NTRUSign 无线认证和密钥协商协议

张利华[1,2],章丽萍[2],张有光[1],吕善伟[1]
ZHANG Li-hua[1,2],ZHANG Li-ping[2],ZHANG You-guang[1],LV Shan-wei[1]

1.北京航空航天大学 电子信息工程学院,北京 100083
2.华东交通大学 电气与电子学院,南昌 330013
1.School of Electronic and Information Engineering,Beihang University,Beijing 100083,China
2.School of Electrical and Electronic Engineering,East China Jiaotong University,Nanchang 330013,China
E-mail:lh_zhang@ee.buaa.edu.cn

ZHANG Li-hua,ZHANG Li-ping,ZHANG You-guang,et al.NTRUSign based wireless authentication and key agreement protocol.Computer Engineering and Applications,2009,45(7):32-35.

Abstract: NTRU is a low cost and fast public key cryptosystem,which is suit to resource constraint applications.NTRUSign is a novel digital signature scheme,which is base on NTRU.A new wireless authentication and key agreement protocol using NTRUSign is also proposed.The security of the protocol relies on the fact that for most lattices,it is very difficult to find extremely short vectors.The protocol has three phases:user registration phase,server registration phase,authentication and key agreement phase.Furthermore,after analyzing the security and performance of the protocol,the proposed protocol is a better scheme with lower cost and strong security.

Key words: wireless authentication;key agreement;security;NTRUSign

摘 要:NTRU 是一个快速、低开销的公钥体制,适合在资源受限的应用中使用。NTRUSign 是基于 NTRU 的数字签名算法。基于 NTRUSign 算法,给出了一个无线认证和密钥协商协议。该协议的安全性基于有限时间内在大维数格计算最短向量的困难性。协议包括三个阶段:用户注册阶段、服务器注册阶段、认证阶段和密钥协商阶段。通过安全性分析和协议性能分析对比,表明该协议是一个安全性和效率比占优的协议。

关键词:无线认证;密钥协商;安全性;NTRUSign
DOI:10.3778/j.issn.1002-8331.2009.07.010 **文章编号**:1002-8331(2009)07-0032-04 **文献标识码**:A **中图分类号**:TP393.08

随着无线通信技术的迅速发展,2G(如 GSM)在全球得到了广泛部署,以支持多种类型、高质量多媒体业务为主要特征的新一代移动通信技术 3G 逐步在全球得到了应用,一些国家也研究和部署了 Beyond 3G 和 4G 实验网络。与此同时,除了最基本的语音服务外,用户更需要以移动通信网络为平台的方便、快捷的各种移动增值业务,如移动购物、移动银行转账、移动小额支付、机票预定、手机缴费、空中下载等。由于移动通信网络本身的开放性、网络设计总体构想的安全缺乏性、网络协议的安全不完备性、通信信道的共用性、网络用户的复杂性和网络攻击手段的多样性,用户的个人权益和隐私等受到很大的威胁,无线移动通信环境比有线环境存在更多的安全隐患[1]。对于移动用户和网络运营商来说,安全仍然是其中至关重要的问题。用户对移动通信中的安全和其隐私的要求也越来越高,特别是用户在使用交易类业务的时候,存在更多的安全顾虑。因此,如何确保用户在移动环境中的通信安全,保护用户的个人权益和隐私是推动移动通信及以移动通信网络为平台的移动增值业务得以健康发展的关键问题。

无线认证和密钥协商协议是在无线移动环境下实现通信双方的身份认证、协商产生动态的会话密钥,确保无线通信安全和用户的个人权益和隐私的关键。无线认证和密钥协商协议要满足如下安全需求:双向认证、抗否认、机密性、用户匿名性和低资源开销[1]。文献[1]研究并给出了一个基于椭圆曲线密码体制的无线认证和密钥协商协议(ASK-WAP 协议)。该协议以椭圆曲线数字签名算法(ECDSA)和 Diffie-Hellman 密钥交换协议为基础,实现了无线移动环境下通信双方的身份认证并协商产生了动态的会话密钥。文献[2]研究了 ASK-WAP 的安全性,指出其不具备前向安全性、已知密钥安全性,不能有效实现用户和服务器双向认证。文献[3]基于 ECDSA 和 MTI/A0 AK 密钥交换协议[4],给出了 ASK-WAP 协议的改进方案(QYH-WSP 协议)。同时,文献[5]在研究 ASK-WAP 协议的安全性的基础上,指出 ASK-WAP 协议不能抵御中间人攻击、拒绝服务攻击和假冒攻击的安全缺陷, 并基于 ECDSA 给出了改进的无线认证和密钥协商协议(UAP 协议),该协议优化了认证和密钥协商过程,是一个低开销的协议。但是该协议只包含服务器对用

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.90306008)。
作者简介:张利华(1972-),男,博士,副教授;章丽萍(1972-),女,副教授;张有光(1963-),男,博士,教授,博导;吕善伟(1937-),男,教授,博导。
收稿日期:2008-10-07 **修回日期**:2008-12-16

户的身份认证过程,没有真正实现双向认证。

NTRU(Number Theory Research Unit)公钥密码体制是一种很有前途的公钥密码方案,和椭圆曲线密码算法 ECC 相比较,具有数学复杂性简单,容易理解,密钥生成和运行的速度快且容易的优点,更适合应用在资源严格受限的场合如嵌入式设备、RFID 标签等[6]。NTRU 算法依据的困难问题是 Appr-cvp 问题,即在一个特定格中(即 NTRU 格),找到离某一个给定向量距离接近最近的向量是困难的。人们先后研究并给出了基于 NTRU 的数字签名算法 NSS、R-NSS 和 NTRUSign [7-8],NSS 和 R-NSS 算法已经被攻破。文献[9]研究并给出了基于 NSS 的低开销的无线认证和密钥协商协议,由于 NSS 算法的安全性缺陷,该协议存在安全隐患。

1　符号定义

设整数环 Z、整数 $N\geq 2$,用 R 表示多项式截断环时,R 可写成:$R=Z[X]/(X^N-1)$。一个多项式 $f(x)\in R$ 可以用一个向量 $\boldsymbol{F}$ 来表示:$\boldsymbol{F}=\sum_{i=0}^{N-1}f_i x^i=(f_0,\cdots,f_{N-1})$。

NTRUSign 公开参数组 $D=(N,q,d_f,d_g,NormBound)$:$N$ 是维数,是一素数;q 是模数;d_f、d_g是密钥参数;$NormBound$ 是验证时使用的限。NTRUSign 的推荐参数为(251,128,73,71,300),具有与 1 024 bit RSA 算法、160 bit ECC 算法同等的安全性[8]。

Server 为服务器;CA 为可信中心;User 为用户;ID_S 为服务器的身份标识;ID_U 为用户的身份标识;EID_S 为服务器的系统身份标识;EID_U 为用户的系统身份标识;T_* 为用户或服务器证书失效时间;$h(\cdot)$为符合文献[8]附录 D 要求的安全 Hash 函数;S_S 为服务器证书;S_U 为用户证书;N、r_S 为随机数;$E(k,*)$为用 K 密钥对数据进行 AES 加密运算;$D(k,*)$为用密钥 K 对数据进行 AES 解密运算;⇒为安全信道;→为一般信道。

2　NTRUSign 数字签名算法

NTRUSign 算法是 2003 年由 Hoffstein et al 给出的一种新型的基于 NTRU 的数字签名算法,迄今为止,还没有发现对此算法的有效攻击方法[10]。在 NTRUSign 算法中,签名者利用私钥产生明文的接近最近向量,这个向量属于 NTRU 格,而把这一向量作为明文的签名。敌手在不知道私钥的情况下,想通过其它方法在 NTRU 格中找到这一最近向量是很困难的[8]。算法包括密钥生成、签名和验证三个部分,其运算建立在环 $R=Z[X]/(X^N-1)$上。

2.1　密钥生成

(1)输入参数组 $D=(N,q,d_f,d_g,NormBound)$,随机选取 $f,g\in R$,满足 f、g 的系数分别只有 d_f、d_g 个 1,其余为 0,且 $\|f\|,\|g\|=O(\sqrt{N})$;

(2)寻找较小的 $F,G\in R$,满足 $f\otimes G-F\otimes g=q$,其中 $\|F\|\approx\|f\|\sqrt{N/12}$,$\|G\|\approx\|g\|\sqrt{N/12}$,且 $\|F\|,\|G\|=O(\sqrt{N})$;

(3)计算公钥 $h\equiv f^{-1}\otimes g(\mathrm{mod}\ q)$,输出公钥 h,私钥 (f,g,F,G)。

密钥生成的详细过程见文献[8]。

2.2　签名过程

(1)输入参数组 $D=(N,q,d_f,d_g,NormBound)$,私钥 (f,g,F,G),消息 m,计算 $h(m)$,然后对 $h(m)$进行模 q 运算,获得多项式 (m_1,m_2),且 m_1、m_2 在环 $R=Z[X]/(X^N-1)$上;

(2)计算 $G\otimes m_1-F\otimes m_2=A+q\otimes B$,$-g\otimes m_1+f\otimes m_2=a+q\otimes b$;其中 $-q/2\leq A,a\leq q/2$;

(3)计算 $s\equiv f\otimes B+F\otimes b(\mathrm{mod}\ q)$,返回$(s)$。

2.3　验证过程

(1)输入参数组 $D=(N,q,d_f,d_g,NormBound)$,公钥 h,签名(s),消息 m,计算 $h(m)$,然后对 $h(m)$进行模 q 运算,获得多项式(m_1,m_2);

(2)计算 $t=s\otimes h(\mathrm{mod}\ q)$;若 $\|s-m_1\|^2+\|t-m_2\|^2\leq Normbound^2$,则返回接受该签名,否则,返回拒绝该签名。

3　基于 NTRUSign 的无线认证和密钥协议

基于 NTRUSign 的无线认证和密钥协商协议 NWAP 假定系统存在一个可信中心(CA)负责用户和服务器证书的产生和分发,证书包括用户或服务器的公开密钥、唯一身份等,并用自己的私钥对证书进行了签名。协议包括三个阶段:用户注册阶段、服务器注册阶段及双向认证和密钥协商阶段。假定 CA 中心根据 NTRUSign 数字签名算法中的密钥生成算法生成自己的公钥/私钥对,其中公钥 PK_{CA} 为 h_{CA},私钥 SK_{CA} 为$(f_{CA},g_{CA},F_{CA},G_{CA})$;用户生成自己的公钥/私钥对,其中公钥 PK_U 为 h_U,私钥 SK_U 为(f_U,g_U,F_U,G_U);服务器生成自己的公钥/私钥对,其中公钥 PK_S 为 h_S,私钥 SK_S 为(f_S,g_S,F_S,G_S)。

3.1　用户注册阶段

注册时,用户通过安全信道向 CA 提交(ID_U,PK_U);CA 接收到之后,生成随机数 N_1,令 $EID_U=ID_U\oplus N_1$ 作为用户的系统身份标识,计算然后对 $h(PK_U\|EID_U\|T_U)$进行签名,生成 S_U,并将(PK_{CA},EID_U,S_U,T_U)通过安全信道发送给用户;用户接收到之后,首先验证 CA 的签名 S_S 的有效性,然后存储$(PK_{CA},PK_U,EID_U,S_U,T_U)$。如图 1 所示。

User		CA
(1)发送(ID_U,PK_U)	→	接收(ID_U,PK_U) 生成随机数 N_1、T_U,计算 $EID_U=ID_U\oplus N_1$ 计算 $m=h(PK_U\|EID_U\|T_U)$,并进行模 q 运算,获得(m_1,m_2) 计算 $G_{CA}\otimes m_1-F_{CA}\otimes m_2=A+q\otimes B$, $-g_{CA}\otimes m_1+f_{CA}\otimes m_2=a+q\otimes b$ $S_U\equiv f_{CA}\otimes B+F_{CA}\otimes b(\mathrm{mod}\ q)$
(2)接收(PK_{CA},EID_U,S_U,T_U)	←	发送(PK_{CA},EID_U,S_U,T_U)
计算 $m=h(PK_U\|EID_U\|T_U)$,并进行模 q 运算,获得(m_1,m_2) 计算 $t_U=S_U\otimes h_{CA}(\mathrm{mod}\ q)$ 若 $\|S_U-m_1\|^2+\|t_U-m_2\|^2\leq Normbound^2$,签名有效,否则终止注册过程		
(3)存储$(PK_{CA},PK_U,EID_U,S_U,T_U)$		存储(EID_U,T_U)

图 1　用户注册阶段

3.2　服务器注册阶段

注册时,服务器通过安全信道向 CA 提交(ID_S,PK_S);CA 接收到之后,生成随机数 N_2,令 $EID_S=ID_S\oplus N_2$ 作为服务器的

系统身份标识,然后对 $h(PK_S \| EID_S \| T_S)$进行签名,生成 S_S,并将(PK_{CA},EID_S,S_S,T_S)、各用户的(EID_U,S_U,T_U)通过安全信道发送给服务器;服务器接收到之后,首先验证 CA 的签名的有效性,然后存储(PK_{CA},PK_S,EID_S,S_S,T_S)、(EID_U,T_U)。如图 2 所示。

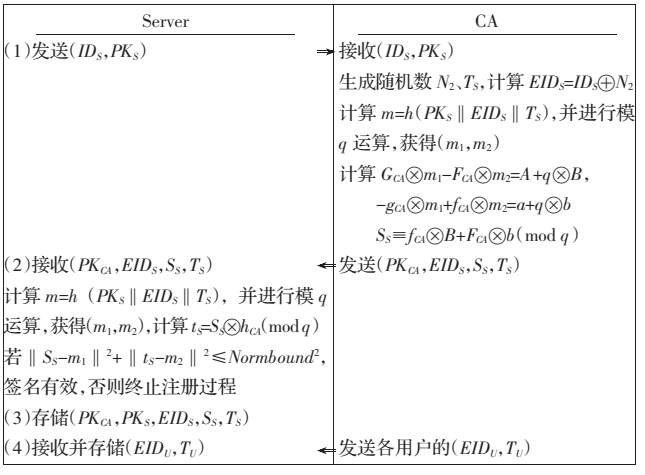

图 2　服务器注册阶段

3.3　双向认证和密钥协商产生阶段

当用户欲和服务器进行通信时,就进入了双向认证和密钥协商阶段。此阶段包括用户对服务器的身份认证、服务器对用户的身份认证、会话密钥生成过程,如图 3 所示。

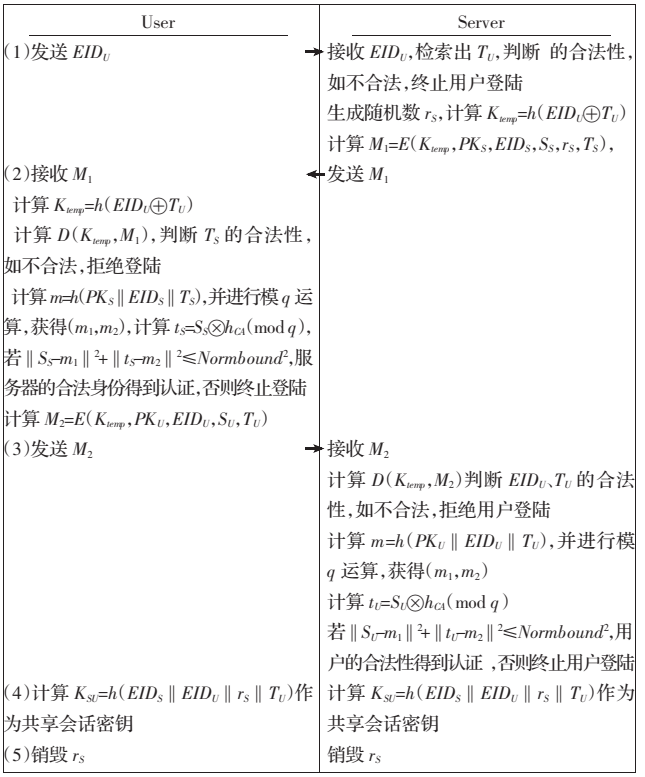

图 3　双向认证和密钥协商阶段

(1)用户对服务器的身份认证

用户向服务器发出通信请求,发送 EID_U;服务器接收到后,根据 EID_U,检索出 T_U,并判断 T_U 的合法性,同时服务器生成一随机数 r_S,并计算临时密钥 $K_{temp}=h(EID_U \oplus T_U)$,计算并将 $M_1=E(K_{temp},PK_S,EID_S,S_S,r_S,T_S)$发送给用户,此时信道是不安全的;用户接收到之后,计算 $D(K_{temp},M_1)$,判断 T_S 的合法性,同时根据 NTRUSign 的数字签名验证算法验证 S_S 的有效性,如果有效,服务器的身份得到认证;然后计算 $M_2=E(K_{temp},PK_U,EID_U,S_U,T_U)$,并发送给服务器。

(2)服务器对用户的身份认证

服务器收到 $M_2=E(K_{temp},PK_U,EID_U,S_U,T_U)$,计算 $D(K_{temp},M_2)$判断 EID_U、T_U 的合法性,同时根据 NTRUSign 的数字签名验证算法验证 S_U 的有效性,如果有效,用户的身份得到认证。

(3)生成会话密钥阶段

完成双向认证后,服务器和用户分别计算 $K_{SU}=h(EID_S \| EID_U \| r_S \| T_U)$作为共享的会话密钥。

4　NWAP 协议的性能分析

NWAP 协议的安全性是基于有效时间内不可能从大维数格中找到最短向量的困难问题,满足了无线认证和密钥协商协议的安全需求,实现了用户和服务器的双向认证。生成的会话密钥是新鲜的并且得到了服务器和用户双方的认可,具备前向安全性和已知密钥安全性、抗否认、机密性和用户匿名性的特性,能够抵御中间人攻击。同时 NWAP 协议基于低开销的 NTRU 公钥算法,可以满足无线移动终端严格资源约束的要求。

4.1　NWAP 协议的安全特性

(1)NWAP 协议实现了用户和服务器的之间的双向身份认证。在使用临时密钥 K_{temp} 解密接收到的数据,并通过 NTRUSign 数字签名算法的验证对服务器的签名 S_S 和对用户的签名 S_U,服务器确认与之通信的用户的身份,用户确认与之通信的服务器的身份,实现了双方的身份认证。

(2)生成的会话密钥是新鲜的并且得到了服务器和用户双方的认可。会话密钥由服务器和用户的系统身份标识、随机数 r_S 和 T_U 通过安全 Hash 运算生成。由于用户的系统身份标识隐藏了用户真正的身份,且是因用户而异的,随机数 r_S 是在一次通信中随机生成的,因此,会话密钥 K_{SU} 是新鲜的。会话密钥 K_{SU} 的生成是建立在服务器和用户双向身份认证的基础上,只有服务器和用户完成双向身份认证才能各自获得相关参数,故生成的会话密钥得到了服务器和用户双方的认可。

(3)前向安全性和已知密钥安全性。在服务器公钥/私钥对和用户公钥/私钥对泄漏的情况下,由于每个用户注册阶段 N_1、服务器注册阶段 N_2 未知,敌手不能计算出合法的签名;又由于 r_S 未知,敌手不能获得以前的会话密钥 K_{SU},因此协议具备前向安全性。同时,即使每个用户的长期密钥 K_{temp} 泄漏或被破解,但是由于 r_S 是在用户登陆服务器的过程中随机产生的,不可能导出每次的会话密钥。故协议是已知密钥安全的。

(4)抗否认。协议基于 NTRUSign 数字签名算法,需要验证对服务器的签名 S_S 和对用户的签名 S_U,因此,具备抗否认的特性。

(5)机密性。在通信过程中,生成临时密钥 K_{temp},密钥 K_{temp} 对不同的用户是不相同的,使用 K_{temp} 对通信过程中传送的数据进行加密;而且会话密钥由服务器和用户的系统身份标识、

随机数 r_S 和生存时间 T_U 进行 Hash 运算生成,Hash 运算的安全单向性,可以确保通信过程中机密性。

(6)用户匿名性和抗中间人攻击。在通信过程中,使用由随机数和用户身份标识运算生成的系统身份标识,具备用户匿名性的特性;而且由于敌手不能获得通信用户的身份,因而可以有效抵御文献[2]中给出的中间人攻击。

4.2 NWAP 协议的效率分析

NWAP 协议在用户端计算负荷、存储空间需求和信息交换次数等方面具有较好的优势。如表 1 所示。

表 1 三个协议效率对比

		QYH-WSP	UAP	NWAP
用户端计算负荷	生成随机数个数	1	1	0
	点乘次数	3	2	0
	对称加密次数	3	1	1
	对称解密次数	1	1	1
	Hash 运算次数	1	1	1
	数字签名验证次数	1(ECDSA)	0	1(NTRUSign)
存储空间		最少	较少(增加了 T_U)	多(增加了 T_U,公私钥对字节数较多)
信息交换次数(发送或接收)		4	3	3

对于同等安全强度的 NTRUSign-251、ECC(2^{163}),在 800 MHzPIII,使用 Win2K 的计算机上,对于 NTRUSign 算法,其签名速度为 2 000 blks/s,验证速度为 3 300 blks/s;对于 ECDSA 算法,签名速度为 616 blks/s,验证速度为 528 blks/s[11]。因此,对用户端而言,NWAP 的计算负荷较小;NWAP 协议只需进行三次信息交换,交换次数和 UAP 协议一样;由于 NTRUSign 的公私钥对字节数较 ECDSA 公私钥对的字节数要多,因此,NWAP 需要增加少量的存储空间,而且传输过程中需要占用相对较多的带宽。但是在密钥生成、签名生成和验证过程中,NTRUSign 内存消耗远低于 ECDSA 算法,且相比较 UAP 协议只实现了单向认证、QYH-WSP 开销大的缺陷而言,NWAP 协议是一个安全性和效率比占优的方案。

5 结束语

TI 公司在其提供的 OMAP 平台的无线安全算法库中集成了 NTRU 算法,却没有包括 ECC 算法,充分说明了 NTRU 算法在无线通信中的应用优势。基于 NTRUSign 的无线认证和密钥协商协议基于有限时间内在大维数格上计算最短向量的困难性,充分利用了 NTRU 优良的计算、存储、带宽开销小,安全性好的特性,满足了无线认证和密钥协商协议的基本特性。虽然文献[10]给出了一种 NTRUSign 算法的延展性攻击方法:一个敌手通过主动窃听,在获得一个消息的合法签名的情况下,能够伪造出此消息的多个合法签名,但是就 NWAP 协议而言,敌手无法获得一个有效的合法签名,而且即使敌手偶然获得一个有效的合法签名,敌手能够伪造出消息的多个合法签名,但由于用户身份的匿名性,无法发起身份认证过程,因而协议的安全性依然是有保证的。同时为了分析 NWAP 协议的安全性,利用 AUTlog 逻辑[12]对协议进行了形式化验证,没有发现明显的安全漏洞。

参考文献:

[1] Aydos M,Sunar B,KOC C K.An elliptic curve cryptograpy based authentication and key agreement protocol for wireless communication[EB/OL].(1998-10).[2005-10].http://islab,oregonstate.edu/papers.

[2] Sun Hung-min.Cryptanalysis of Aydos et al's wireless authentication protocol[EB/OL].http://ieeexplore.ieee.org,2004-03/2005-10.

[3] 邱慧敏,杨义先,胡正名,等.无线认证协议的改进[J].计算机工程与应用,2004,40(31):3-5.

[4] Law L,Menezes A.An efficient protocol for authenticated key agreement Technical report CORR[R].1998.

[5] mangipudi K,Malneedi N,Katti R,et al.Attacks and solutions on aydos-savas-koc's wireless authentication protocol[J].IEEE Communication Society,Golbecom,2004:2229-2234.

[6] Hoffstein J,Silverman J H.NTRU:a ring based public key cryptosystem[C]//Algotithmic Number Theory(ANTS III).[S.n.]:Sprinner-Verlag,1998,1423:267-288.

[7] Hoffstein J,Silverman J H.NSS:the NTRU signature scheme[C]//Proc of Eurocrypt'01,2045:211-228.

[8] Hoffslein J,Graham N,Pipher J,el al.NTRUSign:digital Signatures using the NTRU Lattice[C]//CT-RSA'03,[S.n.]:Spring-Verlag,2003:122-140.

[9] Jun Jiang,Chen He.A novel mutual authentication and key agreement protocol based on NTRU cryptography for wireless communication [J].Journal of Zhejiang University Science,2005,6A(5):399-402.

[10] Min S,Yamamoto G,Kim K.Weak property of malleability in ntrusign[C]//Australasian Conference on Information Security and Privacy(ACISP04).[S.n.]:Springer-Verlag,2004,31:379-390.

[11] Hoffstein J,Silverman J H.NTRUSign introducted[EB/OL].(2001-12).[2005-10].http://www.NTRU.com.

[12] Gabriele W,Volker K.Formal semantics for authentication logics[C]//LNCS 1146:Computer Security-ESORIC 96.Berlin:Springer-Verlag,1996,9:215-241.