doi:10.3969/j.issn.1000-436x.2012.z1.033

Otway-Rees 协议改进及形式化证明

鲁来凤[1]，段新东[2]，马建峰[3]
（1. 陕西师范大学 数学与信息科学学院，陕西 西安 710062；2. 南阳理工学院 软件学院，河南 南阳 473004；
3. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071）

摘 要：选取认证密钥分配协议 Otway-Rees 协议作为研究对象，利用协议组合逻辑（PCL）作为协议证明工具，对安全协议形式化分析及证明进行了研究。首先给出了 Otway-Rees 协议常见的攻击形式，分析了存在的缺陷，提出了改进方案（AOR 协议）；然后，为了更好地形式化描述 AOR 协议，对传统的 PCL 进行一定的扩展；紧接着，用扩展后的 PCL 对改进的协议中各个实体的行为和协议的安全属性进行形式化描述，将改进后的协议进行模块化划分，并利用 PCL 进行组合证明；最后，得出改进后的 AOR 协议具有密钥保密属性。

关键词：安全协议；形式化方法；协议组合逻辑；Otway-Rees 协议
中图分类号：TP393.09 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0250-05

Improvement and formal proof on protocol Otway-Rees

LU Lai-feng[1], DUAN Xin-dong[2], MA Jian-feng[3]
(1. College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062,China;
2. School of Software Nan Yang Institute of Technology, Nanyang 430074, China;
3. Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071,China)

Abstract: Choosing the authentication key distribution protocol Otway-Rees as the research object, using protocol composition logic (PCL) as proof tool, the security protocol analysis and formal proof was studied. Firstly, this paper gave the forms of security attack, analyzed the Otway-Rees defects and put forward the amended protocol (named as AOR protocol). Then, PCL was extended. And then PCL was used to describe and prove the behavior of each entity and the safety of the protocol attribute formally. Finally, the conclusion was given that the amended AOR protocol has the security attribute of key confidentiality.

Key words: security protocol; formal methods; protocol composition logic; protocol Otway-Rees

1 引言

安全协议的安全性分析一直是一个复杂而困难的问题，对安全协议的研究已成为世界上信息与网络安全方面的一个重要研究方向[1,2]。实践证明，形式化方法是安全协议安全性分析更为可靠和有效的途径[3]。

Otway-Rees 认证协议[4]是由 Dave Otway 和 Owen Rees 提出的基于共享密钥的认证密钥分配协议，其目标是完成发起者和响应者之间的双向认证，并且分发服务器产生的会话密钥。该协议的特点是简单实用，

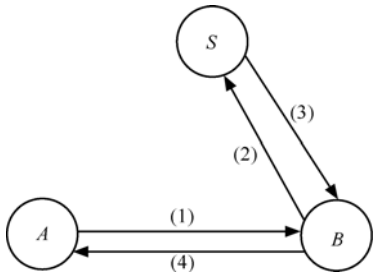
收稿日期：2012-07-05
基金项目：国家自然科学基金资助项目（61173190）；陕西省自然科学基金资助项目（2009JM8002, 2012JQ8023）；中央高校基本科研业务费基金资助项目（GK200902051, GK201002041, GK201002037）
Foundation Items: The National Natural Science Foundation of China (61173190); The Natural Science Foundation of Shaanxi Province (2009JM8002, 2012JQ8023); The Fundamental Research Funds for the Central Universities (GK200902051, GK201002041, GK201002037)

没有使用复杂的同步时钟机制或双重加密，仅用少量的信息提供了良好的时效性。但该协议并不安全，存在缺陷，易受到攻击。因此有必要对它改进并进行形式化的安全性证明，而协议组合逻辑(PCL)[5~9]就是一种新的针对协议安全性证明的有力工具。

PCL 是由美国斯坦福大学信息安全实验室的 Datta 博士等人 2003 年提出来的，是一种新的 Floyd-Hoare 类型的组合逻辑推导系统。它采用标准逻辑概念，使用 Cords 演算描述协议，可以用来证明安全协议的认证性和私密性等安全属性，通过逻辑公理和模块化推理方法支持复杂安全协议的组合推理（包括并行组合和顺序组合）。PCL 形式化系统由协议建模工具、协议逻辑和证明系统 3 部分构成。其中，协议模型化是使用基于“线索（Cords）”概念的协议编程语言形式化描述协议本身及其执行的过程（区别于非形式化的箭头—信息表示法）；协议逻辑用来描述协议的安全属性（主要包括认证性和保密性），包括逻辑语法（Syntax，描述安全属性本身）和逻辑语义（Semantics，描述安全属性的含义）；证明系统包含了用于形式化证明的若干公理和推理规则以及不同形式的协议安全性证明方法。

2　Otway-Rees 协议及改进

Otway-Rees[4]认证协议采用的是基于可信第三方的通信机制，参加协议的主体有 3 个：包括通信双方 A、B，还有认证服务器 S。该协议交互过程如图 1 所示。



(1) $A \to B: M, A, B, \{N_a, M, A, B\}_{K_{as}}$

(2) $B \to S: M, A, B, \{N_a, M, A, B\}_{K_{as}}, \{N_b, M, A, B\}_{K_{bs}}$

(3) $S \to B: M, \{N_a, K_{ab}\}_{K_{as}}, \{N_b, K_{ab}\}_{K_{bs}}$

(4) $B \to A: M, \{N_a, K_{ab}\}_{K_{as}}$

图 1　Otway-Rees 认证协议

其中，A、B 表示协议的参与方；T 表示协议攻击者；S 表示认证服务器；N_a、N_b 分别是 A、B 随机取定的值，用来保证 A、B 收到的消息是 S 最近发出的，而不是一个重放的消息；M 是 A 随机取定的值，帮助 A 识别它和 S 间的通信是由 B 转发的；K_{as}、K_{bs} 是 S 分别与 A、B 共享的密钥；K_{ab} 由 S 生成，作为 A 和 B 之间通信的会话密钥。

由协议描述可得，（M，A，B）在通信过程中都是公开的。攻击者 T 首先截获从 B 发给服务器 S 的消息，去掉明文消息（A，B）后，冒充 S 重发消息，由于消息位数的特殊性，使 A，B 误认（M，A，B）是会话密钥，这样攻击者成功地进行了攻击，今后可以用会话密钥（M，A，B）窃听 A 和 B 之间的会话。

类似地，攻击者 T 还可以冒充 B，重放消息（1）中的加密分量，将它作为消息（4）中的加密分量发送给 A。这里针对 Otway-Rees 协议的攻击就是一个典型的类型缺陷攻击，攻击之所以能成功是因为协议的描述对于协议中出现的变量没有提供足够的明确的类型信息，消息相关的名字不是很明确，协议实现时的消息格式过于对称。

另外，该协议还有一个缺陷，就是在消息（4）中，A 收到了 B 发来的消息，通过解密获得了 S 分发的会话密钥 K_{ab}，但它并不能确定 B 是否也已经获得了同样的会话密钥。

鉴于以上的协议攻击形式及缺陷分析，对协议改进如下（amended Otway-Rees，记为 AOR 协议）：

1) $A \to B: M, A, B, \{N_a, M, A, B\}_{K_{as}}$;

2) $B \to S: M, A, B, \{N_a, M, A, B\}_{K_{as}}, \{N_b, M, A, B\}_{K_{bs}}$;

3) $S \to B: M, \{A, N_a, N_b, K_{ab}\}_{K_{as}}, \{B, N_b, K_{ab}\}_{K_{bs}}$;

4) $B \to A: M, \{A, N_a, N_b, K_{ab}\}_{K_{as}}, \{N_b\}_{K_{ab}}$。

第一是在 3）、4）消息中增加身份信息，使得消息身份信息明确，同时能够避免因消息结构固定、对称而引起的攻击；第二是在 3）、4）消息第一个加密项中添加 N_b 同时在消息 4）中增加消息分量 $\{N_b\}_{Kab}$，使得 A 能够确定它所收到的会话密钥是否与 B 收到的一致。

3　改进型的 Otway-Rees 协议建模

为了更好地形式化描述改进型的 Otway-Rees 协议，需要对传统的 PCL 进行一定的扩展。在此基础上，可以进行协议建模工作。协议的建模工作又分为协议本身的形式化和协议安全属性的形式化描述。

3.1　PCL 扩展

1) 扩展 1

基本的 PCL 语法系统是针对公钥密码体制。本

文为了更好地描述基于对称密码体制的 Otway-Rees 协议，扩展了对称加解密语法如下。

K 表示加密密钥，$\bar{K}$ 表示解密密钥。在公钥密码体制中，两者并不相同；而在私钥（对称）密码体制中，$K=\bar{K}$。

$\{t\}_{\bar{K}}$ 在公钥密码系统中表示用 $\bar{K}$ 对消息项 t 签名，而在对称密码体制中，表示利用 $\bar{K}$ 对消息项 t 解密。

定义对称加解密的动作 *sec_sk* 和 *dec_sk*。具体含义为：(*sec_sk* u，K)表示对称密码系统中用密钥 K 加密 u，(*dec_sk* u，$\bar{K}$)表示对称系统中用 $\bar{K}$ 对 u 进行解密，由于对称密码体制中 $K=\bar{K}$，有时加解密密钥均使用 K。

2) 扩展 2

扩展定义协议项的减法动作“−”：$t-t_1$ 代表从组合项 t 中剔除子项 t_1，若项 t 中不包含子项 t_1，则该操作无意义，直接返回 t。例如令 $t=(t_1, t_2)$即 t 是由不相同的项 t_1 与 t_2 拼接起来的项，则此时 $t-t_1$ 的结果为 t_2。

3.2 协议本身建模

采用 PCL 描述上述改进型协议 AOR 实体执行协议模型，有协议交互方 A，B 和服务器 S 3 个角色，它们的执行过程分别如下。

$AOR\_A=(\hat{Y}, K_{as})$

$[new\ M;\ \ new\ N_a;$

$t_1 := enc\_sk\{N_a, M, \hat{X}, \hat{Y}\}, K_{as}\ ;$

$send\ \hat{X}, \hat{Y}, \{M, \hat{X}, \hat{Y}, t_1\};$

$\cdots;$

$receive\ \hat{Y}, \hat{X}, \{m, u_1, u_2\}\ ;$

$t_2 := dec\_sk\{u_1\}, K_{as};\ K_{ab} := t_2 - \{A, N_a, N_b\};$

$t_3 := dec\_sk\{u_2\}, K_{ab};\ \ match\ t_3/N_b;$

$]<K_{ab}\ >;$

$AOR\_B=(\hat{X}, \hat{Z}, K_{bs})$

$[receive\ \hat{X}, \hat{Y}, \{M, A, B, u_3\};$

$new\ N_b;\ \ t_4 := enc\_sk\{N_b, M, \hat{X}, \hat{Y}\}, K_{bs};$

$send\ \hat{Y}, \hat{Z}, \{M, A, B, u_3, t_4\};$

$receive\ \hat{Z}, \hat{Y}, \{M, u_4, u_5\};$

$t_5 := dec\_sk\{u_5\}, k_{bs};\ \ K_{ab} := t_5 - (B, N_b);$

$t_6 := enc\_sk\{N_b\}, K_{ab}$

$send\ \hat{Y}, \hat{X}, \{M, u_4, t_6\};$

$]<K_{ab}\ >;$

$AOR\_S=(\hat{Y}, K_{as}, K_{bs})$

$[receive\ \hat{Y}, \hat{Z}, M, A, B, u_6, u_7;$

$t_7 := dec\_sk\{u_6\}, K_{as};$

$t_8 := dec\_sk\{u_7\}, K_{bs};$

$t_9 := t_7 - \{M, A, B\};$

$t_{10} := t_8 - \{M, A, B\};$

$new\ K_{ab};\ \ t_{11} := enc\_sk\{A, t_9, t_{10}, K_{ab}\}, K_{as};$

$t_{12} :=\ enc\_sk\{B, t_9, K_{ab}\}, K_{bs};$

$send\ \hat{Z}, \hat{Y}, \{M, t_{11}, t_{12}\};$

$]<>$。

3.3 安全属性建模

Otway-Rees 协议主要功能是完成发起者和响应者之间的双向认证，并且分发服务器产生的会话密钥。会话密钥的保密性是基本的要求，本文主要讨论该安全属性。

定义 1　改进型 Otway-Rees 协议（简写成 AOR 协议）的密钥保密性。

当公式 $\phi_{\text{AOR-Sec}}$ 成立时，Otway-Rees 协议能够保证密钥保密性。其中，

$$\phi_{\text{AOR-Sec}} = Honest(\hat{A}) \wedge Honest(\hat{B}) \wedge Honest(\hat{S}) \wedge Has(Z, K_{ab}) \supset (Z=\hat{A} \vee Z=\hat{B} \vee Z=\hat{S})$$

4 改进型的 Otway-Rees 协议证明

首先，将协议进行划分。改进型 Otway-Rees 协议记为 Q，它包含 3 个主体，分别为通信主体 A、B 和服务器 S，将协议 Q 划分为 3 个子协议模块 Q_1、Q_2 和 Q_3，其中，Q_1 包含消息 1），Q_2 包含消息 2）和 3），Q_3 包含消息 4）。

下面将对各个子协议模块及组合协议进行证明。

4.1 子模块 *Q*1 证明

引理 1　$\Phi[Q_1]_A\psi_1$成立，其中，

$$\Phi = Has(\mathrm{A}, \mathrm{K}_{as}) \wedge Has(B, K_{bs}) \wedge Has(\mathrm{S}, \mathrm{K}_{as}) \wedge Has(S, K_{bs}), \psi_1 = Has(B, M) \wedge Has(B, \{N_a, M, A, B\}_{Kas})$$

证明　引理 1 描述的是以角色 A 的形式执行协议 Q_1 的情形，详细的证明过程如图 2 所示。

AAl	$[new\ M]_A New(A,M)$	(1)
(1), *ORIG*	$Has(A,M)$	(2)
AAl	$[new\ N_a]_A New(A,N_a)$	(3)
(3), *ORIG*	$Has(A,N_a)$	(4)
REC	$\Diamond \mathrm{Re}ceive(B,(M,A,B,\{N_a,M,A,B\}_{K_{as}}))$	(5)
(5), *PROJ*	$Has(B,M)$	(6)
(5), *PROJ*	$Has(B,\{N_a,M,A,B\}_{K_{as}})$	(7)
(6),(7)	$Has(B,M)\wedge Has(B,\{N_a,M,A,B\}_{K_{as}})$	(8)

图 2　引理 1 的证明过程

从图 2 中式（8）能够得出引理 3 成立。

若以角色 *B* 的形式执行协议 Q_1，类似的结论显然成立。所以有定理 1 成立。

定理 1　$\Phi[Q_1]\psi_1$成立，其中，

$\Phi = Has(\mathrm{A},\mathrm{K}_{as})\wedge Has(B,K_{bs})\wedge Has(\mathrm{S},\mathrm{K}_{as})\wedge Has(S,K_{bs}),\psi_1 = Has(B,M)\wedge Has(B,\{N_a,M,A,B\}_{Kas})$

4.2　子模块 *Q*2 证明

引理 2　$\psi_1[Q_2]_S\psi_2$成立，其中，

$\psi_1 = Has(B,M)\wedge Has(B,\{N_a,M,A,B\}_{Kas}),$

$\psi_2 = Honest(\hat{B})\wedge Honest(\hat{S})\wedge Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})$

证明　若按照角色 *S* 来执行协议 Q_2，引理 2 成立，详细证明过程如图 3 所示。

AAl	$[new\ N_b]_B New(B,N_b)$	(9)
(9), *ORIG*	$Has(B,N_b)$	(10)
AAl	$[new\ K_{ab}]_S New(S,K_{ab})$	(11)
(11), *ORIG*	$Has(S,K_{ab})$	(12)
(11), *AN*3	$[new\ K_{ab}]_S Fresh(S,K_{ab})$	(13)
(12), *P*1	$Has(S,K_{ab})[Q_2]Has(S,K_{ab})$	(14)
REC	$\Diamond \mathrm{Re}ceive(B,(M,\{A,N_a,N_b,K_{ab}\}_{K_{as}},\{B,N_b,K_{ab}\}_{K_{bs}}))\supset(Has(B,(M,\{A,N_a,N_b,K_{ab}\}_{K_{as}},\{B,N_b,K_{ab}\}_{K_{bs}})$	(15)
(15), *PROJ*	$Has(B,\{A,N_a,N_b,K_{ab}\}_{K_{as}})$	(16)
(15), *PROJ*	$Has(B,\{B,N_b,K_{ab}\}_{K_{bs}})$	(17)
(17), Ψ_1, *DEC*	$Has(B,\{B,N_b,K_{ab}\}_{K_{bs}})\wedge Has(B,K_{bs})\supset Has(B,(B,N_b,K_{ab}))$	(18)
(18), *PROJ*	$Has(B,K_{ab})$	(19)
(12)(19)	$Has(S,K_{ab})\wedge Has(B,K_{ab})$	(20)
SEC, ϕ	$Honest(\hat{B})\wedge Honest(\hat{S})\wedge\Diamond dec\_sk(Z,\{B,N_b,K_{ab}\}_{K_{bs}})\supset Z=B\vee Z=S$	(21)
(20)(21)	$Honest(\hat{B})\wedge Honest(\hat{S})\wedge Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})\wedge Has(Z,K_{ab})\supset Z=B\vee Z=S$	(22)

图 3　引理 2 的证明过程

若按角色 *B* 的方式执行协议 Q_2 有类似的结论成立。所以有定理 2 成立。

定理 2　$\psi_1[Q_2]\psi_2$成立，其中，

$\psi_1 = Has(B,M)\wedge Has(B,\{N_a,M,A,B\}_{Kas},$

$\psi_2 = Honest(\hat{B})\wedge Honest(\hat{S})\wedge Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})$

4.3　子模块 *Q*3 证明

引理 3　$\psi_2[Q_3]_B\psi$成立，其中，

$\psi_2 = Honest(\hat{B})\wedge Honest(\hat{S})\wedge, Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})$

$\psi = Honest(\hat{A})\wedge Honest(\hat{B})\wedge Honest(\hat{S})\wedge Has(\hat{A},K_{ab})\wedge Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})\wedge Has(Z,K_{ab})\supset Z=A\vee Z=B\vee Z=S$

证明　若按照角色 *B* 来执行协议 Q_3，引理 3 成立，详细证明过程如图 4 所示。

REC	$\Diamond \mathrm{Re}ceive(A,(M,\{A,N_a,N_b,K_{ab}\}_{K_{as}},\{N_b\}_{K_{ab}}))\supset(Has(A,(M,\{A,N_a,N_b,K_{ab}\}_{K_{as}},\{N_b\}_{K_{ab}}))$	(23)
(23), *PROJ*	$Has(A,\{A,N_a,N_b,K_{ab}\}_{K_{as}})$	(24)
(24), *DEC*	$Has(A,\{A,N_a,N_b,K_{ab}\}_{K_{as}})\wedge Has(A,K_{as})\supset Has(A,(A,N_a,N_b,K_{ab}))$	(25)
(25), *PROJ*	$Has(A,K_{ab})$	(26)
(18), *SEC*, Φ	$Honest(\hat{A})\wedge Honest(\hat{B})\wedge Honest(\hat{S})\wedge\Diamond dec\_sk(Z,\{A,N_a,N_b,K_{ab}\}_{K_{as}})\supset Z=A\vee Z=S$	(27)
Ψ_2,(26),(27)	$Honest(\hat{A})\wedge Honest(\hat{B})\wedge Honest(\hat{S})\wedge Has(\hat{A},K_{ab})\wedge Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})\wedge Has(Z,K_{ab})\supset Z=A\vee Z=B\vee Z=S$	(28)

图 4　引理 3 的证明过程

若按角色 *A* 的方式执行协议 Q_3，有类似的结论成立。所以有定理 3 成立。

定理 3　$\psi_2[Q_3]\psi$成立，其中，

$\psi_2 = Honest(\hat{B})\wedge Honest(\hat{S})\wedge, Has(\hat{B}K_{ab})\wedge Has(\hat{S},K_{ab})$

$\psi = Honest(\hat{A})\wedge Honest(\hat{B})\wedge Honest(\hat{S})\wedge Has(\hat{A},K_{ab})\wedge Has(\hat{B},K_{ab})\wedge Has(\hat{S},K_{ab})\wedge Has(Z,K_{ab})\supset Z=A\vee Z=B\vee Z=S$

4.4　协议组合证明

由定理 1、定理 2 和定理 3 可知，$\Phi[Q_1]\psi_1$,

$\psi_1[Q_2]\psi_2, \psi_2[Q_3]\psi$ 成立，其中，$\Phi = Has(A, K_{as}) \wedge Has(B, K_{bs}) \wedge Has(\mathrm{S}, \mathrm{K}_{as}) \wedge Has(S, K_{bs})$，$\psi_1 = Has(B, M) \wedge Has(B, \{N_a, M, A, B\}_{Kas})$，

$\psi_2 = Honest(\hat{B}) \wedge Honest(\hat{S}) \wedge Has(\hat{B}, K_{ab}) \wedge Has(\hat{S}, K_{ab})$，

$\psi = Honest(\hat{A}) \wedge Honest(\hat{B}) \wedge Honest(\hat{S}) \wedge Has(\hat{A}, K_{ab}) \wedge Has(\hat{B}, K_{ab}) \wedge Has(\hat{S}, K_{ab}) \wedge Has(Z, K_{ab}) \supset Z = A \vee Z = B \vee Z = S$

根据模态顺序组合规则 $S1$[9]，由定理 1、定理 2，有公式 $\Phi[Q_1Q_2]\psi_2$ 成立。由该公式和定理 3，再次应用模态顺序组合规则 S1，可得如下公式：$\Phi[Q_1Q_3Q_3]\psi$，其中，

$S1$ 为 $\dfrac{\phi_1[P]_A\phi_2 \quad \phi_2[P']_A\phi_3}{\phi_1[PP']_A\phi_3}$

$\Phi = Has(\mathrm{A}, \mathrm{K}_{as}) \wedge Has(B, K_{bs}) \wedge Has(\mathrm{S}, \mathrm{K}_{as}) \wedge Has(S, K_{bs})$,

$\psi = Honest(\hat{A}) \wedge Honest(\hat{B}) \wedge Honest(\hat{S}) \wedge Has(\hat{A}, K_{ab}) \wedge Has(\hat{B}, K_{ab}) \wedge Has(\hat{S}, K_{ab}) \wedge Has(Z, K_{ab}) \supset Z = A \vee Z = B \vee Z = S$

即改进型的 Otway-Rees 协议满足密钥的保密属性。

5　结束语

安全协议是现代网络系统安全性的基石，安全协议安全性分析是一项紧迫且意义重大的工作。自 BAN 逻辑[10]被提出以来，用形式化的方法分析安全协议的安全性已成为信息安全研究的热点之一[3]。

本文选取认证密钥分配协议 Otway-Rees 协议作为研究对象，利用协议组合逻辑作为协议证明工具展开研究。给出了 Otway-Rees 协议常见的攻击形式，分析了存在的缺陷，提出了改进方案（AOR 协议）；为了更好地形式化描述 AOR 协议，对传统的 PCL 进行了扩展；紧接着，用扩展后的 PCL 对改进的协议中各个实体的行为和协议的安全属性进行形式化描述，将改进后的协议进行模块化划分，并利用 PCL 进行组合证明。最后，得出是改进后的 AOR 协议具有密钥保密属性。

参考文献：

[1] 范红,冯登国.安全协议理论与方法[M].北京:科学出版社, 2003.
FAN H, FENG D G. Theories and Methods for Security Protocols[M]. Beijing: Science Press, 2003.

[2] 卿斯汉.安全协议 20 年研究进展[J].软件学报.2003,14(10):1740- 1752.
QING S H. Twenty years development of security protocols research[J]. Journal of Software. 2003, 14(10): 1740-1752.

[3] 李建华,张爱新,薛质等.网络安全协议的形式化分析与验证[M].北京:机械工业出版社.2010.
LI J H, ZHANG A X, XUE Z, *et al.* Formal Analysis and Verification of Network Security Protocols[M]. Beijing: China Machine Press.2010.

[4] OTWAY D, REES O. Efficient and timely mutual authentication[J].Operating Systems Review, 1987, 21(1):8-10.

[5] DATTA A. Security Analysis of Network Protocol: Compositional Reasoning and Complexity Theoretic Foundations[D]. Computer Science Department, Stanford University, September 2005.8-72.

[6] DATTA A, DEREK A, MITCHELL J, *et al.* Secure protocol composition[A]. Proceedings of the 2003 ACM workshop on Formal methods in security engineering[C]. 2003. 11-23.

[7] DURGIN N, MITCHELL J, PAVLOVIC D. A compositional logic for proving security properties of protocols[J]. Journal of Computer Security, 2003, 11(4): 677-721.

[8] ROY A, DATTA A, DEREK A, *et al.* Secrecy analysis in protocol composition logic[A]. Advances in Computer Science-ASIAN. 2006. Secure Software and Related Issues[C].2006. 197-213.

[9] DATTA A, ROY A, MITCHELL J C, *et al.* Protocol composition logic(PCL)[J]. Electronic Notes in Theoretical Computer Science, 2007,172(1): 311-358.

[10] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

作者简介：

鲁来凤（1979-），女，安徽桐城人，博士，陕西师范大学讲师，主要研究方向为无线网络安全。

段新东（1974-），男，河南南阳人，博士，南阳理工学院讲师，主要研究方向为密码学和存储网络安全。

马建峰（1963-），男，陕西西安人，西安电子科技大学计算机学院院长、教授、博士生导师，主要研究方向为密码学和无线网络安全等。