西南交通大学

硕士学位论文

基于Strand Space模型的安全协议形式化分析研究

姓名：程娜

申请学位级别：硕士

专业：密码学

指导教师：何大可

20060501

摘 要

随着网络的普及以及电子商务和电子政务的蓬勃兴起，网络安全问题日显突出。安全协议，作为解决安全问题最行之有效的方法，也就变得越来越重要。然而，在复杂的网络环境中，要确保安全协议的正确性却是件很难解决的问题，它已成为一项重要的研究课题。20年来，为了应对这一挑战，科学家们在安全协议分析这一领域投入了大量的精力。在已有的理论和方法中，形式化分析方法的成果较为突出。

在各种形式化分析方法中，被普遍认为最有前景的最新研究成果是由Fabrega, Herzog和Guttman三人提出的Strand Space模型。它充分吸收了前人的研究成果，使用一种节点间存在因果关系的有向图来表示协议中主体、入侵者的动作序列，利用证明的方法推导协议的正确性，可以防止状态空间爆炸。它是一种直观、简洁、严格、有效的形式化分析方法。

本文深入研究了Strand Space理论，并用该理论分析了若干协议：

1. Yahalom协议。建立了Yahalom协议的Strand Space模型，并进行了深入的讨论；

2. 一种传输模型的认证协议。建立了该协议的Strand Space模型，通过分析，发现协议存在漏洞，并构造出了一种攻击方法，最后针对漏洞对协议进行了改进；

3. ISI支付协议。将Strand Space理论运用到电子商务协议公平性的分析中，得到了与其他分析方法一致的结果。

此外，本文在基础理论部分对代理多重签名进行了研究，提出了一种增强的代理多重签名方案。

关键词：安全协议；形式化分析；Strand Space模型；公平性；代理多重签名

Abstract

With the popularization of network and Internet applications, security issues are becoming more and more important. Accordingly, security protocol, the most effective way to solve security issues, is of the same importance. But it is not an easy work to ensure the validity of security protocol in the sophisticated network environment, which has become an important research subject. Great efforts have been made by scientists to meet this challenge during the past 20 years, which in a sense shows the difficulty of security protocols analysis. Among all existing theories and methods, formal analysis is an outstanding one.

The updated research fruit--Strand Space Model (SSM) brought forward by Fabrega, Herzog and Guttman is of the best prospect among varieties of formal analysis methods at large. It fully absorbs former researching results and uses a kind of order graph between its nodes existing casual relationship to demonstrate the action sequence of main body and intruder of the protocol and deduce the validity of the protocol by means of certification. It can prevent the bursting of status space and is practical, intuitive and strict for formal analysis of security protocol.

This paper does a further study on the SSM, and then analyses numbers of security protocols based on it as follows:

1. Yahalom protocol

Establish the SSM of Yahalom protocol and conduct the further discussion;

2. A kind of authentication protocol based on a transmission model

With SSM, we find out its dropper and create a new attack on this protocol and make some improvement;

3. ISI payment protocol

We apply the SSM to the analysis of fairness of E-business protocol.

Additionally, we study on proxy multi-signature scheme in basic theory and present a strengthened proxy multi-signature scheme.

Key word: Security protocol; Formal analysis; Strand Space Model; Fairness; Proxy multi-signature

第1章 绪论

1.1 研究背景

计算机网络正以惊人的速度向各个领域渗透，成为各领域发展的新源泉，各种现实世界里的组织与系统正在走进网络这个虚拟的世界，使网络世界变得更加精彩；与此同时，安全问题也变得日益突出、复杂，解决安全问题对许多网络应用来说已是头等大事。从目前解决安全问题的方式来看，安全协议是最有效的手段之一。它可以有效地解决以下一些重要的安全问题：源认证和目标认证、消息的完整性、匿名通信、抗拒绝服务、抗抵赖、授权等。另一方面，随着网络技术的飞速发展，多播技术已不断走向成熟，由多播应用带动的安全问题也变得更加复杂，为解决这些问题也是通过一种称为群协议的安全协议来完成的。目前研究热点之一的多主体系统中的安全主体问题，在很大程度上也是依靠有效的安全协议的设计来完成的。可见，安全协议是一个十分重要的研究课题。

在一个分布式的互联网网络环境中，人们通过安全协议来具体实现安全共享网络资源的需求。然而，安全协议的设计极易出错，而且十分困难，即使我们只讨论安全协议中最基本的认证协议，其中参加协议的主体只有两三个，交换的消息只有3-5条，设计一个正确的、符合认证目标的、没有冗余的认证协议也十分困难。正如实际应用中已有的安全协议往往被证实并不如它们设计者期望的那样安全，复杂而恶意的网络环境使得攻击者可利用安全协议自身的缺陷来实施各种各样的攻击，从而达到破坏网络的目的。即使一个安全协议被很小心仔细地设计了，并被使用了很多年，仍然包含一些微妙的漏洞没有被发现。设计一个符合安全目标的协议，仅仅知道系统的安全需求远远不够，我们需要确保所设计的协议在系统参与的各方之间能够运行良好。因此，安全协议的安全性成为网络安全的关键。

考量和分析一个安全协议的安全性，我们称之为安全协议的分析。二十多年来为了应对这一挑战，科学家们投入了大量的精力设计开发了不同种类的研究理论与方法，比如形式化方法、可证明安全理论、零知识证明理论等。

形式化分析就是将安全协议及其所处的环境视为一个系统，运用各种正规的、模型化的、标准的、客观的方法（这些方法可以是理论推证、也可以是工程技术实现；可以是协议分析专用的、也可以是一般目的性的），来验证安全协议的说明是否能够达成其预期的目标。

安全协议形式化分析从89年起至今，十几年的时间里发展极为迅速，目前已成为安全协议研究领域一个极为重要、颇具理论深度，同时也是任何人无法回避的一个前沿课题。

1.2 论文的研究意义

安全协议的形式化分析研究已取得了许多显著的成果，其中具有代表性的就是著名的Dolev-Yao模型[1]和BAN逻辑[2]。但是安全协议的研究也同样面临巨大挑战，是一件复杂、困难的工作。安全协议的研究存在最大的一个困惑就是：被证明不正确的安全协议肯定有漏洞，但被证明为正确的安全协议却不能保证没有漏洞。导致上述问题的原因是多方面的。首先，安全目标本身十分微妙，也不确定，例如，关于认证性的定义，至今存在各种不同的观点。其次，安全协议运行环境非常复杂，攻击者无时无刻不存在，手段和能力无法具体估计和量化；刻画安全协议的运行环境和形式化描述攻击者的能力都是艰巨的任务。最后，安全协议的运行是不确定的，因为它们具有高并发性。

目前，在安全协议形式化分析领域最有前景的方向就是结合采用模型检测技术和定理证明方法开发分析协议的自动验证工具，目前已取得了一些研究成果：FDR[3]、Murcp[4]、Interrogator[5]和Brutus[6]。自动验证工具的优势在于易用性和实用性，但缺点在于容易受到状态空间严重爆炸问题的困扰，这使得它们不能分析一些大型复杂的协议。

Strand Space模型由Fabrega, Herzog和Guttman三人于1998年提出[7]，Strand Space模型的提出为解决安全协议设计与分析的困难提供了一种可能。“该方法吸纳了NRL协议分析器、Schneider秩函数和Paulson归纳法等思想”[8]，它是现有安全协议形式化方法中最为直观、简洁、严格和有效的方法，它充分吸收了前人的研究工作成果。它的直观性表现在使用一种节点间存在因果关系的有向图来表示协议的运行；它的简洁性表现在对于小型协议完全可以使用手工的方法完成证明；它的严格性表现在它使用了节点之间的因果

关系来确保证明的逻辑性和证明的正确性；它的有效性可以通过文献[7,9,10]中给出的实例来说明。利用 Strand Space 理论分析安全协议的安全性已经取得了很多成果，在理论研究和工具开发方面都有新的进展。Cervesato、Durgin、Kanovich 和 Scedrov 使用线形逻辑对 Strand Space 进行解释[11]，Syverson 使用 Strand Space 的语义表现认证性逻辑[12]。另外，D.Song 对 Strand Space 模型进行了扩充[13]，引入了 Strand Space 中各要素的语法和语义，并对安全协议的认证性进行了逻辑的表示，在此基础上又使用 SML 语言开发了一个安全协议自动验证工具 ATHENA 实现了对认证性安全协议的自动验证，但该工具对秘密性协议的证明是不完善的。

综上所述，对 Strand Space 模型的研究应用既有理论意义也有现实意义。

1.3 论文的主要工作及组织结构

论文共分为五章，主要工作涉及基础理论研究和基于 Strand Space 模型的安全协议分析研究两大部分。具体安排如下：

第一章：绪论

介绍了论文的研究背景，意义及总体框架。

第二章：基础理论研究

介绍了安全协议形式化分析的密码学理论基础；介绍了数字签名技术及公钥体制，提出了一种增强的代理多重签名方案。

第三章：安全协议形式化分析综述

介绍了安全协议的定义、分类、性质、设计原则及可能存在的缺陷类型；概述了安全协议形式化分析的历史、研究现状、分类。

第四章：Strand Space 理论与模型

介绍了 Strand Space 理论与模型，定义了一些基本概念，给出一些命题、引理和定理以及相关的证明，指出了 Strand Space 模型的优点及不足。

第五章：若干密码协议的 Strand Space 模型及分析

介绍了 NSL 协议的 Strand Space 模型及分析；构造了 Yahalom 协议的 Strand Space 模型并对其进行了分析；运用 Strand Space 模型对一种传输模型的认证协议进行了分析并发现了漏洞，给出了一种攻击，并对协议进行了改进；将 Strand Space 模型运用于安全协议的公平性分析，分析了 ISI 支付协议

的公平性，得到了其他分析方法相同的结论。

结论：总结了本论文的主要工作，对以后工作进行了展望。

最后是参考文献，致谢以及攻读学位期间发表和即将发表的论文。

第2章 基础理论研究

2.1 密码学简介

密码学是网络信息安全科学和技术研究最为直接的基础学科，是保证信息安全的关键技术。密码学（源于希腊语，英文为cryptogoraphy）有着漫长、丰富的历史，它研究如何把信息转换成一种隐蔽的方式，阻止其他人理解获得。在过去，密码学用于重要的交流活动中，如间谍活动和反间谍活动之间，或外交官和总部联系之间等。密码学方法分为两类：一类叫隐写术（steganography），另一类叫密码编码学。前者是将秘密信息隐藏在大量无用的信息当中，信息的冗余度较大，后者是通过各种文本转换的方法使得信息为外部不可理解。本文所涉及到的密码学是指密码编码学，以下称为密码学。

现代密码学是一门跨多学科，涉及理论、工程面广的复合型科学。它可以被看作是信息论理论，使用了大量的数学领域的工具，如众所周知的数论和有限域知识。密码学也可以说是工程学的一个分支，不同的是它必须应对一些活动频繁、高度智慧、怀有恶意的敌人的攻击。早期的密码学采用两种方法：把给定信息的字母打乱顺序进行重排，或者使用一组字母替换另一组字母，如著名的恺撒密码和Hill密码，进行这种操作需要一个密码本（code book）。现代的密码学，由于使用了计算机对信息进行处理，所以与传统的密码编码学有了很大的不同，操作的对象从以前的字母或者文字变成了计算机内部表示的0,1序列;通信双方进行交互传递的信息也不再是字母或者文字，而是可以被计算机理解的0，1序列。近几十年来，随着计算机和网络的普及，密码学取得了惊人进展，它的使用范围和功能越来越广，从保密性和认证性，扩充到了匿名性、不可否认性等等。

2.2 密码体制

密码体制是信息安全的基石。原始的未被处理过的信息，称为明文（plaintext），被保护后的明文，称为密文（ciphertext）。将明文转换成密文（plaintext），被保护后的明文，称为密文（ciphertext）。将明文转换成密文

这一过程称为加密（encryption / enciphering）操作，反之称为解密（decryption / deciphering）操作。加、解密操作中所使用的类似于钥匙的额外附加信息，分别称为加密密钥、解密密钥。把明文加密成密文的具体步骤和方法，称为加密算法，反之称为解密算法。一般而言，加解密算法是公开的，而保密性是基于对密钥访问的约束。加、解密算法的有机结合构成了密码体制，密码体制分为私钥密码体制和公钥密码体制。

1．私钥密码体制

加密密钥和解密密钥是相同的，或者两者之间容易互相导出的密码体制，称为私钥密码体制，也称为对称密码体制。在这种系统中，加密密钥或者解密密钥暴露将会使得整个加密体制被攻破。因此，私钥系统密码的一个严重缺陷就是在任何密文传输之前，会话通信的双方必须使用一个严格安全的信道预先协商加、解密密钥。在实际中，达到这一点是很难的。在私钥密码体制中，使用最为广泛也最为著名的就是20世纪80年代公布的数据加密标准DES（Data Encryption Standard）和2000年公布的高级加密标准AES（Advanced Encryption Standard）。私钥密码体制的优点在于速度快，硬件实现比较容易，因为大部分的操作都是逻辑和置换。在现实生活中，银行的ATM机一般都使用DES加密体制。

2．公钥密码体制

加密密钥和解密密钥是不同的，且两者之间难于互相推导的密码体制，称为公钥密码体制，也称为非对称密码体制。公钥密码体制既可用于加密又可用于数字签名，数字签名可以为每个人确定一个身份，而不需要使用传统的手工签名等方法来鉴别和证明身份，这是公钥密码体制的一个伟大创新。公钥密码体制的思想提出以后，各种算法的加密体制和数字签名方案纷纷出台。其中最著名的是由Rivest, Shamir和Adleman在1978年提出的RSA体制[14]。RSA体制是一种基于数论中大素数分解的困难性的公钥密码体制，是历史最悠久、应用最广泛的公钥密码体制。另外就是基于离散对数求逆困难性问题建立起来的ElGamal体制和椭圆曲线密码体制（ECC）。公钥密码体制的优点在于安全性和应用广泛性，但缺点是运算速度太慢，不适合直接用于对原始信息的加密和签名。在现实中，公钥密码体制的应用已经十分非常广泛，如PEM（Privacy Enhanced Mail）、S-MIME、PGP、X.509等。

综合私钥密码体制和公钥密码体制各自的优缺点，在密码学的解决方案中经常使用公钥密码体制来保护私钥密码体制中所使用到的加密密钥，如

Diffie-Hellman 密钥交换算法，而在签名的解决方案中则引进了 Hash 函数，只对签名信息的 Hash 结果（固定长度的信息，称为消息摘要）进行签名操作。

2.3 数字签名

2.3.1 数字签名技术

一个数字签名方案至少应满足以下三个条件：

(1) 签名者事后不能否认自己的签名，而任何其他人都不能伪造签名；

(2) 接受者能验证签名；

(3) 当双方关于签名的真伪发生争执时，第三方能解决双方之间发生的争执。

根据数字签名标准 DSS，数字签名的步骤一般有以下几步：

步骤 1：发送方用一个 Hash 函数（如 SHA-1 或 MD5 算法）对消息进行处理，形成一个固定长度的消息摘要 m_1；

步骤 2：发送方用自己的私钥对消息摘要 m_1 进行数字签名计算，生成数字签名；

步骤 3：将数字签名和原始消息一起发送给接收方；

步骤 4：接收方用同样的 Hash 函数作用于接收到的原始消息，生成消息摘要 m_2；

步骤 5：接收方用发送方的公钥解密数字签名得到消息摘要 m_1'，与消息摘要 m_2 对比，二者相同则通过该数字签名的验证，否则该数字签名验证失败。

2.3.2 数字签名技术与加密技术的结合

在实际应用中，如果信息是公开的，仅要求不可伪造（如网页信息），则可利用数字签名技术来保证信息的完整性和不可伪造性。如果信息是保密的（如 E-mail、电子商务等），则不仅要保证其完整性，还要保证其秘密性，此时需要信息加密技术与数字签名技术同时使用。一般工作过程如下：

发送方 *A*

(1) 形成发送消息 *P* 的消息摘要 *m*，并用私钥对此摘要加密生成 *Cm*；

(2) 将消息 *P* 与 *Cm* 一起用对称密钥加密生成 *Cp*；

(3) 用接收方 B 的公钥加密对称密钥生成 Ck;

(4) 将 Cp 和 Ck 一起发送给接收方 B。

接收方 B 接收到消息后

(1) 用私钥解密 Ck，得到对称密钥;

(2) 用对称密钥解密 Cp，得到消息 P 和加密后的摘要 Cm;

(3) 用同样的 Hash 函数生成消息 P 的摘要 m'，并用发送方 A 的公钥解密 Cm 得到 m，比对 m 和 m'，若二者相等则说明消息 P 正确。

2.3.3 一种增强的代理多重数字签名方案

1. 基本概念

(1) 代理签名[15]：在一个代理签名方案中，一个被指定的代理签名者可以代表原始签名者生成有效的签名。

(2) 多重代理签名[16]：在一个多重代理签名方案中，多个原始签名人分别将签名权委托给各自的代理签名者，多个代理签名者可以代表各自的原始签名者生成有效的签名。

(3) 代理多重签名[16]：在一个代理多重签名方案中，多个原始签名人将各自的签名权委托给同一个代理签名者，此代理签名者可以同时代表多个原始签名者生成有效的签名。

2. Qi 和 Harn 的代理多重数字签名方案[17]。

安全参数：p、q 为大素数，且 $q|(p-1)$，$g \in Z_p^*$ 是一个 q 阶元，h 是一个安全的 Hash 函数，设 A_i 是若干原始签名人，B 为代理签名人，其身份标识号分别为 $ID_{A_1},...,ID_{A_n},ID_B$。每一位原始签名人和代理签名人的私钥分别为 x_i，$x_B \in [1, p-1]$，公钥为 $y_i = g^{x_i} \bmod p$，$y_B = g^{x_B} \bmod p$。

授权过程

设 m 为待签名的消息。

(1) 每个 A_i 随机选取 $k_i \in [1, p-1]$，并计算 $K_i = g^{k_i} \bmod p$，公开 K_i，从而每个 A_i 都可以计算

$$K = \prod_{i=1}^{n} K_i \bmod p, \quad s_i' = Kk_i + ID_B x_i \bmod q (i = 1,2,...,n)$$

A_i 送代理子密钥 (K_i, s_i', ID_B) 给 B。

(2) B 取得 (K_i, s_i', ID_B) 后验证授权方程

$$g^{s_i'} = K_i^K y_i^{ID_B} \bmod p \tag{2-1}$$

如果(2-1)式成立，接收(K_i, s_i', ID_B)，否则拒绝接收(K_i, s_i', ID_B)。

签名过程

B选取随机数$t \in [1, p-1]$，并计算

$$s_i = s_i' x_B^{-1} \bmod q,\quad s = \sum_{i=1}^{n} s_i \bmod q,\quad u = y_B^t \bmod p,\quad v = t + sh(m,u) \bmod q,$$

$$y_G = \prod_{i=1}^{n} y_i \bmod p$$

s作为代理签名的密钥，B送(u, v, ID_B, m)给签名验证者 V。

代理签名验证过程

V接收到(u, v, ID_B, m)后，计算$K = \prod_{i=1}^{n} K_i \bmod p$，$y_G = \prod_{i=1}^{n} y_i \bmod p$，并验证验证方程

$$u = y_B^v [(K^K y_G^{ID_B})^{-1}]^{h(m,u)} \bmod p \qquad (2\text{-}2)$$

如果(2-2)式成立，V接收(u, v, ID_B, m)，否则拒绝接收(u, v, ID_B, m)。

3．Wang和Fu构造的伪造攻击及其方案改进[18]

设n个原始签名人中A_i企图伪造一个有效的代理多重签名。A_i作如下操作：

(1) A_i随机选取x_i，$k_i \in [1, p-1]$，并计算

$$y_i = y_B^{x_i} \prod_{j=1, j\neq i}^{n} y_j^{-1} \bmod p,\quad K_i = y_B^{k_i} \prod_{j=1, j\neq i}^{n} K_j^{-1} \bmod p$$

并公布y_i是他的公钥。其中$y_1, y_2, \cdots, y_{i-1}, y_{i+1}, \cdots, y_n$是$A_1, A_2, \cdots, A_{i-1}, A_{i+1}, \cdots, A_n$的公钥。

(2) A_i随机选取$t \in [1, p-1]$，并计算

$$K = \prod_{i=1}^{n} K_i \bmod p,\quad u = y_B^t \bmod p,\quad v = t + (x_i ID_B + Kk_i) h(m,u) \bmod q$$

A_i假冒B送伪造的签名数据(u, v, ID_B, m)给签名验证者 V。

(3) V接收到(u, v, ID_B, m)后，计算$K = \prod_{i=1}^{n} K_i \bmod p$，$y_G = \prod_{i=1}^{n} y_i \bmod p$，并验证验证方程(2-2)式，伪造的$(u, v, ID_B, m)$能使(2-2)式成立，其原因为

$$y_G = \prod_{i=1}^{n} y_i = y_1 \cdots y_{i-1} (y_i' \prod_{j=1, j\neq i}^{n} y_j^{-1} \bmod p) y_{i+1} \cdots y_n = y_B^{x_i} \bmod p,$$

$$K=\prod_{i=1}^{n}K_i=K_1...K_{i-1}(K_i'\prod_{j=1,j\neq i}^{n}K_j^{-1}\bmod p)K_{i+1}...K_n=y_B^{k_i}\bmod p,$$

$$y_B^{v}=y_B^{t}(y_B^{x_iID_B}y_B^{Kk_i})^{h(m,u)}=u(y_G^{ID_B}K^{K})^{h(m,u)}\bmod p$$

则(2-2)式成立。因此，伪造的签名(u,v,ID_B,m)能通过验证方程的验证。

为了避免上述伪造攻击，文献[18]对文献[17]方案进行了改进，增加一个代理签名管理中心CA，由CA对原始签名人的公钥进行验证，避免了原始签名人可能的伪造攻击。限于篇幅考虑，该改进方案在此不再赘述。

4．改进的代理多重数字签名方案

在Qi和Harn的方案中，伪造攻击有效的主要原因是在验证方程中可求出表达式

$$y_i=f(\prod_{j=1,j\neq i}^{n}y_j^{-1}),\qquad k_i=f(\prod_{j=1,j\neq i}^{n}k_j^{-1})$$

使得$y_G=y_B^{x_i}, K=y_B^{k_i}$就可以避开验证方程中所包含的代理签名人的私有信息通过验证。根据以上分析，本文提出的改进方案如下。

安全参数：p、q为大素数，且$q|(p-1)$，$g\in Z_p^*$是一个q阶元，h是一个安全的Hash函数，设A_i是若干原始签名人，B为代理签名人，其私钥分别为x_i，$x_B\in[1,p-1]$，公钥分别为$y_i=g^{x_i}\bmod p$，$y_B=g^{x_B}\bmod p$。公开委任状w_i是A_i将签名权利委托给B的文件，它明确了A_i与B之间的代理关系，$w_i=(ID_{A_i},ID_B,T,Scope,etc)$，其中$ID_{A_1},...,ID_{A_n}$是$A_i$的身份，$ID_B$是$B$的身份，$T$是授权证书的有效期，$Scope$是授权范围，$etc$是其他的相关参数。

授权过程

设m为待签名的消息。

(1) 每个A_i随机选取$k_i\in[1,p-1]$，并计算

$$K_i=g^{k_i}\bmod p,\quad e_i=h(y_i,w_i),\quad s_i'=K_ik_i+x_ie_i\bmod q(i=1,2,...,n)$$

A_i送代理子密钥(K_i,s_i',w_i)给B。

(2) B取得(K_i,s_i',w_i)后验证授权方程

$$g^{s_i'}=K_i^{K_i}y_i^{e_i}\bmod p \tag{2-3}$$

如果(2-3)式成立，接收(K_i,s_i',w_i)，否则拒绝接收(K_i,s_i',w_i)。

签名过程

B选取随机数$t\in[1,p-1]$，并记录时间戳T_B，之后计算

$$s=x_B^{-1}\sum_{i=1}^{n}s_i' \bmod q,\quad u=y_B^t \bmod p,\quad v=t+sh(m,u,T_B) \bmod q$$

s作为代理签名的密钥，B送代理签名数据$(ID_{A_1},...,ID_{A_n},u,v,T_B,m)$给签名验证者$V$。

代理签名验证过程

V接收到$(ID_{A_1},...,ID_{A_n},u,v,T_B,m)$后，在原始签名人公开信息处取得委任状$w_i$，核对$m$以及代理签名人的身份是否在所有委任状的集合$(w_1,w_2,...,w_n)$许可的范围内，如有任何一条不符，拒绝接收$(ID_{A_1},...,ID_{A_n},u,v,T_B,m)$，否则计算$e_i$后验证验证方程

$$y_B^v=u[\prod_{i=1}^{n}K_i^{K_i}\prod_{i=1}^{n}y_i^{e_i}]^{h(m,u,T_B)} \bmod p \tag{2-4}$$

如(2-4)式成立，V接收$(ID_{A_1},...,ID_{A_n},u,v,T_B,m)$，否则拒绝接收$(ID_{A_1},...,ID_{A_n},u,v,T_B,m)$。

5．安全性分析与讨论

(1) 攻击分析

1) 由于在授权方程中含有原始签名人的私有信息，所以任何人不可能在截取代理子密钥后冒充原始签名人A_i进行非法授权；

2) 由于在验证方程中包含有所有原始签名人的私有信息，所以任何人包括代理签名人不可能在没有得到原始签名人A_i合法授权情况下，进行非法代理；

3) 反之，原始签名人A_i不可抵赖合法的授权；

由于代理签名及验证方程中所包含的代理签名人B的私有信息x_B，可以有效地保证代理签名由代理签名人B发出，如果攻击者欲伪造签名来通过验证，其计算难度等价于离散对数的分解难度，所以本方案可有效抵御4) 5)；

4) 原始签名人的合谋攻击；

5) 攻击者截获代理子密钥后冒充代理签名人B伪造代理签名；

6) 显然本方案可有效的抵御文献[18]所提出的伪造攻击；

7) 反之代理签名人B也不能对合法的代理多重数字签名进行抵赖；

8) 由于引入了委任状w_i，原始签名人就可对代理签名人B的签名能力进行限制，可以通过w_i明确B只能在一定的有效期、一定的范围内参与多重签名，V不接受超出权限的签名。一旦超出有效期，代表原始签名人收回代理签名权。这样，避免了B滥用签名权力，对原始签名人是公平的。

9) 由于在代理签名过程中系统加入了时间戳 T_B，可以让验证用户能够检测该签名的时间信息，有效抵御重复攻击。

(2) 任何人可验证代理多重签名的有效性。因为有

$$y_B^v = y_B^{r+sh(m,u,T_B)} = y_B^r[g^{x_B x_B^{-1}(\sum_{i=1}^{n} K_i k_i + x_i e_i)}]^{h(m,u,T_B)} = u[\prod_{i=1}^{n} K_i^{K_i} \prod_{i=1}^{n} y_i^{e_i}]^{h(m,u,T_B)} \bmod p$$

(3) 无需引入第三方，对整个系统实现而言，减少了不安全因素。

通过以上分析可知，新方案是一个增强的代理多重数字签名体制，满足以下性质：

1) 可验证性：任何验证人都可以验证代理多重签名是否有效；根据有效的代理多重签名，确认所有原始签名人都承认已经签名过的文件；

2) 强不可伪造性：因为代理多重签名包含代理签名人的私有信息，除了代理签名人之外的任何其他人都无法伪造代理签名；

3) 强身份证实性：因为代理多重签名中包含代理签名人的公钥，任何人可以从代理签名中确认参与的代理签名人身份；

4) 强不可抵赖性：任何一个原始签名人和代理签名人都不能否认一个由他们参与生成的代理多重签名。

综上所述，此方案在不引入可信任第三方的前提下，对文献[17]提出的代理多重数字签名方案进行了改进，有效的克服了文献[18]提出的攻击方法，不但保留了文献[17]的代理多重数字签名方案的优点，而且在授权时效、范围和加入代理签名的时间信息等方面有所加强，可以更加安全有效地实现由一个代理签名人生成代表多个原始签名人的代理签名的目的。同时，无需引入第三方以及验证方程中无需为求逆而作大量的计算使得本方案更加简洁实用。我们认为，这种签名方案在电子商务和网络安全通信方面有广泛的应用前景，可用于构造具有良好性质的公平交换协议，电子选取协议等。

第3章 安全协议形式化分析方法

计算机网络正以惊人的速度向各个领域渗透，成为各领域发展的新源泉，各种现实世界里的组织与系统正在走进网络这个虚拟的世界，使网络世界变得更加精彩；与此同时，安全问题也变得日益突出、复杂，解决安全问题对许多网络应用来说已是头等大事。从目前解决安全问题的方式来看，安全协议是最有效的手段之一。它可以有效地解决以下一些重要的安全问题：源认证和目标认证、消息的完整性、匿名通信、抗拒绝服务、抗抵赖、授权等。另一方面，随着网络技术的飞速发展，多播技术已不断走向成熟，由多播应用带动的安全问题也变得更加复杂，为解决这些问题也是通过一种称为群协议的安全协议来完成的。目前研究热点之一的多主体系统中的安全主体问题，在很大程度上也是依靠有效的安全协议的设计来完成的。可见，安全协议是一个十分重要的研究课题。

尽管安全协议是保护信息系统安全的有效手段之一，但是安全协议自身安全性的分析却是一个非常困难的问题。目前已经有多种研究安全协议的理论与方法，如形式化分析方法、可证明安全理论、零知识证明理论等。本章主要综述安全协议形式化分析的理论与方法。为了便于更好地理解这些理论和方法的应用背景，首先对安全协议的一些基本问题作一简要概述。

3.1 安全协议

3.1.1 基本概念

1. 协议

协议是一系列的规则和协定，它们被用于定义两个或两个以上的参与者之间的一个通信框架。就是两个或两个以上的参与者采取一系列步骤以完成某项特定的任务。由此可知协议至少应该具有如下基本性质[19]：

(1) 协议的参与者不能少于两个，一个人可以通过执行一系列的步骤来完成一项任务，但它不构成协议；

(2) 协议包含一系列的消息接收和消息发送行为，参与者还可能会对消

息进行内部处理；

(3) 协议是有目的的事件，参与各方希望通过执行协议达到一个目的，可能是交流秘密信息，也可能是确认身份等；

(4) 协议的成功依赖于参与各方遵守规则的参与执行，任何一方破坏规则都将导致协议无法顺利完成。

2．安全协议

安全协议也叫密码安全协议，或者密码协议，就是在消息处理环节采用了若干密码算法的协议。

安全协议运行过程之中的参与者，称为主体，这里的主体的概念很广泛，可能是人，也可能是一个程序，或者是一个服务器。协议的运行由一些相互独立的有先后顺序的动作序列和步骤构成，这种独立的动作序列被称为一个角色或者身份。每个角色的功能是独立的，但相互之间是关联的、交互的，比如发起者、响应者等等。在协议中，主体与角色的概念是不尽相同的，一个主体可能就代表一个角色，同样也可能扮演多个角色和身份。从发起者发起一个协议开始，到最终协议的结束，称为协议的一轮运行。一轮协议的运行当中所涉及到的参与者的数目，或者角色不一定恰好符合安全协议的规定，其中那些破坏协议的正常运行，或者不遵守协议规定步骤的参与者称为攻击者（或者叫做攻击者角色），其他的参与者称为诚实参与者（或者叫做诚实角色）。协议的一个参与者 A（这里也可以使用主体或者角色代替）向另外一个参与者 B（这里也可以使用主体或者角色代替）传递一个消息，称 A 的动作为发送，B 的动作为接收，A 称为消息的发送者，B 称为消息的接收者。一个安全协议 P 在运行过程中，假如有攻击者（攻击角色）存在，并且没有被系统或者诚实角色所察觉，同时攻击者在参与过程之中并没有利用任何密码学上的漏洞，称安全协议 P 被攻破，即安全协议 P 存在设计上的漏洞。

3．安全协议与算法的区别和联系

协议与算法的概念是不尽相同的。算法应用于协议中消息处理的环节，协议对不同的消息处理方式则要求用不同的算法，而对算法的具体化则可定义出不同的协议类型。由此可见，密码算法和安全协议处于网络安全体系的不同层次，是网络数据安全的两个主要内容。具体而言，密码算法为网络上传递的消息提供高强度的加解密操作和其他辅助算法（如 Hash 函数），而安全协议是在密码算法的基础上，为各种网络安全性方面的需求提供实现方案。

安全协议是一门跨领域、跨学科的科目，涉及到许多领域的知识。密码学是安全协议的学科基础，如果密码体制被破解则安全协议将会随之被破解而变得毫无意义。一般情况下我们认为在安全协议中使用的加密算法是安全的、不会被破解的，加密算法对于安全协议而言被看作是一个黑盒子，它提供对通信协议信息处理环节的加密解密操作。现实的网络提供安全协议运行所需要的环境，然而，网络的不稳定和不可靠，或者低质量又会影响安全协议的实际使用效果。安全协议是一门艺术的科学，设计安全协议绝非简单的工作，它需要精确的和复杂的科学思维。安全协议涉及大量数学领域的知识，安全协议目标的精确和标准的定义必须要借助于数学语言的描述和刻画，对安全协议的形式化分析同样必须借助数学的模型和手段。安全协议也可以看作是一门工程的科学，不同的是它必须应对一些活动频繁的、高度智慧的、怀有恶意的敌人的攻击，我们所指的攻击不是针对密码学体制的攻击，而是针对安全协议设计本身漏洞的发现和查找。

4．安全协议的功能

随着网络的高度发展和普及以及电子商务和电子政务的蓬勃兴起，安全协议的作用变得越来越重要，功能变得越来越强大。早期的安全协议的目标主要是两个方面，即信息的保密性和身份的认证性。保密的目的是防止机密信息在传送过程中被对手破译，保密性常常被用于传递秘密信息的事务当中。认证的目的有两个：一是验证信息的发送者是确定的和真正的，而不是未知的、假冒的；二是验证信息的完整性，在信息的传送或存储过程中未被篡改、重放或延迟等。在许多情况下，认证性协议都包含着保密性的附加目标，即在主体之间安全地分配密钥或其他各种秘密。认证性常被用于网络上的身份识别事务当中。现在的安全协议的目标已经多种多样，比如，非否认性、匿名性和公平性等。非否认性隐含两层意思：一个是信息发送方的非否认性（non-repudiation of origin），即非否认协议向接收方提供不可抵赖的证据，证明收到消息的来源的可靠性；另一个是信息接收方的非否认（non-repudiation of receipt），即非否认协议向发送方提供不可抵赖的证据，证明接收方已收到了某条消息。非否认性常被用于电子签名和电子政务活动当中。匿名的目的是确保参与者在参与协议的过程中不泄露任何有关自己身份和其他方面的信息，匿名性常被用于电子交易和电子商务活动当中。公平的目的在于确保协议参与各方的地位和作用平等，参与各方所拥有的能力也是相同的，公平性常被用于电子选举和电子投票事务当中。

5．安全协议的分类

在网络通信中最常用的、最基本的安全协议按照其目的可以分成以下4类：

(1) 密钥交换协议。这类协议用于完成会话密钥的建立。一般情况下是在参与协议的2个或者多个实体之间建立共享的秘密，如用于1次通信中的会话密钥。协议中的密码算法可采用对称密码体制，也可以采用非对称密码体制。

(2) 认证协议。认证协议包括实体认证（身份认证）协议、消息认证协议、数据源认证协议和数据目的认证协议等，用来防止假冒、篡改、否认等攻击。

(3) 认证密钥交换协议。这类协议将认证协议和密钥交换协议结合在一起，先对通信实体的身份进行认证，在认证成功的基础上，为下一步安全通信分配所使用的会话密钥，它是网络通信中应用最普遍的一种安全协议。常见的认证密钥交换协议有互联网密钥交换（IKE）协议、分布式认证安全服务（DASS）协议、Kerberos认证协议[20]、X.509协议[21]等。

(4) 电子商务协议。与上述协议最为不同的是，电子商务协议中主体往往代表交易的双方，其利益目标是不一致的，或者根本就是矛盾的。因此，电子商务协议最为关注的就是公平性，即协议应保证交易双方都不能通过损害对方利益而得到它不应得的利益。常见的电子商务协议有SET协议，IKP协议等。

Clark和Jacob在文献[22]中按安全协议所用的密码算法对其进行了分类，列举了一系列有研究意义和实用价值的安全协议。他们将现有的安全协议进行了如下的分类：

(1) 无可信第三方的对称密钥协议。属于这一类的典型协议包括以下的ISO系列协议[23]：ISO对称密钥on-pass和two-pass单方认证协议、ISO对称密钥two-pass双方认证协议、ISO对称密钥three-pass双方认证协议，还有Andrew安全RPC协议[24]等。

(2) 应用密码校验函数（CCF）的认证协议。属于这一类的典型协议包括以下ISO系列协议[25]：ISO应用CCF的on-pass和two-pass单方认证协议、ISO应用CCF的two-pass双方认证协议、ISO应用CCF的three-pass双方认证协议。

(3) 具有可信第三方的对称密钥协议。属于这一类的典型协议包括NS私钥协议[26]、Otway-Rees协议[27]、Yahlom协议[2]、大嘴青蛙协议[2]、Denning-Sacco协议[29]、Woo-Lam协议[30]。

(4) 对称密钥重复认证协议。属于这一类的典型协议有Kerberos协议版本5、Neuman-Stubblebine协议[31]、Kao-Chow重复认证协议[32]等。

(5) 无可信第三方的公开密钥协议。属于这一类的典型协议包括以下ISO系列协议[33]：ISO公开密钥on-pass和two-pass单方认证协议、ISO公开密钥two-pass双方认证协议、ISO公开密钥three-pass双方认证协议、ISO公开密钥two-pass并行双方认证协议，还有Diffie-Hellman协议[34]等。

(6) 具有可信第三方的公开密钥协议。属于这一类的典型协议有NS公钥协议[26]、TMN密钥分发协议[35]等。

3.1.2 安全协议系统模型

如果将协议及其所处的环境视为一个系统，那么在这个系统中，一般而言包括发送和接收消息的诚实的主体和一个攻击者，以及用于管理消息发送和接收的规则。协议的合法消息可被攻击者截取、重放和篡改。攻击者将所有已知的消息放入其知识集合KS（Knowledge Set）中。诚实主体之间交换的任何消息都将被加入到攻击者的KS中，并且，攻击者可对KS中的消息进行操作，所得消息也将加入到其KS中。攻击者可进行的操作至少包括级联、分离、加密和解密。一个被动攻击者可在线窃听敏感信息，而一个主动攻击者则可截获数据包，并对其进行任意的修改，甚至可以伪装成通信主体，欺骗诚实主体与其进行非法通信。加密运算可以有效地阻止主动入侵，因为在不知道密钥的前提下，对密文消息的丝毫改动都将导致解密运算的失败，此时攻击者能做的仅仅是阻止消息送达或准时送达其目的地。归纳起来，攻击者的行为表现为以下几种形式：

(1) 将消息发送到其意定接收者；

(2) 延迟消息的送达；

(3) 将消息篡改后转发；

(4) 将消息与以前接收的消息合并；

(5) 改变部分或全部消息的目的地址；

(6) 重放消息。

在认证系统中，假设每一个主体与可信服务器之间共享一个秘密密钥，密钥是通过离线方式建立的。当两个主体要进行秘密通信时，它们要建立一个仅为其所知的秘密密钥，这个秘密密钥的作用相当于一个秘密通道，不知道密钥的攻击者无法干扰通信。

综上所述，我们使用以下几个主要部分来刻画安全协议的系统环境模型：诚实的参与者（包括个人、可信服务器、组织等），诚实参与者的能力（发送和接收消息，以及对消息进行加密和解密运算），攻击者（包括个人、程序、组织等），攻击者能力（上面所描述的六种能力），加密体制（包括公钥体制和私钥体制），网络通信实体，全局时钟，明文消息空间，密文消息空间。任何一种研究分析安全协议的方法都必须要对上述要素进行考虑，并给出具体的描述或者假定。

3.1.3 安全协议的安全性质及实现

安全协议的主要目的是通过协议消息的传递来实现通信主体身份的识别与认证，并在此基础上为下一步的秘密通信分配会话密钥。因此，对通信主体双方身份的认证是基础、是前提。而且在认证的过程中，对关键信息的秘密性及完整性的要求也是十分必要的。另外，作为与认证协议不同的另一类协议—电子商务协议，由于其自身的特点，也有一些特殊的性质要求。简单的说，安全协议的目的就是保证安全性质在协议执行完成时能够得以实现，换言之，评估安全协议的安全性就是检查其安全性质在协议执行时是否受到破坏。协议的安全性质包括：

1．认证性

认证性是最重要的安全性质之一，是分布式系统中的主体进行身份识别的过程，所有其他的安全性都依赖于此。在协议中，当某一成员（声称者）提交一个主体身份并声称它是那个主体时，需要运用认证以确认其身份是否如其声称所言，或者声称者需拿出证明其真实身份的证据，这个过程称为认证的过程。

安全协议的实体认证可以是单向的也可以是双向的，其实现是基于密码体制的，具体有以下几种方法：

(1) 声称者使用仅为其与验证者知道的密钥封装消息，如果验证者能够成功解密消息或验证封装是正确的，则声称者身份得到证实；

(2) 声称者使用其私钥对消息签名，验证者使用声称者的公钥验证签名，

如正确，则声称者身份得到证实；

(3) 声称者通过可信第三方来验证自己。

上述方法中所传递的消息都应包含不可重复值以抗重放攻击，它们往往被综合使用以建立可靠的认证系统。

2. 秘密性

秘密性的目的是保护协议消息不被泄漏给未被授权拥有此消息的人，即使是攻击者观测到了消息的格式，它也无法从中得到消息的内容或提炼出有用的消息。保证协议消息秘密性最直接的方法是对消息进行加密。加密使得消息由明文变为密文，并且任何人在不拥有密钥的情况下是不能解密消息的。公钥加密体制的密钥管理更为简单，而私钥加密体制的执行效率更高，并且在同一类体制中，不同的密码算法有不同的强度和代价。安全协议一般并不考虑具体的密码算法的执行细节，但在实际应用中这往往有可能造成协议秘密性的缺陷。

3. 完整性

完整性的目的是保护协议消息不被非法篡改、删除和替代。最常用的方法是封装和签名，即使用 Hash 函数或加密的方法产生一个明文的摘要（完整性校验值 ICV）附在传送的消息上，作为验证消息完整性的依据。关键的问题是，通信双方必须事先达成有关算法选择项的共识。如果被保护的消息有一定的冗余，加密消息的冗余则能保证消息完整性。因为如果一个攻击者不知道机密密钥而修改了密文的一部分，则会导致在解密过程中产生不正确的结果。在 SSL 握手协议、IKE 协议等操作性较强的协议的消息交换中就涉及保护协议消息完整性的具体实现细节。

4. 非否认性

非否认性是电子商务协议的一个重要的性质。非否认协议的主体可收集证据，以便事后能够向仲裁证明对方主体的确发送了或接受了某个消息，以保证其自身合法利益不受侵害，即协议主体必须对自己的合法行为负责，不能也无法事后否认。证据一般是以签名消息的形式出现的，从而对消息与消息的发送者进行了绑定。而要达成非否认这一目标，协议必须具有以下两个特点：一证据的有效性；二交易的公平性。此外电子商务协议的一些其它的相关性质有：适时中止性、公平性、可追究性等。

3.1.4 安全协议的设计原则及缺陷

许多安全协议只包含为数不多的几条消息传递，其中每一条消息都是经过巧妙设计的，消息之间存在着复杂的相互作用和制约；同时，安全协议中经常会使用多种不同的密码体制，这样就导致安全协议非常复杂、精致，更有可能存在着无法估计和判断的安全缺陷（安全漏洞）。造成安全协议存在安全缺陷的原因主要有两个：一是协议设计者误解或者采用了不恰当的技术；二是协议设计者对环境要求的安全需求研究不足。从来源上讲，安全协议存在安全缺陷的原因可分为两类：一类是由于设计时不规范引发的；一类是在具体执行时产生的。如果能在协议设计阶段就充分考虑一些不当的协议结构有可能造成的协议安全性的破坏从而避免不必要的协议错误，将是事半功倍的。Martin Abadi 和 Roger Needham 提出了设计协议应遵循的原则，归纳起来涉及以下几个方面：

(1) 消息独立完整性原则；

(2) 消息前提准确原则；

(3) 主体身份标识原则；

(4) 加密目的原则；

(5) 随机数的使用原则；

(6) 签名原则；

(7) 时戳的使用原则；

(8) 编码原则。

尽管协议设计者在协议设计时尽可能回避错误，但是安全协议在实际应用中仍会出现各种类型的缺陷，并且产生的原因十分复杂，很难有一种通用的分类方法将安全协议的安全缺陷进行分类。Gritzalis 和 Spinellis[19]根据安全缺陷产生的原因和相应的攻击方法把安全协议的缺陷分为如下六类：

(1) 基本协议缺陷：是指在安全协议的设计中没有采取或者只采取很少防范攻击者攻击的措施，文献[36]中的认证密钥交换协议存在这种安全缺陷；

(2) 口令/密钥猜测缺陷：这类缺陷产生往往是因为用户从一些常用的单词、词组中选择他的密钥/口令，从而导致攻击者能够采取字典攻击的手段进行口令猜测攻击；另外的可能是因为用户选取了不安全的伪随机数生成算法构造密钥，使得一些强大的攻击者能够恢复该密钥，文献[37-41]中协议可能存在这种安全缺陷；

(3) 陈旧消息缺陷：主要由于在安全协议设计时没有充分考虑消息的时间相关性，从而使攻击者能够进行消息重放攻击，包括消息源的攻击、消息目的的攻击等等，文献[42]中的协议已经被发现存在这种安全缺陷；

(4) 并行会话缺陷：也叫应答机会话缺陷、多角色漏洞，主要是由于攻击者可以通过交换适当的消息从而获得他真正想得到的消息，文献[41]中给出了存在这种缺陷的协议范例；

(5) 内在性缺陷：由于协议的消息可达性存在问题，安全协议的参与者中至少有一方不能够完成所有必须的动作而导致的一种协议缺陷，文献[42]中给出了存在这种缺陷的协议范例；

(6) 密码体制缺陷：这是一种根本性的安全协议缺陷，因为安全协议的可靠性在很大程度上就依赖于密码算法的安全和可靠，如果安全协议中所使用的密码算法存在根本性缺陷，则必将导致协议参与各方之间所有交互的加密消息都可能会被解密，由此造成攻击者可以非常容易或者有很大可能的充当合法的角色参与协议，欺骗诚实的角色。

3.2 安全协议的形式化分析

安全协议的安全性是一个很难解决的问题，前面已经指出，安全协议的运行不是独立的，而是处于某种不安全的环境之中的，因而它是容易出错的，并且错误很难完全由人工识别。许多事例已经向我们表明，即使在设计一个安全协议时对运行环境做了最为充分的估计，并且很小心仔细地进行了设计，而且使用了很多年，但依然包含一些微妙的漏洞没有被发现。

安全协议分析的困难性在于：

(1) 安全目标本身的微妙性和不确定性。例如，表面上十分简单的“认证性目标”就十分微妙，关于认证性的定义，至今存在各种不同的观点；

(2) 协议运行环境的复杂性。实际上，当安全协议运行在一个十分复杂的公开环境时，攻击者处处时时都存在。我们必须形式化地刻画安全协议的运行环境，这当然是一项艰巨的任务；

(3) 攻击者模型的复杂性。我们必须形式化地描述攻击者的能力，对攻击者和攻击行为进行分类和形式化的分析；

(4) 安全协议在实际运行中的异常复杂性。因为在很多时候，多轮协议是并发执行的，同一个主体在这些协议中又会充当不同的角色。

以上四点原因使得安全协议的分析变得更加复杂并具有挑战性。从安全协议的分析和设计角度来看，我们必须要对协议的安全性作出理论的分析，并借助于一些自动化的工具来完成安全协议安全性的分析和证明。20年来为了应对这一挑战，科学家们投入了大量的精力设计开发了不同种类的研究理论与方法，比如形式化方法、可证明安全理论、零知识证明理论等等，其中以形式化分析方法的成果最为显著和突出，其发展前景被安全领域的专家们普遍看好。

3.2.1 安全协议形式化分析的历史及现状

1．安全协议形式化分析的历史

如前所述，在安全协议安全性的分析和证明方面，形式化的分析方法的成果最为显著和突出，其发展前景被安全领域的专家们普遍看好。安全协议形式化分析技术至今已有二十多年的历史，并日趋成熟，它已经成为了安全协议安全性研究的热点，有许许多多的理论和模型被构造出来。

安全协议形式化分析的思想由Needham和Schroeder[26]两人在1978年最先提出，同时他们为进行共享和公钥认证的服务器系统的实现建立了一个安全协议。1981年，Denning和Sacco在文献[29]中指出NS私钥协议的一个错误，人们开始关注安全协议的形式化分析。在这一领域具有里程碑意义的事情发生于20世纪80年代，Dolev和Yao发表了文章"On the Security of Public Key Protocols" [1]，它真正开始了使用形式化方法分析安全协议的历史，自此之后使用形式化的方法研究安全协议逐渐兴起。Dolev和Yao在他们的文章中开创性地给出了安全协议可以多步并发执行的形式化系统模型，在这个系统模型中，包含了那些可以对信息流进行恶意窃取、修改和删除的入侵者和不诚实的参与者，同时密码学算法被认为是完备的，在分析时仅仅把它看作是一个满足一些代数性质的黑盒子，即使是主动攻击者也无法通过密码学算法对安全协议进行攻击。紧接着，Dolev, Even和Karp开发研究出了一系列的多项式时间算法，使用这些算法来分析一个限制严格的安全协议簇。但遗憾的是，在随后的研究中发现它们可以分析的协议太有限，一旦稍许放宽对这个协议簇的限定都将使得协议的安全性变成不确定的问题，因此这方面的工作并未得到进一步的展开。随后，在Dolev-Yao模型及其变形的基础上发展了很多形式化分析安全协议的工具。它们大部分采用状态搜索的技术，即首先定义一个状态空间和安全协议的系统模型，然后进行在此模型内搜索

检测以确定是否存在一条路径对应于攻击者的一次成功的攻击。还有一些工具采用了归纳定理推证技术（简称定理证明）开发安全协议分析的通用工具，并取得了一定的研究成果，其中包括：Interrogator[5]、NRL 协议分析器[43]、Longley-Rigby 工具[44]，以及其他一些用来解决这个问题的形式化方法。这些早期的验证分析工具都曾成功地发现一些已有安全协议中存在的漏洞，而在这之前的人工的分析并没有能够发现这些漏洞的存在，如 NRL 协议分析器搜索的空间规模可以确保安全性，并成功地发现了 Simmons 的选择性广播协议[43]的缺陷，Longley-Rigby 工具发现了 Banking 协议的缺陷[44]等。

安全协议的形式化分析技术领域的神秘感一直到 1989 年才被打破，Burrows, Abadi 和 Needham 引入了逻辑的方法，提出了 BAN 逻辑[2]的概念，并逐渐引起了人们广泛的关注。BAN 逻辑采用了与状态搜索技术完全不同的方法，它是关于主体拥有的知识与信仰，以及用于从已有信仰推知新的信仰的推理规则的逻辑。这种逻辑通过对认证协议的运行进行形式化分析，来研究认证双方如何通过相互发送和接收消息的方式，从最初的信仰逐渐发展到协议运行最终要达到的目的—认证双方的最终信仰。BAN 逻辑的规则十分简洁和直观，因此易于使用。BAN 逻辑成功地对 NS 协议、Kerberos 协议等几个著名的协议进行了分析，找到了其中若干已知和未知的漏洞。BAN 逻辑的成功极大地激发了密码学家对安全协议形式化分析的兴趣，并导致许多安全协议形式化分析方法的产生。但是，由于逻辑的方法是对安全协议分析问题的一种更高层次上的抽象，所以在一般情况下它的能力要弱于状态搜索和定理证明技术。1989 年 GLowe 使用通用的模型检测工具 FDR 发现了 NS 公钥密码协议中存在着中间人攻击。在这之后，在 Dolev-Yao 模型及其变形的基础上结合使用状态搜索技术和定理证明方法的分析研究工作又取得了很大的进展，并不断涌现出一些新的形式化方法和工具，比如，1997 年 Paulson 提出的基于协议消息和事件的攻击结构方法注记的证明方法，也被称为 Paulson 归纳法[45]，1998 年由 Fabrega, Herzog 和 Gunman 三人提出的基于协议消息节点间一种偏序关系的可证安全的 Strand Space 模型[7,9,10]，以及 2002 年李先贤和怀进鹏提出的密码协议代数模型 CPA[28]。

文献[8]把安全协议形式化分析理论与方法的研究历史分为以下 4 个阶段：

（1）早期阶段。这一阶段的研究主要集中于对具体协议的观测、分析和研究；

(2) 形式化分析初期阶段。以 Dolev-Yao 的工作为标志，BAN 类逻辑以及 CKT5 等基于知识逻辑的有效应用，表明研究进入了以信仰逻辑为主体的时期；

(3) 转折阶段。以 G.Lowe 的著名论文“An attack on the Needham -Schroeder public key authentication protocol”[46]为标志，各种一般用途的模型检测方法被用于协议分析的研究；

(4) 理论证明阶段。以 1997 年 Paulson 的归纳方法[45]及 1998 年 Fabrega, Herzog 和 Guttman 的 Strand Space 理论[7,9,10]为代表，开始了安全协议形式化分析理论的发展时期。

2. 安全协议形式化分析的现状

虽然形式化分析已取得显著成绩，也是安全协议分析领域公认最有前景的方法，但就其自身而言，形式化分析技术仍是有局限性的。这是因为协议系统的运行不是独立的，而是处于某种环境之下的，系统的形式化说明是基于对系统的某些假设之上的，但只有假设成立时，证明才成立。所以，一旦某种假设不成立，一切证明就无从谈起。而攻击者只要违反了系统假设，就可以成功侵入系统。而且，即使明确给出假设的详细说明（虽然这并不切实际），但总不可避免地会遗漏一些情况。另外，越是追求系统的安全性，为之付出的代价就越大。并且，安全性是由数据的完整性、秘密性、实体识别、消息认证和可追究等诸多特性组成，根据用户所要达成的不同协议目的，一些安全特性要比另一些安全特性更重要。一个特性可能会与另一个特性发生冲突，或者满足了一个特性却使另一个特性无法满足等。如在现实中，电子商务协议的匿名性和可追究性就是发生冲突的两个特性。因此，没有一个系统是百分之百安全的，也不可能对某一系统的安全性给出百分之百的证明。

尽管如此，安全协议的形式化分析仍是必要的，因为它至少可以完成以下工作：

(1) 界定安全协议的边界，即协议系统与其运行环境的界面；

(2) 更准确地描述安全协议的行为；

(3) 更准确地定义安全协议的特性；

(4) 证明安全协议满足其说明，以及证明安全协议在什么条件下不能满足其说明。

因此，安全协议形式化分析可使用户：

(1) 通过系统说明使协议设计者的注意力集中于接口、协议所处环境的

假设、不同条件下安全协议的状态、条件不满足时出现的情况以及安全协议不变的属性等；

(2) 通过安全协议性质的验证为其提供附加的安全保证。

目前在安全协议形式化分析领域中比较活跃的国外群体有：以 Meadows 和 Syverson 为代表的美国空军研究实验室，以 Lowe 为代表的英国 Leicester 学院，以 Schneider 为代表的英国 London 学院，以 Roscoe 为代表的英国 Oxford 学院，以 Milen 为代表的美国 Carnegie Mellon 学院，以 Stoller 为代表的美国 Indiana 大学，以 Thayer、Herzog 和 Guttman 为代表的 MITRE 公司，以 Stubblebine 代表的美国 AT&T 实验室，以 Paulson 为代表的英国 Cambridge 学院等。在国内方面，主要有以下几个团体在对安全协议进行研究：信息安全国家重点实验室、国家智能计算机研究开发中心、西安电子科技大学和解放军信息工程大学。

3.2.2 安全协议形式化分析方法的分类

目前，对安全协议进行分析的方法粗略可以划分为两大类：一类是构造攻击检验方法，另一类是形式化模型检测的分析方法。

所谓攻击检验方法就是搜集使用目前的对协议的有效攻击方法，逐一对安全协议进行攻击，检验安全协议是否具有抵抗这些攻击的能力。在分析的过程中主要使用自然语言和示意图，对安全协议所交换的消息进行剖析。这种分析方法往往是非常有效的，关键在于攻击方法的选择。它的缺点在于只能类比已有的攻击方法，而不能够找到未知的安全缺陷。

而形式化的分析方法是采用各种形式化的语言或者模型，为安全协议建立模型，并按照规定的假设和分析、验证方法证明协议的安全性。自 Dolev-Yao 模型诞生以来，信息安全领域的科学家们已经提出了许许多多关于安全协议形式化的分析方法，以检验安全协议中是否存在安全缺陷。根据已有的文献，如果更进一步地细化，我们可以将目前出现的安全协议形式化分析方法划分为以下四类：

(1) 使用基于知识和信仰的逻辑来建立给定协议的安全需求模型，其主要思想是运用逻辑系统从用户接收和发送的消息出发，通过一系列的推理公理推证协议是否满足其全部说明。这些逻辑系统通常由一些命题和推理公理组成。命题表示主体对消息的知识和信仰，而运用推理公理可以从已知的知识和信仰推导出新的知识和信仰。文献[47]中给出了一个有关此领域的讨论。

在这类方法中，最著名的是 BAN 及 BAN 类逻辑[2,46-48]，以及用于分析电子商务协议的 Kailar 逻辑[46]。一般来说，BAN 逻辑只能推出认证的结果，而不能对一般的安全性进行证明。使用 BAN 逻辑分析安全协议的步骤如下：(a)协议的理想化转化；(b)假设所有的协议初始状态；(c)使用逻辑规则对系统的状态作出断言；(d)运用逻辑原理得到关于信任的断言。最新的研究是 Kindred 提出的安全协议的生成理论 RV 逻辑[50]。

(2) 使用通用的、并非为分析安全协议单独专门设计的形式化描述语言和协议验证工具。这是一种传统的模型检测方法，其主要思想是把安全协议看作一个模型，方法的目的就是验证这个模型是否满足安全协议目标，比如一般目的模型检测工具 FDR[3]和 Murcp[4]等。这方面最为突出的贡献是 1996 年 Gavin Lowe 使用 FDR（Failures Divergences Refinement Checker）[3]发现了 NS 协议的一个以前从未被发现的漏洞。由于此类方法将安全协议视为一般的目标，在不考虑其独有特性的前提下验证其正确性，因此它的最大的不足是仅考虑了正确性，却忽略了安全性。在这一类形式化分析工具中往往用到了状态机的概念。状态机应用可达性分析技术来对认证协议进行分析，对于每一次迁移，使用主体状态和主体之间信道状态来描述系统的全局状态，分析每一个全局状态并判断其性质，如死锁、正确性等，如果分析表明一个主体在某一已知状态下应接收到某一消息却并未收到时，则说明协议是有问题的。可达性技术通过对协议的说明来判断协议的正确与否，但它并不能保证协议的秘密性不受到主动攻击。

(3) 安全协议的设计者设计专门的用于分析和研究出现的各种情况的特别目的的专家系统，如 Interrogator[5]和 NRL 协议分析器[43]，其主要思想是使用专家系统发现协议是否能够达到不合理的状态（比如密钥的泄露等等）。这类系统可以找出已知的攻击，但是不能证明协议的安全性，也无法找出未知的攻击，其分析协议的能力是有限的，但提供了一个新的研究思路。它从一个不安全的状态出发，并试图发现从出事状态到这一不安全状态是否是可达的，如果可达则说明协议存在漏洞。在文献[43]中，Longley 和 Rigby 指出了专家系统在协议形式化分析中所作出的贡献如下：(a)为认证协议的理解提供新的视觉；(b)是一种不断精炼协议模型的技术；(c)可与模型交互作用，从而使得分析者更能洞察协议内部的操作；(d)能回答 what if 问题；(e)可对协议模型所提出修改的性能进行测试。专家系统可以与其他形式化分析工具配合使用，但不能取而代之。

(4) 基于密码学系统的代数特性开发协议的形式化模型。这种方法是将安全协议系统当作一个代数系统模型，表示出协议的参与者的各种状态，然后分析某种状态的可达性。在此模型中包含了那些可以对信息流进行恶意窃取、修改和删除的入侵者和不诚实的参与者，同时密码学算法被看作是一个满足一些代数性质的黑盒子，但此模型的缺点在于对可验证的协议簇限制过于严格。这一领域最著名的是 Dolev-Yao 模型，此后 Paulson[45]、Schneider[51]、Meadows[52]、Woo 和 Lam[53]等都在此领域做出了很大的贡献。最近一些新的研究为安全协议的分析提供了自动化的支持，那就是结合模型检测技术和定理证明方法开发安全协议的自动验证工具。目前在这方面最有前景和最新的研究成果是 Fabrega, Herzog 和 Guttman 提出的 Strand Space 模型，并已经取得了很大的进展。

安全协议的形式化分析方法本身是研究的热点，但是其应用并不是非常广泛，主要原因是安全协议的安全性的形式化过程比较困难。需要指出的是，由于安全协议本身的复杂性，目前并没有一种方法能够给出安全协议安全性的充分而且必要的理论证明。上述每一类方法都有不同的侧重点，或者说或多或少地存在不足之处，我们在使用上述方法分析安全协议的时候，应当仔细分析协议的特点、应用环境和需求，综合使用这些分析方法，以得到一个比较合理的结果。

第 4 章 Strand Space 理论与模型

在前面章节中提到，目前在安全协议形式化分析各种方法中最有前景和最新的研究成果是 Strand Space 模型，本章将较为详细的介绍该理论与模型。

Strand Space 模型是由 Fabrega, Herzog 和 Guttman 在 1998 年提出的一种安全协议形式化分析方法[7,9,10]，这是一种结合定理证明和协议迹的混合方法，该方法吸纳了 NRL 协议分析器[43]、Schneider 秩函数[51]和 Paulson 归纳法[45]等思想，它是一种新型有效的安全协议形式化分析方法。串（Strand）指的是一轮协议运行到某个时刻某个主体所发生的行为事件的一个消息序列，由发送和接收的消息顺次组成。串空间（Strand Space）是某个协议的运行当中所有可能出现的串的集合，包括所有诚实参与者的串和所有攻击者的串。

Strand Space 模型是现有安全协议形式化方法中最为直观、简洁、严格和有效的方法。它的直观性表现在使用一种节点间存在因果关系的有向图来表示协议的运行。它的简洁性表现在对于小型协议完全可以使用手工的方法完成证明。它的严格性表现在它使用了节点之间的因果关系来确保证明的逻辑性和证明的正确性。它的有效性可以通过文献[7,9,10]中给出的实例来说明。

D.X. Song 对串空间模型进行了扩充[13]，引入了串空间中各要素的语法和语义，并对安全协议的认证性进行了逻辑的表示。在上述基础上使用 SML 语言开发了一个安全协议自动验证工具 ATHENA，实现了对认证性安全协议的自动验证，但该工具对协议秘密性的证明是不完善的。

4.1 Strand Space 基础知识

4.1.1 消息空间和代数假设

1．消息空间

定义两个不相交的原子项集合：**T** 和 **K**。**T** 是原子消息的集合，它包含几种不同类型的原子信息，比如人名、随机数、银行帐号和时间戳等，**T** 中的元素使用字母表示；**K** 是所有密钥的集合，**K** 中元素使用字母 K 表示，使

用K^{-1}表示密钥K的逆，K^{-1}同样是K中的元素。其次，用A表示协议运行过程当中，协议参与各方相互交换传递的消息集合，即集合A为一个包含子集K和子集T，且K∩T=∅的“代数结构”。

进一步定义A上的三种“运算”：

encr: K×A→A

inv: K→K

join: A×A→A

简便起见，将*encr*(*K*, *m*)记为$\{m\}_K$；*inv*(*K*)记为K^{-1}；*join*(*a*, *b*)记为*ab*。这三种“运算”代表了密码协议中的消息构造和消息加密。用*E*代表*encr*函数的值域。K∪T∪E中的元素为A的“简单”元（即不可再拆分的元，也即所谓的具有原子性的元）。

在消息集合A中有：

(1) $t\in\mathbf{T}$，则$t\in\mathbf{A}$；

(2) $K\in\mathbf{K}$，则$K\in\mathbf{A}$，$K^{-1}\in\mathbf{A}$；

(3) $t\in\mathbf{T}$，$K\in\mathbf{K}$；则$\{t\}_K\in\mathbf{A}$；

(4) $m_1\in\mathbf{A}$，$m_2\in\mathbf{A}$；则$m_1m_2\in\mathbf{A}$；

2. 代数假设

集合A中的代数运算需要符合如下的假定：

(1) 自由加密假定：如果$\{m\}_K=\{m'\}_{K'}$，则一定可以推出$m=m'$，$K=K'$；

(2) 自由连接假定：如果$m_1m_2=m_3m_4$，则一定可以推出$m_1=m_2$，$m_2=m_4$；

(3) 连接加密互斥：$m_1m_2\neq\{m_3\}_K$；

(4) 原子不可拆分：$m_1m_2\notin\mathbf{T}\cup\mathbf{K}$。

在*A*中递归定义元素之间的子项关系⊂：

(1) 若$a\subset t$，则$a=t$，其中$t\in\mathbf{T}$；

(2) 若$a\subset K$，则$a=K$，其中$K\in\mathbf{K}$；

(3) 若$a\subset\{g\}_K$，则$a\subset g\vee a=\{g\}_K$；

(4) 若$a\subset gh$，则$a\subset g\vee a=gh$。

4.1.2 基本概念

1. 动作集（Actions）和事件集（Events）

定义4.1 集合{+, -}是串空间的动作集，其中元素“+”表示发送消息的

动作，元素“-”表示接收消息的动作。

定义4.2 元素对$<\sigma, a>$表示一个事件，其中$\sigma \in \{+, -\}$，$a \in \mathbf{A}$。常常使用$+a$或$-a$表示一个事件，$+a$和$-a$又叫做带符号的消息。使用$\pm \mathbf{A}$表示串空间的事件集合，使用$(\pm \mathbf{A})^*$表示带符号消息的有限序列集，序列集合中的元素使用$<< \sigma_1, a_1>, ..., < \sigma_n, a_n>>$表示，这里的n是序列长度。

2．串（Strand）和串空间（Strand Space）

定义4.3 串指的是一轮协议运行到某个时刻时某个协议的参与者所执行的事件的序列，一个串就代表一个参与者。为了使得串的描述更加形象化，使用映射tr将一个串映射到有限序列消息集$(\pm \mathbf{A})^*$，映射tr称为迹映射，映射的像（某个有限消息序列）称为原像（所给的串）的迹，通常我们就把串的迹称为串。

定义4.4 一个串空间是指一个集合Σ且在该集合上存在迹映射：tr：$\Sigma \rightarrow (\pm \mathbf{A})^*$。集合$\Sigma$中的元素称为串。

一个确定的串空间具有如下性质：

(1) 节点是二元组$<s, i>$，其中$s \in \Sigma$，i为满足$1 \le i \le \text{length}(\text{tr}(s))$的一个整数，节点集合记为$\mathbf{N}$，称节点$<s, i>$属于串$s$。显然，每个节点属于唯一的串；

(2) 如果$n=<s, i> \in \mathbf{N}$，则$\text{index}(n)=i$，$\text{strand}(n)=s$，$\text{term}(n)=(tr(s))_i$，$(tr(s))_i$表示串s的迹中的第i个符号项；

(3) 对于$n_1, n_2 \in \mathbf{N}$，存在一条边$n_1 \rightarrow n_2$，当且仅当$\text{term}(n_1)=+a$且$\text{term}(n_2)=-a$，其中$a \in \mathbf{A}$。故这类边意味着n_1发送消息a，节点n_2接收消息a，它记录了串间的一种因果连接；

(4) 如果$n_1=<s, i> \in \mathbf{N}$，$n_2=<s, i+1> \in \mathbf{N}$，则存在边$n_1 \Rightarrow n_2$，这类边表示$n_1$是$n_2$在串$s$上的直接因果前驱。用$n' \Rightarrow^+ n$表示$n'$是$n$在同一个串上的因果前驱（不一定是直接因果前驱）；

(5) 无符号项t出现在$n \in \mathbf{N}$，当且仅当$t \sqsubset \text{term}(n)$；

(6) 令$\mathbf{I}$为无符号项集合，节点$n \in \mathbf{N}$是$\mathbf{I}$的进入点，当且仅当$\text{term}(n)=+t$，其中$t \in \mathbf{I}$，且对所有的$n' \Rightarrow^+ n$，$\text{term}(n') \notin \mathbf{I}$；

(7) 无符号项t起源于$n \in \mathbf{N}$，当且仅当n是集合$\mathbf{I}=\{t': t \sqsubset t'\}$的进入点；

(8) 无符号项t是唯一起源的，当且仅当t唯一起源于$n \in \mathbf{N}$。

3．丛（bundles）和节点的关系

定义4.5 $\mathbf{N}$以及两类边$n_1 \rightarrow n_2$和$n_1 \Rightarrow n_2$的集合是一个有向图$<\mathbf{N}, (\rightarrow \cup \Rightarrow)>$。丛是这个图的一个有限子图。

假设$\rightarrow_C \subset \rightarrow$；$\Rightarrow_C \subset \Rightarrow$，$C=<N_C, (\rightarrow_C \cup \Rightarrow_C)>$是$<N, (\rightarrow \cup \Rightarrow)>$的子图，$C$是丛，当且仅当：

(1) C是一个有限无环图；

(2) 若$n_1 \in N_C$且term(n_1)为负，则必然唯一存在一个n_2使得$n_2 \rightarrow_C n_1$；

(3) 若$n_1 \in N_C$且$n_2 \Rightarrow n_1$，则$n_2 \Rightarrow_C n_1$。

若$n \in N_C$，则称节点n在丛$C=<N_C, (\rightarrow_C \cup \Rightarrow_C)>$中，记为$n \in C$，若串$s$中所有的节点均在$N_C$中，则称串$s$在丛$C$中。可见丛的边表示节点之间的因果依赖关系无论通信是同步的还是异步的，上述关于丛的定义都形式化了一个通信过程模型的三个特征：

(1) 一个串可以发送或接收一个消息，但是不能同时进行这两种操作；

(2) 当一个串收到一个消息，有唯一的一个节点发送了该消息；

(3) 当一个串发送了一个消息，可能有很多串接收到该消息。

一个简单的丛，如图4-1所示。

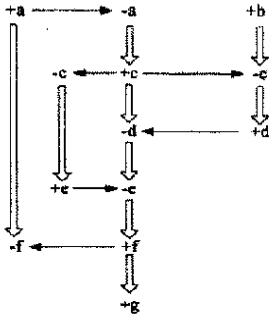


图4-1 丛示意图

定义4.6 丛高度（c-height）是指丛C中使得节点$<s, i> \in C$最大的i的值，称为串s的丛高度。

若串s的迹为$tr(s)=<tr(s)(1),\ldots, tr(s)(m)>$，则m=$C$-height($s$)，即m就是串$s$的丛高度。

定义4.7 节点关系

假设**S**是一个边的集合，且$S \subset (\rightarrow \cup \Rightarrow)$，$N_S$是附属于各边的节点集。对于$\forall n_1, n_2 \in N_S$，定义节点之间的关系“$\prec_s$”和关系“$\leq_s$”：

$n_1 \prec_s n_2$ 表示在 S 中存在一条从节点 n_1 到节点 n_2 的由→和⇒类型边组成的路径，边的数目必须大于零；

$n_1 \leq_s n_2$ 表示在 S 中存在一条从节点 n_1 到节点 n_2 的由→和⇒类型边组成的路径，边的数目必须大于或者等于零。

显然 $\prec_s$ 关系具有传递和闭合的性质，而 $\leq_s$ 关系满足自反、传递和闭合的性质。如果 S 是一个丛，则关系 $\leq_s$ 是偏序的。

引理 4.1 假定 C 是丛，因为二元关系 $\leq_c$ 是偏序的，所以 C 的任意非空节点子集都有 $\leq_c$-最小元，一般使用 $\leq$ 代替 $\leq_c$。

上述引理是串空间理论的重点，大部分的证明都将被转换成求解某个节点集的 $\leq$-最小元。证明的思路就是求解“一个主体知道什么消息，他又是什么时候知道这些消息的？”这样一个问题的答案，这是一种归纳法的原理，它吸纳了 Schneider 秩函数和 Paulson 归纳法的思想。

引理 4.2 假定 C 是丛，S 是 C 的一个节点子集，并限定该子集中的所有满足等式的 uns_term(m)=uns_term(m')两个节点 m 和 m' 必须具有隶属关系一致性，即要么都属于 S，要么都不属于 S。在上述前提下，如下结论成立：如果节点 n 是 S 的一个 $\leq_c$-最小元，则 sign(n)=+，即节点 n 为发送消息的节点。

证明：假设 sign(n)=-，则根据丛性质第二条，在 C 中必定存在一个节点 n' 满足 $n' \prec n$，由于 uns_term(n)=uns_term(n')，所以 $n' \in C$，与前提条件中 n 的最小元性质相矛盾。 ※

引理 4.3 假定 C 是丛，$t \in \mathbf{A}$，并且 $n \in C$ 是 $\{m \in C: t \sqsubset \text{uns\_term}(m)\}$ 节点集的 $\leq_c$-最小元，则消息项 t 发源于节点 n。

证明：假设 Strand(n)=s，根据引理 3.2，有 sign(n)=+，对任意节点 $n' \in s$，$n' \prec n$，即 $n' \Rightarrow^+ n$，则 $n' \in C$，因为 n 的最小元性质，所以 $t \not\sqsubset \text{uns\_term}(n')$，由此根据发源节点定义可以推出引理结论。 ※

4.1.3 攻击者模型

攻击者模型是安全协议系统模型中至关重要的一个组成部分，它将决定一个安全协议系统的安全性和可靠性。不同形式化方法中的安全协议系统模型对攻击者模型有不同的描述，但一般情况下，都不会考虑攻击者攻破密码体制的可能，因为已经假定了密码体制是完备的，只是在寻找安全协议设计上存在的漏洞，也就是分析攻击者根据已有知识来攻破系统的可能性。

在串空间模型中，攻击者能力使用两方面的因素来描述：攻击者所掌握的密钥集合和根据所有已知消息构造新消息的能力。攻击者所掌握的密钥集合用 $\mathbf{K_P}$ 表示。集合 **K**，包含了攻击者初始知道的所有密钥，它包括所有的公开密钥和攻击者的私有密钥，以及根据协议规则所掌握的和其他主体会话的对称密钥，也可能会包括被一些粗心的主体丢失的密钥。攻击者的能力使用攻击者串来表示，攻击者串描述了攻击者拆分、构造、联结和使用已知密钥加解密消息的能力，属于攻击者串的节点称为攻击者节点（用 p 表示），其余称为正规节点，攻击者能力使用下面列出的攻击者串来描述：

M[t]. $\langle +t \rangle, t \in \mathbf{T}$：　攻击者可以随意发出一个原子项消息；

F[g]. $\langle -g \rangle$：　攻击者截获到一个消息；

T[g]. $\langle -g, +g, +g \rangle$：　攻击者截获到一个消息以后又转发出去；

C[g,h]. $\langle -g, -h, +gh \rangle$：　攻击者将截获的两个消息联结后发送出去；

S[g,h]. $\langle -gh, +g, +h \rangle$：　攻击者将截获的联结消息拆分后发送出去；

K[k]. $\langle +k \rangle, k \in \mathbf{K_P}$：　攻击者发送一个已知的密钥出去；

E[k,h]. $\langle -h, -k, +\{h\}_k \rangle$：　攻击者使用所截获到的加密密钥加密截获到的消息，并发送出去；

D[k,h]. $\langle -k^{-1}, -\{h\}_k, +h \rangle$：　攻击者使用所截获到的解密密钥解密截获到的密文消息，并发送出去。

由于攻击者的能力由攻击者的密钥集和攻击者串进行定义，所以这种能力是独立于任何特定协议的。因此，我们就可以得到关于攻击者能力的一般事实，并在我们对一个新的协议进行分析时重用它们。下述命题就描述了攻击者能力的限定，符号“**S** \ **T**”，表示集合 **S** 与 **T** 的差：

命题 4.1 假设 C 是丛，密钥 $K \in (\mathbf{K} \backslash \mathbf{K_P})$。如果 K 不会起源于一个正规节点，则对于任意节点 $n \in C$，有 $K \sqsubset \text{uns\_term}(n)$。特别的对于任意的攻击者节点 $p \in C$，有 $K \sqsubset \text{uns\_term}(p)$。

证明：考虑集合 $\mathbf{S}=\{n \in C: K \subset \text{uns\_term}(n)\}$。假定 **S** 是非空的（由此将得出一个矛盾，从而证明命题的正确性），因此 **S** 有 $\leq_c$-最小元。根据引理 4.3，K 起源于 **S** 的任意 $\leq_c$-最小元，结合命题的前提条件可以推出所有这些最小元都是攻击者节点，再根据引理 4.2 可以推出这些最小元都是发送消息的节点。下面我们逐一检验攻击者串中的发送消息节点：

M. 攻击者串形式为$\langle +t \rangle$，$t \in \mathbf{T}$，但 $K \sqsubset t$；

F. 攻击者串形式为$\langle -g \rangle$，没有发送消息的节点；

T. 攻击者串形式为<-g, +g, +g>，因为发送的消息是接受到消息之后转发出去的，所以不存在消息项起源于发送消息节点；

C. 攻击者串形式为<-g, -h, +gh>，因为发送的消息是接受到的消息联结之后发送出去的，所以不存在消息项起源于发送消息节点；

S. 攻击者串形式为<-gh, +g, +h>，因为发送的消息是接受到的消息拆分之后发送出去的，所以不存在消息项起源于发送消息节点；

K. 攻击者串形式为<+k_0>, $k_0 \in \mathbf{K_P}$，如果 $K \sqsubset k_0$，与命题前提条件 $K \in (\mathbf{K} \setminus \mathbf{K_P})$相矛盾；

E. 攻击者串形式为<-h, -k, +$\{h\}_k$>，根据子项的定义，若 $K \sqsubset \{h\}_k$，则 $K \sqsubset h$ 或者 $K = \{h\}_k$，后一种情况与“连接加密互斥”假定相矛盾，所以不存在消息项起源于发送消息节点；

D. 攻击者串形式为<-k^{-1}, -$\{h\}_k$, +h >，若 $K \sqsubset h$，则 $K \sqsubset \{h\}_k$，所以不存在消息项起源于发送消息节点。

根据以上分析，**S** 中不存在攻击者节点，同样也就推出整个集合为空。但是假如**S**为空，则对任意节点 $n \in C$，有 $K \propto \text{uns\_term}(n)$。 ※

4.2 理想和诚实

4.2.1 理想

定义 4.8 假如 $\acute{\mathbf{K}} \subset \mathbf{K}$，定义集合 **A** 的一个 $\acute{\mathbf{K}}$-理想 **I**：**I** 是 **A** 的子集，且对于所有的 $h \sqsubset \mathbf{I}$，$g \sqsubset \mathbf{A}$ 和 $K \in \acute{\mathbf{K}}$ 满足：

(1) $hg, gh \in \mathbf{I}$；

(2) $\{h\}_K \in \mathbf{I}$。

另外，使用 $\mathbf{I}_{\acute{\mathbf{K}}}[h]$表示包含消息项 h 的最小 $\acute{\mathbf{K}}$-理想。

由上述定义理解可以得出结论：$g \sqsubset h$，当且仅当 $h \in \mathbf{I}_{\acute{\mathbf{K}}}[g]$。

定义 4.9 对于 $\mathbf{S} \subset \mathbf{A}$，定义 $\mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}]$是包含 **S** 的最小 $\acute{\mathbf{K}}$-理想。

命题 4.2 假如 $\mathbf{S} \subset \mathbf{A}$，则 $\mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}] = \cup_{x \in S} \mathbf{I}_{\acute{\mathbf{K}}}[x]$。

证明：集合 $\acute{\mathbf{K}}$-理想的实质就是下述映射的闭合运算：$x \mapsto xa$；$x \mapsto ax$；$x \mapsto \{x\}_K$，$K \in \acute{\mathbf{K}}$。因此 $\acute{\mathbf{K}}$-理想的合集还是一个 $\acute{\mathbf{K}}$-理想，即 $\cup_{x \in S} \mathbf{I}_{\acute{\mathbf{K}}}[x]$是包含 **S** 的一个 $\acute{\mathbf{K}}$-理想。又显然有 $\cup_{x \in S} \mathbf{I}_{\acute{\mathbf{K}}}[x] \subset \mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}]$。 ※

引理 4.4 假设 $\mathbf{S}_0 = \mathbf{S}$，$\mathbf{S}_{i+1} = \{\{g\}_K : g \in \mathbf{I}_\Phi[\mathbf{S}_i], K \in \acute{\mathbf{K}}\}$，则 $\mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}] = \cup_i \mathbf{I}_\Phi[\mathbf{S}_i]$。

证明：因为 $\mathbf{S}_i \subset \mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}]$，因此 $\cup_i \mathbf{I}_\Phi[\mathbf{S}_i] \subset \mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}]$，又因为 $\cup_i \mathbf{I}_\Phi[\mathbf{S}_i]$显然是包含

S的一个$\dot{K}$-理想，所以可以推出命题的结论。 ※

定义 4.10 一个消息项的宽度递归定义如下：

(1) $t\in\mathbf{T}$，则 t 的宽度为 1；

(2) $K\in\mathbf{K}$，则 K 的宽度为 1；

(3) $t\in\mathbf{A}$，$K\in\mathbf{K}$，则$\{t\}_K$的宽度为 1；

(4) $m_1\in\mathbf{A}$，$m_2\in\mathbf{A}$，则 m_1m_2 的宽度为 m_1 的宽度与 m_2 的宽度和。

命题 4.3 假设 $K\in\mathbf{K}$，$\mathbf{S}\subset\mathbf{A}$：对任意 $s\in\mathbf{S}$，s 宽度为 1，且 s 不是使用 K 加密的消息项$\{g\}_K$。如果$\{h\}_K\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$，则 $h\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$。

证明：假定 $K\in\mathbf{K}$，$\{h\}_K\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$，且 $h\notin\mathbf{I}_{\dot{K}}[\mathbf{S}]$。集合 $\mathbf{I}'=\mathbf{I}_{\dot{K}}[\mathbf{S}]\backslash\{\{h\}_K\}$。因为 S 不包含一个最外层加密密钥为 K 的元素，所以 $\mathbf{S}\subset\mathbf{I}'$。又因为 $\mathbf{I}_{\dot{K}}[\mathbf{S}]$是一个理想，$h\notin\mathbf{I}_{\dot{K}}[\mathbf{S}]$，且$\{h\}_K$不是消息项的连接，根据“自由加密假定”对任意 $h'\notin\mathbf{I}'$，$\{h'\}_{K'}$，由此 I′满足定义 4.8 关于理想的两条规定，所以 I′是一个 $\dot{K}$-理想，即I′是包含 S 的 $\dot{K}$-理想，与 $\mathbf{I}_{\dot{K}}[\mathbf{S}]$是包含 S 的最小 $\dot{K}$-理想相矛盾。 ※

命题 4.4 假设 $K\in\mathbf{K}$，$\mathbf{S}\subset\mathbf{A}$：对任意 $s\in\mathbf{S}$，s 宽度为 1，且 s 不是使用 K 加密的消息项$\{g\}_K$。如果$\{h\}_K\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$，则 $K\in\dot{K}$。

证明：同命题 4.3。 ※

命题 4.5 假设 $\mathbf{S}\subset\mathbf{A}$：对任意 $s\in\mathbf{S}$，s 宽度为 1。若有 $gh\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$，则要么 $g\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$，要么 $h\in\mathbf{I}_{\dot{K}}[\mathbf{S}]$。

证明：根据引理 4.4 的结论，必定存在某个 i 使得 $gh\in\mathbf{I}_{\Phi}[\mathbf{S}_i]$。再根据命题 4.2 必定存在某个 $x\in\mathbf{S}_i$，使得 $gh\in\mathbf{I}_{\Phi}[\mathbf{S}_i]$，显然 x 宽度为 1。由此可以判定，$g\in\mathbf{I}_{\Phi}[\mathbf{S}]$或者 $h\in\mathbf{I}_{\Phi}[\mathbf{S}]$，否则可以推出集合 $\mathbf{I}_{\Phi}[\mathrm{x}]\backslash\{\{h\}_K\}$是包含 x 的$\varnothing$-理想，与 $\mathbf{I}_{\Phi}[\mathrm{x}]$的最小性相矛盾。 ※

推论 4.1 假定 $K\neq K'$且$\{h'\}_K\subset\{h\}_K$，则$\{h'\}_K\subset h$。

证明：假设即指$\{h\}_K\in\mathbf{I}_K[\{h'\}_K]$，由命题暗指 $h\in\mathbf{I}_K[\{h'\}_K]$ ※

4.2.2 入口点和诚实

定义 4.11 定义 4.4 中已经顺带给出了入口点的定义：节点 $n\in\mathbf{N}$ 是消息项集合 $\mathbf{I}\subset\mathbf{A}$ 的入口点，当且仅当 term(n)=+t，其中 $t\in\mathbf{I}$，且对所有的 $n'\Rightarrow^+n$，uns_term(n')$\notin\mathbf{I}$。

命题 4.6 假设 C 是 A 上的丛，m 是节点集$\{m\in C$：uns_term(m)$\in\mathbf{I}\}$的最小元节点，则 m 是 I 的入口点。

证明：首先 term(m)=+h；其次，若存在 $m'\Rightarrow^+m$，且 uns_term(m')$\in\mathbf{I}$，根

据从定义第三条可推出 $m' \in C$，与 m 的最小元性质矛盾。 ※

定义 4.12 集合 $\mathbf{I} \subset \mathbf{A}$ 对从 C 是诚实的：当且仅当若 I 的入口点中有攻击者节点 p，则 p 是 M 节点或 K 节点。

关于节点集诚实的定义有一个直观的说明和解释，就是攻击者节点成为节点集 I 的入口点的唯一可能性就是依靠猜测，要么猜中一个新鲜的随机数（M 节点），要么猜中一个密钥或者口令（K 节点），但不可能通过对所掌握的知识集 KS 和他的合法密钥集合合理的加密、解密、连接和拆分运算来达到这个目的。

4.2.3 攻击者的能力

定理 4.1 假设 C 是 A 上的丛，$s \subset \mathbf{T} \cup \mathbf{K}$，$\acute{K} \in \mathbf{K}$，且 $K \in \mathbf{S} \cup \acute{K}^{-1}$，则理想 $\mathbf{I}_{\mathbf{K}}[\mathbf{S}]$ 是诚实的。

证明：令 $\mathbf{I}=\mathbf{I}_{\mathbf{K}}[\mathbf{S}]$。因为 $\mathbf{I} \cap \mathbf{K} = \mathbf{S} \cap \mathbf{K}$，所以推出 $\mathbf{K} \setminus \mathbf{I} = \mathbf{K} \setminus \mathbf{S} \subset \acute{K}^{-1}$；又因为 $s \subset \mathbf{T} \cup \mathbf{K}$，S 中元素全部为原子项消息，所以可以运用命题 4.3 和命题 4.5，假设节点 m 是攻击者节点，且是集合 I 的入口点。下面考察所有类型的攻击者串，逐一判断 m 的可能情况。首先根据入口点的定义可以排除 F 和 T 类型串，其余情况如下：

C.此串迹为$\langle -g, -h, +gh \rangle$。因为 $gh \in \mathbf{I}$，根据命题 4.5，要么 $g \in \mathbf{I}$，要么 $h \in \mathbf{I}$，与入口点定义矛盾；

S.此串迹为$\langle -gh, +g, +h \rangle$。无论是 $g \in \mathbf{I}$，还是 $h \in \mathbf{I}$，根据理想的定义，都可推出 $gh \in \mathbf{I}$，与入口点定义矛盾；

D.此串迹为$\langle -k^{-1}, -\{h\}_k, +h \rangle$。根据入口点的定义，$k^{-1} \notin \mathbf{I}$，因此 $k^{-1} \notin \mathbf{S}$；又因为 $K \in \mathbf{S} \cup \acute{K}^{-1}$，因此 $k^{-1} \in \acute{K}^{-1}$，所以 $k \in \acute{K}$。根据理想的定义，都可推出 $\{h\}_k \in \mathbf{I}$，与入口点定义矛盾；

E.此串迹为$\langle -h, -k, +\{h\}_k \rangle$。$\{h\}_k \in \mathbf{I}$，根据命题 4.3 可以推出 $h \in \mathbf{I}$，与入口点定义矛盾；

剩余的可能就是 m 位于 M 类型串或 K 类型串上。 ※

推论 4.2 假设 C 是 A 上的丛，$\mathbf{K}=\mathbf{S} \cup \acute{K}^{-1}$，且 $\mathbf{S} \cap \mathbf{K}_{\mathbf{P}} = \varnothing$。若存在节点 $m \in C$，且 $\text{uns\_term}(m) \in \mathbf{I}_{\mathbf{K}}[\mathbf{S}]$，则必定存在正规节点 $n \in C$，且 n 是 $\mathbf{I}_{\mathbf{K}}[\mathbf{S}]$ 的入口点。

证明：假定不存在正规节点是 $\mathbf{I}_{\mathbf{K}}[\mathbf{S}]$ 的入口点。由题设可知节点集合 $\psi = \{n \in C: \text{uns\_term}(n) \in \mathbf{I}_{\mathbf{K}}[\mathbf{S}]\}$ 非空，因此集合 ψ 包含有最小元节点 m。根据

命题 4.6，m 是理想 $\mathbf{I}_{\dot{K}}[\mathbf{S}]$的入口点，$m$ 非正规节点。根据定理 4.1，m 是 M 节点或 K 节点。因为 $\mathbf{K}=\mathbf{S}\cup\dot{\mathbf{K}}^{-1}$，$\mathbf{S}\subset\mathbf{K}$，则 $\mathbf{I}_{\dot{K}}[\mathbf{S}]\cap\mathbf{T}$，所以 m 非 M 节点。又因为 $\mathbf{S}\cap\mathbf{K}_{\mathbf{P}}=\varnothing$，因此 m 非 K 节点。 ※

推论 4.3 假设 C 是 $\mathbf{A}$ 上的丛，$\mathbf{K}=\mathbf{S}\cup\dot{\mathbf{K}}^{-1}$，且 $\mathbf{S}\cap\mathbf{K}_{\mathbf{P}}=\varnothing$。已知 C 中的正规节点都不是 $\mathbf{I}_{\dot{K}}[\mathbf{S}]$的入口点，则所有 $\{g\}_K$ 形式的消息项都不会起源于攻击者节点，其中 $K\in\mathbf{S}$。

证明：根据推论 4.2，对任意节点 $m\in C$，$\mathrm{uns\_term}(m)\notin\mathbf{I}_{\dot{K}}[\mathbf{S}]$。假定 $\{g\}_K$ 起源于攻击者节点 m，其中 $K\in\mathbf{S}$。下面考察所有类型的攻击者串，逐一判断 m 的可能情况。首先可以排除 M, F, C, S, K 和 T 类型串，其余情况如下：

E. 此串迹为$\langle -h, -k_0, +\{h\}_{k0}\rangle$。根据前面推出的结论 $k_0\notin\mathbf{I}$，因此 $k_0\neq K$。又因为 $\{g\}_K\subset\{h\}_{k0}$，$\{g\}_K\subset h$，这将与入口点定义矛盾；

D. 此串迹为$\langle -k_0^{-1}, -\{h\}_{k0}, +h\rangle$。显然 $\{g\}_K$ 不可能起源于 $+h$。 ※

4.3 Strand Space 模型的优缺点

Strand Space 模型的特点是协议模型简洁，并且对协议正确性证明是比较容易的。这一方法的一个有趣的概念是使用插图法来启发式地描述和推证协议的正确性，因此可使分析者描绘出安全协议的画面，包括所受到的攻击、正确性定理以及证明中的关键性步骤等。归纳起来，Strand Space 形式化分析方法的优点可体现在以下几方面：

(1) 可以证明协议的正确性，这是基于推理的形式化方法的缺陷，并给出了正确性的多种定义，包括秘密性和认证性的说明与推证；

(2) 给出攻击者可能行为的一个详细模型，从而可开发出用于界定攻击者能力的一般性定理，并与所分析的协议是不相关的；

(3) 给出一些数据项，如随机数或会话密钥的新鲜性只能出现在一轮协议中的假设的清晰语义；

(4) 可以有效防止状态空间爆炸，这是基于攻击的形式化方法的缺陷。

虽然 Strand Space 有显著优点，但作为一种发展中的形式化分析工具仍不乏不足之处：

(1) 语言描述能力有限，对许多应用型的协议仍不可描述、分析；

(2) 与模型对应的形式推理或检测的自动工具仍不完善。

第5章 若干密码协议的Strand Space模型及分析

在第四章中，对Strand Space模型进行了较为详细的介绍，本章将运用该模型对以下几种密码协议进行分析：

1．NSL\NS公钥认证协议；

2．Yahalom协议；

3．一种传输模型的认证协议；

4．ISI支付协议。

在分析具体协议之前，我们先对Strand Space模型中协议正确性的定义作一说明。认证协议正确性包含认证性和保密性两方面。

1．认证性

当协议主体B作为消息项m的响应者完成一轮协议时，如果B认为是与主体A完成的此轮协议，那么唯一存在一轮协议是由A作为发起者发出消息项m，且A同样认为是与B完成的该轮协议。

这样的证明可在Strand Space模型中转化为boundle的建立，每当一个boundle C包含一个表示使用m的响应者串时，C也唯一包含一个使用m的发起者串。

2．保密性

受保护的数据在任何节点（包含正规节点和攻击者节点）都不会以未受保护的形式出现在术语中。

消息m在Strand Space模型中是安全的，描述为：任何$n \in C, term(n) \neq m$。

5.1 NSL\NS协议的Strand Space模型及分析

5.1.1 NSL和NS公钥认证协议

NSL协议[46]是Gavin Lowe对Needham和Schroeder提出的一个公钥认证协议的改进协议，原始的Needham-Schroeder（以下简称NS）公钥认证协议被G. Lowe使用FDR和CSP发现存在漏洞[3,54]。

NSL 协议的最直观的形式化描述如下：

(1) $A \rightarrow B$ ： $\{N_a A\}_{K_B}$

(2) $B \rightarrow A$ ： $\{N_a N_b B\}_{K_A}$

(3) $A \rightarrow B$ ： $\{N_b\}_{K_B}$

协议目的：实现主体之间的相互认证。

NSL 协议与 NS 协议的区别在于协议的第二步，在 NS 协议中没有包含角色 B 的名字。在文献[3]中，G.Lowe 证明了 NSL 协议的正确性。

Fabrega, Herzog 和 Guttman 在文献[9]中以 NSL 协议为例说明了如何利用 Strand Space 模型证明协议的正确性，下面我们详细介绍此证明过程。

5.1.2 NSL 串空间

首先，对将要使用到的消息项代数运算做一下说明：角色名称集合 $\mathbf{T}_{name} \subset \mathbf{T}$，一般使用 A、B、S 等来代表 $\mathbf{T}_{name}$ 中的元素；密钥映射 K: $\mathbf{T}_{name} \rightarrow \mathbf{K}$，一般使用 K_A 表示 A 的象，同时假定此映射是单射，即 $K_A = K_B$ 必定推出 $A=B$；假如映射 K 非单射则协议将不能满足它的认证性目标。

定义 5.1 NSL 串空间（如图 5-1 所示）

(1) 集合 Init$[A, B, N_a, N_b]$中的元素 $s \in \Sigma$ 且 s 具有如下迹：

$$<+\{N_a A\}_{K_B}, -\{N_a N_b B\}_{K_A}, +\{N_b\}_{K_B}>$$

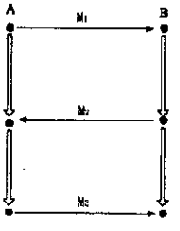
这里的 $A, B \in \mathbf{T}_{name}$，$N_a, N_b \in \mathbf{T}$，但是 $N_a \notin \mathbf{T}_{name}$。与串 $s \in$ Init$[A, B, N_a, N_b]$ 相关联的主体是 A。

(2) 集合 Resp$[A, B, N_a, N_b]$中的元素 $s \in \Sigma$ 且 s 具有如下迹：

$$<-\{N_a A\}_{K_B}, +\{N_a N_b B\}_{K_A}, -\{N_b\}_{K_B}>$$

这里的 $A, B \in \mathbf{T}_{name}$，$N_a, N_b \in \mathbf{T}$，但是 $N_b \notin \mathbf{T}_{name}$。与串 $s \in$ Resp$[A, B, N_a, N_b]$ 相关联的主体是 B。

NSL 串空间是一个渗入串空间 Σ，Σ=Init∪Resp∪**P**。其中 **P** 代表侵入者串的集合。



M1=$\{N_a A\}_{K_B}$

M2=$\{N_a N_b B\}_{K_A}$

M3=$\{N_b\}_{K_B}$

图 5-1 NSL 协议 Strand Space 模型的 boudle 图

如果 $s \in \text{Init}[A, B, N_a, N_b]$或者 $s \in \text{Resp}[A, B, N_a, N_b]$是一个正规串，则我们分别称 A 和 B 为串 s 的发起者和响应者，N_a 和 N_b 是分别代表发起者和响应者的值。一般要求 N_a 和 N_b 是具有新鲜性的随机数，也就是说它们应该唯一地起源于 NSL 串空间，另外并不要求发起者串和响应者串总是完全包含三个节点，在有些丛中可能仅仅包含第一或前两个节点。

由以上定义我们知道当给定一个串时，我们根据串的迹就可以唯一地确定它是正规串还是攻击者串。

5.1.3 NSL\NS 协议正确性分析

1．NSL 协议响应者的认证性

命题 5.1 假定下述条件成立：

(1) Σ是一个 NSL 串空间，C 是Σ中的某个丛，s 是 C 中的一个响应者串，s 的迹为 $\text{Resp}[A, B, N_a, N_b]$，且 s 的丛高度为 3；

(2) $K_A^{-1} \notin \mathbf{Kp}$；

(3) $N_a \neq N_b$，且 N_b 唯一起源于串空间Σ。

则丛 C 包含一个发起者串 $t \in \text{Init}[A, B, N_a, N_b]$，且 t 的丛高度为 3。

证明：首先说明在没有特别说明情况下，Σ、C、A、B、N_a 和 N_b 和上面命题中的表述一致。使用 n_0 代表节点$\langle s, 2\rangle$，使用 v_0 代表节点$\langle s, 2\rangle$的消息项，使用 n_3 代表节点$\langle s, 3\rangle$，在证明过程中将会添加两个节点 n_1 和 n_2，它们满足关系：$n_0 \prec n_1 \prec n_2 \prec n_3$。

为证明此命题，我们引入引理 5.1-5.4 并证明之，最后由引理 5.4 的结论，即得证本命题。 ※

引理 5.1 N_b 起源于节点 n_0。

证明：根据命题假定，$N_b \sqsubset v_0$，$\text{sign}(n_0)=+$。因此，我们仅仅需要验证这个关系式 $N_b \sqsubset \text{uns_term}(n')$是否成立，其中 n'是节点$\langle s, 1\rangle$，$\text{uns\_term}(n') = \{N_a A\}_{K_B}$。

依据命题 5.1 题设(3)，$N_a \neq N_b$，及定义 5.1 第(2)条 $N_b \neq A$，以及消息项代数运算假定之“连接加密互斥”，可以得到：$N_b \sqsubset \text{uns\_term}(n')$。 ※

引理 5.2 集合 $\mathbf{S}=\{n \in C: N_b \sqsubset \text{uns_term}(n) \wedge v_0 \not\sqsubset \text{uns_term}(n)\}$有 $\leq$-最小元 n_2，节点 n_2 是正规节点，且 $\text{sign}(n_2)=+$。

证明：显然 n_3 属于 **S**，所以集合 **S** 非空。因此根据引理 4.1，集合 **S** 至

少有一个≤-最小元 n_2；根据引理 4.2，sign(n_2)=+。下面需要证明 n_2 不可能是一个攻击者节点（如图 5-2 所示）。考察所有的攻击者串中的发送消息节点：

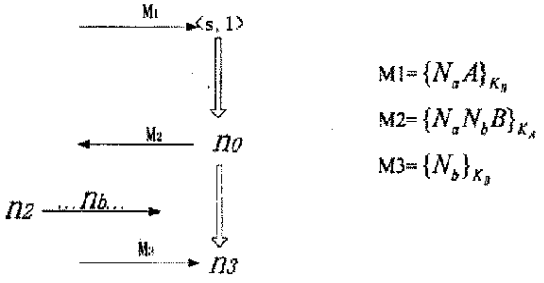


图 5-2 正规节点 n_2

M. 此串形式为<+t>。因为 t∈**T**，所以 t=N_b，则 N_b 起源于此串，与 N_b 唯一起源于正规节点 n_0 矛盾（引理 5.1）；

F. 此串形式为<-g>。没有发送消息的节点；

T. 此串形式为<-g, +g, +g>。因为发送的消息是接受到消息之后转发出去的，所以发送消息节点不可能是最小元节点；

C. 此串形式为<-g, -h, +gh>。因为发送的消息是接受到的消息联结之后发送出去的，所以发送消息节点不可能是最小元节点；

K. 此串形式为<+k_0>，$k_0 \in K_P$。显然 $N_b \not\sqsubset k_0$，故排除此串；

E. 此串形式为<-h, -k, +$\{h\}_k$>。根据内项的定义，若 $N_b \sqsubset \{h\}_k$，且 $v_0 \not\sqsubset \{h\}_k$，因为，$N_b \neq \{h\}_k$，则必有 $N_b \sqsubset h$，又因为 $v_0 \not\sqsubset h$（否则必有 $v_0 \not\sqsubset \{h\}_k$不能成立），所以排除此串；

D. 攻击者串形式为<-k^{-1}, +$\{h\}_k$, +h>。如果发送消息节点是最小元节点，则，$v_0 \not\sqsubset h$ 且 $v_0 \sqsubset \{h\}_k$，因此 $v_0=\{h\}_k$，应用"自由加密假定"可以推出：$h=N_a N_b B$，且 $K=K_A$，根据假定 $K_A^{-1} \notin K_P$，结合命题 4.1 可以推断 K_A^{-1} 起源于一个正规节点，但显然这是不可能的；

S. 攻击者串形式为<-gh, +g, +h>。因为发送消息的两个节点是对称的，所以我们只需要考虑一种情况。假设 uns_term(n_2)=g，因为 $n_2 \in S$，$N_b \sqsubset g$，且 $v_0 \not\sqsubset g$。根据节点 n_2 的最小元性质可以推出 $v_0 \sqsubset gh$，根据"连接加密互斥"可以推出 $v_0 \neq gh$，因此 $v_0 \sqsubset h$。

根据对 S 类型串的分析，我们有结论 $N_b \subset g$，$v_0 \not\subset g$，$v_0 \subset h$，结合对消息项代数运算规则，如果 g 是消息连接的形式，则可以假定消息项 g 可以拆分出消息项 g_1（否则 g_1 就是 g 本身）；这里的 g_1 要么等于 N_b，要么是一个加密消息块，并满足 $N_b \subset g_1$，$v_0 \not\subset g_1$，同理可以假定消息项 h 可以拆分出消息项 h_1，这里的 h_1 是一个加密消息块，并满足 $v_0 \subset h_1$ 显然这里的 g_1 和 h_1 是不可以被拆分的消息项，它们都不是两个消息项的连接。

考察集合 $\mathbf{T}=\{m \in C: m \prec n_2 \wedge g_1 h_1 \subset \text{uns\_term}(m)\}$，因为 NSL 串空间中没有一个正规节点可能包含子项 $g_1 h_1$（这里的 h_1 是一个加密形式的子项），所以集合 T 中全部是攻击者节点。显然，gh 属于集合 **T**，所以 T 非空，并且 T 有 $\prec$-最小元，且为发送消息节点。所以我们需要再次考察所有攻击者串来验证这个最小元的存在性：

M, F, T, S, E, D, K 显然 **T** 的最小元不能位于这些串上；

C. 攻击者串形式为<-g', -h', +$g'h'$>。若上述集合 T 的最小元在此串上，必有 $g_1 h_1 \subset g'h'$。根据 g_1 和 h_1 的不可拆分性，必然可以推出结论 $g'=g_1$，$h'=h_1$，或者 $g'=h_1$，$h'=g_1$，无论是哪一种情况都与前提结论 g 是集合 **S** 的 $\prec$-最小元相矛盾。

根据上述分析，S 中不存在攻击者节点，n_2 只能是正规节点。 ※

引理 5.3 定义节点 n_2 如引理 5.2 中所述，则存在节点 n_1 与节点 n_2 位于相同的串上，n_1 先于 n_2 发生，且 $\text{uns\_term}(n_1)=\{N_a N_b B\}_{K_A}$。

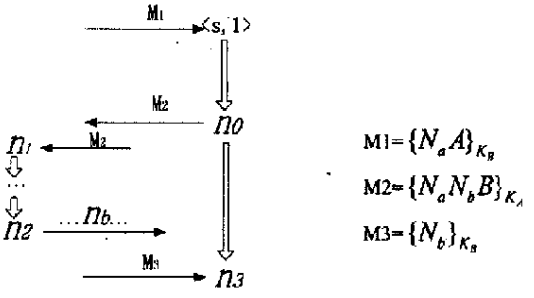


图 5-3 节点 n_1

证明：（如图 5-3 所示）N_b 起源于节点 n_0（引理 5.1），且唯一起源于串空间Σ（命题 5.1 假设第三条）。因为 $v_0 \subset \text{uns\_term}(n_0)$，$v_0 \not\subset \text{uns\_term}(n_2)$，所

以 $n_2 \neq n_0$。由以上条件可以推出：N_b 不可能起源于节点 n_2。因此，必定有节点 n_1 先于 n_2，且与节点 n_2 位于相同的串上，同时 $N_b \subset \text{uns\_term}(n_1)$。根据 n_2 的最小元性质，必定可以推出消息项关系式 $v_0=\{N_a N_b B\}_{K_A} \subset \text{uns\_term}(n_1)$。通过观察正规节点可以发现，没有正规节点包含一个加密消息块作为子项，因此推出结论：$\{N_a N_b B\}_{K_A} = \text{uns\_term}(n_1)$。 ※

引理 5.4 包含上述引理 5.2 和引理 5.3 中推出的节点 n_1 和 n_2 的串是发起者串，且在丛 C 中。

证明：节点 n_2 是发送消息的正规节点，且发生在一个形如 $\{XYZ\}_K$ 形式的节点之后（称为 n_1）。通过观察和比较串空间Σ中的正规串可知包含此二节点的串是发起者串；其次，n_1 和 n_2 分别是发起者串的第二和第三个节点；另外，它的丛高度显然就是 3。 ※

命题 5.2：假如Σ是一个 NSL 串空间，N_a 唯一起源于Σ，则对于任意 A、B 和 N_b 至多存在一个发起者串 $t \in \text{Init}[A, B, N_a, N_b]$。

证明：假设 $t \in \text{Init}[A, B, N_a, N_b]$，因为 $N_a \subset \text{uns\_term}(\langle t, 1\rangle)$，因此 N_a 起源于此串，由 N_a 的唯一起源性可知Σ中至多有一个 t。 ※

上述我们已经从响应者的角度证明了 NSL 协议的认证性，假如希望证明整个协议的认证性，则需要假定发起者挑选的值 N_a 是唯一起源于串空间Σ，证明发起者认证性（见后）。

2. NS 协议响应者的认证性

NS 协议响应者的认证性的分析与 NSL 协议响应者的认证性的分析几乎是平行的，仅需对引理 5.3 作如下修改：

引理 5.5：定义节点 n_2 如引理 5.2 中所述，则存在节点 n_1 与节点 n_2 位于相同的串上，n_1 先于 n_2 发生，且 $\text{uns\_term}(n_1)=\{N_a N_b\}_{K_A}$。

说明：此结果相对于引理 5.3 是很弱的，我们将不再能够推导出包含节点 n_1 和 n_2 的串 $t \in \text{Init}[A, B, N_a, N_b]$，因为消息项 $\{N_a N_b\}_{K_A}$ 无法标识出响应者。此时，仅仅能够推出 $t \in \text{Init}[A, X, N_a, N_b]$，这就是 NS 协议存在的漏洞。

3. NSL 协议响应者的保密性

要证明响应者的随机数 N_b 在协议运行中是保秘的，前提是要假定响应者的私钥没有被破解，否则攻击者可以直接得到 N_b 的值。

命题 5.3 假定下述条件成立：

(1) Σ是一个 NSL 串空间，C 是Σ中的某个丛，s 是 C 中的一个响应者串，s 的迹为 $\text{Resp}[A, B, N_a, N_b]$，且 s 的丛高度为 3；

(2) $K_A^{-1} \notin \mathbf{Kp}$, $K_B^{-1} \notin \mathbf{Kp}$;

(3) $N_a \neq N_b$, 且 N_b 唯一起源于串空间Σ。

则对于所有的节点 $m \in C$, $N_b \sqsubset \text{uns\_term}(m)$, 满足 $\{N_a N_b B\}_{K_A} \sqsubset \text{uns\_term}(m)$ 或者 $\{N_b\}_{K_B} \sqsubset \text{uns\_term}(m)$, 而且 $N_b \neq \text{uns\_term}(m)$。

证明: 规定Σ、C、A、B、N_a 和 N_b 和上面命题中的表述一致。使用 n_0 代表节点<s, 2>, 使用 v_0 代表节点 n_0 的消息项 $\{N_a N_b B\}_{K_A}$, 使用 n_3 代表节点<s, 3>, 使用 v_3 代表节点 n_3 的消息项 $\{N_b\}_{K_B}$。考察节点集:

$\mathbf{S}=\{n \in C: N_b \sqsubset \text{uns\_term}(n) \wedge v_0 \not\sqsubset \text{uns\_term}(n) \wedge v_3 \not\sqsubset \text{uns\_term}(n)\}$

假如集合 **S** 非空, 则有≤-最小元。首先证明两个引理: 引理 5.6 将首先证明最小元节点不是正规节点, 引理 5.7 将证明最小元节点不是攻击者节点。因此集合 **S** 为空集, 由此得证本命题。 ※

引理 5.6 集合 **S** 的最小元不是正规节点。

证明: 假设最小元 $m \in \mathbf{S}$ 是正规节点, 则 sign(m)=+。

(1) 假设节点 m 在响应者串 s 上

因为仅有节点 n_0 是发送消息节点, 且 v_0 = uns_term(n_0), 而点集 **S** 要求 $v_0 \not\sqsubset \text{uns\_term}(n)$, 所以 m 不可能在响应者串 s 上。

(2) 假设节点 m 在响应者串 $s' \neq s$ 上

因为 sign(m)=+, 所以此时 m=<s', 2>, 因此 uns_term(m)= $\{NN'C\}_{K_B}$。因为 $N_b \sqsubset \text{uns\_term}(m)$, 所以 N_b=N 或者 N_b=N'。对这两种情况分别进行讨论:

a. 假设 N_b=N, $N_b \sqsubset \text{uns\_term}(<s', 1>)=\{N_b D\}_{K_C}$, 又因为 $v_0 \not\sqsubset \{N_b D\}_{K_C}$, 且 $v_3 \not\sqsubset \{N_b D\}_{K_C}$, 所以<$s'$, 1>∈$S$, 又<$s'$, 1>≺$m$, 与 m 的最小元性质矛盾, 故假设不成立;

b. 假设 $N_b \neq N$ 且 N_b=N', 则 N_b 起源于节点 m, 与 N_b 唯一起源于节点 n_0 相矛盾, 故假设不成立。

由 *a* 和 *b* 可知 m 不可能在响应者串 s'上。

(3) 假定节点 m 在发起者串 **s'**上

因为 sign(m)=+, 所以此时 m 必定是第一或者第三个节点。对这两种情况分别进行讨论:

a. 假设 m=<s', 1>, 因为 $N_b \sqsubset \text{uns\_term}(m)$, 所以 N_b 起源于节点 m, 与 N_b 唯一起源于节点 n_0 相矛盾, 故假设不成立;

b. 假设 m=<s', 3>,则 uns_term(m)= $\{N_b\}_{K_C}$。因此节点<s', 2>的迹为 $\{xN_b C\}_K$, 又因为 $C \neq B$, 否则 $v_3 \sqsubset \text{uns\_term}(m)$, 因此<$s'$, 2>≺$m$, 与 m 的最

小元性质矛盾，故假设不成立。

由 a 和 b 可知 m 不可能在发起者串 s' 上。

综上可知最小元 $m \in \mathbf{S}$ 不在正规串上，故不是正规节点。 ※

引理 5.7 集合 S 的最小元不是攻击者节点。

证明：此引理的证明与引理 5.2 的证明几乎类似，区别在于 D 类型的攻击者串需要考虑两种情况：首先是 $h=N_aN_bB$，且 $K_0=K_A$，其明文和密钥是 v_0 产生的；其次是 $h=N_b$，且 $K_0=K_B$ 其明文和密钥是 v_3 产生的。因此需要使用到命题 4.1 的结论，同时也解释了命题 5.3 中的题设(2)，要求两个私钥都确保未被泄露。 ※

4．NSL 协议发起者的保密性和认证性

命题 5.4 （保密性）假定下述条件成立：

(1) Σ是一个 NSL 串空间，C 是Σ中的某个丛，s 是 C 中的一个发起者串，s 的迹为 $\mathrm{Init}[A, B, N_a, N_b]$；

(2) $K_A^{-1} \notin \mathbf{Kp}$，$K_B^{-1} \notin \mathbf{Kp}$；

(3) $N_a \neq N_b$，且 N_a 唯一起源于串空间Σ。

则对于所有的节点 $m \in C$，$N_a \subset \mathrm{uns\_term}(m)$，满足 $\{N_aN_bB\}_{K_A} \subset \mathrm{uns\_term}(m)$ 或者 $\{N_aA\}_{K_B} \subset \mathrm{uns\_term}(m)$，而且 $N_a \neq \mathrm{uns\_term}(m)$。

证明：此命题的证明与命题 5.3 类似。 ※

命题 5.5 （认证性）假定下述条件成立：

(1) Σ是一个 NSL 串空间，C 是Σ中的某个丛，s 是 C 中的一个发起者串，s 的迹为 $\mathrm{Init}[A, B, N_a, N_b]$，且 s 的丛高度为 3；

(2) $K_A^{-1} \notin \mathbf{Kp}$，$K_B^{-1} \notin \mathbf{Kp}$；

(3) N_a 唯一起源于串空间Σ。

则丛 C 包含一个响应者串 $t \in \mathrm{Resp}[A, B, N_a, N_b]$，且 t 的丛高度至少为 2。

说明：相对于命题 5.1，此命题的假定更为严格。显然，如果 $K_B^{-1} \notin \mathbf{Kp}$，则攻击者可以完全替代角色 B 完成和 A 的通信。

证明：考察节点集合 $\{n \in C: \{N_aN_bB\}_{K_A} \subset \mathrm{uns\_term}(n)\}$。因为它包含节点 $\langle s, 2\rangle$，集合非空，所以它包含最小元节点 m_0。如果节点 m_0 位于正规串 t 上，则 $t \in \mathrm{Resp}[A, B, N_a, N_b]$，且丛高度至少为 2；如果节点 m_0 位于攻击者串 t 上，则 t 将是一个 E 类型串，迹为 $\langle -K_A, -N_aN_bB, +\{N_aN_bB\}_{K_A}\rangle$，命题 5.4 指出 N_a 不能以明文的形式出现，所以 m_0 不可能在攻击者串 t 上。 ※

命题 5.5 假如Σ是一个 NSL 串空间，N_b 唯一起源于Σ，则对于任意 A、B

和 N_a 至多存在一个响应者串 $t \in \text{Resp}[A, B, N_a, N_b]$，前提是 $N_a \neq N_b$。

证明：假设 $t \in \text{Resp}[A, B, N_a, N_b]$，因为 $N_b \subset \text{uns\_term}(<t, 2>)$，又因为 $\text{uns\_term}(<t, 2>) = \{N_a\}_{K_a}$，且 $N_a \neq N_b$，因此 N_b 起源于此串，由 N_b 的唯一起源性可知Σ中至多有一个 t。 ※

5.2 Yahalom 协议的 Strand Space 模型及分析

5.2.1 Yahalom 协议

我们讨论Gavin Low在文献[55]中提出的Yahalom协议[2]的修改版。协议形式化描述如下：

(1) $A \rightarrow B$ ： AN_a

(2) $B \rightarrow S$ ： $\{AN_aN_b\}_{KBS}$

(3) $S \rightarrow A$ ： $\{BK_{AB}N_aN_b\}_{KAS}$

(4) $S \rightarrow B$ ： $\{AK_{AB}\}_{KBS}$

(5) $A \rightarrow B$ ： $\{ABSN_b\}_{KAB}$

其中 A、B、S 为协议主体，N_a、N_b 为新鲜的随机数，K_{AS}、K_{BS}、K_{AB} 为协议主体间共享的对称密钥。

协议的目的：S 为协议主体 A，B 产生并发送共享会话密钥 K_{AB}，并确保 K_{AB} 的机密性；同时 B 能认证 A。

5.2.2 Yahalom 串空间

在文献[10]中，作者曾提到他们利用串空间理论验证了 Yahalom 协议，但并未发现他们公开发表对 Yahalom 协议的分析结果。

首先给出以下约定：集合 $\mathbf{T}_{\text{name}} \subset \mathbf{T}$，其集合元素为协议主体的名称；映射 K: $\mathbf{T}_{\text{name}} \rightarrow \mathbf{K}$，$K$ 将协议主体名称映射到该主体和服务器 S 间共享的长期密钥，例如 $K(A)=K_{AS}$。假定该映射 K 为一一映射，且 $K_{AS}=K_{AS}^{-1}$（即协议使用对称密码）；变量 A，B 在 $\mathbf{T}_{\text{name}}$ 上取值；变量 K 在 $\mathbf{K}$ 上取值；变量 N，M 在 $\mathbf{T} \backslash \mathbf{T}_{\text{name}}$ 上取值，即 N，M 不是协议主体的名称。

定义 5.2 Yahalom 串空间（如图 5-4 所示）

(1) 集合 $\text{Init}[A, B, S, N, M, K]$ 中的元素 $s \in \Sigma$ 且 s 具有如下迹：

$$<+AN, -\{BKNM\}_{KAS}, +\{ABSM\}_K>$$

和某个 $s \in \text{Init}[A, B, S, N, M, K]$ 相关联的协议主体是 A。

(2) 集合 Resp[A, B, S, N, M, K]中的元素 $s\in\Sigma$且 s 具有如下迹：

$$<-AN, +\{ANM\}_{KBS}, -\{AK\}_{KBS}, -\{ABSM\}_{K}>$$

和某个 $s\in$Resp[A, B, S, N, M, K]相关联的协议主体是 B。

(3) 集合 Serv[A, B, S, N, M, K]，其中 $K\notin\mathbf{K_P}$ 且 $K\notin\{K_{AS}: A\in\mathbf{T_{name}}\}$且 $K=K^{-1}$，该集合中的元素 $s\in\Sigma$且 s 具有如下迹：

$$<-\{ANM\}_{KBS}, +\{BKNM\}_{KAS}, +\{AK\}_{KBS}>$$

和某个 $s\in$Serv[A, B, S, N, M, K]相关联的协议主体是 S_0。

为方便起见，我们用*来代替某些可变的项，例如，对 N 和 M。

Yahalom 串空间是一个渗入串空间Σ，Σ=Init∪Resp∪Serv∪**P**。其中 **P** 代表侵入者串的集合。

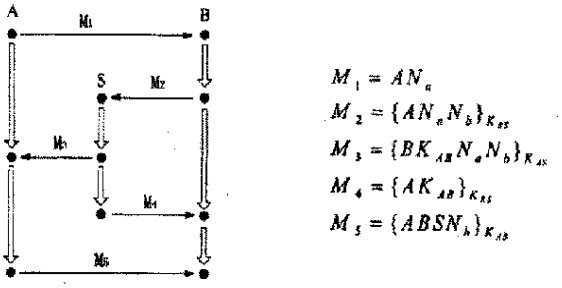


图 5-4 Yahalom 协议 Strand Space 模型的 boundle 图

5.2.3 Yahalom 协议正确性分析

1．保密性

(1) S 分发的会话密钥的保密性

我们要证明出服务器 S 发布的会话密钥 K 不会泄露，除非侵入者拥有某一长期密钥 K_{AS} 或 K_{BS}。也就是说我们要说明会话密钥 K 绝对不会以这样的形式出现：K 被非协议主体所持有的长期密钥所加密。

命题 5.7 假定 C 是 Yahalom 串空间Σ中的一个丛；A，$B\in\mathbf{T_{name}}$；K 是唯一起源的；K_{AS}，$K_{BS}\notin\mathbf{K_P}$；且 $s_{serv}\in$Serv[A, B, S, N, M, K]。让 $\mathbf{S}=\{K_{AS}, K_{BS}, K\}$ 且 $\acute{\mathbf{K}}=\mathbf{K}\backslash\mathbf{S}$。则对每个节点 $m\in C$，term(m)$\notin\mathbf{I}_{\acute{\mathbf{K}}}[K]$。

证明：由命题 4.2，我们可转化为证明更强的命题：对每个节点 $m\in C$，term(m)$\notin\mathbf{I}_{\acute{\mathbf{K}}}[\mathbf{S}]$。由于 $\mathbf{S}\cap\mathbf{K_P}=\varnothing$，$\acute{\mathbf{K}}=\acute{\mathbf{K}}^{-1}$ 且 $\mathbf{K}=\acute{\mathbf{K}}\cup\mathbf{S}$，由推论 4.2，仅需证明不存在正常节点 m 是 $\mathbf{I}_{\mathbf{K}}[\mathbf{S}]$的进入点即可。

利用反证法，假定存在一个正常节点 m 是 $\mathbf{I}_{\dot{K}}[S]$的进入点。由此 term(m)必然为集合 $\mathbf{I}_{\dot{K}}[S]$的成员。由命题 4.2 和定义 4.8，这意味着 K_{AS}, K_{BS}和 K 中的某一个是 term(m)的子项。由图 5.2 可见，K_{AS}, K_{BS}并不是任何正常节点的消息项的子项。而 K 起源于服务器 S，故 K 是 term(m)的子项。

若 m 为某一个正常串 s 上的一个符号为正的正常节点，则 $K\sqsubset$term(m)意味着：

$s\in$Serv 且 $m=\langle s, 2\rangle$，这里 K 就是 s 的会话密钥，或者 $s\in$Serv 且 $m=\langle s, 3\rangle$

考虑情形 $s\in$Serv$[A, B, S, N, M, K]$且 $m=\langle s, 2\rangle$，由于 K 是唯一起源的，故 $s=s_{serv}$，所以 term(m)=$\{BKNM\}_{K_{AS}}$。由命题 4.4，$K_{AS}\in\dot{\mathbf{K}}$，与命题假设 $\dot{\mathbf{K}}=\mathbf{K}\backslash\mathbf{S}$ 矛盾。

对于情形 $s\in$Serv 且 $m=\langle s, 3\rangle$，由于 K 是唯一起源的，故 $s=s_{serv}$，所以 term(m)=$\{AK\}_{K_{BS}}$。由命题 4.4，$K_{BS}\in\dot{\mathbf{K}}$，与命题假设 $\dot{\mathbf{K}}=\mathbf{K}\backslash\mathbf{S}$ 矛盾。 ※

(2) B 的随机数的保密性

命题 5.8 假定 C 是 Yahalom 串空间Σ中的一个丛；A，$B\in\mathbf{T}_{name}$；M 是唯一起源的；K_{AS}，$K_{BS}\notin\mathbf{K}_P$；且 $s_{resp}\in$Resp$[A, B, S, N, M, K]$。让 $\mathbf{S}=\{K_{AS}, K_{BS}, M\}$ 且 $\dot{\mathbf{K}}=\mathbf{K}\backslash\mathbf{S}$。则对每个节点 $m\in C$，term(m)$\notin\mathbf{I}_{\dot{K}}[M]$。

证明：类似命题 5.7 的证明。 ※

2. 认证性

(1) B 认证 A 和 S

命题 5.9 假定 C 是 Yahalom 串空间Σ中的一个丛；$A\neq B$；在 C 中 N_b 是唯一起源的；且 K_{AS}、$K_{BS}\notin\mathbf{K}_P$。若 $s\in$Resp$[A, B, S, N_a, N_b, K]$且 C-height(s)=4，则 C 中必然存在正常串

1) $s_{init}\in$Init$[A, B, S, *, N_b, K]$且 C-height(s_{init})=3；

2) $s_{serv}\in$Serv$[A, B, S, N, M, K]$且 C-height(s_{serv})=3。

说明：为证明此命题，我们先引入引理 5.8-5.12 并证明之(见后)。

证明：据假设，s 在 C 中的迹至少包含：$\langle -AN_a, +\{AN_aN_b\}_{K_{AS}}, -\{AK\}_{K_{BS}}, -\{ABSN_b\}_K\rangle$，据引理 5.9，$\{ABSN_b\}_K$起源于 C 中的正常节点。据引理 5.12，该正常节点属于串 s_{init}，$s_{init}\in$Init$[A, B, S, N, N_b, K]$，这里 $N\in\mathbf{T}\backslash\mathbf{T}_{name}$。由于该节点为$\langle s_{init}, 3\rangle$且$\langle s_{init}, 3\rangle\in C$，故 C-height(s_{init})=3。

据引理 5.8，$\{AK\}_{K_{BS}}$起源于 C 中的正常节点。据引理 5.12，该正常节点属于串 s_{serv}，$s_{serv}\in$Serv$[A, B, S, N, M, K]$，这里 N、$M\in\mathbf{T}\backslash\mathbf{T}_{name}$。由于该节点为$\langle s_{serv}, 3\rangle$且$\langle s_{serv}, 3\rangle\in C$，故 C-height(s_{serv})=3。据引理 5.8，

term(<s_{serv}, 1>)=$\{ANM\}_{KBS}$起源于 C 中的正常串 s_1，再据引理 5.12 及在 C 中 N_b 是唯一起源的，故 $s_1=s$，且 $N=N_a$，$M=N_b$，从而 $s_{serv}\in$Serv[A, B, N_a, N_b, K]。

由此可见 B 能够认证 A 和 S。 ※

引理 5.8 考虑 Yahalom 串空间Σ中的一个丛 C。假定 $X\in\mathbf{T}_{name}$ 使得 $K_{XS}\notin\mathbf{K_P}$。则对 $X\in\mathbf{T}_{name}$，不存在这样的消息项，该消息项起源于 C 中的一个侵入者节点且形如$\{g\}_{KXS}$。

证明：让 $\mathbf{S}=\{K_{XS}\}$且 $\acute{\mathbf{K}}=\mathbf{K}$。为了利用推论 4.3，必须首先证明不存在任何的正常节点是 $\mathbf{I}_{\acute{\mathbf{K}}}$[**S**]的进入点。等价地，必须证明 K_{XS} 不起源于任何正常节点。

正如在命题 5.7 证明过程中所得到的结果，对于 Yahalom 串空间Σ中的密钥，只有会话密钥 K 才起源于正常节点。而 K 不属于长期密钥集合$\{K_{XS}\}$。因此根据推论 4.3 有：形如$\{g\}_{KXS}$的消息项只能起源于正常节点。 ※

引理 5.9 考虑 Yahalom 串空间Σ中的一个丛 C。假定 K 是唯一起源的，则不存在这样的消息项，该消息项起源于 C 中的一个侵入者节点且形如$\{g\}_K$。

证明：反证。假定 $t_1=\{g\}_K$起源于一个侵入者节点 m。根据攻击者模型的描述，m 不可能出现在类型为 F、T、K、M、C 或 S 的侵入者串上。考虑剩下的情形：

E. 攻击者串形式为<-K_0, -h, +$\{h\}_{K0}$>。根据命题 5.7，$K\neq K_0$，而$\{g\}_K\sqsubset\{h\}_{K0}$，据推论 4.1 有$\{g\}_K\sqsubset h$。与进入点的定义矛盾。

D. 攻击者串形式为<-K^{-1}, -$\{h\}_K$, +h>。而$\{g\}_K\sqsubset h$，故$\{g\}_K\sqsubset\{h\}_K$。与进入点的定义矛盾。 ※

引理 5.10 如果$\{H\}_{KXS}$起源于正常串 s，则 $s\notin$Init 且

1) 如果 $s\in$Serv[A, B, S, N, M, K]，则 $H=YKNM$ 或者 $H=YK$，其中 $Y\in T_{name}$，$K\in$**K**，N、$M\in\mathbf{T}\backslash\mathbf{T}_{name}$；

2) 如果 $s\in$Resp[A, B, S, N, M, K]，则 $H=YNM$，其中 $Y\in\mathbf{T}_{name}$，而 N、$M\in\mathbf{T}\backslash\mathbf{T}_{name}$。

证明：由定义 4.4，若$\{H\}_{KXS}$起源于节点 m，则节点 m 的符号为正。故 $s\notin$Init。若 $s\in$Init[A, B, S, N, M, K]，则 m 只能等于<s, 2>，但<s, 2>符号为负。

若 $s\in$Serv[A, B, S, N, M, K]，则 m=<s, 2>或者 m=<s, 3>。故 term(m)形如$\{YKNM\}_{KXS}$或者$\{YK\}_{KXS}$。

若 $s\in$Resp [A, B, S, N, M, K]，则 m=<s,2>。故 term(m)形如$\{YNM\}_{KXS}$。 ※

引理 5.11 如果$\{H\}_K$起源于正常串 s，则 $s\in$Init 且 $H=XYZM$ 其中 X、Y

和 $Z \in \mathbf{T}_{name}$，$M \in \mathbf{T} \backslash \mathbf{T}_{name}$。

证明：s 只可能属于 Init[A, B, S, N, M, K]或者 Resp[A, B, S, N, M, K]。由定义 4.4，若 $\{H\}_K$ 起源于节点 m，则节点 m 的符号为正。若 $s \in$ Resp[A, B, S, N, M, K]，则 m 只能等于<s, 4>，但<s, 4>的符号为负。故 $s \notin$ Resp[A, B, S, N, M, K]。若 $s \in$ Init[A, B, S, N, M, K]，则 m=<s, 3>，故 term(m)形如 $\{XYZM\}_K$。 ※

引理 5.12 假定 s 是 Yahalom 串空间Σ中的一个正常串，且 $A \neq B$

1）若 $\{BKNM\}_{KAS}$ 起源于 s，则 $s \in$ Serv[A, B, S, N, M, K]，该消息项起源于节点<s, 2>且密钥 K 也起源于 s；

2）若 $\{AK\}_{Kbs}$ 起源于 s，则对 N、$M \in \mathbf{T} \backslash \mathbf{T}_{name}$，$s \in$ Serv[A, B, S, N, M, K]，该消息项起源于节点<s, 3>；

3）若 $\{ANM\}_{Kbs}$ 起源于 s，则对 $K \in \mathbf{K}$，$s \in$ Resp[A, B, S, N, M, K]，该消息项起源于节点<s, 2>。M 起源于 s；

4）若 $\{ABSM\}_K$ 起源于 s，则对 $N \in \mathbf{T} \backslash \mathbf{T}_{name}$，$s \in$ Init[A, B, S, N, M, K]，该消息项起源于节点<s, 3>。

证明：由于 s 是正常串，$s \in$ Serv $\cup$ Init $\cup$ Resp。Serv、Init、Resp 三集合两两不相交，由引理 5.10 和引理 5.11 很容易得证。 ※

(2) A 认证 B 和 S

命题 5.10 假定 C 是 Yahalom 串空间Σ中的一个丛；$A \neq B$；且 K_{AS}、$K_{BS} \notin \mathbf{K_P}$。若 $s \in$ Init[A, B, S, N_a, N_b, K]且 C-height(s)=3，则 C 中必然存在正常串

1) $s_{resp} \in$ Resp[A, B, S, N_a, N_b, K]且 C-height(s_{resp})至少为 2；

2) $s_{serv} \in$ Serv[A, B, S, N, M, K]且 C-height(s_{serv})至少为 2。

证明：据假设，s 在 C 中的迹至少包含：<+AN_a, -$\{BKN_aN_b\}_{KAS}$, +$\{ABSN_b\}_K$>，据引理 5.8，$\{BKN_aN_b\}_{KAS}$ 起源于 C 中的正常节点。据引理 5.12，该正常节点属于串 s_{serv}，$s_{serv} \in$ Serv[A, B, S, N_a, N_b, K]。由于该节点为<s_{serv}, 2>且<s_{serv}, 2>$\in C$，故 C-height(s_{serv})至少为 2。据引理 5.8，$term$(<s_{serv}, 1>)=$\{AN_aN_b\}_{Kbs}$ 起源于 C 中的正常节点，再据引理 5.12，该正常节点属于串 s_{resp}，$s_{resp} \in$ Resp[A, B, S, N_a, N_b, K]。由于该节点为<s_{resp}, 2>且<s_{resp}, 2>$\in C$，故 C-height(s_{resp})至少为 2。 ※

虽然协议设计的意图是让 B 从 A 收到 $\{ABSN_b\}_K$，但是我们无法阻止侵入者替换或阻断该消息。因此不能证明 B 的 C-height 至少为 4。同样，无法确定 B 是否收到 $\{AK\}_{Kbs}$，从而无法确定 S 是否发出 $\{AK\}_{Kbs}$，故不能证明 S 的 C-height 至少为 3。

(3) S 认证 A 和 B

命题 5.11 假定 C 是 Yahalom 串空间Σ中的一个丛；$A \neq B$；在 C 中 K 是唯一起源的；且 K_{AS}、$K_{BS} \notin \mathbf{K_P}$。若 $s \in \text{Serv}[A, B, S, N_a, N_b, K]$ 且 $C\text{-height}(s)=3$，则 C 中必然存在正常串 $s_{\text{resp}} \in \text{Resp}[A, B, S, N_a, N_b, *]$ 且 $C\text{-height}(s_{\text{resp}})$ 至少为 2；

证明：据假设，s 在 C 中的迹至少包含：$<-\{AN_aN_b\}_{K_{BS}}, +\{BKN_aN_b\}_{K_{AS}}, +\{AK\}_{K_{BS}}>$，据引理 5.8，$\{AN_aN_b\}_{K_{BS}}$ 起源于 C 中的正常节点。据引理 5.12 该正常节点属于 s_{resp}，$s_{\text{resp}} \in \text{Resp}[A, B, S, N_a, N_b, K']$，这里 $K' \in \mathbf{K}$。由于该节点为 $<s_{\text{resp}}, 2>$ 且 $<s_{\text{resp}}, 2> \in C$，故 $C\text{-height}(s_{\text{resp}})$ 至少为 2。 ※

虽然协议设计的意图是让 B 从 S 收到 $\{AK\}_{K_{BS}}$，但是无法阻止侵入者替换或阻断该消息。故不能证明 B 的 C-height 至少为 3。同样虽然协议设计的意图是让 A 从 S 收到 $\{BKN_aN_b\}_{K_{AS}}$，但是无法阻止侵入者替换或阻断该消息。故不能证明 A 的 C-height 至少为 2。而且在证明了 B 的 C-height 至少为 2 以后，虽然可以确信 B 收到了 AN，但是无法确认 AN 是来自 A 还是来自侵入者。故 S 无法认证 A。

5.3 一种传输模型的认证协议的 Strand Space 模型及分析

5.3.1 一种传输模型的认证协议

1. 传输模型

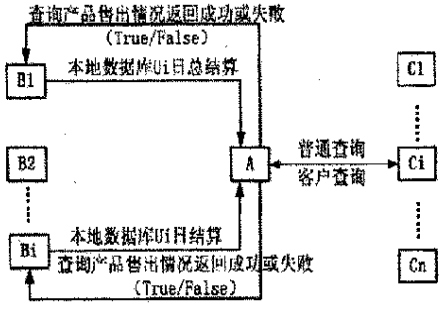


图 5-5 传输模型

在图 5-5 中，A 表示某公司总部；Bi 代表第 i 个销售处（i=1,2...）；Ui 表示第 i 个销售处日结算时需要上传的数据库；C 表示普通用户。

2．协议形式化描述[56]

(1) $A \rightarrow S$ ： AB_iN_a

(2) $S \rightarrow B_i$ ： $\{AK\}_{KBi}\{B_iKN_a\}_{KA}$

(3) $B_i \rightarrow A$ ： $\{B_iKN_a\}_{KA}$

(4) $A \rightarrow B_i$ ： $\{\text{“get”}\}_K$

其中A、B_i为协议主体，S是服务器，N_a为新鲜的随机数，K_A、K_{Bi}是协议主体与服务器间共享的对称密钥，K是服务器为A和B_i分配的共享会话密钥。

协议的目的：S为协议主体A，B_i产生并发送共享会话密钥K，并确保K的机密性；同时主体之间，主体与服务器之间能有效鉴别。

5.3.2 传输认证协议的串空间

首先给出以下约定：集合 $\mathbf{T}_{name} \subset \mathbf{T}$，其集合元素为协议主体的名称；映射 K: $\mathbf{T}_{name} \rightarrow \mathbf{K}$，$K$将协议主体名称映射到该主体和服务器 S 间共享的长期密钥，例如 K_A 即为 K_{AS}，假定该映射 K 为一一映射，且 $K_A=K_A^{-1}$（即协议使用对称密码）；变量 A, B_i 在 $\mathbf{T}_{name}$ 上取值；变量 K 在 $\mathbf{K}$ 上取值；变量 N_a 在 $\mathbf{T}\backslash\mathbf{T}_{name}$ 上取值，即 N_a 不是协议主体的名称。

定义 5.3 传输认证协议串空间（如图 5-6 所示）

(1) 集合 Init[A, B_i, S, N_a, K]中的元素 $s \in \Sigma$且 s 具有如下迹：

$$\langle +AB_iN_a, -\{B_iKN_a\}_{KA}, +\{\text{“get”}\}_K \rangle$$

和某个 $s \in$ Init[A, B_i, S, N_a, K]相关联的协议主体是 A。

(2) 集合 Resp[A, B_i, S, N_a, K]中的元素 $s \in \Sigma$且 s 具有如下迹：

$$\langle -\{AK\}_{KBi}\{B_iKN_a\}_{KA}, +\{B_iKN_a\}_{KA}, -\{\text{“get”}\}_K \rangle$$

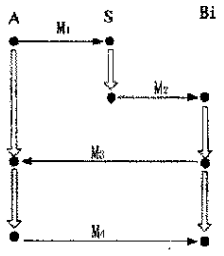
和某个 $s \in$ Resp[A, B_i, S, N, K]相关联的协议主体是 B_i。

(3) 集合 Serv[A, B_i, S, N_a, K]，其中 $K \notin \mathbf{K_P}$ 且 $K \notin \{K_{AS}: A \in \mathbf{T}_{name}\}$ 且 $K=K^{-1}$，该集合中的元素 $s \in \Sigma$且 s 具有如下迹：

$$\langle -AB_iN_a, +\{AK\}_{KBi}\{B_iKN_a\}_{KA} \rangle$$

和某个 $s \in$ Serv[A, B_i, S, N_a, K]相关联的协议主体是 S。

传输认证协议协议串空间是一个渗入串空间Σ，Σ=Serv∪Init∪Resp∪$\mathbf{P}$。其中$\mathbf{P}$代表侵入者串的集合。



$M_1=AB_iN_a$

$M_2=\{AK\}_{KBi}\{B_iKN_a\}_{KA}$

$M_3=\{B_iKN_a\}_{KA}$

$M_4=\{\text{"get"}\}_K$

图 5-6 传输认证协议 Strand Space 模型的 boundle 图

5.3.3 协议正确性分析

1．保密性

(1) S 分发的会话密钥的保密性

我们要证明由服务器 S 发布的会话密钥 K 不会泄露，除非侵入者拥有某一长期密钥 K_{AS} 或 K_{BS}。也就是说我们要说明会话密钥 K 绝对不会以这样的形式出现：K 被非协议主体所持有的长期密钥所加密。

命题 5.12 假定 C 是传输认证串空间Σ中的一个丛；A，B_i，$S\in\mathbf{T}_{name}$；K 是唯一起源的；K_A、$K_{Bi}\notin\mathbf{K_P}$；且 $s_{serv}\in\text{Serv}[A, B_i, S, N_a, K]$。让 $\mathbf{S}=\{K_A, K_{Bi}, K\}$ 且 $\acute{\mathbf{K}}=\mathbf{K}\backslash\mathbf{S}$。则对每个节点 $m\in C$，$\text{term}(m)\notin\mathbf{I}_{\acute{K}}[K]$。

证明：由命题 4.2，我们可转化为证明更强的命题：对每个节点 $m\in C$，$\text{term}(m)\notin\mathbf{I}_{\acute{K}}[\mathbf{S}]$。由于 $\mathbf{S}\cap\mathbf{K_P}=\varnothing$，$\acute{\mathbf{K}}=\acute{\mathbf{K}}^{-1}$ 且 $\mathbf{K}=\acute{\mathbf{K}}\cup\mathbf{S}$，由推论 4.2，仅需证明不存在正常节点 m 是 $\mathbf{I}_{\acute{K}}[\mathbf{S}]$的进入点即可。

利用反证法，假定存在一个正常节点 m 是 $\mathbf{I}_{\acute{K}}[\mathbf{S}]$的进入点。由此 $\text{term}(m)$ 必然为集合 $\mathbf{I}_{\acute{K}}[\mathbf{S}]$的成员。由命题 4.2 和定义 4.8，这意味着 K_A，K_{Bi}和 K 中的某一个是 $\text{term}(m)$的子项。由图 5.2 可见，K_A，K_{Bi}并不是任何正常节点的消息项的子项。而 K 起源于服务器 S，故 K 是 $\text{term}(m)$的子项。

若 m 为某一个正常串 s 上的一个符号为正的正常节点，则 $K\sqsubset\text{term}(m)$意味着 $s\in\text{Serv}$ 且 $m=\langle s, 1\rangle$，这里 K 就是 s 的会话密钥。由于 K 是唯一起源的，故 $s=s_{serv}$，所以 $\text{term}(m)=\{AK\}_{KBi}\{B_iKN_a\}_{KA}$。由命题 4.4，有 K_A、$K_{Bi}\in\acute{\mathbf{K}}$，这与命题假设 $\acute{\mathbf{K}}=\mathbf{K}\backslash\mathbf{S}$ 矛盾。 ※

(2) A 的随机数的保密性

显然，由于随机数 N_a 是明文传输，无法保障其保密性。

2．认证性

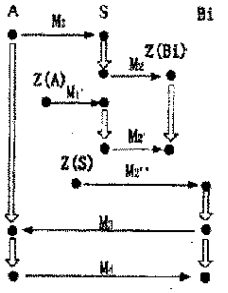
(1) S 认证 A

由于主体 S 与 A 之间只有一次数据传送，没有消息交互，且随机数 N_a 是明文传输，所以 S 无法认证 A，即无法确认消息项 AN_a 是来自合法主体 A 还是来自侵入者 P。

(2) B_i 认证 S

由于 S 发出的消息没有随机数或私有信息来保证消息的新鲜性、唯一性，所以无法防止被攻击者截取后重放，故 B_i 无法认定 S。

3．协议攻击方法描述



$M_1=AB_iN_a$

$M_2=\{AK\}_{KBi}\{B_iKN_a\}_{KA}$

$M_1'=AB_iN_a'$

$M_2'=\{AK'\}_{KBi}\{B_iK'N_a'\}_{KA}$

$M_2''=\{AK'\}_{KBi}\{B_iKN_a\}_{KA}$

$M_3=\{B_iKN_a\}_{KA}$

$M_4=\{\text{“get”}\}_K$

图 5-7 协议漏洞——不匹配的会话密钥

攻击的形式化描述如下（如图5-7所示）：

(1) $A\rightarrow S$ ： AB_iN_a

(2) $S\rightarrow Z(B_i)$ ： $\{AK\}_{KBi}\{B_iKN_a\}_{KA}$

1) $Z(A)\rightarrow S$ ： AB_iN_a'

2) $S\rightarrow Z(B_i)$ ： $\{AK'\}_{KBi}\{B_iK'N_a'\}_{KA}$

(2') $Z(S)\rightarrow B_i$ ： $\{AK'\}_{KBi}\{B_iKN_a\}_{KA}$

(3) $B_i\rightarrow A$ ： $\{B_iKN_a\}_{KA}$

(4) $A\rightarrow B_i$ ： $\{\text{“get”}\}_K$

说明：以上攻击是由“无法认证”这个漏洞产生的，“B_i 无法认证 S”同样可构造出类似的攻击：当 A 向服务器 S 申请与 B_i、B_k（其中 $i\neq k$）的共享密钥时，攻击者可截获服务器 S 发给 B_i 或 B_k 的消息项，然后重置后转发给

B_i或B_k以制造不匹配的会话密钥。

显然，A得到的共享会话密钥是K，而B_i得到的共享会话密钥确是K'，这样原协议第4步对共享密钥的校验也是徒劳的。可见该协议在实际运用中无法抵御攻击者蓄意的破坏，同时也无法防止因此漏洞的存在B_i的抵赖行为，以拖延上报数据的时间。当然，此漏洞不是致命的，因为共享密钥并未泄漏。

4．协议改进

改进协议形式化描述如下：

(1) $A \rightarrow S$ ： $\{AB_iN_a\}_{K_A}$

(2) $S \rightarrow B_i$ ： $\{A, K, \{B_iKN_a\}_{K_A}\}_{K_{Bi}}$

(3) $B_i \rightarrow A$ ： $\{B_iKN_a\}_{K_A}$

同时，服务器数据库记录每次收到的AB_iN_a，对于已有记录的AB_iN_a对不再发放会话密钥，以防止攻击者重放、截取制造不匹配密钥。

5.4 ISI支付协议的Strand Space模型及其公平性分析

5.4.1 ISI支付协议

假定在完成了交易双方的身份认证之后，ISI协议[57]所执行的支付协议的形式化描述如下：

(1) $A \rightarrow B$ ： $\{\{\text{money}\}_{K_{CS}^{-1}}, SK_A, K\_ses, S\_id\}_{K_B}$

(2) $B \rightarrow CS$ ： $\{\{\text{money}\}_{K_{CS}^{-1}}, SK_B, \text{Transaction}\}_{K_{CS}}$

(3) $CS \rightarrow B$ ： $\{\{\text{new\_money}\}_{K_{CS}^{-1}}\}_{SK_B}$

(4) $B \rightarrow A$ ： $\{\{\text{amount, tid, date}\}_{K_B^{-1}}\}_{SK_A}$

其中A表示付款人（公司或企业），B是收款人，CS是货币服务器，其中SK_A、SK_B为主体A、B的签名公钥，K_A、K_B、K_{CS}为主体公钥，S_id为CS标识符，Transaction为交易名称，{amount, tid, date}为票据。

协议目的：B审核A的付款数目后向CS发出申请，并在收到付款后向A开据票据。

5.4.2 ISI 支付协议串空间

在给出协议的串空间模型之前，先给出以下约定：

集合$\mathbf{T}_{name}\subseteq\mathbf{T}$，其集合元素为协议主体的名称，集合**K**为密钥集合，包含协议主体的公钥/私钥、签名公钥/私钥、会话密钥，变量A，B，CS在$\mathbf{T}_{name}$上取值，变量K在**K**上取值，变量N，M在$\mathbf{T}\backslash\mathbf{T}_{name}$上取值，即$N$，$M$不是协议主体的名称。

定义5. 4 ISI支付协议串空间（如图5-8所示）

(1) 集合Init[N, SK_A, K_ses, S_id, M]中的元素$s\in\Sigma$且s具有如下迹：

$$<+\{N,SK_A,K\_ses,S\_id\}_{K_B},-\{M\}_{SK_A}>$$

与某个$s\in$Init[N, SK_A, K_ses, S_id, M]相关联的协议主体是A。

(2) 集合Resp[N, SK_B, Transtion, N', M]中的元素$s\in\Sigma$且s具有如下迹：

$$<-\{N,SK_A,K\_ses,S\_id\}_{K_B},+\{N,SK_B,\text{Transaction}\}_{K_{CS}},-\{N'\}_{SK_B},+\{M\}_{SK_A}>$$

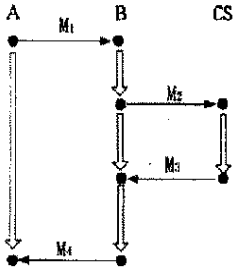
与某个$s\in$Resp[N, SK_B, Transtion, N', M]相关联的协议主体是B。

(3) 集合Serv[N, SK_B, Transtion, N']，该集合中的元素$s\in\Sigma$且s具有如下迹：

$$<-\{N,SK_B,\text{Transaction}\}_{K_{CS}},+\{N'\}_{SK_B}>$$

与某个$s\in$Serv[N, SK_B, Transtion, N']相关联的协议主体是CS。

ISI支付协议串空间是一个渗入串空间Σ，Σ=Serv∪Init∪Resp∪**P**。其中**P**代表侵入串的集合。



M1=$\{\{\text{money}\}_{K_{CS}^{-1}},SK_A,K\_ses,S\_id\}_{K_B}$

M2=$\{\{\text{money}\}_{K_{CS}^{-1}},SK_B,\text{Transaction}\}_{K_{CS}}$

M3=$\{\{\text{new\_money}\}_{K_{CS}^{-1}}\}_{SK_B}$

M4=$\{\{\text{amount, tid, date}\}_{K_B^{-1}}\}_{SK_A}$

图5-8 ISI支付协议Strand Space模型

5.4.3 ISI支付协议公平性分析

1. 公平性分析

为了满足公平性在Strand Space模型中的分析，我们对ISI支付协议的公平性做如下更具体的定义。

定义5.5 ISI支付协议是公平的，如果B收到付款，当且仅当A收到收据。

命题5.14 假定C是ISI支付协议串空间Σ中的一个丛，若$s \in \text{Init}[N, SK_A, K_ses, S_id, M]$且$C\text{-height}(s)=2$，则$C$中必然存在正常串

$$s_{\text{resp}} \in \text{Resp}[N, SK_B, \text{Transtion}, N', M] \text{且} C\text{-height}(s_{\text{resp}})=4$$

证明：由假设$s \in \text{Init}[N, SK_A, K_ses, S_id, M]$且$C\text{-height}(s)=2$，$s$在$C$中的迹为：$\langle +\{N, SK_A, K\_ses, S\_id\}_{K_B}, -\{M\}_{SK_A} \rangle$，其中$\text{uns_term}\langle s, 2\rangle = \{M\}_{SK_A}$，$M = \{\text{amount}, \text{tid}, \text{date}\}_{K_B^{-1}}$，根据攻击者模型的描述，包含消息项$M$的节点一定不在入侵者串上，故$\text{uns_term}\langle s, 2\rangle$起源于$C$中的正常节点。

又$\text{uns_term}\langle s, 2\rangle$属于串$s_{\text{resp}}$和$s_{\text{init}}$，但$s_{\text{resp}} \in \text{Resp}[N, SK_B, \text{Transtion}, N', M]$中该节点$\langle s_{\text{resp}}, 4\rangle$符号才为正，由串空间性质可知，$\text{uns_term}\langle s, 2\rangle$的唯一源节点为$\langle s_{\text{resp}}, 4\rangle$且$\langle s_{\text{resp}}, 4\rangle \in C$，由此可证$C\text{-height}(s_{\text{resp}})=4$。

可见，若有$C\text{-height}(s)=2$，则定有$C\text{-height}(s_{\text{resp}})=4$，即当$A$收到票据时，$B$一定收到了款项。 ※

命题5.15 假定C是ISI支付协议串空间Σ中的一个丛，若$s \in \text{Resp}[N, SK_B, \text{Transtion}, N', M]$且$C\text{-height}(s)=3$，则$C$中必然存在正常串

$$s_{\text{init}} \in \text{Init}[N, SK_A, K\_ses, S\_id, M] \text{且} C\text{-height}(s_{\text{init}})=2$$

证明：由假设，$s \in \text{Resp}[N, SK_B, \text{Transtion}, N', M]$且$C\text{-height}(s)=3$，$s$在$C$中的迹至少包含：

$$\langle -\{N, SK_A, K\_ses, S\_id\}_{K_B}, +\{N, SK_B, \text{Transaction}\}_{K_{CS}}, -\{N'\}_{SK_B} \rangle$$

由协议之前的身份认证协议可知N是A从CS处唯一获得，故在此协议中$\text{subterm}\langle s, 1\rangle = N$唯一源发于$C$中的正常节点$\langle s_{\text{init}}, 1\rangle$且$\langle s_{\text{init}}, 1\rangle \in C$，故$C\text{-height}(s_{\text{init}})$至少为1。

虽然协议设计的意图是让B从A收到$\{M\}_{SK_A}$，但是我们在假设B收到款项的前提下不能保证B的C-height为4，即不能保证$\{M\}_{SK_A}$的产生，故无法确定A是否收到$\{M\}_{SK_A}$，从而无法证明A的C-height为2。 ※

可见，若有$C\text{-height}(s)=3$，不一定有$C\text{-height}(s_{\text{init}})=2$，即当$B$收到款项时，$A$不一定收到票据，这对$A$是不公平的。

由命题5.15的证明结果可见，ISI支付协议不能保证公平性。与文献[58]结论相同。

2．协议改进

改进协议形式化描述如下：

(1) $A \rightarrow B$ ： $\{\{\text{money}\}_{K_{CS}^{-1}}, SK_A, K\_ses, S\_id\}_{K_B}$

(2) $B \rightarrow CS$ ： $\{\{\text{money}\}_{K_{CS}^{-1}}, SK_A, SK_B, \text{Transaction}, \{\text{amount, tid, date}\}_{K_B^{-1}}\}_{K_{CS}}$

(3) $CS \rightarrow B$ ： $\{\{\text{new\_money}\}_{K_{CS}^{-1}}\}_{SK_B}$

(4) $CS \rightarrow A$ ： $\{\{\text{amount, tid, date}\}_{K_B^{-1}}\}_{SK_A}$

以上修改是建立在CS的诚信基础上，B将票据传给CS，由CS代转给A。

结 论

作为网络安全的重要课题之一，安全协议的研究和分析已有二十多年的历史，安全领域的科学家已经开发了许多不同种类的形式化方法和理论，本文首先对安全协议形式化分析方法二十多年来的发展进行了综述介绍，经过对现有的形式化分析方法的分析和比较，我们选择了 Strand Space 模型作为本文的研究对象。

Strand Space 模型是现有安全协议形式化方法中最为直观、简洁、严格和有效的方法，它充分吸收了前人的研究成果。它的直观性表现在使用一种节点间存在因果关系的有向图来表示协议的运行；它的简洁性表现在对于小型协议完全可以使用手工的方法完成证明；它的严格性表现在它使用了节点之间的因果关系来确保证明的逻辑性和证明的正确性；它的有效性可以通过文中给出的实例来说明。

本文在深入研究 Strand Space 理论的基础上，运用该理论对若干协议进行了分析。建立了 Yahalom 协议的 Strand Space 模型，并进行了深入的讨论；建立了一种传输模型的认证协议的 Strand Space 模型，通过分析，发现协议存在漏洞，并构造出了攻击，针对漏洞对协议进行了改进；将 Strand Space 理论运用到对 ISI 支付协议公平性的分析，得到了与其他分析方法一致的结果。

通过以上的研究和应用可以发现，虽然 Strand Space 理论研究已取得显著成果，但其理论本身仍处于发展阶段，进一步的工作应从以下几方面开展：

1. 扩展语言描述能力，使之能运用到更多类型的应用型协议的分析中；
2. 开发模型的形式推理或检测的自动工具；
3. 将理论运用于安全协议说明与设计阶段，减小发现错误的代价。

本文所做的工作，只是对丰富形式化分析研究方法进行了一些有益的尝试，我们相信，通过更多的研究和探索，安全协议的形式化分析将会有着更加辉煌的前景。

致 谢

首先要感谢我的导师何大可教授三年来对我的帮助和教育。何老师严谨的治学态度和谆谆教诲以及渊博的学识和独到的见解，给我以极大的鼓舞和启迪，不仅让我在研究生阶段学到了大量的专业知识，树立了我正确的治学态度，而且让我在何老师那里学到了谦逊、乐观、积极、热情的生活态度。在未来的人生旅途中，我将永远铭记何老师的言传身教，这是我生命中宝贵的财富。

感谢彭代渊、唐小虎老师，我所取得的成绩与他们辛勤的授业解惑密不可分。

感谢成都30所刘璟博士后在我论文期间给我的帮助，不断的提供信息，乐于与我分享他的知识。

感谢西南交通大学计算机安全和通信保密研究所的师兄、师姐、同学和朋友们，他们都给了我无私的帮助和莫大的启迪，他们是：王剑波、缪祥华、张文芳、余位驰、郑宇、赖欣、路献辉、周承毅、武强、李文、刘影等，在此无法一一列举。我会永远想念这个我们共同营造的相亲相爱、互助合作，如同一个大家庭一样的实验室。

感谢我的父母把我带到这个世界，并给了我智慧和力量，让我可以体会到人生的酸甜苦辣。在我的成长过程中，父母倾注了大量的心血，含辛茹苦把我抚育成人，用朴质的言语和行动教会我做人的准则和做事的态度，没有他们就不可能有现在的我。是他们无私而伟大的爱让我永远都对未来充满信心，奋斗不已。他们永远是我的精神支柱。

感谢我的男友陈浩，伴我一路走来，不断给我鼓励和帮助，点点滴滴历历在目。

向所有关心、帮助过我的人们表示衷心的感谢！

参考文献

[1] D.Dolev and A.Yao. On the security of public key protocols. Technical Report, No.STAN-CS-81-854, Dept of Computer Science, Stanford University, May 1981.Also in Transactions on Information Theory, 1983, 29(2):198-208.

[2] M.Burrows, M.Abadi and R.Needham. A logic of authentication. ACM Transactions on Computer Systems, February 1990, 8(1): 18-36.

[3] G.Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In Tools and Algorithms for the Construction and Analysis of Systems, volume 1055 of Lecture Notes in Computer Science, Springer-Verlag, 1996, pages 147-166.

[4] J.C.Mitchell, M.Mitchell and U. Stern. Automated analysis of cryptographic protocols using murcp. In proceedings of the 1997 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 1997.

[5] J.Millen. The Interrogator model. In Proceedings of the 1995 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 1995, pages 251-260.

[6] R. Needham and M. Schroeder. Using encryption for authentication in large network of computers. Communications of the ACM, 1978, 12(12):993-999.

[7] F.Javier Thayer Fabrega, Jonathan C.Herzog and Joshua D.Guttman. StrandSpaces: Why is a security protocol correct? IEEE Computer Press, In Proceedings of the 1998 IEEE Symposium on Security and Privacy, 1998, pages 160-171.

[8] 冯登国，范红. 安全协议形式化分析理论与方法研究综述. 中国科学院研究生院学报, 2003, Vol.20, NoA: 389-406.

[9] Javier Thayer Fabrega, Jonathan C.Herzog, and Joshua D.Guttman. Honest Idealson Strand Spaces. In proceedings 11th IEEE Computer Security Foundations Workshop (CSFW), IEEE Computer Society, 1998, pages 66-77.

[10] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(2, 3):191-230.

[11] I.Cervesato, N. Durgin, M. Kanovich and A. Scedrov. Interpreting Strands in Linear Logic.In 2000 Workshop on Formal Methods and Computer Security——FMCS'00 (H.Veith, N. Heintze and E. Clark, editors), Chicago, IL, 20 July 2000.

[12] Paul. Syverson: "Towards a Strand Semantics for Authentication Logic". Electronic Notes in Theoretical Computer Science 20, 1999.

[13] D.X. Song. Athena: a new efficient automated checker for security protocol analysis. In Proceedings of the 12th IEEE Computer Security Foundations Workshop. IEEE Computer Society Press, June 1999.

[14] R. L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2):120-126.

[15] M.Mambo, K.Usuda and E.Okamoto. Proxy signatures: Delegation of the power to sign message. IEICE Trans Fundamentals, 1996, E79-A (9): 1338-1354.

[16] Yi L J, Bai G Q and Xiao G Z. Proxy multi-signature scheme: A new type of proxy signature scheme. Electronics Letters, 2000, 36(6): 527-528.

[17] 祁明, Harn L. 基于离散对数的若干新型代理签名方案. 电子学报, 2000, 28(11):114-115.

[18] Wang X, Fu F. Cryptanalysis of a proxy multisignature scheme. Journal of China Institute of Communications, 2002, 23(4): 98-102.

[19] Stefanos Gritzalis and Diomidis Spinellis. Cryptographic protocols over opendistributed systems: A taxonomy of flaws and related protocol analysis tools. In Peter Daniel, editor, 16th International Conference on Computer Safety, Reliability and Security: SAFECOMP'97, 1997, pages 123-137.

[20] Miller SP, Neuman C, Schiller JI, Saltier JH. Kerberos authentication and authorization system. Project Athena Technical Plan Section E.2.1, MIT, 1987.

[21] CCITT.CCITT draft recommendation X.509. The Directory-Authentication Framework, Version 7, 1987.

[22] Clark J, Jacob J. A survey of authentication protocol literature: Version 1.0. http://www-users.cs.york.ac.uk/-jac/ under the link Security Protocols Review. 1997.

[23] ISO/EEC. Information technology and security techniques. entity authentication mechanisms part 2: Entity authentication using symmetric techniques, 1993.

[24] Satyanarayanan M. Integrating security in a large distributed system. Technical Report, CMU-CS, CMU, 1987, p87-179.

[25] ISO/IEC. Information technology and security techniques. entity authentication mechanisms part 4: Entity authentication using cryptographic check functions. 1993.

[26] R.Needham and M. Schroeder. Using encryption for authentication in largenetworks

of computers. Communications of the ACM, 1978, 12(12):993-999.

[27] Otway D, Rees O. Efficient and timely mutual authentication. Operating Systems Review, 1987, 21(1): 8-10.

[28] 李先贤, 怀进鹏. "分布式网络环境下密码协议形式模型和安全性" .中国科学院研究生院学报, 2002, Vol. 19, No.3 : 311-323.

[29] Denning D, Sacco G. Timestamps in key distribution protocols. Communications of the ACM, 1981, 24(8): p533-536.

[30] Woo T, Lam S. A lesson on authentication protocol design. Operating Systems Review, 1994, 28(3): p24-37.

[31] Neuman BC, Stubblebine SG. A note on the use of timestamps as nonces. Operating Systems Review, 1993, 27(2): p10-14.

[32] Kao IL, Chow R. An efficient and secure authentication protocol using uncertified keys. Operating Systems Review, 1995, 29(3): p14-21.

[33] ISO/IEC. Information technology and security techniques.entity authentication mechanisms part 3: Entity authentication using a public key algorithm. 1995.

[34] Diffie W, Hellman ME. New directions in cryptography. IEEE Transactions on Information Theory, 1976, IT-22(6): p644-654.

[35] Makoto Tatebayashi and Natsume Matsuzaki and Newman Jr. Key Distribution Protocol for Digital Mobile Communication Systems. Advances in Cryptology: Proceedings of Crypto-'89, 1990, LNCS 435.

[36] Nesset D. A Critique of the BAN Logic. ACM Operating Systems Review, 1990, 24(2): 35-38.

[37] Gong L. Optimal Authentication Protocols Resistant to Password Guessing Attacks. In: Proceedings of the 1995 IEEE Computer Security Foundations Workshop VIII. IEEE Computer Society Press, 1995, p24-29.

[38] Tardo J. and Alagappan K. SPX: Global Authentication Using Public Key Certificates. In: Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press, 1991, p23-24.

[39] Bellovin S. and Merritt M. Encrypted Key Exchange: Password-Based ProtocolsSecure against Dictionary Attacks. In: Proceedings of the 1992 IEEE Symposium on Securitv and Privacv. TFEE Comnuter Societv Press_ n72-R4_ 1992

[40] Gong L, Lomas M, Needham R, Saltzer J. Protecting Poorly Chosen Secrets from

Guessing Attacks. IEEE Journal on Selected Areas in Communications, 1993, Vol. 11, No.5, p648-656.

[41] Shamir A, Rivest R, Adleman L, Mental Poker. MIT Laboratory for Computer Science, 1978, Report TM-125: 178-184.

[42] Carlsen U. Cryptographic Protocol Flaws. In: Proceedings of the 1994 IEEE Computer Security Foundations Workshop VII. IEEE Computer Society Press, 1994, p192-200.

[43] C.Meadows. Appying Formal Methods to the Analysis of a Key Management Protocol. Journal of Computer Securtiy, 1992, 1:5-53.

[44] D. Longley and S. Rigby. An Automatic Search for Security Flaws in Key Management Schemes. Computers and Security, 1992, 11(l):75-90.

[45] L.C.Paulson. Proving properties of security protocols by induction. Proceedings of the IEEE Computer Security Foundations Workshop XJEEE Computer Society Press, 1997, 70-83.

[46] G.Lowe. An attack on the Needham-Schroeder public key authentication protocol. Information Processing Letters, November 1995, 56(3):131-136.

[47] P.F.Syverson, P.C.van Oorschot. On Unified Some Cryptographic Protocol Logics. In: Proceeding of the 1994. IEEE Computer Society Press, 1994.

[48] M.Abadi, M.R.Tuttle. A Semantic for a Logic of Authentication. In: Proceeding of the Tenth ACM Symposium on Principles of Distributed Computing, ACM Press, 1991, 201-216.

[49] R.Kailar. Accountability in Electronic Commerce Protocols. IEEE Trans on Software Engineering, 1996, 22(5):313-328.

[50] D.Kindred. Theory Generation for Security Protocols: [Ph. D Thesis]. Computer Science Department, Carnegie Mellon University, 1999.

[51] Schneider S. Verifying authentication protocols with CSP. Proceedings of the IEEE Computer Security Foundations Workshop X, IEEE Computer Society Press, 1997, 3-17.

[52] C. Meadows. A Model of Computation for the NRL Protocol Analyzer. In: Proceeding of the 7th Computer Security Foundations Workshop. IEEE Computer Society Press, 1994.

[53] Thomas Y. C. Woo, Simon S. Lam. Authentication for Distributed Systems. IEEE Computer, 1992, 25(1): 39-52.

[54] Gavin Lowe, Bill Roscoe. Using CSP to Detect Errors in the TMN Protocol. In: IEEE Transactions on Software Engineering- volume 23_ number 10_ 1997.

[55] Gavin Lowe. Towards a completeness result for model checking of security protocols. Technical Report 1998/6, Dept. of Mathematics and Computer Science, University of Leicester, 1998.

[56] 张少武, 郭建. 一个传输模型的认证协议设计. 计算机应用研究,2004, 05:155-156.

[57] Medvinsky G, Neuman B C. Netcash: A Design of Practical Electronic Currency on the Internet In: Denny D, Pyle R.eds. Proceeding of ACM Conference on Computer and Communication Security. Fairfax, Virginia, ACM Press, 1993: 76-83.

[58] 谢晓尧, 张焕国. 基于有穷自动机模型的电子商务协议的公平性分析.密码学进展, 2004, 331-333.

[59] 范红, 冯登国.《安全协议理论与方法》. 科学出版社, 北京, 2003.

[60] William Stallings.《密码编码学与网络安全：原理与实践（第二版）》.杨明, 胥光辉, 齐望东等译, 电子工业出版社, 2001.

[61] Steve Burnett, Stephen Pains.《密码工程实践指南》. 冯登国等译, 清华大学出版社, 2001.

[62] Bruce Sehneier.《应用密码学—协议、算法和 C 源程序》. 机械工业出版社, 2000.

[63] Andrew S.Tanenbaum.《计算机网络（第三版）》. 熊桂喜, 王小虎译, 清华大学出版社, 1998.

[64] 冯登国, 裴定一.《密码学导引》. 科学出版社, 1999.

攻读硕士学位期间发表的论文

[1] 程娜，何大可.代理多重数字签名方案的改进.信息安全与通信保密，2005.7，P128-129.

[2] 程娜，赖欣，何大可.一种认证协议的 Strand Space 模型及攻击方法.信息、电子与控制技术学术会议论文集（IECT'2005），2005，P226-228.

[3] 程娜，何大可.一种传输模型的认证协议的攻击方法. 计算机应用研究，已录用.

基于Strand Space模型的安全协议形式化分析研究

作者：程娜
学位授予单位：西南交通大学

参考文献(65条)

1. 参考文献

2. D Dolev. A Yao On the security of public key protocols[Technical Report,No.STAN-CS-81-854,Dept of Computer Science,Stanford University] 1981

3. M Burrows. M Abadi. R Needham A logic of authentication 1990(01)

4. G Lowe Breaking and fixing the Needham-Schroeder public-key protocol using FDR 1996

5. J C Mitchell. M Mitchell. U Stern Automated analysis of cryptographic protocols usingmurcp 1997

6. J Millen The Interrogator model 1995

7. R Needham. M Schroeder Using encryption for authentication in large network of computers 1978(12)

8. F Javier Thayer Fabrega. Jonathan C Herzog. Joshua D Guttman StrandSpaces:Why is a security protocol correct? IEEE Computer Press 1998

9. 冯登国. 范红 安全协议形式化分析理论与方法研究综述[期刊论文]-中国科学院研究生院学报 2003(4)

10. Javier Thayer Fabrega. Jonathan C Herzog. Joshua D Guttman Honest Idealson Strand Spaces 1998

11. Thayer FJ. Herzog JC. Guttman JD Strand spaces:Proving security protocols correct 1999(2-3)

12. I Cervesato. N Durgin. M Kanovich. A. Scedrov Interpreting Strands in Linear Logic 2000

13. Paul Syverson Towards a Strand Semantics for Authentication Logic 1999

14. D X Song Athena:a new efficient automated checker for security protocol analysis 1999

15. R L Rivest. A Shamir. L Adleman A method for obtaining digital signatures and public-key cryptosystems 1978(02)

16. M Mambo. K Usuda. E Okamoto Proxy signatures:Delegation of the power to sign message 1996(09)

17. Yi L J. Bai G Q. Xiao G Z Proxy multi-signature scheme:A new type of proxy signature scheme 2000(06)

18. 祁明. L. Harn 基于离散对数的若干新型代理签名方案[期刊论文]-电子学报 2000(11)

19. Wang X. Fu F Cryptanalysis of a proxy multisignature scheme 2002(04)

20. Stefanos Gritzalis. Diomidis Spinellis Cryptographic protocols over opendistributed systems:A taxonomy of flaws and related protocol analysis tools 1997

21. Miller SP. Neuman C. Schiller JI. Saltier JH Kerberos authentication and authorization system. Project Athena Technical Plan Section E.2.1 1987

22. CCITT CCITT draft recommendation X.509. The Directory-Authentication Framework 1987

23. Clark J. Jacob J A survey of authentication protocol literature:Version 1.0 1997

24. ISO. EEC Information technology and security tec hniques. entity authentication mechanisms part 2:Entity authentication using symmetric techniques 1993

25. Satyanarayanan M Integrating security in a large distributed system[Technical Report,CMU-CS,CMU] 1987

26. ISO. IEC Information technology and security techniques. entity authentication mechanisms part

4:Entity authentication using cryptographic check functions 1993

27. R Needham. M Schroeder Using encryption for authentication in largenetworks of computers 1978(12)

28. Otway D. Rees O Efficient and timely mutual authentication 1987(01)

29. 李先贤. 怀进鹏 分布式网络环境下密码协议形式模型和安全性[期刊论文]-中国科学院研究生院学报 2002(3)

30. Denning D. Sacco G Timestamps in key distribution protocols 1981(08)

31. Woo T. Lam S A lesson on authentication protocol design 1994(03)

32. Neuman BC. Stubblebine SG A note on the use oftimestamps as nonces 1993(02)

33. Kao IL. Chow R An efficient and secure authentication protocol using uncertified keys 1995(03)

34. ISO. IEC Information technology and security techniques.entity authentication mechanisms part 3:Entity authentication using a public key algorithm 1995

35. Diffie W. Hellman ME New directions in cryptography 1976(06)

36. Makoto Tatebayashi. Natsume Matsuzaki. Newman Jr Key Distribution Protocol for Digital Mobile Communication Systems 1990

37. Nesset D A Critique of the BAN Logic 1990(02)

38. Gong L Optimal Authentication Protocols Resistant to Password Guessing Attacks 1995

39. Tardo J. Alagappan K SPX:Global Authentication Using Public Key Certificates 1991

40. Bellovin S. Merritt M Encrypted Key Exchange:Password-Based ProtocolsSecure against Dictionary Attacks 1992

41. Gong L. Lomas M. Needham R. Saltzer J Protecting Poorly Chosen Secrets from Guessing Attacks 1993(05)

42. Shamir A. Rivest R. Adleman L. Mental Poker MIT Laboratory for Computer Science[Report TM-125] 1978

43. Carlsen U Cryptographic Protocol Flaws 1994

44. C Meadows Appying Formal Methods to the Analysis of a Key Management Protocol 1992

45. D Longley. S Rigby An Automatic Search for Security Flaws in Key Management Schemes 1992(01)

46. L C Paulson Proving properties of security protocols by induction 1997

47. G Lowe An attack on the Needham-Schroeder public key authentication protocol 1995(03)

48. P F Syverson. P C van Oorschot On Unified Some Cryptographic Protocol Logics 1994

49. M Abadi. M R Tuttle A Semantic for a Logic of Authentication 1991

50. R Kailar Accountability in Electronic Commerce Protocols 1996(05)

51. D Kindred Theory Generation for Security Protocols 1999

52. Schneider S Verifying authentication protocols with CSP 1997

53. C Meadows A Model of Computation for the NRL Protocol Analyzer 1994

54. Thomas Y C Woo. Simon S Lam Authentication for Distributed Systems 1992(01)

55. Gavin Lowe. Bill Roscoe Using CSP to Detect Errors in the TMN Protocol 1997(10)

56. Gavin Lowe Towards a completeness result for model checking of security protocols[Technical Report 1998/6,Dept.of Mathematics and Computer Science,University of Leicester] 1998

57. 张少武. 郭建胜 一个传输模型的认证协议设计[期刊论文]-计算机应用研究 2004(5)

58. Medvinsky G. Neuman B C Netcash:A Design of Practical Electronic Currency on the Internet 1993

59. 谢晓尧. 张焕国 基于有穷自动机模型的电子商务协议的公平性分析 2004

60. 范红. 冯登国 安全协议理论与方法 2003

61. William Stallings. 杨明. 胥光辉. 齐望东 密码编码学与网络安全:原理与实践 2001

62. Steve Bumett. Stephen Pains. 冯登国 密码工程实践指南 2001

63. Bruce Sehneier 应用密码学-协议、算法和C源程序 2000

64. Andrew S Tanenbaum. 熊桂喜. 王小虎 计算机网络 1998

65. 冯登国. 裴定一 密码学导引 1999