基于 ECC 的 SIP 身份认证密钥协商协议

黄朝阳*，陈金木

(厦门海洋学院信息工程学院 福建 厦门 361100)

【摘要】为在 SIP 认证协议中实现用户匿名性并提高协议的安全性能，将挑战/应答机制、椭圆曲线密码技术和口令认证相结合，提出一种新的匿名 SIP 认证协议。协议仅使用少量的椭圆曲线点乘运算，既保障认证的安全性又有效降低了整体运算量。协议在认证过程中引入高熵随机数，认证双方使用挑战/应答机制的三次握手实现双向认证，同时协商生成后续会话所需密钥。通过对协议的 BAN 逻辑分析和多种已知攻击的非形式化分析，证明该协议具有较高的安全性能。经与相关协议的效率比较，协议认证过程所需的运算量更小。

关 键 词 挑战/应答； 椭圆曲线密码； Hash 函数； 口令认证； SIP 协议

中图分类号 TP309.7 **文献标志码** A doi:10.12178/1001-0548.2022182

A SIP Identity Authentication Key Agreement Protocol Based on ECC

HUANG Chaoyang* and Chen Jinmu

(School of Information Engineering, XiaMen Ocean College Xiamen Fujian 361100)

Abstract In order to provide user anonymity in SIP (session initialization protocol) authentication protocol and improve the security performance of the protocol, a new anonymous SIP authentication protocol is proposed by combining challenge/response mechanism, elliptic curve cryptography and password authentication. The protocol only uses few point multiplication operations of elliptic curve cryptography, which not only ensures the security of authentication, but also effectively reduces the overall amount of computation. The protocol introduces high-entropy random number in the authentication process. The authentication parties use three handshakes of challenge/response mechanism to realize two-way authentication, and generate the key required for subsequent sessions at the same time. Through the BAN (Burrows, Abadi and Needham) logic analysis of the protocol and the informal analysis aim at many known attacks, it is proved that the protocol has high security performance. Compared with the efficiency of related protocols, the protocol authentication process requires less computation.

Key words challenge/response; elliptic curve cryptography; Hash function; password authentication; session initialization protocol

身份认证协议作为网络安全的首道屏障，其重要性不言而喻。随着网络应用的增长，特别是自新型冠状病毒肺炎疫情暴发以来，带来了远程办公等工作方式的转变，全球即时通信应用程序和服务的使用呈指数级增长，导致基于 SIP 协议的即时通信服务的需求与日俱增。

SIP 协议 (session initialization protocol) 具有灵活、开放和可扩展的特性，为多种即时通信业务提供完整的会话创建和会话更改服务。因此，SIP 协议的安全性对于即时通信的安全起着至关重要的作用。SIP 协议一般工作在不安全的公共信道环境。而且传统 SIP 的原始身份认证机制是基于 HTTP 摘要的，其强度不足以提供针对各种流行攻击所需的安全性，这一先天缺陷使它很容易受到攻击[1]。现有的 SIP 协议中所使用的身份认证机制可能被攻击者绕过，导致未经授权的访问和信息泄露需要安全

收稿日期：2022－06－13；修回日期：2023－05－22
基金项目：中国高校产学研创新基金 (2020ITA05024)
作者简介：黄朝阳 (1975－)，男，副教授，主要从事信息安全方面的研究.
*通信作者：黄朝阳，E-mail：trippercat@sina.com

且高效的 SIP 认证和密钥协商协议来解决即时通信的安全要求。设计一种可证安全且高效的 SIP 身份认证协议具有紧迫性和重要意义。

近年来对于 SIP 协议的研究和改良层出不穷，为了提高传统 SIP 协议的安全性，先后引入了多种安全机制，如 Hash 函数、公钥密码体制、双线性对映射、椭圆曲线密码技术、混沌映射、生物特征和智能卡等。但各种研究表明：公钥密码体制面临 PKI 体系证书管理复杂的困难、双线性对映射在效率上的缺陷明显、结合生物特征和智能卡的认证协议则可能出现效率明显下降等问题。而引入 Hash 函数、椭圆曲线密码技术或混沌映射的安全、可扩展和轻量级的 SIP 身份认证协议正成为当前研究热点。

在相同的安全级别上，椭圆曲线密码 (elliptic curve cryptography) 在密钥长度上比 RSA 小很多，能有效降低计算和存储的成本开销。鉴于 ECC 的明显优势，文献 [2] 提出了基于 ECC 的 SIP 认证协议，并声称其有更好的安全性和效率。文献 [3] 在 2009 年证明了文献 [2] 协议对已知的 Denning-Sacco 攻击、Stolen-Verifier 攻击和离线口令猜测攻击是不安全的，并提出了改良的基于 ECDH(elliptic curve diffie –hellman key exchange) 的身份认证协议。2011 年，文献 [4] 又揭示了文献 [3] 的协议不能抵抗内部人员攻击和离线口令猜测攻击。文献 [5] 于 2012 年指出文献 [3] 协议无法抵御 Stolen-Verifier 攻击和离线口令猜测攻击，并提供了一种改进的方案。然而，次年文献 [6] 又证明了文献 [5] 协议仍然受到离线口令猜测攻击和冒充服务攻击威胁，并给出了一种增强方案。

匿名认证是指用户在证明自己身份合法性的同时能够确保自己身份信息、位置信息的匿名性。在身份认证过程中保护用户匿名性是当下身份认证技术的发展趋势。2015 年，文献 [7] 在文献 [6] 工作的基础上提出了一种基于椭圆曲线密码技术的匿名 SIP 认证协议，声称可以很好地保护用户隐私。文献 [8] 研究发现该协议不能抵御内部人员攻击，并在此基础上提出一种更为安全的 SIP 认证协议，声称协议可以抵御各种已知攻击，同时比其他相关协议具有更低的计算成本。2018 年，文献 [9] 研究发现文献 [8] 协议也存在无法保护用户匿名性的安全漏洞。

本文深入研究了文献 [8] 提出的 SIP 协议，在分析其安全漏洞的基础上通过改进认证消息构成，提出一种基于 ECC 的更为安全高效的 SIP 协议。新协议秉承 ECC 安全高效的特征，采用标准的挑战/应答信息交互模式，运算量小的优势明显。通过对新协议的 BAN 逻辑分析、非形式化安全分析证明其更为安全；通过性能比较分析展示其在效率方面的实用性。

1 文献 [8] 协议及其安全漏洞分析

本文所用符号如表 1 所示。

表 1 协议中的符号标记与含义

符号标记	含义
U	用户
R_x	x挑选的高熵随机数
ID_i	用户i的账号
PW_i	用户i的口令
PW_i^{new}	用户i的新口令
S	SIP服务器
Kpri_x	x的私钥
Kpri_x^{new}	x的新私钥
$\|$	字符串连接运算符
$\oplus$	异或运算符
Hash(•)	hash函数
•	椭圆曲线点乘运算
$K_{X,Y}^n$	由X所生成用以X、Y之间通信的一次性会话密钥，n指认证次数

文献 [8] 协议的认证阶段在用户端所构造生成的登录请求消息 M_request 存在设计缺陷，敌手可以根据在公共信道上窃取的登录请求消息来验证自己对用户账号的猜测，从而非法获得用户 U 的账号 ID_i 这一关键信息；该协议的认证阶段在服务器端所构造生成的挑战消息 M_challenge 同样存在设计缺陷，这一缺陷将使敌手可以根据已掌握的用户账号 ID_i 和公共信道上窃取的登录请求消息轻易伪造出可以通过用户验证的挑战消息 M_challenge，从而成功实施冒充服务器攻击。文献 [8] 协议的注册及认证阶段细节如图 1 所示，针对文献 [8] 协议的安全漏洞分析如下。

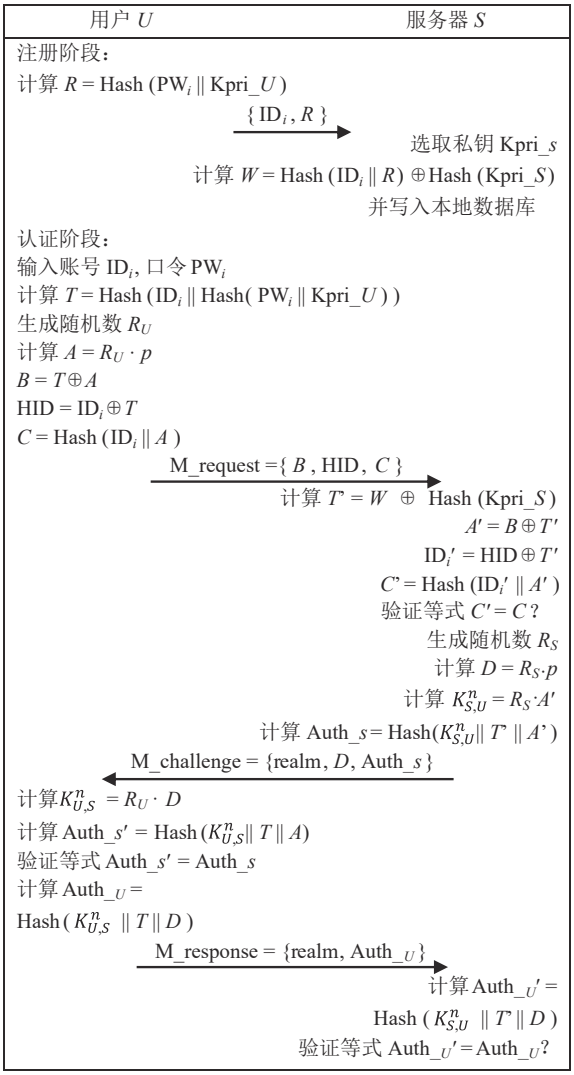

图 1　文献 [8] 协议的注册及认证阶段细节

1.1　无法抵御冒充服务器攻击

敌手 U_{att} 可以通过以下方法非法获取用户 U 的账号信息 ID_i。U_{att} 在公共信道上窃取的 U 登录请求消息 M_request = {B, HID, C}，计算 HID⊕B = ($ID_i \oplus T$) ⊕ ($T \oplus A$) = $ID_i \oplus A$。继而，U_{att} 使用一个猜测的用户账号信息 ID_i'计算出 $A' = HID \oplus B \oplus ID_i'$，然后 U_{att} 通过验证等式 $hash(ID_i' \| A') = C$ 是否成立来判断所猜测用户账号信息 ID_i'的正确性。U_{att} 可以变换猜测新的 ID_i''，不断验证上述等式直到找到正确的用户账号信息 ID_i 为止。在获取用户 U 的账号信息 ID_i 后，U_{att} 可以通过下列步骤实施冒充服务器攻击。

1) U_{att} 根据拦截到的用户登录请求消息 M_request ={B, HID, C}和已获取的用户账号信息 ID_i 计算出 $T' = HID \oplus ID_i$，$A'' = B \oplus T'$。

2) U_{att} 生成随机数 R_S*并计算 $D^* = R_S^* \cdot p$，$K^{n*}_{S,U} = R_S^* \cdot A''$，Auth_$s$* = Hash($K^{n*}_{S,U}$|| T'|| A'')，然后发送挑战消息 M_challenge* = {realm, D*, Auth_s* } 给用户。

3) 用户 U 收到 U_{att} 发来的 M_challenge*后，根据已有的高熵随机数 R_U 计算出$K^n_{U,S} = R_U \cdot D^*$ 和 Auth_s' = Hash($K^n_{U,S}$ || T|| A)，随后验证等式 Auth_s' = Auth_s*是否成立。由于 U_{att} 已事先找到正确的用户账号信息 ID_i，故等式必然成立。敌手 U_{att} 的冒充服务器攻击得以实现。图 2 给出了针对文献 [8] 协议实施冒充服务器攻击的细节。

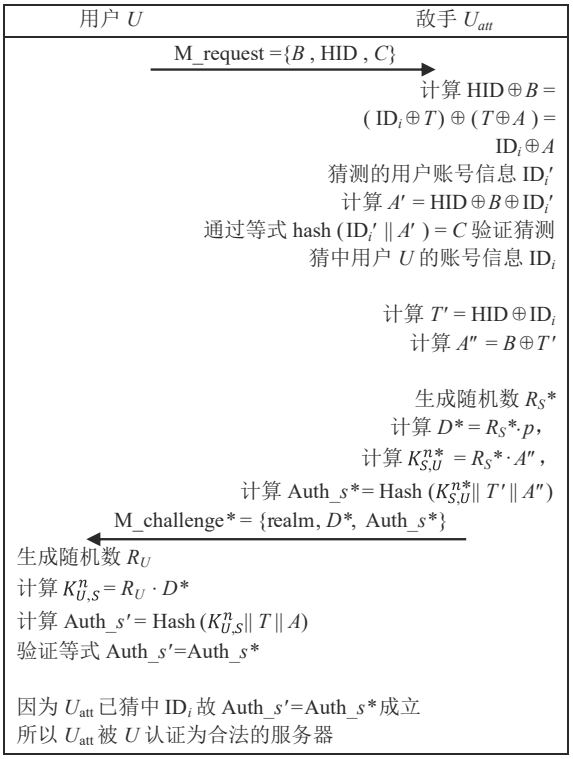

图 2　针对文献 [8] 协议实施冒充服务器攻击的细节

1.2　无法保护用户匿名性和实现双向认证

根据上述分析，敌手 U_{att} 可以获取合法注册用户的账号信息。因此，文献 [8] 协议无法保护用户匿名性。由于敌手可以假冒合法服务器骗取用户的认证，这意味着文献 [8] 协议无法实现双向认证。

2　新的 SIP 认证协议

为了克服文献 [8] 协议所暴露的安全问题，本文提出一种更为安全高效的 SIP 认证协议。协议所使用的椭圆曲线离散对数难题 (ECDLP) 以及单向 hash 函数是其可靠的安全基石[10]。

协议由用户注册、双向认证和口令更新 3 个阶段构成。协议中所用符号如表 1 所示。

2.1 用户注册

1) 用户 U 选定自己的账号 ID_i、口令 PW_i 和私钥 Kpri_U，计算出 $C=\text{Hash}(PW_i \| \text{Kpri\_}U)$，$U$ 通过安全信道向服务器 S 发送向注册请求消息$\{ID_i, C\}$。

2) S 收到 U 的消息$\{ID_i, C\}$后，结合自己的私钥 Kpri_S 计算出 $W=\text{Hash}(ID_i \| C) \oplus C \oplus \text{Hash}(\text{Kpri\_}S)$。$S$ 于本地数据库中写入 W。新协议注册阶段的细节如图 3 所示。

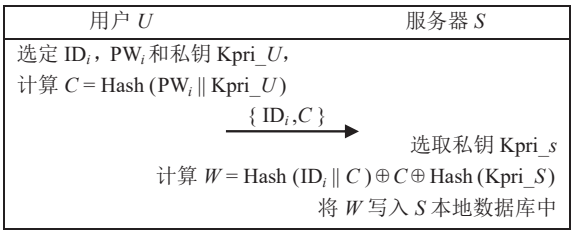

图 3 新协议注册阶段的细节

2.2 双向认证

用户 U 与服务器 S 通过以下步骤实现双向认证及密钥协商。

1) 用户 U 输入自己的账号 ID_i，口令 PW_i，计算出 $TE=\text{Hash}(ID_i \| \text{Hash}(PW_i \| \text{Kpri\_}U))$。$U$ 生成高熵随机数 R_U，并计算 $A=R_U \cdot p$，$V=\text{Hash}(A \| \text{Hash}(PW_i \oplus \text{Kpri\_}U))$。$U$ 向 S 发送登录请求消息 M_request ={ TE, A, V}。

2) 服务器 S 接收用户 U 的登录请求消息{ TE, A, V}，计算 $TF=W \oplus \text{Hash}(\text{Kpri\_}S)$，$C'=TE \oplus TF$，$V'=\text{Hash}(A \| C')$。$S$ 验证等式 $V'=V$，若等式不成立，则 S 忽略此登录请求同时结束会话。否则，由 S 生成两个高熵随机数 R_{S1} 和 R_{S2}，并计算 $B=R_{S1} \cdot p$，$K_{S,U}^n=R_{S1} \cdot A$，$\text{Auth\_}s=\text{Hash}(K_{S,U}^n \| A \| C' \| R_{S2})$。$S$ 将挑战消息 M_challenge = {realm, B, Auth_s, R_{S2} }发送给 U，此处 realm 定义为作用域的信息。

3) U 接收 S 发来的挑战消息，计算出后续一次性会话密钥 $K_{U,S}^n=R_U \cdot B$ 和 $\text{Auth\_}s'=\text{Hash}(K_{U,S}^n \| A \| C \| R_{S2})$。随后验证等式 Auth_$s'$ = Auth_s 是否成立，如果验证通过，U 完成计算 $\text{Auth\_}U=\text{Hash}(K_{U,S}^n \| B \| C \| R_{S2}+1)$ 后，发送应答消息 M_response = {realm, Auth_U}给 S。否则中止会话，结束此次双向认证过程。

4) S 接收 U 的应答消息后，计算 $\text{Auth\_}U'=\text{Hash}(K_{S,U}^n \| B \| C' \| R_{S2}+1)$，并验证等式 Auth_$U'$ = Auth_U。如等式不成立，会话终止。若验证通过，则 S 成功认证 U 的身份，并将 $K_{S,U}^n=RS1 \cdot A=RS1 \cdot RU \cdot p=RU \cdot RS1 \cdot p=RU \cdot B=K_{U,S}^n$ 作为后续一次性会话密钥。新协议的登录和双向认证阶段细节如图 4 所示。

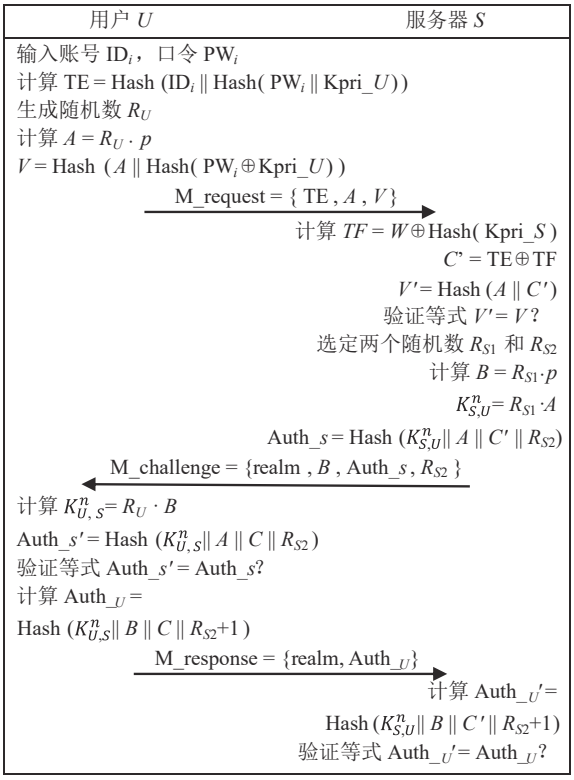

图 4 新协议登录和双向认证阶段的细节

2.3 口令更新

用户 U 凭借成功双向认证后所协商产生的一次性会话密钥 $K_{U,S}^n$，随时可以依据下列步骤替换自己的新口令 PW_i^{new}。

1) 用户 U 选取新的口令 PW_i^{new} 和新的私钥 Kpri_x^{new}，计算出 $TN=\text{Hash}(K_{U,S}^n \| \text{Hash}(ID_i \| \text{Hash}(PW_i \| \text{Kpri\_}U)) \oplus \text{Hash}(PW_i \| \text{Kpri\_}U))$，$TM=\text{Hash}(ID_i \| K_{U,S}^n) \oplus \text{Hash}(ID_i \| \text{Hash}(PW_i^{new} \| \text{Kpri\_}x^{new})) \oplus \text{Hash}(PW_i^{new} \| \text{Kpri\_}x^{new})$。$U$ 向 S 发送计算结果{ ID_i, TN, TM }。

2) 服务器 S 接收 U 的消息后，通过验证等式 $\text{Hash}(ID_i \| W \oplus \text{Hash}(\text{Kpri\_}S))=TN$ 来确认 U 身份的合法性。等式证明如下：

$$\text{Hash}(K_{S,U}^n \| W \oplus \text{Hash}(\text{Kpri\_}S))=$$

$$\text{Hash}(K_{S,U}^n \| \text{Hash}(ID_i \| C) \oplus C \oplus \text{Hash}(\text{Kpri\_}S) \oplus \text{Hash}(\text{Kpri\_}S))=\text{Hash}(K_{S,U}^n \| \text{Hash}(ID_i \| \text{Hash}(PW_i \| \text{Kpri\_}U)) \oplus$$

$$\text{Hash}(PW_i \| \text{Kpri\_}U) \oplus \text{Hash}(\text{Kpri\_}S) \oplus$$

$$\text{Hash}(\text{Kpri\_}S))=\text{Hash}(K_{S,U}^n \| \text{Hash}(ID_i \| \text{Hash}(PW_i \| \text{Kpri\_}U)) \oplus$$

$$\text{Hash}(PW_i \| \text{Kpri\_}U))=TN$$

等式验证通过后，S 计算出 $W^{new}=TM \oplus \text{Hash}(ID_i \| K_{S,U}^n) \oplus \text{Hash}(\text{Kpri\_}S)$。最后，$S$ 用 W^{new} 替换

数据库中的 W，口令更新完成。

新协议在认证阶段巧妙设计了在用户端所生成的登录请求消息 M_request 格式，让用户账号及其伴随信息都置于 hash 函数的保护之下，规避了用户账号信息泄露的可能性，真正实现用户匿名性；同时，新协议改进了服务器端挑战消息 M_challenge 的组成部分 Auth_s 的格式，使敌手无法通过在公共信道上窃取的消息计算出 Auth_s*，有效阻止敌手通过伪造服务器的挑战消息实施冒充服务器攻击。新协议增加一个服务器端所生成的高熵随机数 R_{S2}，以保证后续消息的新鲜性，有效防止重播攻击。

3　BAN 逻辑分析

Burrows、Abadi 和 Needham 于 1989 年提出 BAN 逻辑分析方法具有里程碑式的意义，它是第一个将形式化手段用于验证密码协议安全性的分析方法，作为分析密码协议一种公认的重要工具而广为使用[11]。它在用户设置的理想假设和协议步骤的前提下，对协议能否在没有冗余信息的条件下实现安全认证的目的，以及协议中的加密信息是否在明文传输时不会影响协议的安全性这两个问题给出解答[12]。BAN 逻辑分析过程所使用的符号与含义如表 2 所示。

表 2　BAN 逻辑的符号与含义

符号	含义
P	主体
X,Y	语句
K	密钥
$P\mid\equiv X$	主体P相信X为真
$P\lhd X$	P接收到X
$P\mid\sim X$	P曾发送X
$P\mid\Rightarrow X$	P对X有管辖权
$\#(X)$	X是新鲜的
$(X,Y)_K$	使用K作为密钥的X和Y hash值
$\{X,Y\}_K$	使用密钥K对包含X和Y的信息加密后的密文
SK	用户和服务器的共享密钥
$P\overset{K}{\longleftrightarrow}Q$	P与Q之间共享密钥K
$<X>_Y$	X可以由Y异或生成

BAN 逻辑是一种基于信仰的内涵逻辑，它不计量由于协议的真实实现额外带来的安全问题，也不考虑由于加密体制的安全缺陷可能带来的协议缺陷，所以 BAN 逻辑存在一定的局限性。但是，在协议设计阶段使用 BAN 逻辑分析可尽早规避潜在的设计缺陷。

下面在假定密码算法是安全的前提下，使用 BAN 逻辑分析方法对协议本身结构的安全性展开形式化证明。

3.1　BAN 逻辑推理法则

本文所使用的 BAN 逻辑推理法则主要有：

1) R1 消息含义法则：$\dfrac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q,P\lhd\{X\}K}{P\mid\equiv Q\mid\sim X}$

2) R2 临时值验证法则：$\dfrac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$

3) R3 管辖权法则：$\dfrac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$

4) R4 消息新鲜法则：$\dfrac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$

5) R5 信念法则：$\dfrac{P\mid\equiv X,P\mid\equiv Y}{P\mid\equiv(X,Y)}$

3.2　协议理想化

本协议的理想化形式为：

1) $U\rightarrow S:\langle C\rangle_{U\overset{\mathrm{TE}}{\longleftrightarrow}S},(A)_{U\overset{C}{\longleftrightarrow}S},\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,B,R_{S2}\right)_{U\overset{C}{\longleftrightarrow}S}$

2) $S\rightarrow U:\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,A,R_{S2}\right)_{U\overset{C}{\longleftrightarrow}S}$

3.3　形式化安全假设

本文协议满足下列基本假设：

P1: $U\mid\equiv\#R_{Ui},S\mid\equiv\#R_{S2}$

P2: $S\mid\equiv\#R_{S1},S\mid\equiv\#R_{S2}$

P3: $S\mid\equiv\left(U\overset{C}{\longleftrightarrow}S\right)$

P4: $U\mid\equiv\left(U\overset{C}{\longleftrightarrow}S\right)$

P5: $S\mid\equiv U\mid\Rightarrow\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right)$

P6: $U\mid\equiv S\mid\Rightarrow\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right)$

3.4　协议目标

假设协议所设置的参数和流程是正确的，那么本文协议必须满足下列安全目标：

G1: $S\mid\equiv U\mid\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right)$

G2: $S\mid\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right)$

G3: $U\mid\equiv S\mid\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right)$

G4: $U\mid\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right)$

3.5　安全证明

分析推理过程如下。

由 $S\lhd\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,B,R_{S2}\right)_{U\overset{C}{\longleftrightarrow}S}$ 和 P3，以及消息含义法则 R1 可得：

$$S\mid\equiv U\mid\sim\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,B,R_{S2}\right)\tag{1}$$

由 P2 和消息新鲜法则 R4 可得：

$$S|\equiv\#\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,B,R_{S2}\right) \tag{2}$$

由式 (1)、式 (2) 和临时值验证法则 R2 可得：

$$S|\equiv U|\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,B,R_{S2}\right) \tag{3}$$

由式 (3) 和信念法则 R5 可得：

$$S|\equiv U|\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right) \tag{4}$$

于是，G1 得以证明。

由式 (4) 和 P5，以及管辖权法则 R3 可得：

$$S|\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right) \tag{5}$$

于是，G2 得以证明。

由$U\triangleleft\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,A,R_{S2}\right)_{U\overset{C}{\longleftrightarrow}S}$和 P4，以及消息含义法则 R1 可得：

$$U|\equiv S|\sim\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,A,R_{S2}\right) \tag{6}$$

由 P1 和消息新鲜法则 R4 可得：

$$U|\equiv\#\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S,A,R_{S2}\right) \tag{7}$$

由式 (6)、式 (7) 和临时值验证法则 R2 可得：

$$U|\equiv S|\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right) \tag{8}$$

由式 (8) 和信念法则 R5 可得：

$$U|\equiv S|\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right) \tag{9}$$

于是，G3 得以证明。

由式 (9) 和 P6，以及管辖权法则 R3 可得：

$$U|\equiv\left(U\overset{\mathrm{SK}}{\longleftrightarrow}S\right) \tag{10}$$

于是，G4 得以证明。

通过上述 BAN 逻辑形式化证明，本协议的 4 个安全目标全部得以证实。所以，在理想化的环境下，本协议可以实现真实有效的双向认证和会话密钥协商。

4 安全性分析

围绕几个相关协议[2-3,5,7-8]所暴露出来的安全问题，对本协议的一些重要的安全目标开展启发式安全分析。

1) 抵御重播攻击

在本协议框架内，假定某敌手 U_{att} 伪装成合法用户 U 向服务器 S 重播登录请求消息 M_request = {TE, A, V}，S 将返回挑战消息 M_challenge = {realm, B, Auth_s, R_{S2}}。但 U_{att} 因不掌握 R_U 和 C 从而无法伪造出 Auth_U 进行应答，从而无法通过 S 的验证。同时，由于随机数 R_U 和 R_{S2} 的新鲜性，U_{att} 如果通过重播 S 的挑战消息 M_challenge = {realm, B, Auth_s, R_{S2} }来伪装成合法 S 时，根本无法通过 U 方 Auth_s' = Auth_s 这一等式验证。所以协议可以抵御重播攻击。

2) 保护用户匿名性

在新协议的双向认证实施过程中，公共信道上传输的用户账号信息以 hash 函数散列值的形式 TE = Hash(ID_i ‖ Hash(PW_i ‖ Kpri_U)) 存在。根据 hash 函数的单向安全特性，敌手 U_{att} 无法从截取的 TE 中计算获取用户 U 的账号信息 ID_i。与用户账号信息 ID_i 同时存在于 TE 中的伴随信息是 C = Hash(PW_i ‖ Kpri_U)，协议设计了用户在注册阶段通过安全信道发送 C 给服务器 S，C 也不以明文的形式存储于 S 的数据库中，故如果敌手 U_{att} 使用本文 1.1 节所述方法来猜测并验证用户账号信息必然失败。所以新协议可以实现保护用户匿名性的目标。

3) 抵御冒充服务器攻击

敌手 U_{att} 想成功冒充服务器 S 骗取用户 U 的认证，必须能生成正确的挑战消息 M_challenge = {realm, B, Auth_s, R_{S2}}，但因 U_{att} 无法获取 S 的私钥 Kpri_S 和 S 本地数据库所存储的 W，故不能计算得出 C'，当然也就无法生成正确的挑战消息要件 Auth_s。所以，U_{att} 无法成功冒充服务器 S 骗取用户 U 的认证。

4) 抵御内部人员攻击

在注册阶段，用户的口令以密文 C = Hash (PW_i ‖ Kpri_U) 的形式在安全信道上传输，服务器数据库中所存储 W = Hash(ID_i ‖ C) ⊕ C ⊕Hash (Kpri_S) 也非明文形式。在没有掌握 U 口令 PW_i 和私钥 Kpri_U 的前提下，敌手 U_{att} 无法在多项时间内把它们同时猜中，更无法使用 W 来验证这一猜测。并且，由于 hash 函数的单向安全特性，从 C 中计算得出 U 的口令 PW_i 也是行不通的。所以，内部人员无法从用户的注册信息中获取 U 的口令 PW_i。内部人员攻击对本协议无效。

5) 抵御身份假冒攻击

如前 1) 所证明，重播攻击已无法实施。敌手 U_{att} 伪装成 U 实现身份假冒攻击的前提是能生成正确的登录请求消息 M_request ={TE, A, V}和应答消

息 M_response = {realm, Auth_U}，但并不掌握的 U 的账号 ID$_i$、口令 PW$_i$ 和私钥 Kpri_U，根本无法计算出 TE，生成正确的 C 和 V 则更为困难，根本伪造不出正确的 M_request 和 M_response 要件 Auth_U，从而无法通过 S 的身份认证。所以，身份假冒攻击无法实施。

6) 抵御离线口令猜测攻击

敌手随机猜测用户的口令值，然后使用非法获取的消息来验证这一猜测，所以离线口令猜测攻击往往最具有破坏性。假定 U_{att} 在公共信道上截取认证过程的所有交互消息{TE, A, V, B, Auth_s, R_{S2}, Auth_U}。然后 U_{att} 猜测一个口令 PW$_i'$，但在未掌握用户私钥 Kpri_U 的前提下，显然无法使用 TE 或 V 验证所猜测口令 PW$_i'$的正确性。所以，离线口令猜测攻击对本协议无效。

7) 实现双向认证同时协商一次性会话密钥

协议在整体框架上采用挑战/应答机制，U 通过验证等式 Hash($K_{U,S}^n \| A \| C \| R_{S2}$) = Auth_$s$ 来验证 S 的身份；S 则通过验证等式 Hash (A ‖ (TE ⊕ (W ⊕ Hash(Kpri_S)))) = V 和验证等式 Hash($K_{S,U}^n$‖ B ‖ C' ‖ R_{S2}+1) = Auth_U 来认证 U 的身份。在双向认证的过程中，只有合法的用户和服务器才可能拥有正确的信息来计算出响应对方请求的应答消息。

认证双方各自生成的会话密钥$K_{S,U}^n = R_{S1} \cdot A = R_{S1} \cdot R_U \cdot p = R_U \cdot R_{S1} \cdot p = R_U \cdot B = K_{U,S}^n$是相等的，可以用于后续会话的加密通信。本协议具备密钥协商功能。

根据以上分析，本协议在安全性上填补了相关协议的常见漏洞，同时展现出较强的保护用户匿名性和双向认证功能，可以协商生成一次性会话密钥，具有较高的安全性能。

5　效能分析

5.1　效率比较

效率比较主要考量各相关协议在双向认证阶段执行椭圆曲线点乘、切比雪夫多项式、对称加密/解密、模逆运算和 hash 运算所需的计算开销。与上述运算相比较而言，字符串连接操作和异或运算所需耗时要小得多，不列入各协议的计算开销比较[13]。用户注册和口令更新为非经常性操作，其计算开销也不计算在内[14-15]。

为了更准确地评估各相关协议在双向认证阶段的计算效率，在运行平台 Windows 10、Intel Core i7-3 770、16GB RAM，matlab 仿真环境中测试 ECC 点乘、切比雪夫多项式、模逆运算、AES-128 和 SHA-3 运算耗时。每种密码操作均运行 10 000 次后，统计所需耗时的算术平均值如表 3 所示。相关协议和本文新协议在双向认证阶段的主要计算开销及交互次数比较如表 4 所示。

表 3　各种密码运算所需耗时的算术平均值　ms

操作	T_{CP}	T_{PM}	T_{SED}	T_{INV}	T_H
算术平均值	9.893 2	8.105 7	0.174 2	0.073 5	0.029 4

表 4　效率比较

协议	计算开销			总耗时/ms	交互次数
	用户端	服务器端	小计		
文献[8]协议	$3T_{PM}+9T_H$	$4T_{PM}+8T_H$	$7T_{PM}+17T_H$	57.239 7	3
文献[16]协议	$4T_{PM}+8T_H$	$5T_{PM}+7T_H+2T_{INV}$	$9T_{PM}+15T_H+2T_{INV}$	73.539 3	3
文献[17]协议	$3T_{PM}+7T_H$	$3T_{PM}+6T_H$	$6T_{PM}+13T_H$	49.016 4	3
文献[18]协议	$3T_{PM}+2T_{SED}+8T_H$	$3T_{PM}+2T_{SED}+2T_H$	$6T_{PM}+4T_{SED}+10T_H$	49.625 0	3
文献[19]协议	$2T_{CP}+2T_{SED}+6T_H$	$T_{CP}+3T_{SED}+4T_H$	$3T_{CP}+5T_{SED}+10T_H$	30.844 6	3
本协议	$2T_{PM}+6T_H$	$2T_{PM}+4T_H$	$4T_{PM}+10T_H$	32.716 8	3

表中，T_{CP} 为计算一次切比雪夫多项式；T_{PM} 为执行一次椭圆曲线点乘；T_{SED} 为执行一次对称加密/解密；T_{INV} 为执行一次模逆运算；T_H 为执行一次 hash 运算。

从表 4 可知，本协议的总计算开销为 $4T_{PM}+10T_H$，总耗时为 32.716 8 ms，与文献 [19] 协议基本持平，并明显少于其他相关协议。本协议展现出更高的计算效率。各相关协议在双向认证阶段所需总交互次数都是 3 次，无差别。各相关协议认证阶段的主要运算总耗时比较如图 5 所示。

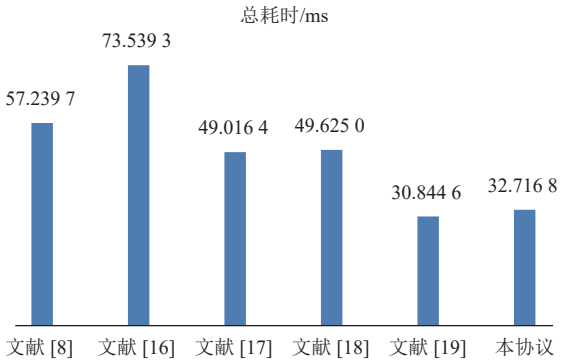

图 5 认证阶段的主要运算总耗时比较

5.2 安全特性比较

本协议与其他几个相关协议的安全特性对比如表 5 所示。文献 [8] 协议无法抵御冒充服务器攻击，无法保护用户匿名性，无法真正实现双向认证。文献 [17-19] 未给部分安全特性的分析结果。本文协议克服了文献 [8] 协议的安全缺陷，能抵御多种常见攻击，提供用户匿名性保护和前向安全性，可以真正实现双向认证，展示出比文献 [17-19] 更高的安全性能。文献 [16] 虽然也可以抵御各种已知攻击，但它在认证过程中所使用的椭圆曲线点乘点运算达 9 次之多，明显增加了运算总用时。根据表 4 和表 5 的比较分析可知，本协议在安全性和效率方面的综合性能优于其他相关协议。

表 5 安全特性比较

安全特性	文献[8]协议	文献[16]协议	文献[17]协议	文献[18]协议	文献[19]协议	本协议
抗重播攻击	√	√	√	NA	√	√
抗离线口令猜测攻击	√	√	√	√	√	√
抗Stolen-Verifier攻击	√	√	√	√	NA	√
抗冒充服务器攻击	×	√	NA	√	√	√
抗身份假冒攻击	√	√	NA	√	√	√
抗内部人员攻击	√	√	√	√	√	√
抗Denning-Sacco攻击	√	√	NA	NA	√	√
保护用户匿名性	×	√	√	√	√	√
具备前向安全性	√	√	√	√	√	√
实现双向认证	×	√	√	√	√	√

备注：√表示该协议支持这一安全特性；×表示该协议不支持这一安全特性；NA表示该安全特性不适用于此协议

6 应用场景分析

与所有新兴技术一样，即时通信面临着需要克服安全方面的挑战，以确保该技术能够成功大规模部署。在保密性、完整性和真实性方面，安全方面的挑战尤为重要。SIP 协议有良好的可扩展性，在语音通信、视频通信、网络游戏、物联网等领域应用前景广阔，但如果把生物特征、智能卡和公钥密码体制等多种安全因素同时糅合到改良的 SIP 协议中，确实可以大大提升 SIP 协议的安全性能，但同时也将给协议带来臃肿，执行效率退化等问题。

身份认证协议的安全级别越高，它所需的运算量、带宽要求、应用成本等各种开销也大。找寻认证协议的安全性能和开销的合理平衡点一直是协议设计者的追求目标。本协议使用少量的椭圆曲线点乘运算和必要的 hash 运算，较好地保持了 SIP 协议轻量化的优势，可以认为本协议在认证安全性能与认证开销之间获得一个较好的平衡点，适用于对安全性能有较高要求的应用场景：涉及商业机密的企业通信、涉及国家机密的政府和军事应用、涉及个人健康信息的医疗保健行业以及可能使用 SIP 协议来传输银行交易敏感信息的金融机构。

7 结 束 语

本文对文献 [8] 提出的 SIP 认证协议展开深入研究，指出其存在的安全缺陷。通过改良协议的认证消息格式，提出一种新的 SIP 认证协议。通过 BAN 逻辑形式化分析，以及多种非形式化的安全分析证明，新的 SIP 认证协议可以安全地抵御各种已知的安全攻击，既保护了用户匿名性又可以实现双向认证，具备协商生成后续会话所需一次性密钥的功能。通过效能比较分析可知，新协议是高效、安全的，具有较高的实际应用和推广价值。

参 考 文 献

[1] FENG Y T, XIONG F, HUANG W C, et al. Security analysis of session initiation protocol digest access

authentication scheme[C]//2021 7th International Conference on Big Data Computing and Communications (BigCom). [S.l.]: IEEE, 2021, 5: 129-135.

[2] DURLANIK A, SOGUKPINAR I. SIP authentication scheme using ECDH[J]. International Journal of Computer, Control, Quantum and Information Engineering, 2007, 1(8): 2624-2627.

[3] YOON E J, YOO K Y. Cryptanalysis of DS-SIP authentication scheme using ECDH[C]//2009 International Conference on New Trends in Information and Service Science. Beijing: IEEE, 2009: 642-647.

[4] LIU F, KOENIG H. Cryptanalysis of a SIP authentication scheme[C]//Communications and Multimedia Security. Berlin: IFIP, 2011, 134-143.

[5] XIE Q. A new authenticated key agreement for session initiation protocol[J]. International Journal of Communication Systems, 2012, 25(1): 47-54.

[6] FARASH M S, ATTARI M A. An enhanced authenticated key agreement for session initiation protocol[J]. European Integration Studies, 2013, 42(4): 333-342.

[7] ZHANG Z Z, QI Q Q, KUMAR N, et al. A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography[J]. Multimedia Tools & Applications, 2015, 74(10): 3477-3488.

[8] LU Y R, LI L X, PENG H P, et al. A secure and efficient mutual authentication scheme for session initiation protocol[J]. Peer-to-Peer Networking and Applications, 2016, 9(2): 449-459.

[9] KUMARI S, KARUPPIAH M, DAS A K, et al. Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography[J]. Journal of Ambient Intelligence and Humanized Computing, 2018, 9(3): 643-653.

[10] 戴聪. 基于国密算法和模糊提取的多因素身份认证方案[J]. 计算机应用, 2021, 41(S2): 139-145.
DAI C. Multi-Factor authentication scheme based on national secret algorithm and fuzzy extractor[J]. Journal of Computer Applications, 2021, 41(S2): 139-145.

[11] 黄可可, 刘亚丽, 殷新春. 一种基于 PUF 的超轻量级 RFID 标签所有权转移协议[J]. 密码学报, 2020, 7(1): 115-133.
HUANG K K, LIU Y L, YIN X C. A PUF-based ultra-lightweight ownership transfer protocol for low-cost RFID tags[J]. Journal of Cryptologic Research, 2020, 7(1): 115-133.

[12] 吴恺凡, 殷新春. 基于随机运算符的轻量级匿名射频识别系统双向认证协议[J]. 计算机应, 2021, 41(6): 1621-1631.
WU K F, YIN X C. Lightweight anonymous mutual authentication protocol based on random operators for radio frequency identification system[J]. Journal of Computer Applications, 2021, 41(6): 1621-1631.

[13] 黄朝阳, 赵玉超. 安全高效的三因素远程身份认证协议[J]. 电子科技大学学报, 2022, 51(3): 425-431.
HUANG C Y, ZHAO Y C. A secure and efficient remote authenticated protocol based on three factor[J]. Journal of University of Electronic Science and Technology of China, 2022, 51(3): 425-431.

[14] 张平, 果亚敏. 前向安全的椭圆曲线数字签名方案[J]. 计算机工程与应用, 2020, 56(1): 115-120.
ZHANG P, LI Y M. Forward secure elliptic curve digital signature scheme[J]. Computer Engineering and Applications, 2020, 56(1): 115-120.

[15] 曹阳, 基于扩展混沌映射的动态身份认证密钥协商协议[J]. 成都理工大学学报 (自然科学版), 2021, 48(4): 505-512.
CAO Y. Dynamic identity authentication key agreement protocol based on extended chaos mapping[J]. Journal of Chengdu University of Technology (Science & Technology Edition), 2021, 48(4): 505-512.

[16] ZHOU Y S, CHEN X Y. An anonymous and efficient ECC-based authentication scheme for SIP[J]. Wireless Communications and Mobile Computing, 2020, 2020(11): 1-11.

[17] HASSAN U M, CHAUDHRY S A, IRSHAD A, et al. An improved SIP authenticated key agreement based on dongqing[J]. Wireless Personal Communications, 2020, 110(4): 2087-2107.

[18] LU Y R, ZHAO D W. An anonymous SIP authenticated key agreement protocol based on elliptic curve cryptography[J]. Mathematical Biosciences and Engineering, 2021, 19(1): 66-85.

[19] MAHOR V K, PADMAVATHY R, CHATTERJEE S. Chebyshev chaotic map-based efficient authentication scheme for secure access of VoIP services through SIP[J]. International Journal of Security and Networks, 2022, 17(1): 39-47.

编　辑　税　红