认证与密钥协商协议的设计及其应用

章丽平　著

科学出版社

认证与密钥协商协议的设计及其应用

章丽平 著

科学出版社

北京

内 容 简 介

本书主要介绍认证与密钥协商协议的设计方法及协议中涉及的相关知识，针对不同应用环境，如 VoIP 网络、E-health 环境、智能电网等，采用不同方法构建适用于不同应用环境的认证与密钥协商协议，实现不同应用环境中通信实体间的相互认证和密钥协商，还提出基于椭圆曲线的认证与密钥协商协议、基于混沌映射的认证与密钥协商协议、基于三因子的认证与密钥协商协议等一系列协议，并从多个角度对提出的认证与密钥协商协议进行深入剖析，为认证与密钥协商协议的构建提供参考。

本书适合高等院校本科生、研究生或从事认证与密钥协商协议领域研究的科研工作者阅读。

图书在版编目（CIP）数据

认证与密钥协商协议的设计及其应用/章丽平著. —北京：科学出版社，2019.11

ISBN 978-7-03-063175-6

Ⅰ. ①认… Ⅱ. ①章… Ⅲ. ①计算机网络-网络安全-研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 246534 号

责任编辑：闫 陶 / 责任校对：高 嵘
责任印制：彭 超 / 封面设计：莫彦峰

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
北京虎彩文化传播有限公司 印刷
科学出版社发行 各地新华书店经销
*
2019 年 11 月第 一 版 开本：B5（720×1000）
2019 年 11 月第一次印刷 印张：9 3/4
字数：195 000
定价：65.00 元
（如有印装质量问题，我社负责调换）

前　言

认证与密钥协商协议是实现信息在互联网中安全传输的一种有效手段。当通信实体通过不安全的网络进行信息传输时，易遭攻击者的各种恶意攻击，因此需要采用安全防护措施保护传输信息的安全。为了有效抵御各种恶意攻击，通信实体在通信之前需要实现相互身份认证，确认通信方的合法性。此外，还需要在相互认证的过程中协商一个只有通信双方认可的共享会话密钥，该密钥将用于加密后信息的传输，从而实现信息在互联网中安全传输。

认证与密钥协商协议的应用较为广泛，不同的应用环境对认证与密钥协商协议所需满足的安全需求也不相同，有些应用环境对安全性的需求较高，有些应用环境对能耗的要求较为严格。针对不同的应用环境，认证与密钥协商协议所采用的设计方法也不相同。例如，在数字医疗健康网络(E-health)环境中，认证与密钥协商协议的构建不仅需要充分考虑用户的隐私保护问题，还需要考虑低能耗医疗传感设备计算能力的受限问题。因此，在 E-health 中构建认证与密钥协商协议时应尽量避免采用耗时的操作，这也为认证与密钥协商协议的设计带来了挑战。尽管如此，诸多学者针对不同的应用环境，深入研究认证与密钥协商协议的设计理论和方法，也设计出一系列的高效认证与密钥协商协议。然而，如何在不安全的网络环境中，构建能满足安全需求的轻量级认证与密钥协商协议，仍然是一个有待进一步研究解决的难题。

本书针对不同应用环境的安全与性能需求，提出若干认证与密钥协商协议的设计方法和具体设计过程，并对提出的认证与密钥协商协议的安全性和性能进行分析，并将本书提出的协议与当前其他认证与密钥协商协议进行对比分析。提出的若干认证与密钥协商协议采用不同的设计方法，有的是基于椭圆曲线加密体制的，有的是基于混沌映射的，有的是基于动态验证列表的。认证与密钥协商协议的设计是一个复杂的过程，在协议构建过程中需要考虑诸多因素，需要满足一系列的安全需求，还要考虑能耗的限制。认证与密钥协商协议的构建更注重细节上的设计，精巧的设计可以使认证与密钥协商协议更加完美，在达到轻量级要求的同时满足更多的安全需求。

本书提出不同的认证与密钥协商协议设计的详细过程及设计思想，并提出不同的安全性分析与证明方法，最后给出实验过程。目的在于，对近几年从事的认

证与密钥协商协议研究工作做一个总结，并供研究认证与密钥协商协议的学术同仁参考。希望本书能起到抛砖引玉的作用，让更多的学者参与到认证与密钥协商协议的研究中，推动认证与密钥协商协议研究的发展。由于认证与密钥协商协议研究领域的快速发展，加之作者水平有限，疏漏之处在所难免，望各位学术同仁不吝赐教。

章丽平

2019 年 8 月 31 日于中国地质大学(武汉)

目　录

第1章 绪 论

1.1 认证与密钥协商协议概述

认证与密钥协商协议(authenticated key agreement scheme)是实现互联网实体间安全通信的一种有效方法。通信实体在互联网中的信息传输易遭攻击者的恶意攻击。攻击者可以通过窃听等方式获取通信实体间传输的信息，进而可以实施各种有针对性的攻击，如重放攻击、中间人攻击、假冒攻击等，从而获取相应的信息，达到一定的目的。认证与密钥协商协议可以有效保护通信实体之间的信息传输。为了在互联网中实现信息的安全传输，在通信实体进行交互之前，需要完成通信实体间的身份认证,并由通信实体协商一个仅有通信方知道的共享会话密钥。该密钥将用于加密通信实体间之后需要传输的信息，从而实现通信实体间信息的安全传输。

认证与密钥协商协议为不安全信道间消息的安全传输提供了一种有效的保护手段,受到了学术界和工业界的广泛关注。许多应用环境,如 VoIP(voice over internet protocol)网络、E-health、智能电网等，都采用了认证与密钥协商协议来实现信息在通信实体间的安全传输。以 E-health 为例，当用户需要与医疗服务器进行通信来获取相关医疗服务时，为了确保医疗数据在互联网中的传输安全，首先需要用户与医疗服务器完成相互认证，以确认用户和医疗服务器的合法性，通过身份认证后，用户与医疗服务器应协商出一个秘密的共享会话密钥，该密钥将用于加密之后需要传输的医疗数据，从而实现用户与医疗服务器之间信息的安全传输。

认证与密钥协商协议可以为通信实体间的信息传输提供保障。但认证与密钥协商协议的设计却是一项复杂的工作。认证与密钥协商协议需要满足一系列的安全需求，针对不同的应用环境还可能面临严格的能耗限制，对认证与密钥协商协议的构建提出了挑战。认证与密钥协商协议需要满足的安全需求如下。

(1) 相互认证。为了确保只有合法的通信方才能接收到信息，通信双方需要完成相互认证。

(2) 具备通信实体匿名和不可追踪性。为了保护通信实体的隐私，需要具备通信实体匿名和不可追踪性。通信实体匿名和不可追踪安全属性确保了攻击者既

不能获取通信实体的真实身份又不能区分两次会话是否来自同一个通信实体，从而为通信实体的隐私提供有效的安全防护。

(3) 密钥协商。通信实体间的信息传输需要采用共享密钥进行加密来保护传输的信息。密钥协商确保了采用的共享会话密钥在每一轮会话过程中都是唯一的，且只有进行会话密钥协商的通信方知道该共享会话密钥。

(4) 提供安全特征。认证与密钥协商协议需要提供一系列的安全特征，包括完美前向安全、已知密钥安全、会话密钥安全和无时钟同步需求等。

(5) 抵抗已知攻击。认证与密钥协商协议能抵抗已知攻击，包括重放攻击、假冒攻击和中间人攻击等。

1.2 认证与密钥协商协议的应用

认证与密钥协商协议可以应用在多种场景，用于保护信息的安全传输。本书选取了几个有代表性的应用场景，如 VoIP 应用环境、E-health 应用环境和智能电网应用环境。下面对上述应用环境进行简单的介绍。

VoIP 应用环境中的通信实体主要包括用户和服务器(SIP 服务器)，为了确保语音信息在互联网中的安全传输，可采用认证与密钥协商协议实现用户与服务器之间的相互认证和密钥协商，并采用协商出的密钥加密之后需要传输的语音信息。在该应用环境中，认证与密钥协商协议的设计需要充分考虑响应时间，这意味着认证与密钥协商协议中不能采用耗时的操作，以免导致计算时间较大，延长响应时间。

E-health 应用环境中包含大量的低能耗医疗传感设备，这些传感设备佩戴在人体身上或植入人体内，获取人体的生物医学信号，并通过互联网传输到医院等健康监测中心，为患者和医务人员提供持续的健康监测和实时的信息反馈。在该应用环境中，信息生物医学信号的传输需要通过互联网，而患者极度隐私的医疗信息在互联网传输过程中有可能会泄露或遭受到诸如窃听、篡改、假冒等各种有针对性的恶意攻击。一旦医疗信息在传输过程中被攻击，将直接影响医生对病情的诊断，甚至威胁患者的生命。采用认证与密钥协商协议可实现用户与医疗服务器之间的相互认证和密钥协商，可在互联网中有效保护用户传输的医疗信息。目前，E-health 环境中涉及的低能耗医疗传感设备受到能量的严格限制。例如，植入式医疗传感设备(心脏起搏器等)，其更换需要外科手术的介入。因此，在保证安全性、提供用户隐私保护的前提下，认证与密钥协商协议的设计应尽可能地降低协议所需的计算开销，以延长低能耗医疗传感设备的使用时间。

在智能电网环境中，通信实体间的信息交互是通过互联网实现的，信息在不

安全的网络上进行传输时，易遭攻击者的各种恶意攻击。例如，攻击者可以轻易地通过窃听来拦截消息，并发起各种攻击以获取相关信息。一旦敏感信息被攻击者获取，智能电网可能会面临更大的安全挑战。认证与密钥协商协议可以为智能电表与其相应的电力服务提供商之间的信息传输提供安全保障。采用认证与密钥协商协议可以实现用户与电力服务提供商之间的相互认证，在确认通信方的合法身份后，用户与电力服务提供商之间将协商出一个只有通信双方知道的共享会话密钥。该密钥可用于加密之后需要传输的信息，从而确保智能电表与电力服务提供商在互联网中的安全通信。由于智能电表端不具备输入功能，口令和生物信息等需要输入技术的支持，不能应用于该环境下的认证与密钥协商协议设计中。从而，增加了智能电网环境下认证与密钥协商协议的设计难度。

根据上述分析，VoIP 应用环境、E-health 应用环境和智能电网应用环境中，认证与密钥协商协议的设计具有不同的特征。因而，采用的技术和方法也有所不同。但认证与密钥协商协议所需满足的安全需求在上述三种应用环境中是相同的。就计算开销而言，相比 VoIP 应用环境和智能电网应用环境，E-health 应用环境对能耗的限制更加严格，应采用轻量级操作构建认证与密钥协商协议。本书将针对这三类应用环境，采用不同的方法构建认证与密钥协商协议，并对提出的协议安全性和性能进行详细的分析。

第 2 章　VoIP 环境下认证与密钥协商协议设计

2.1　VoIP 应用环境概述

VoIP 是一种以 IP 电话为主，并推出相应增值业务的技术[1]。VoIP 不仅可以在 IP 网络上廉价地传输语音，还能提供视频、数据传输和传真功能，以及相应的增值服务，如电视会议、虚拟电话、电子商务等。与传统电话相比，VoIP 的通话费用，尤其是国际长途通话费用，要便宜几十倍。目前，至少有 5 亿人采用 VoIP 提供商 Skype 提供的服务。Skype、Gtalk 和 iPhone 的广泛应用，以及运营商投资 VoIP 认证和安全传输技术的研究有效促进了 VoIP 网络的快速发展。随着下一代网络的迅速发展，VoIP 必将取代传统的 PSTN(public switched telephone network，公共交换电话网络)，成为信息传输的主流形式。

然而，在 VoIP 的发展过程中，运营商和设备制造商将重点放在语音质量的改善和多种通信网融合上面，并没有充分考虑其安全特性。VoIP 技术发展至今已面临诸多安全威胁：一方面，以 Internet 为基础的 VoIP 应用，继承了来自 Internet 的安全威胁，如 DoS(denial of service)攻击和窃听等；另一方面，存在专门针对 VoIP 的攻击，如 SPIT(SPam over internet telephony)攻击[2]和通话拦截等。这些安全威胁严重阻碍了 VoIP 网络的快速发展。随着 VoIP 用户的大量增加，VoIP 网络安全通信将成为一个严峻的技术挑战。这也关系到用户是否会持续选择使用 VoIP 网络。

采用认证与密钥协商协议可以为语音信息在 VoIP 网络中的传输提供安全保护。然而，大多数针对 VoIP 网络的认证与密钥协商协议存在一定的局限性：服务器需要存储验证列表，易遭有针对性地盗取验证列表攻击和服务器欺骗攻击；口令更新困难，方案难于扩展；需要通过发送用户的真实身份来实现通信实体之间的相互认证，泄露了用户的隐私等。如何实现通信实体间的相互认证和密钥协商，为 VoIP 网络通信提供安全保护已成为 VoIP 网络快速发展急需解决的首要问题之一。为了有效解决上述难题，诸多学者开展了一些有价值的工作。

会话初始协议(session initial protocol，SIP)是 VoIP 网络中应用最广泛的应用

层信令控制协议[3]。该协议定义了通信实体间会话过程的建立、修改和终止[4]。与H.232协议相比，SIP设计得更加灵活、轻便。然而，传统的基于SIP的认证机制采用的是基于超文本传输协议的摘要认证机制，易于遭受各种类型的安全威胁和攻击。Yang等[5]首次指出传统的SIP认证机制不能有效抵抗离线词典攻击和服务器欺骗攻击，并基于D-H(Diffie-Hellman)密钥交换[6]提出了一个新的认证协议。然而，提出的改进认证协议[5]被证明同样不能有效抵抗离线词典攻击，且需要执行昂贵的模乘运算[7-8]。Palmieri等[9]采用数字签名技术和流加密技术实现了通信实体间的认证和密钥协商。但该协议存在密钥托管问题。闻英友等[10]采用双线性映射实现了VoIP环境中跨域的身份认证和密钥协商[11]。Liao和Wang[12]基于椭圆曲线密码体制，采用自认证公钥技术构造了一个安全的认证和密钥协商机制。但上述协议需要执行昂贵的模乘或双线性映射运算，导致终端设备的计算量大。

为了在增强安全性的同时有效降低计算量，Wu等[13]基于椭圆曲线加密体制构建了一个低能耗的认证协议，并采用CK安全模型[14]对提出的协议进行了形式化安全证明。然而，提出的协议需要预先在ISIM(IM services identity module)和认证中心(authentication center，AC)之间共享一个秘密。共享秘密的预先分配使得该协议难于扩展。此外，该协议还易于遭受离线词典攻击、Denning-Sacco攻击及盗取验证列表攻击。Yoon等[15]针对Wu等提出的协议存在的安全问题进行了改进。但Pu[16]和Gokhroo等[17]对Yoon等提出的改进协议进行了安全性分析后，指出改进的协议仍然存在同样的安全问题。Tsai[18]基于Nonce构建了一个认证协议。该协议仅使用了哈希(Hash)函数和异或操作，实现了通信实体间的相互认证和密钥协商，从而进一步降低了通信节点的计算开销。然而，Tsai[18]提出的协议不能有效抵抗离线词典攻击、Denning-Sacco攻击及盗取验证列表攻击，且不具备前向安全性[19-20]。Yoon等[19]基于Tsai的工作，提出了一个安全性增强的改进协议。但提出的改进协议并没有解决上述安全问题[21]。Xie也针对Tsai提出的协议存在的安全问题进行了改进[20]，然而，提出的改进协议仍然不能有效抵抗离线词典攻击[22]。

尽管诸多学者对基于SIP的认证协议进行了研究，但上述研究成果存在一些局限性：①大多需要在SIP服务器端存储口令或验证列表，用于验证注册用户的有效身份，该类协议容易遭受词典攻击、盗取验证列表攻击和服务器欺骗攻击；②由于口令或验证列表通常非常庞大，验证列表的维护使得该类协议难于扩展；③未考虑用户隐私保护问题，在认证过程中，用户的真实身份采用明文传输，因此，攻击者可以通过窃听等方式获取用户的真实身份，从而实施有针对性的攻击；④不提供口令更新功能，用户口令更新困难。

为了避免服务器端存储验证列表，以有效抵抗针对验证列表的攻击，Yoon和

Yoo 通过引入生物认证技术和智能卡技术，有效解决了服务器端需要存储验证列表的难题[23]。笔者针对上述问题进行了研究，采用智能卡技术，在无须服务器端存储验证列表的情况下，实现了通信实体间的相互认证和密钥协商，并给出了高效的用户口令更新方法[24]。在研究过程中，笔者发现尽管以上协议有效地避免了服务器端存储验证列表，但存在用户隐私(身份信息、生物特征信息)保护问题。因此，如何保证生物特征信息的安全已成为上述协议需要解决的关键。为了解决上述问题，笔者进行了逐步深入的研究，针对 VoIP 应用环境，综合考虑认证与密钥协商协议所需满足的安全需求，采用不同的方法构造了几个适用于 VoIP 网络的认证与密钥协商协议[25]。下面将针对提出的协议进行详细阐述。

2.2 基于椭圆曲线的认证与密钥协商协议设计

在 VoIP 网络中，为了有效抵抗攻击者的恶意攻击(如中间人攻击)，需要为通信双方提供快速有效的身份认证和密钥协商。然而，在基于 SIP 的 VoIP 网络中，大多数认证与密钥协商协议需要在服务器端维护验证列表。服务器端存储验证列表的解决方案，易于遭受盗取验证列表攻击和服务器欺骗攻击，且面临用户口令更新困难和协议难于扩展等问题。本节针对 VoIP 应用环境，采用椭圆曲线密码体制构建三个基于 SIP 的认证与密钥协商协议。提出的协议中，SIP 服务器端无须存储验证列表，一方面有效抵抗了针对验证列表的各种恶意攻击，另一方面也消除了因验证列表造成的口令更新困难和难于扩展问题。

2.2.1 无验证列表的认证与密钥协商协议设计

1. 协议设计

本节对无验证列表的认证与密钥协商协议进行详细描述。如图 2-1 所示，提出的认证与密钥协商协议包括四个阶段：系统初始化阶段、用户注册阶段、认证与密钥协商阶段及用户口令更新阶段。

1) 系统初始化阶段

系统初始化阶段，用户 U 和 SIP 服务器 S 协商一系列参数。

步骤 S1：SIP 服务器 S 选取椭圆曲线 $E_p(a, b)$: $y^2=x^3+ax+b \pmod p$，其中 p 为大素数，$a, b \in F_p$，且 $4a^3+27b^2 \neq 0 \pmod p$。椭圆曲线上所有整点的集合构成循环加法群 G，且 G 有素数阶 q, P 为生成元。

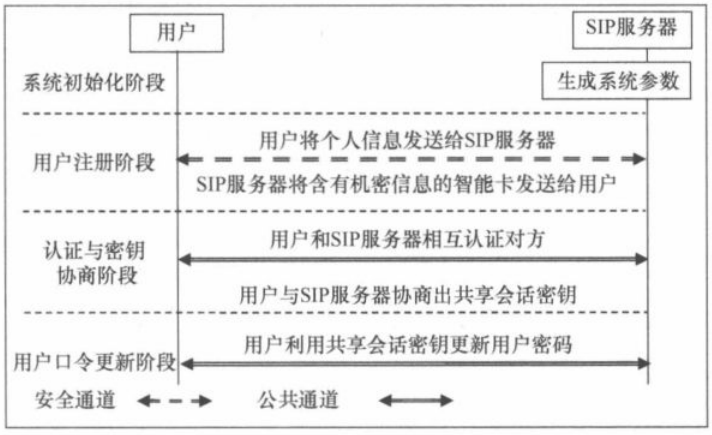

图 2-1　认证与密钥协商机制

步骤 S2：SIP 服务器 S 选择一个高熵随机数 $s \in_R Z_q^*$ 作为自己的私钥，进行秘密保存。并构造两个安全的单向哈希函数 $h(\cdot)$: $\{0,1\}^* \to \{0,1\}^k$ 和 $h_1(\cdot)$: $G \times G \times G \times \{0,1\}^* \to \{0,1\}^k$。

步骤 S3：SIP 服务器 S 发布公共信息 $\{E_p(a, b), P, h(\cdot), h_1(\cdot)\}$。

2) 用户注册阶段

当用户 U 向 SIP 服务器 S 进行注册时，需要执行如下步骤。

步骤 R1：$U \to S$: $(h(PW||a), username)$。

用户 U 自由选择用户口令 PW 和一个高熵随机数 $a \in_R Z_q^*$。然后，用户 U 计算 $h(PW||a)$，并通过安全方式将消息 $\{h(PW||a), username\}$ 发送给 SIP 服务器 S。

步骤 R2：$S \to U$ 智能卡含有信息®。

SIP 服务器 S 接收到用户 U 发送的消息后，为用户 U 计算秘密信息 $R = \dfrac{h(PW\|a)}{h(username)+s} P$ 的值。然后，SIP 服务器 S 将机密信息 R 存储在用户 U 的智能卡内存中，并将该智能卡通过安全方式发送给用户 U。

步骤 R3：智能卡用户(R, a)。

当用户 U 接收到 SIP 服务器 S 发送的智能卡后，他将高熵随机数 a 写入智能卡内存中。此时，智能卡中存储的秘密信息为(R, a)。

3) 认证与密钥协商阶段

当用户 U 需要登录 SIP 服务器 S 时，智能卡和 SIP 服务器 S 合作完成如下步骤来实现相互认证和密钥协商，具体过程如图 2-2 所示。

步骤 A1：$U \to S$: $REQUEST(username, V, W)$。

用户 U 选取一个高熵随机数 $b \in_R Z_q^*$，并计算 $V=bR$ 和 $W=bh(PW||a)P$。然后，

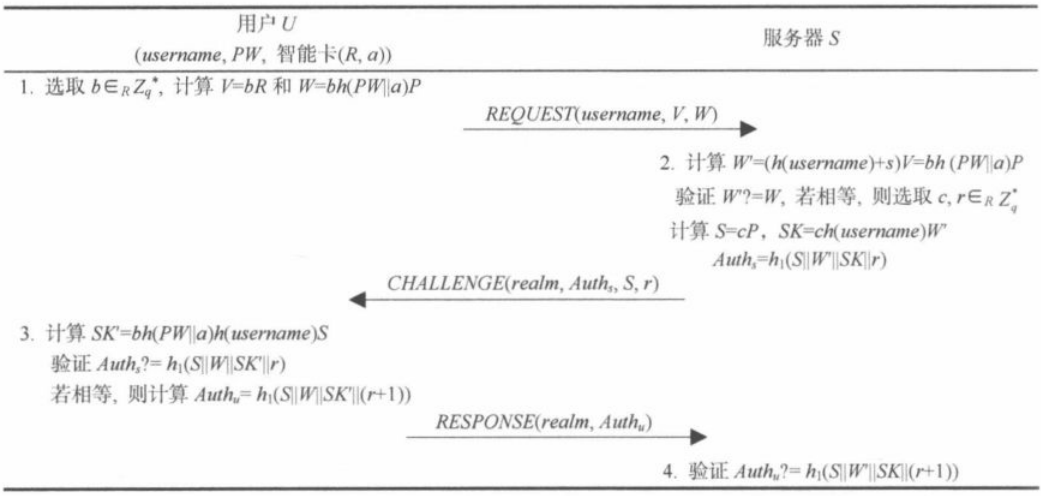

图 2-2　无验证列表的认证与密钥协商过程

用户 U 发送请求信息 $REQUEST(username, V, W)$给 SIP 服务器 S。

步骤 A2：$S \rightarrow U$: $CHALLENGE(realm, Auth_s, S, r)$。

当接收到用户 U 发送的请求信息后，SIP 服务器 S 计算 $W'=(h(username)+s)V=(h(username)+s)bR=bh(PW||a)P$ 的值。然后验证等式 $W'=W$ 是否成立。如果等式成立，则选择两个高熵随机数 c, $r \in_R Z_q^*$，并计算 $S=cP$，$SK=ch(username)W'=cbh(PW||a)h(username)P$ 和认证信息 $Auth_s=h_1(S||W'||SK||r)$。最后，SIP 服务器 S 发送挑战信息 $CHALLENGE(realm, Auth_s, S, r)$给用户 U。

步骤 A3：$U \rightarrow S$: $RESPONSE(realm, Auth_u)$。

当用户 U 接收到 SIP 服务器发送的挑战信息后，用户 U 输入其用户口令信息 PW 和用户名 $username$ 来计算共享会话密钥 $SK'=bh(PW||a)h(username)S=cbh(PW||a)h(username)P$。然后，用户 U 验证等式 $Auth_s=h_1(S||W||SK'||r)$是否成立。如果等式成立，用户 U 则计算用户认证信息 $Auth_u=h_1(S||W||SK'||(r+1))$，并发送应答信息 $RESPONSE(realm, Auth_u)$给 SIP 服务器 S；否则，用户 U 删除接收到的信息，并终止认证与密钥协商协议。

步骤 A4：当接收到用户 U 发送的应答信息后，SIP 服务器 S 将验证等式 $Auth_u=h_1(S||W'||SK||(r+1))$是否成立。如果等式成立，SIP 服务器 S 将计算得到的会话密钥 SK 作为它与用户 U 之间的共享会话密钥进行保存；否则，SIP 服务器 S 将删除接收到的信息，并终止协议。

4) 用户口令更新阶段

当用户 U 想要更新他的用户口令时，首先需要在先前的认证过程中与 SIP 服

务器 S 协商出一个共享会话密钥 SK。然后，用户 U 再按如下步骤更新口令。用户口令更新的详细过程如图 2-3 所示。

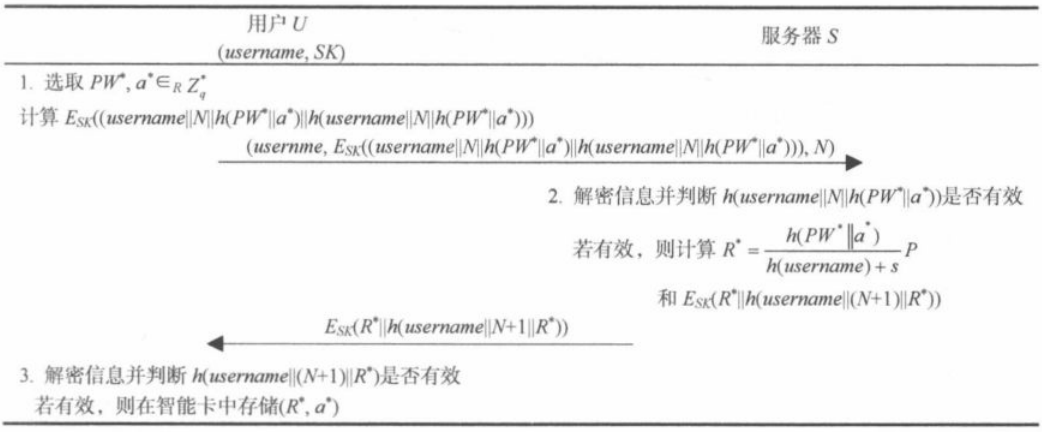

图 2-3　用户口令更新过程

步骤 P1：$U \rightarrow S$: $(usernme, E_{SK}((username||N||h(PW^*||a^*)||h(username||N||h(PW^*||a^*))), N)$。

用户 U 选择新的用户口令 PW^* 和一个高熵随机数 $a^* \in_R Z_q^*$。然后，采用之前与 SIP 服务器 S 协商的共享会话密钥 SK 对新的口令信息 $(username, h(PW^*||a^*))$ 进行加密。接下来用户 U 将用户名 $username$，加密信息 $E_{SK}((username||N||h(PW^*||a^*)||h(username||N||h(PW^*||a^*)))$ 和新鲜性检验信息 N 发送给 SIP 服务器 S。

步骤 P2：SIP 服务器 S 接收到信息后，首先采用共享会话密钥 SK 解密接收到的信息，然后验证认证标识 $h(username||N||h(PW^*||a^*))$ 是否有效。如果有效，则计算新的秘密信息 $R^* = \dfrac{h(PW^* \| a^*)}{h(username)+s} P$。接下来，SIP 服务器 S 将采用共享会话密钥 SK 加密机密信息生成 $E_{SK}(R^*||h(username||(N+1)||R^*))$，并将该值发送给用户 U。

步骤 P3：当用户 U 接收到 SIP 服务器 S 发送的信息后，他首先采用共享会话密钥 SK 解密接收到的信息，然后验证认证标识 $h(username||(N+1)||R^*)$ 的有效性。如果该认证标识有效，用户 U 将用新的机密信息 (R^*, a^*) 替换之前存储在智能卡内存中的 (R^*, a^*)，并进行秘密保存。

2. 安全性分析

1) 提出的协议可以有效抵抗重放攻击

假设攻击者 Bob 截获了用户 U 发送给 SIP 服务器 S 的请求信息 $REQUEST(username, V, W)$，并将该信息再次发送给 SIP 服务器 S。然而，攻击者 Bob 在不知道 SIP 服

务器 S 私钥信息 s，用户选取的高熵随机数 b，或者正确猜测用户口令 PW 和两个高熵随机数(a，b)的情况下，将无法计算出合适的 SK 来构造有效的认证信息 $Auth_u$，当 SIP 服务器 S 对认证信息 $Auth_u$ 进行验证时，将发现该攻击。当攻击者 Bob 试图从截获的信息 V 或 W 中猜测(s, b)或(PW, a, b)时，他将面临解决椭圆曲线离散对数问题。

另外，假设攻击者 Bob 截获了 SIP 服务器 S 发送给用户 U 的挑战信息 $CHALLENGE$ ($realm$, $Auth_s$, S, r)，并将该信息重新发送给用户 U。该信息将无法通过用户 U 的认证过程。这是因为高熵随机数 b 是由用户 U 随机选择的，且在每次会话过程中都是不一样的。显然攻击者 Bob 无法控制 b 的生成。这样，当用户 U 验证认证信息 $Auth_s = h_1(S||W||SK'||r)$是否成立时，将会发现该攻击。在此情况下，攻击者 Bob 不会收到任何应答信息。因此，提出的协议能有效抵抗重放攻击。

2) 提出的协议可以有效抵抗中间人攻击

在提出的协议中，用户 U 和 SIP 服务器 S 只有在相互认证后才会生成共享会话密钥 SK。因此攻击者 Bob 在没有通过 SIP 服务器 S 认证的情况下，无法跟 SIP 服务器 S 生成共享会话密钥，并欺骗 SIP 服务器 S，使其相信该共享密钥是与用户 U 协商生成的。如果攻击者 Bob 试图通过 SIP 服务器 S 的认证，他将面临解决椭圆曲线离散对数问题。同理，攻击者 Bob 也不能假冒 SIP 服务器 S 来与用户 U 共享一个会话密钥。因此，提出的协议能有效抵抗中间人攻击。

3) 提出的协议可以有效抵抗 Denning-Sacco 攻击

在提出的协议中，用户 U 与 SIP 服务器 S 协商生成的共享会话密钥为 $SK = ch(username)W' = cbh(PW||a)h(username)P$。假设攻击者 Bob 获取了先前的会话密钥，他也无法从截获的信息及先前的共享会话密钥 SK 中获取用户 U 的用户口令。这是因为想要从 SK 中提取用户 U 的用户口令，将面临解决椭圆曲线离散对数问题。因此，提出的协议能有效抵抗 Denning-Sacco 攻击。

4) 提出的协议可以有效抵抗盗取验证列表攻击

假设攻击者 Bob 试图通过偷盗 SIP 服务器 S 中的验证列表来实施盗取验证列表攻击，以获取有用的信息。在提出的协议中，SIP 服务器 S 端无须存储用户口令列表或验证列表，显然攻击者 Bob 无法在提出的协议中实施盗取验证列表攻击。因此，提出的协议能有效抵抗盗取验证列表攻击。

5) 提出的协议可以有效抵抗假冒攻击

假设攻击者 Bob 通过构造 V^* 和 W^*，伪造了用户发送给 SIP 服务器 S 的请求信息($username$, V^*, W^*)，并假冒用户 U 将该伪造信息发送给 SIP 服务器 S。由于攻击者 Bob 在不知道 SIP 服务器 S 私钥 s 的情况下无法构造一个有效的 R 值，SIP 服务器在验证 W' 和 W^* 值是否相等时，将会发现该攻击。此外，即使攻击者 Bob 是一个合法用户(不是用户 U)，他也不能用自己的私钥计算出其他合法用户的私钥。这是因为攻击者 Bob 在不知道 SIP 服务器 S 私钥 s 的情况下无法构造一个有效的 R 值。