一种新的安全协议及其串空间模型分析

皮建勇[1] 杨 雷[2] 刘心松[3] 李泽平[3]

(贵州大学计算机科学与信息学院 贵阳 550025)[1] (中国人民解放军第二炮兵工程设计研究院 北京 100011)[2]

(电子科技大学计算机科学与工程学院 成都 610054)[3]

摘 要 针对有限域上计算离散对数的困难,提出了一种新的身份认证与密钥协商安全协议——PJY。PJY安全协议通过两次握手就可以验证通信双方的身份,同时产生对等的会话密钥。采用串空间模型分析该安全协议的正确性,通过构造渗透串空间模型,采用认证测试证明了PJY安全协议在任意一种攻击串模式下都具有单射一致性和机密性,从而证明了PJY安全协议的正确性。

关键词 PJY安全协议,串空间模型,认证测试,单射一致性,机密性

中图法分类号 TP309.2 **文献标识码** A

Novel Security Protocol and Strand Space Analysis

PI Jian-yong[1] YANG Lei[2] LIU Xin-song[3] LI Ze-ping[3]

(School of Computer Science and Information, Guizhou University, Guiyang 550025, China)[1]

(Engineering Design & Research Institute of Second Artillery Corps, PLA, Beijing 100011, China)[2]

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)[3]

Abstract We proposed a novel PJY identity authentication and key agreement security protocol based on computational difficulty of discrete logarithm in finite field. The PJY security protocol can validate identity of the both parties with two session, and generate peer session key. We analyzed the correctness of the security protocol on strand space model. First we constructed infiltrate strand space, and proved the PJY security protocol has injective agreement and secrecy by authentication tests under arbitrary penetration strand, so proved the PJY security protocol is correct.

Keywords PJY security protocol, Strand space, Authentication tests, Injective agreement, Secrecy

网络通信中需要高效和安全的身份认证和密钥协商机制来构成通信安全协议,并能通过形式化方式验证安全协议的正确性。本文基于身份标识签名和密钥协商机制的PJY安全协议,通信双方实际会话过程中进行两次会话,就可以互相验证对方的身份并生成对等会话密钥。PJY安全协议采用串空间(Strand Space)模型进行形式化的分析[1],对一致性证明采用了基于串空间模型的认证测试方法(Authentication Tests)[2],使得证明过程简洁、直观,同时验证了PJY安全协议的机密性,因而证明PJY安全协议在单射一致性和机密性上是正确的。

1 身份认证与密钥协商机制

首先假定存在一个可信的初始化认证方,功能在于对通信双方的身份标识进行签名,但认证过程并不参与通信双方实际的会话过程。

1.1 初始化过程

令 *Auth* 为第三方的初始化认证方,*Alice* 为通信会话的发起者,*Bob* 为通信会话的响应者,有

$$m_{Alice}, m_{Bob}, \exists m_{Alice} \neq m_{Bob}$$

分别为 *Alice* 和 *Bob* 的主体标识。首先取 p 为一个大素数,令 $Z_p=\{0,1,2,\cdots,p\}$,于是有 $Z_p^*=\{1,2,\cdots,p-1\}$。又令 $g\in Z_p^*$,g 是 Z_p^* 上随机选取的乘法生成元,所以 Z_p 是一个有限域 $GF(p)$,并且满足 *Alice* 和 *Bob* 的标识信息 $m_{Alice}, m_{Bob}\in GF(p)$,即

$$0\leqslant m_{Alice}\leqslant(p-1), 0\leqslant m_{Bob}\leqslant(p-1)$$

初始化认证方选取任意元素 $V_{Auth}\in GF(p)$,并计算

$$Y_{Auth}\equiv g^{V_{Auth}} \bmod p \tag{1}$$

其中,V_{Auth} 作为 *Auth* 认证方的私钥由认证方秘密保存,Y_{Auth},p,g 则作为 *Auth* 认证方的公钥分发给 *Alice* 和 *Bob*[3]。

1.2 签名过程

令 i 为任意的通信方,*Auth* 随机选取 $s_i\in GF(p)$,且 $s_i<p-1$ 和 $s_i'\in GF(p)$,且 $s_i'<p-1$,并要求

$$\gcd(s_i, p-1)=1 \tag{2}$$

$$\gcd(s_i', p-1)=1 \tag{3}$$

到稿日期:2009-02-18 返修日期:2009-05-20 本文受四川省应用基础研究项目(04JY029-017-2),科技型中小企业技术创新基金(04C26225110223)资助。

皮建勇(1973—),男,博士,副教授,主要研究方向为信息安全、分布式并行计算,E-mail:pijianyong@hotmail.com;杨 雷(1965—),男,高级工程师,主要研究方向为无线通信、信息安全;刘心松(1940—),男,教授,博士生导师,主要研究方向为分布式并行计算、宽带网络与通信;李泽平(1964—),男,博士生,副教授,主要研究方向为分布式计算、流媒体技术。

计算 $W_i \equiv g^{s_i} \pmod p$，$Q_i \equiv g^{s_i'} \pmod p$，并由

$$m_i s_i' \equiv V_{Auth} W_i + U_i \pmod{p-1} \tag{4}$$

解出 U_i，将 (W_i, Q_i, U_i) 作为通信双方的身份标识签名和 Y_{Auth}, p, g 一起发给通信方，但通信方必须秘密保存 (W_i, Q_i, U_i)，而对 Y_{Auth}, p, g 各节点也应当妥善保管，以备后用，即 $Sig(m_i, V_{Auth}) = (W_i, Q_i, U_i)$。

1.3 身份验证过程

要验证各节点的认证码，则要验证

$$g^{m_i s_i'} \equiv g^{V_{Auth} W_i + U_i} \pmod p \tag{5}$$

即需要验证

$$Q_i^{m_i} \equiv Y_{Auth}^{W_i} g^{U_i} \pmod p \tag{6}$$

因此身份验证可表示为

$$Verify_{(g, Y_{Auth}, p)}(m_i, (W_i, Q_i, U_i)) = \text{True} \tag{7}$$

1.4 PJY 安全协议

令 *Alice* 为通信的发起人，*Bob* 为通信的响应者，*Alice* 和 *Bob* 共同认定一个对称密钥算法 K。分别以 A, B 作为下标表示。包含身份认证与密钥协商过程的安全协议如下：

Step1 *Alice* 随机产生两个大整数 x 和 x'，计算

$$Q_A^{x'} \equiv \Delta_A g^{xx'} \pmod p \text{且} \gcd(\Delta_A, p) = 1, \text{解出 } \Delta_A \tag{8}$$

$$\Delta_A X \equiv Q_A^{m_A + x'} \pmod p, \text{解出 } X \tag{9}$$

$$X' \equiv g^{U_A + xx'} \pmod p \tag{10}$$

Alice 将 (m_A, W_A, X, X') 发给 *Bob*。

Step2 *Bob* 随机产生一个大整数 y'，令 y 为另一个未知大整数，计算

$$\Delta_B X \equiv Q_B^{m_B + y'} \pmod p \text{且} \gcd(\Delta_B, p) = 1, \text{解出 } \Delta_B \tag{11}$$

$$Q_B^{y'} \equiv \Delta_B g^{yy'} \pmod p, \text{解出 } g^{yy'} \tag{12}$$

$$Y' \equiv g^{U_B + yy'} \pmod p \tag{13}$$

Bob 将 (m_B, W_B, X, Y') 发给 *Alice*。

Step3 *Alice* 为了认证 *Bob* 的身份，不改变同余性，将式(12)×式(6)，即需要验证

$$Q_B^{y'} Q_B^{m_B} \equiv Y_{Auth}^{W_B} g^{U_B} \Delta_B g^{yy'} \pmod p \tag{14}$$

由式(11)、式(13)，得出需要验证

$$X \equiv Y_{Auth}^{W_B} Y' \pmod p \tag{15}$$

如果式(15)成立，则 *Bob* 的身份是可信的。

Step4 *Bob* 为了认证 *Alice* 的身份，不改变同余性，将式(8)×式(6)，即需要验证

$$Q_A^{x'} Q_A^{m_A} \equiv Y_{Auth}^{W_A} g^{U_A} \Delta_A g^{xx'} \pmod p \tag{16}$$

由式(9)、式(10)，得出需要验证

$$X \equiv Y_{Auth}^{W_A} X' \pmod p \tag{17}$$

如果式(17)成立，则 *Alice* 的身份是可信的。

Step5 *Alice* 在收到 (m_B, W_B, X, Y') 后，计算

$$k_1 \equiv Y'^{U_A + xx'} \pmod p \tag{18}$$

Step6 *Bob* 在收到 (m_A, W_A, X, X') 后，因为已知 $g^{yy'}$，所以可以计算

$$k_2 \equiv X'^{U_B + yy'} \pmod p \tag{19}$$

Step7 *Alice* 与 *Bob* 分别产生的 k_1, k_2 即为双方秘密通信所需的对称会话密钥，并且

$$k_1 = k_2 \equiv g^{(U_A + xx')(U_B + yy')} \pmod p \tag{20}$$

Alice 对 Y' 用对称加密算法 K 得到密文 $\{Y'\}_{k_1}$，发给 *Bob*，*Bob* 计算 $K^{-1}\{\{Y'\}_{k_1}\}_{k_2}$，如果有

$$Y' = K^{-1}\{\{Y'\}_{k_1}\}_{k_2} \tag{21}$$

则表明会话密钥 k 协商成功，可以进行后继的数据传递工作。

从上述安全协议可以看出，通信双方通过两次会话交互过程，就可以进行双方身份认证和密钥协商，因而 PJY 安全协议有较高的执行效率。

2 安全协议的串空间模型分析

串空间模型(Strand Space)是一种结合定理证明和协议轨迹的混合方法，能构造攻击过程，以揭示安全协议是否存在内在缺陷[4]。

实际的通信过程中，由于认证方签名过程并不参与到实际的通信过程中，因此不考虑初始化过程中对通信双方身份标识的签名过程，令 A, B 为通信双方。为了更细致地描述 PJY 协议，根据式(9)和式(13)，由于 X, Y' 和 x', y' 分别满足离散对数的计算关系，因此可以将 X, Y' 分别看成项 x', y' 的加密项，即 $X = \{x'\}_{k_A}$ 和 $Y' = \{y'\}_{k_B}$，其中 $k_A^{-1}, k_B^{-1} \notin \mathcal{K}_P$，这里 $\mathcal{K}_P$ 表示不安全的密钥集合。将本文所提出的 PJY 安全协议简化描述如下。

(1) $A \rightarrow B: \{m_A, W_A, \{x'\}_{k_A}, X'\}$

(2) $B \rightarrow A: \{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}$

(3) $A \rightarrow B: \{\{y'\}_{k_B}\}_k$

令 T 为正文集合，表示 PJY 协议中的原子消息。标识符集合 $T_{name} \subseteq T$，即 $m_A, m_B \in T_{name}$。其中标识符 $m_A \neq m_B$，并且 $W_A \neq W_B$。此处 $x', X', y' \in T$，但 $x', X', y' \notin T_{name}$。$k$ 为协商的会话密钥，且 $k^{-1} \notin K_p$。

2.1 PJY 串空间模型

定义 1 设 $(\Sigma, \mathcal{P})$ 是一个渗透串空间，如果 Σ 由下述 3 种串组成，就称它为一个 PJY 串空间。

(1)攻击者串 $p \in \mathcal{P}$。

(2)发起者串 $t \in Init[m_A, m_B, W_A, W_B, x', X', y']$，其迹为

$\langle +\{m_A, W_A, \{x'\}_{k_A}, X'\}, -\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}, +\{\{y'\}_{k_B}\}_k \rangle$，其中 $m_A \neq m_B, W_A \neq W_B$。$Init[m_A, m_B, W_A, W_B, x', X', y']$ 表示所有具有上述迹的串的集合，与这种串对应的主体为 A。

(3)响应者串 $s \in \text{Re } sp[m_A, m_B, W_A, W_B, x', X', y']$，其迹为

$\langle -\{m_A, W_A, \{x'\}_{k_A}, X'\}, +\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}, -\{\{y'\}_{k_B}\}_k \rangle$，其中 $m_A \neq m_B, W_A \neq W_B$。$\text{Re } sp[m_A, m_B, W_A, W_B, x', X', y']$ 表示所有具有上述迹的串的集合，与这种串对应的主体为 B。

如果串 $t \in Init[m_A, m_B, W_A, W_B, x', X', y']$ 或者串 $s \in \text{Re } sp[m_A, m_B, W_A, W_B, x', X', y']$ 是正则串，则分别称 A, B 为发起者与响应者。同时分别称 x', X', y' 为发起方值和响应方值。建立 PJY 串空间模型的目的之一是要证明这些值的随机性，即 x', X', y' 在 Σ 中是惟一起源的，同时需要证明 PJY 串空间的一致性和机密性，如图 1 所示。

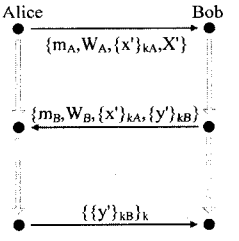

图 1 PJY 安全协议串空间模型

为了后续证明的叙述方便，给出串空间模型中认证测试关于出测试的两条性质[5]。

认证测试中出测试的原理如下：令 C 为丛，$n' \in C, n \Rightarrow^+ n'$ 是 a 在 $t=\{h\}_K$ 中的出测试，其中项 $t=\{h\}_K$ 为项 a 在结点 n 中的测试分量，边 $n \Rightarrow^+ n'$ 是关于 a 的被变换边。于是有

(1)存在正则结点 $m, m' \in C$，使得 t 是 m 的分量，且 $m \Rightarrow^+ m'$ 是对于 a 的被变换边；

(2)假设除此之外 a 只在 m' 的分量 $t_1=\{h_1\}_{K_1}$ 中出现，且 t_1 不是任何正则分量的真子项，同时 $K_1^{-1} \notin \mathcal{K}_P$，于是存在一个负正则结点 m''，其中 t_1 是 m'' 的分量。

2.2 一致性：响应者的保证

命题 1 假设下列条件成立。

(1)Σ 是一个 PJY 串空间，C 是 Σ 中的一个丛，s 是一个串 Re $sp[m_A, m_B, W_A, W_B, x', X', y']$ 中的响应者串，且 $C-height(s)=3$；

(2)$k_A^{-1} \notin \mathcal{K}_P, k_B^{-1} \notin \mathcal{K}_P$，且 $k^{-1} \notin \mathcal{K}_P$；

(3)$m_A \neq m_B, W_A \neq W_B, x' \neq y', X' \neq y'$，且 y' 在 Σ 中是惟一起源的项。

于是，C 中包含一个发起者串

$t \in Init[m_A, m_B, W_A, W_B, x', X', y']$

且 $C-height(t)=3$。

随后将通过证明一系列引理来证明上述命题。串 s 的结点 $\langle s,2\rangle$ 输出值为 $\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}$。为后续证明方便，将这个结点记为 n_2，项记为 v_2。结点 $\langle s,3\rangle$ 收到值 $\{\{y'\}_{k_B}\}_k$ 后，将这个结点记为 n_5，项记为 v_5。在证明过程中，还要用到另外 4 个结点 n_0, n_1, n_3, n_4，它们满足传递闭包关系 $n_2 \prec n_3 \prec n_4 \prec n_5$，如图 2 所示。

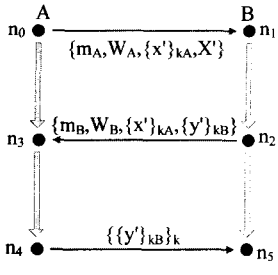

图 2 PJY 串空间模型简化图

引理 1 y' 惟一起源于 n_2。

证明：由假设，$y' \sqsubset n_2$，且 n_2 的符号为正，因此，只需要证明 $y' \not\sqsubset n_1$，其中 n_1 是与结点 n_2 在同一个响应串的前驱结点 $\langle s,1\rangle, term(n_1)=\{m_A, W_A, \{x'\}_{k_A}, X'\}$。需要验证 $y' \neq x'$，$y' \neq X'$。由命题 1 假设 $x' \neq y', X' \neq y'$，且由第 2 节中的式(9)、式(10)、式(13)，$x' \neq y', X' \neq y'$。最后验证 $y' \neq m_A$ 和 $y' \neq W_A$，由前提假设条件 $x', X', y' \notin T_{name}$，可知 $y' \neq m_A$ 成立；由第 2 节中的式(13)，可知 $y' \neq W_A$ 也同样成立。因此 $y' \not\sqsubset n_1$ 成立，即 y' 惟一起源于 n_2。

引理 2 集合 $S=\{n \in C: y' \sqsubset term(n) \wedge v_2 \not\sqsubset term(n)\}$ 有一个 $\preceq$ 极小元 n_4，结点 n_3, n_4 是正则结点且 n_4 符号为正。

证明：因为 $n_5 \in C$，且 n_5 包含 y'，但不包含 v_2，所以 $v_2 \in S$，因此 S 为非空集合。由串空间丛的性质，S 至少有一个 $\preceq$ 极小元 n_4，再由丛中极小元的性质可知，n_4 的符号为正。

下面证明 n_3, n_4 不可能在攻击者串上。根据串空间模型中攻击者串的 6 种攻击者迹模型，依次考察 n_4 为攻击者结点的各种可能情形。

(1)M. 迹 $tr(p)$ 具有形式 $\langle +t\rangle$，其中 $t \in \mathcal{T}$，因此必然有 $y'=t$。而此时 y' 起源于这个串，这与引理 1 相矛盾，且命题 1 中假设“y' 在 Σ 中是惟一起源的项”相矛盾。

(2)C. 迹 $tr(p)$ 具有形式 $\langle -g, -h, +gh\rangle$，因此它的正则结点不会是 S 中的极小元。

(3)K. 迹 $tr(p)$ 具有形式 $\langle +K_0\rangle$，其中 $K_0 \in \mathcal{K}_P$，但是 $y' \not\sqsubset K_0$，因此这种情况是不可能的。

(4)E. 迹 $tr(p)$ 具有形式 $\langle -K_0, -h, +\{h\}_{K_0}\rangle$。假设 $y' \sqsubset \{h\}_{K_0} \wedge n_2 \not\sqsubset \{h\}_{K_0}$。因为 $y' \neq \{h\}_{K_0}$，故有 $y' \sqsubset h$。但是 $n_2 \not\sqsubset h$，因此这个正结点不会是 S 中的极小元。

(5)D. 迹 $tr(p)$ 具有形式 $\langle -K_0^{-1}, -\{h\}_{K_0}, +h\rangle$，如果它的正结点是 S 中的极小元，则必有 $v_2 \not\sqsubset h$，且 $v_2 \sqsubset \{h\}_{K_0}$。因此由自由加密假设，必有 $h=y'$ 且 $K_0=k_B$。因此，存在一个结点 n(这个串上的第一个结点)，使得 $term(n)=k_B^{-1}$。由假设 $k_B^{-1} \notin \mathcal{K}_P$，并根据丛中的密钥性质，推导出 k_B^{-1} 起源于一个正则结点。但是没有发起者串或响应者串起源于 k_B^{-1}。

(6)S. 迹 $tr(p)$ 具有形式 $\langle -gh, +g, +h\rangle$。假设 $term(n_4)=g$，当 $term(n_4)=h$ 时可以类似地进行证明。因为 $n_4 \in S$，故 $y' \sqsubset g$ 且 $v_2 \not\sqsubset g$。由 n_4 的极小性有 $v_2 \sqsubset gh$。但是，$v_4 \neq gh$，因此 $v_4 \sqsubset h$。

令 $T=\{m \in C: m \prec n_4 \wedge gh \sqsubset term(m)\}$，因为没有正则结点包含子项 gh(其中 h 包含加密子项)，所以 T 中每个元素都是攻击者结点。

因为 $\langle p,1\rangle \in T$，所以 T 是非空集合。由串空间丛的性质，T 中包含一个极小元 m，并且 m 的符号为正。下面说明 m 可能在什么类型的攻击者串上。

(1)T 中的极小元不会在 M, K 型的串上。

(2)S. 若 $gh \sqsubset term(m)$，此处 m 是一个正结点，位于 S. 型攻击者串 p' 上，则有 $gh \sqsubset term(\langle p',1\rangle)$，并且 $\langle p',1\rangle \prec m$，与 m 在 T 中的极小性相矛盾。

(3)E. 若 $gh \sqsubset term(m)$，此处 m 是一个正结点，位于 E. 型攻击者串 p' 上，则有 $gh \sqsubset term(\langle p',2\rangle)$，并且 $\langle p',2\rangle \prec m$，与 m 在 T 中的极小性相矛盾。

(4)D. 若 $gh \sqsubset term(m)$，此处 m 是一个正结点，位于 D. 型攻击者串 p' 上，则有 $gh \sqsubset term(\langle p',2\rangle)$，并且 $\langle p',2\rangle \prec m$，与 m 在 T 中的极小性相矛盾。

(5)C. 若 $gh \sqsubset term(m)$，此处 m 是一个正结点，位于 C. 型攻击者串 p' 上，且 m 是 T 中的极小元，则有 $gh \sqsubset term(m)$，且 p' 的迹具有形式 $\langle -g, -h, +gh\rangle$。因此 $term(\langle p',1\rangle)=term(n_4)$ 并且 $\langle p',1\rangle \prec n_4$，与 n_4 在 S 中的极小性相矛盾。

由以上证明可知，n_4 不可能在攻击者串上，因此 n_4 必然在一个正则串上。

由引理 1，y' 不起源于 n_4，又由串空间丛的性质，因此在串 t 上存在一个 n_4 的前驱结点 n_3，使得 $y' \sqsubset term(n_3)$，即 $n_3 \Rightarrow^+ n_4$，所以 n_3 也是正则结点。

引理 3 响应者 s 成功地认证发起者 t。

证明：由命题 1 假设，C 是 Σ 中的一个丛，$s \in$ Re $sp[m_A, m_B, W_A, W_B, x', X', y']$，且 $C-height(s)=3$，显然 $n_1 \in C$。由于 $k, k_B^{-1} \notin \mathcal{K}_P$，$y'$ 惟一起源于 n_2，边 $n_2 \Rightarrow^+ n_5$ 是 y' 在 $\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}$ 中的出测试。根据认证测试出测中的原理(1)，存在正则结点 $m, m' \in C$，使得 $\{y'\}_{k_B}$ 是 m 的分量，且

$m \Rightarrow^+ m'$是对于y'的变换边。这时结点m只可能是发起者串$t \in Init[m_A, m_B, W_A, W_B, x', X', y']$中的结点$\langle t, 2\rangle$，即结点$n_3$。于是变换边$m \Rightarrow^+ m'$必为$\langle t, 2\rangle \Rightarrow^+ \langle t, 3\rangle$，亦即$n_3 \Rightarrow^+ n_4$，且$C-hight(t)=3$。因此证明了在PJY安全协议中响应者$s$成功地认证了发起者$t$，即响应者串$s$与发起者串$t$之间存在惟一的单射一致性。

由引理2和引理3，立即可以得到命题1。得证。

2.3 机密性：响应者的临时值

在PJY协议中，可以证明响应者的临时值y'在协议中是保密的。

命题2 假设下述条件成立。

(1)Σ是一个PJY串空间，C是Σ中的一个丛，s是串$\mathrm{Re}\, sp[m_A, m_B, W_A, W_B, x', X', y']$中的一个响应者串，且$C-hight(s)=3$；

(2)$k_A^{-1}, k_B^{-1}, k^{-1} \notin \mathcal{K}_P$；

(3)$x' \neq y', X' \neq y'$，且y'在Σ中是惟一起源的项。

于是，对于任意满足$y' \sqsubset term(n)$的结点$n \in C$，有$\{y'\}_{k_B} \sqsubset term(n)$。特别地，$y' \neq term(n)$。

证明：选定任意一个满足命题1中假设的$\Sigma, C, s, m_A, m_B, x', X', y'$，将结点$n_2$的项$\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}$记为$v_2$，结点$n_5$收到值$\{\{y'\}_{k_B}\}_k$，其项记为$v_5$，考察以下集合：

$$S=\{n \in C: y' \sqsubset tem(n) \wedge v_2 \not\sqsubset term(n) \wedge v_5 \not\sqsubset term(n)\}$$

由串空间模型中丛的性质可知，如果S是非空集合，则S中至少存在一个$\preceq$极小元。在下面的引理4中，首先证明S的极小元不是正则结点。然后在引理5中，证明S的极小元也不是攻击者结点，因此S是一个空集，从而命题2得证。

引理4 S的极小元不是正则结点。

证明：假设存在一个极小元$n \in S$是正则结点，由串空间丛的极小元性质，n的符号为正。

(1)因为只有n_2的符号为正，且$n_2 = term(n_2)$，因此n不可能位于串s上。

(2)n也不可能位于响应者串$s' \neq s$上，否则$n=\langle s', 2\rangle$，$term(n)=\{m_C, W_C, \{N\}_{k_d}, \{N'\}_{k_d}\}$。由于$y' \sqsubset term(n)$，因此$y'=N$或者$y'=N'$。

(a)如果$y'=N$，由于有$\langle s', 1\rangle$的项为$\{N, D\}_{k_C} = \{y', D\}_{k_C}$，从而$y' \sqsubset term(\langle s', 1\rangle)$。此外$v_2 \not\sqsubset \{y', D\}_{k_C}$，且$v_5 \not\sqsubset \{y', D\}_{k_C}$，因此$\langle s', 1\rangle \in S$。但是$\langle s', 1\rangle \prec n$，与$n$的极小性相矛盾。

(b)如果$y'=N$且$y'=N'$，则y'起源于n，与y'惟一起源于n_2相矛盾。

(3)再假设n位于一个发起者串s'上，则n或者是s'的第一个结点，或者是它的第三个结点。

(a)如果$n=\langle s', 1\rangle$，由于$y' \sqsubset term(n)$，则y'起源于n，与y'惟一起源于n_2的假设相矛盾。

(b)如果$n=\langle s', 3\rangle$，则$term(n)=\{\{y'\}_{k_B}\}_k$，从而第2个结点$\langle s', 2\rangle$具有形式$\{m_C, W_C, \{y'\}_k, \{x\}_k\}$。因此$C \neq B$，否则有$v_5 = term(n)$。从而$\langle s', 2\rangle \prec n$是$S$中的元素，与$n$的极小性相矛盾。

引理5 S的极小元不是攻击者结点。

证明：本引理的证明与引理2证明有相似之处，惟一区别在于攻击者串为D型时，要考虑3种情况。

(1)v_1由下述明文与密钥构成，即$h=x', y'$且$K_0=k_A$；

(2)v_2由下述明文与密钥构成，即$h=x', y'$且$K_0=k_B$；

(3)v_5由下述明文与密钥构成，即$h=\{y'\}_{k_B}$且$K_0=k$。

因此，需要将自由假设应用于3个密钥k_A^{-1}, k_B^{-1}和k^{-1}，并且假设这两个密钥没有被泄露。其他攻击者情形的证明与引理2相同。

2.4 机密性与一致性：发起者的保证

命题3 假设下列条件成立。

(1)Σ是一个PJY串空间，C是Σ中的一个丛，t是一个串$init[m_A, m_B, W_A, W_B, x', X', y']$中的发起者串，且$C-hight(s)=3$；

(2)$k_A^{-1}, k_B^{-1} \notin \mathcal{K}_P$；

(3)x'在Σ中是惟一起源的。

于是，对于任意满足$x' \sqsubset term(n)$的结点$n \in C$，有$\{m_A, W_A, \{x'\}_{k_A}, X'\} \sqsubset term(n)$成立，或者$\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\} \sqsubset term(n)$成立。特别地，$x' \neq term(n)$。

证明：本命题涉及对发起者临时值x'的机密性证明，与命题2给出的证明类似，此处不赘述。

命题4 假设下述条件成立。

(1)Σ是一个PJY串空间，C是Σ中的一个丛，t是一个串$init[m_A, m_B, W_A, W_B, x', X', y']$中的发起者串，且$C-hight(s)=3$；

(2)$k_A^{-1}, k_B^{-1} \notin \mathcal{K}_P$；

(3)x'在Σ中是惟一起源的。

于是，C中存在一个响应者串$s \in \mathrm{Re}\, sp[m_A, m_B, W_A, W_B, x', X', y']$，且$C-hight(t)=2$。即证明发起者成功地认证响应者。

证明：由于$k_A^{-1}, k_B^{-1} \notin \mathcal{K}_P$，$x'$惟一产生在结点$n_0$，边$n_0 \Rightarrow^+ n_3$是$x'$在$\{m_A, W_A, \{x'\}_{k_A}, X'\}$中的出测试。根据出测试的原理(1)，存在正则结点$m, m' \in C$，使得$\{x'\}_{k_A}$是$m$的分量，且$m \Rightarrow^+ m'$是$x'$的变换边。这时$m$只可能为$\langle t, 1\rangle$，其中$s \in \mathrm{Re}\, sp[m_A, *, W_A, *, x', X', (y')']$。

基于同样理由，边$\langle s', 2\rangle \Rightarrow^+ \langle s', 3\rangle$是$(y')'$在$\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}$中的出测试。根据出测试的原理(2)，$\{m_B, W_B, \{x'\}_{k_A}, \{y'\}_{k_B}\}$是某个负正则结点$m''$的分量。但是$m''$只能是$\langle s', 2\rangle$，其中$s' \in \mathrm{Re}\, sp[*, m_B, *, W_B, x', X', (y')']$，因为只有发起者串的第2个结点收到这种形式的分量。由发起者串的形状可知，x'产生于$\langle s', 1\rangle$。因为x'是惟一产生的，故$\langle s', 1\rangle = \langle s, 1\rangle$，因此$s'=s$，且$(y')'=y'$。于是丛$C$包含响应者串$s \in \mathrm{Re}\, sp[*, m_B, *, W_B, x', X', y']$，$C-hight(s)=2$。由此证明了在PJY安全协议中发起者$t$成功地认证响应者$s$，即发起者串$t$与响应者串$s$之间存在惟一的单射一致性。

结束语 对PJY安全协议采用串空间模型及其认证测试方法，分别从发起者和响应者角度进行了单射一致性和机密性的证明，说明PJY安全协议是安全的。同时PJY协议采用的是基于零知识身份证明的方法，因此认证效率和密钥协商效率也是比较高的[6]，所以PJY身份认证与密钥协商安全协议具有很好的实用价值。

参考文献

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

(下转第180页)

$q_7, N(q_4) \rightarrow q_7\}$

根据定义，秘密项树自动机 A_{sec} 接受的语言集 $L(A_{sec}) = \{N(agt(A)), N(agt(B))\}$。

6.3 逼近求解和验证

对 NSPK 的每一条规则，执行第 4 节逼近算法，完成一系列的重写和知识扩张。例如首先对规则 1 和初始实例化树自动机 A_0 合一，得到一个从 $Pos_X(l)$ 到 Q 的替换 σ，使得 $\sigma(1.1) = q_1, \sigma(2.1) = q_2, \sigma(3) = q_s$，则根据 A_0 中的转移关系 $agt(q_A) \rightarrow q_{agtA}$ 和 $agt(q_B) \rightarrow q_{agtB}$，可知 $goal(q_{agtA}, q_{agtB}, q_s) \rightarrow q_{net}$，即满足可知 $l\sigma \rightarrow_{A_0}^{*} q_{net}$，但 $r\sigma \not\rightarrow_{A_0}^{*} q_{net}$。

对规则右边的项 $r\sigma$ 进行标准化，需要加入一个正规的转移集，对 msg 操作符的非变量替换的位置，定义过逼近函数 γ_1：

$\gamma_1(1) = q_4, \gamma_1(2) = q_5, \gamma_1(3) = q_9, \gamma_1(3.1) = q_8,$

$\gamma_1(3.2) = q_7, \gamma_1(3.1.1) = q_5, \gamma_1(3.2.1) = q_6, \cdots$

加入转移 Δ 如下：

$N(q_4) \rightarrow q_6, cons(q_6, q_4) \rightarrow q_7, pubkey(q_5) \rightarrow q_8,$

$enc(q_7, q_8) \rightarrow q_9, msg(q_4, q_5, q_9) \rightarrow q_{13}$

加入的标识 $initiate$ 加入正规的转移：$ds(q_{agtA}, q_{agtB}) \rightarrow q_{net}$

由于 $\Delta_{i+1} \neq \Delta_i$，树自动机 A_0 扩张为 A_1 且 $r\sigma \rightarrow_{A_1}^{*} q_{net}$。

根据该协议已知的攻击路径，依次应用其所有规则，经过手动推导，该条路径最后得到的树自动机包含如下标识：

$initiate(a, i, Na, s1), initiate(b, a, Nb, s2),$

$finish(a, b, Nb, s1), finish(b, a, Na, s2)$。

根据认证性的形式化描述可知，a 对 b 的存活性无法保证，b 对 a 也只能保证存活性。协议违背了认证性的安全目标，同时违背了秘密性的安全目标。

结束语 定理证明是一种“证明”的形式化分析方法，可以处理无限状态系统的验证问题，是分析安全协议的有效手段，但由于其推理过程复杂，不易于实现自动化推演。本文的主要贡献在于给出语义清晰的协议形式化模型和可自动化的不动点树自动机求解算法，提出秘密性和认证性的形式化描述和验证方法，最后以 NSPK 协议为例进行了验证，以便进一步开展自动化研究工作。在下一步研究中，将以此模型为基础着重研究其自动化分析过程中尚未处理的问题，如如何统一处理特殊运算符的代数属性，如何与模型检测方法结合进一步增强模型对大型实用安全协议（如 IPsec 等）的适用性，以及如何兼容其他类型安全属性等，都有待于进一步深入研究。

参 考 文 献

[1] 冯登国. 第三届安全协议研讨会[C]//北京：信息安全国家重点实验室，2007

[2] Baader F, Nipkow T. Term Rewriting and All that[M]. Cambridge: Cambridge University Press, 1999

[3] Comon H, Dauchet M, Gilleron R, et al. Tree automata and techniques and applications[EB/OL]. http://13ux02.univ-lille3.fr/tata/, 2002

[4] Cousot P, Cousot R. Abstract Interpretation and Application to Logic Programs[J]. The Journal of Logic Programming, 1992, 13: 103-179

[5] Gent T, Klay F. Rewriting for Cryptographic Protocol Verification[J]. Lecture Notes in Computer Science, 2000(1831/2000): 271-290

[6] Ohsaki H, Takai T. Actas: a system design for associative and commutative tree automata theory[A]//Proceedings of the 5th International Workspace on Rule-based Programming: RULE'2004[C]. Aachen: Elsevier, 2005: 97-111

[7] Boichut Y, Heam P C, Kouchnarenko L. Automatic Verification of Security Protocols Using Approximation[R]. INRIA CASSIS Project, RR-5727. 2005

[8] Automated Validation of Internet Security Protocols and Applications (AVISPA)[J/OL]. http://www.avispa-project.org/

[9] 李建新，李先贤，卓怀亮，等. SPA：新的高效安全协议分析系统[J]. 计算机学报，2005，28(3)：309-318

[10] 李梦君，李舟军，陈火旺. SPVT：一个有效的安全协议验证工具[J]. 软件学报，2006，17(4)：898-906

[11] 苏开乐，岳伟亚，陈清亮，等. 实例化空间：一种新的安全协议验证逻辑语义模型[J]. 计算机学报，2006，29(9)：1657-1665

[12] Gilleron R, Tison S. Regular tree languages and rewrite systems [J]. Fundamenta Informaticae, 1995, 24: 157-175

[13] Lowe G. A Hierarchy of Authentication Specifications[A]// Proceedings of the 10th IEEE Workshop on Computer Security Foundations[C]. Washington: IEEE Computer Society Press, 1997: 31-43

[14] Boichut Y. A theoretical limit for safety verification techniques with regular fix-point computations[J]. Information Processing Letters, 2008, 108(1): 1-2

(上接第 121 页)

[2] Guttman J D, Thayer F J. Authentication tests[C]//Proceedings of IEEE Symposium on Security and Privacy. 2000: 96-109

[3] Harn L, Xu Y. Design of generalised ElGamal type digital signature schemes based on discrete logarithm[J]. Electronics Letters, 1994, 30(24): 20-

[4] Thayer F F J, Herzog J C, Guttman J D. Mixed strand spaces [C]//Proceedings of the 12th IEEE Computer Security Foundations Workshop. 1999: 72-82

[5] Guttman J D. Security protocol design via authentication tests [C]//Proceedings of 15th IEEE Computer Security Foundations Workshop. 2002: 92-103

[6] Vadhan S P. An unconditional study of computational zero knowledge[C]//Proceedings of 45th Annual IEEE Symposium on Foundations of Computer Science. 2004: 176-185