ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.4, April 2006, pp.868−875
DOI: 10.1360/jos170868

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种认证密钥协商协议的安全分析及改进*

周永彬[1,2+], 张振峰[1,2], 冯登国[1,2]

[1](中国科学院 软件研究所,北京 100080)

[2](信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

Analysis and Improvement of a Security-Provable Mutually Authenticated Key Agreement Protocol

ZHOU Yong-Bin[1,2+], ZHANG Zhen-Feng[1,2], FENG Deng-Guo[1,2]

[1](Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[2](State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

+ Corresponding author: Phn: +86-10-82612797, Fax: +86-10-62520469, E-mail: zyb@is.iscas.ac.cn, http://www.is.iscas.ac.cn

Zhou YB, Zhang ZF, Feng DG. Analysis and improvement of a security-provable mutually authenticated key agreement protocol. *Journal of Software*, 2006,17(4):868−875. http://www.jos.org.cn/1000-9825/17/868.htm

Abstract: Deng, *et al*. proposed a security-provable mutually authenticated key agreement protocol MAKAP for mobile communication in 2003. This paper demonstrates by mounting an effective attack against MAKAP that the protocol has security flaws. It is vulnerable against unknown key-share attack. This paper investigates the reasons why such flaws exist and proposes an improved protocol version (called MAKAP-I protocol). The MAKAP-I protocol is not only provably secure within the random oracle model but also more efficient and practical in terms of computation and communication cost memory requirement and implementation cost, than the original MAKAP protocol.

Key words: authenticated key agreement protocol; unknown key-share attack; provable security

摘 要: 针对用于移动通信的可证安全的双向认证密钥协商协议 MAKAP 给出了一种有效攻击,指出该协议存在安全缺陷,它不能抵抗未知密钥共享攻击.分析了这些安全缺陷产生的原因,并给出了一种改进的协议MAKAP-I.改进后的 MAKAP-I 协议不但是可证安全的,而且无论从计算开销、通信开销、存储开销以及实现成本等方面,都比原 MAKAP 协议更高效、更实用.

关键词: 认证密钥协商协议;未知密钥共享攻击;可证明安全性

中图法分类号: TP309 文献标识码: A

两通信实体之间的双向认证密钥协商协议,可以使得通信双方确信对方的真实身份,同时,协议结束之后双方确信:两者共享了一个只有他们知道的秘密会话密钥.该秘密会话密钥可为此后的通信提供数据保密性和数据完整性等保护.除了必须满足一些基本的安全性质以外(如显式认证、能抵抗一般意义下的被动和主动攻击

* Supported by the National Natural Science Foundation of China under Grant Nos.60503014, 60373039, 60273027, 90304007 (国家自然科学基金)

Received 2004-08-20; Accepted 2005-06-20

等),这类协议还经常被希望具有一些其他良好的安全属性,如已知会话密钥安全性、前向安全性、抗密钥泄漏伪装、抗未知密钥共享攻击、抗 DoS 攻击等[1−4].

随着移动通信系统中的安全问题越来越多地受到重视,通过认证密钥协商协议来确认网络和用户的身份,已成为这种环境中的一个基本安全问题.尽管也有许多基于对称密码技术构造的认证密钥协商协议,但由于密钥管理简单以及可扩展性强等明显的优势,基于公钥密钥技术构建认证密钥协商协议已成为当前认证密钥协商协议设计的主流[1,5−8].文献[1]中提出的 MAKAP 协议就是这样一种用于移动通信系统中的、可证安全的双向认证密钥协商协议.

对认证密钥协商协议的未知密钥共享攻击是这样一种攻击:攻击完成后,实体 A 确信和实体 B 共享了一个秘密会话密钥,而实体 B 则(错误地)认为他和另外一个实体 $E(E\neq A)$共享了该秘密会话密钥.这种攻击方法及其严重后果,最早是由 Diffie 等人给出的[5].文献[1]称 MAKAP 协议是安全的,并且在随机预言机模型[9]下证明了其安全性.本文指出了该协议存在安全缺陷,它不能抵抗未知密钥共享攻击.我们给出一种改进的 MAKAP-I 协议.MAKAP-I 协议不但是可证明安全的(在随机预言机模型下),而且比原 MAKAP 协议更高效,更实用.

1 MAKAP 协议

本节简要介绍 MAKAP 协议.本文的工作和 MAKAP 协议都基于一个公认的基本假设:DH 问题是难解的.协议中使用了 3 个不同的抗碰撞的单向杂凑函数 h_1,h_2 和 H,以及一个安全的对称加密算法 $ENC(\cdot)$,其中 K 为密钥.设系统全局参数为 g,q,p,其中 $g\in\mathbb{Z}_p^*$ 是一个 q 阶生成元,$\mathbb{Z}_q^*$ 为由 g 生成的 q 阶子群,p 和 q 均为大素数且满足 $q|(p-1)$.MAKAP 协议中,每一个网络服务器(即服务网络,用 B 表示)都有一对密钥(PK_B,SK_B),其中 PK_B 为公钥,SK_B 为私钥.每一个用户都有自己的长期秘密 $a\in\mathbb{Z}_q^*$ (即其私钥 SK_B).密钥的真实性可由证书权威(用 CA 表示)签发的数字证书来保证[2].这里,用户的公钥为 $PK_A=\langle g,p,q,g^a\rangle$,证书为 $Cert(A)=\left\langle ID_A,PK_A,\{ID_A,PK_A\}_{sig_{CA}}\right\rangle$;相应地,服务器端证书为 $Cert(B)=\left\langle ID_B,PK_B,\{ID_B,PK_B\}_{sig_{CA}}\right\rangle$.

假设 A,B 为协议的两个诚实执行者,其中 A 为用户,B 为网络服务器,则 MAKAP 协议执行过程(如图 1 所示).具体过程如下:

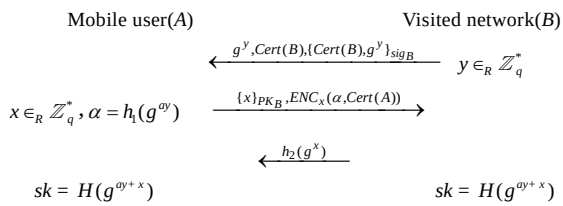

Fig.1 MAKAP protocol

图 1 MAKAP 协议

(1) B 随机选择一个秘密值 $g\in\mathbb{Z}_p^*$,计算 g^y.B 使用自己的私钥对$(g^y,Cert(B))$做数字签名 $\{g^y,Cert(B)\}_{sig_B}$.B 把 $g^y,Cert(B),\{g^y,Cert(B)\}_{sig_B}$ 发送给 A.

(2) A 验证 B 的数字签名,并检查 $1<g^y<q$ 是否成立.如果不成立,则终止协议,认证失败.

(3) A 随机选择一个秘密值 $g\in\mathbb{Z}_p^*$,并用 B 的公钥 PK_B(来自于 B 的证书 $Cert(B)$)加密 x.A 计算$\alpha=h_1((g^y)^a)$,并用 x 加密α和 $Cert(A)$.A 把 $\{x\}_{PK_B}$,$ENC_x(\alpha,Cert(A))$发送给 B.

(4) B 用 SK_B 解密 $\{x\}_{PK_B}$,并用 x 解密 $ENC_x(\alpha,Cert(A))$,获得α和 $Cert(A)$.B 验证 $Cert(A)$.如果不成功,则终止协议,认证失败.

(5) B 计算$\beta=h_1((g^a)^y)$,并与α进行比较.如果两者不同,则协议终止,认证失败.

(6) B 计算 $h_2(g^x)$,并把它发送给 A 作为确认消息.

(7) A 计算 $h_2(g^x)$,并与 B 发送来的消息进行比较:如果两者不同,则终止协议,认证失败.

(8) 此时,A 和 B 分别计算会话密钥 $sk=(g^{ya+x})$.

文献[1]声称:在 Bellare-Rogaway 模型(即随机预言机模型)下,MAKAP 协议是可证安全的.

2 对 MAKAP 协议的一种有效攻击

假设攻击者为 E.为成功对 MAKAP 协议进行攻击,攻击者需要生成自己的长期私钥 $e\in\mathbb{Z}_q^*$,并向证书权威机构申请自己的证书 $Cert(E)$.一旦这个准备过程完成,攻击者 E 就可对 MAKAP 协议实施未知密钥共享攻击,攻击过程(如图 2 所示)如下:

(1) B 随机选择一个秘密值 $y\in\mathbb{Z}_q^*$,计算 g^y.B 使用自己的私钥对 $g^y,Cert(B)$ 做数字签名 $\{g^y,Cert(B)\}_{sig_B}$.B 把 $g^y,Cert(B),\{g^y,Cert(B)\}_{sig_B}$ 发送给 A.

(1′) E 截获 B 发送给 A 的消息,并使用自己的证书 $Cert(E)$替换 B 的证书 $Cert(B)$,同时使用自己的签名 $\{g^y,Cert(E)\}_{sig_E}$ 替换 B 的签名 $\{g^y,Cert(B)\}_{sig_B}$.E 将 $g^y,Cert(E),\{g^y,Cert(E)\}_{sig_E}$ 发送给 A.

(2) A 验证 E 的数字签名,并检查 $1<g^y<q$ 是否成立:如果不成立,则终止协议,认证失败.

(3) A 随机选择一个秘密值 $x\in\mathbb{Z}_q^*$,并用 E 的公钥 PK_B(来自于 E 的证书 $Cert(E)$)加密 x.A 计算 $\alpha=h_1((g^y)^a)$,并用 x 加密 α和 $Cert(A)$.A 把 $\{x\}_{PK_E},ENC_x(\alpha,Cert(A))$发送给 E.

(3′) E 用 SK_B 解密 $\{x\}_{PK_E}$,并用 PK_B 再次加密 x,然后再把 $\{x\}_{PK_B},ENC_x(\alpha,Cert(A))$发送给 B.

(4) B 用 SK_B 解密 $\{x\}_{PK_B}$,并用 x 解密 $ENC_x(\alpha,Cert(A))$,获得α和 $Cert(A)$.B 验证 $Cert(A)$:如果不成功,则终止协议,认证失败.

(5) B 计算$\beta=h_1((g^a)^y)$,并与α进行比较:如果两者不同,则终止协议,认证失败.

(6) B 计算 $h_2(g^x)$,并把它发送给 A 作为确认消息.

(6′) E 截获 B 发送的消息 $h_2(g^x)$,并把它转发给 A 作为确认消息.

(7) A 计算 $h_2(g^x)$,并与 E 发送来的消息作比较:如果两者不同,则终止协议,认证失败.

(8) 此时,A 和 B 分别计算会话密钥 $sk=H(g^{ya+x})$.

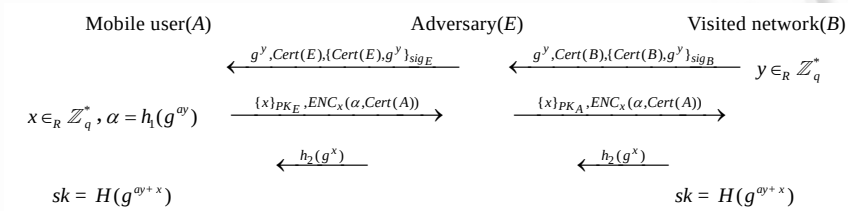

Fig.2 An effective unkown key-share attack against MAKAP protocol

图 2 对 MAKAP 协议的一种有效的未知密钥共享攻击

上述攻击过程成功执行后,A 和 B 都可以计算出共享的会话密钥 sk,而用户 A 则错误地认为他正和攻击者 E 共享该会话密钥 sk.尽管攻击者 E 并不知道会话密钥 sk,但是该攻击已经彻底破坏了协议的安全目标.

由图 2 可以看出,MAKAP 协议之所以不能抵抗未知密钥共享攻击,是因为在协议的第 1 个消息中,对数字签名的使用方法有误:在签名生成后的协议消息流中,没有任何关于签名者身份的确认机制.可见,使用这种错误的数字签名不能达到预期的安全目标,反而徒增了协议的计算复杂性.

结论 **1**. 存在对 MAKAP 协议的有效未知密钥共享攻击.

3 一种改进的 MAKAP 协议——MAKAP-I 协议

本节给出一种改进的 MAKAP 协议(本文称为 MAKAP-I 协议),其执行过程(如图 3 所示)如下:

(1) B 随机选择一个秘密值 $y\in\mathbb{Z}_q^*$,计算 g^y .B 把 g^y,$Cert(B)$发送给 A.

(2) A 检查 $1<g^y<q$ 是否成立:如果不成立,则终止协议,认证失败.

(3) A 随机选择一个秘密值 $x\in\mathbb{Z}_q^*$,计算 g^x,并用 B 的公钥 PK_B(来自于证书 $Cert(B)$)加密 g^x.然后,A 计算 $\alpha=h_1((g^y)^a||g^x||g^a||g^b)$,并把 $\{g^x\}_{PK_B}$,$Cert(A)$,α发送给 B.

(4) B 用 SK_B 解密 $\{g^x\}_{PK_B}$,检查 $1<g^x<q$ 是否成立.如果不成立,则终止协议,认证失败;否则,B 验证α和 $Cert(A)$.如果不成功,则终止协议,认证失败.

(5) B 计算$\beta=h_1((g^a)^y||g^x||g^a||g^b)$,并与$\alpha$进行比较:如果两者不同,则终止协议,认证失败.

(6) B 计算 $h_2(g^{xy}||g^b||g^a)$,并把它发给 A 作为确认消息.

(7) A 计算 $h_2(g^{xy}||g^b||g^a)$,并与 B 发送来的消息作比较:如果两者不同,则终止协议,认证失败.

(8) 此时,A 和 B 分别计算会话密钥 $sk=H(g^{yx}||g^a||g^b)$.

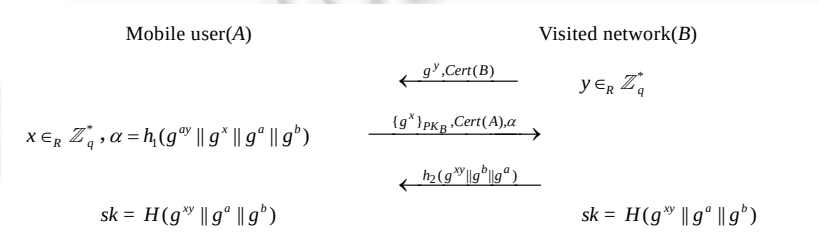

Fig.3 MAKAP-I protocol

图 3 MAKAP-I 协议

由图 3 可以看出,在 MAKAP-I 协议中,第 2 个消息和第 3 个消息中都使用了显示的用户身份标识(由于 g^a 和 g^b 是从相应的证书 $Cert(A)$和 $Cert(B)$中得到的,这等价于在消息中显式绑定了 ID_A 和 ID_B),故 MAKAP-I 协议可以抵抗未知密钥共享攻击.

推论 **1**. MAKAP-I 协议可抵抗未知密钥共享攻击.

MAKAP-I 协议中,即便获得了服务网络的长期私钥 SK_B ,由于无法知道 g^x 和 g^y 所对应的 x 值和 y 值,攻击者仍然无法获得以前会话所使用的秘密会话密钥(由 DH 假设可知,仅获得 g^x 和 g^y 仍然无法计算出 g^{xy}).

推论 **2**. MAKAP-I 协议可提供前向安全性.

4 MAKAP-I 协议的安全性证明与性能分析

4.1 安全性证明

我们将基于 ROM 模型来证明 MAKAP-I 协议的安全性,其方法则采用 Menezes 等人给出的经典的认证密钥协商协议安全性形式化模型和定义[2].ROM 模型[9,10]是一种分布式计算模型.在这种模型中,被称为“预言机”的运行于机器上的进程被刻画为协议参与实体的一个实例,而攻击者的能力则被刻画为对这些预言机的查询.在 ROM 模型中,认证密钥协商的安全性分别使用“匹配的会话”(用以刻画认证性质)和“不可区分性”(用以刻画保密性质)来形式地定义[2,9].本文将采用与文献[2]中相同的符号和定义,关于各种符号定义、预言机、可忽略函数、匹配回话以及函数 $NoMatching^E(k)$和函数 $Advantage^E(k)$的有关细节,请参见文献[2].

定义 **1**.[2,9] 一个密钥协商协议 P 是安全的,如果满足下列条件:

(1) 协议 P 是精确定义的.在一个良性攻击存在的情况下,预言机 $\Pi^s_{i,j}$ 和 $\Pi^t_{j,i}$ 在协议 P 结束时都处于接受状态,并且拥有同样的会话密钥.

(2) 协议 P 为参与实体提供了同一个实时会话.即如果两个没有变坏的预言机有匹配的会话,则它们都处于接受状态,并且拥有相同的会话密钥.

(3) 协议 P 的消息是可认证的,即 $NoMatching^E(k)$的概率是可忽略的.

(4) 协议 P 保护了新鲜的会话密钥,即 $Advantage^E(k)$是可忽略的.

在 ROM 模型中,所有实体之间的任意通信都在攻击者的控制之下.攻击者可以任意地读取、插入、删除、篡改、延迟发送、重放任何消息,也可以在任何时候发起与任何参与者的任意会话.尽管攻击者的能力是如此的强大,ROM 模型对攻击者也作了一个基本的限制:即攻击者必须是一个概率多项式时间图灵机(PPT).

定理 **1**. 假设安全的公钥加密方案和抗碰撞的单向函数存在,基于 DH 假设,则 MAKAP-I 协议是安全的.

要证明 MAKAP-I 协议是安全的,只要证明它满足定义 1 的每一个条件就足够了.

引理 **1**. MAKAP-I 协议是精确定义的.

证明:按照 MAKAP-I 协议的描述,存在良性攻击的情况下, $\Pi^s_{i,j}$ 和 $\Pi^t_{j,i}$ 在协议结束时都会处于接受状态,并且拥有同样的会话密钥 $sk=H(g^{xy}\|g^a\|g^b)$.也即 MAKAP-I 协议是精确定义的. □

引理 **2**. MAKAP-I 协议为参与双方提供了同一个实时会话.

证明:如果两个预言机 $\Pi^s_{i,j}$ 和 $\Pi^t_{j,i}$ 有匹配的会话,则说明两者都诚实地执行了协议.按照 MAKAP-I 协议的描述,则 $\Pi^s_{i,j}$ 和 $\Pi^t_{j,i}$ 一定会正常结束,并且都会处于接受状态,也能计算出相同的会话密钥 $sk=H(g^{xy}\|g^a\|g^b)$.也即 MAKAP-I 协议为 $\Pi^s_{i,j}$ 和 $\Pi^t_{j,i}$ 提供了同一个实时回话. □

引理 **3**. MAKAP-I 协议是一个双向认证协议.

用反证法证明.假定 E 是一个任意的攻击者并且 $Pr[NoMatching^E(k)]$是不可忽略的,我们将证明假定为安全的密码原语就会被攻破.这里,将引理 3 的证明分成两部分,首先证明移动客户端身份认证,然后证明服务器身份认证.

(1) 移动客户端身份认证

这里仅需要考虑 MAKAP-I 协议的前两条消息.

命题 **1**. 如果存在安全的公钥加密方案,基于 DH 假设,则在收到第 1 个消息后,只有 A 能够正确计算出第 2 个消息,即对于任意一个 PPT 类型的攻击者 E,有一个可忽略的函数$\varepsilon(k)$,对于足够大的 k,有:

$$Pr[E(1^k,Y,ID_B,PK_B)=h_1(g^{ay}\|g^x\|g^a\|g^b)\,|\,y\xleftarrow{R}\mathbb{Z}_q^*;Y\leftarrow g^y]\le\varepsilon(k).$$

证明:令 $ForgeRes$ 表示上述事件,即给定输入 1^k,g^y,ID_B,PK_B,E 在不知道 SK_A 的情况下,可以在多项式时间内,成功计算出 $h_1(g^{ay}\|g^x\|g^a\|g^b)$.令 $NoSendA$ 表示这样一个事件:服务器发送了 g^y,$Cert(B)$之后,接收到了 $\alpha=h_1(g^{ay}\|g^x\|g^a\|g^b)$,如果此时服务器验证接受,但这个$\alpha$实际上却不是 A 发送的.

显然, $NoSendA$ 事件可以很容易地在多项式时间内归约到事件 $ForgeRes$,即有 $Pr[NoSendA]=Pr[ForgeRes]$.

对于 $NoSendA$ 事件,则有:

1. 这个α可能是攻击者自己猜测出来的.假设一共进行了 q 次预言机查询,且 $h_1(\cdot)$的输出长度为 l_1,那么攻击者猜测正确的概率不超过 $\frac{q}{2^{l_1}}$.

2. 或 g^y 是以前某个预言机查询时已经询问过的.假设以前一共查询了 q'次,现在移动查询了 q 次,那么 g^y 被询问过的概率不超过 $\frac{q}{q'}$.

3. 或者攻击者能计算出 g^{ay},并由此计算出 $h_1(g^{ay}\|g^x\|g^a\|g^b)$.显然,攻击者能计算出 g^{ay} 的事件是一个 CDH 事件,记为 $Event^{CDH}$.故有 $Pr[ForgeRes]=Pr[NoSendA]\le Pr\left\{Event^{CDH}+\frac{q}{2^{l_1}}+\frac{q}{q'}\right\}$.

注意,证明过程中没有考虑 g^x 的参与.这是由于任意的攻击者都可以很容易地计算出一个合法的 $\{g^x\}_{PK_B}$,因此如果攻击者能够计算出 g^{ay},那么它自然可以随机选择某个 $r \in \mathbb{Z}_p^*$,并发送对应的消息.也就是说,攻击者获得 g^x 的事件包含在他能计算 g^{ay} 事件之内.由 DH 困难性假设可知,事件 $Event^{CDH}$ 的概率是可忽略的.

令 $\varepsilon(k) = Pr\left\{Event^{CDH} + \frac{q}{2^{l_1}} + \frac{q}{q'}\right\}$,故命题 1 得证. □

(2) 服务器端身份认证

命题 **2**. 如果存在安全的公钥加密方案,基于 DH 假设,则在发出第 1 个消息和收到第 2 个消息之后,只有 B 能够正确计算出第 3 个消息,即对于任意一个 PPT 类型的攻击者 E,有一个可忽略的函数 $\varepsilon(k)$,对于足够大的 k,有: $Pr[E(1^k, X, ID_B, PK_B, PK_B) = h_2(g^{xy} \| g^b \| g^a) \mid x \xleftarrow{R} \mathbb{Z}_q^*; X \leftarrow \{g^x\}_{PK_B}] \le \varepsilon(k)$.

证明:命题 2 的证明与命题 1 的证明类似,此略. □

根据命题 1 和命题 2,引理 3 成立.即 MAKAP-I 协议是一个双向认证协议. □

引理 4. MAKAP-I 协议保护了新鲜的会话密钥.

证明:由于 MAKAP-I 协议中所使用的杂凑函数是抗碰撞且具有一定伪随机形式的函数,因此,如果要正确计算出会话密钥 $sk=H(g^{xy} \| g^a \| g^b)$,必须要获得 g^{xy} 的值.也即要在 *Test* 查询中获得 g^{xy} 的值.

按照 MAKAP-I 协议的规范,必须首先由 $\{g^x\}_{PK_B}$ 获得 g^x 的值,进而才有可能得到 x 值;或者直接自 $\{g^x\}_{PK_B}$ 获得 x 的值.由假设所使用的公钥加密体制是安全的可知,获得 g^x 的概率是可忽略的,这自然也就意味着获得 x 值的概率也是可忽略的.因此,获得 g^{xy} 值的概率是可忽略的.

也就是说, $Advantage^E(k)$是可忽略的,即 MAKAP-I 协议保护了新鲜的会话密钥. □

定理 1 的证明:根据引理 1~引理 4,定理 1 成立. □

由推论 1~推论 2 以及定理 1,不难得出:

推论 **3**. MAKAP-I 协议比 MAKAP 协议具有更高的安全性.

4.2 性能分析

这里,我们将从计算开销、通信开销、存储开销以及实现成本等方面对 MAKAP-I 协议进行分析,并将其与 MAKAP 协议进行比较.

4.2.1 计算开销

与 MAKAP 协议相比,MAKAP-I 协议的服务器端减少了 1 次签名运算,但仍然需要 3 次模指数运算;而移动用户端则减少了 1 次签名验证运算(对于 ElGamal 类签名而言,签名验证至少需要 2 次模指数运算),取而代之,增加了 1 次模指数运算.原协议和 MAKAP-I 协议的预计算特性相同,但是 MAKAP-I 协议的移动客户端和服务器端都没有使用任何对称加密/解密运算.

为了便于比较,我们可以简单地将模指数运算和签名生成、签名验证所需要的计算量大致等同起来处理.同时,鉴于与对称加密运算相比,杂凑运算的速度快很多,这里忽略杂凑运算的影响.两协议的计算开销比较见表 1.不难看出,无论是服务器端,还是移动客户端,MAKAP-I 协议的计算开销比 MAKAP 协议的计算开销都要小.

Table 1 Computational cost comparison between MAKAP and MAKAP-I (times)

表 **1** MAKAP-I 协议与 MAKAP 协议的计算开销比较 (times)

	MAKAP		MAKAP-I	
	Modular exponentiation	Symmetric encryption/decryption	Modular exponentiation	Symmetric encryption/decryption
Visited network	5	1	4	0
Mobile user	4	1	4	0

4.2.2 通信开销

由图 1 和图 3 可以看出,与 MAKAP 协议相比,MAKAP-I 协议的通信开销有明显的降低.其通信开销的降低

主要由两个协议的第 1 条消息决定,其减少量大致为 MAKAP 协议第 1 条消息中使用的安全数字签名方案所输出的一个有效签名的长度(单位为字节或比特).

4.2.3 存储开销

MAKAP-I 协议中没有采用数字签名运算和对称加密/解密运算,因此,无须实现这些功能所必需的存储单元.可见,与 MAKAP 协议相比,MAKAP-I 协议中移动客户端和服务器端的存储开销都更小.

4.2.4 实现成本

由上述对比不难得出结论:MAKAP-I 协议比 MAKAP 协议的实现成本更小.

综上所述,MAKAP-I 协议在计算开销、通信开销、存储开销以及实现成本等方面都明显优于原 MAKAP 协议.即 MAKAP-I 协议更高效,因而实用性更好.

结论 **3**. MAKAP-I 协议比 MAKAP 协议更高效、更实用.

5 结束语

认证密钥协商协议对于移动通信环境中的通信双方通过公开的网络建立安全通信至关重要.本文通过给出一种有效的攻击,指出文献[1]所给出的用于移动通信的可证安全的双向认证密钥协商协议 MAKAP 中存在安全缺陷,它不能抵抗未知密钥共享攻击.文中分析了这类安全缺陷产生的原因,并给出了一种改进的 MAKAP-I 协议.改进后的 MAKAP-I 协议不但是可证安全的,而且无论从计算开销、通信开销、存储开销以及实现成本等方面都比原 MAKAP 协议更高效.因而,其实用性更好.

本文的研究再次表明:在随机预言机模型下的可证明安全性,只能提供一定程度的安全保证,并不能保证密码协议对于已知的各种攻击都是安全的.合理的安全模型是进行安全性分析的重要前提条件.

References:

[1] Deng HS, Zuo YQ, Zhao YM, Bao ZD. A security-provable mutually authenticated key agreement protocol in mobile communication. Journal of Software, 2003,14(8):1489−1494 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1489.htm

[2] Wilson SB, Johnson D, Menezes A. Key agreement protocols and their security analysis. In: Darnell M, ed. Proc. of the 6th Int'l Conf. on Crypotography and Coding. LNCS 1355, Berlin: Springer-Verlag, 1997. 30−45.

[3] Canetti R, Krawczyk H. Analysis and key-exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. Advances in Cryptology—EUROCRYPT 2001. LNCS 2045, Berlin: Springer-Verlag, 2001. 453−474.

[4] Boyd C, Mathuria A. Protocols for Authentication and Key Establishment. Berlin: Springer-Verlag, 2003. 137−199.

[5] Diffie W, van Oorschot PC, Wiener MJ. Authentication and authenticated key exchange. Designs, Codes and Cryptography, 1992, 2:107−125.

[6] Wong DS, Chan AH. Mutual authentication and key exchange for low power wireless communications. In: Edmonds A, Yenser G, Ferrari G, eds. Proc. of the IEEE MILCOM 2001 Conf. Washington: IEEE Communication Society, 2001. 39−43.

[7] Jakobsson M, Pointcheval D. Mutual authentication for low-power mobile devices. In: Syverson P, ed. Financial Cryptography 2001. LNCS 2339, Berlin: Springer-Verlag, 2001. 178−195.

[8] Wong DS, Chan AH. Efficient and mutually authenticated key exchange for low power computing devices. In: Boyd C, ed. Advances in Cryptology—ASIACRYPT 2001. LNCS 2248, Berlin: Springer-Verlag, 2001. 272−289.

[9] Bellare M, Rogaway P. Entity authentication and key distribution. In: Stinson DR, ed. Advances in Cryptology—CRYPTO'93. LNCS 773, Berlin: Springer-Verlag, 1993. 232−249.

[10] Bellare M, Rogaway P. Provably secure session key distribution-the three party case. In: Leighton FT, Borodin A, eds. Proc. of the 27th ACM Symp. on the Theory of Computing. Las Vegas: ACM Press, 1995. 57−66.

附中文参考文献:

[1] 邓红素,左益强,赵一鸣,鲍振东.移动通信中可证安全的双向认证密钥协商协议.软件学报,2003,14(8):1489–1494. http://www.jos.org.cn/1000-9825/14/1489.htm

周永彬(1973–),男,博士,副研究员,主要研究领域为应用密码学,网络与信息安全理论与技术.

冯登国(1965–),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为网络和信息安全.

张振峰(1972–),男,博士,副研究员,主要研究领域为密码学,信息安全理论与技术.

✧✧