第34卷 第14期 计 算 机 工 程 2008年7月
Vol.34 No.14 Computer Engineering July 2008
·安全技术· 文章编号：1000—3428(2008)14—0174—02 文献标识码：A 中图分类号：TP393.08

# 一种可证安全性的无线网络密钥协商协议

赵宗渠，刘艳霞
(河南理工大学计算机科学与技术学院，焦作 454003)

**摘 要：**在无线网络的分布式环境中，通信双方间建立安全的会话很重要。在借鉴以往无线通信密钥协商协议的基础上，提出一个在对称实体之间可相互认证的密钥协商协议 SAKAP，在随机预言机模型下证明其安全性，并给出协议的性能分析。与以往的协议相比，该协议是可证明安全的，且具有较高的可行性。

**关键词：**认证密钥协商协议；可证安全性；随机预言机模型

# Key Agreement Protocol with Provable Security in Wireless Network

ZHAO Zong-qu, LIU Yan-xia
(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003)

**【Abstract】** In the distributed computing environments such as wireless network, it is critical to establish a secure session between communicators. A mutual key agreement protocol, namely Symmetrical Authenticated Key Agreement Protocol(SAKAP), is proposed to authenticate identities and establish secure session key between symmetrical users. The security of the protocol is proved in Random Oracle(RO) model, and its performances are analyzed. SAKAP has the advantages of provable security and considerable feasibility over other protocols.

**【Key words】** authenticated key agreement protocol; provable security; Random Oracle(RO) model

## 1 概述

移动通信中的认证协议是建立安全会话的关键，通信媒介的开放性使通信双方在认证过程中更易受到攻击。通过安全的认证协议，会话双方确认对方的身份，建立共同的会话密钥，对无线通信提供进一步的安全保障。这种认证通信双方身份并建立共享密钥的协议称为带认证的密钥协商协议。

基于对称密钥体制的协议需要通信实体事先共享一个长期密钥，或者通过在线的可信第三方参与协议执行。在这类系统中，密钥管理和系统的可扩展性是主要问题。使用公钥密码体制的密钥建立协议时会受处理能力、存储空间及传输速度的限制，移动通信方使用互联网中常用的 SSL 等密钥建立协议则成本太高，如果协议中有过多的加密、解密运算，还会降低协议的执行速度。基于证书的认证系统可以通过证书来保证通信用户身份的真实性，证书的离线验证减少了通信量，因此，成为无线网络中常用的密钥协商机制。

密钥协商协议的可证明安全性是通过规划协议的形式化安全模型来避免或减少协议中可能会出现的漏洞，随机预言机(Random Oracle, RO)模型方法论[1]的提出使得过去仅作为纯理论研究的可证明安全性理论迅速在实际应用领域取得了重大进展。

文献[2]提出的 MAKAP 协议是基于 RO 模型的可证明安全的认证密钥建立协议，文献[3]指出其会受到一种未知密钥共享攻击，并将其改进为 MAKAP-1 协议。但是改进的协议在身份认证过程中使用了加密/解密方式对服务器身份进行认证，这种认证方式存在密码服务滥用的安全缺陷。虽然还没有发现具体的攻击实例，但是协议中额外提供的解密预言机不但没有增强安全性，反而带来了安全隐患；另外，加密/解密本身的代价增加了协议的计算开销(增加了 2 次模指数运算)。

本文介绍一种适用于移动环境、对等实体通过公钥证书进行相互认证和密钥协商的协议——SAKAP(Symmetrical Authenticated Key Agreement Protocol)，并且在 RO 模型下证明协议的安全性是基于 Computational Diffie-Hellman(CDH)问题的。

## 2 SAKAP 协议描述

本文提出了新的密钥协商协议SAKAP，其中使用的杂凑函数$h_1, h_2, h_3$是抗碰撞的单向杂凑函数。

设$g, p, q$为系统全局参数，其中，$g \in \mathbb{Z}_p^*$是一个$q$阶生成元；$\mathbb{Z}_q^*$为由$g$生产的$q$阶子群；$p$和$q$均为大素数，且满足$p|q-1$。在应用环境中，每个用户都有一个长期秘密$a \in \mathbb{Z}_q^*$和对应的公开秘密$g^a \bmod q$，用户向一个权威机构(CA)注册其公开秘密，其真实性由CA签发的数字证书来保证。用户$A$的公钥为$PK_A=\langle g, p, q, g^a\rangle$，证书为$Cert(A)=\langle ID_A, PK_A, \{ID_A, PK_A\}_{sigCA}\rangle$。相应地，用户$B$的公钥和证书分别为$PK_B=<g, p, q, g^b>$和$Cert(B)=<ID_B, PK_B, \{ID_B, PK_B\}_{sigCA}>$。CA保证每一个用户的标识在系统中是唯一的，防止攻击者注册与合法用户相同的公钥后冒充用户参与协议。

CDH问题：给定$g^x$和$g^y$($x$和$y$是随机选择的)计算$g^{xy}$目前被认为多项式时间内不可解的。

假设 $A, B$ 是 2 个欲通过协议建立安全信道的用户，协议由 $A$ 发起，则 SAKAP 的过程如下：

(1)$A$ 随机选择一个秘密值 $x \in \mathbb{Z}_p^*$，计算 $g^x \bmod q$，并将

**基金项目：**河南理工大学青年基金资助项目(646155)
**作者简介：**赵宗渠(1974－)，男，助教，主研方向：网络安全，对等网络；刘艳霞，讲师
**收稿日期：**2008-01-03 **E-mail：**zhaozong_qu@hpu.edu.cn

结果和 $A$ 的数字证书发送给用户 $B$。

(2)$B$验证$A$证书的安全性，并检查 $1<g^x<q$是否成立，若不成立则终止协议，认证失败。

(3)$B$ 随机选择一个秘密值 $y\in\mathbb{Z}_p^*$，计算 $g^y \bmod q$ 和 $\alpha=h_1(g^{xb}\| g^y \| ID_B \| ID_A)$，将结果发送给$A$。

(4)$A$计算$h_1(g^{bx}\| g^y \| ID_B \| ID_A)$，验证其值与$\alpha$是否相等，若不等则协议终止，认证失败。

(5)$A$计算$\beta=h_2(g^{ay}\| g^x \| ID_A \| ID_B)$后，发送给$B$作为确认　消息。

(6)$B$验证重新计算$h_2(g^{ay} \| g^x \| ID_A \| ID_B)$并与$A$发送的数据作比较；如果两者不同，终止协议，认证失败。

(7)$A$ 和 $B$ 计算出 $SK=h_3(g^{bx}\| g^{ay} \| ID_A \| ID_B)$ 作为本次的会话密钥，协议完成。

整个协议如图 1 所示，其中，$\alpha=h_1(g^{xb}\| g^y \| ID_B \| ID_A)$；$\beta=h_2(g^{ay}\| g^x \| ID_A \| ID_B)$；$SK=h_3(g^{bx}\| g^{ay} \| ID_A \| ID_B)$。

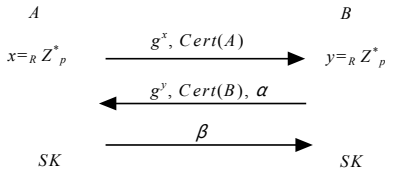


**图 1　SAKAP 协议**

协议中使用的$h_1()$, $h_2()$, $h_3()$都是$\{0,1\}^*\rightarrow\{0,1\}^k$的杂凑函数，它们可以看成RO模型中实例化的RO，杂凑函数的安全性满足文献[1]的要求。

## 3　协议安全性证明

本文基于 RO 模型证明协议的安全性，其描述方法和符号定义均采用文献[4]中密钥协商协议的安全性形式化模型和定义。在 RO 模型中，可以用对事先定义的预言机的询问来仿真协议参与者和攻击者的行为。协议的安全性分为认证性质和保密性质，其中，认证性质通过参与协议的各方之间“匹配的会话”来描述；保密性质通过会话密钥与某随机数的计算不可区分性来定义(基本方法是使会话密钥和一个敌手易于得到的某伪随机数紧密联系)。

$P=(\Pi, \psi, LL)$是一个多项式时间可计算的三元组函数，其中，$\Pi$描述诚实方的行为；$\psi$描述 $S$ 的行为；$LL$ 描述用户主密钥的初始分布。

**定义**[4-5] 一个密钥协商协议$P$是安全的，如果满足下列条件：

(1)在良性攻击存在的情况下，预言机 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^t$ 在 $P$ 结束时都处于接收状态，并且已经建立相同的会话密钥。

(2)如果 2 个没有变坏的预言机有匹配的对话，则它们都处于接收状态且拥有相同的会话密钥。

(3)协议$P$的消息是可认证的，即不匹配会话的概率$Nomatching^E(k)$是可忽略的。

(4)对$challenge$“猜测”正确的优势函数$Advantage^E(k)$是可忽略的。

在 RO 模型中，攻击者 $E$ 可以控制所有合法方之间的通信(可以控制协议启动时间或篡改、替换、删除数据等)，其能力可以形式化为一个概率多项式时间图灵机(PPT)。

**定理**　如果存在安全的数字签名方案和抗碰撞的单向函数，则协议是基于 CDH 问题安全的。

要证明协议是安全的，只要证明它满足定义的每个条件。

**引理 1** SAKAP 是精确定义的。

**证明**　按照协议的描述，存在良性攻击的情况下，$\Pi_{i,j}^s$ 和 $\Pi_{j,i}^t$ 在协议结束时都处于接收状态，并且拥有同样的会话密钥 $SK=h_3(g^{bx}\| g^{ay} \| ID_A \| ID_B)$，因此，SAKAP 是精确定义的。

**引理 2** SAKAP 为参与双方提供同一个实时会话。

**证明**　根据定义的条件(2)，如果 2 个预言机 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^t$ 有匹配的对话，说明两者都诚实地执行了协议，能够计算出相同的会话密钥，因此，协议能为通信双方提供实时会话伙伴。

**引理 3** SAKAP 能够认证双方身份，即它是一个可相互认证的协议。

考察协议的结构不难发现，在第 1 个消息中，$A$ 使用自己数字证书向 $B$ 证明其公钥的真实性，在消息 2 中 $A$ 也收到了 $B$ 的真实公钥。按照 CDH 问题，只要 $A$ 和 $B$ 能够计算出 $\alpha$ 和 $SK$。

用反证法先证明对 $B$ 的身份认证。

**命题**　基于CDH问题，在收到消息 1 后，只有$B$能够计算出$\alpha=h_1(g^{bx}\| g^y \| ID_B \| ID_A)$，并且$A$接收到消息 2 后能够验证$\alpha$的完整性。对于任意一个PPT类型的攻击者，有一个可忽略的函数$\varepsilon(k)$，对于足够大的$k$，有

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

**证明**　令$Forge$表示上述事件，即给定 $1^k$, $g^y$, $ID_B$, $PK_B$，$E$ 在不知道$B$的长期秘密$b$的情况下，可以在多项式时间内成功计算出$h_1(g^{bx}\| g^y \| ID_B \| ID_A)$。令$NoSendB$表示如下事件：$A$收到的$g^y$, $Cert(B)$, $\alpha$实际上不是$B$发送的。显然$NoSendB$事件可以在多项式事件内规约到$Forge$事件，即有

$Pr[NoSendB]=Pr[Forge]$

对于 $NosendB$ 事件，有：

(1)这个$\alpha$是攻击者通过$q$次预言机查询猜测得到的，且$h_1(\cdot)$的输出长度为$l_1$，那么这个概率不超过 $q/2^{l_1}$。

(2)$g^x$是以前某个预言机查询时已经询问过的，假设以前查询了 $q'$ 次，当前查询次数为$q$次，那么$g^x$被询问的概率不超过 $q/q'$。

(3)若攻击者能够计算出$g^{bx}$，则可以计算出$h_1(g^{bx}\|g^y\| ID_B\|ID_A)$。显然，攻击者在不知道$B$的长期秘密$b$的情况下计算出$g^{bx}$是一个CDH事件，记为$Event^{\mathrm{CDH}}$。

(4)用户 $A$ 收到消息 2 后，可以计算出 $\alpha$。

因此，

$$Pr[Forge]=Pr[NoSendB]\le Pr\{Event^{\mathrm{CDH}}+q/2^{l_1}+q/q'\}$$

令 $\varepsilon(k)=Pr\{Event^{\mathrm{CDH}}+q/2^{l_1}+q/q'\}$，则命题得证。

同理，$B$ 收到消息 3 后验证 $h_2(g^{ay} \| g^x \| ID_A \| ID_B)$，即可对 $A$ 的身份进行认证。

**引理 4** SAKAP 保护了新鲜的会话密钥。

**证明**　因为协议$P$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，所以要正确计算出会话密钥 $SK=h_3(g^{bx}\| g^{ay} \| ID_A \| ID_B)$，必须获得$g^{bx}$和$g^{ay}$的值，由于用$g^x$, $g^y$, $g^b$和$g^a$求$g^{bx}\|g^{ay}$的困难性基于CDH问题，因此对$challenge$“猜测”可以在多项式时间内规约到求CDH问题，即对$challenge$“猜测”正确的优势函数$Advantage^E(k)$是可忽略的。

## 4　性能分析

本文从协议的计算开销和实现成本等方面对协议进行分析。

(下转第 178 页)