两个认证密钥协商协议的前向安全性分析

程庆丰 马玉千*

(战略支援部队信息工程大学 郑州 450001)

(数学工程与先进计算国家重点实验室 郑州 450001)

摘 要：目前，网络安全及隐私受到广泛关注。前向安全性是Günther在1989年提出的一种认证密钥协商协议(AKA)的安全属性(doi: 10.1007/3-540-46885-4_5)，该性质经过30年的蓬勃发展已经成为研究领域的热点之一。该文主要分析了MZK20和VSR20两个AKA协议。首先在启发式分析的基础上，利用BAN逻辑分析了MZK20协议不具有弱前向安全性；其次利用启发式分析和Scyther工具证明了VSR20协议不具备前向安全性。最后，在分析VSR20协议设计缺陷的基础上，提出了改进方案，并在eCK模型下证明了改进后协议的安全性；并且，结合Scyther软件证明了改进VSR20协议与VSR20协议相比明显提高了安全性。

关键词：安全协议形式化工具分析；认证密钥协商协议；前向安全性

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2022)12-4294-10

DOI: 10.11999/JEIT211137

Cryptoanalysis on the Forward Security of Two Authenticated Key Protocols

CHENG Qingfeng MA Yuqian

(*Strategic Support Force Information Engineering University*, *Zhengzhou* 450001, *China*)

(*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Zhengzhou* 450001, *China*)

Abstract: At present, network security and privacy have attracted extensive attention. Forward security is a security attribute of Authenticated Key Agreement protocol (AKA) proposed by Günther in 1989. Since then, this property has become one of the hot topics. This paper analyzes the security properties of two AKA protocols, MZK20 and VSR20. First, based on heuristic analysis and BAN logic, MZK20 protocol is proved that it does not satisfy weak forward security. Second, using heuristic analysis and Scyther, it is proved that VSR20 protocol does not fulfill forward security. Finally, the enhanced VSR20 protocol is designed and proved more secure than VSR20. The security of the modified VSR20 is verified both by the use of security reduction under eCK model and Scyther.

Key words: Formal analysis of security protocols; Authenticated Key Agreement protocols (AKA); Forward Security

1 引言

1989年，Günther[1]首次提出了前向安全性的概念，同时提出了一个基于身份的AKA协议，并在文中证明了该协议满足前向安全性。随后，前向安全性受到越来越多的学者关注，具有前向安全特性的AKA协议也相继被提出，例如Matsumoto等人[2]提出了能够满足弱前向安全性质的密钥协商协议，Jeong等人[3]提出了能够满足强前向安全性质的一轮密钥协商协议。2005年，Krawczyk[4]指出，一轮AKA协议最多只能达到弱前向安全性。事实上，2010年，Boyd等人[5]指出该结论是不正确的，并给出了用于改进协议的通用模板，该模板能够在敌手不能够进行临时密钥泄露问询的情况下，使得一轮AKA协议达成强前向安全性。在现实生活应用中，前向安全性也正在逐步成为各方的研究热点。2014年，曹晨磊等人[6]为保证分属于不同层级的云实体能够进行安全的通信，提出了一个基于层级化身份的AKA协议，并在eCK模型下证明该协议能够满足前向安全性、已知密钥安全性等多种安全属性。2015年，杨孝鹏等人[7]利用格上判定带误

收稿日期：2021-10-15；改回日期：2022-04-20；网络出版：2022-05-10

*通信作者： 马玉千 yuqianm2000@qq.com

基金项目：国家自然科学基金(61872449)

Foundation Item: The National Natural Science Foundation of China (61872449)

差学习问题困难假设构造了一个AKA协议，同时证明了该协议在CK模型下是可证明安全的，能够达成弱前向安全性。2017年，熊婧和王建明[8]针对RFID技术在信息传递过程中的弱点提出了一个基于哈希函数的双向认证协议，并声明该协议具有一定程度上的防窃听、前向安全性、防位置追踪等属性。2020年，Li等人[9]面向无线医疗传感器网络系统提出了一个三方用户认证协议，并声称该协议能够满足前向安全性。然而一年后，Saleem等人[10]分析得出Li等人的协议不能够抵抗传感器节点的伪装攻击，并且不能够提供匿名性。连接至物联网中的设备计算能力、存储能力参差不齐，而它们需要满足的安全性质并没有减弱，许多学者面向物联网的不同应用环境提出了满足前向安全性的多个协议[11–16]。再以目前网络中广泛应用的传输层协议TLS为例，现在最新版本的TLS 1.3版本[17]仅允许使用满足前向安全的密钥交换方案。2021年，Boyd等人[18]将协议下的前向安全性扩展到其他密码原语中，并总结给出了为在不同密码原语中达到前向安全性的方法。更进一步的，Boyd等人通过将前向安全性进行分类、提出了能力更强的敌手，并声称该能力在之前的安全模型中并未包含。

另外，在前向安全性提出之后，研究者还将该性质添加至了安全模型中，从而使得AKA协议的前向安全性分析更加有说服力。2007年，结合前向安全性这个概念，LaMacchia等人[19]在原有CK模型[20]中添加了包含前向安全性在内的其他性质，提出了eCK模型，进一步完善了AKA协议的安全模型。目前，前向安全性经过30多年的蓬勃发展，可以根据敌手能力的不同分为以下几类：

(1) 前向安全性(Forward Security)。称一个协议具有前向安全性是指，当协议参与方中一方或多方的长期密钥泄露，协议之前达成的会话密钥仍是安全的。

(2) 部分前向安全性(Partial Forward Security)。称一个协议具有部分前向安全性是指，当协议参与方中指定一方或多方的长期私钥泄露，协议之前达成的会话密钥仍是安全的。

(3) 弱前向安全性(Weak Forward Security)。称一个协议具有弱前向安全性是指，在敌手为被动敌手的情况下，当协议参与方中一方或多方的长期私钥泄露，协议之前达成的会话密钥仍是安全的。

(4) 强前向安全性(Strong Forward Security)称一个协议具有强前向安全性是指，在敌手为主动敌手的情况下，当协议参与方中一方或多方的长期私钥泄露，协议之前达成的会话密钥仍是安全的。

在上述研究的基础上，本文首先分析了MZK20和VSR20两个AKA协议，首先利用BAN逻辑分析了MZK20协议不具有弱前向安全性；其次利用启发式分析和Scyther形式化证明工具证明了VSR20协议不具备前向安全性。进一步，本文在分析VSR20协议设计缺陷的基础上提出了改进方案，并在eCK模型下证明了改进后协议的安全性；并且，结合Scyther软件证明了改进VSR20协议与VSR20协议相比明显提高了安全性。

2　基础知识

2.1　数学困难问题

本节介绍分析和改进协议时用到的数学困难问题[21]。

定义1　椭圆曲线上的离散对数问题(Discrete Logarithm Problem over Elliptic Curve, ECDLP)。设E是定义在有限域Z_q上的椭圆曲线，P,Q是E上的任意两点，则求解满足等式$kP=Q$成立的唯一整数k是困难的。

定义2　椭圆曲线上的计算性Diffie-Hellman问题(Computational Diffie-Hellman Problem over Elliptic Curve, ECCDH)。设E是定义在有限域Z_q上的椭圆曲线，G是与E对应的有限循环群，给定$P,aP,bP\in G$，则求解$abP\in G$是困难的。

2.2　形式化分析工具

本文主要用到了BAN逻辑和Scyther软件两种形式化工具方法，下面分别简要介绍这两种工具。

(1) BAN逻辑。BAN逻辑是Burrows等人于1990年提出的[22]，BAN逻辑因其简洁直观的证明过程、方便易学的规则而引起了研究者的普遍关注。BAN逻辑的提出为解决安全协议分析问题做出了很大的贡献，它成功地对Needham-Schroeder, Kerberos等几个著名的协议进行了分析，找到了其中已知和未知的漏洞。

(2) Scyther形式化分析工具。Scyther软件[23]是由牛津和苏黎世联邦理工学院的研究学者联合研发的一个形式化分析工具，该软件首次发行于2008年左右。目前，Scyther软件已经被广泛地应用于协议分析领域，例如，该软件已经用于分析被大家所熟知的HMQV协议、KEA+协议、NAXOS协议等。

2.3　安全模型

本节介绍分析改进协议时所基于的eCK安全模型。eCK模型是LaMacchia等人[19]在2007年提出的，该模型赋予了敌手更加贴近现实环境的攻击能力。

$P=\{P_1,P_2,\cdots,P_m\}$表示eCK模型中用户的集合，其中每一个用户P_i都抽象为一个多项式时间内的图灵机。用户运行的实例$\prod_{i,j}^{\mathrm{sid}}$称为一个会话，其中$\mathrm{sid}=(P_i,P_j,X)$表示会话标识，$P_i$表示会话的发起者，$P_j$表示会话的响应者，$X$表示会话中的消息集合。敌手$\mathcal{A}$同样抽象为一个多项式时间内的图灵机，其可以对网络中的消息进行窃听、删除、修改、重放等攻击，可以完全控制网络通信。敌手$\mathcal{A}$的攻击能力可以通过如下的问询得以体现：

(1) 长期私钥暴露问询StaticKeyReveal(P_i)：通过该问询，$\mathcal{A}$可以获得用户P_i的长期密钥；

(2) 临时私钥暴露问询EphemeralKeyReveal(P_i)：通过该问询，$\mathcal{A}$可以获得用户P_i的临时密钥；

(3) 会话密钥暴露问询SessionKeyReveal(P_i)：通过该问询，$\mathcal{A}$可以获得会话sid的会话密钥；

(4) 发送消息问询Send(sid,m)：通过该问询，$\mathcal{A}$可以向会话sid发送消息m并根据协议规范获得相应的回复消息；

(5) 测试问询Test(sid)：$\mathcal{A}$选定新鲜会话sid进行该问询，模拟算法$\mathcal{S}$随机投掷硬币，根据结果$b\in\{0,1\}$来回答该问询。如果$b=1$，预言机返回该会话的正确会话密钥；如果$b=0$，则返回一个与正确密钥同分布的随机值。

在eCK模型中，模拟算法$\mathcal{S}$通过测试游戏来模拟敌手$\mathcal{A}$的攻击。在测试游戏中某一个时刻，敌手$\mathcal{A}$选定一个已经结束的会话sid作为测试会话，进行问询，具体步骤如下：

(1) $\mathcal{A}$任意进行StaticKeyReveal(P_i)问询、EphemeralKeyReveal(P_i)问询、SessionKeyReveal(P_i)问询和Send(sid,m)问询；

(2) 在某个时刻，$\mathcal{A}$选定一个标识为sid的新鲜会话进行1次Test(sid)问询；

(3) $\mathcal{A}$根据需要继续进行StaticKeyReveal(P_i)问询、EphemeralKeyReveal(P_i)问询、SessionKeyReveal(P_i)问询和Send(sid,m)问询；

(4) $\mathcal{A}$输出猜测结果。

定义3 eCK安全性 设τ为安全参数，$P[\mathcal{A}]$表示$\mathcal{A}$赢得测试会话的概率，$\mathrm{Adv}_{\mathcal{A},\prod}^{\mathrm{2P\text{-}AKA}}(\tau)=|2P[\mathcal{A}]-1|$表示$\mathcal{A}$对两方AKA协议$\prod$的优势。则称$\prod$在eCK模型下是安全的，如果该协议满足如下的条件：

(1) 匹配会话能够得到相同的会话密钥；

(2) 不存在敌手能够以不可忽略的优势赢得测试游戏。

3 两个协议的前向安全性分析

3.1 MZK20协议安全性分析

2020年，Akram等人[24]提出了一个用于多方服务器情况的AKA协议(以下简称MZK20协议)，并声称该协议具有匿名性，能够抵抗重放攻击、伪装攻击、口令猜测攻击等。本小节将指出该协议不具备弱前向安全性和匿名性。

3.1.1 MZK20协议描述

MZK20协议共由服务器注册阶段、用户注册阶段、登录和认证阶段、口令更换阶段、重新注册阶段5个部分组成，其中完成1次通信只需服务器注册、用户注册、登录和认证3个阶段，下面主要介绍完成通信的这3个阶段。

(1) 服务器注册阶段

服务器通过如下的步骤在RC处注册成为合法服务器S_j：

步骤1 服务器通过安全信道向RC发送自己的身份标识ID_j；

步骤2 在收到ID_j之后，RC计算$s=h(\mathrm{ID}_j||x)$，$\mathrm{pk}_{\mathrm{S}_j}=sP$，$\mathrm{pk}_{\mathrm{RC}}=xP$，其中$x$是RC的私钥；

步骤3 最后，RC将$s,\mathrm{pk}_{\mathrm{S}_j},\mathrm{pk}_{\mathrm{RC}}$发送给服务器，服务器$\mathrm{S}_j$完成注册。

(2) 用户注册阶段

用户通过如下的步骤在RC处注册成为网络中的合法用户U_u：

步骤1 用户选择自己的身份标识ID_u、口令PW_u和生物特征B_u，并产生一个随机数a。之后，用户计算$M=H(\mathrm{ID}_u||B_u)$，$\mathrm{TW}=h(a\oplus H(B_u||\mathrm{PW}_u))$。最后，用户将$\mathrm{ID}_u,M,\mathrm{TW}$发送给RC；

步骤2 RC在收到用户消息后，计算$X_u=h(\mathrm{ID}_u||\mathrm{pk}_{\mathrm{RC}})$，$Y_u=X_u\oplus h(M||\mathrm{TW})$，$F_u=h(h(\mathrm{ID}_u||\mathrm{TW}))$。之后，RC将$h(),Y_u,F_u$存储在智能卡$\mathrm{SC}_u$中发送给用户；

步骤3 用户在智能卡信息中增添随机数a，最后，用户U_u的智能卡信息为$\{h(),Y_u,F_u,a\}$。

(3) 登录和认证阶段

步骤1 U_u输入$\mathrm{ID}_u,\mathrm{PW}_u$和$B_u$。智能卡计算$\mathrm{TW}=h(a\oplus H(B_u||\mathrm{PW}_u))$并检验$F_u=h(h(\mathrm{ID}_u||\mathrm{TW}))$的正确性。如果正确，则智能卡计算$M=H(\mathrm{ID}_u||B_u)$，$\mathrm{U}_u$选择一个随机数$C_u$并计算$O_p=C_u\mathrm{pk}_{\mathrm{S}_j}=C_usP$，之后依次计算$\mathrm{PID}_u=C_uP\oplus\mathrm{ID}_u$，$X'_u=Y_u\oplus h(M||\mathrm{TW})$和$\mathrm{DID}_u=h(\mathrm{ID}_u||X'_u||C_uP)$。最后，$\mathrm{U}_u$发送消息$M_1=<\mathrm{PID}_u,\mathrm{DID}_u,O_p>$给$\mathrm{S}_j$；

步骤2 在收到M_1后，S_j用私钥s计算$s^{-1}O_p=C_uP$，$\mathrm{ID}_u=C_uP\oplus\mathrm{PID}_u$，$X_u=h(\mathrm{ID}_u||\mathrm{pk}_{\mathrm{RC}})$。利

用这3个结果验证等式$\mathrm{DID}_u = h(\mathrm{ID}_u||X_u||C_uP)$是否成立。如果成立，$\mathrm{S}_j$首先选择随机数$D_j$，然后依次计算$T_u = h(\mathrm{ID}_u||X_u)$, $V_j = D_j \oplus X_u$和$Q_{uj} = h(\mathrm{ID}_u||T_u||C_uP||D_j||X_u||\mathrm{ID}_j)$。最后，$\mathrm{S}_j$将$M_2 =< Q_{uj}, V_j >$发送给$\mathrm{U}_u$；

步骤3　在收到M_2后，U_u计算$D_j = V_j \oplus X_u$，并验证等式$h(\mathrm{ID}_u||h(\mathrm{ID}_u||X'_u)||C_uP||D_j||X'_u||\mathrm{ID}_j) = Q_{uj}$的正确性；

步骤4　如果等式正确则U_u进一步计算会话密钥$\mathrm{SK}_{uj} = h(\mathrm{ID}_u||C_uP||D_j||X'_u||\mathrm{ID}_j)$以及$Z_{uj} = h(\mathrm{SK}_{uj}||\mathrm{ID}_u||D_j||X'_u||\mathrm{ID}_j)$。最后，$\mathrm{U}_u$将$M_3 = Z_{uj}$发送给$\mathrm{S}_j$；

步骤5　在收到M_3后，S_j首先按照$\mathrm{SK}_{uj} = h(\mathrm{ID}_u||C_uP||D_j||X_u||\mathrm{ID}_j)$计算会话密钥，其次验证等式$h(\mathrm{SK}_{uj}||\mathrm{ID}_u||C_uP||X_u||\mathrm{ID}_j) = Z_{uj}$的正确性。

3.1.2 MZK20协议分析

(1) 启发式分析方法。当服务器的长期私钥s泄露时，指出该协议不具备弱前向安全性和匿名性。具体攻击步骤如下(假设敌手为$\mathcal{A}$)：

步骤1　敌手$\mathcal{A}$通过长期私钥泄露问询获知服务器S_j的长期私钥s；

步骤2　$\mathcal{A}$截获用户发送给服务器的消息$M_1 =< \mathrm{PID}_u, \mathrm{DID}_u, O_p >$，从而获知如下信息：

(a)根据$O_p = C_usP = sC_uP$可得C_uP；

(b)根据$\mathrm{PID}_u = C_uP \oplus \mathrm{ID}_u$可得$\mathrm{ID}_u$；

(c)根据$X_u = h(\mathrm{ID}_u||\mathrm{pk}_{\mathrm{RC}})$可得$X_u$；

步骤3　$\mathcal{A}$截获服务器发送给用户的消息$M_2 =< Q_{uj}, V_j >$，从而可以根据$V_j = D_j \oplus X_u$可得D_j；

步骤4　$\mathcal{A}$根据获知的信息C_uP, ID_u和D_j，可得会话密钥$\mathrm{SK}_{uj} = h(\mathrm{ID}_u||C_uP||D_j||X_u||\mathrm{ID}_j)$。

通过上述步骤，敌手$\mathcal{A}$在通信中只进行了窃听，通过计算就可获得用户的身份标识和计算得到最终的会话密钥。

(2) 利用BAN逻辑分析MZK20协议。下面用BAN逻辑对MZK20协议进行分析。首先给出BAN逻辑中的规定[20]，其中A,B表示用户，X,Y表示某一陈述，K表示密钥：

(a) A belives X：用户A相信陈述X；

(b) A sees X：用户A收到了陈述X；

(c) A said X：用户A曾给某一协议参与方发送了陈述X；

(d) A controls X：用户A能够管理陈述X；

(e) fresh(X)：陈述X在协议之前的消息中都未曾被使用过，保证陈述的新鲜性；

(f) $\mathrm{A} \overset{K}{\leftrightarrow} \mathrm{B}$：用户A,B之间共享密钥$K$；

(g) $\overset{K}{\rightarrow}\mathrm{A}$：密钥$K$是用户A的公钥；

(h) $\mathrm{A} \overset{\mathrm{X}}{\Leftrightarrow} \mathrm{B}$：用户A,B之间共享秘密X；

(i) $\{\mathrm{X}\}_K$：由密钥K加密的陈述X；

(j) $<\mathrm{X}>_{\mathrm{Y}}$：秘密陈述Y与陈述X进行捆绑。

由于消息M_1, M_2, M_3中，$\mathrm{DID}_u, Q_{uj}, M_3$都是用于验证双方身份的，所以将$\mathrm{S}_j$和$\mathrm{U}_u$之间的通信消息进行简化表述。最终用BAN逻辑分析MZK20协议的过程如表1所示。

由此，U_u并不能保证相信该会话密钥，即并不能满足协议目标G4，因此利用BAN逻辑分析得出该协议存在安全性质上的不足。

3.2 VSR20协议安全性分析

2020年，Sureshkumar等人[25]面向智能电网环境，提出了一个双向AKA协议(以下简称该协议为VSR20协议)，并声称该协议具有匿名性、前向安全性、不可追踪性等多种安全属性。本小节将指出VSR20协议不具备弱前向安全性，且不能够抵抗临时私钥泄露攻击。

3.2.1 VSR20协议描述

VSR20协议共由系统建立阶段、注册阶段、登录和认证阶段、密钥建立阶段4个部分组成，下面具体介绍每个阶段的步骤。

(1) 系统建立阶段。服务器(以下简称SP)通过如下的步骤生成系统参数：

步骤1　SP在域Z_q上建立一个椭圆曲线$E(a,b): y^2 = x^3 + ax + b$，其中$q$是大素数。$G$是椭圆曲线上的加法阿贝尔群，$Q$是群$G$的生成元。

步骤2　SP选择一个哈希函数$h: \{0,1\}^* \rightarrow \{0,1\}^{160}$。

(2) 注册阶。SP执行如下的步骤完成第k个用户(以下简称SM_k)的注册：

步骤1　SP在域Z_q上选择两个随机数s和x_k，用s作为自己的私钥，用x_k作为SM_k的秘密参数。并计算自己的公钥$S = sQ$。

步骤2　SP为SM_k选择一个160 bit的身份标识ID_k，并将ID_k和x_k存储在数据库中。

步骤3　SP通过安全信道将$<\mathrm{ID}_i, x_i, S, Q, h(\cdot)>$发送给$\mathrm{SM}_i, i = 1, 2, \cdots, k, \cdots, n$。

(3) 登录和认证阶段。SP通过如下的步骤发起与SM_k的通信，如图1所示。

步骤1　SP选择一个随机数$d \in Z_q$，并计算$D_1 = dQ$。之后将消息$M_1 =< D_1, \mathrm{TS}_1 >$进行广播，其中$\mathrm{TS}_1$是SP此刻的时间戳。

步骤2　在收到M_1后，SM_k选择一个随机数$r \in Z_q$，并计算$R = rQ$, $D_2 = rS = rsQ$, $D_3 = h(D_1||D_2||R||\mathrm{TS}_2)$, $D_4 = \mathrm{ID}_k \oplus D_3$和$D_5 = h(\mathrm{ID}_k||R||x_k)$。$\mathrm{SM}_k$将登录消息$M_2 =< D_2, D_4, D_5, \mathrm{TS}_2 >$发送给SP，其中$\mathrm{TS}_2$是此刻的时间戳。

表 1 BAN逻辑分析MZK20协议

MZK20协议期望达成的目标如下(参与双方用S_j和U_u表示，K_{uj}表示双方达成的会话密钥)：
G1. S_j believes K_{uj};
G2. S_j believes (U_u believes K_{uj});
G3. U_u believes K_{uj};
G4. U_u believes (S_j believes K_{uj}).

消息：
Message 1 $U_u \rightarrow S_j :< \{ID_u\}_{K_u}, \{C_u\}_{K_S} >$;
Message 2 $S_j \rightarrow U_u :< D_j >_{<ID_u>_{K_{RC}}}$;

假设：
A1.U_u believes fresh(C_u)，S_j believes fresh(D_j);
A2.U_u believes C_u，S_j believes D_j;
A3.U_u believes ($U_u \overset{K_u}{\Leftrightarrow} S_j$)，$U_u$ believes ($U_u \overset{K_u}{\Leftrightarrow} S_j$);
A4.U_u believes (S_j controls K_{uj})，S_j believes (U_u controls K_{uj});
A5.S_j believes K_{RC}，U_u believes K_{RC}.

推理过程：
F1. S_j sees $< \{ID_u\}_{K_u}, \{C_u\}_{K_S} >$;
F2. S_j sees $\{ID_u\}_{K_u}$，S_j sees $\{C_u\}_{K_s}$;
F3. S_j believes (U_u said ID_u)，S_j believes (U_u said C_u)($ID_u = C_uP \oplus PID_u$, $X_u = h(ID_u||pk_{RC})$且$PID_u = \{ID_u\}_{K_u}$);
F4. S_j believes (U_u believes C_u)，S_j believes (U_u believes X_u);
F5. S_j believes (U_u believes K_{uj})($K_{uj} = SK_{uj} = h(ID_u||C_uP||D_j||X_u||ID_j)$);
F6. S_j believes K_{uj};
F7. U_u sees $< D_j >_{<ID_u>_{K_{RC}}}$;
F8. U_u believes (S_j said D_j)($K_{uj} = SK_{uj} = h(ID_u||C_uP||D_j||X_u||ID_j)$).

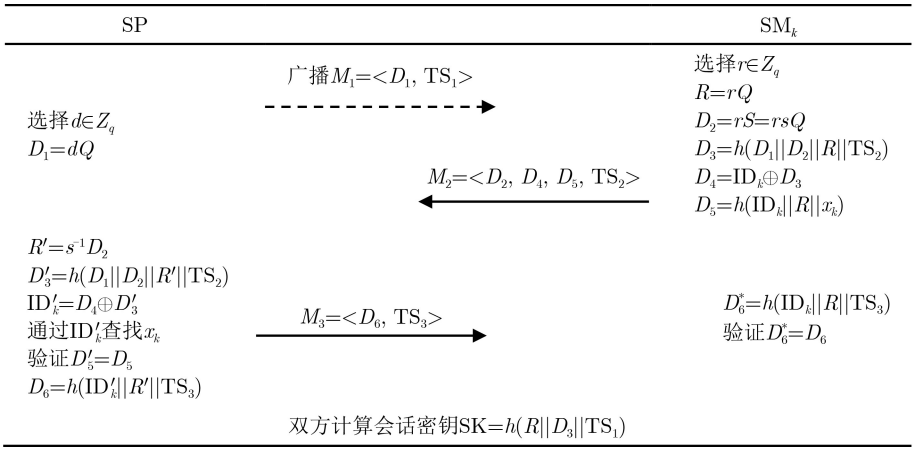


图 1 VSR20协议的登录和认证阶段

步骤3 在收到M_2后，SP验证时间戳TS_2的有效性。如果验证通过，则SP计算$R' = s^{-1}D_2$，$D'_3 = h(D_1||D_2||R'||TS_2)$，$ID'_k = D_4 \oplus D'_3$。之后，SP在数据库查找ID'$_k$，若该身份标识存在，则通过数据库获知与ID'$_k$相对应的$x_k$，并计算$D'_5 = h(ID'_{kk}||R'||x_k)$，SP验证等式$D'_5 = D_5$是否成立，如果成立，则认证完成，SP执行步骤4。

步骤4 SP计算$D_6 = h(ID'_k||R'||TS_3)$将消息$M_3 =< D_6, TS_3 >$发送给SM_k。

步骤5 在收到M_3后，SM_k验证时间戳TS_3的有效性。如果验证通过，则SM_k计算$D^*_6 = h(ID_k||R||TS_3)$，SM_k验证等式$D'_6 = D_6$是否成立，如果成立，则认证完成。

(4) 密钥建立阶段。SP与SM_k之间的相互认证完成后，双方就可以分别计算会话密钥$SK = h(R||D_3||TS_1)$。

3.2.2 VSR20协议安全分析

本小节分别通过启发式分析的方法和Scyther形式化工具方法[23]，指出了VSR20协议在安全性上的不足，具体分析如下。首先通过启发式的分析指出该协议不具备弱前向安全性，并且不能抵抗临时私钥泄露攻击。其次用Scyther软件证明了启发式分析方法的正确性。

(1) 启发式分析方法。

(a)弱前向安全性。当SP的长期私钥s泄露时，指出该协议不具备匿名性和弱前向安全性。具体攻击步骤如下(假设敌手为$\mathcal{A}$)：

步骤1 敌手$\mathcal{A}$通过长期私钥泄露问询获知服务器SP的长期私钥s；

步骤2　$\mathcal{A}$截获服务器发送给用户的消息$M_1 = < D_1, \mathrm{TS}_1 >$；

步骤3　$\mathcal{A}$截获用户发送给服务器的消息$M_2 =< D_2, D_4, D_5, \mathrm{TS}_2 >$，从而获知如下信息：

① 根据D_2可得R；

② 根据R, D_1, D_2和TS_2，可计算得$D_3 = h(D_1||D_2||R||\mathrm{TS}_2)$；

步骤4　$\mathcal{A}$根据获知的信息R, D_3, D_4和TS_1，从而获知如下信息：

① 可计算得会话密钥$\mathrm{SK} = h(R||D_3||\mathrm{TS}_1)$；

② 可计算得用户的身份标识$\mathrm{ID}_k = D_4 \oplus D_3$。

通过上述步骤，敌手$\mathcal{A}$仅通过窃听就能够同步获得用户与服务器之间的会话密钥，因此该协议不具有弱前向安全性。并且敌手$\mathcal{A}$可以恢复出用户的身份标识ID_k，因此该协议同时不能具有匿名性。

(b) 临时私钥泄露攻击。当SM_k的临时私钥泄露时，指出该协议不能够抵抗临时私钥泄露攻击。具体攻击步骤如下(假设敌手为$\mathcal{A}$)：

步骤1　$\mathcal{A}$通过临时私钥泄露问询获知用户SM_k的临时私钥r；

步骤2　$\mathcal{A}$截获服务器发送给用户的消息$M_1 =< D_1, \mathrm{TS}_1 >$；

步骤3　$\mathcal{A}$截获用户发送给服务器的消息$M_2 =< D_2, D_4, D_5, \mathrm{TS}_2 >$；

步骤4　$\mathcal{A}$根据获知的信息r、D_1、D_2、TS_1和TS_2，从而获知如下信息：

① 可计算得$D_3 = h(D_1||D_2||R||\mathrm{TS}_2) = h(D_1||D_2||rQ||\mathrm{TS}_2)$；

② 可计算得会话密钥$\mathrm{SK} = h(R||D_3||\mathrm{TS}_1) = h(rQ||D_3||\mathrm{TS}_1)$。

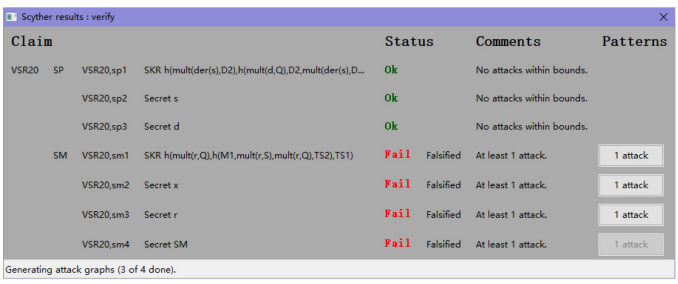
通过上述步骤，敌手$\mathcal{A}$在获知用户临时私钥r的情况下能够同步恢复出会话密钥SK，因此该协议不能够抵抗临时私钥泄露攻击。

(2) 利用Scyther软件进行分析。利用形式化分析工具Scyther分析VSR20协议，Scyther分析结果如图2所示，给出的具体攻击路径如图2(b)所示。根据图2可得，该协议不具备完全的安全性质，存在至少一种攻击方法，即如图2(b)所示，该协议不能够抵抗用户临时私钥泄露攻击。

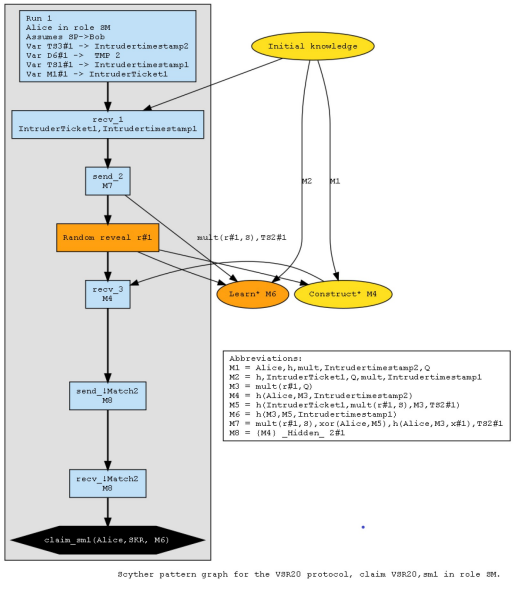
3.3　VSR20协议的改进与分析

总结并分析上述两个协议的安全性不足，在MZK20协议中，用户采用服务器的长期公钥与自己的临时密钥进行捆绑，但忽略了服务器长期私钥泄露的情况；同样地，在VSR20协议中，当敌手获取服务器的长期私钥时，敌手即可从消息中恢复用户的临时密钥。当敌手恢复出用户的临时密钥时，敌手就可以利用临时密钥对之后的消息进行解密。并且协议最后计算会话密钥时，两个协议没有将双方的临时密钥进行捆绑，只采用了一方的临时密钥，在这种情况下，当该方的临时密钥泄露时就很容易计算出最终的会话密钥。因此，在安全的AKA协议中计算会话密钥时应该既考虑长期私钥又考虑临时私钥。

(1) 改进VSR20协议描述。根据3.2.2节的分析，针对VSR20协议登录和认证阶段的不足，给出了如下的改进方案，在最后的计算会话密钥阶段将



(a) Scyther软件分析安全性质



(b) Scyther软件给出的攻击路径

图 2 Scyther软件分析VSR20协议

用户的临时密钥和服务器的临时密钥进行捆绑，用户的长期密钥和服务器的长期密钥进行捆绑(如图3所示)，提高协议的抗攻击能力。对于SP，会话密钥为$\mathrm{SK}_{\mathrm{SP}}=h(sR||dxQ||D_3||\mathrm{TS}_1)$；对于$\mathrm{SM}_k$，会话密钥为$\mathrm{SK}_k=h(rS||xD_1||D_3||\mathrm{TS}_1)$。

(2) 改进VSR20协议的安全性分析。首先证明匹配会话在协议结束后会得到相同的会话密钥。因为

$$\begin{aligned}\mathrm{SK}_{\mathrm{SP}}&=h(sR||dxQ||D_3||\mathrm{TS}_1)\\&=h(srQ||dxQ||D_3||\mathrm{TS}_1)\\&=h(rS||xD_1||D_3||\mathrm{TS}_1)\\&=\mathrm{SK}_k\end{aligned}$$

所以SP和SM_k计算的会话密钥相同，即$\mathrm{SK}_{\mathrm{SP}}=\mathrm{SK}_k$。

其次证明不存在多项式时间敌手能够以不可忽略的优势赢得测试游戏。

定理1 若h是随机预言且ECCDH假设在群G中成立，那么改进后的VSR20协议在eCK模型中是安全的。

证明 设敌手$\mathcal{A}$在系统安全参数为τ的情况下，最多能够激活n个诚实用户和s个会话。如果$\mathcal{A}$能够获得生成会话密钥的非平凡信息，则有可能以不可忽略的优势成功赢得测试游戏。由于h是随机预言，因此$\mathcal{A}$在进行完测试游戏后只能够以下列的方式区分正确的会话密钥和与正确会话密钥同分布的随机值：

事件1 猜测攻击：$\mathcal{A}$通过猜测的方式获得正确的会话密钥；

事件2 会话密钥复制攻击：$\mathcal{A}$通过某种方式建立一个与测试会话不匹配的会话sid’，但是能够与测试会话生成相同的会话密钥，此时，$\mathcal{A}$通过查询sid’就可以获得测试会话的会话密钥，赢得测试游戏；

事件3 伪造攻击：$\mathcal{A}$在某个时刻对随机预言h进行了与测试会话的会话密钥相同的查询。

对于事件1，由于h是一个随机预言，$\mathcal{A}$对会话密钥猜测正确的概率为$O(1/2^{\tau})$，这个概率是可以忽略的，因此事件1的情况可以不予考虑。

对于事件2，这种情况下相当于对h进行碰撞攻击，而h是一个随机预言，对其实施碰撞攻击成功的概率为$O(s^2/2^{\tau})$，这个概率也是可以忽略的，因此事件2的情况也可以不予考虑。

对于事件3，可以将会话分为以下两种情形：

情形1 测试会话存在匹配会话，而且匹配会话的拥有者是诚实用户；

情形2 测试会话不存在匹配会话，或者匹配会话的拥有者不是诚实用户。

下面针对这两种情形，分别进行分析。证明的思路是如果存在敌手能够以不可忽略的优势赢得测试游戏，那么可以以该敌手为子算法构造能够以不可忽略优势解决ECCDH问题的算法。

情形1 $\mathcal{A}$主要通过如下4种方式对测试会话发起攻击：

情形1.1 $\mathcal{A}$对测试会话及其匹配会话同时进行临时密钥暴露问询。给定ECCDH实例$aQ,bQ\in G$，下面构造模拟算法$\mathcal{S}$能够以不可忽略的优势解决ECCDH问题。$\mathcal{S}$可以以至少$1/n^2$概率猜测$\mathcal{A}$选择用户SP作为测试会话的拥有者，选择用户SM_k作为测试会话的匹配会话的拥有者。将aQ设为SM_k的临时公钥，bQ设为SP的长期公钥，剩余用户正常的分配公私钥对。然后，$\mathcal{S}$模拟一个协议的运行环境，保证$\mathcal{A}$不能以不可忽略的概率区分模拟环境和现实环境。当$\mathcal{A}$对除了SP,SM_k以外的用户进行问询时，$\mathcal{S}$按照协议规范如实回答$\mathcal{A}$；当$\mathcal{A}$问询的对象与SP,SM_k有关时，$\mathcal{S}$按照如下的方式回复$\mathcal{A}$的问询：

(a) StaticKeyReveal(C)问询：如果用户C是

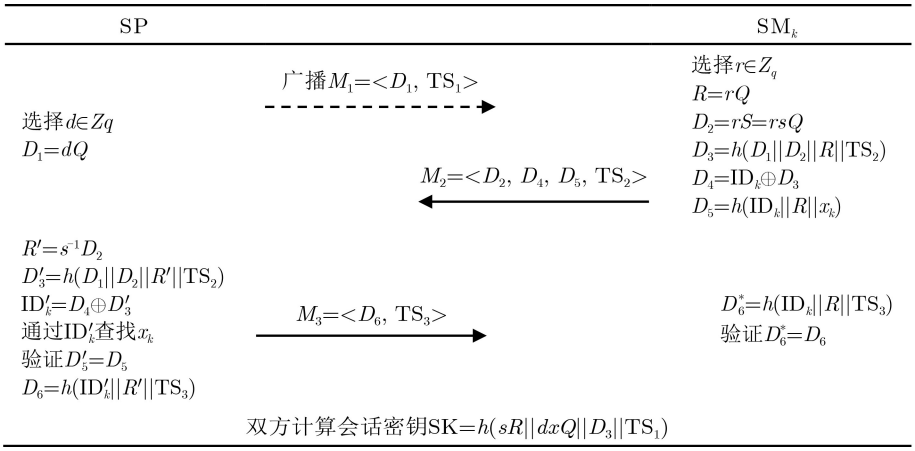


图 3 改进VSR20协议

SM_k或者SP，则$\mathcal{S}$放弃本次模拟运行；否则，$\mathcal{S}$提供用户C的长期私钥作为应答，其中长期私钥是$\mathcal{S}$在模拟初始阶段生成的；

(b) EphemeralKeyReveal(C,sid)问询：$\mathcal{S}$提供用户C在会话sid中的临时私钥作为应答；

(c) SessionKeyReveal(sid)问询：$\mathcal{S}$以如下方式提供会话密钥作为本次问询的应答：设会话标识为$\mathrm{sid}=(A,C,D_1,D_2,D_3,D_4,D_5,D_6,\mathrm{TS}_1,\mathrm{TS}_2,\mathrm{TS}_3)$，则相应的会话密钥是$\mathrm{SK}=h(\sigma)$，其中随机预言的输入为

$\sigma=$
$(\mathrm{ECCDH}(\mathrm{pk}_{\mathrm{SP}},\mathrm{epk}_k)||\mathrm{ECCDH}(xQ,\mathrm{epk}_{\mathrm{SP}})||D_3||\mathrm{TS}_1)$。

$\mathcal{S}$查询随机预言h输入是否已经被问询过，如果未被问询过，则输出一个与会话密钥同分布的随机值；如果已经被问询过，则输出正确的会话密钥。

如此，$\mathcal{S}$就模拟了$\mathcal{A}$运行协议的环境。如果$\mathcal{A}$赢得伪造攻击，则$\mathcal{A}$必须要对h查询包含ECCDH(bQ,aQ)的内容，这表示$\mathcal{S}$已经解决了ECCDH问题。除此之外，唯一需要考虑的是$\mathcal{A}$在时间t内解决ECDLP，令这个优势为$\mathrm{Adv}_G^{\mathrm{ECDLP}}(\tau,t)$。

综上可知，在情形1.1中成功解决ECCDH问题的优势为

$$\mathrm{Adv}_G^{\mathrm{ECCDH}}(\tau,t,\mathcal{S})\geq 1/n^2\cdot P_1(\tau,t)-\mathrm{Adv}_G^{\mathrm{ECDLP}}(\tau,t) \tag{1}$$

其中，$P_1(\tau,t)$表示情形1.1发生且$\mathcal{A}$成功的概率。

情形1.2　$\mathcal{A}$对测试会话及其匹配会话同时进行长期私钥暴露问询。给定ECCDH实例$aQ,bQ\in G$，下面构造模拟算法$\mathcal{S}$能够以不可忽略的优势解决ECCDH问题。$\mathcal{S}$可以以至少$1/s^2$概率猜测$\mathcal{A}$选择会话sid′作为测试会话，且测试会话的拥有者为用户SP，测试会话的匹配会话的拥有者为用户SM_k。将aQ设为SP的长期公钥，bQ设为SM_k的临时公钥，剩余用户正常的分配公私钥对。然后，$\mathcal{S}$模拟一个协议的运行环境，保证$\mathcal{A}$不能以不可忽略的概率区分模拟环境和现实环境。当$\mathcal{A}$对除了SP,SM_k以外的用户进行问询时，$\mathcal{S}$按照协议规范如实回答$\mathcal{A}$；当$\mathcal{A}$问询的对象与SP,SM_k有关时，$\mathcal{S}$按照如下的方式回复$\mathcal{A}$的问询：

(a) StaticKeyReveal(C)问询：如果用户C是SP或者SM_k，则$\mathcal{S}$放弃本次模拟运行；否则，$\mathcal{S}$提供用户C的长期私钥作为应答，其中长期私钥是$\mathcal{S}$在模拟初始阶段生成的；

(b) EphemeralKeyReveal(C,sid)问询：$\mathcal{S}$提供用户在会话sid中的临时私钥作为应答；

(c) SessionKeyReveal(sid)问询：$\mathcal{S}$以如下方式提供会话密钥作为本次问询的应答：设会话标识为$\mathrm{sid}=(A,C,D_1,D_2,D_3,D_4,D_5,D_6,\mathrm{TS}_1,\mathrm{TS}_2,\mathrm{TS}_3)$，则相应的会话密钥是$\mathrm{SK}=h(\sigma)$，其中随机预言的输入为$\sigma=(\mathrm{ECCDH}(\mathrm{pk}_{\mathrm{SP}},\mathrm{epk}_k)||\mathrm{ECCDH}(xQ,\mathrm{epk}_{\mathrm{SP}})||D_3||\mathrm{TS}_1)$。

$\mathcal{S}$查询随机预言h输入是否已经被问询过，如果未被问询过，则输出一个与会话密钥同分布的随机值；如果已经被问询过，则输出正确的会话密钥。

如此，$\mathcal{S}$就模拟了$\mathcal{A}$运行协议的环境。如果$\mathcal{A}$赢得伪造攻击，则$\mathcal{A}$必须要对h查询包含ECCDH(aQ,bQ)的内容，这表示$\mathcal{S}$已经解决了ECCDH问题。除此之外，唯一需要考虑的是$\mathcal{A}$在时间t内解决ECDLP，令这个优势为$\mathrm{Adv}_G^{\mathrm{ECDLP}}(\tau,t)$。

综上可知，在情形1.2中成功解决ECCDH问题的优势为

$$\mathrm{Adv}_G^{\mathrm{ECCDH}}(\tau,t,\mathcal{S})\geq 1/s^2\cdot P_2(\tau,t)-\mathrm{Adv}_G^{\mathrm{ECDLP}}(\tau,t) \tag{2}$$

其中，$P_2(\tau,t)$表示情形1.2发生且$\mathcal{A}$成功的概率。

情形1.3　$\mathcal{A}$对测试会话进行长期密钥暴露查询，对测试会话的匹配会话进行临时密钥暴露查询。给定ECCDH实例$aQ,bQ\in G$，下面构造模拟算法$\mathcal{S}$能够以不可忽略的优势解决ECCDH问题。$\mathcal{S}$可以以至少$1/sn$概率猜测$\mathcal{A}$选择会话sid'作为测试会话，且测试会话的拥有者为SP，测试会话的匹配会话的拥有者为用户SM_k。将SP的临时公钥设置为aQ，SM_k的长期公钥设置为bQ，剩余用户正常分配公私钥对。然后，模拟一个协议运行环境，保证不能以不可忽略概率区分这个模拟环境与现实环境。情形1.3中各种查询的模拟与情形1.1相似，则情形1.3中成功解决ECCDH问题的优势估计为

$$\mathrm{Adv}_G^{\mathrm{ECCDH}}(\tau,t,\mathcal{S})\geq 1/ns\cdot P_3(\tau,t)-\mathrm{Adv}_G^{\mathrm{ECDLP}}(\tau,t) \tag{3}$$

其中，$P_3(\tau,t)$表示情形1.3发生且$\mathcal{A}$成功的概率。

情形1.4　$\mathcal{A}$对测试会话进行临时密钥暴露查询，对测试会话的匹配会话也进行长期密钥暴露查询。这种情形与情形1.3相似，所以情形1.4中成功解决ECCDH问题的优势估计为

$$\mathrm{Adv}_G^{\mathrm{ECCDH}}(\tau,t,\mathcal{S})\geq 1/ns\cdot P_4(\tau,t)-\mathrm{Adv}_G^{\mathrm{ECDLP}}(\tau,t) \tag{4}$$

其中，$P_4(\tau,t)$表示情形1.4发生且$\mathcal{A}$成功的概率。

情形2　在这种情况下，测试会话不存在匹配会话。$\mathcal{A}$主要通过以下两种方式对测试会话进行攻击：

情形2.1　$\mathcal{A}$对测试会话进行临时密钥暴露问询，由于测试会话不存在匹配会话，因此当$\mathcal{A}$获得

测试会话拥有者的临时密钥时，$\mathcal{A}$相当于也获得了测试会话预通信方的临时密钥。这种情形下，与情形1.1类似。根据情形1.1的分析，如果$\mathcal{A}$成功赢得测试游戏，则$\mathcal{S}$能够以不可忽略的优势解决ECCDH问题。

情形2.2 $\mathcal{A}$对测试会话进行长期密钥暴露问询，由于测试会话不存在匹配会话，因此当$\mathcal{A}$获得测试会话拥有者的长期密钥时，$\mathcal{A}$相当于也获得了测试会话预通信方的临时密钥。这种情形下，与情形1.4类似。根据情形1.4的分析，如果$\mathcal{A}$成功赢得测试游戏，则$\mathcal{S}$能够以不可忽略的优势解决ECCDH问题。

综合上述分析，情形1和情形2情况下都有，如果$\mathcal{A}$能够成功赢得测试游戏，那么$\mathcal{S}$都能够以不可忽略的优势解决ECCDH问题，这与ECCDH在群G中时困难的相矛盾。 证毕

利用Scyther软件形式化分析改进后的VSR20协议，具体结果如图4所示。通过Scyther软件分析可以直观地看到改进后的VSR20协议弥补了VSR20协议的不足，抗攻击能力提高，改进后VSR20协议能够保证双方长期密钥和临时密钥的安全性，同时会话密钥的安全性也有所加强。

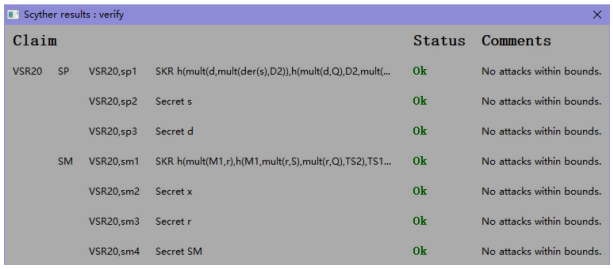


图 4 Scyther软件分析改进后VSR20协议

4 结束语

前向安全性能够为使用者提供重要的安全保障，使得协议在用户的长期私钥泄露的情况下仍然能够保证会话密钥的安全性。目前，分析AKA协议是否具有前向安全性、怎样使得AKA协议能够满足前向安全性已经成为协议研究的重要方面。本文通过给出协议的有效攻击方法，分析了MZK20和VSR20两个AKA协议。文中采用了不同的分析方法分别研究这两个协议，首先利用BAN逻辑分析了MZK20协议不具有弱前向安全性；其次利用启发式分析和Scyther工具证明了VSR20协议不具备前向安全性，并且该协议不能够抵抗临时密钥泄露攻击。文中简要分析了产生这类安全缺陷的原因，并给出了针对VSR20协议不足的改进方案，改进后的VSR20协议不但是可证明安全的，并且能够利用Scyther软件证明其安全性。

参 考 文 献

[1] GÜNTHER C G. An identity-based key-exchange protocol[C]. Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, 1989: 29–37. doi: 10.1007/3-540-46885-4_5.

[2] MATSUMOTO T, TAKASHIMA Y, and IMAI H. On seeking smart public-key-distribution systems[J]. *Transactions of the Institute of Electronics and Communication Engineers of Japan Section E*, 1986, 69(2): 99–106.

[3] JEONG I R, KATZ J, and LEE D H. One-round protocols for two-party authenticated key exchange[C]. The 2nd International Conference on Applied Cryptography and Network Security, Yellow Mountain, China, 2004: 220–232. doi: 10.1007/978-3-540-24852-1_16.

[4] KRAWCZYK H. HMQV: A high-performance secure Diffie-Hellman protocol[C]. The 25th Annual International Cryptology Conference, Santa Barbara, USA, 2005: 546–566. doi: 10.1007/11535218_33.

[5] BOYD C and NIETO J G. On forward secrecy in one-round key exchange[C]. The 13th IMA International Conference on Cryptography and Coding, Oxford, UK, 2011: 451–468. doi: 10.1007/978-3-642-25516-8_27.

[6] 曹晨磊, 刘明奇, 张茹, 等. 基于层级化身份的可证明安全的认证密钥协商协议[J]. 电子与信息学报, 2014, 36(12): 2848–2854. doi: 10.3724/SP.J.1146.2014.00684.

CAO Chenlei, LIU Mingqi, ZHANG Ru, *et al*. Provably secure authenticated key agreement protocol based on hierarchical identity[J]. *Journal of Electronics & Information Technology*, 2014, 36(12): 2848–2854. doi: 10.3724/SP.J.1146.2014.00684.

[7] 杨孝鹏, 马文平, 张成丽. 一种新型基于环上带误差学习问题的认证密钥交换方案[J]. 电子与信息学报, 2015, 37(8): 1984–1988. doi: 10.11999/JEIT141506.

YANG Xiaopeng, MA Wenping, and ZHANG Chengli. New authenticated key exchange scheme based on ring learning with errors problem[J]. *Journal of Electronics & Information Technology*, 2015, 37(8): 1984–1988. doi: 10.11999/JEIT141506.

[8] 熊婧, 王建明. 基于HASH函数的RFID安全双向认证协议研究[J]. 中国测试, 2017, 43(3): 87–90,96. doi: 10.11857/j.issn.1674-5124.2017.03.018.

XIONG Jing and WANG Jianming. Based on HASH function of RFID security authentication protocol and analysis[J]. *China Measurement & Test*, 2017, 43(3): 87–90,96. doi: 10.11857/j.issn.1674-5124.2017.03.018.

[9] LI Xiong, PENG Jieyao, OBAIDAT M S, *et al*. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems[J]. *IEEE Systems Journal*, 2021, 14(1): 39–50. doi: 10.1109/JSYST.2019.2899580.

[10] SALEEM M A, SHAMSHAD S, AHMED S, *et al*. Security analysis on “A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems” [J]. *IEEE Systems Journal*, 2021, 15(4): 5557–5559. doi: 10.1109/JSYST.2021.3073537.

[11] YANG Zheng, HE Jun, TIAN Yangguang, *et al*. Faster authenticated key agreement with perfect forward secrecy for industrial internet-of-things[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(10): 6584–6596. doi: 10.1109/TII.2019.2963328.

[12] CHANG C C and LE H D. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(1): 357–366. doi: 10.1109/TWC.2015.2473165.

[13] GOPE P and HWANG T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks[J]. *IEEE Transactions on Industrial Electronics*, 2016, 63(11): 7124–7132. doi: 10.1109/TIE.2016.2585081.

[14] 王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议[J]. 计算机学报, 2020, 43(4): 683–700. doi: 10.11897/SP.J.1016.2020.00683.

WANG Chenyu, WANG Ding, WANG Feifei, *et al*. Multi-factor user authentication scheme for multi-gateway wireless sensor networks[J]. *Chinese Journal of Computers*, 2020, 43(4): 683–700. doi: 10.11897/SP.J.1016.2020.00683.

[15] QIU Shuming, WANG Ding, XU Guoai, *et al*. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(2): 1338–1351. doi: 10.1109/TDSC.2020.3022797.

[16] SHAMSHAD S, SALEEM M A, OBAIDAT M S, *et al*. On the security of a lightweight privacy-preserving authentication protocol for VANETs[C]. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021: 1766–1770. doi: 10.1109/ICAIS50930.2021.9395888.

[17] RESCORLA E.Internet Engineering Task Force. RFC 8446-The Transport Layer Security (TLS) protocol version 1.3[S]. 2018.

[18] BOYD C and GELLERT K. A modern view on forward security[J]. *The Computer Journal*, 2021, 64(4): 639–652. doi: 10.1093/comjnl/bxaa104.

[19] LAMACCHIA B, LAUTER K, and MITYAGIN A. Stronger security of authenticated key exchange[C]. The 1st International Conference on Provable Security, Wollongong, Australia, 2007: 1–16. doi: 10.1007/978-3-540-75670-5_1.

[20] CANETTI R and KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Innsbruck, Austria, 2001: 453–474. doi: 10.1007/3-540-44987-6_28.

[21] MOHAMED M I, WANG Xiaofen, and ZHANG Xiaosong. Adaptively-secure authenticated key exchange protocol in standard model[J]. *International Journal of Network Security*, 2018, 20(2): 345–358. doi: 10.6633/IJNS.201803.20(2).16.

[22] BURROWS M, ABADI M, and NEEDHAM R M. A logic of authentication[J]. *Proceedings of the Royal Society A:Mathematical, Physical and Engineering Sciences*, 1989, 426(1871): 233–271. doi: 10.1098/rspa.1989.0125.

[23] CREMERS C J F. The scyther tool: Verification, falsification, and analysis of security protocols[C]. International Conference on Computer Aided Verification, Princeton, USA, 2008: 414–418. doi: 10.1007/978-3-540-70545-1_38.

[24] AKRAM M A, GHAFFAR Z, MAHMOOD K, *et al*. An anonymous authenticated key-agreement scheme for multi-server infrastructure[J]. *Human-centric Computing and Information Sciences*, 2020, 10(1): 22. doi: 10.1186/s13673-020-00227-9.

[25] SURESHKUMAR V, ANANDHI S, AMIN R, *et al*. Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication[J]. *IEEE Systems Journal*, 2021, 15(3): 3565–3572. doi: 10.1109/JSYST.2020.3039402.

程庆丰：男，博士，教授，研究方向为公钥密码和密码协议.
马玉千：女，硕士生，研究方向为密码协议.

责任编辑：马秀强