ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*, Vol.20, No.10, October 2009, pp.2799−2809
doi: 10.3724/SP.J.1001.2009.03310

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

# 突破认证测试方法的局限性*

刘家芬+, 周明天

(电子科技大学 计算机科学与工程学院,四川 成都 610054)

## Overcome the Limitation on Authentication Test

LIU Jia-Fen+, ZHOU Ming-Tian

(College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)

+ Corresponding author: E-mail: ljfwhy@gmail.com

**Liu JF, Zhou MT. Overcome the limitation on authentication test. *Journal of Software*, 2009,20(10): 2799−2809.** http://www.jos.org.cn/1000-9825/3310.htm

**Abstract**: Authentication test is a newly presented method that testifies protocols' authentication properties. Its proving process is simple and precise; unfortunately it can not analyze protocols with test components multi-encrypted. This paper analyzes the authentication test scheme improved by Perrig and Song and points out its deficiency. Then it proposes an Enhanced Authentication Test theory and proves its soundness in formal. The enhanced authentication test lifts the restriction that test component can not be multi-encrypted in protocol messages, also repairs the inaccuracies in Perrig's scheme.

**Key words**: security protocol; formal analysis method; strand space; authentication test

**摘 要**: 认证测试是一种用于证明安全协议认证属性的新方法,该方法能够简化协议认证属性的证明过程,但其局限性是无法应用于认证测试元素被多重加密的情况.指出 Perrig 和 Song 提出的认证测试改进方案在多个方面所存在的问题.在此基础上提出新的改进方案,并进行了形式化证明.新的认证测试定理突破了认证测试元素在整个协议消息中不能被加密的限制,扩展了认证测试理论的应用范围.

**关键词**: 安全协议;形式化方法;串空间;认证测试

**中图法分类号**: TP309 **文献标识码**: A

安全协议用来具体实现安全共享网络资源的需求,因此,安全协议的安全性是网络安全的重要因素之一.但是人们精心设计,并得到广泛应用的多个安全协议被证实并不如预期的那样安全,例如 Needham-Schroeder 公钥协议在使用多年后才被证实为有缺陷的[1].人们在安全协议的设计和分析上投入了大量的精力,形成了为数众多的研究方法和理论.由 Thayer,Herzog 和 Guttman 在 1998 年提出的串空间[2−4]方法综合了 NRL 分析器、Schneider 秩函数以及 Paulson 归纳法的思想,是一种有效的协议形式化分析方法.认证测试方法[5,6]则是基于串空间理论提出来的一种用于证明安全协议认证属性的新方法.认证测试方法能够大为简化协议的认证属性的证明过程,但是"该方法不能处理测试元素多重加密的情况"[5].

* Supported by the National High-Tech Research and Development Plan of China under Grant No.863-104-03-01 (国家高技术研究发展计划(863)); the National Key Technology R&D Program of China under Grant No.2006DAH02A04 (国家科技支撑计划)

Received 2007-05-20; Revised 2007-10-09; Accepted 2008-03-12

本文着重于认证测试局限性的分析研究,并提出一种新的认证测试改进方案,使其能够分析特定环境下测试元素多重加密的情况.第 1 节给出本文的研究背景和国内外研究现状.第 2 节简单介绍文中需要用到的认证测试理论的定义和基本定理.第 3 节首先对 Perrig 和 Song 提出的认证测试改进方案进行分析,通过实例指出其缺陷,以及证明过程出现中的纰漏.在此基础上提出一种新的认证测试局限性改进方案,进行理论证明,并通过具体的协议实例验证新认证测试定理在应用范围上的突破.最后总结本文在前人基础上所做的工作,并指出今后的研究方向.

## 1 研究背景

认证测试方法是由 Guttman 和 Thayer 在 2001 年提出来的用于证明协议认证属性的新方法.认证测试方法以挑战-应答机制为基础,其基本思想是:如果协议丛中包含某个认证测试实例,则可以证明该丛中还包含特定的常规结点.该方法较串空间经典理论中构造集合、寻找集合 M-minimal 元素进行证明的方法更为直观、简练,更易于使用.

认证测试方法的提出引起了广泛关注,许多研究人员纷纷提出自己的应用或者改进方案,形成了以下 3 类成果.其一就是应用认证测试方法分析各种协议,证明协议的认证安全性或找出协议在认证属性上存在的问题并加以改进.人们使用认证测试方法分析了 Needham-Schroder 协议、Otway-Rees 协议、Neuman-Stubblebine 协议和 X.509 等常规协议,还成功地找出了 Yang-Shieh 智能卡认证协议[7]、3G 网络中 EAP-AKA 协议[8]等新的特殊用途协议的认证正确性问题.其二是将认证测试方法作为协议设计的辅助手段,Guttman 于 2002 年在文献[9]中首次将认证测试定理用于安全协议的辅助设计,为认证测试定理的应用开辟了一个新的空间.国内也有很多研究人员借鉴这一思路,使用认证测试定理设计出了一种双向认证的密钥协商协议 KNP[10]和新的 Internet 密钥交换协议 ESIKE[11].其三就是对认证测试理论本身进行的研究与扩展.文献[12]提出了增强认证测试和相关函数的概念,对认证测试证明为不安全的协议提供了更为详细的失败原因,能够辅助协议设计人员对协议存在的缺陷进行修正.文献[13]认为,可以将主动测试定理的结论由“存在常规正结点以 $t$ 为组成元素”扩展为“存在常规正结点使得 $t$ 在该结点中首次出现”,但没有给出形式化证明.文献[14]通过实例分析了在认证测试元素多重加密的情况下认证测试方法失效的原因,指出在特定情况下,即使认证测试元素被多重加密,认证测试方法依然有效;由此提出:可以对认证测试定理进行改进从而扩大其适用范围,并对输入测试定理的改进进行了尝试,但文献[14]中没有给出具体的改进方案.

本文在文献[14]发现认证测试存在问题的基础上,研究了 Perrig 和 Song 提出的改进方案并指出其缺陷,然后提出自己的认证测试局限性改进方案,通过形式化证明和协议实例分析,从两方面验证了新的认证测试不仅突破了原认证测试定理“协议中测试元素不能嵌套加密”的限制,也有效避免了 Perrig 认证测试定理证明中出现的错误,能够更加准确地描述协议满足认证属性所需的条件.

## 2 认证测试

### 2.1 表示方法

文中所用标识意义如下:

$A,B$ 表示主体;

$KA$ 表示 $A$ 的公钥;

$KA^{-1}$ 表示 $A$ 的私钥;

$KAB$ 表示 $A$ 和 $B$ 之间的共享密钥;

$N_A,N_B$ 分别表示 $A$ 和 $B$ 产生的随机数;

$\{M\}_{KA}$ 表示消息 $M$ 用 $A$ 的公钥 $KA$ 加密形成的消息;

$\{M\}_{KA^{-1}}$ 表示消息 $M$ 用 $A$ 的私钥 $KA^{-1}$ 加密形成的消息;

$P$ 表示攻击者所有可能获知的消息的集合,并假设任何主体的公钥都可以通过 PKI 机制安全、可靠地公开获得.

### 2.2 概念和定理

下面给出本文中用到的基本概念和定理,定理的具体证明请参见文献[5,6].

**定义 1**. 子项关系⊂(subterm)递归定义如下:(1) 原子项 $a$ 为自身的子项,$a\subset a$;(2) $a\subset\{h\}_K$ 当且仅当 $a\subset h$;(3) $a\subset gh$ 当且仅当 $a\subset g$ 或 $a\subset h$.如果 $a\subset h$ 但 $a\neq h$,则称 $a$ 为 $h$ 的真子项(proper subterm).

**定义 2**. 若项 $t_0$ 不能分解成连接项 $gh$ 的形式,则称 $t_0$ 为简单项(simple term).如果简单项 $t_0\subset t$,并且所有满足 $t_1\neq t_0$ 且 $t_0\subset t_1\subset t$ 的 $t_1$ 均为连接项,则称 $t_0$ 是 $t$ 的组成元素(test component),下文中也简称为元素.

**定义 3**. $n=\langle s,i\rangle$,项 $t$ 是 $term(n)$的组成元素,如果对于 $j<i$ 的所有结点$\langle s,j\rangle$,$t$ 不是$\langle s,j\rangle$的组成元素,则称 $t$ 是结点 $n$ 上的新元素.

**定义 4**. $t=\{h\}_K$,如果:(1) $a\subset t$ 并且 $t$ 是 $n$ 的组成元素;(2) 消息项 $t$ 不是任何常规结点 $n'\in\Sigma$的消息组成元素的真子项,则称为 $a$ 在 $n$ 中的测试元素(test component).

**定义 5**. 在边 $n\Rightarrow^+n'$中,如果 $n$ 为正,$n'$为负,项 $a\subset term(n)$,结点 $n'$中包含新元素 $t'$,并且 $a\subset t'$,则称 $n\Rightarrow^+n'$为变换边(transformed edge).

**定义 6**. 在边 $n\Rightarrow^+n'$中,如果 $n$ 为负,$n'$为正,项 $a\subset term(n)$,结点 $n'$中包含新元素 $t'$,并且 $a\subset t'$,则称 $n\Rightarrow^+n'$为变换进行边(transforming edge).

**定义 7**. 如果结点 $n=\langle s,i\rangle$为正并且 $t\subset term(n)$,但对于任何 $j<i$,$t\not\subset term(\langle s,j\rangle)$,则称项 $t$ 源发于结点 $n$.

**定义 8**. 如果项 $t$ 在串空间$\Sigma$中有且仅有一个源发结点 $n$,则称 $t$ 唯一源发于 $n$.

**定义 9**. 如果 $a$ 唯一源发于 $n$ 并且 $n\Rightarrow^+n'$为 $a$ 的变换边,则称 $n\Rightarrow^+n'$为 $a$ 的测试边.

**定义 10**. 如果边 $n\Rightarrow^+n'$是 $a$ 的测试边,$t=\{h\}_K$ 为 $a$ 在 $n$ 中的测试元素,$K^{-1}\notin P$,并且 $a$ 不出现在 $n$ 除 $t$ 以外的其他元素中,则边 $n\Rightarrow^+n'$构成输出测试(outgoing test).

**定义 11**. 如果边 $n\Rightarrow^+n'$是 $a$ 的测试边,$t'=\{h\}_K$ 为 $a$ 在 $n'$中的测试元素,$K\notin P$,则边 $n\Rightarrow^+n'$构成输入测试(incoming test).

**定理 12**. 如果 $t=\{h\}_K$ 是 $a$ 在负结点 $n$ 中的测试元素,并且 $K\notin P$,则结点 $n$ 构成主动测试(unsolicited test).

**定理 1(输出测试定理)**. 从 $C$ 中 $n'\in C$,构成 $a$ 的输出测试,以 $t$ 为测试元素,则有(1) 存在常规结点 $m,m'\in C$ 使得 $t$ 是 $m$ 的元素并且 $m\Rightarrow^+m'$是 $a$ 的变换进行边.(2) 假设 $a$ 仅出现在 $m'$的元素 $t_1=\{h_1\}_{K_1}$ 中,并且 $t_1$ 不是任何常规结点消息的组成元素的真子项,$k_1^{-1}\notin P$,则 $C$ 中存在负的常规结点 $m''$,$t_1$ 为该结点的元素.

**定理 2(输入测试定理)**. 从 $C$ 中 $n'\in C$,$n\Rightarrow^+n'$构成 $a$ 的输入测试,以 $t'$为测试元素,则存在常规结点 $m,m'\in C$ 使得 $t'$是 $m'$的元素并且 $m\Rightarrow^+m'$是 $a$ 的变换进行边.

**定理 3(主动测试定理)**. 从 $C$ 中,负结点 $n\in C$,并且 $n$ 构成 $t=\{h\}_K$ 的主动测试,则从 $C$ 中存在一个正常规结点 $m\in C$,$t$ 是 $m$ 的元素.

## 3 认证测试局限性研究

### 3.1 认证测试元素嵌套加密的限制

认证测试的局限性在测试元素的定义中就有所体现,“测试元素不能是任何常规结点消息的组成元素的真子项”,也就是说,协议消息中测试元素不能被再次加密.文献[14]中通过两个例子说明了认证测试定理中对测试元素嵌套加密进行限制的原因.

例 1:假设从 $C$ 中存在如下消息序列,其中 $a$ 唯一源发于$\langle s,1\rangle$,$KA^{-1}\notin P$.如图 1 所示.

例 1 中根据定理 2,从 $C$ 中应存在一个常规串来完成从消息 $\{\{M\}_{KA^{-1}}\}_{KB^{-1}}$ 到 $\{M\}_{KA^{-1}}$ 之间的形式变换.但事实上,这个变换完全可以由攻击者串来完成.

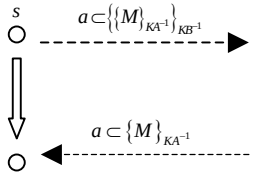



Fig.1 Multi-Encryption of test component in incoming test

图 1 输入测试元素嵌套加密的情况

例 2:假如从 $C$ 中存在如下消息序列,其中 $a$ 唯一源发于$\langle s,1\rangle$,并且 $a$ 不出现在$\langle s,1\rangle$除$\{M\}_{KA}$以外的其他子项中,$KA^{-1}\notin P$ 且 $KB^{-1}\notin P$.如图 2 所示.

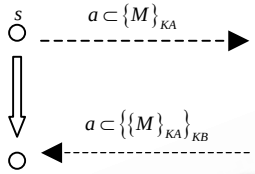



Fig.2 Multi-Encryption of test component in outgoing test

图 2 输出测试元素嵌套加密的情况

根据定理 1,从 $C$ 中应存在一个常规串来完成从消息$\{M\}_{KA}$到$\{\{M\}_{KA}\}_{KB}$之间的形式变换.但实际上,这个变换完全可以由攻击者串来完成.

### 3.2 Perrig和Song对认证测试的改进

Perrig 和 Song 在文献[15]中提到认证测试方法可用于有效地删减 Athena[16,17]运行时的状态空间,但是"认证测试方法不允许特定项被加密".为了解决这一问题,他们对认证测试的概念和相关定理进行了修改,并试图通过理论证明来确认这一改进.

#### 3.2.1 Perrig 和 Song 的改进方案

**定义 13**. 如果 $a$ 为原子消息,$m=\{t\}_K$,$a$ 是 $t$ 的组成元素,则 $a$ 和 $m$ 之间满足关系 $a\sqsubset_K m$.

**定理 4(Perrig 输入测试定理)**. 从 $C$ 中,$n\Rightarrow^+n'$,如果 $a$ 唯一源发于 $n$,并且与 $term(n')$的子项 $t_1\subset term(n')$满足关系 $a\sqsubset_K t_1$,$t_1\not\subset term(n)$,则 $C$ 中必然存在 $a$ 的变换进行边 $m\Rightarrow^+m'$,$t_1$ 为测试元素,并有 $t_1\subset term(m')$,$t_1\not\subset term(m)$,$a\subset term(m)$.另外,如果 $K\notin P$,则该变换进行边一定位于常规串上.

文献[15]的附录 C 使用传统串空间理论中构造特定集合,寻找最小元素的方法,给出了 Perrig 输入测试定理和输出测试定理的证明概要.具体证明如下:

证明:令从 $C$ 中所有包含 $t_1$ 的结点构成集合 $\Psi$,即集合 $\Psi$ 中的任意元素 $n_i$ 满足 $t_1\subset term(n_i)$.由于 $n'\in\Psi$,因此,$\Psi$ 非空.从 $C$ 中结点的任何非空子集均存在 $\leq_C$-minimal 元素,因此,集合 $\Psi$ 存在 $\leq_C$ 上的最小元素,记为 $n_0$.由于 $n\notin\Psi$,$n\neq n_0$.

由于 $a$ 唯一源发于 $n$,故 $C$ 中一定存在边 $n_0'\Rightarrow^+n_0$ 并且 $a\subset n_0'$.由于 $n_0$ 为 $\Psi$ 中的 $\leq_C$-minimal 元素,故 $n_0'\notin\Psi$,则有 $t_1\not\subset n_0'$.根据变换进行边的定义,$n_0'\Rightarrow^+n_0$ 即为 $a$ 的变换进行边.如果 $K\notin P$,并假设 $n_0'\Rightarrow^+n_0$ 不在常规串上,则 $n_0'\Rightarrow^+n_0$ 只能位于 $D$-或者 $E$-串上.若 $n_0'\Rightarrow^+n_0$ 位于 $D$-串,则 $n_0'$ 形为$\{h\}_{K'}$,于是有 $t_1\subset h$ 与 $t_1\subset n_0'$ 相矛盾.因此 $n_0'\Rightarrow^+n_0$ 不可能位于 $D$-串上.若 $n_0'\Rightarrow^+n_0$ 位于 $E$-串,$n_0$ 应形为$\{h'\}_{K''}$,其中 $K''\neq K$,因此有 $t_1\subset h'$,与 $t_1\not\subset n_0$ 相矛盾,故 $n_0'\Rightarrow^+n_0$ 不可能在 $E$-串上.

故在 $K\notin P$ 的情况下,$n_0'\Rightarrow^+n_0$ 只可能位于常规串上. □

**定理 5(Perrig 输出测试定理)**. 从 $C$ 中,$n\Rightarrow^+n'$,如果 $a$ 唯一源发于 $n$,并且 $a$ 仅出现在 $term(n)$的子项 $t_1\subset term(n)$中,并且 $a\sqsubset_K t_1$.$a\subset term(n')$但 $t_1\not\subset term(n')$,则 $C$ 中必然存在 $a$ 的变换进行边 $m\Rightarrow^+m'$,$t_1$ 为测试元素.并且

$m'$中存在一个新的子项 $t_2 \subset term(m'), a \subset t_2, t_1 \not\subset t_2$.另外,如果 $K^{-1} \notin P$,则该变换进行边一定位于常规串上.

证明:构造集合 $\Psi$,使得集合中的元素 $n_i$ 满足 $a \subset n_i$ 并且 $t_1 \not\subset n_i$.由于 $n' \in \Psi$,因此 $\Psi$非空.从 $C$ 中结点的任何非空子集均有 $\leq_C$ -minimal 元素,因此集合 $\Psi$存在 $\leq_C$ 上的最小元素,记为 $n_0$.由于 $n \notin \Psi, n \neq n_0$.

由于 $a$ 唯一源发于 $n$,故 $C$ 中一定存在边 $n_0' \Rightarrow^+ n_0$ 并且 $a \subset n_0'$.由于 $n_0$ 为 $\Psi$中的 $\leq_C$ -minimal 元素,故 $n_0' \notin \Psi$,则有 $t_1 \subset n_0'$.根据变换进行边的定义,$n_0' \Rightarrow^+ n_0$ 即为 $a$ 的变换进行边.

如果 $K^{-1} \notin P$,并假设 $n_0' \Rightarrow^+ n_0$ 不在常规串上,则 $n_0' \Rightarrow^+ n_0$ 只能位于 $D$-或者 $E$-串上.若 $n_0' \Rightarrow^+ n_0$ 位于 $D$-串,则 $D$-串的密钥边不为 $K^{-1}$,因为假设中有 $K^{-1} \notin P$. $n_0'$ 应形为 $\{h\}_{K'}$,其中 $K' \neq K$.因此,$t_1 \subset h$,而这与 $t_1 \not\subset n_0$ 矛盾.故 $n_0' \Rightarrow^+ n_0$ 不可能位于 $D$-串上.若 $n_0' \Rightarrow^+ n_0$ 位于 $E$-串,$n_0$ 应形为 $\{h'\}_{K''}$,而 $t_1 \not\subset h'$ 与 $t_1 \subset n_0'$ 相矛盾,因此,$n_0' \Rightarrow^+ n_0$ 不可能位于 $E$-串.

故 $n_0' \Rightarrow^+ n_0$ 必然位于常规串上. □

**定理 6(Perrig 主动测试定理)**. $n$ 为从 $C$ 中的一个负结点,若有 $t_1 \subset term(n)$并且 $a \sqsubset_K t_1$,其中 $K \notin P$,则从 $C$ 中存在一个常规正结点 $m \in C$ 使得 $t_1 \subset term(m)$.

3.2.2 Perrig 认证测试定理分析

从文字上看,Perrig 和 Song 将认证测试定理的应用范围从“测试元素在整个协议中不能被嵌套加密”扩展到了“测试元素在测试边上不能被嵌套加密”,试图通过定理 4 中的“$t_1 \not\subset term(n)$”来排除类似例 1 的失效情况,通过定理 5 中“$t_1 \not\subset term(n')$”来排除类似例 2 的失效情况.那么,是否只要保证认证测试元素在变换边上不被嵌套加密,即可保证认证测试方法的有效性呢?事实并非如此,下面我们用一个例子来加以说明.如图 3 所示.

例 3:假设从 $C$ 中存在如下消息序列.其中 $a$ 唯一源发于$\langle s,1\rangle$,$KA^{-1} \notin P$ 且 $KB^{-1} \notin P$.

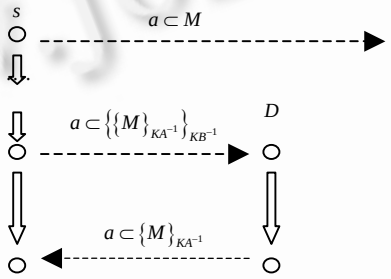



Fig.3 Failure of Perrig’s incoming test

图 3 Perrig 输入测试定理证明出错的情况

从 $C$ 中有$\langle s,1\rangle \Rightarrow {}^+\langle s,3\rangle$,$a$ 唯一源发于$\langle s,1\rangle$,$\langle s,3\rangle$中 $a \sqsubset_K t_1 = \{M\}_{KA^{-1}}$ 并且 $t_1 \not\subset \langle s,1\rangle$.根据定理 4,应存在 $a$ 的变换进行边 $m \Rightarrow^+ m'$,$t_1$ 为测试元素,有 $t_1 \subset term(m')$,$t_1 \not\subset term(m)$,$a \subset term(m)$.由于 $KA^{-1} \notin P$,该变换进行边应位于常规串上.但除了串 $S$ 以外,这里并不能证明 $C$ 中存在其他常规串,攻击者完全可以利用前面的消息 $\{\{M\}_{KA^{-1}}\}_{KB^{-1}}$ 进行解密操作完成.由此可以看出,仅限制认证测试元素在变换边上不被嵌套加密是不可行的.

实际上,Perrig 和 Song 对定理 4 的证明过程中第 2 段有纰漏.$n_0$ 是从 $C$ 中所有包含 $t_1$ 的结点构成的集合 $\Psi$ 的 $\leq_C$ -minimal 元素,$a$ 唯一源发于 $n$ 且 $n \neq n_0$,则 $a$ 不能源发于 $n_0$.又根据 $\leq_C$ -minimal 元素的定义,$n_0$ 必然为正,故从 $C$ 中至少存在一个结点 $n_0'$ 满足 $n_0' \Rightarrow^+ n_0$ 并且 $a \subset n_0'$,假设 $n_0'$ 是 $n_0$ 所在串中包含 $a$ 的最小结点.这时要分两种情况对 $n_0'$ 进行分析.若 $n_0' \neq n$,同样 $a$ 不能源发于 $n_0'$,故 $n_0'$ 为负,得证.若在 $n_0' = n$ 的情况下,$n_0'$ 为正.而变换进行边的定义为“边 $n \Rightarrow^+ n'$中,如果 $n$ 为负,$n'$为正,项 $a \subset term(n)$,结点 $n'$中包含新元素 $t'$,并且 $a \subset t'$,则称 $n \Rightarrow^+ n'$为变换进行边”.这里仅能证明 $n_0$ 为正,不能证明 $n_0'$ 为负,因此不满足变换进行边的定义,证明失败.

定理 5 的证明过程也存在同样问题,不再赘述.定理 5 的失败也对应着下面这种情况.

例 4:假设从 $C$ 中存在如下消息序列.其中,$a$ 唯一源发于$\langle s,1\rangle$并且不出现在$\langle s,1\rangle$除$\{M\}_{KA}$ 之外的其他子项中,$KA^{-1} \notin P$.如图 4 所示.

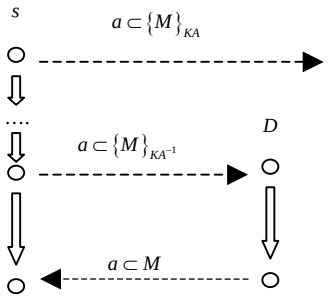



Fig.4 Failure of Perrig's outgoing test

图 4 Perrig 输出测试定理证明出错的情况

从 $C$ 中$\langle s,1\rangle \Rightarrow^{+} \langle s,3\rangle$,$a$ 唯一源发于$\langle s,1\rangle$并且仅出现在$\langle s,1\rangle$的子项 $t_1=\{M\}_{KA}$ 中,$a \sqsubset_K t_1$.$a \subset term(\langle s,3\rangle)$但$t_1 \not\subset term(\langle s,3\rangle)$.根据定理 5,应存在 $a$ 的变换进行边 $m \Rightarrow^{+} m'$,$t_1$ 为测试元素;由于 $KA^{-1} \notin P$,该变换进行边应位于常规串上.但实际上,攻击者可以利用前面的消息 $\{M\}_{KA^{-1}}$ 进行解密操作完成,无法证明协议中除 $S$ 以外其他常规串的存在.

除了上述问题,Perrig 输入测试定理和输出测试定理中没有限制边 $n \Rightarrow^{+} n'$中结点 $n$ 和 $n'$的符号.虽然可以由"$a$ 唯一源发于 $n$"推断出 $n$ 为正,但是 $n'$的符号无法确定.在 $n'$也为正的情况下,失去了身份认证的基础,显然不构成输入或输出测试.另外,Perrig 的改进方案,包括主动测试定理,都忽略了测试元素本身为多重加密形式的情况.

例 5:假设从 $C$ 中存在如下消息序列,$KB^{-1} \notin P$.如图 5 所示.

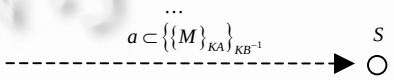



Fig.5 Multi-Encryption in test component itself

图 5 测试元素本身为多重加密形式的情况

定义 13 中 $a \sqsubset_K m=\{t\}_K$ 要求 $a$ 为原子消息,并且 $a$ 是 $t$ 的组成元素.本例中 $m=\{\{M\}_{KA}\}_{KB^{-1}}$,$t=\{M\}_{KA}$,不满足 $a$ 是 $t$ 的组成元素,因而不符合 Perrig 认证测试定理的使用条件,无法进行分析.实际上,这个例子可以使用主动认证测试进行分析,主动测试元素为 $\{\{M\}_{KA}\}_{KB^{-1}}$.应将 $\sqsubset_K$ 关系定义更改为"如果 $a$ 为原子消息,$m=\{t\}_K$,$a \subset t$,定义 $a$ 和 $m$ 之间满足关系 $a \sqsubset_K m$."

### 3.3 认证测试定理改进方案

#### 3.3.1 重新分析输入测试和输出测试

由例 4 可以看出,在某些情况下,即使测试元素没有被嵌套加密,认证测试定理同样也无法完成证明.另外,输入认证测试也有类似的情况,如例 6 所示.

例 6:假设从 $C$ 中存在如下消息序列,其中 $a$ 唯一源发于$\langle s,1\rangle$,$KA^{-1} \notin P$.如图 6 所示.

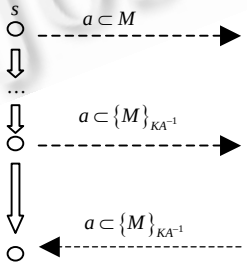



Fig.6 Another failure of Perrig's incoming test

图 6 Perrig 输入认证测试定理证明出错的另一情况

根据 Perrig 输入测试定理,协议中应存在 $a$ 的变换进行边,完成从消息形式 $M$ 到 $\{M\}_{KA^{-1}}$ 的转换.实际上,该形式变换由消息 $M$ 的产生者自己完成,并不能证明协议中除串 $S$ 以外还存在其他常规串,也无法证明变换进行边的存在.本例只能使用主动测试,证明在 $KA^{-1}\notin P$ 的情况下,消息 $\{M\}_{KA^{-1}}$ 由持有 $KA^{-1}$ 的常规主体最先生成.

Perrig 和 Song 的改进方案认为,只要测试元素在测试边上不被加密即可保证认证测试定理的有效性,我们已经证明是不正确的.回顾认证测试定理的基本思想,只有持有对应密钥的合法主体才能解读或者构造出认证测试所需的关键信息.输入测试中的关键信息即认证测试元素$\{\dots a\dots\}_K$,只有持有密钥 $K$ 的主体才能构造出测试元素$\{\dots a\dots\}_K$.因此,在测试边所在串 $S$ 中测试元素$\{\dots a\dots\}_K$不应出现在测试边完成之前,更不用说以嵌套加密的形式出现.实际上,例 3 和例 6 中问题出现的根本原因就是由于协议消息无意泄露了完成认证测试所需的关键信息.而输出测试中关键信息为测试元素$\{\dots a\dots\}_K$中的 $a$ 值,只有持有密钥 $K^{-1}$ 的主体才能读取$\{\dots a\dots\}_K$中 $a$ 的值.为了保证关键信息不被无意泄露,测试边所在串 $S$ 中不允许 $a$ 在测试结点 $n'$之前以$\{\dots a\dots\}_K$之外的其他形式出现.这里所说的其他形式不包括输出测试元素的多重加密形式$\{\dots\{\dots a\dots\}_K\dots\}_{K'}$,因为$\{\dots\{\dots a\dots\}_K\dots\}_{K'}$不会泄露关键信息 $a$.我们将类似的消息形式变换,例如对测试元素的加密$\{\dots a\dots\}_K\rightarrow\{\dots\{\dots a\dots\}_K\dots\}_{K'}$称为无意义的形式变换,因为任何主体都可以使用自己掌握的密钥进行加密操作来完成该变换.为了避免无意义的形式变换——无须持有对应密钥即可完成消息形式的变换,输出测试中还需要限制测试元素在测试边上不能被嵌套加密.

3.3.2 一种新的改进方案

我们将在前一节非形式化分析的基础上,结合原认证测试定理和 Perrig 的改进思想,提出一种新的认证测试改进方案,使用串空间方法证明如下.

**定理 7(新输入测试定理)**. 丛 $C$ 中 $n\Rightarrow^{+}n'$,如果原子消息 $a$ 唯一源发于 $n$,负结点 $n'$的子项 $t=\{h\}_K$ 满足 $a\sqsubset t.n$ 所在串 $S$ 中所有满足 $n''\prec_C n'$的正结点 $n''$都有 $t\not\sqsubset term(n'')$,$K\notin P$,则 $C$ 中必然存在常规结点 $m,m'\in C$ 使得 $t$ 是 $m'$ 的元素并且 $m\Rightarrow^{+}m'$是 $a$ 的变换进行边(transforming edge).

证明:令丛 $C$ 中所有包含 $t$ 的结点构成集合 $\Psi$,集合 $\Psi$中的任意元素 $n_i$ 满足 $t\sqsubset term(n_i)$.由于 $n'\in\Psi$,因此 $\Psi$非空.丛中结点的任何非空子集均有 $\leq_C$-minimal 元素,因此集合 $\Psi$存在 $\leq_C$ 上的最小元素,记为 $m'$.串 $S$ 中满足 $n''\prec_C n'$ 的所有结点 $n''$都有 $t\not\sqsubset term(n'')$,则 $S$ 中所有 $\prec_C n'$的结点都不在集合 $\Psi$中,故 $n\neq m'$.由于 $a$ 唯一源发于 $n$ 且 $n\neq m'$,则 $a$ 不能源发于 $m'$.又根据 $\leq_C$-minimal 元素的定义,$m'$为正,故 $m'$所在串上至少存在一个结点 $m^*$满足 $m^*\Rightarrow^{+}m'$并且 $a\sqsubset term(\mathrm{m}^*)$,令 $m$ 是满足 $\mathrm{m}^*\Rightarrow^{+}m'$并且 $a\sqsubset term(m^*)$的 $m^*$中最小的结点.

假设 $m=n$,则 $\Psi$的最小元素 $m'$位于串 $S$ 上,由于 $S$ 中所有 $\prec_C n'$的正结点 $n''$都有 $t\not\sqsubset term(n'')$,故 $m'$只可能为 $n'$.但 $n'$为负结点,而 $m'$为正,故假设不成立.因此,$m\neq n$,$a$ 同样不能源发于 $m$,可得出 $m$ 为负.由于 $m'$为 $\Psi$中的 $\leq_C$-minimal 元素,故 $m\notin\Psi$,则有 $t\not\sqsubset m$.根据变换进行边的定义,$m$ 为负,$m'$为正,$a\sqsubset term(m)$,结点 $m'$中包含新元素 $t$ 并且 $a\not\sqsubset t$,故 $m\Rightarrow^{+}m'$即为 $a$ 的变换进行边.

假设变换进行边 $m\Rightarrow^{+}m'$不在常规串上,由于 $m'$中出现了新元素,$m\Rightarrow^{+}m'$只能位于 $D$-或者 $E$-串上.若 $m\Rightarrow^{+}m'$位于 $D$-串,则 $term(m)$形如$\{h'\}_{K'}$.显然 $t\sqsubset h'\sqsubset\{h'\}_{K'}$,$t\sqsubset term(m)$.而这与 $m'$是集合 $\Psi$最小元素相矛盾,因此 $m\Rightarrow^{+}m'$不可能位于 $D$-串上.若 $m\Rightarrow^{+}m'$位于 $E$-串,则 $term(m')$应形为$\{h'\}_{K'}$,由于 $K\notin P$,$K'\neq K$,因此有 $t\sqsubset h'$,$t\sqsubset term(m)$,与 $m'$是集合 $\Psi$最小元素相矛盾,故 $m\Rightarrow^{+}m'$也不可能在 $E$-串上.

故在 $K\notin P$ 的情况下,$C$ 中必然存在常规结点 $m,m'\in C$ 使得 $t$ 是 $m'$的元素并且 $m\Rightarrow^{+}m'$是 $a$ 的变换进行边.□

**定理 8(新输出测试定理)**. 丛 $C$ 中 $n\Rightarrow^{+}n'$,如果原子消息 $a$ 唯一源发于 $n$,$term(n)$的组成元素 $t=\{h\}_K$ 满足 $a\not\sqsubset t$,负结点 $n'$满足 $a\sqsubset term(n')$但 $t\not\sqsubset term(n')$.$K^{-1}\notin P$,并且对于 $n$ 所在串 $S$ 中 $\prec_C n'$的所有正结点 $n''$,如果任何子项 $t_0$ 满足 $a\not\sqsubset t_0$,则必然有 $t\not\sqsubset t_0$.

(1) $C$ 中存在常规结点 $m,m'\in C$ 使得 $t$ 是 $m$ 的元素并且 $m\Rightarrow^{+}m'$是 $a$ 的变换进行边.

(2) $m,m'$所在主体串记为 $S'$,$a\sqsubset t_1=\{h_1\}_{K_1}\sqsubset term(m')$.常规串上,如果以 $t=\{h\}_K$ 为组成元素的负结点仅出现在 $S'$上,并且串 $S'$的所有正结点中 $a$ 不以除 $t_1$ 以外的形式出现,$k_1^{-1}\notin P$,则 $C$ 中存在负的常规结点,$t_1$ 为该结点的组成元素.

证明:

(1) 构造集合$\Psi$,使得集合中的任意元素 $n_i$ 满足 $a\subset term(n_i)$并且 $t\not\subset term(n_i)$.由于 $n'\in\Psi$,因此$\Psi$非空.从中结点的任何非空子集均有 $\leq_C$-minimal 元素,因此集合$\Psi$存在 $\leq_C$ 上的最小元素,记为 $m'$.由于 $n\notin\Psi$,$n\neq m'$.由于 $a$ 唯一源发于 $n$ 且 $n\neq m'$,则 $a$ 不能源发于 $m'$.又根据 $\leq_C$-minimal 元素的定义,$m'$为正,故 $m'$所在串上至少存在一个结点 $m^*$满足 $m^*\Rightarrow^+m'$并且 $a\subset term(m^*)$,令 $m$ 是满足 $m^*\Rightarrow^+m'$并且 $a\subset term(m^*)$的 $m^*$中最小的结点.

假设 $m=n$,则集合$\Psi$的最小元素 $m'$也位于串 $S$ 上,而 $S$ 的所有 $\prec_C n'$的正结点 $n''$中,任何子项 $t_0$ 满足 $a\subset t_0$ 则必然有 $t\subset t_0$,故 $m'$只可能为 $n'$.但 $n'$为负结点,而 $m'$为正,故假设不成立.因此,$m\neq n$,$a$ 同样不能源发于 $m$,可得出 $m$ 为负.由于 $m'$为$\Phi$中的 $\leq_C$-minimal 元素,故 $m\notin\Psi$,而 $a\subset term(m)$,则 $t\subset term(m)$.根据变换进行边的定义,$m$ 为负,$m'$为正,$a\subset term(m)$,结点 $m'$中包含新元素 $t_1$ 并且 $a\subset t_1$,故 $m\Rightarrow^+m'$即为 $a$ 的变换进行边.

假设 $m\Rightarrow^+m'$不在常规串上,则 $m\Rightarrow^+m'$只可能位于 $D$-或者 $E$-串.如果 $m\Rightarrow^+m'$位于 $D$-串,由于 $K^{-1}\notin P$,$D$-串的密钥边不可能为 $K^{-1}$,故 $term(m)$形为$\{h'\}_{K'}$,其中 $K'\neq K$.$t\subset term(m')=h'$,因此 $t\subset\{h'\}_{K'}=term(m)$.而这与 $m'$是集合$\Psi$最小元素相矛盾,因此 $n_0'\Rightarrow^+n_0$ 不可能位于 $D$-串上.如果 $m\Rightarrow^+m'$位于 $E$-串,$term(m')$应形为$\{h'\}_{K'}$,显然 $t\subset term(m)=h'$,亦有 $t\subset\{h'\}_{K'}\subset term(m')$,与 $m\in\Psi$矛盾,因此 $m\Rightarrow^+m'$也不可能位于 $E$-串.故变换进行边 $m\Rightarrow^+m'$只可能位于常规串上.

故 $C$ 中必然存在常规结点 $m,m'\in C$ 使得 $t$ 是 $m$ 的元素并且 $m\Rightarrow^+m'$是 $a$ 的变换进行边.

(2) 令 $n'$中包含 $a$ 的新元素为 $t'$.若 $t_1=t'$,显然存在负常规结点 $n',t_1$ 为该结点的元素.

如果 $t_1\neq t'$,则在 $\succ_C m'$的结点中构造集合$\Psi'$,使得集合中的任意元素 $n_i'$满足 $a\subset term(n_i')$并且 $t_1\not\subset term(n_i')$.由于 $n'\in\Psi'$,因此$\Psi'$非空.从中结点的任何非空子集均存在 $\leq_C$-minimal 元素,因此集合$\Psi'$存在 $\leq_C$ 上的最小元素,记为 $u'$,显然,该结点为正.$S$ 的所有 $\prec_C n'$的结点中,$a$ 不以除 $t$ 以外的其他任何形式出现,因此 $u'$不在 $S$ 串上.$a$ 不源发于 $u'$,则至少存在一个结点 $u^*$满足 $u^*\Rightarrow^+u'$,$a\subset term(u^*)$,令 $u$ 为满足上述条件的 $u^*$中的最小值.$u$ 不在 $S$ 串上,$a$ 不源发于 $u$,故 $u$ 为负.

假设 $u\prec_C m'$,而 $m'$为满足丛 $C$ 中满足 $a\subset term(n_i)$且 $t\not\subset term(n_i)$的最小元素,故 $t\subset term(u)$.$u\Rightarrow^+u'$构成 $a$ 的变换进行边.假设 $u\Rightarrow^+u'$不在常规串上,由于 $u'$中出现了新元素,$u\Rightarrow^+u'$只可能位于 $D$-串或者 $E$-串.假设 $u\Rightarrow^+u'$位于 $D$-串,由于 $k^{-1}\notin P$,$D$-串的密钥边不可能是 $K^{-1}$,故 $term(u)$形如$\{h'\}_{K'}$,其中 $K'\neq K$,则有 $t\subset h'\subset\{h'\}_{K'}$,与 $u'\notin\Psi'$相矛盾,因此 $u\Rightarrow^+u'$不在 $D$-串上.假设 $u\Rightarrow^+u'$位于 $E$-串,则 $t\subset term(u)\subset term(u')$,与 $u'\notin\Psi'$矛盾,$u\Rightarrow^+u'$也不可能位于 $E$-串.因此 $u\Rightarrow^+u'$只可能位于常规串.以 $t=\{h\}_K$ 为组成元素的负结点只可能出现在 $S'$中,即 $u$ 只可能位于 $S'$串上,$u'$也位于 $S'$串.$a\subset term(u')$,$t_1\not\subset term(u')$,与题设“串 $S'$的所有正结点中 $a$ 不以除 $t_1$ 以外的形式出现”相矛盾,故假设 $u\prec_C m'$不成立.

$u\succ_C m'$,由于 $u'$为集合$\Psi'$上的最小元素,故有 $u\notin\Psi'$,$t_1\subset term(u)$.$u\Rightarrow^+u'$构成 $a$ 的变换进行边.假设 $u\Rightarrow^+u'$不在常规串上,由于 $u'$中出现了新元素,$u\Rightarrow^+u'$只可能位于 $D$-串或者 $E$-串.假设 $u\Rightarrow^+u'$位于 $D$-串,由于 $k_1^{-1}\notin P$,$D$-串的密钥边不可能是 $K_1^{-1}$,故 $term(u)$形如$\{h'\}_{K'}$,其中 $K'\neq K_1$,则有 $t_1\subset h'\subset\{h'\}_{K'}$,与 $u'\in\Psi'$相矛盾,因此,$u\Rightarrow^+u'$不在 $D$-串上.假设 $u\Rightarrow^+u'$位于 $E$-串,则 $t_1\subset term(u)$,$term(u)\subset term(u')$,与 $u'\in\Psi'$ 相矛盾,$u\Rightarrow^+u'$不可能位于 $E$-串.

故 $C$ 中必然存在负的常规结点 $u,t_1$ 为该结点的组成元素. □

**定理 9(新主动测试定理)**. 丛 $C$ 的负结点 $n$ 中,若原子消息 $a$ 满足 $a\subset t=\{h\}_K\subset term(n)$,并且 $K\notin P$,则 $C$ 中必然存在常规正结点 $m$ 使得 $t$ 是 $m$ 的组成元素,并且 $t$ 源发于 $m$.

证明:令丛 $C$ 中所有包含 $t$ 的结点构成集合$\Psi$,集合$\Psi$中的任意元素 $n_i$ 满足 $t\subset term(n_i)$.由于 $n\in\Psi$,因此$\Psi$非空.从中结点的任何非空子集均有 $\leq_C$-minimal 元素,因此集合$\Psi$存在 $\leq_C$ 上的最小元素,记为 $m$.根据最小元素的定义,$m$ 为正.由于 $t\subset term(m)$,因此 $m$ 不可能位于 $M$-串或 $K$-串.另外,结点 $m$ 中出现了新元素 $t$,故 $m$ 也不可能位于 $C$-串,$S$-串,$T$-串和 $F$-串上.

假设 $m$ 位于 $D$-串,显然 $m$ 位于明文边,密文边结点 $m'$消息形如$\{h'\}_{K'}$,$m$ 位于明文边.显然 $m'\Rightarrow m$,$\{h\}_K\subset h'$,而 $h'\subset\{h'\}_{K'}$,故 $t\subset\{h'\}_{K'}$,与 $m$ 是集合$\Psi$的最小元素相矛盾.假设 $m$ 位于 $E$-串,显然 $m$ 位于密文边,消息格式为$\{h'\}_{K'}$.由于 $K\notin P$,密钥边不可能为 $K$,因此 $K\neq K'$.显然 $\{h\}_K\subset h'$,与 $m$ 是集合$\Psi$的最小元素相矛盾.因此,结点 $m$

只可能位于常规串上.

由于 $m$ 是从 $C$ 中包含 $t$ 的所有结点中最小的,因此对于 $m$ 所在串 $S$,显然有 $t \sqsubset term(m)$,但对于任何 $m' \Rightarrow^{+} m$, $t \not\sqsubset term(m')$.故 $C$ 中必然存在常规正结点 $m$ 使得 $t$ 是 $m$ 的元素,并且 $t$ 源发于 $m$. □

3.3.3 新认证测试定理的应用

新认证测试定理去掉了认证测试元素在整个协议消息中不能嵌套加密的限制:输出测试要求测试元素在测试边 $n \Rightarrow^{+} n'$ 上不被嵌套加密,并且测试边所在串 $\prec_C n'$ 的正结点中 $a$ 只能出现在认证测试元素中;输入测试中要求测试元素不出现在测试边 $n \Rightarrow^{+} n'$ 所在串 $n'$ 前的正结点中;主动测试定理则完全去除了嵌套加密的限制.

对于例 4 中的消息序列,满足 Perrig 输出测试定理的使用条件,但得到的结论是错误的.$a$ 在 $\prec_C n'$ 的结点 $\langle S,2\rangle$ 中又以 $\{M\}_{KA^{-1}}$ 形式出现,不满足新输出测试定理"$a$ 在 $\prec_C n'$ 的正结点中不以其他形式出现"的要求,无法证明协议中存在包含特定消息的常规串.例 6 满足 Perrig 输入测试定理的使用条件,但证明结论与事实不相符合,出现了错误.认证测试元素 $\{M\}_{KA^{-1}}$ 在结点 $n'$ 前出现在结点 $\langle S,2\rangle$ 消息中,不满足新输入测试定理要求,无法证明该变换是由常规主体完成的.使用新主动测试定理也只能证明,$C$ 中存在含组成元素 $\{M\}_{KA^{-1}}$ 的常规正结点 $m$,与事实相符.

在有第三方参与的认证协议中,经常会将令牌封装在另一个消息的加密形式中加以发送.通常这种情况下令牌就是某主体进行身份认证所需的关键信息,例如 Woo-Lam 协议的多个版本、Needham-Schroder 对称密钥协议、Kerberos 协议和 Denning-Sacco 协议等.对于这种测试元素被再次加密的情况,原认证测试定理无能为力,无法进行分析.下面我们将使用新认证测试定理,以 Woo-Lam 改进协议为例进行分析.

例 7:Woo-Lam 协议是基于对称密钥,有可信第三方参与的单向认证协议,用于主体 $A$ 借助认证服务器 $S$ 向另一主体 $B$ 证明自己的身份.针对原 Woo-Lam 协议出现的攻击方法[18],文献[19]中对其进行了分析改进.改进的协议消息序列如图 7 所示.

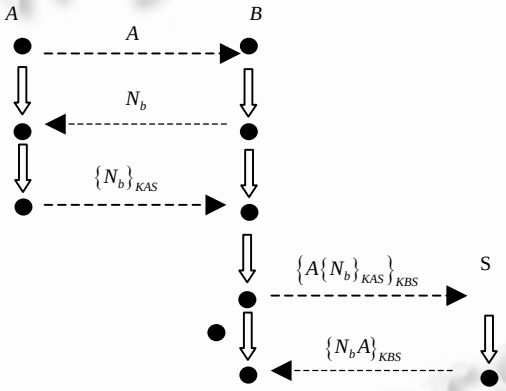



Fig.7 Bundle of Woo-Lam

图 7 Woo-Lam 协议消息图

Woo-Lam 协议串空间Σ,包括以下 4 类串集合:

(1) 发起者串 $init[A,S,N_b]$,消息迹为 $\langle +A,-N_b,+\{N_b\}_{KAS}\rangle$.

(2) 响应者串 $resp[A,B,S,N_b,H]$,消息迹为 $\langle -A,+N_b,-H,+\{AH\}_{KBS},-\{N_bA\}_{KBS}\rangle$.

(3) 服务器串 $serv[A,B,S,N_b]$,消息迹为 $\langle -\{A\{N_b\}_{KAS}\}_{KBS},+\{N_bA\}_{KBS}\rangle$.

(4) 攻击者串 $P$,

其中,$H$ 表示主体不能识别内容的加密项.Woo-Lam 是单向认证协议,只要求服务提供者 $B$ 认证用户 $A$ 的身份.因此假设 Woo-Lam 协议串空间$\Sigma$中,$C$ 为包含响应者串 $S_r \in resp[A,B,S,N_b,H]$ 的丛,响应者串 $S_r$ 的 $C$-height 为 5.$KAS \notin P$,$KBS \notin P$,并且 $N_b$ 在$\Sigma$中唯一源发.

证明:根据协议消息图,$N_b$ 在串空间$\Sigma$中唯一源发于$\langle S_r,2\rangle$,负结点$\langle S_r,5\rangle$的消息项 $t=\{N_bA\}_{KBS}$ 满足 $N_b\sqsubset t.B$ 串中$\langle S_r,5\rangle$之前的所有正结点消息都不含 $\{N_bA\}_{KBS}$,并且 $KBS\notin K_P$,因此边 $\langle S_r,2\rangle\Rightarrow\langle S_r,5\rangle$ 构成 $N_b$ 的输入测试,$\{N_bA\}_{KBS}$ 为测试元素.根据新输入认证测试定理,从 $C$ 中应存在常规结点 $m$ 和 $m'$,$\{N_bA\}_{KBS}$ 为 $m'$的组成元素,并且 $m\Rightarrow^+m'$为 $N_b$的变换进行边.观察协议消息格式,包含 $\{N_bA\}_{KBS}$ 形式的正结点只可能出现在服务器串的$\langle S,2\rangle$结点上.故从 $C$ 中必然存在服务器串 $S_S\in serv[A,B,S,N_b]$,并且其 $C$-height 为 2.

负结点$\langle S_S,1\rangle$中,$N_b\sqsubset\{N_b\}_{KAS}\sqsubset\{A\{N_b\}_{KAS}\}_{KBS}$,$KAS\notin P$,则结点$\langle S_S,2\rangle$构成主动测试,根据新主动测试定理,$C$ 中必然存在常规正结点 $m$ 使得$\{N_b\}_{KAS}$是 $m$ 的元素,并且$\{N_b\}_{KAS}$源发于 $m$.显然,在常规正结点中,该消息格式只可能出现在发起者串的$\langle A,3\rangle$结点中.故从 $C$ 中必然存在发起者串 $S_i\in init[A,S,N_b]$.由于$\langle S_i,3\rangle$结点存在,故 $S_i$ 串的 $C$-height 为 3.

由此可以看出:当响应者 $B$ 认为与发起者 $A$ 完成了一轮协议会话时,$A$ 确实作为发起者曾与 $B$ 执行过该协议,并且两个主体对临时值 $N_b$ 达成一致.由于 $N_b$ 在$\Sigma$中唯一源发,因此 $B$ 的每一轮会话均唯一对应着 $A$ 的一轮会话.故 $B$ 对主体 $A$ 的身份认证满足强一致性. □

在这个例子中,测试元素 $\{N_b\}_{KAS}$ 在协议消息 $\{A\{N_b\}_{KAS}\}_{KBS}$ 中被嵌套加密,新认证测试定理仍然能够正确地证明协议的认证属性.由此可以看出,新认证测试不仅突破了原认证测试定理“协议中测试元素不能嵌套加密”的限制,也有效避免了 Perrig 认证测试定理证明中出现的错误.

## 4 小 结

与现有工作相比,本文主要对认证测试理论的应用范围进行扩展,首先讨论了 Perrig 和 Song 对认证测试定理的改进方案,指出其改进方案存在的缺陷;对输入、输出和主动测试这 3 种认证测试形态分别提出了新的定理,形成完整的认证测试改进方案.并使用串空间方法证明了新认证测试定理的正确性.新认证测试定理有效突破了认证测试方法在认证测试元素在整个协议消息中不能被嵌套加密的限制,能够更准确地描述协议满足目标认证属性所需要满足的条件.

下一阶段的工作重点将放在认证测试方法的高性能自动化分析上,对协议自动分析工具进行扩展,增加认证测试模块,对于符合认证测试应用条件的协议采用认证测试模块进行分析,提高分析效率.

**致谢** 在此,我们向对本文工作给予支持和建议的同行,尤其是中山大学信息科学及技术学院的刘璟博士表示感谢.

**References**:

[1] Lowe G. An attack on the needham-schroeder public-key authentication protocol. Information Processing Letters, 1995,56(3): 131−136.

[2] Fabrega FJT, Herzog JC, Guttman JD. Strand space: Why is a security protocol correct. In: Proc. of the 18th IEEE Symp. on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1998. 160−171. http://www.mitre.org/work/tech_papers/tech_papers_00/ guttman_strands/index.html

[3] Fabrega FJT, Herzog JC, Guttman JD. Strand space: Proving security protocols correct. Journal of Computer Security, 1999,7(2,3): 191−230.

[4] Fabrega FJT, Herzog JC, Guttman JD. Honest ideals on strand space. In: Proc. of the 11th IEEE Computer Security Foundations Workshop (CSFW). Washington: IEEE Computer Society Press, 1998. 66−77. http://www.mitre.org/work/tech_papers/tech_papers_00/guttman_honest/index.html

[5] Guttman JD, Thayer FJ. Authentication tests and the structure of bundles. Theoretical Computer Science, 2002,283(2):333−380.

[6] Guttman JD, Thayer FJ. Key Compromise, Strand Spaces and the Authentication Tests. In: Proc. of the 17th Conf. on the Mathematical Foundations of Programming Semantics. Elsevier BV, 2001. 141−161.

[7] Jiang R, Pan L, Li JH. Further analysis of password authentication schemes based on authentication tests. Computer & Security, 2004,23(6):469−477.

[8] Li XH, Hao LM, Yang ST, Li JH. Formal verification of EAP-AKA with improved authentication tests. In: Proc. of the Int'l Conf. on Wireless Communications, Networking and Mobile Computing. Wuhan, 2006. 1−4. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4149477

[9] Guttman JD. Security protocol design via authentication tests. In: Proc. of the 2002 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 2002. 92−103. http://www.dcs.qmul.ac.uk/~joshuag/pubs/at_design.pdf

[10] Liu JF, Zhou MT. Designing authentication protocols via authentication test. In: Proc. of the IEEE Symp. on Computers and Communications. Aveiro Portugal: IEEE Computer Society Press, 2007. 475−480. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4381592

[11] Jiang R, Hu AQ, Li JH. Research on formal design of ESIKE based on Authentication Tests. Chinese Journal of Computers, 2006,29(9):1694−1701 (in Chinese with English abstract).

[12] Yang M, Luo JZ. Analysis of security protocols based on authentication test. Journal of Software, 2006,17(1):148−156 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/148.htm

[13] Li YJ, Pang J. Generalized unsolicited tests for authentication protocol analysis. In: Proc. of the 7th Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies. IEEE Computer Society Press, 2006. 509−514. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4032236

[14] Liu JF, Zhou MT. Research and improvement on authentication test's limitation. High Technology Letters, 2008,14(3):266−270.

[15] Perrig A, Song D. Looking for diamonds in the desert-extending automatic protocol generation to three-party authentication and key agreement. In: Proc. of the 13th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 2000. 64−76. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=856926

[16] Song D. Athena: A new efficient automatic checker for security protocol analysis. In: Proc. of the 1999 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1999. 192−202. http://ieeexplore.ieee.org/iel5/6332/16921/00779773.pdf?tp=&arnumber=779773&isnumber=16921

[17] Song D, Berezin S, Perrig A. Athena: A novel approach to efficient automatic security protocol analysis. Journal of Computer Security, 2001,9(1):47−74

[18] Clark J, Jacob J. A survey of authentication protocol literature: Version 1.0. University of York, Department of Computer Science, http://www-users.cs.york.ac.uk/～jac/Security Protocols Review

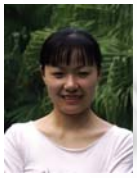
[19] Lin XJ, Hu SL. Informal methods for the analysis of authentication protocols. Journal of Chinese Computer Systems, 2003,24(11):1912−1915 (in Chinese with English abstract).

**附中文参考文献**:

[11] 蒋睿,胡爱群,李建华.基于 Authentication Test 方法的高效安全 IKE 形式化设计研究.计算机学报,2006,29(9):1694−1701.

[12] 杨明,罗军周.基于认证测试的安全协议分析.软件学报,2006,17(1):148−156. http://www.jos.org.cn/1000-9825/17/148.htm

[19] 林贤金,胡山立.认证协议攻击与非形式化分析.小型微型计算机系统,2003,24(11):1912−1915.



**刘家芬**(1980－),女,湖北荆州人,博士生,主要研究领域为网络信息安全,网络计算.

**周明天**(1939－),男,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络,网络计算,中间件技术,网络与信息系统安全.