第 42 卷 第 6A 期
2015 年 6 月
计 算 机 科 学
Computer Science
Vol. 42 No. 6A
June 2015

基于单向同构函数的三方认证密钥协商协议

陈海红
(湖南永州职业技术学院计算机系 永州 425000)

摘 要 密钥协商是实现参与者在公平的开放环境下建立会话密钥的重要手段。提出了一种新的可实现第三方对参与者身份进行认证的三方密钥协商协议。新协议利用单向同构函数生成会话密钥,避免了 Hash 函数的不安全问题。之后,利用定义的标准模型对协议进行了严格的形式化证明,并对协议的安全性和计算量进行了横向比较。结果显示,新协议具备已知密钥安全、绝对前向安全性和抗密钥泄露伪装攻击,且计算量也可被接受。

关键词 密码学,密钥协商,单向同构函数,密码分析,标准模型
中图法分类号 TP309 文献标识码 A

Three-party Authenticated Key Agreement Protocol Based on One-way Isomorphism

CHEN Hai-hong
(Computer Department, Yongzhou Vocational Technology College, Yongzhou 425000, China)

Abstract Key agreement is an important mean to realize the secure communication between participants under the open and fair environment. This paper proposed a novel three-party key agreement protocol which has the sender authentication property. We used a one-way isomorphism to generate session key. And this mean avoids the insecurity of Hash function. We then gave the rigid security proof for our new protocol and compared the computational cost with some refe-rences. The result shows that our protocol has known key security, perfect forward security and can resist on the key compromise impersonation attack, and our protocol also has the acceptable computational cost.

Keywords Cryptography, Key agreement, One-way isomorphism, Cryptanalysis, Standard model

1 引言

密钥协商协议是密钥建立的一种有效方式。通过这种手段,参与者仅需交换各自的公开信息即可建立一个第三方无法获取的临时会话密钥,从而为后续秘密通信提供加密手段。另外,安全的密钥协商协议也是构造复杂高层综合通信协议的前提和基础。

设计高效安全的密钥协商协议一直是研究热点。Diffie 和 Hellman 最早提出了利用公钥密码体制实现密钥协商的方式,它允许从未共享过密钥的双方可以在开放的网络环境中通过交换信息建立共享的会话密钥。2000 年,Joux 等人[1]在 Diffie-Hellman 协议的基础上提出了单轮三方密钥协商协议。但上述协议均没有考虑到参与者之间的身份认证问题,因此极易受到中间人攻击。随后,学者们围绕上述协议展开研究,设计了大量的满足不同安全需求和应用场景的协议[2-5]。

可认证参与者身份的协议是认证密钥协商协议的一个重要分支。这类协议的最大特点是:除了参与者各方,可信第三方也可以利用公开信息验证参与者的身份,从而为协议的可信度提供保障。1995 年,Nyberg 等人[6]首先提出了双方可认证参与者身份的密钥协商协议,但遗憾的是,该协议不具备前向安全性。之后,Choie-Jeong-Lee[7]和 Popescu[8]分别提出了满足前向安全性的双方可认证参与者身份的协议,Zhang-Liu-Kim[9]和 Shim[10]首次提出了基于身份的三方可认证身份的协议,Du-Wang-Ge-Wang[11]将其扩展到了多方的情形。其中,文献[10]是目前安全性和效率最好的一个方案。但遗憾的是,上述的这些方案都没有对协议本身进行严格的形式化证明,其宣称的安全性并不可靠。另外,上述方案都使用了假设安全的 Hash 函数,协议的安全性也基于随机预言模型,但目前我们常用的如 MD5、SHA-1 等 Hash 函数并不是随机预言机,因此,如何构建在标准模型下安全的可认证参与者身份的密钥协商协议就成为学术界关注的重点之一。

本文基于乘法循环群中的单向同构函数,设计了一种新的三方可认证参与者身份的密钥协商协议,并在标准模型下对方案进行了安全性证明。与 Zhang-Liu-Kim[9](简化版本)和 Shim[10]的协议相比,新协议在性能方面仍有一定的优势。

本文第 2 节为基础知识,简述本文用到的一些基本概念,并对安全性进行定义,第 3 节给出可认证参与者身份的密钥协商协议的定义;第 4 节介绍本文用的标准模型;第 5 节进行安全性和性能分析;最后总结全文。

2 基础知识

本节将定义单向同构函数和双线性映射的概念,并定义 3 个安全属性:已知密钥安全、完美的前向安全性和密钥泄露伪装安全。

2.1 单向同构函数

假设 G_1,G_2 和 G_T 是 3 个阶均为 p 的乘法循环群,g_2 是

陈海红(1982—),女,硕士,讲师,主要研究领域为安全协议设计、RFID 安全。

群 G_2 的一个生成元。

单向同构函数：如果函数 $f:G_2\to G_1$ 满足 $f(g_2^x)=g_1^x$，则称该函数为单向同构函数，这里 $x\in Z_p$，g_1 是群 G_1 的一个生成元。文献[12]对该函数给出了更详细的定义，并对其单向性进行了严格的证明。

2.2 安全性定义

文献[13,14]对已知密钥安全、完美前向安全性和密钥泄露伪装攻击进行了定义，本文沿用这些定义。

已知密钥安全(Known Key Security，KKS)：一个协议具有已知密钥安全，是指即使敌手已经知道了除当前会话之外的会话密钥，也不会影响当前会话的安全。这一安全属性已经成为密钥协商的标准需求之一。

完美前向安全性(Perfect Forward Security，PFS)：粗略地说，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，则称该协议具有前向安全性。根据会话性质的不同，前向安全性可分为完美前向安全性和弱的完美前向安全性。具体来说，如果长期私钥泄露前的会话受到了敌手的破坏(该攻击者获得了参与者的长期私钥，并为其选择了这次会话的临时私钥)，而敌手仍无法获得这次会话的会话密钥，则称该协议具有完美前向安全性；若协议只能保证在获得参与者的长期私钥后，之前的那些未被敌手破坏的会话的会话密钥不能被敌手获得，则称该协议具有弱的完美前向安全性。Krawczyk[15]对协议的前向安全性进行了详细研究，指出基于公钥的两轮的双方认证密钥协商协议都无法实现完美前向安全性，而只能实现弱的完美前向安全性。

抗密钥泄露伪装攻击(Key Compromise Impersonation Security，KCIS)：假设实体 A 和 B 是协议的两个参与者，则当 A 的长期私钥被敌手获得后，该敌手显然能够冒充 A 与其他协议的参与者(例如 B)进行通信。然而，如果该协议抗密钥泄露伪装攻击，则这一密钥泄露不能使得敌手反过来向实体 A 冒充为其他参与者(例如 B)。

3 可认证参与者身份的密钥协商

本节我们正式定义可认证参与者身份的密钥协商协议(Sender Authenticated Key Agreement Protocol，SAKAP)，同时定义一个 SAKAP 协议的 (q,t,ε)-KKS 安全性，(q,t,ε)-PFS 安全性和 (q,t,ε)-$KCIS$ 安全性。同时，本节还对协议的安全性提出了两个假设条件。

3.1 SAKAP

定义 1(SAKAP) 对于一个认证密钥协商协议而言，如果参与者知道其自身长期私钥可以被其他参与者甚至是第三方利用收到的信息来确认这一事实，则这一协议就称为 SAKAP 协议。一个 SAKAP 协议通过 5 个阶段实现：

参数生成：输入一个安全参数，输出将公开的共享信息。

密钥生成：将共享信息作为输入，输出一组公私钥对。其中，公钥可以被任何人获取，而私钥只有其拥有者知道。

消息生成：每个参与者将共享信息和自己的私钥作为输入(以及部分或全部参与者的公钥)，并生成协商信息和自己的短期秘密，同时将这一协商的信息发送给其它参与者，将短期秘密保存下来。

验证：将共享信息和协商信息(以及部分或全部参与者的公钥)作为输入，返回正确或者不正确。

密钥协商：每个参与者将各自的协商信息、短期秘密、自己的私钥作为输入(以及部分或全部参与者的公钥)，返回本次会话的会话密钥。

3.2 安全性

本节将通过挑战者 B 和敌手 $\vec{A}$ 之间的游戏定义协议的安全性。

KKS 游戏：令 n 是一个 SAKAP 协议的参与者个数。

起始阶段：挑战者 B 随机选择一个参数 k，并模拟所有参与者执行上述参数生成和密钥生成阶段的步骤，并把由此得到的共享信息和公钥发送给敌手 $\vec{A}$，同时保存每个参与者对应的私钥。

阶段 1：对于 $i=1,2,\cdots q'$，敌手 $\vec{A}$ 请求协商信息 Q_i 以及对应的协商密钥 R_i，这里 $Q_i=(Q_{1i},\cdots Q_{ni})$，其中 Q_{ji} 是第 j 个实体的第 i 个信息。收到请求后，挑战者 B 生成 (Q_i,R_i) 并将其发送给敌手 $\vec{A}$。

挑战：挑战者 B 生成用于挑战的协商信息元组 $Q_*=(Q_{1*},\cdots,Q_{n*})$，这里 Q_{j*} 是第 j 个实体的某个协商信息。B 随机选择 $b_*\in\{0,1\}$，如果 $b_*=1$，则其计算 Q_* 对应的协商密钥 R_*；如果 $b_*=0$，则从协商密钥中随机选择一个作为 R_*，并将 (Q_*,R_*) 发送给敌手 $\vec{A}$。

阶段 2：对于 $i=q'+1,\cdots,q$，敌手 $\vec{A}$ 请求协商信息 Q_i。收到请求后，挑战者 B 生成 Q_i 并将其发送给敌手 $\vec{A}$。

猜测：最后，敌手 $\vec{A}$ 输出自己的猜测值 $b'\in\{0,1\}$，如果 $b'=b_*$，则敌手 $\vec{A}$ 赢得了游戏。

我们定义 $AdvKKS_{\vec{A}}=|\Pr[b_*=b']-\frac{1}{2}|$。

定义 2((q,t,ε)-KKS) 如果敌手 $\vec{A}_{(q,t,\varepsilon)}$ 在最多时间 t 内破坏了 KKS 游戏，A 最多可以请求 q 次对参与者协商信息的查询，且 $AdvKKS_{\vec{A}}$ 至少为 ε。如果没有敌手 $\vec{A}_{(q,t,\varepsilon)}$ 能破坏它，则称该 SAKAP 协议具有 (q,t,ε) 已知密钥安全。

PFS 游戏：假设 n 是一个 SAKAP 协议的参与者数量。

起始阶段：挑战者 B 随机选择一个安全参数 k，执行每个参与者的上述参数生成和密钥生成阶段，并把所有的对应共享信息和参与者公钥都发送给敌手 $\vec{A}$，同时 B 保留所有参与者的私钥。

阶段 1：对于 $i=1,2,\cdots q'$，敌手 $\vec{A}$ 请求协商信息 Q_i 以及对应的协商密钥 R_i，这里 $Q_i=(Q_{1i},\cdots Q_{ni})$，其中 Q_{ji} 是第 j 个实体的第 i 个信息。收到请求后，挑战者 B 生成 Q_i 并将其发送给敌手 $\vec{A}$。

挑战：挑战者 B 生成用于挑战的协商信息元组 $Q_*=(Q_{1*},\cdots,Q_{n*})$，这里 Q_{j*} 是第 j 个实体的某个协商信息。B 随机选择 $b_*\in\{0,1\}$，如果 $b_*=1$，则其计算 Q_* 对应的协商密钥 R_*；如果 $b_*=0$，则从协商密钥中随机选择一个作为 R_*，得到 R_* 后，挑战者 B 将 (Q_*,R_*) 发送给敌手 $\vec{A}$。

阶段 2：对于 $i=q'+1,\cdots,q$，敌手 $\vec{A}$ 请求协商信息 Q_i。收到请求后，挑战者 B 生成 Q_i 并将其发送给敌手 $\vec{A}$。

猜测：最后，敌手 $\vec{A}$ 输出自己的猜测值 $b'\in\{0,1\}$，如果

$b'=b_*$，则敌手 $\vec{A}$ 赢得了游戏。我们定义 $AdvPFS_{\vec{A}}=|Pr[b_*=b']-\frac{1}{2}|$。

定义 3（(q,t,ε)-PFS） 如果敌手 $\vec{A}(q,t,\varepsilon)$ 在最多时间 t 内破坏了 PFS 游戏，$\vec{A}$ 最多可以请求 q 次对参与者协商信息的查询，且 $AdvPFS_{\vec{A}}$ 至少为 ε。如果没有敌手 $\vec{A}(q,t,\varepsilon)$ 能破坏它，则称该 SAKAP 协议具有 (q,t,ε) 绝对前向安全性。

KCIS 游戏：假设 n 是一个 SAKAP 协议的参与者数量。

起始阶段：挑战者 B 随机选择一个安全参数 k，执行每个参与者的上述参数生成和密钥生成阶段，并把所有的对应共享信息和参与者公钥都发送给敌手 $\vec{A}$，同时 B 保留所有参与者的私钥。

阶段：挑战者 B 将某个实体 $l(l\in\{1,2,\cdots,n\})$ 的私钥发送给敌手 $\vec{A}$，对于 $i=1,2,\cdots,q$，敌手 $\vec{A}$ 请求协商信息 Q_i 以及对应的协商密钥 R_i，这里 $Q_i=(Q_{1i},\cdots Q_{ni})$，其中 Q_{ji} 是第 j 个实体的第 i 个信息。收到请求后，挑战者 B 生成 Q_i 并将其发送给敌手 $\vec{A}$。

猜测：最后，敌手 $\vec{A}$ 输出消息 Q_{j*}，如果 $Q_{j*}\notin\{Q_{j1},\cdots,Q_{jq}\}(j\neq l$，且 $j\in\{1,2,\cdots,n\})$，对于某个参与者 j 是正确的，敌手 $\vec{A}$ 赢得了游戏。

我们定义 $AdvKCIS_{\vec{A}}=|\vec{A}$ 赢得了 $KCIS$ 游戏$|$。

定义 4（(q,t,ε)-$KCIS$） 如果敌手 $\vec{A}(q,t,\varepsilon)$ 在最多时间 t 内破坏了 $KCIS$ 游戏，$\vec{A}$ 最多可以请求 q 次对参与者协商信息的查询，且 $AdvKCIS_{\vec{A}}$ 至少为 ε。如果没有敌手 $\vec{A}(q,t,\varepsilon)$ 能破坏它，则称该 SAKAP 协议具有抗密钥泄露伪装攻击性。

4 新协议

如前所述，本文提出的三方可认证参与者身份的密钥协商协议将按照 3.1 中的定义分 5 个阶段。

参数生成：对于生成元 $g_2\in G_2$ 和 $g_1:=f(g_2)\in G_1$，假设 $\hat{E}:=e(g_1,g_2)$。令 $(G_1,G_1,G_T,p,e,f,g_1,g_2,\hat{E})$ 是共享信息。

密钥生成：令 A、B 和 C 是协议的 3 个参与者，参与者 A 生成一个长期私钥 $S_A=g_2^a\in G_2$，这里 $a\in_R Z_p^*$。计算 $P_A:=f(g_2^a)(=g_1^a\in G_1)$ 作为长期私钥。这里，P_A 已经被可信第三方(TTP)认证。类似地，参与者 B 和 C 也进行类似的运算，从而得到如下结论：

参与者 A：公钥 $P_A:=g_1^a$；私钥 $S_A=g_2^a$

参与者 B：公钥 $P_B:=g_1^b$；私钥 $S_B=g_2^b$

参与者 C：公钥 $P_C:=g_1^c$；私钥 $S_C=g_2^c$

消息生成：实体 A 使用某个短期秘密 $r_A\in Z_p^*$ 生成一个消息：$(A_1,A_2):=(g_2^{r_A},S_A^{-1}\cdot g_2^{1/r_A})(=(g_2^{r_A},g_2^{-a+1/r_A}))$，并将 (A_1,A_2) 发送给实体 B 和 C。类似地，B 将 (B_1,B_2) 发送给实体 A 和 C；C 将 (C_1,C_2) 发送给实体 A 和 B。如下所示：

$A\rightarrow B,C:(A_1,A_2):=(g_2^{r_A},g_2^{-a+1/r_A})$

$B\rightarrow A,C:(B_1,B_2):=(g_2^{r_B},g_2^{-b+1/r_B})$

$C\rightarrow A,B:(C_1,C_2):=(g_2^{r_C},g_2^{-c+1/r_C})$

验证：实体 A 使用从 B 和 C 处得到的 (B_1,B_2) 和 (C_1,C_2) 验证 $e(P_Bf(B_2),B_1)\stackrel{?}{=}e(P_Cf(C_2),C_1)\stackrel{?}{=}\hat{E}(e(g_1,g_2))$，如果两个等式都成立，则输出 $valid$，否则输出 $invalid$，类似地，B 和 C 也做如下验证：

$$A:e(P_Bf(B_2),B_1)\stackrel{?}{=}e(P_Cf(C_2),C_1)\stackrel{?}{=}\hat{E}$$

$$B:e(P_Cf(C_2),C_1)\stackrel{?}{=}e(P_Af(A_2),A_1)\stackrel{?}{=}\hat{E}$$

$$C:e(P_Af(A_2),A_1)\stackrel{?}{=}e(P_Bf(B_2),B_1)\stackrel{?}{=}\hat{E}$$

密钥协商：实体 A 利用 r_A、B_1 和 C_1 计算会话密钥：$Z_A:=e(f(B_1),(C_1)^{r_A})$。类似地，$B$ 和 C 计算：

$A:Z_A:=e(f(B_1),(C_1)^{r_A})$

$B:Z_B:=e(f(C_1),(A_1)^{r_B})$

$C:Z_C:=e(f(A_1),(B_1)^{r_A})$

显然，$Z_{ABC}=Z_A=Z_B=Z_C=e(g_1,g_2)^{r_Ar_Br_C}$

5 讨论

本节讨论方案的安全性和性能。

5.1 安全性

本节将证明新方案满足已知密钥安全、完全前向安全性，并可以抵抗密钥泄露伪装攻击。

定理 1 新方案满足已知密钥安全性。

证明（反证法）：假设存在一个算法 A'，可以破坏新 SAKAP 协议的 (q,t,ε)-KKS。如前所述，我们可以让敌手 $\vec{A}$ 模拟 KKS 游戏中的挑战者，利用其持有的

$$(G_1,G_2,G_T,p,e,f,g_1,g_2,\hat{E}) \tag{1}$$

为 3 个参与者 A、B 和 C 生成公私钥对：

$$\begin{cases}(P_A,S_A):=(f(g_2^a),g_2^a),\text{对于 } a\in_R Z_P^*\\(P_B,S_B):=(f(g_2^b),g_2^b),\text{对于 } b\in_R Z_P^*\\(P_C,S_C):=(f(g_2^c),g_2^c),\text{对于 } c\in_R Z_P^*\end{cases} \tag{2}$$

并将 $(G_1,G_2,G_T,p,e,f,g_1,g_2,\hat{E})$ 和 (P_A,P_B,P_C) 发送给 A'。对于 $r_{Ai},r_{Bi},r_{Ci}\in_R Z_p^*$，敌手 $\vec{A}$ 计算协商信息：

$$\begin{cases}Q_{Ai}:=g_2^{r_{Ai}},S_A^{-1}\cdot g_2^{1/r_{Ai}}\\Q_{Bi}:=g_2^{r_{Bi}},S_B^{-1}\cdot g_2^{1/r_{Bi}}\\Q_{Ci}:=g_2^{r_{Ci}},S_C^{-1}\cdot g_2^{1/r_{Ci}}\end{cases} \tag{3}$$

以及协商密钥

$$R_i:=e(g_1,g_2)^{r_{Ai}r_{Bi}r_{Ci}} \tag{4}$$

并将其发送给 A'。同时，敌手 $\vec{A}$ 还要生成挑战信息和挑战密钥：

$$\begin{cases}Q_{A*}:=g_2^{r_A},S_A^{-1}\cdot g_2^{1/r_A}\\Q_{B*}:=g_2^{r_B},S_B^{-1}\cdot g_2^{1/r_B}\\Q_{C*}:=g_2^{r_C},S_C^{-1}\cdot g_2^{1/r_C}\\R_*:=R\end{cases} \tag{5}$$

并将其发送给 A'。之后，敌手 $\vec{A}$ 生成 (Q_{Ai},Q_{Bi},Q_{Ci}) 并将其发送给 A' 这里 $i=q'+1,\cdots,q$。

在 KKS 游戏的猜测阶段，敌手 $\vec{A}$ 已经收到了来自 A' 的 $b'\in\{0,1\}$，之后敌手 $\vec{A}$ 输出 b' 作为对概率 $\geqslant\varepsilon$ 的 KKS 安全假设的回应。但显然，这与 (t_0,ε_0)-KKS 假设是相矛盾的。从而，定理得证。

定理 2 方案满足绝对前向安全性。

证明（反证法）：假设存在一个算法 A'，可以破坏新 SAKAP 协议的 (q,t,ε)-PFS。如前所述，我们可以让敌手 $\vec{A}$ 模拟 PFS 游戏中的挑战者。利用定理 1 中的共享信息(1)，敌手 $\vec{A}$ 生成公私钥对(2)，协商信息(3)$(i=1,\cdots,q)$，协商密

钥(4)($i=1,\cdots,q'$)以及挑战信息和挑战密钥(5),并以 PFS 游戏规定的方式将其发送给算法 A'。在 PFS 游戏的猜测阶段,敌手 $\vec{A}$ 已经收到了来自 A' 的 $b'\in\{0,1\}$,之后敌手 $\vec{A}$ 输出 b' 作为对概率 $\geqslant\varepsilon$ 的 PFS 安全假设的回应。但显然,这与 (t_0,ε_0)-PFS 假设是相矛盾的。从而,定理得证。

定理 3　协议可以抵抗密钥泄露伪装攻击。

证明(反证法):假设存在一个算法 A',可以破坏新 SAKAP 协议的 (q,t,ε)-$KCIS$。如前所述,可以让敌手 $\vec{A}$ 模拟 KCIS 游戏中的挑战者。敌手 $\vec{A}$ 随机选择 $c_*\in\{0,1,2\}$,并生成 3 个实体 A、B 和 C 的公私钥对,如果 $c_*=0$,计算:

$$\begin{cases}(P_A,S_A):=((g_1^x),-)\\(P_B,S_B):=(f(g_2^b),g_2^b),\text{对于 } b\in_R Z_P^*\\(P_C,S_C):=(f(g_2^c),g_2^c),\text{对于 } c\in_R Z_P^*\end{cases}\tag{6}$$

如果 $c_*=1$,计算:

$$\begin{cases}(P_A,S_A):=(f(g_2^a),g_2^a),\text{对于 } a\in_R Z_P^*\\(P_B,S_B):=((g_1^x),-)\\(P_C,S_C):=(f(g_2^c),g_2^c),\text{对于 } c\in_R Z_P^*\end{cases}$$

如果 $c_*=2$,计算:

$$\begin{cases}(P_A,S_A):=(f(g_2^a),g_2^a),\text{对于 } a\in_R Z_P^*\\(P_B,S_B):=(f(g_2^b),g_2^b),\text{对于 } b\in_R Z_P^*\\(P_C,S_C):=((g_1^x),-)\end{cases}$$

以 $c_*=0$ 为例,敌手 $\vec{A}$ 将共享信息式(1)和式(6)中的 (P_A,P_B,P_C) 发送给 A'然后,敌手 $\vec{A}$ 随机选择 $d'\in\{0,1\}$,如果 $d'=0$,则将 S_B 发送给 A',如果 $d'=1$,则将 S_C 发送给 A'。之后,以 $d'=1$ 为例,对于 $i=1,\cdots,q$ 敌手 $\vec{A}$ 生成

$$\begin{cases}Q_{Ai}:=g_2^{r_i},g_2^{x+1/r_i}\\Q_{Bi}:=g_2^{r_{Bi}},S_B^{-1}\cdot g_2^{1/r_{Bi}},\text{对于 } r_{Bi}\in_R Z_p^* \text{ 并将其发送给 } A'。\\Q_{Ci}:=g_2^{r_{Ci}},S_C^{-1}\cdot g_2^{1/r_{Ci}},\text{对于 } r_{Ci}\in_R Z_p^*\end{cases}$$

在 $KCIS$ 游戏的猜测阶段,敌手 $\vec{A}$ 收到来自 A' 的协商协议 Q_*,在 SAKAP 协议的验证阶段,Q_* 对于 A 或 C 是正确的。如果 Q_* 对于 C 是正确的,敌手 $\vec{A}$ 放弃该游戏。否则,这意味着存在 $r_*\in Z_p^*$ 使得 $r_*\notin\{r_1,\cdots,r_q\}$ 且 $Q_*=g_2^{r*}$,g_2^{x+1/r_*}。之后敌手 $\vec{A}$ 输出 Q_* 作为对概率 $\geqslant\varepsilon$ 的 KCIS 安全假设的回应。但显然,这是与 (q_0,t_0,ε_0)-$KCIS$ 假设是相矛盾的。从而,定理得证。

表 1 是新协议与最近提出的文献[9,10]的安全性比较,可以看出,这两个协议都不满足绝对前向安全性和抗密钥泄露伪装攻击。

表 1　方案的安全性比较

	已知密钥安全	完美前向安全性	抗密钥泄露伪装攻击
文献[9]	否	否	否
文献[10]	否	否	否
新协议	是	是	是

5.2　性能比较

除了安全性,方案的性能也是影响协议能否大规模推广的一个重要因素,如表 2 所列,尽管新方案使用了单向同构函数,但并未使用 Hash 函数,而且,新协议的模指数运算的量也远远小于其它两个方案。据我们所知,一次模指数运算的计算资源消耗量是远远大于其它运算的。

表 2　方案的计算量比较

	双线性映射 e	G_1 和 G_2 上的模指数运算	G_T 上的模指数运算	Hash 运算 H	单向同构函数 f
文献[9]	5(0+4+1)	5(3+2+0)	1(0+0+1)	3(1+2+0)	0(0+0+0)
文献[10]	3(0+2+1)	5(3+2+0)	1(0+0+1)	3(1+2+0)	0(0+0+0)
新协议	3(0+2+1)	2(2+0+0)	1(0+0+1)	0(0+0+0)	3(0+2+0)

结束语　三方密钥协商是多方密钥协商的基础。本文探索研究了可认证参与者身份的三方密钥协商协议,并在标准模型下进行了严格的形式化证明。与现有的类似方案相比,新方案的安全性和性能都具有一定的优势。

构建满足认证参与者身份性质的多方密钥协商是本研究的一个重要延伸方向,与三方协议不同,这类协议需要考虑成员的加入和退出问题,这是一个非常值得研究的方向。

参 考 文 献

[1] Joux A. A one round protocol for tripartite Diffie-Hellman[J]. ANTS. LNCS1838, Springer-Verlag, 2000: 385-394

[2] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings[J]. IEEE Computer Society Press, CS-FW-16, 2003: 219-233

[3] 游子毅,谢晓尧. 一种基于第三方认证的无线组密钥协商协议[J]. 计算机应用研究,2011(1):34-37

[4] 李海峰,蓝才会,左为平,等. 独立网络中新的双方密钥协商协议[J]. 计算机应用,2013(5):138-141

[5] Nalla D, Reddy K C. ID-based tripartite authenticated key agreement protocols from pairings[R]. Cryptology ePrint Archive, Report 2003/004, 2003. http://eprint.iacr.org/

[6] Nyberg K. On one-pass authenticated key establishment schemes[C]// Selected Areas in Cryptography(SAC'95). 1995: 2-8

[7] Choie Y J, Jeong E, Lee E. Efficient identity-based authenticated key agreement protocol from pairings[J]. Appl. Math. Comput., 2005, 162(1): 179-188

[8] Popescu C. A secure key agreement protocol using elliptic curves [J]. Int. J. Comput. Appl., 2005, 27(3): 147-152

[9] Zhang F, Liu S, Kim K. ID-based one-round authenticated tripartite key agreement protocol with pairings[C]// 2003 IEEE International Symposium on Information Theory, Yokohama, Japan, 2003

[10] Shim K. Cryptanalysis of ID-based tripartite authenticated key agreement protocols[R]. Cryptology ePrint Archive, Report 2003/115, 2003. http://eprint.iacr.org/

[11] Du X, Wang Y, Ge J, et al. ID-based authenticated two round multi-party key agreement[R]. Cryptology ePrint Archive, Report 2003/247, 2003. http://eprint.iacr.org/

[12] Hoshino S F, Uchiyama S, Kobayashi T. Candidate one-way functions on non-super singular elliptic curves [J]. IEICE Trans. Fundamentals, 2006, E89-A(1): 144-150

[13] Yacobi Y, Shmuely Z. On key distribution systems [M]. Crypto1989. LNCS, Berlin: Springer, 1989, 435: 344-355

[14] Yacobi Y. A key distribution "paradox" [M]// Crypto 1990, LNCS, Berlin: Springer, 1990, 537: 268-273

[15] Krawczyk H. HMQV: a high-performance secure Diffie-Hellman protocol[M] // Crypto 2005. LNCS, Berlin: Springer, 2005, 3621: 546-566