无线网络中高效的匿名漫游安全协议

金海旻[①②]　许胤龙[①]　王　石[②]
[①](中国科学技术大学计算机科学与技术学院安徽省高性能计算重点实验室　合肥　230026)
[②](香港城市大学计算机科学系　香港)

摘　要：无线漫游安全(Secure Wireless Roaming，SWR)协议允许隶属于本地服务器的用户漫游到外地时，可以与外地服务器互相验证身份并建立安全的会话密钥。在此基础上，匿名 SWR 协议能保证即使所有外地服务器串通情况下漫游用户的匿名性和不可追踪性。该文提出了一个匿名的无线漫游安全协议 SYM-SWR (SYMmetric key based SWR)。而且就目前所知，该协议是第 1 个完全基于对称密钥的匿名 SWR。同其他已知协议相比，SYM-SW 的通信复杂度和计算复杂度均最低。因为 SYM-SWR 只需要 4 次消息传送，且不需要 PKI (Public Key Infrastructure)而采用消息验证码(Message Authentication Code，MAC)和对称密钥加密这两种高效的运算。

关键词：无线漫游安全；可认证密钥交换；匿名性；不可追踪性；可证明安全性
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2010)08-1961-07
DOI: 10.3724/SP.J.1146.2009.01038

Highly Efficient Anonymous Roaming For Wireless Network

Jin Hai-min[①②]　Xu Yin-long[①]　Wong S. Duncan[②]
[①](*School of Computer Science and Technology, University of Science and Technology of China, Key Laboratory on High Performance Computing, Anhui Province, Hefei* 230026, *China*)
[②](*Department of Computer Science, City University of Hong Kong, Hong Kong, China*)

Abstract: Secure Wireless Roaming (SWR) allows a roaming user under the subscription of its home server to establish a secure session key with a foreign server in an authenticated way such that both the foreign server and the roaming user can mutually authenticate each other. Anonymous SWR provides an additional service to the roaming user so that the roaming user can keep anonymous and untraceable even if all the visited foreign servers are colluding with each other. In this paper, an anonymous SWR called SYM-SWR (SYMmetric key based SWR) is proposed. To best of our knowledge, it seems to be the first pure symmetric key based anonymous SWR. Compared with other existing SWR protocols both of the computation complexity and communication complexity of SYM-SWR are lowest, since it involves only 4 message flows and no PKI (Public Key Infrastructure) but only highly efficient cryptographic operations are needed which include Message Authentication Code (MAC) and symmetric key encryption.

Key words: Secure Wireless Roaming (SWR); Authenticated key exchange; Anonymity; Untraceability; Provable security

1　引言

无线漫游服务允许人们不受地理位置的限制通过移动设备穿梭于不同的无线网络，享受不同服务商提供的服务。这项服务被广泛地应用于诸如全球移动网络 GSM[1]，3GPP[2]等系统中。支持无线漫游的网络通常由漫游用户 U，U 所访问的外地服务器 V 及用户的隶属服务器 H 组成。其中 U 和 V 之间，V 和 H 之间可直接通信，而 U 和 H 之间则不能。所有已知的漫游协议如文献[3–9]等均基于此结构。

本文提出了一种高效的匿名无线漫游安全协议 SYM-SWR (SYMmetric key based Secure Wireless Roaming)，该协议满足以下所有匿名 SWR 的安全性需求：

(1)服务器身份可认证：漫游用户可以验证所访问的外地服务器的身份。

(2)用户身份可认证：外地服务器可以确认漫游用户的合法性及其隶属服务器的身份。

(3)建立安全的会话密钥：用户和外地服务器之

2009-07-24 收到，2010-03-11改回
国家自然科学基金(60773036)资助课题
通信作者：金海旻　jhm1213@gmail.com

间可随机生成一个只有彼此知道的会话密钥。

(4)向前保密性：攻击者即使获得用户的长期密钥，也无法获得在此密钥泄露之前用户与外地服务器成功建立的会话密钥。

(5)强用户匿名性及不可追踪性：除了用户本身及其隶属服务器，包括外地服务器在内的所有攻击者均不能确认用户的身份，也不能获得用户的行踪即确认某两次协议运行(会话)是同一用户所为。特别地，当一个用户同时进行多个会话时，仍保持该用户的匿名性和不可追踪性。

SYM-SWR 协议还具有以下优点：(1)只需要 4 次消息传送，是目前已知此类协议中最少的；(2)完全基于对称密钥，采用高效的对称密钥加密和消息验证码(Message Authentication Code，MAC)；(3)同最近分别在文献[6–8]中提出的 3 个协议相比，通信复杂度不增加而计算复杂度降低了 50%以上，同时解决了文献[8]遇到的同步失败的问题(详见 3.1.2 节)；(4)在 CK 模型下是可证明安全的。

人们提出了多种无线漫游安全协议(Secure Wireless Roaming, SWR)[3−10]。然而文献[3,4]中的协议不支持用户匿名性和不可追踪性。文献[11]指出文献[5]中第 1 个协议(本文称其为 JLSS-I)不具备向前保密性，只满足部分(Partial)用户匿名性及不可追踪性，即虽然任何攻击者都不能获得用户的身份，但任何网络偷听者都可以追踪该用户。文献[5]中第 2 个协议(本文称其为 JLSS-II)会暴露用户的身份。文献[12]指出文献[9,10]提出的协议中任何用户只需要通过偷听就可以获知其他用户的身份和行踪。正如文献[11]所回顾的那样，大多数已知 SWR 协议其用户不可追踪性仅仅是针对网络偷听者而言，即弱不可追踪性。最近文献[6–8]中提出的协议是已知的少数几个满足强用户匿名性及不可追踪性的匿名 SWR 协议，然而与本文的 SYM-SWR 相比这 3 个协议的性能都比较低。而且文献[7]对漫游用户的访问次数有限制，每当次数快达到限制时用户必须回到本地网络与隶属服务器重新更新一组别名，因此不适用于长期漫游的用户。另外，事实上已广泛采用的标准 GSM[1]，3GPP[2]只满足弱用户匿名性和不可追踪性。

还有一类本地化漫游协议(localized roaming)[13−15]，即用户漫游时只需要与当地服务器交换认证信息而无需其隶属服务器的参与，从而降低通信复杂度。然而正如文献[15]所述，这类协议在实际应用中面临的最大问题是用户撤回(user revocation)机制(比如由于欠费、安全等原因，隶属服务器要求注销某一用户)都比较复杂。文献[15]同时指出文献[13]中的协议可扩展性不好且不支持用户匿名性。文献[14]中提出的协议没有考虑用户撤回的问题。文献[15]基于动态群签名机制[16]提出了一种新的可证明安全的本地化匿名 SWR，然而动态群签名机制本身及相应的用户撤回机制的复杂性影响了该协议的实际应用。

本文提示的SYM-SWR协议不但可以被证明满足匿名 SWR 的最安全性要求，而且完全基于对称密钥加密和 MAC，所以更加高效，适合实际应用。

2 SYM-SWR 协议

SYM-SWR 协议由用户注册和匿名的可认证密钥交换两个阶段组成。为了获得更高的效率，本协议采用椭圆曲线密码机制(Elliptic Curve Cryptography，ECC)。设 E 是在有限域 $\mathrm{GF}(n)$ 中的安全椭圆曲线群，其中 $n=2^k$，素数 k 是安全参数，通常设为 163 或者 211。表 1 中列举了 SYM-SWR 协议中的相关符号。

表 1 SYM-SWR 协议有关的符号定义

$E(\mathrm{GF}(n))$	有限域 $\mathrm{GF}(n)$ 中的椭圆曲线群
P	$P\in E(\mathrm{GF}(n))$，设生成元 P 的秩(order)为素数 q
H	移动用户的隶属服务器
U	漫游用户
V	外地服务器
alias_U	从 $\{0,1\}^k$ 中随机挑选具有固定长度 k 的二进制串充当 U 的别名
K_{HU1}， K_{HU2}	M 和 H 之间两个独立的长期对称密钥
K_{HV}	H 和 V 之间的长期对称密钥
$\mathrm{MAC}_K(\cdot)$	密钥为 K 的消息验证码函数，定义域为 $\{0,1\}^*$，值域为 $\{0,1\}^k$
COUNT_A	计数器 A 的值
$\mathcal{H}(\cdot)$	抗碰撞 hash 函数 $\mathcal{H}(\cdot):\{0,1\}^*\to\{0,1\}^k$
$\varepsilon_K(\cdot)$	密钥为 K 的对称密钥加密，明文空间 $\{0,1\}^{\lvert\mathrm{COUNT}\rvert+k}$,密文空间 $\{0,1\}^l$。其中计数器值的长度为$\lvert\mathrm{COUNT}\rvert$，$l$ 为安全参数。

用户注册阶段：目的是在 U 和 H 之间分配必要的秘密参数。当 U 向 H 注册时，H 随机挑选两个相互独立的对称密钥 K_{HU1} 和 K_{HU2} 与 U 共享。H 为 U 随机生成具有固定长度 k 的别名 alias_U，并在其数据库中记录匹配关系 $\mathrm{alias}_U\leftrightarrow\mathrm{ID}_U$。初始化 U 的计数器 COUNT_U 为 0。H 将 K_{HU1}，K_{HU2} 和 alias_U 注入 U 的 SIM 卡中。

匿名的可认证密钥交换阶段：目的是让 U 和 V 在 H 的协助下互相确认身份的合法性后以匿名的方式建立安全的会话密钥。协议如图 1 所示，具体描述如下：

(1)当 U 漫游至由 V 控制的网络时，U 向 V 发送 H 的身份标识、用自己的密钥加密过的用于身份认证的有关信息以及用于生成会话密钥的有关信息

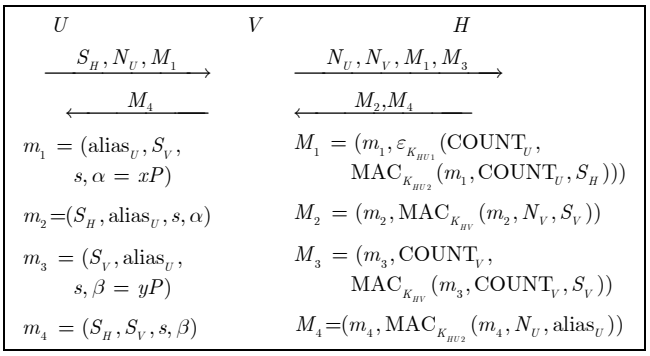

图 1 SYM-SWR 协议

等消息。具体过程如下：U 从 SIM 卡中读取别名 $\text{alias}_U \in \{0,1\}^k$，随机挑选 $N_U \in \{0,1\}^k$ 和 $x \in Z_q^*$ 并计算 $\alpha = xP$。然后构造消息 $m_1 = (\text{alias}_U, S_V, s, \alpha = xP)$，其中 S_V 是 V 的身份标识，s 是随机挑选的会话序号。U 读取当前计数器值 COUNT_U，并构造消息 $M_1 = (m_1, \varepsilon_{K_{HU1}}(\text{COUNT}_U, \text{MAC}_{K_{HU2}}(m_1, \text{COUNT}_U, S_H)))$，其中 S_H 是 H 的身份标识。U 将 S_H, M_1 和 N_U 发送给 V 后，如下更新别名：$\text{alias}_U = \mathcal{H}(\text{COUNT}_U + 1, K_{HU1})$。关于 alias_U 的同步更新细节请见 3.2 节。

(2)当 V 收到来自 U 的消息 (S_H, N_U, M_1) 时，V 向 H 发送用于 U 和 V 身份认证及用于生成会话密钥的有关信息，目的是请求 H 在验证 U 和 V 的身份之后，帮助他们建立会话密钥。具体过程如下：V 随机挑选 $y \in Z_q^*$，计算 $\beta = yP$ 并构造消息 $m_3 = (S_V, \text{alias}_U, s, \beta)$。然后读取当前计数器值 COUNT_V，形成消息 $M_3 = (m_3, \text{COUNT}_V, \text{MAC}_{K_{HV}}(m_3, \text{COUNT}_V, S_V))$。最后，$V$ 随机挑选 $N_V \in \{0,1\}^k$ 并将 (N_V, N_U, M_1, M_3) 发送给 H。

(3)当 H 收到来自 V 的消息 (N_V, N_U, M_1, M_3) 时，H 利用 alias_U 在数据库中查找匹配关系 $(\text{ID}_U \rightarrow \text{alias}_U)$ 得到 ID_U。然后用相应的 K_{HU1} 解密 M_1 中 $\varepsilon_{K_{HU1}}(\text{COUNT}_U, \text{MAC}_{K_{HU2}}(m_1, \text{COUNT}_U, S_H))$，再用 K_{HU2} 验证所得 MAC 的有效性。关于验证的细节请见 3.1.2 节。若验证失败，立即终止会话。否则，H 继续验证 M_3 中 $\text{MAC}_{K_{HV}}(m_2, N_V, S_V)$ 的有效性。若验证失败，立即终止会话。否则构造消息 $M_2 = (m_2, \text{MAC}_{K_{HV}}(m_2, N_V, S_V))$，$M_4 = (m_4, \text{MAC}_{K_{HU2}}(m_4, N_U, \text{alias}_U))$，其中 $m_2 = (S_H, \text{alias}_U, s, \alpha)$，$m_4 = (S_H, S_V, s, \beta)$。之后更新 U 的别名 $\text{alias}_U = \mathcal{H}(\text{COUNT}_U + 1, K_{HU1})$，并将 M_2, M_4 发送给 V。

(4)当收到来自 H 的消息 M_2, M_4 时，V 用 K_{HV} 验证消息 M_2 中的 MAC。若无效，立即终止会话。否则，V 相信 U 是隶属于 H 的合法用户并生成最终的会话密钥 $SK_V = y\alpha = yxP$。然后将 M_4 发送给 U。

(5)当收到来自 V 的消息 M_4 时，U 验证其中 MAC 的有效性。若无效，立即终止会话。否则，U 相信 V 是被隶属服务器 H 所确认的合法外地服务器并计算最终的会话密钥 $SK_U = x\beta = xyP$。

3 SYM-SWR 的安全性分析

3.1 用户身份可认证、服务器身份可认证和建立安全的会话密钥

2001 年，Canetti 和 Krawczyk 在文献[17]中创造性地提出了一种可认证密钥交换的新模型(CK model)和此模型下的一种模块化密钥交换协议构造法。该构造法设计的密钥交换协议具有可证明安全的用户身份可认证、服务器身份可认证、建立安全的会话密钥这 3 条安全性。下面简要介绍一下 CK model 以及该构造法。

CK model 定义了两类攻击模型：(1)无认证链接攻击模型(Unauthenticated-links adversarial Model，UM)，根据 UM 的定义，一个 UM 下安全的密钥交换协议在现实世界中也是安全的。(2)已认证连接攻击模型(Authenticated-linked adversarial Model，AM)。有关细节请参阅文献[17]。

构造法：如文献[17]定理 6 所述，当 π 是一个在 AM 下具备建立安全的会话密钥的密钥交换协议且 λ 是一个消息传输认证者(MT-authenticator)时，将 λ 运用于协议 π 每条消息的发送，所构造出来的协议 π_λ 就是一个 UM 下满足用户身份可认证、服务器身份可认证和建立安全的会话密钥的密钥交换协议。有关 MT-authenticator 的细节请见文献[17,18]。

设计思路：按如下步骤设计协议 SYM-SWR：

(1)设计一个 AM 下的 SWR 协议满足建立安全的会话密钥。

(2)设计高效的 MT-authenticator。

(3)利用步骤(2)设计的 MT-authenticator 构造 UM 下的 SWR 协议。

3.1.1 AM 下的 SWR 协议　构造 AM 下的 SWR 协议 (SWR_{AM})如图 2 所示，其中有关符号定义见表 1。这里 x，$y \in Z_q^*$ 由 U 和 V 随机挑选。

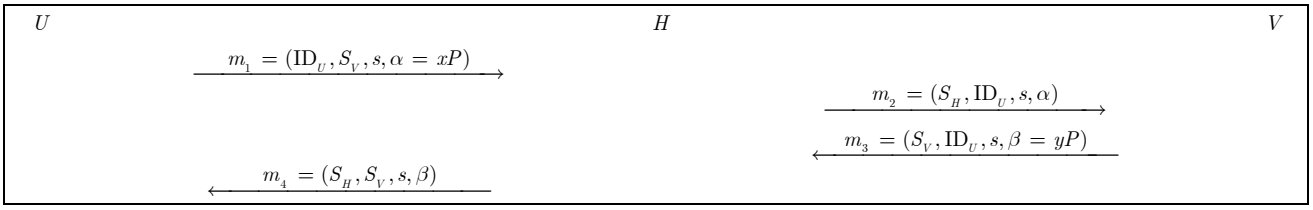

图 2 AM 下的 SWR 协议

推 论 1 在 Elliptic Curve Decision Diffie-Hellman(ECDDH) 困难性假设下，协议 $\mathrm{SWR}_{\mathrm{AM}}$ 在 AM 下可以建立安全的会话密钥。

证明 已知 $\mathrm{SWR}_{\mathrm{AM}}$ 是 AM 下对 Diffie-Hellman 协议的简单扩展。由于 AM 下的攻击者只具备偷听的能力，即使获得 $\alpha = xP$ 和 $\beta = yP$，在 ECDDH 困难性假设下也不能得到会话密钥(xyP)。所以该协议在 AM 下可以建立安全的会话密钥。 证毕

3.1.2 MT-authenticator SYM-SWR 使用了 3 种不同的 MT-authenticator 以兼顾安全和效率，其中两种基于计数器的一次性 MT-authenticator 是本文新提出的。

基于对称密钥的 MT-authenticator 详情请见文献[18]。

基于计数器的一次性 MT-authenticator (One-pass Counter Based MT-authenticator)：一次性 MT-authenticator 由于简化了消息认证过程而具有更高的工作效率。文献[8]，文献[18]提出了基于计数器的一次性 MT-authenticator。然而文献[17]指出文献[18]提出的 MT-authenticator 的安全性证明并不正确。本文指出文献[8]提出的 MT-authenticator 会出现同步失败问题，即当多个会话同时进行时，一些合法的消息很有可能会被拒绝接受。举例来说，当 P_i 依次发起 A 和 B 两个消息传送会话，此时 $\mathrm{COUNT}_{P_i}^{A} < \mathrm{COUNT}_{P_i}^{B}$。由于传输延迟等原因，包含 $\mathrm{COUNT}_{P_i}^{A}$ 的消息比包含 $\mathrm{COUNT}_{P_i}^{B}$ 的消息晚到达 P_j。根据文献[17]的 MT-authenticator，包含 $\mathrm{COUNT}_{P_i}^{A}$ 的消息到达时会被当作旧消息而丢弃。为了解决这个问题，本文利用类似“滑动窗口”的机制改进了这个 MT-authenticator。设 P_i 和 P_j 预先共享密钥 K_{ij}，改进的基于计数器一次性 MT-authenticator 为

$$P_i \to P_j : m, \mathrm{COUNT}_{P_i}, \mathrm{MAC}_{K_{ij}}(m, \mathrm{COUNT}_{P_i}, P_j)$$

同时，利用对称加密 $\varepsilon_K(\cdot)$ 和消息认证码 MAC 构造的全新的基于计数器一次性 MT-authenticator 为

$$P_i \to P_j : m, \mathcal{E}_{K_1}(\mathrm{COUNT}_{P_i}, \mathrm{MAC}_{K_2}(m, \mathrm{COUNT}_{P_i}, P_j))$$

其中 P_i 和 P_j 预先共享密钥 K_1 和 K_2。全新的基于计数器的一次性 MT-authenticator 运作过程如下 (改进的 MT-authenticator 运作过程与之类似):

初始化阶段：发送者 P_i 和接受者 P_j 的计数器 COUNT_{P_i} 和 COUNT_{P_j} 初始化为 0，这里要求每对接受者和发送者都有一对独立的计数器。接受者 P_j 初始化一个大小为 n 的数组 C_j，并将所有元素设置为 0 (即 $C_j[k]=0,\ k \in \{1,\cdots,n\}$)。这里假设在短时间内双方最多允许同时进行 n 个消息传送会话。

发送阶段：每当 P_i 准备发送消息 m 给 P_j 时，P_i 将计数器值 COUNT_{P_i} 加 1，然后发送 ($m, \varepsilon_{K_1}(\mathrm{COUNT}_{P_i}, \mathrm{MAC}_{K_2}(m, \mathrm{COUNT}_{P_i}, P_j))$) 给 P_j 并在本地输出中记录“P_i 发送消息 m 至 P_j”。

验证阶段：当收到消息 ($m, \varepsilon_{K_1}(\mathrm{COUNT}_{P_i}, \mathrm{MAC}_{K_2}(m, \mathrm{COUNT}_{P_i}, P_j))$ 时，P_j 用 K_1 解密密文后，用 K_2 验证 MAC。若无效则输出“拒绝接受该消息”；否则检查是否 $\mathrm{COUNT}_{P_i} > \mathrm{COUNT}_{P_j}$：

(1) 若 $\mathrm{COUNT}_{P_i} > \mathrm{COUNT}_{P_j}$，设 $\mathrm{COUNT}_{P_j} = \mathrm{COUNT}_{P_i}$。

(2) 否则，若 $\mathrm{COUNT}_{P_i} > \mathrm{COUNT}_{P_j} - n$ 且 $\mathrm{COUNT}_{P_i} \neq C_j[k]\ (k = 1,\cdots,n)$，则将 C_j 中最小的元素设置为 COUNT_{P_i}。否则输出“拒绝接受该消息”。

当没有输出“拒绝接受该消息”时，P_j 在本地输出中记录“P_j 从 P_i 接受了消息 m”。

分析：在接收端 P_j 引入了数组 C_j，它收集最近接受到的 n 个消息中的计数器值 COUNT_{P_i}。设想当新到达消息的计数器值 COUNT_{P_i} 小于 COUNT_{P_j} 时(注意，COUNT_{P_j} 的值记录了当前收到的所有消息中包含的最大的 COUNT_{P_i})，只要 $\mathrm{COUNT}_{P_i} > \mathrm{COUNT}_{P_j} - n$ 且不同于 C_j 中的其他任何元素，那么该消息仍被认为有效。这样做是合理的，因为一方面 $\mathrm{COUNT}_{P_i} > \mathrm{COUNT}_{P_j} - n$ 保证了这个消息是 P_i 最近发送的 n 个消息之一；另一方面 COUNT_{P_i} 不同于 C_j 中的其他任何元素保证了该消息不是最近接收到的 n 个消息的重放攻击。所以，当发收双方被限定为至多同时进行 n 个消息传输时，改进的基于计数器的一次性 MT-authenticator 和全新的基于计数器的一次性 MT-authenticator 不但能抵抗重放消息攻击同时也能解决多个会话时的同步失败问题。这两个 MT-authenticator 的安全性是可以被证明的，过程类似文献[8]中对 MT-authenticator 的证明，由于篇幅的限制，这里不再描述。

3.1.3 UM 下的 SWR 协议 本文将 3 种不同的 MT-authenticator 应用到 $\mathrm{SWR}_{\mathrm{AM}}$ 来构造 UM 下的 SWR 协议，如图 3 所示。

由于攻击者可以通过监听 COUNT_U 来追踪用户 U，对 m_1 采用全新的基于计数器的一次性 MT-authenticator。由于对 COUNT_V 的监听无助于追踪用户，对 m_3 采用效率更高的改进的基于计数器的一次性 MT-authenticator。对于 m_2 和 m_4 采用效率更高的基于对称密钥的 MT-authenticator。

至此，UM 下的 SWR 协议(图 3)已满足服务器身份认证、用户身份认证、建立安全的会话密钥这 3 条安全性。采用文献[19]提出的方法对该协议进行消息传送优化(该优化方法不会改变协议的安全

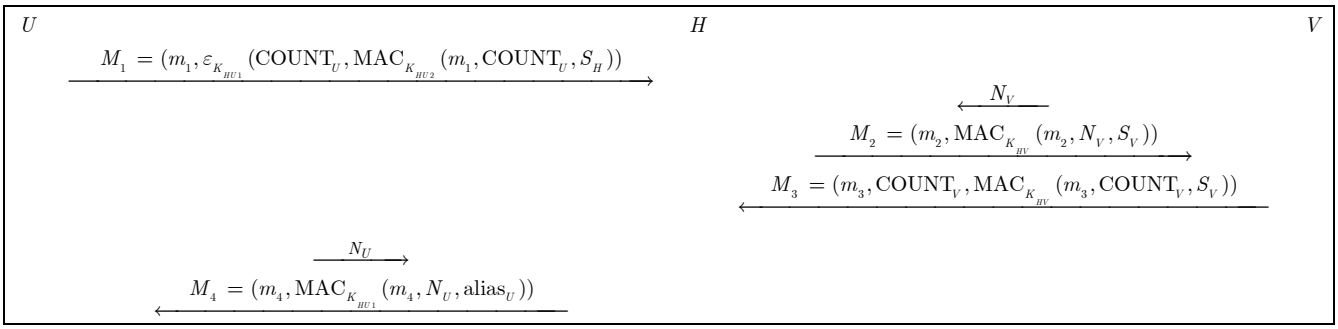

图 3 UM 下的 SWR 协议

性)，同时下一节将看到为了达到用户匿名性和不可追踪性，本文改进了优化后的 SWR 协议最终得到了第 2 节中介绍的 SYM-SWR 协议(图 1)。

3.2 向前保密性、用户匿名性和不可追踪性

向前保密性：根据图 3 所示协议，可知会话密钥为 xyP 且与之相关的消息仅是 $\alpha = xP$ 和 $\beta = yP$。对于一个获得 U 长期密钥的攻击者来说，也不比其他攻击者知道更多，因为 α 和 β 总是分别在 M_1, M_2 和 M_3, M_4 中明文传送的。而在 ECDDH 假设下，即使获得 α 和 β 也无法得到 xyP。

用户匿名性：为了隐藏 U 的身份 ID_U，H 为 U 分配一个长度为 k 的二进制串 alias_U 作为 U 的别名。然后 H 记录下匹配关系($\mathrm{ID}_U \leftrightarrow \mathrm{alias}_U$)。将图 3 中 m_1, m_2, m_3, m_4 包含的所有 ID_U 替换成 alias_U。

用户不可追踪性：为了防止攻击者通过 alias_U 追踪用户 U，U 和 H 需要每次会话后将如下更新 U 的别名 $\mathrm{alias}_U = H(\mathrm{COUNT}_U + 1, K_{HU1})$。假设遇到最坏情况即追踪者是外地服务器 V。根据不可追踪性的定义，如果 V 找出任何两个会话同属于某个用户 U，就认为 V 成功了。根据协议，U 的会话消息中与 U 有关的消息包括：($\alpha, N_U, \mathrm{alias}_U$，$\mathrm{MAC}_{K_{HU2}}(m_4, N_U, \mathrm{alias}_U)$, $\varepsilon_{K_{HU1}}(\mathrm{COUNT}_U, \mathrm{MAC}_{K_{HU2}}(m_1, \mathrm{COUNT}_U, S_H))$)。而其他消息均由 H 和 V 随机挑选或者根据以上消息生成。然而 α，N_U 均为 U 随机生成，与 U 身份无关；V 在不知道 U 密钥的情况下也无法利用 $\mathrm{MAC}_{K_{HU2}}(m_4, N_U, \mathrm{alias}_U)$ 和 $\varepsilon_{K_{HU1}}(\mathrm{COUNT}_U, \mathrm{MAC}_{K_{HU2}}(m_1, \mathrm{COUNT}_U, S_H))$。而 alias_U 每次会话后都如下更新 $\mathrm{alias}_U = H(\mathrm{COUNT}_U + 1, K_{HU1})$，由于 V 不知道 K_{HU1} 和 COUNT_U，alias_U 在 V 看来是无法预测和分辨的。综上所述，即使 V 也无法追踪用户 U。

更新同步问题：U 和 H 需要每次会话后都更新 U 的别名 alias_U。然而由于通信链路的安全无法保障比如攻击者恶意截获消息或者插入消息等，很难保证 U 和 H 之间 alias_U 的更新同步。同步失败时会出现以下情况：U 更新了 alias_U 而 H 则没有。本文采用类似于基于计数器的 MT-authenticator 的“滑动窗口”的办法。同样，这里假设允许 U 最多同时发起 n 个会话。

(1)H 将已接收的来自 U 的消息中最大的计数器值 $\mathrm{COUNT}_U^{\max}$ 设为参考点，并用名单 L_U 记录 U 的 $2n$ 个可能的别名，包括参考点之前 n–1 个可能的别名和参考点之后 n 个可能的别名。L_U 中第 i_{th} 个元素 $L_U[i]$ 如下计算：若 $i \in \{1, n\}$，则 $L_U[i] = H(\mathrm{COUNT}_U^{\max} - (n - i), K_{HU})$；若 $i \in \{n+1, 2n\}$，则 $L_U[i] = H(\mathrm{COUNT}_U^{\max} + i, K_{HU})$。

(2)每当 H 从 V 收到消息后，根据其中的 alias_U 在别名名单搜索直到找到用户的真实身份。由于 U 至多同时发起 n 个会话，当接收到最新消息时，该协议既考虑到有可能之前的 n–1 个消息都还没有到达，也考虑了有可能之后的 n–1 个消息已经到达了这两种极端情况。因此上述同步更新失败的问题不会再发生了。

4　性能及安全性比较分析

本节对 SYM-SWR 和一些已知的漫游协议进行了性能及安全性的分析和比较(请见表 2)。

通信复杂度分析：由表 2 可知，SYM-SWR 只需要 4 次消息传送，是这些协议中最少的。

计算复杂度分析：以上这些协议使用了有多种不同的密码学工具基本构造模块，包括 STR, MAC, SYM, PKE, EXP, ECSM 和 ECBP。而协议的性能正是取决于这些工具的计算代价，因此可以用协议中不同密码学工具的执行次数来衡量该协议计算复杂度，统计结果如表 2 所示。

(1)对于基于 STR，MAC 或 SYM 协议的分析：一般认为这 3 种运算拥有相同的计算代价。文献[20]给出的基准测量数据显示，这 3 者的计算代价比 ECSM 少 3 个数量级。因此协议 GSM [1], 3GPP [2], JLSS-I [5], Chang et al.09 [9]的计算复杂度都比较低。然而这些协议都不满足匿名 SWR 的安全性需求。

(2)对于基于 PKE, EXP, ECSM 或 ECBP 协议的分析：通常认为在达到同样的安全标准时，ECSM

表 2 各漫游协议之间的性能比较

	消息传送次数	计算复杂性	认证能力	用户匿名性及不可追踪性	向前保密性
GSM[1]	6	11 STR	单向	弱	无
3GPP[2]	5	10 SYM	双向	弱	无
JLSS-I[5]	5	10 SYM	单向	Partial	无
Chang et al.09[9]	8	17 SYM	双向	弱	无
JLSS-II[5]	6	6 SYM, 15 EXP	单向	无	有
Yang et al.07[6]	8	$\geq$ 10 PKE	双向	强	有
Wan et al.08[7]	4	10 SYM, 4 ECSM3 ECBP	双向	强	有
Yang et al.08[8]	4	4 MAC, 4 EXP, 6 PKE	双向	强	有
SYM-SWR	4	2 SYM, 8MAC, 4 ECSM	双向	强	有

注：

STR: Stream Cipher Encryption 流加密　　MAC: Message Authentication Code Computation 消息认证码

SYM: Block Cipher Encryption 分组加密　　PKE: Public Key Encryption or Decryption 公钥加密解密

EXP: Modular Exponentiation 模幂运算　　ECSM: Elliptic Curve Scalar Multiplication 椭圆曲线上的标量乘

ECBP: Elliptic Curve Bilinear Pairing 椭圆曲线上的线性 Pairing 运算

的计算代价比 EXP 和 PKE 要低(请参考文献[20]给出的基准测量数据)。本文尽可能地通过转化将其他协议中的 EXP 和 PKE 当作 ECSM 来考虑。这样做是合理的，因为在普通乘法群上 EXP 和 PKE 可以很容易的转化为 ECSM。然而 JLSS-II[5]是个例外，因为协议中形如 $g^{x^y} \bmod n$ 的 EXP 运算无法转化为 ECSM。

(a)JLSS-II[5]需要 15 个 EXP 而安全性不满足要求。

(b)Yang et al.07 [6]满足了匿名 SWR 的所有安全性需求，但所需的消息传送次数是 SYM-SWR 的 2 倍，而且需要至少 10 个 ECSM，因此该协议的计算复杂度和通信复杂度均比 SYM-SWR 高出一倍以上。

(c)Wan et al.08[7]虽然满足安全性需求，但如第 1 节所述不适合长期漫游的用户。而且该协议需要 3 个 ECBP，由于 ECBP 的计算代价远远高于 ECSM，因此其计算复杂度高出 SYM-SWR 至少一倍以上。

(d)Yang et al.08[8]仅需要 4 次消息传送，然而该协议需要至少 10 个 ECSM (SYM-SWR 仅需要 6 个 ECSM)。另外，其中的 6 个 ECSM 的代价远高于 SYM-SWR 中的 ECSM，因为前者运算对象的长度是后者的 3 倍。因此 SYM-SWR 的计算复杂度在 Yang et al.08[8]的 50%以下。

总之，SYM-SWR 是目前满足匿名 SWR 所有安全性需求的协议中通信复杂度和计算复杂度最低的。

5 结束语

本文提出了一种高效的无线匿名漫游安全协议 SYM-SWR。该协议不但满足所有如下安全性需求包括服务器身份可认证、用户身份可认证、建立安全的会话密钥、向前保密性、用户匿名性和不可追踪性，而且是目前已知此类协议中第 1 个完全基于对称密钥且通信复杂度和计算复杂度最低。因为 SYM-SWR 只需要 4 次消息传送而且采用的是 MAC 和对称密钥加密这两类高效的运算而不需要代价高昂的公钥基础结构(PKI)。并且 SYM-SWR 是在 CK model 下构造的，从而是可证明安全的。同时本文提出两个 CK model 下的 MT-authenticator，一个是为了解决多个会话时的同步失败问题，另一个是为了满足用户匿名性和不可追踪性。而且这两个 MT-authenticator 也可被用来构造其他的 CK model 下的密钥交换协议。

参 考 文 献

[1] Mouly M and Pautet M B. The GSM System for Mobile Communications[M]. France: Telecom Publishing, 1992.

[2] 3GPP TS 33.102: 3rd generation partnership project 3GPP, 3G Security, Security Architecture. Technical Specification Group (TSG) SA, Oct. 2003.

[3] Im T R, Lee H, Cho K T, and Lee D H. Secure mutual authentication and fair billing for roaming service in wireless mobile networks. Proceedings of Convergence and Hybrid Information Technolog (ICCIT '08), Busan, Korea, 2008: 466–471.

[4] Li G S and Wang P H. A new provably-secure key agreement protocol for roaming in mobile networks. Wuhan University *Journal of Natural Sciences*, 2008, 13(5): 605–608.

[5] Jiang Y X, Lin C, Shen X M, and Shi M H. Mutual

authentication and key exchange protocol for roaming services in wireless mobile networks. *IEEE Transactions on Wireless Communications*, 2006, 5(9): 2569–2577.

[6] Yang G M, Wong S D, and Deng X T. Anonymous and authenticated key exchange for roaming networks. *IEEE Transactions on Wireless Communications*, 2007, 6(9): 3461–3472.

[7] Wan Z G, Ren K, and Bart P. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks. Proceedings of the first ACM conference on Wireless network security, NY, USA, 2008: 62–67.

[8] Yang G M, Wong S D, and Deng X T. Formal security definition and efficient construction for roaming with a privacy-preserving extension. *Journal of Universal Computer Science*, 2008, 14(3): 441–462.

[9] Chang C C, Lee C Y, and Chiu Y C. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Computer Communications, Elsevier*, 2009, 42(4): 611–618.

[10] Wu C C, Lee W B, and Tsaur W J. A secure authentication scheme with anonymity for wireless communications. *IEEE Communication Letter*, 2008, 12(10): 722–723.

[11] Chen H, Xiao Y, Hong X Y, Hu F, and Xie J. A survey of anonymity in wireless communication systems. Security and Communication Networks, 2008, Published Online by John Wiley & Sons: http://dx.doi.org/10.1002/sec.78.

[12] Youn T Y, Park Y H, and Lim J. Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. *Communication Letter*, 2009, 13(7): 471–473.

[13] Men L, Wu C H, and Irwin J D. Localized authentication for internetwork roaming across wireless LANs. *Proceedings of IEEE Communication*, 2004, 151(5): 496–500.

[14] Zhu H J, Lin X D, Lu R X, Ho P H, and Shen X M. SLAB: secure localized authentication and billing scheme for wireless mesh networks. *IEEE Transactions on Wireless Communications*, 2008, 17(10): 3858–3868.

[15] Yang G M, Huang Q, Wong S D, and Deng X T. Universal authentication protocols for anonymous wireless communications. *IEEE Transactions on Wireless Communications*, 2010, 9(1): 168–174.

[16] Jin H M, Wong S D, and Xu Y L. Efficient group signature with forward secure revocation. Proceedings of International Conference on Security Technology 2009, CCIS, Jeju Island, Korea, 2009, Vol. 58, 124–131.

[17] Canetti R and Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. Proceedings of EUROCRYPT 2001, Innsbruck, Austria, 2001, LNCS, Vol. 2045: 453–474.

[18] Bellare M, Canetti R, and Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols. Proceedings of 30th ACM Symp. on Theory of Computing. ACM, Dallas, Texas, USA, 1998: 419–428.

[19] Tin Y S T, Boyd C, and Nieto J G. Provably secure key exchange: an engineering approach. Proceedings of the Australasian information security workshop. Australian Computer Society, Inc., 2003: 97–104.

[20] Wei D. "Crypto++ 5.2.1 benchmarks." [Online]. Available: http://www.cryptopp.com/benchmarks.html, 2009.

金海旻： 男，1981年生，博士生，研究方向为信息安全、密码学、网络安全等；

许胤龙： 男，1963 年生，教授，博士生导师，安徽省高性能计算重点实验室主任，研究方向为网络编码性能及安全、分布式存储、路由算法等.

王 石： 男， 1971 年生，助理教授(TENURE-TRACK)，博士生导师，研究方向为信息安全、应用密码学等.