计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191100216

一种基于无证书的 SIP 认证密钥协商协议

莫天庆[1]　何咏梅[2]
1 武警重庆总队通信大队　重庆 404100
2 武警西藏总队通信大队　拉萨 850000

摘　要　针对现有 SIP(会话初始协议)认证机制不能抵抗临时秘密泄露攻击和系统开销大的问题,提出了一种基于改进 SIP 协议的 SIP 安全认证模型。借鉴原有协议流程,设计了一种强安全的 SIP 两方匿名认证密钥协商子协议。新协议利用无证书签密的特性实现通信实体的双向认证、密钥协商和不可追踪。在现有 seCK(不仅包含 eCK 模型,而且捕捉了临时中间泄露抵抗的安全性)模型下对新协议进行了安全性证明,其安全性被规约为多项式时间敌手求解 CDH 问题。与现有同类协议相比,新协议只需 7 次点乘运算和 3 次消息交互,具有安全性更强、计算和通信开销较低的特点。

关键词:认证密钥协议;SIP;可证明安全;无证书签密
中图法分类号　TP393

SIP Authentication Key Agreement of Protocol Based on Certificateless

MO Tian-qing[1] and HE Yong-mei[2]
1 Communication Regiment of PAP Chongqing Corps,Chongqing 404100,China
2 Communication Regiment of PAP Xizang Corps,Lhasa 850000,China

Abstract　The existing authentication schemes for SIP do not resist the attack of ephemeral secrets reveal,and have high system costs. A safe communicated model of SIP network based on improved SIP was proposed. Basing on the primary flow of SIP and combing with certificateless signcryption,a new anonymous two-party authenticated key agreement protocol was adopted to achieve mutual authentication and unlinkability. Furthermore,the new protocol is provably secure in the seCK model under the CDH assumption. Comparative analysis results show that our protocol is very simple and efficient.

Keywords　Authentication key agreement,SIP,Provably secure,Certificateless signcryption

1　引言

IMS(IP Multimedia Subsystem)是下一代网络的目标演进方向。SIP 协议是 IMS 网络的核心控制协议,用于建立、修改、终止多媒体会话[1]。但 SIP 协议自身缺少安全性设计,在实际使用时存在很多安全隐患。目前,主要依靠 HTTP Digest Authentication 机制、TLS 协议、S/MIME 协议以及 IPSec 协议来保护通信信令。然而,这些机制存在管理难度大、不能提供双向认证和密钥协商功能的缺陷。因此,对 SIP 的安全机制进行研究是很有必要的。

目前,国内外认可的可用于保障 SIP 协议安全的机制有数据加密机制和身份认证机制[2]。为了增强 SIP 通信安全,Si 等[3]从理论角度提出了一些相关的安全策略。文献[4]通过扩展 SIP 消息头域,利用新增字段,在原有 HTTP 摘要认证机制的基础上提出了一种改进的基于 hash 运算的 SIP 双向动态密钥认证机制。但该方案不仅需要预先共享初始密钥,而且需要用前一次随机数加密本次随机数,具有一定的安全隐患。文献[5-8]中的协议大量使用了公钥加密和数字签名技术,存在基于 PKI 体系证书管理复杂的问题。文献[9]基于椭圆曲线 DL 问题,提出了一种基于 ECDLP 的 SIP 认证密钥协商协议,但该协议的安全性没有得到形式化证明。Wen 等[10]、Li[11]提出的方案都是基于双线性映射设计的,在效率上有较大的缺陷。文献[12]的协议没有使用双线性对运算,但该方案的安全性是在较弱的安全模型(CK(Canetti-Krawczyk)模型)下进行证明的,没有考虑会话临时秘密泄露攻击。

基于上述分析,本文提出了一种基于改进 SIP 协议的 SIP 安全认证模型,在原有协议的基础上,首次引入无证书签密技术,设计了一种适用于 SIP 的两方匿名认证密钥协商子协议,并在现有 seCK 模型下对其安全性进行了形式化证明。

2　相关知识

2.1　困难问题与假设

CDH 问题:群 G 是阶为素数 $q(q>2^k)$ 的循环群,$P\in G$ 是群 G 的生成元,对于任意未知的 $a,b\in Z_q^*$,给定(aP,bP),计算 abP。

CDH 假设:不存在概率多项式时间算法能成功求解 CDH 问题。

2.2　安全定义和安全模型

根据文献[13-15]关于可证安全的无证书密钥协商的研究,下面先简要描述相关概念和定义。

无证书认证密钥协商协议由 PPT 算法六元组组成:(1)建立系统参数(Setup);(2)生成部分私钥(PartialPrivateKeyExtract);(3)设置秘密值(SetSecretValue);(4)设置

通信作者:莫天庆(motianqing11@163.com)

私钥(SetPrivateKey);(5)设置公钥(SetPublicKey);(6)密钥协商(KeyAgreement)。

seCK 模型包括一个协议参与者集合 U,每一个参与者被模拟为一组预言机。假定参与者 i 持有身份 ID_i,预言机 $\Pi_{i,j}^t$ 表示参与者 i 与目标伙伴 j 进行第 t 次密钥协商;一个主动攻击者 $\mathcal{A}\in\{\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}}\}$,其中 $\mathcal{A}_{\mathrm{I}}$ 不知道系统主密钥但能替换任意用户的公钥,$\mathcal{A}_{\mathrm{II}}$ 知道系统主密钥但不能替换用户的公钥。攻击者被定义为一个概率多项式时间图灵机,能访问所有的预言机,模型将攻击者的能力抽象为对预言机的查询。攻击者除了可以进行 eCK 模型中的所有查询外,还可以执行 *ReplacePublicKey*$(i, PK_i^{\mathcal{A}})$, *MasterKeyReveal*, *PartialPrivateKeyReveal*(i), *SecretValueReveal*(i)。具体的查询过程以及会话标识符 *SID*、诚实用户、攻击者获胜优势 $Adv_{\mathcal{A}}(k)$、匹配预言机和新鲜预言机的定义参见文献[13]。

定义 1(密钥协商安全) 当一个无证书认证密钥协商协议同时满足以下两个条件时,我们称该无证书认证密钥协商协议是安全的。

(1)两个互相匹配的会话状态都是诚实的且输出两个相同的会话密钥,两个参与者都没有被执行过 *ReplacePublicKey*$(i, PK_i^{\mathcal{A}})$查询。

(2)$Adv_{\mathcal{A}}(k)$是可忽略的。

2.3 一种基于改进 SIP 协议的 SIP 安全认证模型

SIP 是基于文本的信令协议。SIP 网络的通信归结起来就是建立一通话一结束的过程。保证 SIP 通信的安全,实质上就是确保信令的安全和媒体流的安全。文献[6]提出了基于 SIP 网络的安全通信模型。为了消除基于 PKI 的证书管理问题,本节提出了一种基于改进 SIP 协议的 SIP 安全认证模型(见图 1)。

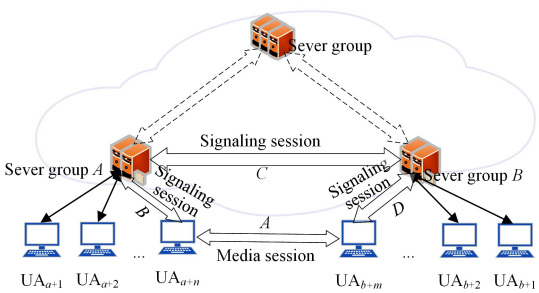

图 1 SIP 安全认证模型

Fig. 1 Safe communicated model of SIP

在本模型中,UA(Users Agent)为用户代理,UA$_{a+n}$为发送方(用 U_a 表示),UA$_{b+m}$为接收方(用 U_b 表示);Sever group A 和 Sever group B 可以实现代理服务器(Proxy)和注册服务器(Registrar)的功能;Sever group 具有 KGC(密钥生成中心)并可以实现重定向服务器(Redirect)和位置服务器(Location Sever)的功能。SIP 利用消息头和消息体来实现信令和多媒体的点到点安全和端到端安全。图 1 中,在路径 A 中需要实现端到端的安全,在路径 B,C,D 上需要实现每一跳的点到点安全。路径 B 和 D 使用 HTTP Digest Authentication 来确保安全;路径 C 的安全性由 IPSec 和 TLS 来完成;路径 A 中的端到端用户的身份认证和安全密钥协商,仅在 SIP 消息头域中设置密话标识,将密钥消息以利用无证书签密技术加密的消息体进行传递,从而为后续的媒体流的机密传输提供保障。

3 一种强安全的 SIP 两方匿名认证密钥协商协议及其安全证明

3.1 一种强安全的 SIP 两方匿名认证密钥协商协议

新协议包含系统建立、节点注册、身份认证及密钥协商 3 个算法。其中,节点注册算法综合了 *PartialPrivateKeyExtract*, *SetSecretValue*, *SetPrivateKey* 以及 *SetPublicKey*。

(1)系统建立

输入安全参数 k,KGC 产生并发布安全参数$\{G, q, P, P_{\mathrm{pub}}, H_0, H_1, H_2, H_3\}$。

其中,群 G 是阶为素数 $q(q>2^k)$的循环群,$P\in G$ 是群 G 的生成元,$P_{\mathrm{pub}}=s\cdot P$ 是 KGC 的公钥,随机数 $s\in Z_q^*$ 是系统主密钥,$H_0:\{0,1\}^n\times G\rightarrow G$, $H_1:\{0,1\}^n\times G\times G\rightarrow Z_q^*$, $H_2: G\times G\rightarrow Z_q^*$ 为碰撞哈希函数,$H_3:\{0,1\}^n\times\{0,1\}^n\times G\times G\times G\times G\times G\rightarrow\{0,1\}^k$为密钥导出函数。

(2)节点注册

用户 ID_u 随机选取 $c_u\in Z_q^*$,计算公开参数 $C_u=c_u\cdot P$, $R_u=H_0(ID_u, C_u)$,将(ID_u, R_u)发送给 KGC。

给定用户的身份标识 ID_u 和公开参数 R_u,KGC 选择随机数 $t_u\in Z_q^*$,计算 $W_u=t_u\cdot P$, $w_u=t_u+s\cdot H_1(ID_u, R_u, W_u)$;将 W_u 和 w_u 通过安全信道发送给用户 ID_u。

用户通过验证等式 $w_u\cdot P=W_u+P_{\mathrm{pub}}\cdot H_1(ID_u, R_u, W_u)$是否成立来确定 W_u 和 w_u 的有效性。若该等式成立,选择随机数 $x_u\in Z_q^*$,计算 $y_u=x_u\cdot P$。用户 ID_u 的公钥为 $Q_u=(C_u, y_u, W_u)$,私钥为 $Ce_u=(c_u, x_u, w_u)$。

(3)身份认证及密钥协商

在 SIP 协议中,身份为 ID_a 的发送方 A 与身份为 ID_b 的接收方 B 之间的消息交互及密钥协商过程如图 2 所示。

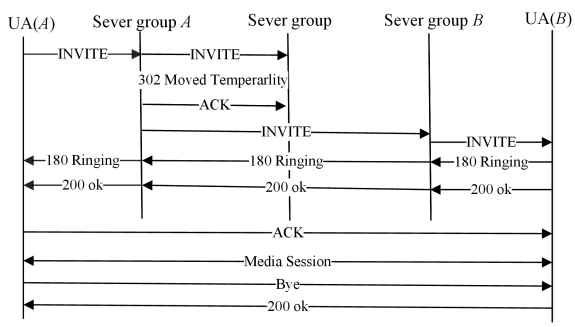

图 2 呼叫建立认证与密钥协商图

Fig. 2 SIP authenticated call establishment flow and key agreement

本文主要利用基于无证书签密技术来解决用户代理 UA(A)和用户代理 UA(B)之间的身份认证和密钥协商,发送方与其所在域服务器组(Sever group A)、接收方与其所在域服务器组(Sever group B)以及 Sever group A 和 Sever group B 之间消息的安全传输不再赘述。$\alpha\rightarrow\beta:\langle M\rangle$ 表示通信实体 α 向通信实体 β 发送消息 M。另外,由于媒体流通信对速度要求较高,因此在完成密钥协商后,采用对称加密算法来保证其安全通信。协议的具体流程如下:

(1)A 向 B 发起 *INVITE* 消息。

$A\rightarrow$Sever group $A: M_1=\langle INVITE \| CMS1\rangle$

1)A 选取随机数 $k_1, k_2\in Z_q^*$,计算 $\upsilon=\dfrac{k_1}{(c_a+w_a)}$;

2)计算 $h_b=H_1(ID_b, C_b, W_b)$, $\tau=k_2\cdot(C_b+W_b+P_{\mathrm{pub}}\cdot h_b)$, $Y=H_2(k_1\cdot P, k_2\cdot P)$, $S=Y\cdot y_a$, $V=Y\cdot x_a\cdot y_b$;

3)计算$h_2=H_2(S,V)$;

4)将(υ,τ,h_2)置入到 S/MIME 协议的消息体 *CMS*1 中。

(2)B 收到 *INVITE* 消息并进行验证后,发送 200 OK 给 A。

$B\rightarrow A:M_2=\langle 200\ \mathrm{OK}\parallel CMS2\rangle$

1)B 先获取 *CMS*1 中的消息(υ,τ,h_2),利用私钥Ce_b和用户 A 的公钥Q_a计算$h_a=H_1(ID_a,C_a,W_a)$;$Y=H_2\left(\upsilon\cdot(C_a+W_a+P_{\mathrm{pub}}\cdot h_a),\frac{\tau}{(c_b+w_b)}\right)$;

2)计算 $S=Y\cdot y_a$;

3)验证等式$h_2=H_2(S,S\cdot x_b)$是否成立。若成立,说明请求是 A 发出的且消息没有被篡改,B 选择随机数$n_1,n_2\in Z_q^*$,计算$\upsilon'=\frac{n_1}{(c_b+w_b)}$,$h_a=H_1(ID_a,C_a,W_a)$,$\tau'=n_2\cdot(C_a+W_a+P_{\mathrm{pub}}\cdot h_a)$,$Y'=H_2(n_1\cdot P,n_2\cdot P)$,$S'=Y'\cdot y_b$,$V'=Y'\cdot x_b\cdot y_a$,$h_2'=H_2(S',V')$。

4)计算共享密钥$K_{b1}=n_1\cdot\upsilon\cdot(C_a+W_a+P_{\mathrm{pub}}\cdot h_a)$;$K_{b2}=n_2\cdot\frac{\tau}{(c_b+w_b)}$;$K_{b3}=n_2\cdot P+\frac{\tau}{(c_b+w_b)}$;$K_{b4}=S\cdot x_b+Y'\cdot x_b\cdot y_a$;$K_{b5}=x_b\cdot C_a$;$K_{b6}=c_b\cdot C_a$;$K_{b7}=c_b\cdot y_a$;计算会话密钥$SK_{ba}=H_3(ID_a\parallel ID_b\parallel K_{b1}\parallel K_{b2}\parallel K_{b3}\parallel K_{b4}\parallel K_{b5}\parallel K_{b6}\parallel K_{b7})$。

5)将(υ',τ',h_2')置入到 S/MIME 协议的消息体 *CMS*2 中,给 A 回应一个 200 OK 消息。

(3)$A\rightarrow B:\langle\mathrm{ACK}\rangle$

A 先获取 *CMS*2 中的(υ',τ',h_2'),并用私钥Ce_a以及用户 B 的公钥Q_b,计算$Y'=H_2\left((\upsilon'\cdot(C_b+W_b+P_{\mathrm{pub}}\cdot h_b),\frac{\tau'}{(c_a+w_a)}\right)$,$S'=Y'\cdot y_b$。验证$h_2'=H_2(S',S'\cdot x_a)$是否成立。若成立,计算共享密钥:$K_{a1}=k_1\cdot\upsilon'\cdot(C_b+W_b+P_{\mathrm{pub}}\cdot h_b)$;$K_{a2}=k_2\cdot\frac{\tau'}{(c_a+w_a)}$;$K_{a3}=k_2\cdot P+\frac{\tau'}{(c_a+w_a)}$;$K_{a4}=Y\cdot x_a\cdot y_b+S'\cdot x_a$;$K_{a5}=c_a\cdot y_b$;$K_{a6}=c_a\cdot C_b$;$K_{a7}=x_a\cdot C_b$。计算会话密钥$SK_{ab}=H_3(ID_a\parallel ID_b\parallel K_{a1}\parallel K_{a2}\parallel K_{a3}\parallel K_{a4}\parallel K_{a5}\parallel K_{a6}\parallel K_{a7})$。发送确认消息 ACK 给 B,并利用SK_{ab}开始会话。

密钥的一致性证明如下:

$(1)K_{b1}=n_1\cdot\upsilon\cdot(C_a+W_a+P_{\mathrm{pub}}\cdot h_a)$

$=n_1\cdot\upsilon\cdot[c_a\cdot P+(W_a+P_{\mathrm{pub}}\cdot h_a)]$

$=n_1\cdot\frac{k_1}{(c_a+w_a)}\cdot(c_a\cdot P+w_a\cdot P)=n_1\cdot k_1\cdot P$

$K_{a1}=k_1\cdot\upsilon'\cdot(C_b+W_b+P_{\mathrm{pub}}\cdot h_b)=k_1\cdot n_1\cdot P$

$\because n_1\cdot k_1\cdot P=k_1\cdot n_1\cdot P$

$\therefore K_{b1}=K_{a1}$

$(2)K_{b2}=n_2\cdot\frac{\tau}{(c_b+w_b)}=n_2\cdot\frac{k_2\cdot(C_b+W_b+P_{\mathrm{pub}}\cdot h_b)}{(c_b+w_b)}$

$=n_2\cdot\frac{k_2\cdot[c_b\cdot P+(W_b+P_{\mathrm{pub}}\cdot h_b)]}{(c_b+w_b)}$

$=n_2\cdot\frac{k_2}{(c_b+w_b)}\cdot(c_b\cdot P+w_b\cdot P)$

$=n_2\cdot k_2\cdot P$

$K_{a2}=k_2\cdot\frac{\tau'}{(c_a+w_a)}$

$=k_2\cdot\frac{n_2\cdot[c_a\cdot P+(W_a+P_{\mathrm{pub}}\cdot h_a)]}{(c_a+w_a)}$

$=k_2\cdot\frac{n_2}{(c_a+w_a)}\cdot(c_a\cdot P+w_a\cdot P)=k_2\cdot n_2\cdot P$

$\because n_2\cdot k_2\cdot P=k_2\cdot n_2\cdot P$

$\therefore K_{b2}=K_{a2}$

$(3)K_{b3}=n_2\cdot P+\frac{\tau}{(c_b+w_b)}=n_2\cdot P+k_2\cdot P$

$K_{a3}=k_2\cdot P+\frac{\tau'}{(c_a+w_a)}=k_2\cdot P+n_2\cdot P$

$\because n_2\cdot P+k_2\cdot P=k_2\cdot P+n_2\cdot P$

$\therefore K_{b3}=K_{a3}$

$(4)K_{b4}=S\cdot x_b+Y'\cdot x_b\cdot y_a$

$=Y\cdot y_a\cdot x_b+Y'\cdot x_b\cdot y_a$

$=(Y+Y')\cdot x_b\cdot x_a\cdot P$

$K_{a4}=Y\cdot x_a\cdot y_b+S'\cdot x_a$

$=Y\cdot x_a\cdot y_b+Y'\cdot y_b\cdot x_a$

$=(Y+Y')\cdot x_a\cdot x_b\cdot P$

$\because(Y+Y')\cdot x_b\cdot x_a\cdot P=(Y+Y')\cdot x_a\cdot x_b\cdot P$

$\therefore K_{b4}=K_{a4}$

$(5)K_{b5}=x_b\cdot C_a=x_b\cdot c_a\cdot P=c_a\cdot x_b\cdot P$

$=c_a\cdot y_b=K_{a5}$

同理可证$K_{b6}=K_{a6}$,$K_{b7}=K_{a7}$。

综合(1)-(5)可知:$SK_{ba}=SK_{ab}$

3.2 新协议的形式化证明及效能分析

3.2.1 安全性证明

k 是安全参数,$H_i(i\in\{0,\cdots,3\})$是随机预言机。假设攻击者 $\mathcal{A}\in\{\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}}\}$最多可以激活 $n(k)$个诚实用户,且最多可发起 $s(k)$次会话。假设 $\mathcal{A}$在游戏中具有一定的优势,且可以访问随机预言机H_i,那么挑战者 C 利用 $\mathcal{A}$可以区分正确密钥与随机数的能力来解决 CDH 问题。

定理 1 $\mathcal{T}$是 2.1 节的协议,如果 $\mathcal{A}$以不可忽略的概率攻破协议 $\mathcal{T}$,那么一定存在一个挑战者 C 以一定的优势解决 CDH 问题。$\mathcal{A}$成功的概率为:

$Adv^{\mathcal{A}}\leqslant 9\,n(k)^2s(k)Adv^{C}(k)[\mathrm{CDH}]$

在文献[14]的 seCK 模型中,协议参与者只要有一个秘密值没有泄露,协议都是安全的。通过猜测攻击者 $\mathcal{A}$不知道的信息,挑战者 C 嵌入相应的困难性问题。我们可以把协议的安全性证明分为以下情况:

情况 1 攻击者不知道用户 A 和用户 B 的秘密私钥;

情况 2 攻击者不知道用户 A 和用户 B 的临时私钥;

情况 3 攻击者不知道用户 A 的秘密私钥和用户 B 的临时私钥;

情况 4 攻击者不知道用户 B 的秘密私钥和用户 A 的临时私钥;

情况 5 攻击者不知道用户 A 的部分私钥和用户 B 的秘密私钥;

情况 6 攻击者不知道用户 B 的部分私钥和用户 A 的秘密私钥;

情况 7 攻击者不知道用户 A 的部分私钥和用户 B 的临时私钥;

情况 8 攻击者不知道用户 B 的部分私钥和用户 A 的临时私钥;

情况 9 攻击者不知道用户 A 和用户 B 的部分私钥。

在游戏开始前,挑战者 C 猜测攻击者 $\mathcal{A}$要进行 Test 查询的预言机。C 在 $n(k)$个成员中随机选择 2 个不同成员 $i\in\{1,\cdots,n(k)\}$和 $j\in\{1,\cdots,n(k-1)\}$,C 猜测成功的概率为 $\frac{1}{n(k)n(k-1)}>\frac{1}{n(k)n(k)}$。然后,$C$ 选择 $t\in\{1,\cdots,s(k)\}$,确

定要进行 Test 查询的预言机$\Pi_{i,j}^{t}$。C 猜对预言机的概率大于$\frac{1}{n(k)^2 s(k)}$。最后，C 从上面 9 种情况中选择一种来与攻击者游戏，从而解决 CDH 困难问题。C 如果没有选对预言机或它没有选对情况，则退出游戏。因此，C 不退出游戏的概率大于$\frac{1}{9\,n(k)^2 s(k)}$。在接下来的每种情况的证明中，C 都猜测 $\mathcal{A}$ 要进行 Test 查询的预言机是 $\Pi_{i,j}^{t}$。

(1)情况 1 的安全性分析

证明：假设挑战者 C 想解决 G 中的 CDH 困难问题，挑战值是(up, vp)，它需要借助攻击者的能力计算 uvp。

C 随机选择系统主密钥 $s \in Z_q^*$，计算 $P_{pub} = s \cdot P$，设置系统参数为 $\{G, q, P, P_{pub}, H_0, H_1, H_2, H_3\}$，将其发送给 $\mathcal{A}$，$H_i (i \in \{0, \cdots, 3\})$是随机预言机。

H_0查询：C 维护一张初始值为空的列表H_0^{list}，每一项的格式为$(ID, C_{ID}, c_{ID}, R_{ID})$。当 C 收到攻击者 $\mathcal{A}$ 发起的$H_0(ID_i)$查询时，如果表H_0^{list}中有一项为(ID_i, C_i, c_i, R_i)，则返回R_i 给 $\mathcal{A}$。否则，C 随机选择$c_i \in Z_q^*$，$R_i \in G$，计算$C_i = c_i \cdot P$，将(ID_i, C_i, c_i, R_i)加入表H_0^{list}并返回R_i 给 $\mathcal{A}$。

H_1查询：C 维护一张初始值为空的列表H_1^{list}，每一项的格式为 $(ID, R_{ID}, W_{ID}, \iota_{ID}, h_{ID})$。$C$ 收到攻击者 $\mathcal{A}$ 发起的$H_1(ID_i)$查询时，如果表H_1^{list}中有一项为$(ID_i, R_i, W_i, \iota_i, h_i)$，则返回$h_i$ 给 $\mathcal{A}$。否则，C 通过$H_0(ID_i)$查询获取R_i，随机选择$\iota_i, h_i \in Z_q^*$，计算$W_i = \iota_i \cdot P$，将$(ID_i, R_i, W_i, \iota_i, h_i)$加入表$H_1^{list}$并返回$h_i$ 给 $\mathcal{A}$。

H_3查询：C 维护一张初始值为空的列表H_3^{list}，每一项的格式为$(IDi, IDj, * \cdots *, h)$。$C$ 收到攻击者 $\mathcal{A}$ 发起的$H_3(ID_i, ID_j, * \cdots *)$查询时，如果表$H_3^{list}$中有一项是$(ID_i, ID_j, * \cdots *, h)$，则返回 h 给 $\mathcal{A}$。否则，C 随机选择 $h \in \{0,1\}^k$，将$(ID_i, ID_j, * \cdots *, h)$加入$H_3^{list}$，返回 h 给 $\mathcal{A}$。

$PartialPrivateKeyReveal(i)$查询：$C$ 维护一张初始值为空的列表L^{list}，每一项的格式为$(ID, R_{ID}, d_{ID} = \langle w_{ID}, W_{ID} \rangle)$，$C$ 收到 $\mathcal{A}$ 关于 ID_i 和公开参数R_i 的部分密钥生成查询时，进行如下操作：

若$(ID, R_i, d_i = \langle w_i, W_i \rangle) \in L^{list}$，返回$d_i = \langle w_i, W_i \rangle$给 $\mathcal{A}$；

否则，C 通过H_0和H_1查询获得W_i，R_i，ι_i，计算$w_i = \iota_i + s \cdot H_1(ID_i, R_i, W_i)$，添加$(ID, R_i, d_i = \langle w_i, W_i \rangle)$到$L^{list}$，返回$d_i = \langle w_i, W_i \rangle$给 $\mathcal{A}$。

公钥查询：C 维护一张初始值为空的列表F^{list}，每一项的格式为$(ID, C_{ID}, W_{ID}, y_{ID}, x_{ID})$。当收到 $\mathcal{A}$ 关于 ID_i 进行公钥查询时，C 进行下述操作：

若$(ID_i, C_i, W_i, y_i, x_i) \in F^{list}$，则返回$(C_i, W_i, y_i)$ 给 $\mathcal{A}$；

否则，如果 $ID_i \neq ID_I$ 且 $ID_i \neq ID_J$，C 通过H_0和H_1查询获得C_i 和 W_i，选取随机数$x_i \in Z_q^*$，计算$y_i = x_i \cdot P$，将$(ID_i, C_i, W_i, y_i, x_i)$加入$F^{list}$并将$(C_i, W_i, y_i)$返回给 $\mathcal{A}$。

如果 $ID_i = ID_I$，C 设置$y_I = u \cdot P$，通过H_0和H_1查询获得C_I和 W_I，将$(ID_I, C_I, W_I, y_I, \perp)$加入$F^{list}$并将$(C_I, W_I, uP)$返回给 $\mathcal{A}$。

如果 $ID_i = ID_J$，C 设置$y_I = v \cdot P$，通过H_0和H_1查询获得C_J和 W_J，将$(ID_J, C_J, W_J, y_J, \perp)$加入$F^{list}$并将$(C_J, W_J, vP)$返回给 $\mathcal{A}$。

$MasterKeyReveal$ 查询：C 将系统主密钥 s 返回给 $\mathcal{A}$。

$ReplacePublicKey(i, y_i^{\mathcal{A}})$查询：如果 $i = I$ 或 $i = J$，C 退出游戏；否则 C 找到表F^{list}中的项$(ID_i, C_i, W_i, y_i, x_i)$并将其替换为$(ID_i, C_i, W_i, y_i^{\mathcal{A}}, \perp)$。

$SecretValueReveal(i)$ 查询：C 找到F^{list} 中的项 $(ID_i, C_i, W_i, y_i, x_i)$，如果$x_i = \perp$，则退出游戏，否则返回$x_i$。

$SessionKeyReveal(\Pi_{i,j}^{t})$查询：$C$ 按如下方式进行回答。

C 查询表H_3^{list}，如果找到与预言机$\Pi_{i,j}^{t}$相对应的记录$(ID_i, ID_j, * \cdots *, h)$($\mathcal{A}$进行 $SessionKeyReveal$ 查询前进行过相应的H_3查询)，C 检查记录中的各项$n_1 k_1 P, n_2 k_2 P, (n_2 + k_2)P, (Y + Y')x_i x_j P, c_i x_j P, c_i c_j P, x_i c_j P$ 的正确性(验证方法与下面相似)。如果通过验证，C 返回 h 给 $\mathcal{A}$。

否则，如果 C 在表F^{list}找到两条记录$(ID_i, C_i, W_i, y_i, \perp)$，$(ID_j, C_j, W_j, y_j, \perp)$(用户可能是 I 或 J，或者被 $\mathcal{A}$ 替换了公钥)，C 随机选择$h \in \{0,1\}^k$。由于 C 知道用户 i 和 j 的部分私钥(w_i 和w_j)、秘密值(c_i 和c_j)及本次会话的临时私钥，它可以计算出$n_1 k_1 P, n_2 k_2 P, (n_2 + k_2)P, (Y + Y'), c_i c_j P, c_i x_j P = c_i y_j, x_i c_j P = c_j y_i$，但 C 无法计算$x_i x_j P$ 的值。C 将$(ID_i, ID_j, * \cdots *, h)$ 加入H_3^{list}，此时记录中对应$(Y + Y')x_i x_j P$ 的项为$\perp$。为了保持游戏的一致性，如果后来 $\mathcal{A}$ 提交相匹配的$H_3(IDi, IDj, * \cdots *)$查询时，$C$ 取出其对应的$(Y + Y')x_i x_j P$，设置$x_i x_j P = x_i^{\mathcal{A}} x_j^{\mathcal{A}} P$，验证$\hat{e}(x_i^{\mathcal{A}} x_j^{\mathcal{A}} P, P) = \hat{e}(y_i, y_j)$是否成立。

若等式成立，C 返回 h 给 $\mathcal{A}$，并将$(ID_i, ID_j, * \cdots *, h)$中对应$(Y + Y')x_i x_j P$ 项的值$\perp$替换为$(Y + Y')x_i^{\mathcal{A}} x_j^{\mathcal{A}} P$。

若等式不成立，C 随机选择 $h \in \{0,1\}^k$ 并将其返回给 $\mathcal{A}$，将$(ID_i, ID_j, * \cdots *, h)$加入$H_3^{list}$。

否则，通过以上询问，C 可计算记录$(ID_i, ID_j, * \cdots *, h)$中各项的值，并将计算出的 h 返回给 $\mathcal{A}$，将$(ID_i, ID_j, * \cdots *, h)$加入$H_3^{list}$。

挑战者 C 完美地仿真了游戏。如果 C 没有退出游戏并且 $\mathcal{A}$赢得了游戏，那么它一定进行过$H_3(ID_I, ID_J, * \cdots *)$查询，$C$ 在H_3^{list} 中检索$(ID_I, ID_J, * \cdots *, h)$并从中取出$(Y + Y')x_I x_J P$ 项的值，设置$x_I x_J P = x_I' x_J' P$，验证$\hat{e}(x_I' x_J' P, P) = \hat{e}(uP, vP)$是否成立。如果成立，退出游戏并返回$x_I' x_J' P$ 作为 CDH 问题的解。

C 解决 CDH 挑战的概率为$Adv^C(k)[\mathrm{CDH}] \geqslant \frac{Adv_7^{\mathcal{A}}(k)}{9\,n(k)^2}$。

(2)情况 2－情况 4 的证明思路与情况 1 的证明类似，不同之处是挑战者 C 把 CDH 困难问题嵌入到不同的值中。容易得出，在情况 2－情况 4 中，C 解决 CDH 挑战的概率为$Adv^C(k)[\mathrm{CDH}] \geqslant \frac{Adv_7^{\mathcal{A}}(k)}{9\,n(k)^2 s(k)}$。

(3)情况 5 的安全性分析

证明：假设挑战者 C 想解决 G 中的 CDH 困难问题，挑战值是(up, vp)，它需要借助攻击者的能力计算 uvp。

C 将系统参数$\{G, q, P, P_{pub}, H_0, H_1, H_2, H_3\}$发送给 $\mathcal{A}$，$H_i (i \in \{0, \cdots, 3\})$是随机预言机。

H_0查询：C 维护一张初始值为空的列表H_0^{list}，每一项的格式为$(ID, C_{ID}, c_{ID}, R_{ID})$。$C$ 收到攻击者 $\mathcal{A}$ 发起的$H_0(ID_i)$查询时，如果表H_0^{list}中有一项为(ID_i, C_i, c_i, R_i)，则返回R_i 给 $\mathcal{A}$。否则，如果 $ID_i \neq ID_I$，C 随机选择$c_i \in Z_q^*$，$R_i \in G$，计算$C_i = c_i \cdot P$，将(ID_i, C_i, c_i, R_i)加入表H_0^{list}并返回R_i 给 $\mathcal{A}$；如果$ID_i = ID_I$，C 设置$C_i = u \cdot P$，返回$\perp$给 $\mathcal{A}$并将$(ID_I, uP, \perp, \perp)$ 加入表H_0^{list}。

H_1查询：C维护一张初始值为空的列表H_1^{list}，每一项的格式为（ID，R_{ID}，W_{ID}，ι_{ID}，h_{ID}）。C收到攻击者$\mathcal{A}$发起的$H_1(ID_i)$查询时，如果表H_1^{list}中有一项为(ID_i，R_i，W_i，ι_i，h_i)，则返回h_i给$\mathcal{A}$。否则，如果$ID_i \neq ID_I$，C通过$H_0(ID_i)$查询获取R_i，随机选择ι_i，$h_i \in Z_q^*$，计算$W_i = \iota_i \cdot P$，将(ID_i，R_i，W_i，ι_i，h_i)加入表H_1^{list}并返回h_i给$\mathcal{A}$；如果$ID_i = ID_I$，C设置$W_I = \alpha$（$\alpha \in G$），返回$\perp$给$\mathcal{A}$并将(ID_I，$\perp$，α，$\perp$，$\perp$）加入表H_1^{list}。

H_3查询：与情况 1 中的H_3查询类似。

PartialPrivateKeyReveal(i)查询：C维护一张初始值为空的列表L^{list}，每一项的格式为$(ID, R_{ID}, d_{ID} = \langle w_{ID}, W_{ID} \rangle)$，$C$收到$\mathcal{A}$关于$ID_i$和公开参数$R_i$的部分密钥生成查询时，进行如下操作：

若$(ID, R_i, d_i = \langle w_i, W_i \rangle) \in L^{list}$，返回$d_i = \langle w_i, W_i \rangle$给$\mathcal{A}$；

否则，如果$ID_i \neq ID_I$，C通过H_0和H_1查询获得W_i，R_i，ι_i，计算$w_i = \iota_i + s \cdot H_1(ID_i, R_i, W_i)$，添加($ID_i$，$R_i$，$d_i = \langle w_i, W_i \rangle$)到$L^{list}$，返回$d_i = \langle w_i, W_i \rangle$给$\mathcal{A}$；如果$ID_i = ID_I$，退出游戏并将($ID_i$，$\perp$，$\perp$)加入表$L^{list}$。

公钥查询：C维护一张初始值为空的列表F^{list}，每一项的格式为(ID，C_{ID}，W_{ID}，y_{ID}，x_{ID})。当收到$\mathcal{A}$关于ID_i进行公钥查询时，C进行下述操作：

若(ID_i，C_i，W_i，y_i，x_i)$\in F^{list}$，则返回(C_i，W_i，y_i）给$\mathcal{A}$；

否则，如果$ID_i \neq ID_J$，C通过H_0和H_1查询获得C_i和W_i，选取随机数$x_i \in Z_q^*$，计算$y_i = x_i \cdot P$，将(ID_i，C_i，W_i，y_i，x_i)加入F^{list}并将(C_i，W_i，y_i)返回给$\mathcal{A}$。

如果$ID_i = ID_J$，C设置$y_I = v \cdot P$，通过H_0和H_1查询获得C_J，W_J，将(ID_J，C_J，W_J，y_J，$\perp$)加入F^{list}并将(C_J，W_J，vP)返回给$\mathcal{A}$。

MasterKeyReveal 查询：C返回$\perp$给$\mathcal{A}$。

ReplacePublicKey$(i, y_i^{\mathcal{A}})$查询：如果$i = J$，C退出游戏；否则C找到表F^{list}中的项(ID_i，C_i，W_i，y_i，x_i)并将其替换为(ID_i，C_i，W_i，$y_i^{\mathcal{A}}$，$\perp$)。

SecretValueReveal(i)查询：C找到F^{list}中的项(ID_i，C_i，W_i，y_i，x_i)，如果$x_i = \perp$，则退出游戏，否则返回x_i。

SessionKeyReveal$(\Pi_{i,j}^s)$查询：C按如下方式进行回答。

C查询表H_3^{list}，如果找到与预言机$\Pi_{i,j}^s$相对应的记录(ID_i，ID_j，$* \cdots *$，h)（$\mathcal{A}$进行 *SessionKeyReveal* 查询前进行过相应的H_3查询），C检查记录中的各项$n_1 k_1 P$，$n_2 k_2 P$，$(n_2 + k_2)P$，$(Y + Y')x_i x_j P$，$c_i x_j P$，$c_i c_j P$，$x_i c_j P$的正确性（验证方法与下面相似）。如果通过验证，则返回h给$\mathcal{A}$。

否则，如果$i = I$，C在表F^{list}找到两条记录(ID_I，C_I，α，$y_I^{\mathcal{A}}$，$\perp$)，(ID_j，C_j，W_j，y_j，$\perp$)（$\mathcal{A}$替换了用户I的公钥，用户j可能是J或者被$\mathcal{A}$替换了公钥）。C随机选择$h \in \{0,1\}^k$。由于C知道用户j的部分私钥、秘密值c_j和本次会话的临时私钥，它可以计算出$n_1 k_1 P$，$n_2 k_2 P$，$(n_2 + k_2)P$，$(Y + Y')x_I x_j P$，$c_I c_j P = c_j C_I$，$x_I c_j P$，但无法计算$c_I x_j P$和$x_I x_j P$的值。C将(ID_I，ID_j，$* \cdots *$，h)加入H_3^{list}，此时记录中对应$x_I x_j P$，$c_I x_j P$的项为$\perp$。为了保持游戏的一致性，如果后来$\mathcal{A}$提交相匹配的$H_3(IDI, IDj, * \cdots *)$查询时，$C$取出其对应的$c_I x_j P$和$x_I x_j P$，设置$c_I x_j P = c_I^{\mathcal{A}} x_j^{\mathcal{A}} P$，$x_I x_j P = x_I^{\mathcal{A}} x_j^{\mathcal{A}} P$，验证$\hat{e}(c_I^{\mathcal{A}} x_j^{\mathcal{A}} P, P) = \hat{e}(C_I, y_j)$和$\hat{e}(x_I^{\mathcal{A}} x_j^{\mathcal{A}} P, P) = \hat{e}(y_I^{\mathcal{A}}, y_j)$是否成立。

若等式都成立，C返回h给$\mathcal{A}$，并将(ID_I，ID_j，$* \cdots *$，h)中对应$c_I x_j P$项的值$\perp$替换为$c_I^{\mathcal{A}} x_j^{\mathcal{A}} P$，将$x_I x_j P$项的值$\perp$替换为$x_I^{\mathcal{A}} x_j^{\mathcal{A}} P$；

否则，C随机选择$h \in \{0,1\}^k$并将其返回给$\mathcal{A}$，将(ID_I，ID_j，$* \cdots *$，h)加入H_3^{list}；

否则，如果C在表F^{list}找到(ID_i，C_i，W_i，$y_i^{\mathcal{A}}$，$\perp$)，(ID_j，C_j，W_j，$y_j^{\mathcal{A}}$，$\perp$)（$\mathcal{A}$替换了用户I和J的公钥），C可以采用情况 1 中 *SessionKeyReveal*$(\Pi_{i,j}^s)$查询的处理方法进行回答；

否则，通过以上询问，C可以计算记录(ID_i，ID_j，$* \cdots *$，h)中各项的值，并将计算出的h返回给$\mathcal{A}$，将(ID_i，ID_j，$* \cdots *$，h)加入H_3^{list}。

C完美地仿真了游戏。如果C没有退出游戏并且$\mathcal{A}$赢得了游戏，那么它一定进行过$H_3(ID_I, ID_J, * \cdots *)$查询，$C$在$H_3^{list}$中检索($ID_I$，$ID_J$，$* \cdots *$，$h$)并从中取出$c_i x_j P$项的值，设置$c_i x_j P = c_I' x_J' P$，验证$\hat{e}(c_I' x_J' P, P) = \hat{e}(uP, vP)$是否成立。如果成立，退出游戏并返回$c_I' x_J' P$作为 CDH 问题的解。

C解决 CDH 挑战的概率为$\mathcal{A}dv^C(k)[\mathrm{CDH}] \geqslant \dfrac{Adv_7^{\mathcal{A}}(k)}{9\, n(k)^2}$。

（4）情况 6－情况 8 的安全性分析与情况 5 的证明类似。在情况 6 中，C解决 CDH 挑战的概率为$Adv^C(k)[\mathrm{CDH}] \geqslant \dfrac{Adv_7^{\mathcal{A}}(k)}{9\, n(k)^2}$。在情况 7 和情况 8 中，$C$解决 CDH 挑战的概率为$Adv^C(k)[\mathrm{CDH}] \geqslant \dfrac{Adv_7^{\mathcal{A}}(k)}{9\, n(k)^2 s(k)}$。

（5）情况 9 的安全性分析

证明：假设挑战者C想解决G中的 CDH 困难问题，挑战值是(up, vp)，它需要借助攻击者的能力计算uvp。

C将系统参数$\{G, q, P, P_{\mathrm{pub}}, H_0, H_1, H_2, H_3\}$发送给$\mathcal{A}$，$H_i$（$i \in \{0, \cdots, 3\}$）是随机预言机。

H_0查询：C维护一张初始值为空的列表H_0^{list}，每一项的格式为(ID，C_{ID}，c_{ID}，R_{ID})。C收到攻击者$\mathcal{A}$发起的$H_0(ID_i)$查询时，如果表H_0^{list}中有一项为(ID_i，C_i，c_i，R_i)，则返回R_i给$\mathcal{A}$。否则，如果$ID_i \neq ID_I$且$ID_i \neq ID_J$，C随机选择$c_i \in Z_q^*$，$R_i \in G$，计算$C_i = c_i \cdot P$，将(ID_i，C_i，c_i，R_i)加入表H_0^{list}并返回R_i给$\mathcal{A}$；如果$ID_i = ID_I$，C设置$C_i = u \cdot P$，返回$\perp$给$\mathcal{A}$并将(ID_I，uP，$\perp$，$\perp$）加入表H_0^{list}；如果$ID_i = ID_J$，C设置$C_i = v \cdot P$，返回$\perp$给$\mathcal{A}$并将(ID_I，vP，$\perp$，$\perp$）加入表H_0^{list}。

H_1查询：C维护一张初始值为空的列表H_1^{list}，每一项的格式为(ID，R_{ID}，W_{ID}，ι_{ID}，h_{ID})。C收到攻击者$\mathcal{A}$发起的$H_1(ID_i)$查询时，如果表H_1^{list}中有一项为(ID_i，R_i，W_i，ι_i，h_i)，则返回h_i给$\mathcal{A}$。否则，如果$ID_i \neq ID_I$且$ID_i \neq ID_J$，C通过$H_0(ID_i)$查询获取R_i，随机选择ι_i，$h_i \in Z_q^*$，计算$W_i = \iota_i \cdot P$，将(ID_i，R_i，W_i，ι_i，h_i)加入表H_1^{list}并返回h_i给$\mathcal{A}$；如果$ID_i = ID_I$，C设置$W_I = \alpha$（$\alpha \in G$），返回$\perp$给$\mathcal{A}$并将(ID_I，$\perp$，α，$\perp$，$\perp$）加入表H_1^{list}；如果$ID_i = ID_J$，C设置$W_J = \beta$（$\beta \in G$），返回$\perp$给$\mathcal{A}$并将(ID_J，$\perp$，β，$\perp$，$\perp$）加入表H_1^{list}。

H_3查询：与情况 1 中的H_3查询类似。

PartialPrivateKeyReveal(i)查询：C维护一张初始值为空的列表L^{list}，每一项的格式为$(ID, R_{ID}, d_{ID} = \langle w_{ID}, W_{ID} \rangle)$。$C$收到$\mathcal{A}$关于$ID_i$和公开参数$R_i$的部分密钥生成查询时，进行如下操作：

若$(ID, R_i, d_i = \langle w_i, W_i \rangle) \in L^{list}$，返回$d_i = \langle w_i, W_i \rangle$给$\mathcal{A}$；

否则，如果$ID_i \neq ID_I$且$ID_i \neq ID_J$，C通过H_0和H_1查询获得W_i，R_i，ι_i，计算$w_i = \iota_i + s \cdot H_1(ID_i, R_i, W_i)$，添加($ID$，$R_i$，$d_i = \langle w_i, W_i \rangle$)到$L^{list}$，返回$d_i = \langle w_i, W_i \rangle$给$\mathcal{A}$；否则，如果

$ID_i=ID_I$ 或 $ID_i=ID_J$，退出游戏并将$(ID_i,\perp,\perp)$加入表L^{list}。

公钥查询：C 维护一张初始值为空的列表F^{list}，每一项的格式为$(ID,C_{ID},W_{ID},y_{ID},x_{ID})$，当收到 $\mathcal{A}$ 关于 ID_i 进行公钥查询时，若$(ID_i,C_i,W_i,y_i,x_i)\in F^{list}$，则返回$(C_i,W_i,y_i)$ 给 $\mathcal{A}$；

否则，如果 $ID_i\neq ID_I$ 且 $ID_i\neq ID_J$，C 通过H_0和H_1查询获得C_i 和 W_i，选取随机数$x_i\in Z_q^*$，计算$y_i=x_i\cdot P$，将(ID_i,C_i,W_i,y_i,x_i)加入F^{list}并将(C_i,W_i,y_i)返回给 $\mathcal{A}$；

否则，如果 $ID_i=ID_I$，选取随机数$x_i\in Z_q^*$，计算$y_i=x_i\cdot P$，将$(ID_i,C_i,\alpha,y_i,x_i)$加入$F^{list}$并将$(C_i,\alpha,y_i)$返回给 $\mathcal{A}$；如果 $ID_i=ID_J$，选取随机数$x_i\in Z_q^*$，计算$y_i=x_i\cdot P$，将(ID_i,C_i,β,y_i,x_i)加入F^{list}并将(C_i,β,y_i)返回给 $\mathcal{A}$。

MasterKeyReveal 查询：C 返回$\perp$给 $\mathcal{A}$。

ReplacePublicKey$(i,y_i^{\mathcal{A}})$查询：C 找到表F^{list}中的项(ID_i,C_i,W_i,y_i,x_i)并将其替换为$(ID_i,C_i,W_i,y_i^{\mathcal{A}},\perp)$。

SecretValueReveal(i)查询：C 找到F^{list}中的项(ID_i,C_i,W_i,y_i,x_i)，如果$x_i=\perp$，则退出游戏，否则返回x_i。

SessionKeyReveal$(\Pi_{i,j}^s)$查询：C 按如下方式进行回答：

C 查询表H_3^{list}，如果找到与预言机$\Pi_{i,j}^s$相对应的记录$(IDi,IDj,*\cdots*,h)$（$\mathcal{A}$进行 *SessionKeyReveal* 查询前进行过相应的H_3查询），C 检查记录中的各项$n_1k_1P,n_2k_2P,(n_2+k_2)P,(Y+Y')x_ix_jP,c_ix_jP,c_ic_jP,x_ic_jP$的正确性（验证方法和下面相似）。如果通过验证，$C$ 返回 h 给 $\mathcal{A}$。

如果 $i=I$ 且 $j=J$，C 在表F^{list}找到两条记录$(ID_I,C_I,\alpha,y_I^{\mathcal{A}},\perp)$，$(ID_J,C_J,\beta,y_J^{\mathcal{A}},\perp)$（$\mathcal{A}$替换了用户 I 和 J 的公钥），C 随机选择$h\in\{0,1\}^k$。由于 C 知道本次会话的临时私钥，但不知道用户 I 和 J 的部分私钥（w_I和w_J）、秘密值（c_I和c_J）以及（x_I和x_J），它可以计算$K_{I1}=k_1\cdot v'\cdot(C_J+W_J+P_{pub}\cdot h_J)=n_1k_1P$和$Y$，但无法计算$K_{I2}=n_2k_2P$，$K_{I3}=(n_2+k_2)P$，$K_{I4}=(Y+Y')x_Ix_JP$，$K_{I5}=c_Iy_J$，$K_{I6}=c_IC_J$，$K_{I7}=x_IC_J$。$C$ 将$(ID_I,ID_J,*\cdots*,h)$加入H_3^{list}，此时记录中对应$K_{I2},K_{I3},K_{I4},K_{I5},K_{I6},K_{I7}$的项全部为$\perp$。为了保持游戏的一致性，如果后来攻击者 $\mathcal{A}$ 提交相匹配的$H_3(ID_I,ID_J,*\cdots*)$查询，C 取出其对应的$K_{I2},K_{I3},K_{I4},K_{I5},K_{I6},K_{I7}$的值（假设为$K_{I2}^{\mathcal{A}},K_{I3}^{\mathcal{A}},K_{I4}^{\mathcal{A}},K_{I5}^{\mathcal{A}},c_I^{\mathcal{A}}c_J^{\mathcal{A}}P,K_{I7}^{\mathcal{A}}$），验证$\hat{e}(c_I^{\mathcal{A}}c_J^{\mathcal{A}}P,P)=\hat{e}(C_I,C_J)$，$\hat{e}(K_{I5}^{\mathcal{A}},P)=\hat{e}(C_I,y_J)$，$\hat{e}(K_{I7}^{\mathcal{A}},P)=\hat{e}(y,C_J)$，$\hat{e}(x_I^{\mathcal{A}}x_J^{\mathcal{A}}P,P)=\hat{e}(y_I,y_J)$，$\tau'\cdot P=(K_{I3}^{\mathcal{A}}-k_2P)\cdot(C_I+\alpha+h_I\cdot P_{pub})$（其中$h_I=H_1(ID_I,C_I,\alpha)$，$\tau'$为用户 J 发送给用户 I 的消息），$K_{I2}^{\mathcal{A}}=k_2K_{I3}^{\mathcal{A}}-k_2\cdot k_2\cdot P$是否成立。如果以上等式都成立，$C$ 返回 h 给 $\mathcal{A}$并将$(ID_I,ID_J,*\cdots*,h)$中对应值为$\perp$的项依次替换为$K_{I2}^{\mathcal{A}},K_{I3}^{\mathcal{A}},K_{I4}^{\mathcal{A}},K_{I5}^{\mathcal{A}},c_I^{\mathcal{A}}c_J^{\mathcal{A}}P,K_{I7}^{\mathcal{A}}$。如果上述等式有一个不成立，$C$ 随机选择 $h\in\{0,1\}^k$ 并将其返回给 $\mathcal{A}$，将$(ID_I,ID_J,*\cdots*,h)$加入H_3^{list}。

否则，如果 $i=I$ 或 $i=J$，且 $j\neq I,j\neq J$，C 在表F^{list}找到两条记录$(ID_j,C_i,W_i,y_i^{\mathcal{A}},\perp)$，$(ID_j,C_j,W_j,y_j,\perp)$（$\mathcal{A}$替换了用户 i 和用户 j 的公钥）。C 可以采用情况 5 中 *SessionKeyReveal*$(\Pi_{i,j}^s)$查询的处理方法进行回答。

否则通过以上询问 C 可计算记录$(ID_i,ID_j,*\cdots*,h)$中各项的值，并将计算出的 h 返回给 $\mathcal{A}$，将$(ID_i,ID_j,*\cdots*,h)$加入H_3^{list}。

C 完美地仿真了游戏。如果 C 没有退出游戏并且 $\mathcal{A}$ 赢得了游戏，那么它一定进行过$H_3(ID_I,ID_J,*\cdots*)$查询，C 在H_3^{list}中检索$(ID_I,ID_J,*\cdots*,h)$并从中取出c_ic_jP项的值，设置$c_ic_jP=c_I'c_J'P$，验证$\hat{e}(c_I'c_J'P,P)=\hat{e}(uP,vP)$是否成立。如果成立，退出游戏，并返回$c_I'c_J'P$作为 CDH 问题的解。

C 解决 CDH 挑战的概率为$Adv^C(k)[\text{CDH}]\geqslant\frac{Adv_{\mathcal{T}}^{\mathcal{A}}(k)}{9\,n(k)^2}$。

结合情况 1－情况 9 的证明，可得出定理 1。

3.2.2 效能分析

本协议不仅避免了一个庞大 PKI 的引入，而且成功解决了通信实体的密钥托管问题（私钥不被 KGC 所知）。表 1 将本文提出的协议与已有 SIP 认证密钥协商协议进行了比较。

表 1 协议的性能比较

Table 1 Costs comparison of protocols

协议	安全	计算开销	消息长度	交互次数
文献[10]方法	×	$2\hat{e}+2E+3p$	$2\|Z_q^*\|+2\|G\|$	3
文献[11]方法	√	$2\hat{e}+2E$	$\|Z_q^*\|+2\|G\|$	4
文献[12]方法	×	$2E+2V$	$\|\sigma\|+\|G\|$	4
本文方法	√	$7E$	$2\|Z_q^*\|+2\|G\|$	3

表 1 中，交互次数表示完成协议实体的相互认证和密钥协商所需交互消息的数目。文献[10]和文献[12]没有对协议的安全性进行形式化的证明，文献[11]只在 CK 模型下给出了协议的安全性证明，本文提出的协议在 seCK 模型下是可证明安全的；通信实体的身份、公钥等公开信息以及可提前计算的相关运算都未统计。相关符号的定义如下：$\hat{e}$表示双线性对运算，E 表示点乘运算，p 表示模指运算，V 表示签名验证，$|Z_q^*|$表示Z_q^*中元素的长度，$|G|$表示群 G 中元素的长度，$|\sigma|$表示签名的长度。

在本协议中，利用签密技术的性质，通信实体的身份信息在任何时候都是加密传输的，除 KGC 外，任何实体都不能将R_u和用户的真实身份联系起来，并且用户可通过等式$w_u\cdot P=W_u+P_{pub}\cdot H_1(ID_u,R_u,W_u)$来完成与 KGC 之间的双向验证。因此，协议满足匿名性和不可追踪性。

结束语 本文在分析现有 SIP 安全机制的基础上提出了一种基于改进 SIP 协议的 SIP 安全认证模型。结合无证书签密技术，设计了一种在 seCK 模型下可证安全的 SIP 两方匿名认证与密钥协商协议。该协议只需进行 7 次点乘运算就能在实现 VoIP 网络中通信实体之间双向认证的同时为双方分配一个安全的会话密钥。与现有的安全协议相比，本文提出的方案在确保安全的同时，更加高效。由于时间和篇幅的原因，本文没有对新协议进行实验仿真，在下一步的工作中将着重对协议的仿真进行研究。

参 考 文 献

[1] DONG Q, LUO G M, ZHU L. Research on SIP based key distribution method of private mobile communication system[J/OL]. Command Control &Simulation. http://kns.cnki.net/kcms/detail/32.1759.TJ.20191218.1203.004.html. 2019.12.

[2] PAN W B. The Security Research of Core Network Protocol Based on Voip[D]. Beijing: Beijing University of Posts and Telecommunicatons, 2018.

[3] SI D F, HAN X H, LONG Q, et al. A Survey on the Core Technique and Research Development in SIP Standard[J]. Journal of Software, 2005, 16(2): 239-249.

[4] GUO Z H, LIU B C. Research and design of improved SIP-based authentication mechanism[J]. Study on Optical Communica-

tions，2013，180(6)：8-11.
[5] JIANG H，PAN W J，HU R L. Design of SIP Authentication Scheme Based on Ring Signature[J]. Computer Technology and Development，2016，26(3)：140-143.
[6] ZHANG ZX，FANG B X，ZHANG H L，et al. Safe comunicated model of SIP network based on improved SIP protocol[J]. Journal on Communication，2007，28(12)：39-46.
[7] WEI Z M，FENG J C. Study on Security Authentication Mechanism for SIP[J]. Computer Science，2008，35(11)：95-97.
[8] LIU J M，GAO L J，LU G Y. Voip authentication and encryption system based on SIP[J]. Journal of Xi'an University of Posts and Telecommunications，2016，21(4)：14-18.
[9] CAO Y. SIP Authentication Key Agreement Protocol Based on ECDLP[J]. Computer Systems & Applications，2016，25(3)：225-228.
[10] WEN Y Y，LUO M，ZHAO H. Research and implementation of a signcryption-based security mechanism in VoIP network[J]. Journal on Communication，2010，31(4)：8-15.
[11] LI X W. Research on Provably Secure Authenticated Key Agreement Protocol[D]. Xi'an：Xidian University，2013.
[12] NI L. Research on Some Issues in Authenticated Key Agreement Protocols[D]. Shanghai：Shanghai Jiao Tong University，2012.
[13] SHU J. Design and Analysis of Authenticated Key Exchange Protocols[D]. Chengdu：University of Electronic Science and Technology of China，2010.
[14] SUN H Y. Authenticated Key Agreement Protocol and ITS Applications[D]. Beijing：Beijing University of Posts and Telecommunicatons，2014.
[15] ZHOU Y W，YANG B，ZHANG W Z. An Improved Two-party Authenticated Certificateless Key Agreement Protocol[J]. Chinese Journal of Computers，2017，40(5)：1181-1190.

MO Tian-qing，born in 1986，network engineer. Her main research interests include information security and cryptography.

（上接第 412 页）

圈，使得 P 圈的通讯顺畅，这种情形下，这两种策略表现出的性能不分上下。

从表 4 可以看出，对于不同的网络，策略一的效率优于策略二。但是两种策略总体上的时间花费都比较短。

表 4 基于两种策略的 TPCS 算法的运行时间

Table 4 TPCS algorithm running time of two strategies (seconds)

（单位：s）

策略	节点数 10	节点数 20	节点数 30	节点数 50
策略一	175	256	316	417
策略二	247	329	374	592

通过上述分析，采用 COST-239 网络拓扑进行的仿真表明：采用 P 圈容量策略一的 TPCS 算法具有的优势表现在运行时间和网络管理上。其在节约网络带宽、降低数据传输时间和网络冗余度方面的性能要低于策略二。除此之外，TPCS 还具有其他优势，比如在规模大小不同的网络中具有良好的性能表现，并且在业务保护规划方面具有较好的实用性，实用范围比较广，可行性大。

结束语 随着 PTN 网络技术的发展以及用户对传输网建设和改造的需求，PTN 提供电信级的 OAM、服务质量(QoS)和保护能力，为 IP 业务提供柔性的传输管道，为用户提供多种组网方案。为了进一步优化 PTN 结构，本文介绍了 PTN 网络通信方式以及 PTN 网络架构，引入了对 PTN 网络进行优化的方式。本文针对业务及流量规划、融入 OTN 核心组网、PTN 网络软件构架以及 p-Cycle 保护算法进行了介绍，使用户在使用过程中能够融合多网络通讯，提高传输带宽、流量等，实现了 PTN 网络技术的灵活应用。

参 考 文 献

[1] 邓旭. PTN 网络架构中 L2 转 L3 设置方案[J]. 电信科学，2017，33(6)：164-170.
[2] 付琪. 关于接入层 PTN 网络结构优化的研究[J]. 通讯世界，2015(4)：15-16.
[3] 郭立强. 光传送网 PTN 网络环网保护[J]. 信息通信，2018(8)：117-123.
[4] 赵菲，何涌波. QoS 技术在保证 PTN 传输网络安全方面的应用研究[J]. 信息通信，2017(7)：220-221.
[5] 李雅丽，李永江. 基于 TCP 通信方案的电力线路状态监测系统研究[J]. 电源技术，2015，39(1)：175-177.
[6] 卢锋. PTN 网络结构及优化[J]. 科技经济导刊，2016，28(8)：73-77.
[7] 陈星豪，黄柳萍，陶国飞. 基于随机矩阵理论的电力大数据表征方法[J]. 电网技术，2017，36(3)：35-38.
[8] 陈子辉，王硕君，刘勇浩，等. 基于数据质量的电能质量监测装置远程可靠性评估[J]. 广东电力，2017，30(1)：73-78.
[9] 周鑫，田兵，许爱东，等. 基于 CYMDIST 的配电网运行优化技术及算例分析[J]. 电网与清洁能源，2015，31(2)：91-97.
[10] 易映萍，罗海，胡四全. 小功率光伏并网逆变器控制策略的研究[J]. 电力系统保护与控制，2016(4)：64-68.
[11] 高迪，路瑶，赵娟娟，等. 基于 Tabu 算法的配电网无功补偿 [J]. 电气自动化，2015(1)：91-93.
[12] 肖雄，刘治. 基于负荷管理终端的电能质量监测研究与分析[J]. 广东电力，2016，29(2)：85-89.
[13] 孙跃，李敏，陈乐然，等. 基于 POTN 技术的电力通信网规划方案[J]. 电信科学，2017(S1)：522-526，552.
[14] 苏永义，隋树法，周忠堂，等. 配电网电能质量智能监控方法的研究[J]. 自动化与仪器仪表，2017(10)：58-60.
[15] 吴富杰，苏小林，阎晓霞，等. 基于多目标的主动配电网有功无功协调优化[J]. 自动化技术与应用，2015，34(11)：59-65.

YAN Zhen，born in 1985，master，deputy senior engineer. His main research interests include power communication technology and so on.