}=\hat{e}(s_Bas_B^{-1}Q_B,bQ_A)=\hat{e}(aQ_B,bQ_A)=\hat{e}(Q_A,Q_B)^{ab}$。

3.2 无第三方认证协议

上述方案中,实体需向 PKG 注册公钥,增加了系统开销。当系统不存在可信第三方认证服务时,提出简单的隐含认证密钥协商协议如下(初始化假设同上):

(1)A 随机选择 $a\in Z_q^*$,计算 $T_A=aQ_A$,将 T_A,Q_A 发送给 B;

(2)B 随机选择 $b\in Z_q^*$,计算 $T_B=bQ_B$,将 T_B,Q_B 发送给 A;

(3)A 计算 $a*b*Q_B$,发送给 B,B 计算 $b*a*Q_A$,发送给 A;

(4)A 利用 a^{-1} 计算 bQ_A,发送给 B,B 利用 b^{-1} 计算 aQ_B,发送给 A;

(5)A 计算 $K_{AB}=\hat{e}(aQ_B+T_B,Q_A)$;$B$ 计算 $K_{BA}=\hat{e}(bQ_A+T_A,Q_B)$。

共享密钥验证:

$K_{AB}=\hat{e}(aQ_B+T_B,Q_A)=\hat{e}(aQ_B+bQ_B,Q_A)=\hat{e}(Q_B,Q_A)^{a+b}=\hat{e}(Q_B,aQ_A+bQ_A)=K_{BA}$

显然,协议步骤(4)可实现通信双方的安全认证,即通过验证对方随机产生的私密值 a,b 确认对方身份,这里假设实体的 ID 信息 Q_A 和 Q_B 是安全可控的。

4 安全与性能分析

为了便于描述,我们记可信第三方协议为协议 1,无第三方协议为协议 2。先分析两个协议满足密钥协商的基本安全属性。

密钥协商安全:两个协议在密钥协商计算时,都包含了随机参数 a,b,会话密钥具有唯一性。

密钥前向安全:a,b 由通信双方随机产生,攻击者即使破解当前协商的密钥,也无法获取之前的协商密钥。另外,协议 1 中 PKG 的私钥仅用来签发通信实体的公钥,即使 PKG 私钥被攻破,也无法破解会话密钥,因此协议 1 具备完美前向安全性。

私钥泄漏安全:假设协议 1 中实体 A 的私钥 S_A 泄漏,攻击者在能破解 K_A 的情况下,想伪造 B 与 A 协商密钥,也必须获得 B 的私钥 S_A,否则无法获得 A 的信任;协议 2 不涉及实体私钥,实体身份可通过点的安全映射控制。

密钥共享安全:假设实体 A 向 B 发起密钥协商请求,则协议 1 需通过 PKG 获得 B 的公钥 K_B,协议 2 需请求 B 的 ID 点映射 Q_B,在获得 K_B,Q_B 之前,A 无法伪造其它实体与 B 协商密钥。

密钥控制安全:实体 A 无法控制实体 B 产生的随机数 b,且计算 b 属于 CDH 问题,同理实体 B 也无法控制密钥参数 a,因此两个协议均能抵抗密钥控制攻击。

密钥托管安全:协议 1 尽管需要 PKG 支持,但通信实体的私钥由自己产生和保管,可抵制 Smart 方案存在的密钥托管单点失效问题;协议 2 不存在密钥托管问题。

下面再给出协议的性能分析。用 M 和 A 分别代表椭圆曲线上的一次乘法和加法操作,P 表示双线性对的一次映射操作;设 G_1 群上的一个点需 L 位二进制表示。我们给出

Smart 协议及本文两个协议的通信性能和计算复杂度见表 1。可信第三方协议通信占用的带宽与 Smart 方案相同，协议执行时比 Smart 方案多 4 次椭圆曲线上的标量乘法运算，但无需点的加法运算，整体性能与 Smart 相差无几；无第三方协议占用的带宽和点乘运算比 Smart 协议多，但协议运行无需第三方密钥分发和托管开销。

表 1　新的协议与 Smart 协议的性能分析

	通信量(二进制位)	计算量(操作数)
Smart 协议	4L	2M+2A+2P
协议 1	4L	6M+2P
协议 2	6L	6M+2A+2P

结束语　本文在分析密钥协商协议的安全属性和 Smart 方案的基础上，提出了两个新的协议：一个基于可信第三方实现公钥分发，通信双方利用私钥完成身份认证与密钥协商；另一个无需第三方支持，结合 CDH 和 BDH 问题给出简洁有效的安全协商模型。两个协议都隐含认证，且在实体身份点映射安全可控的应用环境中，可抵抗中间人攻击。

随着 IBE 公钥体制的发展，基于 ID 的双线性配对密钥协商协议研究越来越受关注。下一步的研究将继续关注对开放网络环境下各类新攻击的抵抗问题，并展开双线性对协议的性能优化研究。

参 考 文 献

[1] Wilson S B, Johnson D, Menenes A. Key Agreement Protocols and their Security Analysis// The 6th IMA International Conference on Cryptography and Coding. LNCS Vol. 1355. Springer-Verlage, 1997: 30-45

[2] Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22: 644-654

[3] LiC K, Chen qun. Identity Based Authenticated Key Agreement Protocols from Pairings. Hewlett-Packard Laboratories, Bristol, 2002

[4] 冯姚刚. 基于 Weil 对的成对密钥协商协议. 软件学报, 2006, 17

[5] Shamir A. Identity based cryptosystems and signature schemes// Lecture Notes in Computer Science. 1984, 196: 47-53

[6] Dan Boneh M F. Identity-Based Encryption from the Weil Pairing// The Proceedings of Crypto. Springer-Verlag, 2001, 2139: 213-229

[7] Smart N P. An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002, 38: 630-632

[8] Li S, Yuan Q. A New Efficient ID-Based Authenticated Key Agreement Protocol. School of Mathematical Sciences. Peking University, Beijing: 2005

[9] Ryu E, Yoon E, Yoo K. An Efficient ID-Based Authenticated Key Agreement Protocol// Networking 2004. 2004, 3042

[10] Wang Y. IEEE 1363.3 Submission: Implicitly Authenticated ID-Based Key Agreement Protocol. UNC Charlotte

[11] Divya Nalla K C R. ID-based tripartite Authenticated Key Agreement Protocols from pairings. Dept of Computer/Info. Sciences. University of Hyderabad, Hyderabad

[12] Chien H Y. Improved ID-based Tripartite Multiple Key Agreement Protocol from Pairings. Department of Information Management, ChaoYang University of Technology, 2004

[13] Colin B, Anish M. Protocols for Authentication and Key Establishment. ISBN 3-540-43107-1. Berlin, Springer-Verlag, New York, Heidelberg, 2003

(上接第 22 页)

ceedings of IEEE Global Telecommunications Conference (Globecom) 2004. Dallas, TX, USA, Nov. 2004

[23] Gruteser M, Grunwald D. A methodological assessment of location privacy risks in wireless hotspot networks// First International Conference on Security in Pervasive Computing. 2003

[24] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security Protocols for Sensor Networks// Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking. ACM Press, 2001: 189-199

[25] Deng J, Han R, Mishra S. Countermeasures against traffic analysis attacks in wireless sensor networks// Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). Washington, DC, USA: IEEE Computer Society, 2005: 113-126

[26] Misra S, Xue G. Efficient anonymity schemes for clustered wireless sensor networks. International Journal of Sensor Networks, 2006, 1(1/2): 50-63

[27] Ouyang Y, Le Z, Xu Y, et al. Providing anonymity in wireless sensor networks// 10th International Conference on Parallel and Distributed Systems (ICPADS 2004)

[28] Wadaa A, Olariu S, Wilson L, et al. On providing anonymity in wireless sensor networks// 10th International Conference on Parallel and Distributed Systems (ICPADS 2004). Newport Beach, CA, USA, 2004: 411-418

[29] Molnar D, Wagner D. Privacy and security in library rfid: Issues, practices, and architectures// ACM CCS. 2004

[30] Shao M, Zhu S, Zhang W, et al. pDCS: Security and Privacy Support for Data-Centric Sensor Networks// IEEE INFOCOM 2007

[31] Girao J, Westhoff D, Schneider M. CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks// 40th International Conference on Communications. IEEE ICC, May 2005

[32] Castelluccia C, Mykletun E, Tsudik G. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks. Mobiquitous, 2005

[33] He W, Liu X, Nguyen H, et al. PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks// 26th Annual IEEE Conference on Computer Communications IEEE INFOCOM 2007. Anchorage, Alaska, May 2007

[34] Wood A D, Stankovic J A. Denial of Service in Sensor Networks [J]. IEEE Computer, 2002, 35 (10): 54-62

[35] Carbunar B, Yu Y, Shi L, et al. Query privacy in wireless sensor networks// Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conferenc. June 2007: 203-212

[36] Deng J, Han R, Mishra S. INSENS: Intrusion-tolerant Routing in Wireless Sensor Network Security[R]. Tech. Rep. CU-CS-939-02. Department of Computer Science, University of Colorado, November 2002

[37] Xi Y, Schwiebert L, Shi W. Preserving privacy in monitoring-based wireless sensor networks// Proceedings of the 2nd International Morkshop on Security in Systems and Networks (SSN'06). IEEE Computer Society, 2006

[38] Ouyang Y, Le X, Chen G, et al. Entrapping adversaries for source protection in sensor networks// World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. International Symposium, June 2006: 10