doi:10.13582/j.cnki.1672-9102.2014.01.013

# 安全的基于身份认证密钥协商协议

刘志远

(湖北理工学院 计算机学院,湖北 黄石 435003)

**摘　要**:由于移动互联网络的快速发展,在不安全的移动通信环境中如何构造安全的密钥协商协议是一个富有挑战性的问题.2012 年高海英设计并实现了一个在标准模型下的安全的认证密钥协商协议.通过对该协议的安全性分析,发现该协议在无会话密钥托管模式下并不满足 PKG 前向安全性.为了弥补该协议的不足,提出了一个安全的基于身份认证密钥协商协议.该协议能够抵抗未知密钥共享和密钥泄露伪装攻击,同时具有前向安全性和已知密钥安全等安全性质.方案的安全性分析表明,新的方案比高海英的协议具有更高的安全性.

**关键词**:认证密钥协商;PKG 前向安全;双线性对;密钥托管

**中图分类号**:TP309　　**文献标志码**:A　　**文章编号**:1672-9102(2014)01-0064-04

# Secure identity-based authenticated key agreement protocol

LIU Zhi-yuan

(College of Computer Science, HuBei Institute of Technology, Huangshi 435003, China)

**Abstract**: With the fast development of the Mobile Internet , How to construct secure key agreement protocol is one of the most challenging in the unsafe mobile communications environment. In 2012, Gao Haiying proposed an efficient Identity Based authenticated key agreement protocol , which is proved to be secure in the standard model. Gao's protocol was analysed and showed that it didn't provide PKG-forward secrecy in key escrowless mode. To solve this problem, a secure protocol was proposed. It also provided known-key security and forward secrecy resists key-compromise impersonation and unknown key share attacks. Results show that the protocol provides PKG-forward secrecy in escrowless mode .

**Key words**: authenticated key agreement;PKG-forward secrecy;bilinear pairing;key escrow

目前,由于移动互联网络的快速发展,越来越多的用户参与其中.如何在开放的网络中建立安全的信道来保证通信双方会话的安全是一个富有挑战性的问题.在通常情况下,如果攻击者从一个不安全的通信信道中获取了通信双方的会话密钥,那么用户之间的整个会话将毫无安全性可言,用户的隐私和切身的经济利益将会受到严重的损害,甚至还会危害到用户之间以后会话的安全.为了降低用户在通信过程中会话密钥泄露给用户带来的危害,认证密钥协商协议成为了倍受关注的方法之一.

常见认证密钥协商协议主要有 2 类:基于口令的认证密钥协商协议和基于身份的认证密钥协商协议.第一个基于口令的密钥协商协议[1]在 1992 年由 Bellovin 和 Merritt 提出随后许多的基于口令的密钥协商协议[2-3]被提出.在实际应用中,基于口令的协议比较容易实现,但是它也存在着比较明显的弱点,那就是口令很容易受到字典攻击或猜测攻击.基于身份的公钥密码体制[4]在 1984 年由 Shamir 首次提出,随后许多基于身份的加密、签名和密钥协商协议被提出.在较早的时候的基于身份

**收稿日期**:2013-11-19

**基金项目**:国家自然科学基金资助项目(60903196);湖北省自然科学基金资助项目(2013CFB039);湖北理工学院重点项目(13xjz06A)

**通信作者**:刘志远(1972-),男,湖北鄂州人,博士,副教授,主要从事密码学,网络安全研究. E-mail:shengdiwl@163.com

的密钥协商协议大多是在随机预言机模型(RO)下实现的. 众所周知,随机预言机模型在实际应用中很难被实现的,因此在 RO 模型下设计的方案的实用性不是很强. 基于上述原因,在文中主要讨论的是在标准模型下实现的基于身份的认证密钥协商协议.

2006 年,Gentry 在欧密会上提出了一个实用的基于身份的加密方案[5]. 基于 Gentry 的方案,第一个标准模型下的基于身份的密钥协商协议[6]由 Wang 等人在 2007 年提出. 随后在标准模型下的基于身份的密钥协商协议[7-9]陆续被提出. 文献[7]和[8]都指出文献[6]的方案是不安全的,因为该方案在有恶意的 PKG 中心存在的情况下,它是不具有 PKG 前向安全的. 在实际的应用中,可以很容易地发现文献[8]依然存在 PKG 前向安全问题. 即在有恶意的 PKG 存在的情况下,该协议中所有用户协商的会话密钥都是可见的. 在文献[8]的基础之上,提出了一种改进的基于身份的密钥协商协议,分析证明本文的方案很好的弥补了高海英方案的不足.

本文剩下部分的组织结构如下:在第 1 节给出方案所需的相关预备知识;第 2 节给出了 Gao 协议以及该协议的安全性分析;第 3 节在 Gao 协议的基础上,提出了一种改进的基于身份的密钥协商协议;方案的安全性分析证明将在第 4 节给出;最后在第 5 节总结了全文.

## 1　密钥协商的安全性与相关的数学知识

### 1.1　双线性映射

双线性映射最早由文献[9]提出,并用于求解椭圆曲线群的离散对数问题. 后因其特有的双线性性,2000 年以后被广泛应用于各类密码方案的设计中. 有关双线性映射更多的细节可以查阅文献[10].

设 $G_1$ 是由 $g$ 生成的加法循环群,阶为素数 $p$. $G_2$ 是一个乘法循环群,阶也是 $p$. 双线性映射 $\hat{e}:G_1 \times G_1 \rightarrow G_2$ 的性质如下:

1)双线性性:如果对所有的 $\forall a,b \in Z_q^*$,都有 $\hat{e}(g^a,g^b) = \hat{e}(g,g)^{ab}$.

2)非退化性:$\hat{e}(g,g) \neq 1$.

3)可计算性:$\forall u,v \in G,\hat{e}(u,v)$ 可由一个多项式时间算法来计算.

### 1.2　认证密钥协商协议需满足的安全性

一个安全的认证密钥协商协议必须满足以下 5 个性质:1)无会话密钥托管;2)前向安全性;3)抵抗密钥泄露伪装攻击;4)已知会话密钥安全;5)未知密钥共享安全性. 各个性质的具体描述参见文献[11].

## 2　高海英协议及其协议的安全性分析

下文中对高海英协议的描述简称为 Gao 协议.

### 2.1　Gao 协议

本节将简要地介绍 Gao 协议,该协议中用到的困难性假设和参数都和文献[8]相同.

1)Setup $(1^k)$ 算法

通过输入安全参数 $1^k$,该算法由 PKG 执行并生成系统用的主公开参数和主秘密参数,具体过程如下:随机选取生成元 $g,h \in G_1,\alpha \in Z_q^*$,计算 $g_1 = g^\alpha$. 哈希函数 $H:\{0,1\}^* \rightarrow \{0,1\}^k$,系统公开参数为 $(g,g_1,h,H)$,系统主密钥为 $\alpha$.

2)用户私钥生成

随机选择 $r_{ID} \in Z_p^*$,计算 $d_{ID} = (r_{ID},h_{ID})$;其中 $h_{ID} = (hg^{-r_{ID}})^{1/(\alpha-ID)}$.

3)用户之间的密钥协商过程

不妨设 Alice 的身份为 $ID_A$,私钥为 $h_{ID_A}$;Bob 的身份为 $ID_B$,私钥为 $h_{ID_B}$. 令 $D_A = e(g,h)^{r_A},D_B = e(g,h)^{r_B},g_A = g_1 g^{-ID_B},g_B = g_1 g^{-ID_A},g_T = e(g,g)$,Alice 和 Bob 可预先计算 $g_A,D_A,g_B,D_B$. 它们之间进行会话密钥协商过程如下:

Step1:Alice 随机选取 $x \in Z_p^*$,计算 $T_{A_1} = g_B^x$,$T_{A_2} = g_T^x,T_{A_3} = D_A^x$,将 $T_A = (T_{A_1},T_{A_2},T_{A_3})$ 发送给 Bob;

Step2:Bob 随机选取 $y \in Z_p^*$;计算 $T_{B_1} = g_A^y$,$T_{B_2} = g_T^y,T_{B_3} = D_B^y$,将 $T_B = (T_{B_1},T_{B_2},T_{B_3})$ 发送给 Alice;

Step3:Alice 计算 $K_{AB} = [e(T_{B_1},h_A) \cdot (T_{B_2})^{r_A}]^x (T_{B_3})^{x \cdot r_A} = e(g,h)^{xy(1+r_A r_B)}$;

$sk_{AB} = H(A,B,T_A,T_B,K_{AB},g^{xy})$;

Bob 计算 $K_{BA} = e(d_{B_1},T_{A_2} g^y) e(d_{B_2}^{-1},T_{A_1} Q_B^y) = e(g,h)^{xy(1+r_A r_B)}$;

$sk_{BA} = H(A,B,T_A,T_B,K_{BA},g^{xy})$.

故此 Alice 和 Bob 的协商会话密钥为 $SK = H(A,B,T_A,T_B,e(g,h)^{xy(1+r_A r_B)})$.

### 2.2　Gao 协议的安全性分析

本节主要分析 Gao 协议的安全性,说明如果有恶意的 PKG 存在的情况下,他是可以计算出所有通信用户双方的会话密钥的. 首先在参数设置部

分,PKG 选取 $g$ 为群 $G$ 的生成元,随机选取 $h \in G$,计算 $h = g^{\sigma}$,保密 $\sigma$,公开参数 $PK = (G, G_T, g, g_1, h, \hat{e}, H)$.

假定恶意的 PKG 从公开信道截获 $T_A = (T_{A_1}, T_{A_2}, T_{A_3})$ 和 $T_B = (T_{B_1}, T_{B_2}, T_{B_3})$,由于 PKG 知道协议参与方 Alice 和 Bob 分别对应的私钥 $d_A = (r_A, h_A)$ 和 $d_B = (r_B, h_B)$,于是他可以计算: $T_{A_1} = g_B^x = g^{x(\alpha - ID)}$,则 $g^x = (T_{A_1})^{(\alpha - ID)^{-1}}$;同理可以求出 $g^y = (T_{B_1})^{(\alpha - ID)^{-1}}$. 那么通过计算可有 $K_{AB} = e(g^x, g^y)^{\sigma(1 + r_A r_B)} = e(g^x, h^y)^{(1 + r_A r_B)} = e(g,h)^{xy(1 + r_A r_B)} = K_{BA}$. 就这样恶意的 PKG 获取了用户 Alice 和 Bob 的协商会话密钥 $H(A, B, T_A, T_B, e(g,h)^{xy(1 + r_A r_B)})$. 由此可见高海英的协议并不满足 PKG 前向安全性.

## 3 安全的基于身份的密钥协商协议

基于文献[8],本文基于身份的认证密钥协商协议如下:

1) Setup ($1^k$) 算法:通过输入安全参数 $1^k$,该算法由 PKG 执行并生成系统用的主公开参数和主秘密参数,具体过程如下:

- 生成 2 个大素数 $p$ 阶群 $G$ 和 $G_T$, $g \in G$,其中 $g$ 是 $G$ 的生成元. 随机选取 $h \in G$,双线性映射 $\hat{e}: G \times G \to G_T$;
- 选择主秘密参数 $\alpha \in Z_p^*$,设定 $g_1 = g^{\alpha}$,选择 $H: \{0,1\}^* \to \{0,1\}^k$;
- 生成主公开参数 $PK = (G, G_T, g, g_1, h, \hat{e}, H)$;

2) Extract ($MK, ID$) 算法:通过输入主秘密参数 $MK$ 和身份信息 $ID$,该算法由 PKG 执行并为身份信息 $ID$ 生成对应的私钥,具体过程如下:

- 随机选择 $r_{ID} \in Z_p^*$,计算 $d_{ID} = (r_{ID}, h_{ID})$;其中 $h_{ID} = (hg^{-r_{ID}})^{1/(\alpha - ID)}$.

3) Exchang ($PK, d_A, d_B$) 算法:通过输入主公开参数 $PK$,身份信息 $ID$ 对应的私钥 $d_{ID}$,令 $D_A = e(g,h)^{r_A}, D_B = e(g,h)^{r_B}, g_A = g_1 g^{-ID_B}, g_B = g_1 g^{-ID_A}, g_T = e(g,g)$.

Alice 和 Bob 认证密钥协商过程如下:

- Alice 随机选取 $x \in Z_p^*$,计算 $T_{A_1} = g_B^x, T_{A_2} = g_T^x, T_{A_3} = D_A^x, T_{A_4} = g^x$,将 $T_A = (T_{A_1}, T_{A_2}, T_{A_3}, T_{A_4})$ 发送给 Bob;
- Bob 收到 $T_A$ 后,随机选取 $y \in Z_p^*$;计算 $T_{B_1} = g_A^y, T_{B_2} = g_T^y, T_{B_3} = D_B^y, T_{B_4} = g^y$ 将 $T_B = (T_{B_1}, T_{B_2}, T_{B_3}, T_{B_4})$ 并发送给 Alice;
- Alice 计算 $K_{AB} = [e(T_{B_1}, h_A) \cdot (T_{B_2})^{r_A}]^x (T_{B_3})^{x \cdot r_A} = e(g,h)^{xy(1 + r_A r_B)}$;

$T_{B_2}^x = g^{xy}, sk_{AB} = H(A, B, T_A, T_B, K_{AB}, g^{xy})$;

- Bob 计算 $K_{BA} = e(d_{B_1}, T_{A_2} g^y) e(d_{B_2}^{-1}, T_{A_1} Q_B^y) = e(g,h)^{xy(1 + r_A r_B)}$;

$T_{A_2}^y = g^{xy}, sk_{BA} = H(A, B, T_A, T_B, K_{BA}, g^{xy})$.

因此,由上可知 Alice 和 Bob 的共享会话密钥为 $SK = H(A, B, T_A, T_B, K_{BA}, g^{xy})$.

## 4 安全性分析

### 4.1 方案的正确性

该方案的密钥协商结果的正确性证明如下:

证明:

$$K_{AB} = [e(T_{B_1}, h_A)(T_{B_2})^{r_A}]^x (T_{B_3})^{x \cdot r_A} =$$
$$[e(g_A^y, (hg^{-r_A})^{\frac{1}{(\alpha - ID)}})(g_T^y)^{r_A}]^x (D_B^y)^{x \cdot r_A} =$$
$$[e((g_1 g^{-ID_B})^y, (hg^{-r_A})^{\frac{1}{(\alpha - ID)}})(e(g,g)^y)^{r_A}]^x e(g,h)^{xyr_A r_B} =$$
$$[e(g^y, (hg^{-r_A}))e(g,g)^{yr_A}]^x e(g,h)^{xyr_A r_B} =$$
$$[e(g^y, h]^x e(g,h)^{xyr_A r_B} =$$
$$e(g,h)^{xy(1 + r_A r_B)};$$
$$K_{BA} = [e(T_{A_1}, h_B)(T_{A_2})^{r_B}]^y (T_{A_3})^{y \cdot r_B} =$$
$$[e(g_A^y, (hg^{-r_B})^{\frac{1}{(\alpha - ID)}})(g_T^x)^{r_B}]^y (D_A^x)^{y \cdot r_B} =$$
$$[e((g_1 g^{-ID_A})^x, (hg^{-r_B})^{\frac{1}{(\alpha - ID)}})(e(g,g)^x)^{r_B}]^y e(g,h)^{xyr_A r_B} =$$
$$[e(g^x, (hg^{-r_B}))e(g,g)^{xr_B}]^y e(g,h)^{xyr_A r_B} =$$
$$[e(g^x, h]^y e(g,h)^{xyr_A r_B} =$$
$$e(g,h)^{xy(1 + r_A r_B)}.$$

由此可以证明 $sk_{BA} = sk_{AB}$,所以 Alice 和 Bob 协商的密钥是正确的.

### 4.2 无会话密钥托管下 PKG 前向安全性

定理 基于 CDH 问题困难性假设,提出的基于身份的密钥协商协议是具有无会话密钥托管情况下 PKG 前向安全性的.

证明:不妨假定敌手获取了系统的主密钥 $\alpha$ 和用户的私钥,以及生成元 $g$ 和 $h$ 之间的关系. 那么敌手是可以计算出 $K_{AB} = e(g,h)^{xy(1 + r_A r_B)}$ 的(具体的计算过程在 2.2 小节已给出). 但是要计算 Alice 和 Bob 的共同协商密钥 $sk_A$ 或 $sk_B$,则必须要计算 $g^{xy}$,亦即要从 $g^x$ 中计算出 $x$ 或从 $g^y$ 中计算出 $y$,这相当于解决 CDH 问题. 因此方案是满足在无会话密钥托管模式下 PKG 前向安全的.

### 4.3 安全性比较

在这一部分,从未知密钥共享安全性、已知会话密钥安全、抵抗密钥泄露伪装攻击、前向安全性、会话密钥托管等几个方面比较本文方案和文献[8]所满足的安全特性. 下表中√表示满足某个特

性,×表示不满足.具体比较结果如下表 1 所示.

表 1　基于身份的认证密钥协商协议安全性比较

| | 本文的方案 | Gao 协议 |
|---|---|---|
| 未知密钥共享安全性 | √ | √ |
| 已知会话密钥安全 | √ | √ |
| 抵抗密钥泄露伪装攻击 | √ | √ |
| 前向安全性 | √ | √ |
| 无会话密钥托管 | √ | × |

综上所述,和文献[8]的方案相比,虽然本文的方案在密钥协商过程中增加了用户的一次指数运算,但是它解决了文献[8]存在的会话密钥托管问题即 PKG 前向安全问题.

## 5　结论

文献[8]提出了一个可证明的基于身份的认证密钥协商协议,并且相比于原有的基于身份的密钥协商方案,该方案提出在 PKG 中心完全可信的情况下可以高效地实现用户之间的密钥协商.但在实际应用过程中恶意的 PKG 不可否认是客观存在的.因此在有恶意的 PKG 存在的情况下如何构造一个安全的密钥协商协议是一个重要的工作.在文献[8]的基础之上,提出了一种安全的基于身份的认证密钥协商协议.同时在文献[8]提出的方案的可证明安全性的基础上,很容易地证明了本文提出的方案比文献[8]具有更高的安全性.

**参考文献:**


[1] Bellovin S, Merritt M. Encrypted key exchange: password – based protocols secure against dictionary attacks[C] // Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy. Oakland, IEEE Computer Society, 1992:72 – 84.

[2] 刘天, 朱宏峰, 潘正祥. 基于椭圆曲线的强壮高效口令认证密钥协商方案[J]. 应用科学学报,2012,30(1):67 – 74.

[3] 谭示崇, 庞辽军,苏万力,等. 高效的匿名的基于口令的认证密钥协商协议[J]. 通信学报,2009:17 – 20.

[4] Shamire A. Identity – based cryptosystems and signatures chemes[C] // Advances in Crypto*logy* (Crypto 84). Califonial Springer – Verlag, 1984:47 – 53.

[5] Gentry C. Practical identity – based encryption without random oracles[C] // Proceedings of the Advances in Cryptology – Eurocrypt'06. Berlin, 2006:445 – 464.

[6] 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 – 1854.

[7] 汪小芬,陈原,肖国镇. 基于身份的认证密钥协商协议的安全分析与改进[J]. 通信学报,2008,29(12): 16 – 21.

[8] 高海英. 可证明安全的基于身份的认证密钥协商协议[J]. 计算机研究与发展,2012,49(8):1685 – 1689.

[9] Alfred J, Okamoto T, Scott A. Reducing elliptic curve logarithms to logarithms in a finite field[J]. IEEE Transactions on Information Theory, 1993,39(5): 1639 – 1646.

[10] Boneh D, Franklin M. Identity – Based Encryption from the Weil Pairing[C] // Advances in Cryptology – CRYPTO 2001, LNCS 2139, Springer – Verlag, 2001: 213 – 239.

[11] 高志刚,冯登国. 高效的标准模型下基于身份的认证密钥协商协议[J]. 软件学报, 2011,22(5):1031 – 1040.