第 38 卷 第 2 期 计 算 机 工 程 2012 年 1 月
Vol.38 No.2 Computer Engineering January 2012

• 安全技术 • 文章编号：1000—3428(2012)02—0138—03 文献标识码：A 中图分类号：TP309

无对运算的无证书隐式认证及密钥协商协议

杨 路

(江南大学物联网工程学院，江苏 无锡 214122)

摘 要：提出一种不含对运算的无证书隐式认证及密钥协商协议。该协议基于离散对数问题和可计算 Diffie-Hellman 假设，仅需要 3 次指数运算和 2 次散列运算，可避免复杂的双线性对运算。在随机预言机模型下的分析结果表明，该协议具有强安全性，计算开销低于同类型的其他协议。

关键词：无证书；双线性对；离散对数问题；隐式认证；密钥协商

Certificateless Implicit Authentication and Key Agreement Protocol Without Pairing Operation

YANG Lu

(School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China)

【Abstract】Due to the large amount of computing cost in bilinear pairing, this paper proposes a certificateless implicit authentication and key agreement protocol without pairing operation, and proves its security in the random oracle model. The new protocol is based on the discrete logarithm problem and the Computational Diffie-Hellman(CDH) assumption, requires only three times exponentiations and two times hash functions. The computing costs of this protocol lower than costs of the other ones that are the same type with the one in this paper.

【Key words】certificateless; bilinear pairing; discrete logarithm problem; implicit authentication; key agreement

DOI: 10.3969/j.issn.1000-3428.2012.02.044

1 概述

无证书的公钥密码体制由文献[1]提出，被用于解决基于身份公钥密码体制中的密钥托管问题。在随后的几年中，无证书的公钥密码体制得到了国内外研究者的广泛关注，涌现出了众多的研究成果。在这些研究中，多数研究基于双线性对理论，然而，要找到满足双线性要求的子群比较困难，并且双线性对运算开销巨大。因此，基于双线性对理论的密码体制还难以应用于实际。

文献[2]提出无双线性对的无证书密码体制，该方案不使用对运算，降低了无证书公钥加密的计算开销。基于这项研究，文献[3-5]提出了不使用双线性对的认证密钥协商协议，文献[6]提出了不含双线性对运算的无证书签密方案。然而，文献[3]提出的认证协议采用显示认证方式，由于显示认证暴露更多信息给攻击者，其安全性低于隐式认证方案。分析结果表明，该协议不满足会话临时秘密值泄露安全性。此外，文献[4]提出的协议同样不满足会话临时秘密值泄露安全，虽然他们对此进行了改进，但是改进后的方案增加了计算开销；文献[5]提出的协议要求任何一方实体需要至少 7 次指数运算，这显然不能达到降低计算开销的目标。

本文在可计算 Diffie-Hellman(Computational Diffie-Hellman, CDH)假设的基础上，提出一种无对运算的高效无证书隐式认证和密钥协商协议，证明其安全性，并与其他同类型协议[3-5]进行计算性能的比较。

2 背景知识

2.1 CDH 假设

设 p, q 是 2 个大素数，且满足 $q|p-1$，设 g 是群 Z_q^* 的生成元。

定义 1(CDH 假设) 不存在概率多项式时间(Probabilistic Pulynomial-time, PPT)算法 A 解决 CDH 问题，即：

$\forall$ PPT algorithms A, $\forall\varepsilon>0$, $\forall\eta$(η 为足够大的数)

$Advantage^A(\eta)=\Pr[<p, q, g, Z_q^*> \leftarrow G(1^\eta); a, b \leftarrow Z_q^*; g^c \leftarrow A(p, q, g, Z_q^*, g^a, g^b): g^c=g^{ab}] \leqslant 1/\eta^\varepsilon$。

定义中 $Advantage^A(\eta)$是一个可忽略的函数，即 CDH 问题在群 Z_q^* 上是难解的。

2.2 安全模型及安全性定义

本文采用文献[7]中定义的无证书认证密钥协商协议安全模型。该模型中定义了 2 类敌手(记为 $Adv\in\{A_\mathrm{I}, A_\mathrm{II}\}$)：

(1)A_I是一个外部的攻击者，他可以替换任何实体的部分公钥，获得部分实体的私钥，但不能获得 KGC 的主密钥和特定实体的部分私钥。

(2)A_II是一个内部攻击者，他拥有 KGC 的主密钥，可获得任何实体的部分私钥，但不能获得实体的私有秘密以及替换特定实体的公钥。

A_II 敌手模拟一个恶意但受限的 KGC，用于分析无证书协议的无密钥托管特性。

Adv 被允许对预言机进行自适应查询，预言机 $\Pi_{i,j}^s$ 定义为实体 i 与 j 在一次会话中的第 s 个实例。无证书认证密钥协商协议被模拟为挑战者 C 与攻击者 Adv 之间的游戏(Game)，定义如下：

(1)Initialization：挑战者 C 运行系统参数生成算法，输入

作者简介：杨 路(1961－)，男，讲师、硕士，主研方向：信息安全，物联网技术

收稿日期：2011-08-01 **E-mail：**yanglu61@yahoo.cn

安全参数 k，输出系统主密钥(msk)和系统参数 $params$。

1)如果 Adv 是 A_{I} 敌手，那么 C 将 $params$ 发送给 Adv，而对 msk 保密。

2)如果 Adv 是 A_{II} 敌手，那么 C 将(msk, $params$)发送给 Adv。

(2)Phase-I：Adv 可以适应性地进行以下查询[7]：Create(ID)，Public-Key(ID)，Partial-Private-Key(ID)，Corrupt(ID)，Public-Key-Replacement(ID, P^*)，Send($\Pi_{i,j}^s$,M)和 Reveal($\Pi_{i,j}^s$)。C 模拟密钥协商方案中的相应算法分别做出回答。

(3)Phase-II：Adv 选择一个 $fresh$-$oracle$ $\Pi_{i,j}^s$ 请求 Test 查询。

Test 查询结束后，除不再请求 $Reveal$ ($\Pi_{i,j}^s$) 查询(或者与 $\Pi_{i,j}^s$ 匹配的 $Reveal$($\Pi_{j,i}^u$)查询)和 $Corrupt$(ID_j)查询外，Adv 仍然可以任意地请求在 Phase-I 中定义的其他查询。最后，Adv 输出对 Test 查询中 b 的猜测 b'，如果 $b'=b$，那么 Adv 赢得 Game。Adv 赢得 Game 的优势定义为：

$$Advantage^{Adv}(k)=|\Pr[b'=b]-1/2|$$

无证书两方认证密钥协商协议安全性定义如下：

定义 2 如果无证书两方认证密钥协商协议满足如下要求，则被认为是安全的：

(1)在 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^u$ 之间存在良性攻击者 Adv(能如实地传递消息称为良性攻击者)的情况下，$\Pi_{i,j}^s$ 与 $\Pi_{j,i}^u$ 总能协商相同的会话密钥 SK，且 SK 在 $\{0,1\}^k$ 上均匀分布。

(2)对于任何攻击者 $Adv\in\{A_{\mathrm{I}}, A_{\mathrm{II}}\}$，$Advantage^{Adv}(k)$ 是可忽略的。

3 无证书密钥协商协议设计

新协议分为系统建立、密钥生成以及会话密钥协商 3 个阶段，包括 6 个算法：Setup，Set-Partial-Key，Set-Secret-Value，Set-Private-Key，Set-Public-Key，Key-Agreement。

(1)Setup：输入安全参数 k，输出系统参数 $params=(p,q,g,P_0,H_1,H_2,k)$。其中，$p$ 和 q 是 2 个大素数，且满足 $q|p-1$；g 是群 Z_q^* 的生成元；$P_0=g^s$ 为 KGC 的公钥，对应的主密钥(msk)为随机选择的 $s\in Z_q^*$；$H_1:\{0,1\}^*\times Z_q^*\to Z_q^*$ 和 $H_2:\{0,1\}^{*2}\times Z_q^*\times Z_q^*\times Z_q^*\to\{0,1\}^k$ 是安全的单向散列函数。

(2)Set-Partial-Key：输入 $(params,s,ID_i)$，KGC 随机选择 $y_i\in Z_q^*$，计算 $Y_i=g^{y_i}$ 和 $d_i=y_i+sQ_i$，其中，$Q_i=H_1(ID_i,Y_i)$，$ID_i\in\{0,1\}^*$ 是实体 i 的身份标识；d_i 输出为 i 的部分私钥；Y_i 输出为 i 的部分公钥。

(3)Set-Secret-Value：输入 $(params,ID_i)$，输出 $x_i\in_R Z_q^*$ 作为实体 i 的长期私有秘密值。

(4)Set-Private-Key：输入 $(params,ID_i,d_i,x_i)$，输出 $S_i=(x_i,d_i)$ 作为 i 的全部长期认证私钥。

(5)Set-Public-Key：输入$(params,ID_i,Y_i,x_i)$，输出$P_i=(X_i,Y_i)$作为 i 的全部公钥，其中，$X_i=g^{x_i}$。

(6)Key-Agreement：假设 Alice 拥有其公私密钥对 (S_A,P_A)，并期望同拥有密钥对 (S_B,P_B) 的 Bob 协商安全的会话密钥，那么 A 与 B 按以下步骤进行密钥协商：

1)A 随机选择 $r_A\in Z_q^*$ 计算 $R_A=g^{r_A}$，并发送 (ID_A,P_A,R_A) 给 B。

2)当 B 收到来自 A 的消息(ID_A,P_A,R_A)时，随机选择 $r_B\in Z_q^*$ 计算 $R_B=g^{r_B}$，并发送 (ID_B,P_B,R_B) 给 A，计算 $k_B=(R_AX_AY_AP_0^{Q_A})^{r_B+x_B+d_B}$ 和会话密钥 $SK_{BA}=H_2(ID_A,ID_B,R_A,R_B,k_B)$。

3)当 A 收到来自 B 的消息 (ID_B,P_B,R_B) 时，计算 $k_A=(R_BX_BY_BP_0^{Q_B})^{r_A+x_A+d_A}$ 和会话密钥 $SK_{AB}=H_2(ID_A,ID_B,R_A,R_B,k_A)$。

协议每一次运行的会话 ID 是 (ID_A,ID_B,R_A,R_B)。

本文的密钥协商是一次典型的 Diffie-Hellman 密钥交换过程，但由于本文方案实现了实体身份的隐式认证，因此避免了 Diffie-Hellman 方案可能遭受的中间人攻击。

4 协议分析

4.1 有效性分析

协议的正确性和有效性通过下式证明。

$$\begin{aligned}k_A&=(R_BX_BY_BP_0^{Q_B})^{r_A+x_A+d_A}=\\&R_B^{r_A}\cdot(X_BY_BP_0^{Q_B})^{r_A}\cdot R_B^{x_A+d_A}\cdot(X_BY_BP_0^{Q_B})^{x_A+d_A}=\\&g^{r_Br_A}\cdot(g^{x_B+y_B+sQ_B})^{r_A}\cdot(g^{r_B})^{x_A+y_A+sQ_A}\cdot(g^{x_B+y_B+sQ_B})^{x_A+y_A+sQ_A}=\\&R_A^{r_B}\cdot(g^{r_A})^{x_B+d_B}\cdot(g^{x_A+y_A+sQ_A})^{r_B}\cdot(g^{x_A+y_A+sQ_A})^{x_B+d_B}=\\&(R_AX_AY_AP_0^{Q_A})^{r_B+x_B+d_B}=k_B\end{aligned}$$

由此可得，SK_{AB}=SK_{BA}，得到相同的会话密钥。

4.2 安全性分析

定理 在 CDH 假设下，本文的无证书两方认证密钥协商协议是安全的。

证明：由于文章篇幅有限，本文仅采用启发式分析方法，在随机预言机模型(见 2.2 节)下分析新协议满足定义 2 中的安全性需求。

(1)从上文分析可见，在存在良性攻击者的情况下，$\Pi_{i,j}^s$ 与 $\Pi_{j,i}^u$ 总能协商相同的会话密钥 SK。另外，会话密钥可看作 H_2 函数的随机输出，因此，可认为 SK 在 $\{0,1\}^k$ 上均匀分布。

(2)对于任意攻击者 $Adv\in\{A_{\mathrm{I}}, A_{\mathrm{II}}\}$，本文给定一个 CDH 问题实例(即给定$(g^a, g^b)$求解 g^{ab})：

对于 A_{I} 敌手，他可以替换任何实体的部分公钥(X_i)，获得部分实体的私钥，但不能获得 KGC 的主密钥(s)和特定实体的部分私钥(d_A 或 d_B)。假设 A_{I}敌手模拟了参与者 Bob，那么他将面临计算：

$$k_B=R_A^{d_B}\cdot R_A^{r_B+x_B}\cdot(X_AY_AP_0^{Q_A})^{r_B+x_B+d_B}=g^{r_Ad_B}\cdot D$$

令 d_B=a, r_A=b, $D=R_A^{r_B+x_B}\cdot(X_AY_AP_0^{Q_A})^{r_B+x_B+d_B}$，这里存在求解 CDH 问题 $g^{r_Ad_B}$(对 A_{I}来说，d_B和 r_A 都是未知的)。反之，如果 A_{I}敌手模拟了参与者 Alice，那么存在求解 CDH 问题 $g^{r_Bd_A}$。根据 CDH 假设，A_{I}敌手求解 CDH 问题的可能性是可忽略的，因此，本文协议在 A_{I}敌手模型下实现了定义 2 中的安全性需求。

对于 A_{II} 敌手，他拥有 KGC 的主密钥(s)，可获得任何实体的部分私钥(d_i)，但不能获得实体的私有秘密(x_i)，且不能替换特定实体的公钥(X_i)。假设 A_{II} 敌手模拟了参与者 Bob，那么他将面临计算：

$$k_B=R_A^{x_B}\cdot R_A^{r_B+d_B}\cdot(X_AY_AP_0^{Q_A})^{r_B+x_B+d_B}=g^{r_Ax_B}\cdot D$$

令 x_B=a, r_A=b, $D=R_A^{r_B+d_B}\cdot(X_AY_AP_0^{Q_A})^{r_B+x_B+d_B}$，这里存在求解 CDH 问题 $g^{r_Ax_B}$。反之，如果 A_{II} 敌手模拟了参与者 Alice，那么存在求解 CDH 问题 $g^{r_Bx_A}$。根据 CDH 假设，A_{II} 敌手求解 CDH 问题的可能性是可忽略的，因此，本文协议在 A_{II} 敌手模型下实现了定义 2 中的安全性需求。

可见，在 CDH 假设成立的情况下，本文协议满足定义 2 中的安全性需求。同文献[7]，本文协议实现了已知会话密钥安全、完美前向安全性、无密钥托管特性、抗密钥泄露伪装、

无密钥控制与密钥完整性、抗未知密钥共享和临时秘密泄露安全性。证毕。

4.3 性能分析与比较

表 1 从计算开销方面比较了本文协议与同类型的其他 3 种协议[3-5]的性能，主要列举了指数运算、散列运算和对称加解密等 3 种主要计算开销，其中，尤以指数运算开销最大。表中数据格式 A/B 分别代表 Alice 与 Bob 的计算次数。

表 1 协议计算开销比较

协议	指数运算次数	散列运算次数	对称加/解密次数
文献[3]协议	4/5	4/4	1/1
文献[4]协议	5/5	2/2	0/0
文献[5]协议	7/7	2/2	0/0
本文协议	3/3	2/2	0/0

此外，4 种协议都需要 2 次通信，位长也基本相当。可见，本文协议的计算性能明显优于其他 3 种协议，真正达到了降低计算开销的目的。文献[3]协议虽然声称其任何一方的指数运算次数仅为 3 次，但由分析可见，该协议未算上计算会话密钥所需要的开销，同时，Bob 在验证解签密时至少还需要增加一次指数运算，因此，实际的指数运算次数分别为 4/5 次。另外，文献[3-4]协议还存在会话临时秘密值泄露安全缺陷，如果改进其缺陷，计算成本还将增加。

5 结束语

本文提出一种无对运算的无证书隐式认证和密钥协商协议。基于离散对数问题和 CDH 假设，新协议实现了两方实体的隐式认证和密钥协商，避免了开销巨大的双线性对运算。在随机预言机模型下，采用启发式分析方式，证明了新协议的有效性和安全性。对比分析表明，新协议具有较低的计算开销和通信开销，真正达到了提高计算性能的目的，能适用于计算能力受限的移动终端通信。本文协议在随机预言机模型下是可证明安全的，标准模型下可证安全的无证书密钥协商是一个开放性问题，这将是下一步的研究方向。

参考文献

[1] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of ASIACRYPT'03. Berlin, Germany: Springer-Verlag, 2003: 452-473.

[2] Baek J, Safavi-Naini R, Susilo W. Certificateless Public Key Encryption Without Pairing[C]//Proc. of the 8th International Conference on Information Security. Singapore: Springer-Verlag, 2005: 134-148.

[3] 朱 辉, 李 晖, 谭示崇, 等. 不使用双线性对的无证书认证协议[J]. 武汉大学学报: 信息科学版, 2010, 35(5): 574-577.

[4] Hou Mengbo, Xu Qiuliang, Jiang Han. A Two-party Certificateless Authenticated Key Agreement Protocol Without Pairing[C]//Proc. of the 4th International Conference on Computer Science and Information Technology. [S. l.]: IEEE Computer Society, 2009: 412-416.

[5] Geng Manman, Zhang Futai. Provably Secure Certificateless Two-party Authenticated Key Agreement Protocol Without Pairing[C]//Proc. of CIS'09. Xi'an, China: IEEE Computer Society, 2009: 208-212.

[6] 葛爱军, 陈少真. 不含双线性对运算的无证书签密方案[J]. 计算机工程, 2010, 36(20): 147-149.

[7] Zhang Lei, Zhang Futai, Wu Qianhong, et al. Simulatable Certificateless Two-party Authenticated Key Agreement Protocol[J]. Information Sciences, 2010, 180(2): 1020-1030.

编辑 金胡考

(上接第 137 页)

4 结束语

本文将专家系统应用到个人电脑的防火墙中，从网络层和应用层 2 个层面通过对数据包的包头信息和应用程序的运行行为信息进行推理判断，使用户几乎不需要具有信息安全的知识(只需要用户确认是否是自己需要的程序)，就能实现防火墙过滤规则的动态更新，从而时刻保障用户的安全。实验结果表明，本文方案可以检测出大部分的网络数据包攻击和木马类软件的攻击，实现防火墙过滤规则的动态生成。但是，本文系统还不能防御分布式拒绝服务攻击和处于不活动状态类的木马攻击。对于来自不同源地址的 SYN 数据包攻击，只能向用户提出警告，不能形成具体的过滤规则，这也是下一步工作需要解决的问题。

参考文献

[1] 赵一铂, 邹恒明. 基于个人防火墙的自适应优化策略[J]. 计算机工程, 2009, 35(10): 109-111.

[2] Rash M. Linux 防火墙[M]. 陈 健, 译. 北京: 人民邮电出版社, 2009.

[3] Zhao Yuehua, Hu Bai, Zhou Conghua. Formal Description and Verification of Security Filtered Rules[C]//Proc. of the 1st International Conference on Networking and Distributed Computing. Hangzhou, China: IEEE Computer Society, 2010.

[4] 李卓群. 智能防火墙核心模块的研究与实现[D]. 南京: 南京理工大学, 2008.

[5] Chiong R, Dhakal S. On the Insecurity of Personal Firewall[J]. Information Technology, 2008, (8): 1-10.

[6] 周瑞丽, 潘剑锋, 谭小彬, 等. 应用专家系统开发 Windows 恶意代码检测系统的研究[J]. 信息安全与通信保密, 2009, (9): 77-79, 82.

[7] Russinovich M E, Solomon D A. Microsoft Windows Internals, Fourth Edition: Microsoft Windows Server 2003, Windows XP, and Windows 2000[M]. Redmond, USA: Microsoft Press, 2004.

[8] 朱雁辉, 朱雁冰. Windows 防火墙与网络封包截获技术[M]. 北京: 电子工业出版社, 2002.

[9] 国内最流行十大木马查杀[EB/OL]. (2006-06-25). http://www.yesky.com/SoftChannel/2355578868924416/2001129/207532.

编辑 张 帆