面向命题投影时序逻辑的安全协议模型检测

杨琛[1,2]，段振华[1]，王小兵[1,2]
（1. 西安电子科技大学计算理论与技术研究所，710071，西安；
2. 武汉大学软件工程国家重点实验室，430072，武汉）

摘要：针对无条件安全通信协议，特别是Russian Cards协议的安全性验证问题，提出基于命题投影时序逻辑(PPTL)的模型检测方法. 根据协议构造规则建立了Russian Cards协议的ProMeLa模型；利用chop算子将多个交互事件进行顺序复合，以表达协议所期望的通信序列；由projection算子定义了协议在该序列上的安全性质，再将该性质转为Never Claim语法结构并连同协议模型作为模型检测器SPIN的输入，以完成验证工作. 验证结果表明，由协议规则构造的Russian Cards通信协议是安全可靠的，该方法也适用于一般的无条件安全通信协议的验证.

关键词：模型检测；协议验证；时序逻辑；安全协议
中图分类号：TP301 **文献标志码**：A **文章编号**：0253-987X(2010)08-0030-06

Model-Checking Security Protocol with Propositional Projection Temporal Logic

YANG Chen[1,2]，DUAN Zhenhua[1]，WANG Xiaobing[1,2]
（1. Institute of Computing Theory and Technology，Xidian University，Xi′an 710071，China；
2. State Key Laboratory of Software Engineering，Wuhan University，Wuhan 430072，China）

Abstract：A method of model-checking is proposed based on propositional projection temporal logic (PPTL) to verify the security of unconditional security communication protocols，in particular the Russian Cards protocols. The protocol model is built up in ProMeLa language according to the rules of constructing Russian Cards protocol that are given in our previous work. The security properties are defined by PPTL，that is，the chop operator is used to compose interactive events sequentially and to formalize the expected communication sequence，and the projection operator is employed to express the security properties over the sequence. Then the PPTL properties are transformed into Never Claim structures. The verification is done in a widely-used model checker-SPIN with the ProMeLa model and the Never Claim properties as the inputs. Experimental results show that Russian Cards protocols constructed using the protocol rules are safe and reliable. The model-checking method is also applicable in verifying ordinary unconditional security communication protocols.

Keywords：model checking；protocol verification；temporal logic；security protocol

在传统公钥/密钥系统里，通信协议的安全性依赖于两个前提条件：①通信者的计算能力是有限的；②存在因计算能力受限而不易求解的加密方法. 然而，不依赖于这些条件的安全通信技术逐渐成为了

收稿日期：2010-02-01. 作者简介：杨琛(1981—)，男，博士生；段振华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金重大国际合作项目(60910004)；国家自然科学基金资助项目(60873018)；国家重点基础研究发展规划资助项目(2010CB328102)；武汉大学软件工程国家重点实验室开放基金资助项目(SKLSE20080713)；中央高校基本科研业务费专项资金资助项目(JY10000903004).

近些年的研究热点，它们被称为无条件的安全通信协议，具有代表性的是 Russian Cards 通信协议[1]. 作者在前期工作中对该协议做了形式化定义以及扩充[1]，本文采用模型检测方法对其安全性进行了验证. 模型检测是一种形式化的验证方法，它能够验证系统的安全性及活性等性质[2-3]. 模型检测中性质通常采用逻辑描述. 文献[4]中虽然也采用模型检测方法验证 Russian Cards 协议，但是没有给出协议的形式化定义和算法，模型仅描述了各个通信主体简单的行为，性质采用认知逻辑描述，通过在认知逻辑框架内推导通信主体认知的信息来实现验证. 认知逻辑描述的性质不能表现协议的通信序列，推导过程不能反映通信的演化过程，而且支持验证的模型检测器也不通用. 针对这些问题，本文采用命题投影时序逻辑[5-8]描述协议性质，该逻辑支持描述期望通信序列(即活性验证)，同时允许在该序列上定义协议的安全性质(即安全性验证). 通信协议依靠交互事件序列实现，该序列可用 chop 算子表达，而协议的安全性质往往依赖于系统变量值的变化，通常又是交互引起这些变量值的变化，所以安全性质仅需定义在交互事件的序列上即可，该定义可通过 projection 算子实现. 文中模型检测基于 Bell 实验室开发的通用模型检测器 SPIN[2] 来实现. 验证结果表明，作者为 Russian Cards 协议定义的通信序列是安全的.

1　命题投影时序逻辑

语法　设 AP 为命题集合，命题投影时序逻辑(PPTL)的语法定义为

$$P:=p\mid\neg P\mid P_1\wedge P_2\mid\bigcirc P\mid P_1;P_2\mid(P_1,\cdots,P_{m-1})\ \mathrm{prj}\ P_m \qquad (1)$$

式中：$p\in AP$；$P_i(i=1,\cdots,m)$和 P 都是 PPTL 公式；非“¬”和与“∧”为布尔算子；“○”(next)、“;”(chop)和“prj”(projection)为时序算子.

语义　状态 $s\in 2^{AP}$ 定义为一个命题集合，包含在 s 中的命题为真，其余命题为假. 区间 $\sigma=<s_0,\cdots,s_{|\sigma|}>$是一个状态序列，其中$|\sigma|<\infty$表示区间长度，它等于状态数减 1. 此外，$\sigma_1\cdot\sigma_2$ 表示由区间 σ_1 的末状态和 σ_2 的首状态连接而成的新区间. PPTL 的解释是一个三元组 $I=(\sigma,k,j)$，其中 σ 是一个区间，$k\leqslant j\leqslant|\sigma|$为整数，解释 $I=(\sigma,k,j)$满足一个公式 P，记作 $I\vDash P$.

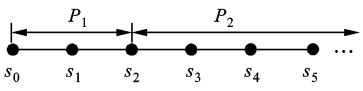
为定义投影算子，需要辅助算子↓. 设$\sigma=<s_0,s_1,\cdots>$是区间，$0\leqslant r_0\leqslant\cdots\leqslant r_h\leqslant|\sigma|$是整数，$\sigma$ 在该整数序列上的投影为$\sigma\downarrow<r_0,\cdots,r_h>=<s_{t0},\cdots,s_{tl}>$，其中 $t_0,\cdots,t_l$ 由删除 $r_0,\cdots,r_h$ 中重复元素所得，如$<s_0,s_1,s_2,>\downarrow<0,0,2,2>=<s_0,s_2>$.

PPTL 的可满足关系⊨定义为：$I\vDash p$ 当且仅当 $p\in s_k$；$I\vDash\neg P$ 当且仅当 $I\mid\neq P$；$I\vDash P_1\wedge P_2$ 当且仅当 $I\vDash P_1$ 并且 $I\vDash P_2$；$I\vDash\bigcirc P$ 当且仅当$(\sigma,k+1,j)\vDash P$；$I\vDash P_1;\ P_2$ 当且仅当存在 $r:k\leqslant r\leqslant j\leqslant|\sigma|$使得$(\sigma,k,r)\vDash P_1$ 并且$(\sigma,r,j)\vDash P_2$；$I\vDash(P_1,\cdots,P_{m-1})$ prj P_m，若存在整数序列 $k=r_0\leqslant\cdots\leqslant r_{m-1}\leqslant j$，使$(\sigma,r_{l-1},r_l)\vDash P_l(1\leqslant l<m)$并且满足$(\sigma',0,|\sigma'|)\vDash P_m$，其中 σ' 为

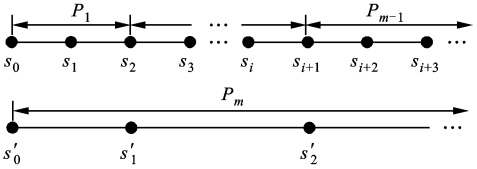
$r_{m-1}<j$ 并且 $\sigma'=\sigma\downarrow(r_0,\cdots,r_{m-1})\cdot\sigma_{(r_{m-1}+1,\cdots,j)}$；

或 $r_{m-1}=j$ 并且 $\sigma'=\sigma\downarrow(r_0,\cdots,r_h)$，其中 $0\leqslant h<m$.

在 PPTL 模型检测中，公式 P 用来表达系统的性质，也就是程序的行为. 从这个角度更容易理解 chop 和 projection 算子. 如图 1 所示，$P_1;P_2$ 表示将 P_1 的区间和 P_2 的区间顺序连接. 直观地讲，chop 算子支持子程序 P_1 和 P_2 的顺序复合. $(P_1,\cdots,P_{m-1})$ prj P_m 从 2 个时间粒度来刻划程序：①细粒度(精化)上程序由子程序 $P_1,\cdots,P_{m-1}$顺序复合而成，即 $P_1;\cdots;P_{m-1}$；②在粗粒度(抽象)上程序的行为可由 P_m 表达，其区间由各个子程序 $P_1,\cdots,P_{m-1}$ 的端点从细粒度上投影下来构成.



(a)$P_1;P_2$



(b)$(P_1,\cdots,P_{m-1})\mathrm{prj}P_m$

图 1　chop 和 projection 算子的语义

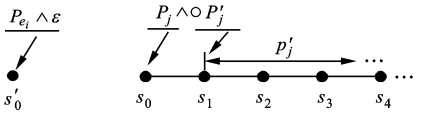
常用的派生公式为：$\varepsilon=\neg\bigcirc\mathrm{true}$，$\Diamond P=\mathrm{true};P$，$\Box P=\neg\Diamond\neg P$. 其中，$\varepsilon$ 表示当前状态是所在区间的末状态；$\Diamond P$(◇意为 eventually)表示 P 在将来某个状态可满足；$\Box P$(□意为 always)表示 P 在每个状态都成立.

定义 1　(正则形)PPTL 公式 P 可转化为正则形

$$P=\bigvee_{i=1}^{l}(P_{e_i}\wedge\varepsilon)\vee\bigvee_{j=1}^{h}(P_j\wedge\bigcirc P'_j) \qquad (2)$$

式中：$h,l\geqslant0$ 且 $h+l\geqslant1$；P'_j 是 PPTL 公式(不要求

是正则形)；P_{e_i} 和 P_j 为 true，或形为合取式 $\dot{p}_1 \wedge \cdots \wedge \dot{p}_m$，其中 $\dot{p}_i$ 代表 p_i 或 $\neg p_i$. 如图 2 所示，正则形在结构上由 terminating 和 future 两部分构成，其中 terminating 部分 $P_{e_i} \wedge \varepsilon$ 表示在由单一状态 s'_0 构成的区间$<s'_0>$上 P_{e_i} 成立，而 future 部分 $P_j \wedge \bigcirc P'_j$ 表示在长度大于 1 的区间中当前状态 s_0 满足 P_j，并且以 s_1 起始的后缀区间$<s_1, s_2, \cdots>$满足 P'_j.



(a)terminating 部分 (b)future 部分

图 2 正则形的结构组成

特别地，若 $\vee_{j=1}^{h} P_j = \text{true}$ 并且 $\vee_{u \neq v}(P_u \wedge P_v) = \text{false}$，则表达式(2)称为完全正则形. 完全正则形用于求解一个 PPTL 公式的否定形式. 假如 P 的完全正则形如表达式(2)，则 $\neg P$ 的正则形为 $\neg P = \vee_{i=1}^{l}(\neg P_{e_i} \wedge \varepsilon) \vee \vee_{j=1}^{h}(P_j \wedge \bigcirc \neg P'_j)$，其证明见文献[7]. 根据模型检测的基本思想，性质 P 需要转化为 $\neg P$，因此完全正则形具有重要作用. 已经证明存在算法可将任意 PPTL 公式转化为正则形[7]. 根据正则形可构造 PPTL 公式的正则图，由正则图可进而得到该 PPTL 公式的 Büchi 自动机，其可接受的语言就是满足该 PPTL 公式的所有区间[8].

定义 2 (正则图)PPTL 公式 P 的正则图是有向图 $G(P)=(V_P, E_P)$，V_P 是结点集合，每个结点是一个 PPTL 公式，E_P 是有向边集合，有向边表示为三元组(v, q, v')，即从结点 v 到结点 v' 有一条标记为 q 的边，其中 q 为 PPTL 公式. 公式 P 的正则图的构造算法可简单描述为

(1)$P \in V_P$；

(2)对于 $V_P - \{\text{false}\}$ 中任意 Q，设其正则形为 $\vee_{i=1}^{l}(Q_{e_i} \wedge \varepsilon) \vee \vee_{j=1}^{h}(Q_j \wedge \bigcirc Q'_j)$，则 $\varepsilon \in V_P$；对于所有 i，存在边$(Q, Q_{e_i}, \varepsilon) \in E_P$；对于所有 j，有 $Q' \in V_P$ 且存在边$(Q, Q_j, Q') \in E_P$.

(3)有限次地应用(1)和(2)生成 P 的正则图.

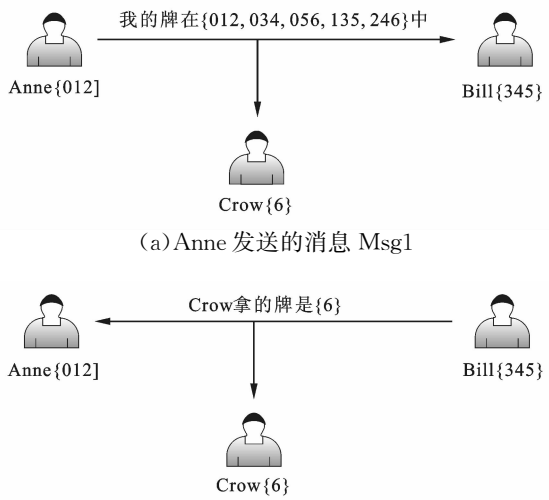
公式 P 的正则图可进而转换化为 Büchi 自动机 $B_P=(V, I, T, L, F)$，其中状态集合 $V=V_P$，起始状态 $I=\{P\}$，迁移集合 $T=E_P$，对每一迁移 $t=(v, q, v') \in E_P$ 有 $L(t)=q$，可接受状态集合 F 包含所有主算子不为 chop 的结点. B_P 的无穷执行序列 $v_0, v_1, \cdots$可接受，当且仅当存在状态 $v \in F$，使得该无穷序列无限次经过状态 v. 该转换的正确性已经得到证明[8].

2 Russian Cards 通信协议

Russian Cards 通信协议最初在 2000 年于莫斯科举办的奥林匹克数学竞赛中提出，其原始表述为："从 7 张牌 0，…，6 中，Anne 和 Bill 各自抽取 3 张牌，剩下的 1 张牌归 Crow 所有. Anne 和 Bill 怎样以广播消息的方式来告知对方自己手里的牌，并且不能让入侵者 Crow 知道他们手里的牌？"

该协议在实际应用中，以所有的牌作为密文编码的基数，通信者将自己所持牌编码为各自的密文，再以广播消息方式交换密文来进行身份认证，从而能够建立安全会话. 可将该协议扩展到 n 个通信者，$n(n-1)+1$个编码基数[1]，从而使得该协议更具实用性. 本文只讨论 3 个通信者 7 个编码基数的协议验证.

为方便起见，将一个集合，例如{0,1,2}简记为 012. 假设 Anne 持有牌 012，Bill 持有 345，Crow 持有 6(牌的分配可记为 012. 345. 6)，一个典型的安全通信序列如图 3 所示. Anne 先将集合{012, 034, 056, 135, 246}发布在公共信道上，表示她的牌在其中，Bill 收到后可根据自己的牌 345 排除集合中 034，056，135，246，从而得知 Anne 拿 012，进而得知 Crow 的牌是 6. 之后 Bill 在公共信道上公布 Crow 拿的牌是 6. Anne 得知 Crow 的牌也就得知 Bill 的牌. 而 Crow 根据自己的牌只能从集合里排除 056，246，只知道 Anne 可能拿 012，034 或者 135，但是不能确定是哪个，因为这 3 种可能包括了除 6 以外的所有的牌，所以 Crow 也不知道 Anne 没有拿哪张牌，同样也不能判断 Bill 拿或没拿什么牌.



(a)Anne 发送的消息 Msg1

(b)Bill 发送的消息 Msg2

图 3 Russian Cards 通信协议的一个安全通信实例

Russian Cards 通信协议的原始表述没有给出安全通信序列的构造规则，为此作者在前期工作中提出了 Anne 公布的集合的构造算法，从而保证 Bill 可根据自己的牌从该集合得知 Anne 的牌，并且 Crow 不能探知任何有关 Anne 和 Bill 所持牌的信息. Anne 公布的集合 $H=\{a_1,a_2,a_3,a_4,a_5\}$ 可改写为矩阵

$$\boldsymbol{B}=\begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix}$$

集合 H 与矩阵 $\boldsymbol{B}$ 的对应关系如图 4 所示. 矩阵 $\boldsymbol{B}$ 的构造算法如图 5 所示. 由该算法就可得到集合 H. 令 h_a、h_b、h_c 分别表示 Anne、Bill 和 Crow 所持牌. 在通信过程中，Bill 通过排除 H 中与 h_b 有交集的元素得 $H_b=\{a_i|a_i\in H$ 且 $h_b\cap a_i=\phi\}$，同理 Crow 得到 $H_c=\{\bigcup a_i|a_i\in H$ 且 $h_c\cap a_i=\phi\}$. 根据协议规则，当

$$|H_b|=1 \tag{3}$$

成立时，Bill 和 Anne 才能得知对方的牌，而当

$$h_c=\{0,1,2,3,4,5,6\}-H_c \tag{4}$$

成立时，Crow 不知道任何有关 Anne 和 Bill 所持牌的信息. 已证明图 5 中的算法使得式(3)和式(4)同时成立[1]，其中式(3)用来判断通信是否有效，式(4)用作判断通信安全的条件. 作者已经用协议元语言(ProMeLa)对该通信协议建模. 模型包括 anne，bill 和 crow 三个通信进程，它们分别代表 Anne，Bill 和 Crow，且以消息方式进行通信. 进程 anne 根据上述算法生成 H 并将其作为第一个消息公布(记为 Msg1). bill 收到 H 后计算得到 H_b. 若式(3)成立，bill 得到 h_b 和 h_c，并将 h_c 作为第二个消息公布(记为 Msg2)，anne 收到该消息便得到 h_b. Crow 试图从这 2 次消息中发现任何有关于 Anne 和 Bill 所持牌的信息.

$a_1=\{b_{1,1},b_{1,2},b_{1,3}\}$　$a_3=\{b_{3,1},b_{3,2},b_{3,3}\}$　$a_5=\{b_{1,3},b_{2,3},b_{3,3}\}$
$a_2=\{b_{2,1},b_{2,2},b_{2,3}\}$　$a_4=\{b_{1,2},b_{2,2},b_{3,2}\}$

图 4　集合 H 与矩阵 $\boldsymbol{B}$ 的对应关系

```
1  input: set M, h //M={0,1,2,3,4,5,6}, h为Anne拿的牌
2  output: matrix B=(b_{i,j})_{3×3};
3  temp variable: integer m;
4  M:=M-h; Let m∈h;
5  h:=h-{m}; //从h中任选一张牌m填充矩阵第一列
6  for i:=1 to 3 {b_{i,1}:=m;}
7  Let m∈h; b_{1,2}:=m; h:=h-{m}; //h中其余牌放在矩阵第一行
8  Let m∈h; b_{1,3}:=m; h:=h-{m};
9  for i:=2 to 3 {
10   for j:=2 to 3 {
11     Let m∈M; b_{i,j}:=m; M:=M-{m};}}
```

图 5　Anne 所公布集合的构造算法

3　Russian Cards 通信协议的模型检测

3.1　协议的性质描述

由上节可知，若式(3)成立则通信协议是有效的. 令命题 a 为真表示 Anne 知道 Bill 的牌，命题 b 为真表示 Bill 知道 Anne 的牌. 由协议规则可知，若通信过程有效则 Bill 先得知 Anne 的牌，而后 Anne 得知 Bill 的牌. 该有效性质可用如下公式表示：

$$Q=\text{true};\ b;\ a \tag{5}$$

若式(4)成立则通信协议是安全的. 为了描述该性质，令命题 r 为真，表示 Crow 不知有关 Anne 和 Bill 所持牌的信息，反之亦然. r 初始为真，当 Anne 先公布消息(即 Msg1)时，Crow 等待截获 Msg1，还不具备计算 H_c 的条件，所以 r 的值此时不发生变化. 在获取 Msg1 之后 Crow 计算 H_c，若计算结果使得式(4)不成立，r 的值就发生变化，即 $\neg r=$true. 这也是 r 的值在整个通信过程中变化的唯一机会. Bill 公布消息(即 Msg2)时，若 r 的值在此之前发生了变化，则此时 $\neg r$ 成立，否则 r 仍为真. 根据上述分析，我们只需关心在每个消息发生时刻 r 的值是否为 true. 令命题 p 和 q 分别表示 Msg1 和 Msg2 发生，该安全性质可用如下公式表示：

$$P=\text{true};\ p;\ (q\ \text{prj}\ r) \tag{6}$$

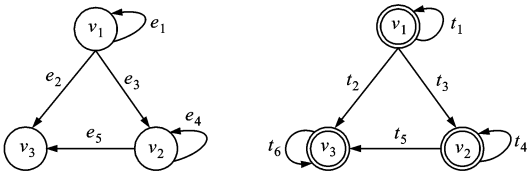
性质(6)既定义了通信消息的顺序，即 p、q 相继发生，又要求在第 2 条消息发生的时刻 r 为真. 由于篇幅限制，这里只验证性质(6)，性质(5)的验证过程与其相似. 在模型检测中，需要首先对性质(6)求非，即 $\neg P$，再将其转为 Büchi 自动机. 利用本文第一节的方法，先计算 $\neg P$ 的正则图，再求 Büchi 自动机. 计算正则图所需的正则形公式如下

$$\neg P=(\neg(p\wedge q\wedge r)\wedge\varepsilon)\vee(\neg p\wedge\bigcirc\neg P)\vee(p\wedge(\neg q\vee\neg r)\wedge\bigcirc\neg(\text{true};\ (q\ \text{prj}\ r))) \tag{7}$$

$$\neg(\text{true};\ (q\ \text{prj}\ r))=(\neg(p\wedge r)\wedge\varepsilon)\vee(\neg(p\wedge r)\wedge\bigcirc\neg(\text{true};\ (q\ \text{prj}\ r))) \tag{8}$$

根据正则形表达式(7)和式(8)，我们得到 $\neg P$ 的正则图，见图 6a. 由正则图，进而得到 $\neg P$ 的 Büchi 自动机，见图 6b，因为自动机中没有主算子为 chop 的结点，所以每个结点都是可接受状态. 此外，在正则图中所有到达 ε 结点的路径实质上是 $\neg P$ 的

有穷模型，而为了在 Büchi 自动机中表达有穷模型，需要在 ε 状态上加入自循环 τ，该技术被称为 τ 扩展[3]，这里 τ 是空迁移，没有任何意义.



(a)正则图 (b)Büchi 自动机

v_1 :¬P
v_2 :¬(true;(q prj r))
v_3 : ε
$e_1(t_1)$:¬p
$e_2(t_2)$:¬p∨¬q∨¬r
$e_3(t_3)$: p∧(¬q∨¬r)
$e_4(t_4)$: ¬q∨¬r
$e_5(t_5)$: ¬q∨¬r
t_6:τ

(c)图(*a*)、(*b*)的状态与边的标注

图 6 性质¬P 的正则图和 Büchi 自动机

3.2 协议的验证

利用 Bell 实验室开发的模型检测器 SPIN 来对 Russian Cards 协议进行验证. SPIN 要求输入以 ProMeLa 描述的模型 M 和用 Never Claim 结构描述的性质¬φ. Never Claim 实际上是对从¬φ 转换来的 Büchi 自动机 $A_{\neg\varphi}$ 的文字描述，其语法可参考文献[3]. 验证 M 是否满足 φ 的工作由检测器自动完成，其原理是将 M 转换为自动机 A_M，再求积自动机 $A_M \times A_{\neg\varphi}$，若其接受的语言为空，则 M 满足 φ，否则该积自动机接受的字就是 M 违反 φ 的执行轨迹，并且检测器会反馈这些轨迹. 作者为 Russian Cards 协议构造的 ProMeLa 模型见文献[9]. 图 6b 中的 Büchi 自动机可转化为图 7 所示的 Never Claim 结构.

在 Russian Cards 协议的 ProMeLa 模型中，Anne 抽到的牌共有 $C_7^3=35$ 种可能，之后 Bill 抽到的牌共有 $C_4^3=4$ 种可能. Anne 发送的集合由其所持牌 h_a 构造. 为证明该模型的正确性，在进程 anne 中植入了一个 bug，使得当 Anne 抽到 016 时可发送集合{023，045，016，126，345}. 注意该集合违反构造规则. 将该模型连同上述的 Never Claim 输入到模型检测器 SPIN 中，得出的验证结果如图 8 所示. 图中 Verification Output 窗口显示检测器发现模型有误(errors:1)，遍历的状态数为 22 838，迁移数为 69 436. Sequence Chart 窗口给出了该错误的

```
1   never{
2   accept_S0:
3   if
4   ::(!p)->goto accept_S0
5   ::(p&&(!q||!r))->goto accept_S1
6   ::(!p||!q||!r)->goto accept_all
7   fi;
8
9   accept_S1:
10  if
11  ::(!q||!r)->goto accept_S1
12  ::(!q||!r)->goto accept_all
13  fi;
14
15  accept_all:
16  skip
17  }
```

图 7 性质¬P 的 Never Claim 结构

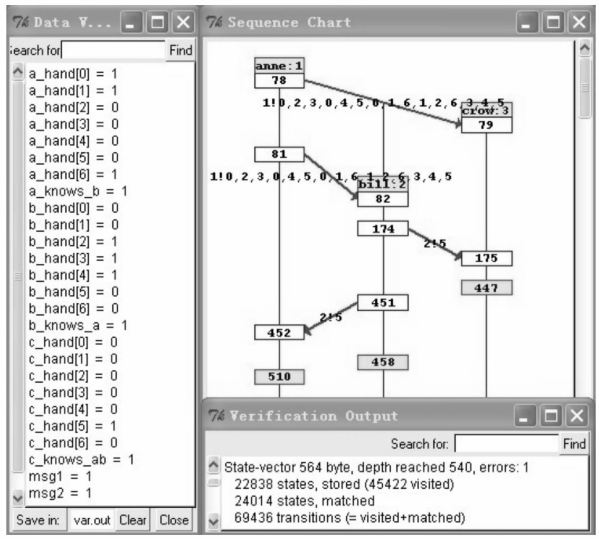


图 8 Russian Cands 协议模型检测结果

执行轨迹. 该轨迹的格式类似于 UML 中的顺序图，包括进程 anne、bill 和 crow，矩形表示系统状态，其中的数字代表状态编号，状态编号自上而下递增，表示系统演化过程. 进程间的交互用箭头表示，图中只显示发生交互的状态. 该轨迹表示 Anne 发送消息{023，045，016，126，345}后，Bill 根据自己的牌 $h_b=\{2,3,4\}$ 排除 023，045，126，345，从而得知 Anne 的牌为 016，而 Crow 由 $h_c=\{5\}$ 排除 045 和 345，得 $H_c=\{0,1,2,3,6\}$. 因为{0,1,2,3,4,5,6}−$H_c=\{4,5\}$ 使得表达式(4)不成立，所以该通信序列不安全(因为 Crow 知道 Anne 没拿 4 这张牌). Sequence Chart 窗口左侧的数据窗口也显示 c_knows_ab = 1，即¬r 成立(3.1 节中 r 定义为 c_knows_ab=0). 再将 bug 从模型中移除，使得 Anne 发送的集合按照图 5 给出的算法构造，重复上

述验证过程，所得结果显示模型正确，因此该协议是安全的. 此外，用与验证性质(6)相同的方法可验证模型也满足性质(5). 因此该协议的通信序列是有效的.

4　结　论

采用基于命题投影时序逻辑(PPTL)的模型检测方法来验证 Russian Cards 无条件安全协议，该模型由已给出的协议构造规则[1]来定义，其性质采用 PPTL 描述，借助该逻辑中的 chop 算子先对通信交互序列进行描述，利用 projection 算子在该交互序列上定义待验证的性质. 最后借助模型检测器 SPIN 进行验证，结果表明由该规则构造的 Russian Cards 协议是安全的. 由于 Russian Cards 协议具有无条件安全通信协议的特点，因此该模型检测方法也适用于一般的无条件安全通信协议的验证.

参考文献：

[1] DUAN Zhenhua, YANG Chen. Unconditional secure communication: a Russian Cards protocol [J]. Journal of Combinatorial Optimization, 2010, 19(4): 501-530.

[2] CLARKE E M, EMERSON E A, SISTLA A P. Automatic verification of finite-state concurrent systems using temporal logic specifications [J]. ACM Transactions on Programming Languages and Systems, 1986, 8(2): 244-263.

[3] HOLZMANN G J. The spin model checker: primer and reference manual [M]. Reading, Mass, USA: Addison-Wesley, 2003.

[4] VAN DITMARSCH H P, VAN DER HOEK W, VANDER MEYDEN R, et al. Model checking Russian Cards [J]. Electronic Notes in Theoretical Computer Science, 2006, 149(2): 105-123.

[5] DUAN Zhenhua. Temporal logic and temporal logic programming [M]. Beijing, China: Science Press of China, 2006.

[6] 王小兵，段振华. 面向投影时序逻辑的 Web 服务模型检测 [J]. 西安交通大学学报，2009, 43(4): 39-44.
WANG Xiaobing, DUAN Zhenhua. Projection temporal logic oriented model checking for web services [J]. Journal of Xi'an Jiaotong University, 2009, 43(4): 39-44.

[7] DUAN Zhenhua, TIAN Cong, ZHANG Li. A decision procedure for propositional projection temporal logic with infinite models [J]. Acta Informatica, 2008, 45(1): 43-78.

[8] TIAN Cong, DUAN Zhenhua. Propositional projection temporal logic, Büchi Automata and Omega-Regular Expressions[C]// Proceedings of TAMC'08. Berlin, Germany: Springer, 2008, 4897: 47-58.

[9] Model of Russian Cards protocol [EB/OL]. [2010-01-01]. http://www.keepandshare.com/doc/view.php?id=1637338&da=y.

(编辑　武红江)