Kailar 逻辑的串空间语义

缪祥华[1] 何大可[2]
(西南交通大学计算机与通信工程学院 成都 610031)[1]
(西南交通大学信息安全与国家计算网格实验室 成都 610031)[2]

摘 要 Kailar 在 1996 年发表了"电子商务协议中的可追究性"一文,使得电子商务协议的形式化分析得到了重大的发展。但是 Kailar 逻辑的语义一直没有人提出来过,而逻辑的语义对于逻辑的正确性是至关重要的。本文的主要工作就是给出了 Kailar 逻辑的串空间语义,从语义的角度证明了 Kailar 逻辑的规则的正确性。

关键词 逻辑,语义,串空间,电子商务协议

A Strand Space Semantics of Kailar Logic

MIAO Xiang-Hua[1] HE Da-Ke[2]
(School of Computer&Communication Engineering, Southwest Jiaotong University, Chengdu 610031)[1]
(Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031)[2]

Abstract In 1996, Kailar presented a paper, namely"accountability in electronic commerce protocol", which quickly became the most widely used and widely discussed formal method for the analysis of electronic commerce protocol. The semantics of logic is very important about soundness of logic, but no one have given a semantics of Kailar logic. In this paper, a strand space semantics of Kailar logic is presented and the correctness of Kailar logic's rules are proved.

Keywords Logic, Semantics, Strand space, Electronic commerce protocol

1 引言

密码协议的形式化分析已经有二十几年历史了,但要从理论上证明一个协议的正确性和安全性是一件很困难的事情。近年来电子商务协议的出现,给密码协议的形式化分析提出了许多新问题。电子商务协议除了要满足安全性和秘密性,还必须满足原子性和可追究性等。传统的逻辑分析方法,如 BAN 逻辑[1]和 BAN 类逻辑[2,3]等,几乎都是一种信念逻辑,它的主要目的是证明某个主体相信某个公式,而电子商务协议中的可追究性的目的在于某个主体要向第三方证明另一方对某个公式负有责任,所以 BAN 逻辑和 BAN 类逻辑不适合用来分析电子商务协议。

Kailar 针对电子商务协议中的可追究性问题提出了一种新的逻辑,即 Kailar 逻辑[4],但是 Kailar 逻辑中并没有给出逻辑系统的形式化语义。Syverson[3]指出:逻辑语义[5]的一个重要作用就是提供了一个证明逻辑系统自身正确的方法。本文把 Kailar 逻辑和串空间(Strand Space)模型结合起来,给出了 Kailar 逻辑的串空间语义,并从串空间的角度证明了 Kailar 逻辑中的推理规则的正确性。

2 Kailar 逻辑和串空间模型

2.1 Kailar 逻辑

P Receives x SignedWith K^{-1}:P 收到一个用 K^{-1} 签名的消息 x。

P Says x:P 声明公式 x 并对 x 以及 x 能推导出的公式负责。

P IsTrustedOn x: P 被协议其他主体所相信 P 声明的公式 x 是正确的。

x in m:x 是 m 中的一个或几个可被理解的域,它的含义是由协议设计者明确定义的,可被理解的域通常是明文或者主体拥有密钥的加密域。

K_p Authenticates P:K_p 能用于验证 P 的数字签名。

P CanProve x:对于任何主体 B,A 能执行一系列操作,使得通过这些操作以后,A 能使 B 相信公式 x,而不泄漏任何秘密 $y(y\neq x)$给 B。

有关 Kailar 逻辑的详细资料,请参见文[4]。

2.2 串空间模型

串(strand)是协议中的主体可以执行的事件序列。对于诚实的主体,该事件序列是由协议定义好的,由发送消息的事件和接收消息的事件所组成;对于攻击者,该事件序列由攻击者的行为来确定。串空间(strand space)是诚实的主体串和攻击者串所组成的集合。束(bundle)是串空间的一个子集,用来表示一个完整的协议。束是一个有限无环图,每个结点由两部分组成,即〈串名,位置〉,其中串名指出该结点所属的串的名称,位置指出该结点在串中的位置编号。束中有两种边,这两种边表示了结点间的因果依赖关系。第一种边:$\langle s,i\rangle\rightarrow\langle s1,i1\rangle$,表示串 s 中的第 i 个结点发送消息给串 $s1$ 中第 $i1$ 个结点;第二种边:$\langle s,i\rangle\Rightarrow\langle s,i+1\rangle$,表示结点 $\langle s,i\rangle$ 是结点 $\langle s,i+1\rangle$ 的直接前驱。在串空间模型中,协议的正确性问题可以表示为不同串之间的因果连接关系。

有关串空间模型的详细资料,请参见文[6~8]。

3 Kailar 逻辑的语义

3.1 基本语句的语义

缪祥华 讲师、博士生,研究方向为信息系统安全理论;何大可 教授、博士生导师,主研信息安全、密码学和计算机网络安全。

设$\langle B,s,i\rangle$表示束B中的点，也就是束B中串s上的第i个结点，则公式φ在$\langle B,s,i\rangle$为真，表示为$\langle B,s,i\rangle \vdash \varphi$。公式$\varphi$蕴涵公式$\psi$，表示为$\varphi \vdash \psi$。$\varphi \vdash \psi$在$\langle B,s,i\rangle$为真，表示为$\langle B,s,i\rangle \vdash (\varphi \vdash \psi)$。用principal($s$)表示执行串$s$的主体。

3.1.1 P receive x SignedWith K^{-1}

$\langle B,s,i\rangle \vdash P$ receive x SignedWith K^{-1}为真，当且仅当束B中存在一个结点$\langle t,j\rangle$，满足：

(a)principal(t)$\neq P$，principal(s)$=P$；(b)$\langle t,j\rangle \preceq \langle s,i\rangle$；(c)term($\langle t,j\rangle$)$=+\{x$ SignedWith $K^{-1}\}$，term($\langle s,i\rangle$)$=-\{x$ SignedWith $K^{-1}\}$。

3.1.2 P Says x

$\langle B,s,i\rangle \vdash P$ Says x 当且仅当束B中存在一个结点$\langle t,j\rangle$，满足：(a)principal(t)$\neq P$，principal(s)$=P$；(b)$\langle s,i\rangle \preceq \langle t,j\rangle$；(c)term($\langle t,j\rangle$)$=-x$，term($\langle s,i\rangle$)$=+x$。

3.1.3 P IsTrustedOn x

$\langle B,s,i\rangle \vdash P$ IsTrustedOn x 当且仅当对于束B中的任意一个结点$\langle t,j\rangle$，满足：(a) principal(s)$=P$；(b)$\langle s,i\rangle \preceq \langle t,j\rangle$；(c)term($\langle t,j\rangle$)$=-x$，term($\langle s,i\rangle$)$=+x$，$\langle B,s,i\rangle \vdash x$。

3.1.4 x in m

$\langle B,s,i\rangle \vdash x$ in m 当且仅当在束B的结点$\langle s,i\rangle$满足$x \sqsubset m$(也就是x是m的子术语)。

3.1.5 K_P Authenticates P

$\langle B,s,i\rangle \vdash K_P$ Authenticates P 当且仅当在束B的结点$\langle s,i\rangle$满足 term($\langle s,i\rangle$)$=-\{x$ SignedWith $K_p^{-1}\}$。

3.1.6 P CanProve x

$\langle B,s,i\rangle \vdash P$ CanProve x 当且仅当在束B的结点$\langle s,i\rangle$满足：(a)principal(s)$=P$；(b)$\langle B,s,i\rangle \vdash x$。

3.2 公理

公理1 设$\langle B,s,i\rangle$为束B中的一个点，φ为公式，$\langle B,s,i\rangle \vdash \varphi$，对于束B中的任意一个结点$\langle t,j\rangle$，如果$\langle s,i\rangle \preceq \langle t,j\rangle$，那么$\langle B,t,j\rangle \vdash \varphi$。

公理2 设$\langle B,s,i\rangle$为束B中的一个点，φ、ψ为公式，如果$\langle B,s,i\rangle \vdash \varphi$并且$\langle B,s,i\rangle \vdash (\varphi \vdash \psi)$，那么$\langle B,s,i\rangle \vdash \psi$。

公理3 设$\langle B,s,i\rangle$为束B中的一个点，φ、ψ为公式，$\langle B,s,i\rangle \vdash (\varphi \wedge \psi)$充要条件是$\langle B,s,i\rangle \vdash \varphi$并且$\langle B,s,i\rangle \vdash \psi$。

公理4 设$\langle B,s,i\rangle$为束B中的一个点，φ、ψ为公式，$\langle B,s,i\rangle \vdash (\varphi \vee \psi)$充要条件是$\langle B,s,i\rangle \vdash \varphi$或者$\langle B,s,i\rangle \vdash \psi$。

公理5 设$\langle B,s,i\rangle$为束B中的一个点，φ为公式，$\langle B,s,i\rangle \vdash \varphi$和$\langle B,s,i\rangle \vdash (\neg\varphi)$只有一个成立($\neg$表示公式的否定)。

3.3 规则的证明

设P、Q、R为主体变量、φ、ψ、ω为公式变量，K为验证签名的公钥，K^{-1}为签名的私钥，下面证明几个主要的规则。

定理1(推理规则) (P CanProve $\varphi \wedge P$ CanProve($\varphi \vdash \psi$) $\vdash P$ CanProve ψ

证明：由P CanProve φ知，束B中存在一个结点$\langle s,i\rangle$，使得

principal(s)$=P$ (1.1)

$\langle B,s,i\rangle \vdash \varphi$ (1.2)

由P CanProve($\varphi \vdash \psi$)知，束B中存在一个结点$\langle s,j\rangle$使得

principal(s)$=P$ (1.3)

$\langle B,s,j\rangle \vdash (\varphi \vdash \psi)$ (1.4)

如果$\langle s,i\rangle \preceq \langle s,j\rangle$，那么由公理1可得

$\langle B,s,j\rangle \vdash \varphi$ (1.5)

由(1.4)、(1.5)和公理2可得$\langle B,s,j\rangle \vdash \varphi$，也就是$P$ CanProve ψ。如果$\langle s,j\rangle \preceq \langle s,i\rangle$，证明方法和$\langle s,i\rangle \preceq \langle s,j\rangle$的情况类似。如果$i=j$，由公理2和(1.2)、(1.4)可直接得出结论。因此，(P CanProve $\varphi \wedge P$ CanProve($\varphi \vdash \psi$) $\vdash P$ CanProve ψ成立。

定理2(连接规则) P CanProve $\varphi \wedge P$ CanProve $\psi \vdash P$ CanProve($\varphi \wedge \psi$)

证明：由P CanProve φ知，束B中存在一个结点$\langle s,i\rangle$，使得

principal(s)$=P$ (2.1)

$\langle B,s,i\rangle \vdash \varphi$ (2.2)

由P CanProve ψ知，束B中存在一个结点$\langle s,j\rangle$，使得

principal(s)$=P$ (2.3)

$\langle B,s,j\rangle \vdash \psi$ (2.4)

不妨设$\langle s,i\rangle \preceq \langle s,j\rangle$(其它情况类似)，那么由公理1可得

$\langle B,s,j\rangle \vdash \varphi$ (2.5)

由(2.4)、(2.5)和公理3可得

$\langle B,s,j\rangle \vdash (\varphi \wedge \psi)$ (2.6)

由(2.6)、(2.3)可得

$\langle B,s,j\rangle \vdash P$ CanProve($\varphi \wedge \psi$)。

因此，P CanProve $\varphi \wedge P$ CanProve $\psi \vdash P$ CanProve($\varphi \wedge \psi$)成立。

定理3(分离规则) P Says(φ,ψ) $\vdash$ (P Says φ)，P Says(φ,ψ) $\vdash$ (P Says ψ)

证明：这里只证明P Says(φ,ψ) $\vdash$ (P Says φ)，P Says(φ,ψ) $\vdash$ (P Says ψ)的证明方法类似。

由P Says(φ,ψ)知，束B中存在一个结点$\langle s,i\rangle$，使得

$\langle B,s,i\rangle \vdash P$ Says(φ,ψ) (3.1)

由(3.1)知，在束B中存在另外一个结点$\langle t,j\rangle$，满足

principal(t)$\neq P$，principal(s)$=P$ (3.2)

$\langle s,i\rangle \preceq \langle t,j\rangle$ (3.3)

term($\langle t,j\rangle$)$=-\{\varphi,\psi\}$，term($\langle s,i\rangle$)$=+\{\varphi,\psi\}$ (3.4)

由(3.4)知

$\varphi \sqsubset$ term($\langle s,i\rangle$) (3.5)

由(3.1)、(3.5)得

$\langle B,s,i\rangle \vdash P$ Says φ (3.6)

因此，P Says(φ,ψ) $\vdash$ (P Says φ)，P Says(φ,ψ) $\vdash$ (P Says ψ)成立。

定理4(签名规则) (P Receives(φ SignedWith K^{-1}) $\wedge$ (ψ in φ) $\wedge$ (P CanProve(K Authenticates Q))) $\vdash P$ CanProve (Q Says ψ)

证明：由P Receives(φ SignedWith K^{-1})可知在束B中存在一个结点$\langle s,i\rangle$，使得

$\langle B,s,i\rangle \vdash P$ Receives(φ SignedWith K^{-1}) (4.1)

由ψ in φ知

$\psi \sqsubset \varphi$ (4.2)

由(4.1)、(4.2)可得

$\langle B,s,i\rangle \vdash P$ Receives(ψ SignedWith K^{-1}) (4.3)

由(4.3)可知，在束B中存在一个结点$\langle t,k\rangle$，满足

principal(t)$\neq P$，principal(s)$=P$ (4.4)

$\langle t,k\rangle \preceq \langle s,i\rangle$ (4.5)

term($\langle t,k\rangle$)$=+\{\psi$ SignedWith $K^{-1}\}$ (4.6)

(下转第96页)

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