非否认协议公平性分析的扩展串空间方法

李磊[1]，陈静[2]，王育民[1]
(1. 西安电子科技大学综合业务网国家重点实验室，710071，西安；2. 西安交通大学电子与信息工程学院，710049，西安)

摘要：针对在非否认协议公平性的形式化分析中，如何弱化初始假定和避免状态空间爆炸等问题，提出了扩展串空间方法. 通过将签名运算引入串空间理论，从而对串空间理论的项集合进行重新定义，进一步通过对子项关系、攻击者迹和自由加密假定的扩展，并结合丛概念，构成了扩展串空间. 分析非否认协议的公平性，首先将协议行为归纳为攻击者串、发送者串、接收者串和可信第3方串，以此构造协议的扩展串空间模型，然后结合协议迹和定理证明验证丛中存在发送者串等价于丛中存在接收者串，从而证明非否认协议公平性. 通过扩展串空间方法对 Zhou-Gollmann 协议公平性的分析，得到了与 Kailar 逻辑和 Lanotte 自动验证方法相同的结果. 与 Kailar 逻辑相比，扩展串空间方法仅使用自由加密假定，弱化了初始假定；与 Lanotte 自动验证方法相比，扩展串空间方法无需使用状态空间搜索，避免了状态空间爆炸问题.

关键词：非否认协议；扩展串空间；协议验证；公平性
中图分类号：TN918 **文献标志码**：A **文章编号**：0253-987X(2010)06-0016-05

An Extended Strand Space Method for Fairness Analysis of Non-Repudiation Protocols

LI Lei[1], CHEN Jing[2], WANG Yumin[1]
(1. National Key Laboratory of Integrated Service Networks, Xidian University, Xi′an 710071, China; 2. School of Electronics and Information Engineering, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: A new formal analysis method using extended strand space is presented to weaken initial assumptions and to avoid state space explosion in analyzing the fairness of non-repudiation protocols. Signature operations are introduced into the strand space theory, so that the set of terms and sub-term relations are redefined in the strand space theory. Then, an extended strand space model is constructed by inducing the action of protocols to the penetrating strand, the origin strand, the receiver strand, and the trusted third party strand. The fairness of non-repudiation protocols is analyzed by verifying that the existence of the origin strand in the bundle is equivalent to the existence of the receiver strand in the bundle depending on the measure of theorem proving. Analyzing results on Zhou-Gollmann protocol show that the proposed method can weaken initial assumptions compared with the logic method, and can avoid state space explosion compared with the state space method.

Keywords: non-repudiation protocol; extended strand space; protocol verification; fairness

非否认协议是实现电子商务的重要基础，它为网络实体之间的交互行为提供不可否认服务. 通常非否认协议必须具备的安全性质为不可否认性、公平性和时限性[1]，其中公平性是非否认协议最重要的属性.

形式化分析的方法是确保协议设计正确性的重

收稿日期：2009-10-02. 作者简介：李磊(1974—)，男，博士生；王育民(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60473027)；国家自然科学基金委员会-广东联合基金重点资助项目(U0835004).

要手段，目前针对非否认协议形式化分析的方法主要分为信念逻辑方法[2-5]和状态空间方法[6-7]两类. 前者扩展 BAN 逻辑，将其应用在非否认协议公平性的分析中，但这种分析方法不仅需要使用自由加密假定，还需要使用信道假定，在分析多方非否认协议时，还需要限定参与协议的实体数量，以防止状态空间爆炸. 后者基于状态空间搜索，其优点是可以进行自动验证，但分析中必须进行人工介入，防止状态空间爆炸.

串空间理论[8-12]仅使用自由加密假定，不受限于参与实体的数量，也不依赖于状态空间搜索，可以分析无限大小的协议，但串空间理论没有定义签名等密码学原语，仅能用来分析密钥交换协议，不适用于分析非否认协议公平性.

本文为串空间理论增加签名运算，扩展了串空间理论，给出了公平性在扩展串空间中的形式化定义，并提出了利用扩展串空间进行公平性分析的方法. 此外，以 Zhou-Gollmann(ZG)协议[13]公平性分析为实例，说明了分析非否认协议公平性的步骤，为非否认协议公平性的形式化分析提供了一种有效的新方法.

1　扩展串空间

串空间是由协议主体，包括诚实主体和攻击者主体的串组成的串集合，是由因果关系生成的有向图. 串是主体发送、接收消息的线性序列，记为 ζ. 协议主体交换的消息称为项，项中最重要的关系为子项关系，记为$\sqsubset$，$a \sqsubset b$ 表示 a 是 b 的子项. 二元组 $\langle \zeta, i \rangle$代表串 ζ 的第 i 个结点，记 $f(n)$代表结点 n 的符号项，$f'(n)$代表结点 n 的符号项的无符号部分.

在基本串空间理论中，对于项集合仅定义了加密和连接运算，没有区分对称密钥和非对称密钥，也没有定义签名运算. 非否认协议依赖加密和签名两种性质不同的密码学原语，因此基本串空间理论不能用于对非否认协议公平性的分析. 本文重新定义项集合 A 如下.

定义 1　项集合 A 满足以下条件：

(1)$W \subseteq A$ 是原子消息集合；

(2)$W_{\text{name}} \subseteq W$ 是标识符集合，本文使用 O、R、T 代表发方主体、收方主体和可信第 3 方主体；

(3)$K \subseteq A$ 是密钥集合，K 与 W 不相交，K 中有 1 个一元算子，求逆 $K \to K$，它将非对称密码系统中的密钥对中的一个映射为另一个，将对称密钥映射为自身；

(4)$P \subseteq K$，$P^{-1} \subseteq K$ 是非对称密钥集合，本文用 P 表示私钥集合，用 P^{-1}表示公钥集合；

(5)$K_s \subset K$ 是对称密钥集合，K_s 与 P 不相交且 K_s 与 P^{-1}不相交；

(6)A 中有 3 个二元算子，加密 $K_s \times A \to A$，连接 $A \times A \to A$，签名 $P \times A \to A$.

本文中用 $E_k(m)$表示用密钥 k 对消息 m 加密；用 $\text{link}(g,h)$表示对消息 g 和 h 进行连接操作，用 $S_p(m)$表示用私钥 p 对消息 m 签名.

由于增加了签名运算，子项关系有如下定义.

定义 2　子项关系递归定义为满足下列关系的最小关系：

(1)$a \sqsubset a$；

(2)$a \sqsubset E_k(g)$，如果 $a \sqsubset g$；

(3)$a \sqsubset S_P(g)$，如果 $a \sqsubset g$；

(4)$a \sqsubset \text{link}(g,h)$，如果 $a \sqsubset g \vee a \sqsubset h$.

攻击者迹用来描述攻击者的能力，由攻击者所具有的原子行为组成.

定义 3　攻击者迹包括如下内容：

(1)发送正文消息　$\langle +w \rangle, w \in W$；

(2)发送密钥　$\langle +k \rangle, k \in K$；

(3)连接　$\langle -g, -h, +\text{link}(g,h) \rangle$；

(4)分解　$\langle -\text{link}(g,h), +g, +h \rangle$；

(5)加密　$\langle -k, -h, +E_K(h) \rangle$；

(6)解密　$\langle -k^{-1}, -E_K(h), +h \rangle$；

(7)签名　$\langle -p, -h, +S_P(h) \rangle, p \in P$；

(8)验证　$\langle -p^{-1}, -S_P(h), +h \rangle$.

自由加密假定规定，一个密文只能用一种方式看待. 基本串空间理论中定义自由加密假定为 A 是由 K 和 W 通过加密和连接运算自由生成的代数[8]，由于本文增加了签名运算，因而扩展如下自由加密假定.

公理 1　对于 $m', m' \in A, k, k' \in K_s, P_a, P_b, P_c \in P, a, b, c \in W_{\text{name}}$，总有：

(1)$S_{P_a}(m) = S_{P_b}(m') \Leftrightarrow m = m' \wedge P_a = P_b \wedge a = b$；

(2)$mm' \neq E_{k'}(m) \neq S_{P_c}(m')$；

(3)$S_{P_c}(m) \notin W \bigcup K$.

丛是具有发送、接收关系以及前趋、后继关系的串组成的集合，是串空间的子集，记为 Ω. 扩展串空间是由重定义的项集合、扩展的子项关系、攻击者迹、自由加密假定以及丛等主要概念，结合协议迹和定理证明的一种形式化分析方法.

2　公平性定义及证明思路

公平性是非否认协议最关键的属性，它包括两

层含义:①协议正常完成后,发送方收到收方非否认证据,记为 Z_{nrr},接收方收到发方非否认证据,记为 Z_{nro};②如果协议异常终止,协议应能保证通信双方都处于同等地位,任何一方都不占有优势.因此,可对公平性进行如下形式化定义.

定义 4 若发送方 O 收到 Z_{nrr},当且仅当接收方 R 收到 Z_{nro},则称非否认协议满足公平性.

对公平性的证明,可以从两方面来考虑:①当发送方 O 收到 Z_{nrr} 时,接收方 R 一定收到了 Z_{nro};②当接收方 R 收到 Z_{nro} 时,发送方 O 一定收到了 Z_{nrr}.这样,当任何一方没有收到期待的数据时,另一方也不可能收到期待的数据,因此满足定义 4 的条件,即可保证协议满足公平性.

在扩展串空间中,Z_{nrr} 和 Z_{nro} 由数据项组成.假设丛 Ω 中包含表示发送方 O 应用 Z_{nrr} 参与协议的串,如果能够证明,丛 Ω 中也包含表示收方 R 应用 Z_{nro} 参与协议的串,则可证明当发送方 O 收到 Z_{nrr} 时,接收方 R 一定收到了 Z_{nro};反之,假设丛 Ω 中包含表示收方 R 应用 Z_{nro} 参与协议的串,如果也能够证明,丛 Ω 中包含表示发方 O 应用 Z_{nrr} 参与协议的串,则可以证明协议满足公平性.

在扩展串空间中,发送者串可表示发方 O 应用 Z_{nrr} 参与协议,接收者串可表示收方 R 应用 Z_{nro} 参与协议.利用串空间模型证明非否认协议公平性可遵循以下几个步骤:

(1)为非否认协议建立串空间模型;

(2)证明若丛 Ω 中存在发送者串,则丛 Ω 中必然存在接收者串;

(3)证明若丛 Ω 中存在接收者串,则丛 Ω 中必然存在发送者串.

3 扩展串空间方法证明 ZG 协议的公平性

3.1 ZG 协议

ZG 协议是典型的非否认协议,协议将待发送的信息 m 分为两部分:加密密钥 k 和密文 $C=E_k(m)$.首先发方 O 将 C 和发方证据 Z_O 发送给收方 R,R 用收方证据 Z_R 进行响应;然后 O 将 k 以 Z_{sk} 的形式提交给可信第 3 方 T;最后 O 和 R 可通过获取操作从 T 处获得 k 和证据 Z_{ck}.假设 L 代表协议本次运行的唯一标识符,记 $Z_O=S_{P_O}(R,L,C)$,$Z_R=S_{P_R}(O,L,C)$,$Z_{sk}=S_{P_O}(R,L,k)$,$Z_{ck}=S_{P_T}(O,R,L,k)$,非否认证据 $Z_{\mathrm{nrr}}=(Z_R,Z_{ck})$,$Z_{\mathrm{nro}}=(Z_O,Z_{ck})$.若产生争议,$O$ 可提交 Z_{nrr},R 可提交 Z_{nro} 给仲裁机构进行仲裁,则 ZG 协议的交互步骤可描述如下:

(1)$O\rightarrow R:R,L,C,Z_O$;

(2)$R\rightarrow O:O,L,Z_R$;

(3)$O\rightarrow T:R,L,k,Z_{sk}$;

(4)$R\leftrightarrow T:O,R,L,k,Z_{ck}$;

(5)$O\leftrightarrow T:O,R,L,k,Z_{ck}$.

3.2 ZG 串空间

ZG 协议中的获取操作可理解为,T 发送给 O 和 R 的消息 m 总能被 O 和 R 收到,因此在扩展串空间下定义获取操作如下.

定义 5 若实体 a 通过获取操作向 T 获取消息 m,则对于满足 $\exists f(\langle\zeta_T,i\rangle)=m$ 的串 ζ_T,令丛 Ω 是满足 $\zeta_T\in\Omega$ 的任意丛,总有串 $\zeta_a\in\Omega$ 满足 $\exists f(\langle\zeta_a,j\rangle)=-m$ 且 $\langle\zeta_T,i\rangle\prec\langle\zeta_a,j\rangle$.

ZG 串空间可描述如下.

定义 6 设 (Σ,ρ) 是一个渗透串空间,如果 Σ 由下述 4 种串组成,就称它为一个 ZG 串空间:

(1)攻击者串 $s\in\rho$;

(2)发送者串 $s\in\zeta_O[O,R,T,L,m,k]$,其迹为 $\langle+RLE_k(m)Z_O,-OLZ_R,+RLkZ_{sk},-ORLkZ_{ck}\rangle$,其中 $O,R,T\in W_{\mathrm{name}}$,$L,m\in W$,但 $L,m\notin W_{\mathrm{name}}$,$k\in K_s$,$\zeta_O[O,R,T,L,m,k]$ 表示所有具有上述迹的串集合,与这种串对应的主体是发送者 O;

(3)接收者串 $s\in\zeta_R[O,R,T,L,m,k]$,其迹为 $\langle-RLE_k(m)Z_O,+OLZ_R,-ORLkZ_{ck}\rangle$,$\zeta_R[O,R,T,L,m,k]$ 表示所有具有上述迹的串集合,与这种串对应的主体是接收者 R;

(4)可信第 3 方串 $s\in\zeta_W[O,R,T,L,k]$,其迹为 $\langle-RLkZ_{sk},+ORLkZ_{ck},+ORLkZ_{ck}\rangle$,$\zeta_T[O,R,T,L,k]$ 表示所有具有上述迹的串集合,与这种串对应的主体是可信第 3 方 T.

称发送者串、接收者串和可信第 3 方串为正则串,正则串上的结点称为正则结点.给定 Σ 中的一个串,从其形式可以唯一确定它是攻击者串、发送者串、接收者串还是可信第 3 方串.因此,在 ZG 串空间 (Σ,ρ) 中,可以省略 ρ 而不会引起混淆.

3.3 ZG 协议的公平性

证明 ZG 协议的公平性,需要证明以下 2 个命题.

命题 1 假设下列条件成立:

(1)Σ 是一个 ZG 串空间,Ω 是 Σ 中的丛,s 是一个 $\zeta_O[O,R,T,L,m,k]$ 中的发送者串;

(2)$P_O\notin K_\rho$,$P_R\notin K_\rho$,$P_T\notin K_\rho$;

(3)$L\neq m$,且 L,m,k 在 Σ 中是唯一起源的项.

于是,丛 Ω 中包含一个接收者串 $r\in\zeta_R[O,R,T,L,m,k]$.

命题 2　假设下列条件成立:

(1)Σ 是一个 ZG 串空间,Ω 是 Σ 中的丛,r 是一个 $\zeta_R[O,R,T,L,m,k]$中的接收者串;

(2)$P_O\notin K_\rho,P_R\notin K_\rho,P_T\notin K_\rho$;

(3)$L\neq m$,且 L,m,k 在 Σ 中是唯一起源的项.

于是,丛 Ω 中包含一个发送者串 $s\in\zeta_O[O,R,T,L,m,k]$.

后面将通过一系列引理证明命题 1. 任意选定一个满足命题 1 中假设的 $\Sigma,\Omega,s,O,R,T,L,m,k$. 结点$\langle s,1\rangle$的输出值为 $RLE_k(m)Z_O$,将其记为 n_0,它的项记为 v_0.

引理 1　项 Z_{dk}起源于正则结点 n_3.

证明　$Z_{dk}=S_{P_T}(O,R,L,k)$,设项 Z_{dk}起源于 n_3,依次考查攻击者迹中正结点的以下各种可能情况:

(1)$\langle+w\rangle,w\in W$,由自由加密假定,$Z_{dk}\not\sqsubset w$,因此它的正结点不是 n_3;

(2)$\langle+k\rangle,k\in K$,由自由加密假定,$Z_{dk}\not\sqsubset k$,因此它的正结点不是 n_3;

(3)$\langle-g,-h,+\mathrm{link}(g,h)\rangle$,若它的正结点是 n_3,则 $Z_{dk}\sqsubset\mathrm{link}(g,h)$,必有 $Z_{dk}\sqsubset g\vee Z_{dk}\sqsubset h$,显然存在正结点 n',使 $Z_{dk}\sqsubset f(n')\wedge n'<n_3$,与 n_3 是源点矛盾;

(4)$\langle-\mathrm{link}(g,h),+g,+h\rangle$,若它的正结点是 n_3,则 $Z_{dk}\sqsubset g\vee Z_{dk}\sqsubset h$,必有 $Z_{dk}\sqsubset\mathrm{link}(g,h)$,显然存在正结点 n',使 $Z_{dk}\sqsubset f(n')\wedge n'<n_3$,与 n_3 是源点矛盾;

(5)$\langle-k,-h,+E_k(h)\rangle$,若它的正结点是 n_3,由于 $E_k(h)\neq Z_{dk}$,因此有 $Z_{dk}\sqsubset h$,显然存在正结点 n',使 $Z_{dk}\sqsubset f(n')\wedge n'<n_3$,与 n_3 是源点矛盾;

(6)$\langle-k^{-1},-E_k(h),+h\rangle$,若它的正结点是 n_3,则 $Z_{dk}\sqsubset h$,必有 $Z_{dk}\sqsubset E_k(h)$,显然存在正结点 n',使 $Z_{dk}\sqsubset f(n')\wedge n'<n_3$,与 n_3 是源点矛盾;

(7)$\langle-p,-h,+S_p(h)\rangle,p\in P$,因 $p\in K_\rho,P_T\notin K_\rho$,所以 $S_p(h)\neq Z_{dk}$,因此若它的正结点是 n_3,则有 $Z_{dk}\sqsubset S_p(h)$,必有 $Z_{dk}\sqsubset h$,显然存在正结点 n',使 $Z_{dk}\sqsubset f(n')\wedge n'<n_3$,与 n_3 是源点矛盾;

(8)$\langle-p^{-1},-S_p(h),+h\rangle$,若它的正结点是 n_3,则 $Z_{dk}\sqsubset h$,必有 $Z_{dk}\sqsubset S_p(h)$,显然存在正结点 n',使 $Z_{dk}\sqsubset f(n')\wedge n'<n_3$,与 n_3 是源点矛盾.

综上所述,n_3 不可能在一个攻击者串上,因此 n_3 是正则结点.

引理 2　设 n_3 在正则串 t 上,则 t 是丛 Ω 中的可信第 3 方串.

证明　结点 n_3 是一个符号为正的正则结点,且包含形为 $S_P(a,b,c,d)$的子项. 在所有正的正则结点中,只有可信第 3 方串的第 2、3 结点包含这样的子项;又 n_3 是 Z_{dk}的源点,故 n_3 是可信第 3 方串的第 2 结点. 由可信第 3 方的可信性,知必存在该串的第 3 结点,因此 t 是丛 Ω 中的可信第 3 方串.

引理 3　项 Z_R 起源于正则结点 n_2.

证明　$Z_R=S_{P_R}(O,L,E_k(m))$,设项 Z_R 起源于 n_2,依次考查攻击者迹,类似于引理 1 的证明,可得到 n_2 是正则结点. 在此不再赘述.

引理 4　m 起源于 n_0.

证明　由假设,$m\sqsubset n_0$,且 n_0 符号为正,由于 n_0 所在串上没有前驱结点,因此 m 起源于 n_0.

引理 5　设 n_2 在正则串 r 上,则 r 上存在 n_2 的前驱结点 n_1,且 $m\sqsubset f(n_1)$.

证明　由于 $Z_R\sqsubset n_2$,但 $Z_R\not\sqsubset n_0$,因此 $n_2\neq n_0$. 由引理 2 知 m 起源于 n_0,且由命题 1 的条件(3) 知,m 在 Σ 中是唯一起源的,因此 m 不起源于 n_2. 又由于 $m\sqsubset Z_R\sqsubset f(n_2)$,因而在串 r 上存在 n_2 的前驱结点 n_1,使得 $m\sqsubset f(n_1)$.

引理 6　包含 n_1 和 n_2 的正则串 r 是丛 Ω 中的接收者串.

证明　正则串 r 上的结点 n_1 和 n_2 满足以下性质:①n_2 是一个正的正则结点;②n_2 包含一个形为 $S_p(a,b,E_k(c))$的子项;③n_1 是 n_2 在串 r 上的前驱结点;④$m\sqsubset f(n_1)$. 考查丛 Ω 中的正则串,满足上述条件的结点只能是接收者串的第 1 个和第 2 个结点,因此包含 n_1 和 n_2 的正则串 r 是丛 Ω 中的接收者串.

由引理 2 知,丛 Ω 中存在可信第 3 方串 t,使 $f(\langle t,3\rangle)=ORLkZ_{dk}$,根据定义 5 可知,接收者串 r 上必存在结点 n',使得 $f(n')=-ORLkZ_{dk}$. 考查丛 Ω 中的接收者串,该结点为接收者串 r 的第 3 个结点.

由以上引理可立即得到命题 1.

对命题 2 的证明,同样可先利用 Z_{dk}的起源证明丛 Ω 中存在可信第 3 方串,然后利用 m、k 和 Z_O 的起源证明丛 Ω 中存在发送者串,证明方法与命题 1 的证明方法类似,在此不再赘述.

4　结　论

本文通过将签名运算引入串空间理论,重新定

义了项集合,并在此基础上扩展了子项关系、攻击者迹和自由加密假定,提出了扩展串空间模型.在扩展串空间模型下,提出了分析非否认协议公平性的思路和步骤.通过对ZG协议公平性的分析,说明扩展串空间方法仅使用自由加密假定,且不依赖于状态空间搜索,就能够得到与以往方法相同的分析结果.

参考文献:

[1] KREMER S, MARKOWITCH O, ZHOU J. An intensive survey of fair non-repudiation protocols [J]. Computer Communications, 2002, 25(17): 1606-1621.

[2] KAILAR R. Accountability in electronic commerce protocols [J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313-328.

[3] 周典萃,卿斯汉,周展飞. 一种分析电子商务协议的新工具[J]. 软件学报, 2001, 12(9): 1318-1328.
ZHOU Diancui, QING Sihan, ZHOU Zhanfei. New approach for the analysis of electronic commerce protocols[J]. Journal of Software, 2001, 12(9): 1318-1328.

[4] 黎波涛,罗军舟. 不可否认协议时限性的形式化分析[J]. 软件学报, 2006, 17(7): 1510-1516.
LI Botao, LUO Junzhou. Formal analysis of timeliness in non-repudiation protocols [J]. Journal of Software, 2006, 17(7): 1510-1516.

[5] 韩志耕,罗军舟. 多方不可否认协议时限性分析与改进[J]. 电子学报, 2009, 37(2): 377-381.
HAN Zhigeng, LUO Junzhou. Analysis and improvement of timeliness of a multi-party non-repudiation protocol [J]. Acta Electronica Sinica, 2009, 37(2): 377-381.

[6] LANOTTE R, MAGGIOLO-SCHETTINI A, TROINA A. Automatic analysis of a non-repudiation protocol [J]. Electronic Notes in Theoretical Computer Science, 2005, 112(S): 113-129.

[7] GUO Yingjun, LIN Chuang, YIN Hao. Formal proof of the IDOP_SP protocol based on the Petri net [C]// Proceedings of the 2008 IEEE International Conference on NAS. Piscataway, NJ, USA: IEEE, 2008: 161-162.

[8] FABREGA F J T, HERZOG J C, GUTTMAN J D. Strand spaces: why is a security protocol correct? [C]// Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos, CA, USA: IEEE Computer Society, 1998: 160-171.

[9] FABREGA F J T, HERZOG J C, GUTTMAN J D. Honest ideals on strand spaces [C]// Proceedings of the Computer Security Foundations Workshop. Los Alamitos, CA, USA: IEEE Computer Society, 1998: 66-77.

[10] FABREGA F J T, HERZOG J C, GUTTMAN J D. Mixed strand spaces [C]// Proceedings of the Computer Security Foundations Workshop. Los Alamitos, CA, USA: IEEE Compute Society, 1999: 72-82.

[11] FABREGA F J T, HERZOG J C, GUTTMAN J D. Strand spaces: proving security protocols correct [J]. Journal of Computer Security, 1999, 7(2): 191-230.

[12] GUTTMAN J D, FABREGA F J T. Authentication tests [C]// Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos, CA, USA: IEEE Computer Society, 2000: 96-109.

[13] ZHOU J, GOLLMANN D. A fair non-repudiation protocol [C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Piscataway, NJ, USA: IEEE, 1996: 55-61.

[本刊相关文献链接]

采用中国剩余定理的群签名方案的安全性分析与改进. 西安交通大学学报,2009, 43(2): 77-80.

具有局部验证者撤销的短群签名方案. 西安交通大学学报,2008, 42(10): 1250-1253.

排序问题的多方保密计算协议. 西安交通大学学报, 2008, 42(2): 231-233.

一种防破坏广播型匿名通信网的多路访问协议. 西安交通大学学报, 2007, 41(6): 674-678.

基于SWIM卡公钥认证的二阶段握手加密套接层协议. 西安交通大学学报, 2007, 41(6): 669-673.

码率约束抗丢包伸缩码流保护的码率分配方法. 西安交通大学学报, 2006, 40(12): 1432-1435.

一个可验证的秘密共享新个体加入协议. 西安交通大学学报, 2006, 40(2): 207-210.

集合相交问题的双方保密计算. 西安交通大学学报, 2006, 40(10): 1091-1093.

(编辑 刘杨)