基于博弈论的百万富翁协议

冯云芝 张 恩
(河南师范大学计算机与信息工程学院 新乡 453007)

摘 要 在经典的百万富翁协议中,一方在得到最后的财富比较结果后,没有动机将结果告诉另一方,或者告诉另一方一个错误的结果。结合博弈论和密码算法,提出一种百万富翁协议。在此协议中,参与者背离协议的收益小于遵守协议的收益,遵守协议是参与者的最优策略,任何百万富翁的欺骗行为都能被鉴别和发现,因此理性的参与者有动机发送正确的数据。最后每个参与者都能公平地得到最后的财富比较结果。

关键词 百万富翁问题,博弈论,安全两方计算,公平性
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.027

Millionaires' Protocol Based on Game Theory

FENG Yun-zhi ZHANG En
(College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China)

Abstract In the setting of classical millionaires' problem, one party maybe tell the other party a wrong value, and he has no incentive to tell the true comparative result. Combining game theory and cryptography, this paper proposed a millionaires' protocol. In the protocol, the participant's payoff of following the protocol is more than the payoff of deviation. It is a best strategy for participant to abide by the protocol, and any cheating of Millionaire can be detected. So rational party has an incentive to abide by the protocol. Finally, every party can obtain the comparative result of wealth.

Keywords Millionaires' problem, Game theory, Secure two-party computation, Fairness

1 引言

百万富翁问题首先由图灵奖获得者姚期智教授在文献[1]中提出:两个富翁如何在不泄露自己财富的前提下,能够比较出谁更富有?可以将其形式化表示为:P_1,P_2 分别拥有私有数据 a,b,两方都希望在不暴露各自私有数据 a,b 的前提下,共同计算 $f(a,b)$,如果 $f(a,b)=1$,那么 $a>b$,否则 $a\leqslant b$。他在文献[1]中给出一个解决方案,但方案要求 P_2 在得到结果后,要诚实地告诉 P_1。

随后,百万富翁问题经过一系列文献[2-6]研究,已经成为密码学中一个非常重要的研究方向,即安全多方计算。文献[2]设计了混淆电路,通过对双方的输入进行双重加密,并借助不经意传输工具及输出转换表,给出了一个在半诚实模型下通用的安全两方计算协议。Goldreich 等人[3,4]提出了一个在任意模型下多方通用的、可以计算任意函数的安全多方计算协议。文献[3,4]将多方计算视为一个算法电路,电路分解为加法门与乘法门。只要有这样的电路存在,就可以设计出通用的方法,这样可以一劳永逸地解决所有有关安全多方计算的问题。Goldreich 将安全多方计算中的攻击者分为被动的攻击者(也称为半诚实者,他们诚实地执行协议,但事后会将所得数据与其他的不诚实者分享,用来分析参与者的输入和输出数据)和积极的攻击者(也称为恶意的)。Goldreich[4]首先设计了半诚实模型下安全的协议,之后又设计了相应的编译器,用以将半诚实模型下安全的协议编译成在恶意模型下安全的协议,但只有在诚实参与者占多数的情况下,协议的公平才能保证,在两方协议中,要求两方都是诚实的情况下才能保证协议的公平性。秦静等[5]基于 Φ 隐藏假设以及同态公钥加密的语义安全性假设,设计了一个安全的两方比较协议,但该协议使用了半诚实的茫然第三方参与协助完成计算。文献[6-8]可以发现和鉴别两方计算协议中恶意参与者的行为,但是无法保证协议的公平性。李顺东等[9]利用不经意传输协议与一种单调不减的函数,构造了一种高效的百万富翁协议。李顺东等[10]利用对称加密方案提出了一种百万富翁协议。文献[9,10]中的方案建立在半诚实模型下,目前对百万富翁问题的研究多数建立在半诚实模型下,一是因为半诚实模型研究起来比较简单,二是他们认为半诚实模型下的安全多方协议存在一个通用的方法来将其"编译"为恶意模型下安全的多方协议,但在编译过程中绝对的公平是非常难达到的。为了获得公平性,文献[11,12]各提出一种公平的百万富翁方案,但协议需要有诚实的第三方参与。文献[13-15]对公平的两方协议进行了研究,但以上两方协议,或者只是保证部分的公平,或者只能用在非常简单的场合。他们的协议都没有考虑参与者的收益,即使平时是诚实的参与者,在遇到自身收益非常大的情况下,同样也会选择违背协议。如果仅依靠一个人的诚实而没有用收益来衡量参与者动机,那么该协议是不可靠和危险的。

到稿日期:2013-12-30 返修日期:2014-03-17 本文受国家自然科学基金项目(61170221,U1204606)资助。
冯云芝 女,讲师,主要研究方向为信息安全、计算机网络,E-mail:yunzhif@126.com;张 恩 男,副教授,主要研究方向为信息安全、密码学。

在现实生活中两个富翁财产的比较结果在某些场合是非常重要的，在竞标或商业谈判中，如果仅有一方知道竞争两方的财产比较，那么他将处于优势，所以如果用传统的安全两方协议来实现比较，那么先得到结果的一方，会马上中断协议或者告诉另一方一个错误的结果。本文利用博弈论分析了传统的百万富翁协议，借助博弈论可使协议更加符合现实。已有一些文献借助博弈论来分析和设计密码协议[16-21]，在我们构建的百万富翁计算协议中，没有半诚实模型的要求，理性的参与者发送正确的信息符合自身利益的最大化，如果背离协议，必然会损害自身利益，因此参与者会自觉遵守协议，最终两个富翁能公平地得到财产比较结果。

2 相关定义

定义 1(多项式时间不可区分) 以自然数为指标集的两个总体 $X \overset{def}{=} \{X_n\}_{n\in N}$ 和 $Y \overset{def}{=} \{Y_n\}_{n\in N}$，如果对于每一个概率多项式时间算法 D、每一个正多项式 $p(\cdot)$ 及所有充分大的 n，都有

$$|\Pr[D(X_n,1^n)=1]-\Pr[D(Y_n,1^n)=1]|<\frac{1}{p(n)} \quad (1)$$

则称这两个总体是在多项式时间内不可区分的。

定义 2(纳什均衡) 在博弈 $\Gamma=(\{A_i\}_{i=1}^n,\{u_i\}_{i=1}^n)$ 中，策略组合 $a=(a_1,\cdots,a_n)\in A$ 是一个纳什均衡，如果任一博弈方 i 的策略都是对其余博弈方策略的最佳对策，则博弈保持

$$u_i(a_i',a_{-i})\leqslant u_i(a) \quad (2)$$

因为纳什均衡具有一致预测的特性，所以每个博弈方都可以预测某个结果，也可以预测对手会预测它，还可以预测对手会预测自己会预测它……，通过预测来了解每个博弈方的策略及博弈的结果。

定义 3(动态博弈[22]) 动态博弈是指在博弈过程中，参与者选择策略有先后顺序，后行动者在行动前能看到先行动者的行动。

动态博弈包括 6 个要素：(1)参与者为理性秘密共享协议博弈过程中决策主体，在本文中记为 P_i；(2)参与者的行动顺序；(3)轮到 P_i 行动时，可供他选择的策略集；(4)轮到 P_i 行动时，他所理解的信息，P_i 所有的信息集的集合为 H_i，某一特定的信息集为 $h_i^k\in H_i$，$k\in K$，K 为 P_i 信息集个数；(5)博弈结束后，每个参与者的收益函数用 $u_i(a)$ 表示；(6)外生事件(自然，记为 N)可能出现的状态及概率分布。

定义 4(子博弈[22]) 由一个动态博弈第一阶段以外的某阶段开始的后续博弈阶段构成的、有初始信息集和进行博弈所需要的全部信息并能成为一个博弈的原博弈的一部分，称为原动态博弈的一个子博弈。

为了能够排除均衡策略中的不可信的承诺或者威胁，需要了解子博弈完美纳什均衡。

定义 5(子博弈精炼纳什均衡) 如果在完美信息动态博弈中，各参与者的策略构成的一个策略组合满足：在整个动态博弈及它的所有子博弈中都构成纳什均衡，那么这个策略组合称为该动态博弈的一个“子博弈完美纳什均衡”。

子博弈完美纳什均衡分析核心方法是逆向归纳法：逆向归纳法是从博弈的最后阶段开始进行分析，并确定参与者的选择，然后，再确定上一个阶段参与者的选择。当后一阶段参与者的选择确定后，前一阶段参与者的选择也就容易确定了。

3 百万富翁问题的经典解决方案

百万富翁问题经典解决方案[1]描述如下：假设 Alice 的秘密输入为 a，Bob 的秘密输入为 b，满足 $1\leqslant a<b\leqslant n$。令 M 是所有 N bit 非负整数的集合，Q_N 是所有从 M 到 M 的一一映射函数的集合。令 E_A 是 Alice 的公钥，它是从 Q_N 中随机抽取的。具体描述如下：输入：Alice 有一个秘密输入 a，Bob 有一个秘密输入 b。输出：Alice 和 Bob 得到 a 和 b 的大小关系。

(1)Bob 随机选取一个 N bit 整数 x，秘密计算 $E_A(x)$ 的值，并把该值记为 k；

(2)Bob 将 $k-b+1$ 发给 Alice；

(3)Alice 秘密计算 $y_u=D_A(k-b+u)$ 的值($u=1,2,\cdots,n$)；

(4)Alice 产生一个 $N/2$bit 的随机素数 p，对所有 u 计算 $z_u=y_u \pmod p$。如果所有的 z_u 在模 p 运算下至少相差 2，则停止，否则重新产生一个随机素数 p 重复上面的步骤，直到所有的 z_u 至少相差 2。用 $p,z_u(u=1,2,\cdots,n)$ 表示最终产生的这些数；

(5)Alice 将素数 p 以及下面的 n 个数 $z_1,z_2,\cdots,z_a,z_{a+1}+1,\cdots,z_n+1$ 都发给 Bob；

(6)Bob 检验由 Alice 传送过来的不包括 p 在内的第 b 个值，若它等于 $x \bmod p$，则 $a\geqslant b$，否则 $a<b$；

(7)Bob 把结论告诉 Alice。

对该方案的分析如下：

(1)正确性分析

上述协议能够使 Alice 和 Bob 正确判断出 a 和 b 的大小关系，因为

$$z_u=D_A[E_A(x)-b+u] \bmod p$$

特别地，有

$$\begin{aligned} z_b &= D_A[E_A(x)-b+b] \bmod p \\ &= D_A[E_A(x)] \bmod p = x \bmod p \end{aligned}$$

如果 $a\geqslant b$，则第 b 个值为 $z_b=x \bmod p$，否则为 $z_b+1=x \bmod p+1\neq x \bmod p$。所以，通过检验由 Alice 传送来的不包括 p 在内的第 b 个值，可判断 a 和 b 的大小。

(2)安全性分析

协议能保证 Alice 和 Bob 都不能得到有关对方财富的更多的信息。首先，除了当 Bob 告诉 Alice 最后的结论后，Alice 能够推测出 b 的范围以外，Alice 将不会了解 Bob 财富的任何信息，因为她从 Bob 那里仅仅得到了一个值 $k-b+1$，由于 k 的存在，使 Alice 不能从中得知 b。其次，Bob 知道 y_b(即 x)的值，因此他也知道 z_b 的值，然而他不知道其他 z_u 的值，而且通过观察 Alice 发送给他的数列，他也无法辨认出哪个是 z_u 哪个是 z_u+1。这一点是由两两 z_u 至少相差 2 保证的。

(3)不足之处

在协议最后一步，Bob 可能欺骗 Alice，使 Alice 得出一个错误的结论。

由于“子博弈完美纳什均衡”能消除策略中不可信的承诺或威胁，因此在动态博弈中也是稳定的均衡。如果用“子博弈完美纳什均衡”来分析以上方案，第 1 阶段 P_1 会选择不发送数据给 P_2，第 2 阶段 P_2 在得到结果后不会发送给 P_1。这是该动态博弈的唯一的子博弈完美纳什均衡，也是该博弈真正稳定的均衡。

4 基于博弈论的百万富翁协议

针对以上问题，本文将博弈论引入百万富翁问题，在本节设计的百万富翁计算协议中，理性的参与者发送正确的信息符合自身利益的最大化，如果背离协议，必然会损害自身利益，从而使得两个百万富翁在执行协议时，没有欺骗的动机，最终两个富翁都能得到财产比较结果。下面给出了具体的理性百万富翁计算协议，协议没有假设半诚实模型，也就是说，任何参与者为了自身利益的最大化，可以发送错误的输入，在得到结果后，也可以随时中断协议。具体计算步骤如下：

第1步　双方运行安全两方计算，每一方都可以随时中断协议。

输入：令 x 和 y 是 P_1，P_2 私有的输入（如果任意一方收到中断符$\perp$，则其也输出中断符$\perp$）。

1.1）从有限域 F_q 中选取一系列元素 $l_1,l_2,\cdots,l_k$，这些元素满足 $l_1<l_2<\cdots<l_k$，k 的值取决于参与者的效益（在定理1中讨论）。选取一个 l 值满足 $l_1<l_2<\cdots<l_k<l$，且满足如果 $f(x,y)=1$，则 l 尾部一位为1，如果 $f(x,y)=0$，则 l 尾部一位为0。随机选取 d^*，如果 $1\leqslant d^*<k$，则用 l 置换 l_{d^*}。如果 $d^*=k$，随机从 $l_{k-1}-l_1,l_{k-1}-l_2,\cdots,l_{k-1}-l_{k-2},l$ 中选取一个元素 l_*，然后用 l_* 置换 l_{d^*}。这样形成 k 个元素 $a_1,a_2,\cdots,a_k$；

1.2）选择 a_i^1,a_i^2 使其满足 $a_i^1\oplus a_i^2=a_i$，这里 $1\leqslant i\leqslant k$；

1.3）随机选择 $s_i^1,s_i^2,b_i^1,b_i^2\in F_q$，$b_i^1,b_i^2\neq 0$，令 $c_i^2=s_i^1+b_i^2\cdot a_i^1\in F_q$，$c_i^1=s_i^2+b_i^1\cdot a_i^2\in F_q(1\leqslant i\leqslant k)$。

①P_1 得到 $a_i^1,s_i^1,c_i^1,b_i^1\in F_q(1\leqslant i\leqslant k)$；

②P_2 得到 $a_i^2,s_i^2,c_i^2,b_i^2\in F_q(1\leqslant i\leqslant k)$。

第2步　在第 i 轮，$i=1,2,\cdots,k-1$，参与双方做以下工作：

2.1）P_2 先发给 P_1 子份额，过程如下：

①P_2 发送 (a_i^2,s_i^2) 给 P_1；

②P_1 收到 (a_i^2,s_i^2) 后，检验 c_i^1 和 $s_i^2+b_i^1\cdot a_i^2$ 是否相等，如果不相等，则说明 P_2 有欺骗行为，P_1 得到 $s=a_{i-1}$，如果 $s=a_0$，则中断协议执行，否则根据 a_{i-1} 尾部一位输出1或者0；如果相等，P_1 得到他的一个输出为 $a_i^1\oplus a_i^2=a_i$。如果重构出的 $a_i<a_{i-1}$，那么 P_1 知道上一轮重构的 a_{i-1} 等于 l，根据 l 尾部一位输出1或者0，并中断协议执行，否则协议继续。

2.2）P_1 发给 P_2 子份额，过程如下：

①P_1 发送 (a_i^1,s_i^1) 给 P_2；

②P_2 收到 (a_i^1,s_i^1) 后，检验 c_i^2 和 $s_i^1+b_i^2\cdot a_i^1$ 是否相等，如果不相等，则说明 P_1 有欺骗行为，P_2 得到 $l=a_{i-1}$，根据 l 尾部一位输出1或者0，并中断协议执行；如果相等，P_2 得到他的一个输出为 $a_i^1\oplus a_i^2=a_i$。如果重构出的 $a_i<a_{i-1}$，那么 P_2 知道上一轮重构的 a_{i-1} 等于 l，根据 l 尾部一位输出1或者0，这时 P_1 已经得到结果，所以 P_2 中断协议的执行，否则协议进行到下一轮。

第3步　如果 $i=k$ 轮，参与双方做以下工作：P_1，P_2 同时发送他们的子份额 (a_k^1,s_k^1)，(a_k^2,s_k^2)，P_1 收到 (a_i^2,s_i^2) 后，检验 c_i^1 和 $s_i^2+b_i^1\cdot a_i^2$ 是否相等，如果不等，说明 P_2 有欺骗行为，P_1 得到 $l=a_{i-1}$，根据 l 尾部一位输出1或者0，并中断协议执行；如果相等，P_1 得到他的输出为 $a_m^1\oplus a_m^2=a_m$。P_2 收到 (a_i^1,s_i^1) 后，检验 c_i^2 和 $s_i^1+b_i^2\cdot a_i^1$ 是否相等，如果不等，则说明 P_1 有欺骗行为，P_2 得到 $l=a_{i-1}$，根据 l 尾部一位输出1或者0，并中断协议执行；如果相等，则 P_2 得到他的输出为 $a_k^1\oplus a_k^2=a_k$。如果 $a_k>a_{k-1}$，那么 P_1，P_2 知道 $a_k=l$，根据 l 尾部一位输出1或者0，如果 $a_k<a_{k-1}$，协议重启。

定理1　方案在满足式(9)的条件下，两个百万富翁没有偏离协议的动机，最终每个人都能公平地得到财富比较结果。

证明：参与者 P_1，P_2 不知道当前轮是 l 所在轮，还是其他的测试轮。如果参与者 P_i 在参与协议前想了解 l，他只能通过猜测，猜对的概率为 ξ，P_i 获得的效益为 U_i^+。猜错的概率为 $1-\xi$，P_i 获得的效益为 U_i^-。所以 P_i 的期望收益为：

$$E(U_i^{guess})=\xi*U_i^+ + (1-\xi)*U_i^- \tag{3}$$

如果 P_i 参与协议时，恰好在 l 所在轮进行攻击的概率为 ω，那么合谋者 P_i 获得的效益为 U_i^+，否则合谋者 P_i 获得的效益为 $E(U_i^{guess})$。因此 P_i 的期望收益至多为：

$$\omega*U_i^+ +(1-\omega)*E(U_i^{guess}) \tag{4}$$

如果参与者 P_i 遵守协议，其获得的效益为 U_i，那么当满足式(5)时，P_i 将没有偏离协议的动机。

$$U_i>\omega*U_i^+ +(1-\omega)*E(U_i^{guess}) \tag{5}$$

我们的协议满足式(6)和式(7)。

$$\xi=q^{-1} \tag{6}$$

$$\omega=k^{-1} \tag{7}$$

由式(5)－式(7)得：

$$U_i>k^{-1}*U_i^+ +(1-k^{-1})*(q^{-1}*U_i^+ +(1-q^{-1})*U_i^-) \tag{8}$$

$$\Rightarrow k>\frac{U_i^+-(q^{-1}*U_i^+ +(1-q^{-1})*U_i^-)}{U_i-(q^{-1}*U_i^+ +(1-q^{-1})*U_i^-)} \tag{9}$$

即当满足式(9)时，P_i 不能通过背离协议来获得更大的收益。最终每个参与者能公平地得到最后的财富比较结果。

结束语　结合博弈论，对传统的百万富翁协议进行了分析，发现传统的百万富翁协议是不公平和不稳定的，参与者执行协议的收益小于没有背离协议的收益，所以理性的参与者没有执行协议的动机。本文构建了百万富翁协议的博弈模型，设计了具有博弈性质的百万富翁协议，使得理性的参与者执行协议符合自身利益最大化，从而有动机诚实地执行协议，最终双方能够公平、正确地得到计算结果。

参 考 文 献

[1] Yao A. Protocols for secure computations[C]// Proc 23th IEEE Symposium on Foundations of Computer Science (FOCS'82). Los Alamitors, CA: IEEE Computer Society, 1982: 160-164

[2] Yao A. How to generate and exchange secrets[C]// Proc 27th IEEE Symposium on Foundations of Computer Science (FOCS'86). Los Alamitors, CA: IEEE Computer Society, 1986: 162-167

[3] Goldreich O, Micali S, Wigderson A. How to play any mental game[C]// Proc of the 19th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1987: 218-229

[4] Goldreich O. Foundations of cryptography-Volume 2, Basic Applications[M]. Cambridge: Cambridge University Press, 2004: 599-759

[5] 秦静，张振峰，冯登国，等. 无信息泄露的比较协议[J]. 软件学报，2004，15(3)：421-427

[6] Lindell Y. Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries[C]// Advances in Cryptology-Crypto,

LNCS 8043. Berlin:Springer,2013:1-17

[7] Yan Huang,Katz J,Evans D. Efficient Secure Two-Party Computation Using Symmetric Cut-and-Choose[C]// Advances in Cryptology-Crypto,LNCS 8043. Berlin:Springer,2013:18-35

[8] 孙茂华,罗守山,辛阳,等. 安全两方线段求交协议及其在保护隐私凸包交集中的应用[J]. 通信学报,2013,34(1):30-42

[9] 李顺东,戴一奇,游启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报,2005,33(5):769-773

[10] Li Shun-dong,Wang Dao-shun,Dai Yi-qi,et al. Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations[J]. Information Sciences,2008,178(1):244-255

[11] Cachin C. Efficient private bidding and anctions with an oblivious third party[C]// 6th ACM Conference on Computer and Communications Security. Singapore,1999:120-127

[12] Li Rong-hua, Wu Chuan-kun, Zhang Yu-qing. A fair and efficient protocol for the millionaires' problem[J]. Chinese Journal of Electronics,2009,18(2):249-254

[13] Gordon S D,Hazay C,Katz J,et al. Complete fairness in secure two-party computation[C]//40th ACM Synmposium on Theory of Computing (STOC). New York:ACM Press,2008:413-422

[14] Pinkas B. Fair secure two-party computation[C]// In Advances in Cryptology-Eurocrypt 2003, LNCS 2656. Berlin: Springer, 2003:87-105

[15] Garay J,MacKenzie P,Prabhakaran M,et al. Resource Fairness and Composability of Cryptographic Protocols[C]// Proc of the 3rd Theory of Cryptography Conference (TCC), LNCS 3876. Berlin:Springer,2006:404-428

[16] Halpern J, Teague V. Rational Secret Sharing and Multiparty Computation[C]// Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC). New York: ACM Press,2004:623-632

[17] 张恩,蔡永泉. 基于双线性对的可验证的理性秘密共享方案[J]. 电子学报,2012,40(5):1050-1054

[18] Zhang E, Cai Y Q. Rational Multi-Secret Sharing Scheme in Standard Point-to-Point Communication Networks[J]. International Journal of Foundations of Computer Science,2013,24(6):879-897

[19] Zhang E,Cai Y Q. Collusion-free Rational Secure Sum Protocol [J]. Chinese Journal of Electronics,2013,22(3):563-566

[20] Zhang Z F,Liu M L. Rational secret sharing as extensive games [J]. Science China Information Sciences,2013,56(3):1-13

[21] Tian Y L,Ma J F,et al. Fair (t,n) threshold secret sharing scheme[J]. IET Information Security,2013,7(2):106-112

[22] 谢识予. 经济博弈论(第二版)[M]. 上海:复旦大学出版社,2002:138-158

(上接第 117 页)

表 2 单个安全属性平均验证时间

系统运行数	平均验证时间
2	0.003s
3	0.016s
4	0.07s
5	0.27s
6	1.20s
7	4.90s

结束语 本文描述的协议自动化验证方法,能够用于多协议环境下协议安全性验证。验证算法思想来源于 Athena 算法,在分析攻击者存在情况下消息的多种构造途径的基础上,提出了消息构造的逆向搜索方法,用以准确地找到攻击者对协议的攻击路径。通过改进消减规则和采用新的方法处理攻击者知识推导,算法具有良好的运行效率,能够实现多协议攻击的自动化验证。下一步工作是引入其它状态削减规则,进一步提高算法效率,并检测更多的多协议攻击。

参 考 文 献

[1] Burrows M,Abadi M,Needham R. A logic of authentication[J]. Mathematical and Physical Sciences,1989,426(1871):233-271

[2] Vigano L. Automated Security Protocol Analysis With the AVISPA Tool[J]. Electronic Notes in Theoretical Computer Science,2006,155:61-86

[3] Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of computer security,1998,6(1):85-128

[4] Fábrega 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

[5] Bella G. What is correctness of security protocols? [J]. Journal of Universal Computer Science,2008,14(12):2083-2106

[6] Khoury P,Hacid M,Sinha S K,et al. A Study on recent trends on integration of security mechanisms[M]//Ras Z W,Dardzinska A. Advances in Data Management. Berlin: Springer-Verlag, 2009:203-224

[7] Mathuria A,Singh A R,Sharavan P V,et al. Some new multiprotocol attacks[C]// Proc of the 15th Int Conf on Advanced Computing and Communications. Washington: IEEE Computer Society Press,2007:465-471

[8] Genge B,Haller P. A Syntactic Approach for Identifying Multi-Protocol Attacks[C]// Ultra Modern Telecommunications and Workshops. Washington:IEEE Computer Society Press,2009:1-5

[9] 杨元原,马文平,刘维博,等. 有效的多协议攻击自动化检测系统[J]. 重庆大学学报,2012,35(2):71-77

[10] Song D,Perrig A,Berezin S. Athena:a novel approach to efficient automatic security protocol analysis[J]. Journal of Computer Security,2001,9(1):47-74

[11] Song D. An Automatic Approach for Building Secure Systems [D]. Berkeley:University of California at Berkeley,2002

[12] Lowe G. A hierarchy of authentication specifications[C]// Proc of The 10th Computer Security Foundations Workshop. Washington:IEEE Computer Society Press,1997:31-43

[13] Security protocols open repository[EB/OL]. 2012-02-11[2013-11-17]. http://www.lsv.ens-cachan.fr/Software/spore/table.html