基于理想的协议安全性分析*

孙海波[1,2], 林东岱[1], 李 莉[3]

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

[2](中国科学院 研究生院,北京 100049)

[3](武汉大学 计算机学院,湖北 武汉 430072)

Protocols Security Analysis Based on Ideal

SUN Hai-Bo[1,2], LIN Dong-Dai[1], LI Li[3]

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

[2](Graduate School, The Chinese Academy of Sciences, Beijing 100049, China)

[3](School of Computer Sciences, Wuhan University, Wuhan 430072, China)

+ Corresponding author: Phn: +86-10-62528254 ext 807, E-mail: hsun@is.iscas.ac.cn, http://www.iscas.ac.cn

Received 2004-02-10; Accepted 2005-06-27

Sun HB, Lin DD, Li L. Protocols security analysis based on ideal. *Journal of Software*, 2005,16(12):2150−2156.
DOI: 13.1360/jos162150

Abstract: Guttman *et al*. introduced a new formulation method, strand spaces theory as a new method for describing and analyzing cryptographic protocols in 1998 and Guttman introduced the ideal of information algebra and honesty to analyze the secrecy of Otway-Rees protocol in 1999. Because of the property of ideal, it can be used to show the relation between different information in some protocol. In this paper, the ideal will be appied to analyze some security properties of cryptographic protocols, such as secrecy, authentication, and so on.

Key words: strand space; cryptographic protocol; ideal

摘 要: 1998 年,Guttman 等人提出了串空间理论作为一种新的密码协议形式化分析的工具.并在 1999 年第 1 次引入了关于消息代数上的理想以及诚实的概念来分析协议的保密性.由于理想结构的特殊性使得它可以刻画协议运行中消息之间的关系.利用理想的结构来分析协议的一些安全性质,例如保密性、认证性、零知识性以及如何抵抗猜测攻击.

关键词: 串空间;密码协议;理想

中图法分类号: TP309 文献标识码: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60373048, 90204016 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.863-317-01-04-99, 2003AA144030 (国家高技术研究发展计划(863)); the National Grand Fundamental Research 973 Program of China under Grant No.2004CB318004 (国家重点基础研究发展规划(973))

作者简介: 孙海波(1977－),男,辽宁盘锦人,博士生,主要研究领域为密码学,信息安全;林东岱(1964－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全,网络分布式计算;李莉(1976－),女,博士,讲师,主要研究领域为网络安全.

1998 年,串空间理论[2,3]作为一种新的协议的形式化分析工具被提出并用于一些简单协议的安全性分析当中.因为串空间理论的描述简单且其特有的图结构,使得对于一些协议的某些安全性质的描述和分析看起来非常直观,并且由于串空间理论不涉及状态转移的问题,使得传统的形式化方法固有的状态爆炸问题得以在一定程度上得到解决.到目前为止,对于串空间理论的应用局限于分析简单协议的秘密性和认证性.与其他形式化方法一样,串空间理论的一大困难在于对协议的安全目标的形式化描述.同时,由于串空间理论为了简化对协议的分析过程做了比较强的假设,这使得对于复杂协议尤其是存在概率加密算法等非确定因素的协议的描述与分析变得非常困难.因此,近来对串空间理论的研究仍然停留在对简单协议的描述与分析上.Guttman 1998 年文献[1]中提出了关于理想和诚实的概念.Guttman 以 Otway-Rees 协议为例,利用理想的性质分析了该协议的秘密性.本文主要目的在于利用理想来分析协议的其他一些安全性质,例如零知识性、认证性等.本文第 1 节给出关于串空间理论基本概念的介绍.第 2 节介绍如何利用理想和诚实分析协议的秘密性.第 3 节利用理想分析协议的认证性.第 4 节利用理想分析协议的零知识性.第 5 节简单介绍协议抵抗猜测攻击的条件.最后是全文的总结.

1 串空间理论的基本介绍

1.1 基本概念

我们首先给定两个不相交的生成元集 T 和 K,其中 T 表示原子信息集合.K 表示密钥集合.定义自由信息空间代数 A 是由这两个生成元集在加密、求逆密钥和拼接运算下生成,分别记作$\{m\}_k$,k^{-1} 和 m_1m_2.由加密和拼接生成的信息集合 E 和 C 我们称为密文集和拼接集,$T\cap K\cap E\cap C=\varnothing$.我们定义如果项 $t\in T\cup K\cup E$,则称项 t 为简单项.这里,A 就是在协议运行过程中参与者可能交换的信息集合.同时,称 A 中的元素为项.用+表示发送信息,用–表示接收信息.

串空间是一个二元组(Σ,tr),其中的Σ是一个串(strand)的集合,这里的串可以用来表示任何序列.tr 表示由Σ到 A 中元素组成的序列的一个映射,我们称其为迹映射,映射的像称为原像的迹(trace).通常,把像的代表元记为$\langle\langle\sigma_1,a_1\rangle,...,\langle\sigma_n,a_n\rangle\rangle$,其中$\sigma_i$ 代表+或–,a_i 代表 A 中的元素.下面还要定义项之间的子项关系$\subseteq$:

1) 若 $a\subseteq a$,则 $a=a$,其中 a 是原子信息.

2) 若 $a\subseteq gh$ 则 $a\subseteq g$ 或 $a\subseteq h$ 或 $a=gh$.

若 $a\subseteq\{g\}_k$,则 $a\subseteq g$ 或 $a=\{g\}_k$.

串空间理论的一些相关概念参见文献[2,3].

一些基本假设:

1) 若 $m_1,m_2\in A$ 且 $K_1,K_2\in K$,则 $\{m_1\}_{k_1}=\{m_2\}_{k_2}\Rightarrow m_1=m_2,K_1=K_2$.

2) 若 $m_1,m_2,m_3,m_4\in A,K\in K$,则 $m_1m_2=m_3m_4\Rightarrow m_1=m_3,m_2=m_4$.$m_1m_2\neq\{m_3\}_K,m_1m_2\notin K\cup T,\{m_1\}_K\notin K\cup T$.

1.2 攻击者能力描述

串空间理论建立了攻击者行为模型,对于攻击者的一些基本攻击进行了形式化的描述.攻击者能力主要由两方面因素描述:一方面是攻击者所掌握的密钥集,另一方面是攻击者由他所获得的消息产生新消息的能力.其中攻击者所掌握的密钥集由 K_p 表示,攻击者的基本行为用下面的一个攻击者的迹的集合来描述:

M. $\langle+t\rangle$,这里,$t\in T$.

F. $\langle-t\rangle$,

T. $\langle-g,+g,+g\rangle$,

C. $\langle-g,-h,+gh\rangle$,

S. $\langle-gh,+g,+h\rangle$,

K. $\langle+K\rangle$,这里 $K\in K_p$,

E. $\langle-K,-h,+\{h\}_K\rangle$,

D. $\langle-K^{-1},-\{h\}_K,+h\rangle$.

可以说,对于一个协议的攻击都可以看作是这些基本行为的组合.这些攻击者的迹给出了对于攻击者能力

的形式化描述,并保证了由攻击者发出的消息对于自由信息空间上的运算是封闭的.攻击者的行为序列称为攻击者串.如果一个节点属于一个攻击者串,就称该节点为攻击者节点,否则称为一般节点.

2 协议秘密性分析

首先给出理想与诚实的定义:

如果 $k\subseteq K$,那么 A 的一个 k 理想是 A 的一个子集,使得对于所有的 $h\in I,g\in A,K\in k$ 满足:

1) $hg,gh\in I$;

2) $\{h\}_k\in I$.

包含 h 的最小 k 理想记作 $I_k[h]$.如果 $S\subseteq A,I_k[S]=\cup_{x\in S} I_k[x]$.我们称一个集合 $I\subseteq A$ 对于 bundle C 是诚实的,当且仅当如果 I 有攻击者节点 p 作为它的入口点并且 p 是 M 节点或 K 节点.

对于协议秘密性的保证主要依赖于:

定理 **1**. 假设 C 是 A 上的一个 bundle.$S\subseteq T\cup K$,且 $K\subseteq S\cup k^{-1}$,则 $I_k[S]$对于 C 是诚实的.

证明:令 $I=I_k[S]$.因为 $I\cap K=S\cap K$,可以推出 $K\backslash I=K\backslash S\subseteq k^{-1}$.又因为 $S\subseteq T\cup K$,所以集合 S 的元素是简单的.假设 m 是一个攻击者节点且是 I 的入口点,我们考虑前面介绍过的攻击者迹的形式.很明显,不可能是 F 和 T.我们考虑其余的几种可能.

C. m 在迹为$\langle -g,-h,+gh\rangle$的串上,因为 $hg\in I$,可以推出 $g\in I$ 或 $h\in I$,这与入口点定义矛盾.

S. m 在迹为$\langle -gh,+h,+g\rangle$的串上,因为 $term(m)$的符号应该为正,因此 m 是这个串上的第 2 个或第 3 个节点.但是由 $g\in I$ 或 $h\in I$ 可以得到 $hg\in I$,与入口点的定义矛盾.

D. m 在迹为$\langle -K^{-1},-\{h\}_K,+h\rangle$的串上.由假设,$m$ 是入口点,因此 $K^{-1}\notin S$.但是因为 $K\subseteq S\cup k^{-1}$.因此 $K^{-1}\in k^{-1}$,所以 $K\in k$.由理想 I 的定义我们知道$\{h\}_K\in I$,与入口点的定义矛盾.

E. m 在迹为$\langle -K,-h,+\{h\}_K\rangle$的串上,由假设$+\{h\}_K\in I$,可以得出 $h\in I$,与入口点的定义矛盾.

由此可以看出,在假设条件下,m 只可能是 M 节点或 K 节点,即理想 $I_k[S]$是诚实的.

在分析协议保密性的过程中,S 是包含协议运行过程中需要保密的信息.而 k 中包含的是密钥空间中除去攻击者无法得到的密钥的集合,也就是攻击者可能知道的密钥.这样,$I_k[S]$就是所有需要保密的消息用攻击者可能知道的密钥处理后的消息的集合.M 节点或 K 节点实际上是说攻击者不能由得到的消息推导出的信息.这样,如果 $I_k[S]$是诚实的,就保证了 S 中的消息攻击者不能够由推导得到.

下面补充证明为什么只要证明 $I_k[S]$是诚实的就足够了.因为 S 中包含的是需要保密的消息.证明协议保密性等价于证明 $I_K[S]$是诚实的.现在已知 $I_k[S]$是诚实的,我们用反证法证明 $I_K[S]$也是诚实的.假设 $I_K[S]$不是诚实的,由诚实的定义,我们知道存在节点 t 为 $I_k[S]$的入口点且不为类型 M,K.有两种情况:第 1 种情况,$term(t)\in I_k[S]$,则 t 是 $I_k[S]$的入口点,这与假设 $I_k[S]$是诚实的矛盾;第 2 种情况,$term(t)\notin I_k[S]$,这时我们分析其余的攻击者迹的情况,显然 F,T,C,S 是不可能的.

E. $\langle -K,-h,+\{h\}_K\rangle$若 $K\in I_K[S]$则与入口点定义矛盾.若 $K\in K$ 且 $K\notin I_K[S]$则 $h\in I_k[S]$与入口点定义矛盾.

D. $\langle -K^{-1},-\{h\}_K,+h\rangle$同理,与入口点定义矛盾.

由 $I_k[S]$是诚实的可以推出 $I_K[S]$是诚实的.在具体的协议分析当中,按照要求适当选取 S 和 k,如果定理的条件能够满足则协议的秘密性就可以得到保证.对于 Otway-Rees 协议的秘密性分析参见文献[1]. □

3 协议认证性分析

由上一节可以看出,理想对于描述某些具有特定性质的消息的集合是非常有效的.例如,在保密性的分析中,理想被用来描述由秘密信息生成的消息集合.该集合是封闭的且攻击者无法有效地进入该集合.本节我们同样基于理想来描述协议的认证性.

首先对于一个以实现身份认证为目的的协议来说,无论是单向认证还是双向认证,认证的方式都是由认证者产生一个特定的可以代表身份的消息,使得验证者可以有效的验证消息的产生者的身份.常用的方法包括:数

字签名,消息认证码,加密等方式.我们称这个特殊的用以认证的消息项为认证项.记为 Auth_term.例如,NSL 协议

$A\rightarrow B$: $\{N_aA\}_{Ka}$;

$B\rightarrow A$: $\{N_aN_bB\}_{Kb}$;

$A\rightarrow B$: $\{N_b\}_{Ka}$

中使用的是公钥密码体制的双向身份认证.这里,消息$\{N_aN_bB\}_{Kb}$和$\{N_b\}_{Ka}$作为认证项.而第 1 项$\{N_aA\}_{Ka}$不能作为认证项,因为任何一个攻击者都可以产生一个这种格式的消息.NSL 协议认证的实现是依赖于随机数的唯一产生和安全传输.同样地,在三方认证协议中身份的认证是由可信第三方也就是服务器来实现的.这样我们可以看到,对于任意一个以身份认证为目的的协议,总可以找到具体的认证项 Auth_term.

我们补充定义一种攻击者迹:

$F.\langle -x_1,-x_2,\ldots,-x_n,+f(x_1,\ldots,x_n)\rangle$.

这里描述了攻击者的计算能力,也包括了当 $n=1,x_1=f(x_1),f(x_1)=x_1$ 时,攻击者逆向求解一个非单向函数的能力.

下面我们定义消息间的推导关系~.

我们称 $M\sim N$ 当且仅当 $M\in A,N\in simple$ 且 N 可以由 M 通过 T,C,S,E,D,F 的操作得出或 $M=N$.例如,当$M=\{\{h\}_K,K\}$时,$N=h,K$.也就是说,N 是可以通过消息 M 由我们所刻画的攻击者的计算能力推导出来的.这刻画了攻击者由协议得到的消息中提取有用信息的能力.

很明显,我们可以得到这样一个结论:如果协议能够实现认证目的,那么对于认证项中的所有简单的子项,攻击者不可能由推导关系全部得到.换句话说,如果协议的认证性可以满足,那么攻击者不可能通过截获的消息和他所具有的推导能力构造有效的认证项.例如,就在上述例子 NSL 协议中的认证项$\{N_aN_bB\}_{Kb}$来说,以我们给定的能力,攻击者不可能由该项推导出其中的子项 N_a 和 N_b,因此他无法构造出这种形式的认证项来冒充 B.

下面我们以理想的形式给出协议实现认证性的条件.

假设协议中传递的所有消息的集合为 M.其中认证项组成的集合为 M_{Auth},攻击者所掌握的消息定义为 M_p.集合 $N=\{n|m\sim n,m\in M\}$表示攻击者由协议传输的消息中可以推导出的简单消息的集合.对于 N 中的元素 n,如果 $n\in K$,则 $K_p=K_p\cup n$.否则,$M_p=M_p\cup n$,即将攻击者得到的消息分别加入到他已经掌握的密钥或消息集中.构造理想 $I_{Kp}[M_p]$的方法见上节.

现在给出认证性满足的条件:

定理 **2**. 假设相关的概念如上所述,理想的构造如第 1 节的定义,那么协议认证性实现的充要条件为 $I_{Kp}[M_p]\cap M_{Auth}=\varnothing$.

证明:必要条件是显然的,如果 $I_{Kp}[M_p]\cap M_{Auth}=\varnothing$,意味着攻击者无法构造认证项,那么认证项的产生可以唯一地确定即协议的认证目的已经达到.现在我们假设协议已经实现认证.假设 $I_{Kp}[M_p]\cap M_{Auth}\neq\varnothing$,那么存在 $n\in I_{Kp}[M_p]\cap M_{Auth}$.因为 $n\in I_{Kp}[M_p]$,所以 n 是由攻击者构造的,那么由攻击者能力的描述可以得出对于任意的 n 的简单子项 $t,t\in M_p$.而 $n\in M_{Auth}$,由上面的结论攻击者不可能得到所有简单的子项,这就推出了矛盾.因此 $I_{Kp}[M_p]\cap M_{Auth}=\varnothing$. □

例如在 Otway-Rees 协议中,$MAB\in M_p,N_a,N_b\notin M_p,K_{AS}.,K_{BS}\notin K_p$ 且攻击者无法通过他的推导得到 N_a,N_b,K_{AS},K_{BS},因此攻击者无法构造认证项 $MAB\{N_aMAB\}_{KAS}\{N_bMAB\}_{KBS}$.即 $I_{Kp}[M_p]\cap M_{Auth}=\varnothing$,从而协议的认证性得到保证.注:攻击者不能把由一个协议中被动得到的认证项原封不动地用于其他协议或该协议的其他运行,就是重放攻击.目前一般的认证协议中都包括会话标识符或随机数来抵抗重放攻击,因此不讨论这种情况.

4 协议零知识性[4]分析

目前,有一些协议被设计成使得某个协议的参与者可以向其他人证明他掌握了某种秘密信息,同时并不泄漏修改秘密的任何信息给验证者.这样的协议称为零知识协议[5].本节主要讨论如何描述协议的零知识性.零知识协议主要考虑的是证明者与验证者之间的消息关系.假设协议参与双方中一个是证明者,一个是验证者.这里

定义验证者掌握的消息集合为 M_V,所掌握的密钥集合为 K_V.理想的生成同前所述.这样验证者掌握的所有消息就是 $I_{KV}[M_V]$.记验证者在协议运行前所掌握的消息为 $I^0_{KV}[M_V]$,在协议运行之后验证者通过协议的运行可能获取一些新的信息.与上一节相似,我们把这些新获取的消息分别加入 M_V 和 K_V,从而生成一个新的理想 $I^1_{KV}[M_V]$.记证明者掌握的知识为 I_P.为了描述协议的零知识性,还需要引进一种新的函数[6]:

$$F:A^n\to A,$$

使得对于每一个 $y=f(x_1,\ldots,m,\ldots,x_n)$,$m$ 不能由 y 计算得出,$x_1,\ldots,x_n$ 与 m 是完全独立的并且如果想要计算 y,必须已经掌握 m.换句话说,只有掌握 m 可以有效地计算 y.如果其中某一个 x_i 是由验证者提供的,那么要求由 $f(x_1,\ldots,m,\ldots,x_n)$计算 x_i 也是计算上不可行的,称这样的函数为零知识函数.

在这个定义中,m 是证明者想要向验证者证明的秘密.这意味着证明者通过零知识函数将秘密信息 m 隐藏在 y 中.验证者通过验证 y 的有效性来确信证明者掌握 m.但是任何人都可以对 m 进行猜测来构造 y,从而声称他自己是证明者.或者如果当零知识函数需要验证者提供参数进行计算时,验证者可以通过猜测构造该参数使得他可以由计算得出的函数值中获取关于 m 的信息.通常这种猜测的概率是一个固定值 k,克服这种问题的方法是将协议运行 n 次,根据安全需要确定 n 的大小,使得猜测的成功率可以忽略.

由以上的定义,我们可以给出协议实现零知识性的条件:

定理 **3**. 假设 C 是 A 上的一个 bundle.m 是证明者想要向验证者证明的秘密.($m\notin I_1(verifier)$).$y=f(x_1,\ldots,m,\ldots,x_n)$是一个关于 m 的零知识函数,且在每一轮的协议运行当中,参数的选取都是随机且独立的.在除零知识函数之外传输的任何消息都与 m 无关,则协议实现零知识性的充要条件是 $I^0_{KV}[M_V]=I^1_{KV}[M_V]$,并且验证者接受 $m\in I_P$ 的概率为 $1-k^n$.

证明:若 $I^0_{KV}[M_V]=I^1_{KV}[M_V]$并且验证者接受 $m\in I_P$ 的概率为 $1-k^n$,意味着验证者以接近 1 的概率相信证明者掌握了消息 m 并且在协议运行过程中验证者掌握的消息集合没有扩大.这就符合了我们关于零知识性的定义.假设协议实现了零知识性,如果 $I^0_{KV}[M_V]\neq I^1_{KV}[M_V]$.由前提假设,在除零知识函数之外传输的任何消息都与 m 无关.那么攻击者掌握的消息集合的扩大来源于零知识函数的传输.但是由零知识函数的定义,$y=f(x_1,\ldots,m,\ldots,x_n)$攻击者不能反向推导出有关自变量的任何消息,即 M_V 和 K_V 都没有变化,因此 $I^0_{KV}[M_V]=I^1_{KV}[M_V]$.矛盾.又由已知关于零知识函数的参数在协议运行每一轮中的选取都是独立并随机的,假设每一次猜测成功的概率为 k,那么运行 n 轮后验证者接受 $m\in I_P$ 的概率为 $1-k^n$.

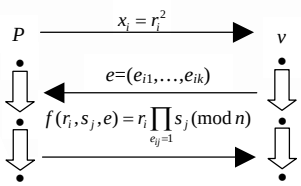

Fig.1
图 1

如图 1 所示,在此协议中首先选取 $n=pq$,然后证明者选择 k 个不同的 j 的值使得 v_j 是(mod n)的二次剩余.证明者计算 $s_j=v_j^{1/2}(\text{mod } n)$作为秘密信息.在向验证者证明的过程中首先告诉验证者 v_j 然后运行该协议.运行协议后,验证者计算 $x_i=f^2(r_i,s_j,e)\Pi v_j(\text{mod } n)$来确定 $f(r_i,s_j,e)$的有效性.这里,$f(r_i,s_j,e)$满足我们的定义是一个零知识函数.因为 e 是验证者提供的.由 $f(r_i,s_j,e)$计算 e 等价于猜测一个 k 比特二进制串.很显然,每一轮协议运行中参数的选取都是随机和独立的,因此验证者将以 $1-k^n$ 接受 $s_j\in I_P$.这样,协议的零知识性就得到了满足.Fiat-Shamir 协议[6,7]也是很好的例子. □

5 协议对于抵抗猜测攻击的分析

我们知道,在实际的通信环境中,攻击者是具有一定猜测能力的.例如,用户的口令通常比较短,这就使得猜测成为可能[7,8].对于公钥体制中的私钥或者常用的对称密钥来说,猜测是不现实的,因为通常这样的密钥作为长期密钥来说都是很长的,猜测的概率基本上可以忽略.这里主要考虑不可检测的在线猜测.

定义攻击者能够猜测的消息集合为 M,例如某些口令,当攻击者进行了某项猜测 m 之后,我们将 m 放入集合 M_P 或 K_P 中.之后,对于协议 P 中传输的消息集合 M_P 中的每一个消息,应用第 3 节中定义的推导关系~,得到一个攻击者可推导出的简单消息的集合 $N=\{n|m\sim n,m\in M\}$.这时,我们构造一个理想 $I_{KP}[N\cup M_P]$.注意,在构造这样的理想的时候,已经把猜测的消息 m 加了进去,并要求每次构造理想,攻击者只能够在猜测一次的基础上进行消息的构造.因为猜测两次以上成功的概率非常小,而且攻击者很难确定猜测的结果正确与否.同时,我们还定义一个

集合 F_P 表示通过攻击者构造的消息使得协议其他参与者产生的包含 M 中元素的消息集合.构成理想和集合之后,有以下结论:

命题 **1**. 假设协议中不应当被攻击者获取的消息的集合为 N_P(例如,有保密性要求的信息或认证协议中认证项中的某些子项等),协议中包含这些消息作为子项的消息项的集合为 T,其他的约定如上,那么协议能够抵抗猜测攻击的条件是$\{I_{KP}[N\cup M_P]\cup F_P\}\cap T=\varnothing$.

直观上看,这个条件就是要求攻击者通过猜测所能构造的项以及通过这种构造使其他参与方产生的项与协议中包含特殊信息的项不同,换句话说,攻击者不能够通过猜测得到某些他不应该得到的东西.下面用两个例子来说明这一点.先给出一个不能抵抗猜测攻击的例子:

$A\rightarrow B$:$P_A(g^{NA}\oplus B)$;

$B\rightarrow S$:$P_A(g^{NA}\oplus B),P_B(g^{NB}\oplus A)$;

$S\rightarrow B$:$(g^{NA})^{NS},(g^{NB})^{NS}$;

$B\rightarrow A$:$(g^{NB})^{NS},C_{BA}$;

$A\rightarrow B$:C_{AB}.

在这个协议中,攻击者 B 可以通过猜测口令 P_A 构造在第 2 步中产生的消息并在第 3 步收到的消息中知道他是否猜测正确,具体的攻击过程见文献[9,10].这个协议问题在于口令是可猜测的,并且通过猜测之后攻击者可以得到 g^{NA} 并构造和正常协议中的消息相同的 $P_A(g^{NA}\oplus B)$,而实际上,$P_A(g^{NA}\oplus B)\in M$,所以该协议不能抵抗猜测攻击.

下面我们再描述一个可以抵抗猜测攻击的例子:

$A\rightarrow B$: $ys(g^{NA},P_A)$;

$B\rightarrow S$: $ys(g^{NA},P_A),ys(g^{NB},P_B)$;

$S\rightarrow B$: R_A,a,R_B,b;

$B\rightarrow A$: R_A,a,C_{BA};

$A\rightarrow B$: C_{AB}.

协议的具体描述参见文献[9].这里,与上面的例子很明显不同的是,引入了服务器的公钥 ys.按照我们的约定,私钥是不能进行猜测的,因此攻击者要构造类似的信息必须同时猜测随机数 N_A 和口令 P_A.而由约定,攻击者不能同时猜测两个以上的信息,因此该协议可以抵抗猜测攻击.

6 结束语

本文主要应用了理想的特殊性质对协议的一些安全性质,如保密性、认证性、零知识性以及如何抵抗猜测攻击,进行了形式化的描述.

Michael[11]探讨了使用BAN逻辑分析零知识验证协议,提出一种使用交互式零知识证明的身份鉴别和数字签名协议,其中使用了定理证明的方法进行了安全性分析.相比这两种方法,理想对于刻画消息集合的封闭性有着很好的性质,使得这种描述和分析变得直观也使得对这些性质的形式化分析变得更容易.

当然,我们的讨论还不完善,例如,对于零知识性的刻画仅仅在于对交互式零知识证明的描述,对于非交互式零知识证明的情况还有待于进一步的研究.

致谢 我们向对本文的工作给予支持和建议的同行,尤其是由信息安全国家重点实验室薛锐副研究员领导的讨论班上的同学和老师表示感谢.

References:

[1] Fábrega FJT, Herzog JC, Guttman JD. Honest ideals on strand spaces. In: Proc. of the 11th IEEE Computer Security Foundations Workshop. IEEE Computer Sociery Press, 1998.

[2] Fábrega FJT, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct? In: Proc. of the 1998 IEEE Symp. on Security and Privacy. IEEE Computer Press, 1998. 160−171.

[3] Fábrega FJT, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999.

[4] Feige U, Fiat A, Shamir A. Zero knowledge proofs of identity. In: Proc. of the 19th ACM Symp. Theory of Computing. 1987. 210−217.

[5] Sun HB, Lin DD, Xue R. Application of strand space theory in zero-knowledge protocols. In: Proc. of the 10th Joint Int'l Computer Conf. 2004. 435−437.

[6] Maneki AP. Honest functions and their application to the analysis of cryptographic protocols. In: Proc. of the Computer Security Foundations Workshop VI., IEEE Computer Society Press, 1993. 147−158.

[7] Desmedt Y, Goutier C, Bengio S. Special uses and abuses of the fiat-Shamir passport protocol. In: Pomerance C, ed. Advances in Cryptology-CRYPTO'87. LNCS 293, 1988. 21−39.

[8] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Proc. of the CRYPTO'86. LNCS 263, 1987. 186−194.

[9] Bellovin SM, Merritt M. Encrypted key exchange: Password-Based protocols secure against dictionary attacks. In: Proc. of the 1992 IEEE Computer Society Conf. on Research in Security and Privacy. 1992. 72−84.

[10] Jablon DP. Strong password-only authenticated key exchange. Computer Communications Review, 1993,11(5):648−656.

[11] Marrotte MT. BAN logic for zero-knowledge identification protocols. http://citeseer.ist.psu.edu/halpern88knowledgebased.html

《软件学报》软件体系结构专刊
征 文 通 知

专刊题目：软件体系结构

特约编辑：梅宏（北京大学）、吕建（南京大学）

一、征文范围

1. 软件体系结构的基本理论、方法和技术，如软件体系结构描述语言、软件体系结构形式化方法、软件体系结构模型、动态体系结构、软件体系结构风格等。

2. 基于软件体系结构的软件开发，如模型驱动体系结构、软件体系结构分析和评估方法、软件体系结构与服务质量关系、体系结构发现与恢复、基于体系结构的演化技术、体系结构转换、从需求到软件体系结构到系统实现的可追踪性问题等。

3. 软件体系结构与其他软件工程领域的交叉研究，如产品线体系结构、系统体系结构和软件体系结构的关系、领域特定的体系结构和参考体系结构、软件体系结构与面向对象技术、基于构件的软件开发、面向服务的体系结构等。

4. 软件体系结构与软件产业，如实例研究、工业界的最佳实践、软件架构师的角色和责任、互操作性和集成、软件架构师的教育、培训和认证、文化、经济和管理问题，软件体系结构对于提高中国软件产业生产力的作用等。

上述各项仅属举例性的，也非优选题目。论文内容并不仅限于此，所有与软件体系结构相关的内容均可投稿。

二、投稿要求

1. 投稿方式：采用“软件学报在线投稿系统”(http://www.jos.org.cn)投稿。请在投稿时，在备注栏中注明“软件体系结构专刊投稿”字样。

2. 稿件格式：参照《软件学报》论文格式 (学报网站上提供了论文模版，可下载)。

3. 投稿文章未在正式出版物上发表过，也不在其他刊物或会议的审稿过程中，不存在一稿多投现象；保证投稿文章的合法性(无抄袭、剽窃、侵权等不良行为)。

4. 其他投稿须知请参阅《软件学报》投稿指南 http://www.jos.org.cn/directory.htm

5. 投稿作者需提交投稿声明；专刊投稿文章不收审理费。录用刊发文章将收取软件学报标准版面费。发表之后，将按软件学报标准支付稿酬，并赠送样刊及单行本。

三、重要时间

截稿日期：2006 年 1 月 10 日

录用通知发出时间：2006 年 3 月 10 日

录用修改稿提交日期：2006 年 4 月 10 日

出版日期：2006 年第 6 期