基于无证书密码学的可认证三方密钥协商协议

陈家琪, 冯 俊, 郝 妍
(上海理工大学 光电信息与计算机工程学院, 上海 200093)

摘 要: 为了使密钥协商协议能够抵抗主动攻击,提出了一个可认证的无证书三方密钥协商协议。首先分析现有密钥协商协议的特点,然后以无证书密码学理论为基础设计一个安全的三方密钥协商协议。该协议只需要一轮消息交换就可以建立起安全的三方会话密钥,有效地克服了密钥托管问题,提供完善的前向安全性。通过性能分析表明,该协议具有较高的安全性和运行效率。

关键词: 密钥协商; 无证书密码学; 密钥托管; 前向安全
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1902-03
doi:10.3969/j.issn.1001-3695.2010.05.085

Authenticated tripartite key agreement protocol based on certificateless cryptography

CHEN Jia-qi, FENG Jun, HAO Yan
(*School of Optical-Electrical & Computer Engineering, University of Shanghai for Science & Technology, Shanghai* 200093, *China*)

Abstract: In order to make key agreement protocol to resist against the active attacks, proposed a certificateless authenticated tripartite key agreement protocol. First, analysed the existing key agreement protocol. Then designed a security tripartite key agreement scheme based on the theory of certificateless cryptography. This protocol builds a security tripartite session key only need one round message exchange, which can strongly overcome the key escrow and offer perfect forward secrecy. The analysis of security and complexity shows that this protocol is secure and effective.

Key words: key agreement; certificateless cryptography; key escrow; forward secrecy

密钥协商是信息安全中一个重要的研究方向,它是指通信系统中的两个或多个参与主体在一个公开的、不安全的信道上通过协商联合建立一个共享的会话密钥,以实现相互间的安全通信。安全的密钥协商协议是构建复杂的高层协议的基础。

自从 1976 年 Diffie 等人[1]提出密钥协商的概念以来,密钥协商协议得到了深入的研究。Diffie-Hellman 协议中通信双方没有进行身份认证,容易受到中间人攻击。Joux[2]利用椭圆曲线的 Weil 对提出一个只需要一轮交换的三方密钥协商协议,该协议效率高但不能抵抗中间人攻击。Al-Riyami 等人[3]对 Joux 的协议进行了改进,提出了基于数字证书的可认证三方密钥协商协议,但 Shim[4]指出此类协议不能抵抗密钥泄露攻击和已知会话攻击。本文以无证书公钥密码学(certificateless public key cryptography, CL-PKC)[5]为基础,根据 Mandt[6]的两方密钥协商协议,提出一种可认证的无证书三方密钥协商协议。

1 相关预备知识

1.1 无证书公钥密码学简介

近几年来,基于身份的密码学(identity-based cryptography, IBC)成为了密码学领域一大研究热点。在 IBC 体制中,用户公钥可以由用户身份信息直接计算得到,不再需要使用数字证书来认证用户公钥。但是,IBC 的私钥生成器 PKG(private key generator)承担密钥托管的职责,如果 PKG 主密钥泄露,会带来灾难性后果。在 2003 年亚洲密码学会议上,Al-Riyami 等人提出了无证书公钥密码学理论。无证书公钥密码学以线性 Diffie-Hellman 问题为基础,是一种综合了 PKI 和 IBC 特性的公钥密码体系。该密码系统拥有一个密钥生成中心(key generation center,KGC),KGC 为用户生成一个部分私钥,用户将这部分私钥与自己产生的一个秘密值组合得到最终私钥,将秘密值与 KGC 的公共参数组合得到公钥。在无证书公钥系统中,用户的私钥不再是只由 KGC 产生,而是由 KGC 和用户共同来产生,这使得用户的私钥只有用户自己知道,解决了基于身份公钥系统中存在的密钥托管问题。

1.2 线性 Diffie-Hellman 问题

设 G_1 与 G_2 是两个阶为 q 的循环群,q 为大素数,其中 G_1 是以加法的形式表示的,G_2 是以乘法的形式表示的,P 为 G_1 的生成元。G_1 和 G_2 这两个群中的离散对数问题都是难解性问题,若映射 $\hat{e}: G_1 \times G_2 \to G_2$ 满足下列性质则此映射称为可容许的双线性映射。

性质 1 双线性。$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$,对所有 $P, Q \in G_1$ 和所有 $a, b \in Z_q^*$ 成立。

性质 2 非退化性。存在 $P \in G_1$ 和 $Q \in G_1$ 使得 $\hat{e}(P, Q) \neq 1$。

性质 3 可计算性。存在有效算法,对所有 $P, Q \in G_1$,可以计算 $\hat{e}(P, Q)$。

相关的密码学困难性问题如下:

收稿日期: 2009-08-23; **修回日期**: 2009-09-28

作者简介:陈家琪(1957-),男,山东莱阳人,教授,主要研究方向为网络与信息安全、计算机控制系统(cjq@usst.edu.cn);冯俊(1985-),男,硕士研究生,研究方向为网络与信息安全;郝妍(1986-),女,硕士研究生,研究方向为网络与信息安全.

a)离散对数问题(discrete logarithm problem, DLP)。给定 P 和 Q,假如有 $Q=nP(n\in Z_q^*)$ 存在,求 n。

b)计算 Diffie-Hellman 问题(computational Diffie-Hellman problem, CDHP)。给定 P、aP、bP。其中 $a,b\in Z_q^*$,计算 abP。

c)双线性 Diffie-Hellman 问题(bilinear Diffie-Hellman problem, BDHP)。给定 P、aP、bP、cP。其中 $a,b,c\in Z_q^*$,计算 $\hat{e}(P,P)^{abc}$。

2　*Nalla* 的基于身份的三方密钥协商协议

在三方密钥协商协议中,Joux 提出的三方密钥协商协议较为典型,他利用双线性 Diffie-Hellman 问题的难解性,构建了一个基于双线性映射的密钥协商协议,但是,这个协议与 DH 协议一样,存在着无法抵抗中间人攻击的缺陷。后来,Nalla[7] 提出了基于身份的可认证三方密钥协商协议,通过一个可信第三方根据用户的身份标志,来生成对应的用户公钥和私钥,减少了系统管理开销,有效地解决了中间人攻击问题。

在 Nalla 的协议中,密钥生成中心 KGC 选择秘密密钥 $s\in Z_q^*$,生成一个随机数 $P\in G_1$,计算得到其公钥 $P_{KGC}=sP$。用户向 KGC 提供其身份 ID,由 KGC 生成用户的公私钥对:用户公钥 $Q_{ID}=H_1(ID)$。其中单向哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$;用户私钥 $S_{ID}=sQ_{ID}$。假设协商三方 A、B、C 都已从 KGC 得到了各自的私钥 $S_A=sQ_A$、$S_B=sQ_B$ 和 $S_C=sQ_C$。A、B、C 各自独立生成随机数 a、b、$c\in Z_q^*$ 作为临时私钥,对应的临时公钥 $T_A=aP$、$T_B=bP$、$T_C=cP$。协议执行过程如下:

a)三方信息交换

$$A\rightarrow B,C:T_A=aP,V_A=a^{-1}(H(T_A)S_A)$$
$$B\rightarrow A,C:T_B=bP,V_B=b^{-1}(H(T_B)S_B)$$
$$C\rightarrow A,B:T_C=cP,V_C=c^{-1}(H(T_C)S_C)$$

b)消息验证及共享密钥计算

A: $\hat{e}(T_B,V_B)\cdot\hat{e}(T_C,V_C)=\hat{e}(P_{KGC},H(T_B)Q_B+H(T_C)Q_C)$

$K_A=\hat{e}(T_B,T_C)^a=\hat{e}(P,P)^{abc}$

B: $\hat{e}(T_A,V_A)\cdot\hat{e}(T_C,V_C)=\hat{e}(P_{KGC},H(T_A)Q_A+H(T_C)Q_C)$

$K_B=\hat{e}(T_A,T_C)^b=\hat{e}(P,P)^{abc}$

C: $\hat{e}(T_B,V_B)\cdot\hat{e}(T_A,V_A)=\hat{e}(P_{KGC},H(T_B)Q_B+H(T_A)Q_A)$

$K_C=\hat{e}(T_B,T_A)^c=\hat{e}(P,P)^{abc}$

如果各方通过计算得出相等的验证值,则获得共享密钥 $K_{ABC}=V(K_A)=V(K_B)=V(K_C)=V(\hat{e}(P,P)^{abc})$,其中 $V:G_2\rightarrow\{0,1\}^*$。

Nalla 所提出的这个三方密钥协商协议很有效地解决了协议执行过程中中间人攻击问题,但是由于各方密钥必须通过 KGC 获得,不可避免地产生了密钥托管的风险。KGC 知道每个用户的私钥,一旦 KGC 被攻破,所有用户密钥泄露,后果不堪设想。

3　可认证的无证书三方密钥协商协议

3.1　无证书密码学原理

1)系统参数生成　设 G_1 为椭圆曲线上的循环加法群,G_2 为循环乘法群,且阶均为 q,P 是 G_1 的生成元。定义双线性映射 $\hat{e}:G_1\times G_1\rightarrow G_2$ 和两个单向哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^n\times G_2\rightarrow Z_q^*$($n$ 为明文长度)。KGC 随机选择 $s\in Z_q^*$ 作为系统主密钥,计算系统公钥 $P_{pub}=sP$,将 s 保存,公开系统参数 $params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2\}$。

2)部分私钥提取　A 向 KGC 提供身份信息 ID_A,KGC 对 ID_A 认证后向系统输入参数 params,主密钥 s 以及 ID_A,计算 Q_A 和部分私钥 D_A,并将 D_A、Q_A 通过安全信道分别发送给 A。其中 $Q_A=H_1(ID_A)$,$D_A=sQ_A$。A 可以通过等式 $\hat{e}(D_A,P)=\hat{e}(Q_A,P_{pub})$ 来验证 D_A 的真实性。

3)秘密值的选取　用户 A 选取 $x_A\in G_1$ 作为长期秘密值。

4)私钥生成　该算法在 A 的客户端执行,A 输入参数 params,部分密钥 D_A 和秘密值 x_A,客户端输出私钥 S_A。其中 $S_A=x_AD_A=x_AsQ_A$。

5)公钥生成　输入系统参数 params,用户 A 的秘密值 x_A,输出公钥 P_A。其中 $P_A=\langle X_A,Y_A\rangle$,$X_A=x_AP$,$Y_A=x_AP_{pub}=x_AsP$。

3.2　单 *KGC* 的无证书三方密钥协商协议

根据 3.1 节介绍的无证书公钥密码学理论,用户 A、B、C 分别将各自的身份信息 ID_A、ID_B、ID_C 提交给密钥生成中心 KGC,KGC 通过安全信道返回部分私钥 D_A、D_B、D_C,其中 $D_i=sQ_i=sH_1(ID_i)$,s 为 KGC 的主密钥。各参与方用户分别生成一个 KGC 所不知的秘密值 $x_i\in Z_q^*$,结合部分私钥 D_i,生成私钥 $S_i=\langle D_i,x_i\rangle$,各用户的公钥 $P_i=x_iP$,短期密钥 $S'_i=D_i+x_iQ_i=(s+x_i)Q_i$。

用户 A、B、C 进行安全通信,密钥协商过程(图 1)如下。

a)A、B、C 分别选择秘密随机数 a、b、$c\in Z_q^*$,计算 $T_A=aQ_A$,$T_B=bQ_B$、$T_C=cQ_C$。

b)A 将$\langle ID_A,T_A,P_A\rangle$发送给 B 和 C,B 将 $<ID_B,T_B,P_B>$ 发送给 A、C:

$$A\rightarrow B,C:ID_A,T_A=aQ_A,P_A;B\rightarrow A,C:ID_B,T_B=bQ_B,P_B$$

c)C 收到 A 和 B 发送的信息后,计算

$K_C=\hat{e}(S'_C,P)^c\cdot\hat{e}(T_A,P_{pub}+P_A)\cdot\hat{e}(T_B,P_{pub}+P_B)$。C 将$\langle ID_C,T_C,P_C,MAC_{Kc}(ID_C,T_C,P_C)\rangle$发送给 A 和 B。其中 $MAC_{Ki}(m)$是用户 i 的消息认证码,确保数据的完整性。

$$C\rightarrow A,B:ID_C,T_C=cQ_C,P_C,MAC_{Kc}(ID_C,T_C,P_C)$$

d)A、B 收到 C 的消息,分别计算 K_A 和 K_B:

$$K_A=\hat{e}(S'_A,P)^a\cdot\hat{e}(T_B,P_{pub}+P_B)\cdot\hat{e}(T_C,P_{pub}+P_C)$$
$$K_B=\hat{e}(S'_B,P)^b\cdot\hat{e}(T_A,P_{pub}+P_A)\cdot\hat{e}(T_C,P_{pub}+P_C)$$

e)验证共享密钥的正确性。A 和 B 验证 C 消息的完整性,如果 $MAC_{KA}(ID_C,T_C,P_C)=MAC_{KB}(ID_C,T_C,P_C)=MAC_{KC}(ID_C,T_C,P_C)$,则 A 将$\langle ID_A,MAC_{KA}(ID_A,T_A,P_A)\rangle$发送给 B、C,B 将$\langle ID_B,MAC(ID_B,T_B,P_B)\rangle$发送给 A、C,各方分别验证消息的完整性。如果验证结果与原始消息匹配,则密钥协商成功,可以生成三方共享密钥;若验证结果不匹配,则说明消息交换过程中受到恶意攻击,需要重新进行密钥协商。

$$A\rightarrow B,C:ID_A,MAC_{KA}(ID_A,T_A,P_A);B\rightarrow A,C:ID_B,MAC_{KB}(ID_B,T_B,P_B)$$

f)若参与者 A、B 和 C 在消息交换过程中都遵守协议所设定的规则,则 $K_A=K_B=K_C$,通过计算可以得到一个共享密钥:

$$K=\hat{e}(Q_A,P)^{a(s+xA)}\cdot\hat{e}(Q_B,P)^{b(s+xB)}\cdot\hat{e}(Q_C,P)^{c(s+xC)}$$

为确保攻击者从会话密钥中不能获得任何信息,A、B、C 三方对 K 进行 hash 处理,最终得到协商的共享密钥 S_K,$S_K=H_2(K\|P_A\|P_B\|P_C)$。

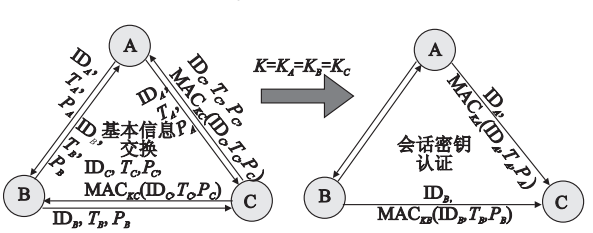

图1　无证书三方密钥协商过程

3.3 多个分布式 KGC 的密钥协商协议

在三个不同的 KGC 域的用户同样可以按照无证书密钥协商协议获得会话密钥。KGC_1、KGC_2、KGC_3 分别表示三个不同的密钥生成中心，各自产生主密钥 $s_1, s_2, s_3 \in Z_q^*$，相应的各 KGC 的公钥为 $P_1 = s_1P, P_2 = s_2P, P_3 = s_3P$。其中 P 是各方都认可的 G_1 生成元。协议参与者 A、B、C 分别是 KGC_1、KGC_2、KGC_3 的用户，依据 3.2 节提出的步骤进行密钥协商：

$$K_A = \hat{e}(S'_A, P)^a \cdot \hat{e}(T_B, P_2 + P_B) \cdot \hat{e}(T_C, P_3 + P_C)$$

$$K_B = \hat{e}(S'_B, P)^b \cdot \hat{e}(T_A, P_1 + P_A) \cdot \hat{e}(T_C, P_3 + P_C)$$

$$K_C = \hat{e}(S'_C, P)^c \cdot \hat{e}(T_A, P_1 + P_A) \cdot \hat{e}(T_B, P_2 + P_B)$$

最终得到会话密钥：

$$K = \hat{e}(Q_A, P)^{a(s_1 + xA)} \cdot \hat{e}(Q_B, P)^{b(s_2 + xB)} \cdot \hat{e}(Q_C, P)^{c(s_3 + xC)}$$

4 协议安全性及性能分析

4.1 安全性分析

文献[8]给出了密钥协商协议需要满足的安全属性，目前对大多数协议的安全分析需要考察以下几个安全属性：隐藏密钥认证、已知会话密钥安全性、前向安全性、抗密钥泄漏伪装攻击、未知密钥共享安全，以及密钥的不可控性。根据这几个安全属性标准，具体分析本文提出的三方密钥协商协议的安全性。

1)隐藏密钥认证　协议中每一方用临时的短期密钥来参与生成会话密钥，每个用户都确信会话密钥只有协议的参与者才知道，攻击者无法获知，提供隐藏密钥认证的密钥协商协议能够抵挡中间人攻击。假设攻击者 U 假冒 A 与 B、C 通信，U 选择随机数 u，将 $T_U = uQ_A, P_A$ 发送给 B、C，从而 U 获得 T_B、P_B 和 T_C、P_C。但是 U 不知道 A 的短期密钥 S'_A 的信息，而且从 $T_B = bQ_B$、$T_C = cQ_C$ 中计算出 b 和 c 相当于解 G_1 上的离散对数难题 DLP。因此，该协议能够抵挡中间人攻击，并提供隐藏密钥认证。

2)已知会话密钥安全性　每执行一次密钥协商协议，参与者 A、B、C 都会相应地选取不同的秘密随机数 a、b 和 c，从而通过协商产生一个不同的会话密钥。协议中先前的某个会话密钥泄露或被攻击者主动获取时，攻击者无法获得其他任何会话密钥。

3)前向安全性　协议中参与者长期私钥泄露，但是其先前的会话密钥并不受任何影响。假设攻击者获取了 A 的长期密钥 S_A，但是由于离散对数问题的难解性，攻击者无法通过 $S_A = x_AD_A$ 计算出 x_A，从而无法得到 A 的短期密钥 S'_A，而且攻击者不知道 A 选择的临时秘密随机数 a，所以会话密钥 K 不受影响。因此，一个用户私钥泄露，不会导致会话密钥泄露，该协议具有前向保密性。无证书密钥协商协议无密钥托管风险，KGC 不知道参与者的私钥，如果 KGC 主密钥 s 泄露，即使攻击者能够计算出用户的部分私钥，因为无法同时获得用户的长期私钥和短期临时密钥，依然不能够计算出会话密钥。

4)抗密钥泄露伪装攻击　假设攻击者 U 知道协议参与者 A 的私钥 $S_A = \langle D_A, x_A \rangle$，如果 U 想冒充 B 或者 C 与 A 通信，U 必须正确计算出 $K = K_A = K_B = K_C$。$K_A = \hat{e}(S'_A, P)^a \cdot \hat{e}(T_B, P_{pub} + P_B) \cdot \hat{e}(T_C, P_{pub} + P_C)$，因为 U 不知道秘密值 a，所以不能正确计算 K_A；若 U 想计算出 K_B 或 K_C，在不知道短期密钥 S'_B、S'_C 和临时秘密值 b、c 的情况下，是无法成功计算出 K_B 和 K_C 的。因此，协议具有抵抗密钥泄露伪装攻击的能力。

5)未知密钥共享安全　攻击者 U 意图强迫 A、B 和 C 三方共享会话密钥 K'，但是协议的三个参与者在不知道对方身份的情况下，没有经过协商是不可能共享一个会话密钥的。在完成密钥协商后，A、B、C 需要通过验证消息完整性来确认会话密钥的有效性。所以，攻击者无法进行未知密钥共享攻击。

6)密钥的不可控性　协议的所有参与者都不能控制会话密钥的输出，则称该协议具有会话密钥的不可控性。在协议中，$\langle ID_i, T_i, P_i \rangle$ 是由各协议参与者自己产生的，并不受哪一方的控制，任何一方都无法预先确定会话密钥值。所以，该协议具有密钥不可控性。

4.2 性能分析

密钥协商协议的效率主要体现在消息交换的通信开销和密钥计算两个方面，在评估协议计算代价时，主要考虑离散对数运算、点乘运算、幂运算以及哈希运算的计算量。本文提出的无证书三方密钥协商协议需要一轮基本信息交换和一轮认证信息交换。下面将本文提出的协议同 Al-Riyami、Nalla 等人提出的协议进行计算代价比较，表 1 是协议计算代价的比较结果。

表1　协议计算代价比较

协议	离散对数	点乘	指数	哈希
Al-Riyami	4	3	1	2
Nalla	4	5	1	4
本文	3	2	1	2

本文提出的协议需要进行三次对数运算，两次点乘运算，一次指数运算和两次哈希运算。通过分析可以看出，无证书三方密钥协商协议比 Al-Riyami 和 Nalla 的协议具有更高的效率。

5 结束语

三方密钥协商具有重要的应用价值不仅因为它是电子会议最普遍的通信模式，而且因为它可以为两方通信提供一些特别的服务。本文基于无证书公钥密码体系提出了一个可认证的三方密钥协商协议，并说明该协议在多 KGC 环境下同样适用，有效地解决了基于身份的密钥协商协议所凸显的密钥托管的缺点，具有完善的隐藏密钥认证和前向保密性，能够抵抗中间人攻击和已知密钥攻击。通过分析表明，本协议具有更高的运算效率，能很好地满足当代通信安全需求。在以后的研究中，进一步探讨协议在多方群组密钥协商中的应用。

参考文献：

[1] DIFFIE W, HELLMAN M. New directions in Cryptography[J]. IEEE Trans on Information Theory, 1976, 22(6): 644-654.

[2] JOUX A. A One-round protocol for tripartite Diffie-Hellman[C]// Proc of Algorithmic Number Theory Symposium. [S. l.]: Springer-Verlag, 2000.

[3] AL-RIYAMI S S, PATERSON K G. Tripartite authenticated key agreement protocols from pairings[M]. [S.l]: Springer-Verlag, 2003.

[4] SHIM K. Efficient one-round tripartite authenticated key agreement protocol form the Weil pairing[J]. Electronics Letters 2003(39): 208-209.

[5] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// Proc of Advances in Cryptology-Asiacrypt. 2003.

[6] MANDT T K. Certificateless authenticated two-party key agreement protocols[D]. Master's Thesis. Gjviik University College, 2006.

[7] NALLA D. ID-based tripartite key agreement with signatures[M]. [S.l]: Springer-Verlag, 2002.

[8] BLAKE-WILSON S, JOHNSON D, MENEZES A. Key agreement protocols and their security analysis[C]// Proc of the 6th IMA International Conference on Cryptography and Coding. [S. l.]: Springer-Verlag, 1997.