一种基于格理论的数字签名方案*)

张文芳[1,2,3] 余位驰[1,2,3] 何大可[2,3] 王小敏[3]
(现代通信国家重点实验室 成都 610041)[1]
(西南交通大学信息安全与国家计算网格省重点实验室 成都 610031)[2]
(西南交通大学计算机与通信工程学院 成都 610031)[3]

摘 要 本文介绍了一种建立在解决NTRU格(NTRU Lattice)中近似最近向量问题(Appr-CVP)基础上的数字签名方案。与现有的基于解决Appr-CVP问题的数字签名方案相比,这种新的数字签名方案通过构造完整的短格基进行签名,在签名与近似最近向量问题之间建立了直接而清晰的关系,因此不需引入任何附加结构,具有更高的安全性。同时,该签名方案引入了适当的扰动,有效地限制了攻击者通过分析大量签名副本所获取的有用信息,具有副本分析免疫性。实验结果表明:该方案不仅安全可靠,而且易于实现。

关键词 格,数论研究组,数字签名,近似最近向量问题,短格基

A Digital Signature Algorithm Based on Lattice Theory

ZHANG Wen-Fang[1,2,3] YU Wei-Chi[1,2,3] HE Da-Ke[2,3] WANG Xiao-Min[3]
(National Laboratory for Modern Communications, Chengdu 610041)[1]
(Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031)[2]
(School of Computer and Communications Engineering, Southwest Jiaotong University, Chengdu 610031)[3]

Abstract A digital signature algorithm based on solving the approximate closest vector problem(Appr-CVP) in NTRU-type lattice is proposed in this paper. Superior to the general Appr-CVP based signature schemes which aid some additional structure to make an incomplete linking with Appr-CVP, this new scheme builds a direct and straightforward linkage between signatures and the Appr-CVP in the underlying NTRU lattice through construction of a full short lattice basis, and so is much more safer. At the same time, by introducing carefully chosen perturbations, this new signature scheme can effectively limit the information that is obtainable from an analysis of a large signature transcript so as to be immune to transcript attacks. Research results show that this new digital signature scheme not only has better security properties, but also can be easily implemented.

Keywords Lattice, Number theory research Unit(NTRU), Digital signature, Approximate closest vector problem(Appr-CVP), Short lattice basis

1 引言

近几年来,格(Lattice)在密码学领域的应用和研究成为一个热点。随着对格上难题(最短向量问题SVP、最近向量问题CVP等)认识的不断深入,格理论在密码分析及加解密体制设计中都得到了广泛的应用[1~3]。然而,如何设计出建立在格理论基础之上的安全而高效的数字签名体制却是一个较为困难的课题。已有的基于解决广义格中Appr-CVP问题的数字签名方案有:由Goldreich、Goldwasser和Halevi提出的GGH签名方案等[4],但是这些方案普遍存在着无法抵抗副本分析攻击的缺陷[5]。此外,最近还有人提出某些基于解决NTRU格中Appr-CVP问题的数字签名方案(如NSS),但是也都相继被攻破了[6],原因是它们的设计者在不具备NTRU格的完整的短格基的情况下,不得不使用附加的结构来完成签名的构造,而正是这些附加的结构导致了签名与其理论基础Appr-CVP之间的不完整的和模糊的关系,造成签名有缺陷和漏洞,从而导致伪造签名和恢复私钥成为可能。

针对这些问题,本文介绍了一种基于解决NTRU格中近似最近向量难题(Appr-CVP)的数字签名方案。新方案首先通过NTRU格中已知的私有短向量找到格中的另一组短向量,从而构造出一个完整的短格基,然后再通过这个完整的短格基找到待签消息的数字签名。在本方案中没有也不需引入任何附加结构,它在签名与近似最近向量问题(Appr-CVP)之间建立了一个直接的、清晰的关系。此外,本签名方案还引入了扰动结构,以增强对副本分析攻击的免疫性,因此具有更高的安全性和抗攻击能力。

本文结构安排如下:首先介绍相关的数学概念和定理;接着介绍本数字签名方案的算法实现以及相关的安全性和时效性分析;最后引出文章的结论和需要进一步探讨的问题。

2 相关的数学概念和原理

2.1 格的定义

格是一种建立在偏序集合上的代数结构[3]。由于研究对象的不同,可以采用不同的形式对它进行定义。在信息领域中,我们通常以如下的方式定义格:

定义1 R^m 上的格 L 是 n 个线性无关向量 $b_1,\cdots,b_n(b_i$

*)基金项目:现代通信国家重点实验室基金资助项目(No:51436010202QT2201)。**张文芳** 博士研究生,主要研究方向:秘密共享及门限密码研究、基于格的密码体制及相关算法研究等;**余位驰** 博士研究生,主要研究方向:基于格的密码体制及相关算法研究等;**何大可** 教授、博士生导师,主要研究方向:网络信息安全与保密,密码设计与密码分析等;**王小敏** 博士研究生,主要研究方向:混沌密码学,嵌入式系统及网络信息安全等。

$\in R^m$, $1\leqslant i\leqslant n, i\in N$)的所有整数线性组合：

$$L=\{\sum_{i=1}^{n}n_ib_i \mid n_i\in Z\}。$$

其中，$b_1,\cdots,b_n$ 称为格 L 的一个基，并且格 L 是 n 维的，记为 $\dim(L)=n$。一般来说，$n\leqslant m$。如果 $n=m$，那么则称格 L 是满维的。在本文中，如果不做特殊说明，我们研究的格都是满维的，并且格是限制在整数集合 Z 上的。显然，如果将格 L 的基 $b_1,\cdots,b_n$ 写成 n 维矩阵形式，有：

$$B=(b_1,\cdots,b_n)=\begin{bmatrix} b_0 & b_2 & \cdots & b_{n-1} \\ b_{n-1} & b_0 & \cdots & b_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \cdots & b_0 \end{bmatrix}$$

则称矩阵 B 为格 L 的生成矩阵，格 L 也可以记为 $L(B)$。格 L 的生成矩阵不是唯一的。

2.2 NTRU 格

定义 2 在 NTRU 体制中，与多项式 $h(X)=h_0+h_1X+h_2X^2+\cdots+h_{N-1}X^{N-1}\in R$ 相关的 NTRU 格 L_h 是满足下列卷积取模关系：$v(X)=h(X)*u(X)(\mathrm{mod}\ q)$ 的向量 $(u,v)\in R\times R\cong Z^{2N}$ 的集合。

其中，R 表示多项式环 $R=Z[X]/(X^N-1)$，$*$ 表示环上的卷积。多项式 $h(X)$ 和 $u(X)$ 的卷积取模运算定义为：$v(X)=h(X)*u(X)(\mathrm{mod}\ q)=v_0+v_1X+v_2X^2+\cdots+v_{N-1}X^{N-1}$，$v_k=\sum_{i+j=k(\mathrm{mod}\ N)}h_i\cdot u_j(\mathrm{mod}\ q)$。因此，NTRU 格也称为卷积模格。NTRU 格 L_h 可以通过下面 $2N$ 维的生成矩阵得到：

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \vdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \vdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \vdots & 0 & 0 & 0 & \cdots & q \end{bmatrix}$$

2.3 向量的范数和向量的距离

在对格中的向量进行讨论时，向量的范数(norm)是一个重要的概念。根据线性代数相关的知识，n 维向量 v 的 p-范数(l_p-norm)定义为：

$$\|v\|_p=(\sum_{i=1}^{n}|v_i|^p)^{1/p},\ p\geqslant 1$$

当 $p=2$ 时，向量 v 的 2-范数 $\|v\|_2$ 也被称为欧几里德范数(简写为 $\|v\|$)。本文中用到的 v 的 2-范数为中心化的欧几里德范数：$\|v\|=(\sum_{i=0}^{n-1}|v_i|^2-(1/n)(\sum_{i=0}^{n-1}|v_i|)^2)^{1/2}$。$n$ 维向量的欧几里德范数也就是该向量在 n 维线性空间中的长度。

本文中，两个 n 维向量 v、w 间的距离指的是它们之间的欧几里德距离，定义为：

$$dist(v,w)=(\sum_{i=1}^{n}(v_i-w_i)^2)^{1/2}$$

2.4 格上的难题——近似最近向量问题(Appr-CVP)

最近向量问题(Closest Vector Problem, CVP)，即找出格中与某个给定向量(不一定包含在格中)距离最短的向量。对于任意一个点 p，格 L 中与之距离最接近的向量称为最近向量，其距离记为 $\lambda_1(p,L)$。同理，将次近向量的距离记为 $\lambda_2(p,L)$，依此类推。

$$\lambda_1(p,L)=\min\{\|v-p\|:v\in L, v\neq 0\}$$

可以证明：在 p-范数($p\geqslant 1$)的形式下，CVP 是 NP 难题[2]。

近似最近向量问题(Appr-CVP)：到目前为止，尚没有多项式时间算法可以解决普通格上的 CVP 难题。但是，在难题做了少许的弱化之后，许多意义重大的结论已经得到证明。这种弱化就是近似化处理，相应的算法称为近似算法。CVP 的近似算法指的是：一个算法对于输入的一个格 L 和任意的一个目标向量 p 能够找到格 L 中距离 p 不超过 $c\lambda_1(p,L)$ 的非零格向量 $v(v\in L)$，(其中 c 是近似因子，是输入格的某个量的函数，例如是格 L 维数的函数)，那么称该算法能以因子 c 近似解决 CVP。已经证明：具有小因子 c 的近似最近向量问题(Appr-CVP)是 NP 难题[7,8]。

本文提出的数字签名方案正是建立在解决 NTRU 格中的小因子 Appr-CVP 基础上的。

3 一种基于 NTRU 格的数字签名方案

3.1 签名方案设计原理

签名者通过在特定的 NTRU 格中其私有的短向量构造一个完整的短格基，进而利用该短格基找到位于同一 NTRU 格中的并且距离消息摘要点(message digest point，由待签名消息通过特定哈希函数产生且不一定在格中)足够近的点，并将该格中的点作为消息的数字签名。数字签名点与消息摘要点之间的距离应该足够短(小于某个限度，并接近最短)，从而使得试图伪造签名成为不可能——基于 NTRU 格中小因子 Appr-CVP 难题。同时，从下面的算法描述中还可以看出本签名方案与 Appr-CVP 之间具有直接而清晰的关系，不需借助任何额外的附加结构，因此具有更高的可证明安全性。

3.2 算法描述

本文提出的数字签名方案由密钥生成、签名和验证 3 部分组成，其具体算法描述如下。

3.2.1 密钥生成

① 输入各参数取值：整型参数 $N,q,d_f,d_g,B>=0$，字符串型参数 t(t="standard"或者"transpose")；其中，N 表示签名方案中使用的多项式的次数，q 表示取模运算的模子，d_f、d_g 分别为签名中用到的两个秘密短向量 f 和 g 中系数为 1 的个数，B 为用于扰动的秘密格向量的个数；

② 产生 B 个用于扰动的秘密格向量 $\{f_i,f'_i,h_i\}(i=1..B)$，以及用于签名的私钥 $\{f_0,f'_0\}$ 和用于验证的公钥 h_0：置 $i=B$，当 $i\geqslant 0$ 时，

(a)随机选择格中的两个短向量 $f,g\in R$(保密)，使 f 和 g 中分别有 d_f 和 d_g 个系数=1，其余系数=0；

(b)求得格中另外两个短向量 $F,G\in R$(保密)，满足

$$f*G-F*g=q \tag{1}$$

F,G 的生成方法如下所示：

因为 $R_f\equiv\prod_{i=1}^{N-1}f(x^i)\bmod\Phi\in z$(其中 $\Phi(X)=\Sigma_{i=0}^{N-1}X^i\in R$)，定义 $\rho_f\equiv\prod_{i=2}^{N-1}f(x^i)\bmod\Phi$，同理定义 ρ_g。

则 $\rho_f f+k_f(X^N-1)=R_f$，且 $\rho_g g+k_g(X^N-1)=R_g$。

假设 R_f 和 R_g 互质，则一定存在 $\alpha,\beta\in Z$，使得 $\alpha R_f+\beta R_g=1$，因此有 $(\alpha\rho_f)f+(\beta\rho_g)g=1+k(X^N-1)$。所以，如果设 $F=-q\beta\rho_g$ 且 $G=q\alpha\rho_f$，则满足 $f*G-F*g=q$。

定理 1 如果 $f,g,F,G\in R$ 满足等式(1)，定义 $h=f^{-1}*g(\mathrm{mod}\ q)$，且定义 L_h 为由 $\{(1,h),(0,q)\}$ 生成的 NTRU 格，则：

Ⅰ. $\{(f,g),(F,G)\}$ 是 L_h 的一组生成基；

Ⅱ. 如果 $F',G'\in R$ 也满足 $f*G'-F'*g=q$，则一定存在 $c\in R$，使得 $F'=F+c*f$ 且 $G'=G+c*g$。

证明：略。

接下来，我们需要将 F,G 约减成短向量：

设 $l=F*f^{-1}\in Q[X]/(X^N-1)$，$k=\lfloor l\rfloor\in R$，其中，$f^{-1}=(1/R_f)\rho_f\in Q[X]/(X^N-1)$，$\lfloor x\rfloor$ 表示离 x 最近的整数。

则由以下等式(2)和等式(3)所确定的 F,G 即为所需短向量。

$$F=F-k*f \tag{2}$$

$$G=G-k*f \tag{3}$$

这样,$\{(f,g),(F,G)\}$就构成了我们需要的用于在签名和 NTRU 格中 Appr-CVP 之间建立直接联系的完整的短格基。

(c)如果 $t=$"standard",置 $f_i=f$, $f'_i=F$;如果 $t=$"transpose",置 $f_i=f$, $f'_i=g$;

(d)计算

$$h_i=f_i^{-1}*f'_i(\mathrm{mod}\ q) \tag{4}$$

并置 $i=i-1$;

③公开输出:各输入参数的取值,以及用于验证签名的公钥 $h(h=h_0\equiv f_0^{-1}*f'_0(\mathrm{mod}\ q))$;

④秘密输出:各公开输出的量值,以及用于签名的私钥$\{f_0,f'_0\}$和用于扰动的秘密的$\{f_i,f'_i,h_i\}(i=1..B)$。

3.2.2 签名

①输入:待签名的数字消息 D,用于签名的私钥$\{f_0,f'_0\}$,以及用于扰动的秘密的$\{f_i,f'_i,h_i\}(i=1..B)$;

②置 $r=0,s=0,i=B$,计算 $m_0=H(D\|r)$,置 $m=m_0$;其中 m 为对数字消息 D 进行哈希后得到的消息摘要。

③使用秘密的格向量$\{f_i,f'_i,h_i\}(i=1..B)$对消息摘要点 m 进行扰动:当 $i\geqslant 1$ 时,

(a)计算 $x=\lfloor -(1/q)m*f'_i\rfloor$, $y=\lfloor (1/q)m*f_i\rfloor$,置 $s_i=x*f_i+y*f'_i$;

(b)置 $m=s_i*(h_i-h_{i-1})\mathrm{mod}\ q$;

(c)置 $s=s+s_i$, $i=i-1$;

④对扰动后的消息摘要点 m 进行签名:

计算 $x=\lfloor -(1/q)m*f'_0\rfloor$, $y=\lfloor (1/q)m*f_0\rfloor$,置 $s_0=x*f_0+y*f'_0$, $s=s+s_0$;

⑤对签名进行检查:

(a)计算

$$b=\|(s,s*h-m_0\ \mathrm{mod}\ q)\| \tag{5}$$

(b)如果 $b\geqslant NB$,置 $r=r+1$ 并 go to step 3;

⑥输出:签名消息三元组(D,r,s);

3.2.3 验证

①输入:签名消息三元组(D,r,s),以及用于验证签名的公钥 h;

②计算 $m=H(D\|r)$;

③计算

$$b=\|(s,s*h-m\ \mathrm{mod}\ q)\| \tag{6}$$

④输出:如果 $b<NB$,签名为真,否则签名为假;

4 安全性及时效性分析

同已有的基于 NTRU 格中 Appr-CVP 难题的数字签名方案 NSS 相比,本签名方案具有更高的安全性和抗攻击能力。这是因为:NSS 签名方案在不具有完整短格基的前提下,不得不通过额外引入一个小素数求模运算的附加结构来构造签名与 Appr-CVP 之间的联系,但正是这种模糊的结构暴露出它的安全缺陷。Gentry、Jonsson 和 Stern 发现利用 NSS 中的附加结构可以在不知道私钥的情况下伪造签名[6];同时,Szydlo 也发现在获得大量签名副本的条件下,利用该附加结构能够恢复出 NSS 的签名私钥[6]。与之不同的是,本签名方案首先通过格中私有短向量构造出完整的短格基,然后利用这个完整的短格基直接构造出距离消息摘要点足够近的格中的点作为签名,它在签名与 Appr-CVP 之间建立了一个直接而清晰的联系,不需引入任何附加结构。实践证明,本签名方案能够抵抗上述两种攻击。

同基于解决广义格中 Appr-CVP 的 GGH 签名方案无法抵抗副本分析攻击相比,本签名方案也通过引入扰动结构很好地解决了这个问题,具有副本分析免疫性。此外,同传统的数字签名方案 RSA、ECDSA 等相比,本签名方案还具有快速和易于实现的优点。

由于格基归约算法在解决 SVP、CVP 等格中难题时较为有效,下面着重对本签名方案抵抗格基归约攻击和副本分析攻击的能力进行分析。

4.1 抵抗格基归约攻击能力

同一个格可以用不同的基来表示。在解决格上相关问题时,即使使用同一个算法,选择不同的基所需要的运算量差别是十分巨大的。所以,我们希望能够找到适合解决问题那一组基。选择这样一组基的过程就称为格基归约,并且称这样的一组基为格的一组归约基。最著名的格基归约方法是 LLL 算法,它是目前发现的解决广义格中 SVP 和 CVP 问题的最有效的方法。可以证明,采用格基归约的方法解决 NTRU 格中的 SVP 和 CVP 时并不比解决广义格中的 SVP 和 CVP 容易。

采用格基归约技术对本签名算法进行攻击的一种可能方法是:通过格基归约试图找到一组能够代替签名私钥(f_0,f'_0)的 NTRU 格中足够短的向量,并进而用这组向量伪造签名。因为(f_0,f'_0)及其转置很可能是格中的最短向量,因此这种方法是通过解决近似最短向量问题(Appr-SVP)来进行攻击的。实验证明:当选择参数$(N,q,c)=(251,128,0.45)$时,攻破时间大于 10^{12} MIPS 年,这是不现实的。

另一种可能方法是通过解决 Appr-CVP 进行攻击。攻击者通过格基归约试图找到另外一组 NTRU 格中的距离消息摘要点足够近的向量,并用它直接作为对该消息的伪造签名。我们同样可以证明这种方法也是不可行的。高斯猜想指出:空间中的点到格中最近点的平均距离为 $\sqrt{Nq/\pi e}$。因此,一个成功的签名与格中真正的最近点到消息摘要点距离之比应满足:

$$\frac{L_{\mathrm{sign}}}{L_{\min}}\leqslant\frac{NormBound}{\sqrt{Nq/\pi e}}=\frac{O(N^{3/2})}{\sqrt{Nq/\pi e}} \tag{7}$$

而采用本签名方案获得的签名满足关系:$NormBound=O(\sqrt{2N}\sqrt{Nq/\pi e})$,因此本签名方案能够在 $O(\sqrt{\dim L})$的数量级上解决 Appr-CVP,且常系数很小(=2)。然而,在不知道签名私钥的前提下,通过格基归约方法虽然也能够在 $O(\sqrt{\dim L})$的数量级上解决 Appr-CVP,但是其常系数却很大。本签名方案的安全性就是建立在如下数学原理基础上的,即在不知道签名私钥的前提下,随着常系数的减小,用所有已知的方法解决 Appr-CVP 的难度都会呈指数级地增加[7]。例如:当选择参数$(N,q,c)=(251,128,0.45)$,式(7)中的比值为 7.91,即 $NormBound=485$,此时通过格基归约解决 Appr-CVP 来伪造签名的难度甚至高于直接寻找签名私钥(f_0,f'_0)的难度。

4.2 抵抗副本分析攻击能力

实验证明,对于一般的 NTRU 格,10,000 个签名副本会泄漏私钥的 2 阶矩信息;100,000,000 个签名副本会泄漏私钥的 4 阶矩信息。而且,若已知私钥的 4 阶矩信息,就能够在多项式时间内恢复出私钥。但是,当在签名中引入适当的扰动时,就可以增加两个附加的未知基向量,从而加大了副本分析攻击的难度——在恢复私钥之前必须首先设法消去这两个未知基向量。比如:当选择参数$(N,q,d,B)=(251,128,72,1)$(引入一组秘密基进行一次扰动)时,获得 Gram 矩阵的条件是使私钥的 6 阶矩收敛,所需的消息签名副本数至少应为

10^{18}个，从而增加了破译的难度。

4.3 时效性分析

同ECDSA和RSA等传统的数字签名算法相比，本文提出的基于格中难题的签名算法具有更快的运行速度而且易于实现。其性能比较如表1所示，测试实验是在800MHz 128MRam Pentium机上实现的。

从表1可以看到，本签名算法的密钥生成过程虽然较ECDSA费时，但是由于在实际应用中密钥一般都事先生成并储存起来，每次签名时直接取出使用即可，在使用了一定周期之后才需更换密钥，因此密钥生成速度并不是影响签名速度的主要因素。而在签名和验证过程中，本签名方案的实现速度均明显优越于ECDSA和RSA算法。此外，从表1还可以看到，在相同的安全级别下，本签名算法密钥长度远远小于RSA所需的密钥长度，与ECDSA接近，同时由于在本签名方案中只涉及到模乘和模加两种简单运算，因此更易于软、硬件实现。

表1 运行速度比较(800MHz 128MRam Pentium)

	本签名算法(N=251)	ECDSA-163	RSA-1024
密钥生成(μs)	180,000	1424	500,000
签名(μs)	500	1424	9090
验证(μs)	303	2183	781

结论 本文针对已有的某些基于格理论的签名方案中存在的结构不清晰以及无法抵抗副本分析攻击等问题，提出了一个改进的基于解决NTRU格中近似最近向量难题(Appr-CVP)的数字签名方案。该方案在签名与近似最近向量问题之间建立了一个直接而清晰的关系，而且通过引入扰动，有效地增强了抵抗副本分析攻击的能力，具有更高的安全性。同时，与ECDSA和RSA等传统签名算法相比，该基于格中近似最近向量难题的签名算法具有更高的时效性且便于实现。

参考文献

1 Daniele Micciancio. Lattice Based Cryptography: A Global Improvement, 1999

2 Schnorr C P. A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science, 1987, 53: 201～224

3 Jacobson N, Basic Algebra I. Second Edition. Freeman W H and Company, 1985

4 Goldreich O, Goldwasser S, Halevy S. Public-key cryptography from lattice reduction problems. In: Proc. CRYPTO'97, 1997, volume 1294 of LNCS: 112～131

5 Goldreich O, Goldwasser S, Halevi S. Challenges for the GGH-Cryptosystem. Available at: http://theory.lcs.mit.edu/～shaih/challenge.html

6 Gentry C, Jonsson J, Stern J, et al. Cryptanalysis of the NTRU Signature Scheme (NSS). Eurocrypt'01, Lecture Notes in Computer Science, Springer-Verlag, 2001

7 Dinur I, Kindler G, Ssfra S. Approximation CVP to within almost-polynomial factors is NP-hard. 39th Annual Symposium on Foundations of Computer Sicence, Palo Alto, California, 1998

8 Goldreich O, Micciancio D, Safra S, et al. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors: [technical reports]. Electronic Colloquium on Computational Complexity, ECCC, 1999

(上接第88页)

$$term(\langle s,i\rangle)=-\{\psi \text{ SignedWith } K^{-1}\} \quad (4.7)$$

由 P CanProve(K Authenticates Q)可知，在束 B 中存在一个结点$\langle s,j\rangle$，使得

$$\langle B,s,j\rangle \vdash (K \text{ Authenticates } Q) \quad (4.8)$$

由(4.6)、(4.8)可知

$$principal(t)=Q \quad (4.9)$$

由(4.6)、(4.9)可得

$$\langle B,t,k\rangle \vdash Q \text{ Says } \psi \quad (4.10)$$

由(4.3)、(4.10)和公理1可得

$$\langle B,s,i\rangle \vdash P \text{ CanProve}(Q \text{ Says } \psi)$$

因此，(P Receives(φ SignedWith K^{-1}) $\wedge$ (ψ in φ) $\wedge$ (P CanProve(K Authenticates Q))) $\vdash$ P CanProve(Q Says ψ)成立。

定理5(信任规则) (P CanProve(Q Says φ) $\wedge$ P CanProve(Q IsTrustedOn φ)) $\vdash$ P CanProve φ

证明：由 P CanProve(Q Says φ)可知，在束B中存在一个结点$\langle s,i\rangle$，满足

$$principal(s)=P \quad (5.1)$$

$$\langle B,s,i\rangle \vdash Q \text{ Says } \varphi \quad (5.2)$$

由 P CanProve(Q IsTrustedOn φ)可知，在束 B 中存在一个结点$\langle s,j\rangle$，满足

$$principal(s)=P \quad (5.3)$$

$$\langle B,s,j\rangle \vdash Q \text{ IsTrustedOn } \varphi \quad (5.4)$$

当$\langle s,i\rangle \preceq \langle s,j\rangle$，由(5.2)、(5.4)和公理1可得

$$\langle B,s,j\rangle \vdash \varphi \quad (5.5)$$

由(5.3)、(5.5)可得

$\langle B,s,j\rangle \vdash P$ CanProve φ。

当$\langle s,j\rangle \preceq \langle s,i\rangle$或者 $i=j$ 时，证明类似。

因此，(P CanProve(Q Says φ) $\wedge$ P CanProve(Q IsTrustedOn φ)) $\vdash$ P CanProve φ成立。

结束语 Kailar逻辑是用来分析电子商务协议中的主体的可追究性的，但Kailar没有给出该逻辑的形式化语义，但逻辑的语义对于逻辑本身的正确性是至关重要的。串空间模型是用来分析协议的正确性和认证性的，它具有良好的语义。本文把Kailar逻辑和串空间模型结合起来，给出了Kailar逻辑的串空间语义，并用串空间语义证明了Kailar逻辑中的主要规则的正确性。

参考文献

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

2 Van Oorschot P. Extending cryptographic logics of CryptographicLogic of Belief to Key Agreement Protocols [C]. In: Proc. of the First ACM Conference on Computer and Communications Security, 1993. 232～243

3 Syverson P, van Oorshot P C. On Unifying Some Cryptographic Protocol Logics [C]. In: 1994 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE Computer Society, 1994. 14～28

4 Rajashekar K. Accountability in electronic commerce protocols [J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313～328

5 Abadi M, Tuttle M R. A Semantics for a logic of Authentication [C]. In: Proc. of the Tenth ACM Symposium on Principles of Distributed Computing, ACM Press, 1991. 201～216

6 Fábrega F J T, Herzog J C, Guttman J D. Strand spaces: Why is a security protocol correct? In: Proc. of the 1998 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 160～171

7 Fábrega F J T, Herzog J C, Guttman J D. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(2-3): 191～230

8 Fábrega F J T, Herzog J C, Guttman J D. Strand spaces: Honest ideals on strand spaces. In: Proc. of the 1998 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998. 66～77