

基于签名的双方密钥协商协议

王天成

(青海师范大学 民族师范学院数学系, 青海 西宁 810008)

摘 要: 双方认证密钥协商是生成会话密钥的重要手段. 对此提出了一种新的基于签名的双方密钥协商协议, 新协议利用传统的签名方案实现参与者之间信息的隐藏, 并通过引入 Hash 函数来加强协议的安全性.

关键词: 密码学; 认证; 密钥协商; 伪造攻击

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2013)06-0019-03

A Two-Party Key Agreement Protocol Based on Signature Scheme

WANG Tian-cheng

(Teachers College of Nationalities, Qinghai Normal University, Xining 810008, China)

Abstract: Two-Party authenticated key agreement is one of methods to generate session key. In this paper, we propose a new Two-Party agreement protocol based on the traditional signature scheme. The new scheme realizes the hiding of the information between the participants. We use Hash function to enhance the security of our protocol.

Key words: cryptography; authentication; key agreement; forgery attack

1 引言

密钥协商协议是密码协议的重要组成部分, 在开放的网络环境下, 可以通过密钥协商来确保会话双方安全通信. 一个有效的密钥协商协议可以帮助利用不安全通信的会话双方协商出一个共同的会话密钥. 而密钥在密码体制中发挥着重要作用, 一旦密钥泄漏, 很多密码系统将被攻破. 因此, 如何建立一个安全的密钥协商协议就成为了研究的焦点.

自从文献[1]中提出公钥密码体制后, 认证密钥协商就得到了蓬勃发展. 1986 年, 文献[2]中提出了三个双方认证密钥协商协议: MTI/A0、MTI/B0 和 MTI/C0. 这些协议能够通过巧妙的消息传递而不需要签名, 为通信双方产生能够抵抗被动攻击者攻击的双向认证的会话密钥. 文献[3-4]中提出了一种高效的可认证密钥协商协议 MQV. 这一协议被文献[1]广泛采纳为密码标准. 但文献[5]中证明这一协议也是不安全的. 为此, 近年来人们在建立安全的密钥协商协议方面做了大量研究[6]等等.

文献[6]中基于 eCK 安全模型提出了一种新的双方认证密钥协商协议(SAKA 协议), 证明了 SAKA 协议可以抵抗未知密钥共享攻击、重放攻击和冒充攻击[7].

本文针对(SAKA 协议)进行了安全性分析, 发现参与者双方的长期私钥如果全部泄漏, 因而是是不安全的; 进而参考文献[8-9]基于签名思想提出一个新的双方认证密钥协商协议, 通过安全性和性能分析可知, 该协议具有较强的实用性.

2 SAKA 协议及安全性分析

2.1 SAKA 协议

在介绍该协议之前, 先定义本节用到的标示.

ID_A, ID_B : 参与者 A 和 B 的身份符号;

F_q : 满足 RSA 安全要求的两个大素数, 其中 $q \mid (p-1)$; 在阶为 q 的循环群 G 中, g 为该群的生成元;

$H_1: \{0, 1\}^* \rightarrow Z_q^*$ 一个随机预言, 用于隐藏参与者的长期私钥和临时私钥;

收稿日期: 2012-08-30; 修回日期: 2012-10-23

基金项目: 国家自然科学基金项目(10571113); 教育部第二类特色专业建设项目(TS2413)

$H: \{0,1\}^* \rightarrow \{0,1\}^\lambda$: Hash 函数, 其中, λ 为安全参数;

SK : A 和 B 为了通过协商得到的会话密钥.

参与者 A 和 B 为了得到协商密钥 T , 将执行如下步骤:

(1) A 随机选取 $a \in Z_q^*$ 作为自己的长期私钥, 计算 $\bar{A} = g^a \bmod p$ 作为其长期公钥, 并公布 $(\bar{A}, ID_A)$; 同理, B 随机选取 $b \in Z_q^*$ 作为自己的长期私钥, 计算 $\bar{B} = g^b \bmod p$ 作为其长期公钥, 并公布 $(\bar{B}, ID_B)$;

(2) A 随机选取 $\chi \in Z_q^*$ 作为自己的临时私钥, 并计算 $x = H_1(a, \chi)$, $K_A = (\bar{B})^x \bmod p$, $s_A = x / (K_A + a) \bmod q$, $R_A = g^{K_A} \bmod p$, 将 (R_A, s_A) 发送给 B ;

(3) 收到 (R_A, s_A) 后, B 计算 $K_A = (R_A \bar{A})^{t_A} \bmod p$ 并验证等式 $R_A = g^{K_A} \bmod p$ 是否成立. 若成立, 则 B 随机选取 $\gamma \in Z_q^*$ 作为自己的临时私钥, 并计算 $y = H_1(b, \gamma)$, $K_B = (\bar{A})^y \bmod p$, $s_B = y / (K_B + b) \bmod q$, $R_B = g^{K_B} \bmod p$. 计算 $K = R_B^{K_A} \bmod p$ 及 $SK = H(K, s_B, s_A, ID_B, ID_A)$, 将 (R_B, s_B) 发送给 A ;

(4) 收到 (R_B, s_B) 后, A 计算

$$K_B = (R_B \bar{B})^{s_B} \bmod p,$$

并验证等式 $R_B = g^{K_B} \bmod p$ 是否成立. 若成立, 计算 $K = R_A^{K_B} \bmod p$ 及

$$SK = H(K, s_B, s_A, ID_B, ID_A).$$

2.2 SAKA 协议安全性分析

在原协议的安全性证明中, 作者指出会话密钥并不完全由参与者双方的长期公私钥协商得到, 而是包含了当前会话的临时私钥, 如果长期私钥泄露前的会话没有被敌手破坏, 即使参与者的长期私钥被敌手获得, 敌手也无法获得这类会话的会话密钥, 因此协议具有弱的完美前向安全性. 但我们的研究发现如果主动攻击者 C 如果拥有了参与者 A 和 B 的长期私钥 a 和 b , 原协议的会话密钥可以被计算出来.

敌手利用公开信道中的 (R_A, s_A) 和 (R_B, s_B) 计算:

$$K_A = (R_A \bar{A})^{t_A} \bmod p, K_B = (R_B \bar{B})^{s_B} \bmod p;$$

利用 $K_A \bmod p$ 和 $K_B \bmod p$ 计算:

$$K' = R_A^{K_B} \bmod p \text{ 和 } K' = R_B^{K_A} \bmod p, \text{ 从而得到}$$

了会话密钥 SK .

所以, SAKA 协议不具有弱的完美前向安全性.

3 新的双方认证密钥协商协议

通过以上分析可知, 由于将 R_A 和 R_B 暴露, 导致敌手可以利用已经获得的长期私钥计算得到会话密钥. 为此, 我们适当调整策略, 利用数字签名思想, 将 s_A 和 s_B 的计算公式进行更改, 并对验证等式进行简单的改造, 即可避免上述问题.

(1) A 随机选取 $a \in Z_q^*$ 作为自己的长期私钥, 计算 $\bar{A} = g^a \bmod p$ 作为其长期公钥, 并公布 $(\bar{A}, ID_A)$; 同理, B 随机选取 $b \in Z_q^*$ 作为自己的长期私钥, 计算 $\bar{B} = g^b \bmod p$ 作为其长期公钥, 并公布 $(\bar{B}, ID_B)$;

(2) A 随机选取两个数 $\chi, r_A \in Z_q^*$, 并计算 $x = H_1(a, \chi)$ 作为自己的临时私钥, 计算 $t_A = g^{r_A} \bmod p$, $X = g^x \bmod p$, 将 X 作为自己的临时公钥. 随后 A 利用 r_A 进行签名: 得到 $s_A = a - (\bar{B})^{r_A+x}$, 将 (t_A, X, s_A) 发送给 B ;

(3) 收到 (t_A, X, s_A) 后, B 验证等式 $\bar{A} = g^{s_A} g^{x_A} \bmod p$ 是否成立. 若成立, B 随机选取两个数 $\gamma, r_B \in Z_q^*$, 并计算 $y = H_1(b, \gamma)$ 作为自己的临时私钥, 计算 $t_B = g^{r_B} \bmod p$, $Y = g^y \bmod p$, 将 Y 作为自己的临时公钥. 随后 B 利用 r_B 进行签名: 得到 $s_B = b - (\bar{A})^{r_B+y}$, 将 (t_B, Y, s_B) 发送给 A ; 然后 B 计算 $k = t_A^{r_B}$ 以及会话密钥 $SK = H(k, s_B, s_A, ID_B, ID_A)$;

(4) 收到 (t_B, Y, s_B) 后, A 验证等式 $\bar{B} = g^{s_B} g^{y_B} \bmod p$ 是否成立. 若成立, 则 A 计算 $k = t_B^{r_A}$ 以及会话密钥 $SK = H(k, s_B, s_A, ID_B, ID_A)$.

4 方案分析

4.1 安全性分析

SAKA 协议可以抵抗未知密钥共享攻击、可以抵抗密钥泄露伪装攻击, 还具有弱的完美前向安全性.

定理 1 SAKA 协议可以抵抗未知密钥共享攻击

假设敌手 C 要冒充参与者 A 发送消息, 则它必须利用自己的私钥对 $\chi, r_A \in Z_q^*$, 计算 $x = H_1$

(a, χ) 并进行签名 $s_A = a - (\bar{B})^{(r_A + \chi)}$. 显然, 由于敌手无法知道随机数 $\chi, r_A \in Z_q^*$, 因此其并不能完成该签名, 而获得 $\chi, r_A \in Z_q^*$ 相当于解决离散对数问题. 假设敌手 C 要冒充参与者 A 发送消息假的消息 (t_A', X', s_A') 给 B , 则无法通过验证等式 $\bar{A} = g^{s_A'} g^{(X' t_A')^b}$. 不仅如此, 新协议的会话密钥 $SK = H(k, s_B, s_A, ID_B, ID_A)$ 中含有身份信息, 从而避免未知密钥共享攻击.

定理 2 SAKA 协议具有弱的完美前向安全性.

证明如果协议参与者的长期私钥被敌手获得, 而敌手不能由此求出参与者在私钥泄露前协商获得的会话密钥的话, 则称该协议具有前向安全性. 根据会话性质不同, 前向安全性分为完美前向安全性和弱的前向安全性. 具体到协议, 因为新协议的会话密钥 $SK = H(k, s_B, s_A, ID_B, ID_A)$ 中, k 是利用临时私钥获得的, 而如前分析, 获得临时私钥的代价等于破解离散对数问题. 另外, 敌手也不能利用 a 从 $s_A = a - (\bar{B})^{(r_A + \chi)}$ 中获得随机数 r_A , 这是显然的. 这就意味着敌手即使获得长期私钥 a 和 b 也无法获得之前参与者 A 和 B 协商得到的会话密钥. 因此, 新协议具备弱的完美前向安全性. 事实上, 文献[9]中指出, 基于公钥的两轮双方认证密钥协商协议都无法实现完美前向安全性.

定理 3 SAKA 协议可以抵抗密钥泄露伪装攻击.

证明: 如果参与者一方 (如 A) 的长期私钥被敌手获得后, 该敌手显然能冒充他与另一方 (如 B) 进行通信, 但敌手不能冒充另一方与 A 进行通信的话, 则称该协议可以抵抗密钥泄露伪装攻击.

在新协议中, 一个只知道参与者 A 的长期私钥 a 的主动攻击者 C 试图冒充参与者 B 与 A 进行会话. C 应该对 r_B 进行签名: 得到 $s_B = b - (\bar{A})^{(r_B + \chi)}$. 由于敌手无法知道参与者 B 的私钥 b , 显然它无法计算该签名. 因此 C 无法冒充 B .

但是, 一个知道参与者 A 的长期私钥 a 的主动攻击者 C 试图冒充参与者 A 与 B 进行会话. C 随机选取两个数 $\chi', r_A' \in Z_q^*$, 将 χ' 作为自己的临时私钥, 并计算 $x' = H_1(a, \chi')$, $t_A' = g^{r_A'} \bmod p$, $X' = g^{x'} \bmod p$, 将 X' 作为自己的临时公钥. 随后 C 进行签名: 得到 $\bar{A} = g^{s_A'} g^{(X' t_A')^b}$ 成立, 所以 C 能充当参与者 A 与 B 进行会话. 综上所述, 新协议 $s_A' = b -$

$(\bar{B})^{(r_A' + \chi')}$, 将 (t_A', X', s_A') 发送给 B , B 显然能验证可以抵抗密钥泄露伪装攻击.

4.2 效率分析

本方案与同类型的文献[8-9]相比, 新协议避免了模逆运算而少量增加了指数运算, 但模逆运算是有限域运算中最复杂, 最耗时且硬件实现难度最大的运算. 所以新协议在计算量相当的情况下, 改善了文献[8]中协议不能抵抗未知密钥共享攻击、不能抵抗密钥泄露伪装攻击的问题, 改善了文献[9]中 SAKA 协议不具有弱的完美前向安全性的问题.

由于此类协议中双方的计算是等量的, 比较各方案其中一方的计算量即可得到上述结论. 具体比较见表 1.

表 1 三种方案的效率比较

协议	计算量	通信量
文献[8]	$5T_E + 4T_M + 2T_I + T_H$	2
文献[9]	$6T_E + 2T_M + T_I + 2T_H$	2
本文	$7T_E + 2T_M + 2T_H$	2

(表中的基本符号描述: T_E 表示计算一次模指数运算的时间; T_M 表示计算一次模乘运算的时间; T_H 表示计算函数的时间; T_I 表示计算一次逆运算的时间.)

5 结束语

双方密钥协商协议在电子商务和电子会议等方面具有重要的应用价值. 为了解决双方密钥协商协议中的安全性问题, 对赵文中的 SAKA 协议进行了分析, 发现其并不具有弱的前向安全性, 进而提出了一种基于签名的新协议, 通过分析可知新协议很好的解决了安全性问题, 且效率较高.

参考文献:

- [1] Diffie W, Hellman M. New directions in cryptography [J]. IEEE Transaction on Information Theory, 1976, IT-22 (22): 644-654.
- [2] Matsumoto T, Takashima Y, Imai H. On seeking smart public-key distribution systems[J]. The Transactions of the IEICE, 1986, E69-E (2): 99-106.
- [3] Menezes A, Qu M, Vanstone S. Some new key agreement protocols providing implicit authentication[C]// SAC '95. New York: IEEE Press, 1995: 22-32.
- [4] Law L, Menezes A, Qu M, et al. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28 (2): 119-134.

(下转第 25 页)

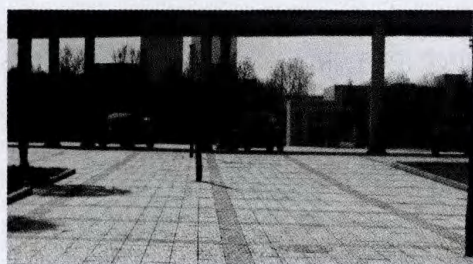


图1 两幅室外图像的拼接结果



图2 本文算法流程图

匹配实验表明,本文准则克服了传统基于距离匹配方法只衡量特征向量整体差异而忽略向量各分量差异的弊病,有效地剔除了误匹配点对,利用互映射原理对匹配点进行双向判断,进一步剔除了误匹配点,两次匹配有效地提高了匹配精度,据此实现了效果良好的图像配准与拼接。实际上,SIFT向量各维度对描述该特征点信息的重要程度是不同的,而本文并没有考虑各个分量的权重关系,如果能按照一定规则赋予向量各维度以不同的权重,理论上将会有更高的匹配精度。

参考文献:

- [1] 曾丹,史浩,张琦. 多相似内容图像的特征匹配[J]. 计算机辅助设计与图形学报, 2011, 23(10): 1725-1733.

(上接第21页)

- [5] Krawczyk H. HMQV: a high-performance secure Diffie-Hellman protocol[C]//Crypto 2005, LNCS. Berlin: Springer, 2005(3621): 546-566.
- [6] 潘操,丁辉,王洪元. 一种新的三方认证密钥协商协议[J]. 微电子学与计算机, 2011, 28(7): 143-145.
- [7] 周四方. 一种新的双方认证密钥协商协议的安全性分析[J]. 计算机应用, 2011, 31(11): 2994-2996.
- [8] 赵建杰,谷大武. eCK模型下可证明安全的双方认证密钥协商协议[J]. 计算机学报, 2011, 34(1): 47-54.

- [2] 易盟,郭宝龙,张旭. 基于复合 Zernike 矩相角估计的图像配准[J]. 光学精密工程, 2012, 20(5): 1117-1125.
- [3] 张锐,张昌芳,李杰. 利用特征点序列截断的图像匹配判决算法[J]. 中国图像图形学报, 2011, 16(6): 1051-1056.
- [4] 郝志成,朱明. 基于多约束准则匹配算法的序列图像配准[J]. 光学学报, 2010, 30(3): 702-707.
- [5] Lowe D G. Distinctive image features from scale-invariant key points [J]. International Journal of Computer Vision, 2004, 60(2): 91-110.
- [6] Beis J S, Lowe G. Shape indexing using approximate nearest-neighbor search in high dimensional spaces [C]//Proceedings of IEEE Computer Society Conference On Computer Vision and Pattern Recognition. Los Alamitos: IEEE Computer Society Press, 1997: 1000-1006.
- [7] 张宇,刘雨东,计钊. 向量相似度测度方法[J]. 声学技术, 2009, 28(4): 532-536.
- [8] Szeliski R. Video mosaics for virtual environment [J]. IEEE Computer Graphics and Application, 1996, 16(2): 22-30.

作者简介:



秦佳男, (1988-), 硕士研究生. 研究方向为图像处理和计算机视觉.

杨建峰男, (1969-), 研究员. 研究方向为空间光学、光谱成像技术等.

作者简介:



王天成(1971-), 硕士, 副教授. 研究方向为代数组与密码学.