认证邮件协议的安全性分析与改进

高悦翔[1,2]，彭代渊[1]，闫丽丽[1,3]

(1. 西南交通大学信息安全与国家计算网格实验室 成都 610031;
2. 四川师范大学计算机科学学院 成都 610068; 3. 成都信息工程学院网络工程学院 成都 610225)

【摘要】认证邮件协议需要满足保密性、公平性、可追究性等安全属性。针对一个典型的认证邮件协议在保密性、可追究性上存在的安全缺陷，对其进行了改进，提出了一个基于离线半可信第三方的认证邮件协议。同时，为更有效地分析协议的安全属性，对如何在组合协议分析框架下应用Kailar逻辑分析公平交换协议安全属性的方法进行了研究。利用该方法分析了改进后的协议，并证明了该协议具有满足保密性、可追究性等安全属性的特点。

关 键 词 认证邮件协议; 组合协议分析; Kailar逻辑; 可追究性
中图分类号 TP309 文献标志码 A doi:10.3969/j.issn.1001-0548.2013.02.023

Analysis and Improvement of a Certified E-Mail Protocol

GAO Yue-xiang[1,2], PENG Dai-yuan[1], and YAN Li-li[1,3]

(1. Information Security and National Computing Grid Laboratory, Southwest Jiaotong University Chengdu 610031;
2. College of Computer Science, SiChuan Normal University Chengdu 610068;
3. Department of Network Engineering, Chengdu University of Information Technology Chengdu 610225)

Abstract The security attributes of certified e-mail protocol include confidentiality, non-repudiation, fairness. Aiming at to remedy the lack of confidentiality and non-repudiation of the a typical certified mail protocol, an improved certified mail protocol with transparent semi-trusted third party is proposed. To improve the protocol efficiency, a method applying Kailar logic in compositional analysis is proposed for analyzing the improved protocol. The analysis results indicate the improved protocol can meet confidentiality and non-repudiation.

Key words certified e-mail protocol; compositional analysis; Kailar logic; non-repudiation

认证邮件协议是一种典型的电子商务协议，是保证电子商务活动正常开展的基础，这类协议需满足保密性、可追究性、公平性、时效性等安全属性。目前，国内外学者在这一领域做了大量的研究工作[1-6]。但这类协议的安全属性一直都难以真正得到保证，如文献[1]提出的CMP1协议在信道不可靠的条件下是非公平的；文献[2]提出的协议不满足可追究性；文献[3]提出的协议不满足公平性。文献[6]提出了一种基于签密方案的认证邮件协议，其开销比加密和签名分开的方案更小，但该协议同样存在不满足保密性和可追究性的缺陷。如何设计及验证这类协议一直以来都成为研究的热点及难点。

目前多采用形式化分析方法对这类协议的安全属性进行分析。在众多形式化分析方法中，文献[7]提出了一种新的逻辑分析方法(Kailar逻辑)，扩展了信念逻辑的分析范围，可以用于分析电子商务协议的可追究性。文献[8]对Kailar逻辑的缺陷进行了改进，可以同时分析电子商务协议的可追究性与公平性。文献[9]在Kailar逻辑的基础上对协议主体的拥有集合给出了形式化定义，将协议的初始状态假设细粒度化，避免因非形式化的初始假设而产生的分析错误。但文献[9]的工作集中于分析基于在线第三方的协议，而对于离线第三方的协议分析能力不足。文献[10-12]提出了一种称为组合协议分析(compositional analysis)的安全协议形式化验证方法。该方法在组合协议分析的框架中采用了PCL逻辑对协议安全属性进行分析，但该逻辑对于公平性及不可否认性等属性的分析能力不够。文献[13]对组合协议分析进行了扩展，提出了IF断言，首次将组合协议分析的方法用于电子合同签订协议的形式化

收稿日期：2011－08－04; 修回日期：2012－12－03
基金项目：四川省教育厅重点项目基金(10ZA009)
作者简介：高悦翔(1975－)，男，博士生，主要从事信息安全、形式化分析方面的研究.

分析中，但该方法只能分析协议的弱公平性。

1　对一个认证邮件协议的分析

1.1　协议流程简介

文献[6]提出了一个基于签密的认证邮件协议，该协议由Exchange协议和Resolve协议构成。

1) Exchange协议：

E1：$A \to B: h(m), E_{\mathrm{sk}_a}(h(m))$

E2：$B \to A: c, r, s, h(\mathrm{receipt}_b), \mathrm{Cert}_{tb}, E_{\mathrm{sk}_b}(h(m))$

E3：$A \to B: m$

E4：$B \to A: \mathrm{receipt}_b$

2) Resolve协议：

R1：$A \to \mathrm{TTP}: \mathrm{Cert}_{tb}, E_{\mathrm{sk}_b}(h(m), m)$

R2：$\mathrm{TTP} \to A: \mathrm{receipt}_b$

R3：$\mathrm{TTP} \to B: m$

协议执行流程可分为两种情况，如图1所示。正常情况下，协议执行完Exchange协议正常结束，若协议执行出现异常，由*A*发起Resolve协议。协议的符号表示以及详细说明请详见文献[6]。

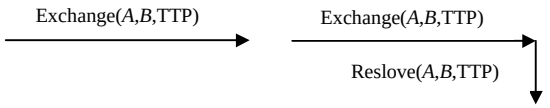

图1　协议的执行过程

1.2　协议所存在的安全隐患

对文献[6]的执行流程及交换数据项进行分析，可以看出该协议存在以下3个缺陷：

1) 文献[6]指出，在Resolve协议的验证过程中“TTP通过*B*的RSA公钥来验证信息*m*和E1中*B*收到的信息是否一致”，通过这一描述可以看出在Resolve协议中，*A*发送给TTP的消息*m*是经过*B*签名的，*A*无法自己生成。但是在协议的前期执行过程中，*A*无法在任何步骤获得 $E_{\mathrm{sk}_b}(h(m), m)$，因此在协议出现异常时，*A*无法发起Resolve协议。

2) 在一些特定的电子商务或电子政务环境下，除了邮件预期的接收者能读取其中的内容，其他的任何主体包括可信第三方都不能读取邮件内容。协议中，执行R1时，*A*直接将签名的*m*发送给TTP，此时TTP验证签名后即可获得*m*的内容，即*m*对于TTP是不保密的，因此该协议对于这一类特殊要求的应用环境是不满足的。同样的，在E3中，*m*明文传输，在信道不可靠的情况下，*m*的保密性不能满足。

3) TTP只需从 Cert_{tb} 中即可恢复收据$\mathrm{receipt}_b$[6]。若不诚实的参与方*A*在Exchange协议中不执行E3，直接发送消息 $\mathrm{Cert}_{tb}, E_{\mathrm{sk}_b}(h(m'), m')$ 给TTP，其中，Cert_{tb} 是在E2中正常获得，$E_{\mathrm{sk}_b}(h(m'), m')$ 是*A*重放曾经和*B*通信所获的信息，按照协议流程，此时TTP通过 Cert_{tb} 恢复收据$\mathrm{receipt}_b$发送给*A*，将 m' 替代正确的*m*发送给*B*。此时*A*获得了*B*关于*m*的收据，而*B*实际上并没有获得*m*。在该情况下，协议对参与方*B*而言是不满足可追究性以及公平性的。

2　改进的认证邮件协议

在分析文献[6]缺陷的基础上，采用文献[6]设计的签密算法，本文提出了一个改进的基于离线半可信第三方(STTP)的认证邮件协议。该协议的目标是在一个不可靠的信道下完成认证邮件的传输，协议需要满足保密性、可追究性以及公平性，即除了邮件的发送者和预期的接收者之外，任何主体包括可信第三方均不能获知邮件的内容。

本文协议由Exchange和Resolve两个子协议构成，仍沿用文献[6]中的符号。

1) Exchange子协议：

E1：$A \to B: h(E_{K_b}(m)), E_{\mathrm{sk}_a}(h(E_{K_b}(m)), E_{K_{\mathrm{sttp}}}(E_{K_b}(m)))$

E2：$B \to A: c, r, s, h(\mathrm{receipt}_b), E_{\mathrm{sk}_b}(\mathrm{Cert}_{tb}, E_{K_{\mathrm{sttp}}}(E_{K_b}(m)), h(E_{K_b}(m)))$

E3：$A \to B: E_{\mathrm{sk}_a}(h(E_{K_b}(m)), E_{K_b}(m))$

E4：$B \to A: \mathrm{receipt}_b$

2) Resolve子协议：

R1：$A \to \mathrm{STTP}: E_{\mathrm{sk}_b}(\mathrm{Cert}_{tb}, E_{K_b}(E_{K_b}(m)), h(m)))$

R2：$\mathrm{STTP} \to A: E_{\mathrm{SK}_{\mathrm{sttp}}}(\mathrm{receipt}_b)$

R3：$\mathrm{STTP} \to B: E_{\mathrm{SK}_{\mathrm{sttp}}}(E_{K_b}(m))$

Exchange子协议中的E1要求*A*发送已签名的 $E_{K_{\mathrm{sttp}}}(E_{K_b}(m))$，防止在文献[6]中存在的*A*发送与*h*(*m*)不匹配的*m*给*B*带来的不满足可追究性的缺陷。

Resolve子协议中，*A*发送给STTP的所有消息在Exchange子协议中的E2阶段均可收到，避免了文献[6]中*A*在异常时无法发起Resolve子协议的缺陷。

整个协议过程中，*m*均用*B*的密钥加密，保证协议执行过程中*m*的保密性。

3　改进后协议的安全性分析

以下采用Kailar逻辑对改进后的协议进行安全性分析。如前所述，由于Kailar逻辑在分析基于离线第三方的协议上存在能力不足的缺点，因此首先探讨如何在组合协议分析的框架下利用Kailar逻辑进

行形式化分析。

3.1 组合协议分析框架简介

文献[10-12]提出了一种组合协议分析的安全协议形式化验证方法，该方法把协议P通过Composition、Refinement及Transformation等操作划分为若干子协议P_1，P_2，…，P_n，分别验证子协议的安全属性，再利用并行组合或串行组合合成验证协议P，从而达到验证整个协议的安全属性的目的。

该方法采用PCL逻辑验证协议的安全属性，该逻辑不同于一般的“信念”逻辑，它提出认证属性是协议动作之间的时间匹配关系，通过逻辑公理和模块化推理方法分析组合协议的安全性。其中使用线束(cord)动态描述参与协议各方的行为结构，线束构成了一个协议的执行流程。协议被看作是由诸如发起方、响应方、第三方等一系列的角色执行一系列的动作构成。PCL逻辑的断言基于协议执行时一系列迹(trace)，在协议的任意会话中进行推理而不显式进行攻击者的分析和推导，可以为协议的正确性证明提供基础。

文献[10-12]利用该方法分析了IEEE 802.11i和TLS协议的认证性和保密性。但PCL逻辑不适合于分析具有公平性、可追究性等特殊安全属性的电子商务协议，因为证明这类属性需要向第三方证明一个主体对某个公式负有责任，而不单只是描述协议动作之间的时间匹配关系。

由于基于离线第三方的电子商务协议往往由几个子协议构成，只需要考虑如何利用组合协议分析中的并行合成或串行合成来合成协议即可。由于这类协议的执行或通过交换子协议执行结束，或通过执行异常处理子协议结束，因此在协议的执行过程中，具有了串行合成的特征。文献[13]利用串行合成及PCL逻辑分析了ASW协议。

3.2 协议的串行合成

文献[9-11]中给出了关于线束串行和协议串行合成的定义。

定义 1 线束的串行合成。给定两线束：$r=(x_0\ x_1\cdots x_{l-1})[R]_x(u_0\ u_1\cdots u_{m-1})$，$s=(y_0\ y_1\cdots y_{m-1})[R]_x\ (t_0\ t_1\cdots t_{n-1})$，它们的串行合成定义为：

$$r;s=(x_0\ x_1\cdots x_{l-1})[RS']_x(t'_0\ t'_1\cdots t'_{n-1})$$

其中，S'和t'_i分别是替代S和t_i的一个实例，在该替代中，每个变量y_k被置换为u_k，RS'是R和S中的动作通过串联所形成的串。

定义 2 串行合成。若一个协议Q中的每一个角色都可以通过Q_1、Q_2中的线束顺序合成而获得，那么称协议Q是Q_1、Q_2的串行合成。

定理 1 对于一组假设Γ_1和Γ_2，线束P和Q，公式ϕ、θ、ψ而言，如果$\Gamma_1\vdash\phi[P]_x\theta$且$\Gamma_2\vdash\theta[Q]_x\psi$，那么有$\Gamma_1\cup\Gamma_2\vdash\theta[P;Q]_x\psi$成立。

其中，$P;Q$是线束P和Q的串行合成。公式$\Gamma_1\vdash\phi[P]_x\theta$成立的含义是：在一组假设前提$\Gamma$下，若$\phi$在$x$执行了协议$P$之前满足，那么执行协议$P$后$\theta$也满足。定理1的证明过程参见文献[10]。

3.3 分析方法及过程

Kailar逻辑侧重于向第三方证明另一个主体对某个公式负有责任，不能有效反映协议执行流程的状况，而PCL逻辑中的线束概念能有效地描述协议动作之间的时间匹配关系，本文首先将线束引入到Kailar逻辑的分析中，通过分析线束的安全属性能否得到满足，再利用线束的串行合成判断整个协议的安全属性是否能够满足。其分析方法如下：

对于任意一个离线第三方电子商务协议，假定其安全性目标为ψ，子协议分别为P和Q。在一组假设前提Γ_1和Γ_2的基础上，可以分别对于P和Q考察是否满足$\Gamma_1\vdash\phi[P]_x\theta$及$\Gamma_2\vdash\theta[P]_x\psi$，由定理1可知，若协议是线束$P$和$Q$的串行合成。则有$\Gamma_1\cup\Gamma_2\vdash\theta[P;Q]_x\psi$成立。

因此，若要考察协议的安全目标ψ是否能得到满足，可采用以下步骤：

1) 分析协议的执行流程，找出协议执行的线束；2) 列举协议要达到的安全性目标；3) 利用Kailar逻辑分别对子协议分析，考察不同的线束是否满足安全属性。4) 利用串行合成分析整个协议是否满足安全性目标。

3.4 改进后协议的安全性分析

改进后的协议执行流程仍然如图1所示，存在两种执行可能：1) 只执行了Exchange协议，记为Exchange^1；2) 出现异常，执行了Resolve子协议，记为Exchange^2。协议的可追究性目标利用线束的概念及Kailar逻辑可以表述为：

$$\Gamma\vdash\text{Start}(A)[P(A,B,\text{STTP})]_A(\theta_1\wedge\theta_2) \qquad (1)$$

式中，P是改进后的协议，可由Exchange^1和Exchange^2串行合成；θ_1为A CanProve B Claims receipt$_b$；θ_2为B CanProve A Claims $E_{K_b}(m)$；Γ为假设前提。

要证明协议是否满足上述目标，需要分别讨论Exchange^1和Exchange^2两个过程的安全目标是否满足，再利用定理1进行证明。以下证明过程中使用的Kailar逻辑公理系统参见文献[9]。

1) 执行$\text{Exchange}^1(A,B,\text{STTP})$。

此时，协议只执行了Exchange子协议而正常结束。若要满足可追求性，即使得：

$$\Gamma_1 \vdash \text{Start}(A)[\text{Exchange}^1(A,B,\text{STTP})]_A(\theta_1 \wedge \theta_2) \quad (2)$$

成立。以下进行证明。

① 协议分析的准备。

a. 列出初始拥有集合：

$O_A^0 = \{K_A^{-1}, K_A, K_B, K_{\text{sttp}}\}$, $O_B^0 = \{K_B^{-1}, K_B, K_A, K_{\text{sttp}}\}$

b. 列出初始假设集合 Γ_1。

i. 基本假设

B1　A CanProve PK(B, K_B)

B2　B CanProve PK(A, K_A)

ii. 可信假设

T1　B CanProve A Controls match$(E_{K_b}(\text{m})), E_{K_b}(m))$

T2　A CanProve B Controls match(h(receipt$_b$), receipt$_b$)

iii. 协议理解假设

C1　A Has$(c, r, s, h(\text{receipt}_b), \text{receipt}_b \wedge$ match$(\text{receipt}_b, h(\text{receipt}_b)) \wedge$ B Claims h (receipt$_b$) $\Rightarrow$ A CanProve B Claims receipt$_b$

C2　A Claims $(h(E_{K_b}(m)), E_{K_b}(\text{m})) \Rightarrow$ A Claims match$(h(E_{K_b}(m)), E_{K_b}(m))$

C3　A Claims$(h(E_{K_b}(m)), E_{K_b}(m)) \wedge$ match$(E_{K_b}(m)), h(E_{K_b}(m))) \Rightarrow$ A Claims $E_{K_b}(m)$

C4　A Has $(h(\text{receipt}_b), \text{receipt}_b) \wedge$ B Claims $h(\text{receipt}_b) \Rightarrow$ B Claims match$(h(\text{receipt}_b), \text{receipt}_b)$

c. 列举EOO和EOR。

$\text{EOO} = E_{\text{sk}_a}(h(E_{K_b}(m)), E_{K_b}(m))$

$\text{EOR} = c, r, s, h(\text{receipt}_b), \text{receipt}_b$

② 可追究性分析。

a. 列举可追究目标。

协议满足可追究性质式(2)成立，即可满足：

$$\Gamma_1 \vdash \text{Start}(A)[\text{Exchange}^1(A,B,\text{STTP})]_A\theta_1 \quad (3)$$

$$\Gamma_1 \vdash \text{Start}(A)[\text{Exchange}^1(A,B,\text{STTP})]_A\theta_2 \quad (4)$$

b. 分析EOO与EOR的设计是否满足可追究性要求。

假定 $\text{EOO} \in O_B$，即 $E_{\text{sk}_a}(h(E_{K_b}(m))$，$E_{K_b}(m)) \in O_B$，故：

$$B \text{ Has } E_{\text{sk}_a}(h(E_{K_b}(m)), E_{K_b}(m)) \quad (5)$$

由签名公理，B2和式(5)可得：

$$B \text{ CanProve } (A \text{ Claims } (h(E_{K_b}(m)), E_{K_b}(m))) \quad (6)$$

由C2和式(6)可得：

$$B \text{ CanProve } (A \text{ Claims match}(h(E_{K_b}(m)), E_{K_b}(m))) \quad (7)$$

由管辖公理、T1和式(7)可得：

$$B \text{ CanProve match}(h(E_{K_b}(m)), E_{K_b}(m)) \quad (8)$$

由C3、连接公理和(8)式可得：

$$B \text{ CanProve } A \text{ Claims } E_{K_b}(m) \quad (9)$$

由(9)式可知式(4)成立，即EOO的设计满足协议可追究性的要求。

假定 $\text{EOR} \in O_A$，即

$$c, r, s, h(\text{receipt}_b), \text{receipt}_b \in O_A \quad (10)$$

由式(10)可知：

$$A \text{ Has } c, r, s, h(\text{receipt}_b), \text{receipt}_b \quad (11)$$

由签名公理、B1和式(11)可得：

$$A \text{ CanProve } (B \text{ Claims } h(\text{receipt}_b)) \quad (12)$$

由C4、式(11)和式(12)可得：

$$A \text{ CanProve}(B \text{ Claims match}(h(\text{receipt}_b), \text{receipt}_b)) \quad (13)$$

由管辖公理、T2和式(13)可得：

$$A \text{ CanProve match}(h(\text{receipt}_b), \text{receipt}_b) \quad (14)$$

由C1、连接公理、式(14)可得：

$$A \text{ CanProve } B \text{ Claims receipt}_b \quad (15)$$

由式(15)可知式(3)成立，即EOR的设计满足协议可追究性的要求。

c. 分析协议是否达到可追究性目标。

综上所述，若A、B双方各自能获得EOR和EOO，则协议的可追究性能够满足，即式(3)和式(4)成立。

在执行Excheange$^1(A,B,\text{STTP})$过程中，双方都能完全执行完Exchange协议，故有 $O_b^3 = O_b^2 \cup \text{EOO}$，$O_a^4 = O_a^2 \cup \text{EOR}$，即 $\text{EOO} \subseteq O_b \wedge \text{EOR} \subseteq O_a$ 成立，因此协议在只执行Exchange协议正常结束的情况下可追究性能够得到满足。

2) 执行 Exchange$^2(A,B,\text{STTP})$。

此时协议执行了Exchange协议和Resolve协议。若要满足可追求性，即：

$$\Gamma_2 \vdash \text{Start}(A)[\text{Exchange}^2(A,B,\text{STTP})]_A(\theta_1 \wedge \theta_2) \quad (16)$$

成立。

根据协议执行流程，Resolve协议由参与方A在以下两种情况下发起：

1) 在Exchange协议的E3执行后，A发送了信息m但没有收到receipt$_b$；

2) A没有执行E3而直接执行Resolve协议。

在上述两种情况下参与方A都已获得 $\phi_1 = E_{\text{sk}_b}(\text{Cert}_{tb}, h(E_{K_b}(m)), E_{K_{\text{sttp}}}(E_{K_b}(m)))$。由于此时Exchange协议中E2已经执行，故$B$已获得 $\phi_2 = E_{\text{sk}_a}(h(E_{K_b}(m)), E_{K_{\text{sttp}}}(E_{K_b}(m)))$，即在$A$发起

Resolve协议时，有：

$$(A \text{ Has } \phi_1) \wedge (B \text{ Has } \phi_2) \tag{17}$$

成立。

协议此时可通过由协议Exchange及Resolve串行合成而得。由定理1及式(17)可知，若要式(16)成立，需下式：

$$\Gamma_1' \vdash \phi_3[\text{Resolve}(A,B,\text{STTP})]_A(\theta_1 \wedge \theta_2) \tag{18}$$

成立。其中：$\Gamma_2 = \Gamma_1 \cup \Gamma_1'$，$\phi_3 = (A \text{ Has } \phi_1) \wedge (B \text{ Has } \phi_2)$。以下对式(18)进行证明。

① 协议分析的准备。

a. 列出初始拥有集合。

$$O_A^0 = \{K_A^{-1}, K_A, K_B, K_{\text{sttp}}, E_{\text{sk}_b}(\text{Cert}_{tb})\}$$

$$O_B^0 = \{K_B^{-1}, K_B, K_A, K_{\text{sttp}}, \phi_2\}$$

b. 列出初始假设集合 Γ_1'。

此时基本假设、可信假设、协议理解假设部分与执行Exchange[1](A,B,STTP)中相同，以下仅列出不同之处。

i. 基本假设：B3 A, B CanProve PK(STTP, K_{sttp})

ii.可信假设：

T3 A, B CanProve STTP Controls recover $(\text{receipt}_b, \text{Cert}_{tb})$

T4 A, B CanProve STTP Controls match $(h(E_{K_b}(m)), E_{K_b}(m))$

iii. 协议理解假设：

C5 STTP Claims $E_{K_b}(m) \Rightarrow$ STTP Claim match$(h(E_{K_b}(m)), E_{K_b}(m))$

C6 A Claims $h(E_{K_b}(m)) \wedge A$ Has $E_{K_b}(m) \wedge$ match $(E_{K_b}(m), h(E_{K_b}(m))) \Rightarrow A$ Claims $E_{K_b}(m)$

C7 A Claims $E_{K_{\text{sttp}}}(E_{K_b}(m)) \Rightarrow A$ Has $E_{K_b}(m)$

C8 STTP Claims $\text{receipt}_b \Rightarrow$ STTP Claim recover$(\text{receipt}_b, \text{Cert}_{tb})$

C9 recover$(\text{receipt}_b, \text{Cert}_{tb}) \wedge B$ Claims $\text{Cert}_{tb} \Rightarrow B$ Claim receipt_b

c. 列举EOO和EOR。

$\text{EOO} = E_{\text{SK}_{\text{sttp}}}(E_{K_b}(m))$，$\text{EOR} = E_{\text{SK}_{\text{sttp}}}(\text{receipt}_b)$

② 可追究性分析。

a. 列举可追究目标：

$$\Gamma_1' \vdash \phi_3[\text{Resolve}(A,B,\text{STTP})]_A(\theta_1 \wedge \theta_2) \tag{19}$$

b. 分析EOO与EOR的设计是否符合可追究性要求。

假定 $\text{EOO} \in O_B$，即 $E_{\text{SK}_{\text{sttp}}}(E_{K_b}(m)) \in O_B$，故：

$$B \text{ Has } E_{\text{SK}_{\text{sttp}}}(E_{K_b}(m)) \tag{20}$$

由B3、签名公理和式(20)有：

$$B \text{ CanProve (TTP Claims } E_{K_b}(m)) \tag{21}$$

由式(21)、C5、T4以及管辖公理，有：

$$B \text{ CanProve match}(h(E_{K_b}(m)), E_{K_b}(m)) \tag{22}$$

由 O_B^0 可知：

$$B \text{ Has } E_{\text{sk}_a}(h(E_{K_b}(m)), E_{K_{\text{sttp}}}(E_{K_b}(m))) \tag{23}$$

由式(23)、B2和签名公理有：

$$B \text{ CanProve (} A \text{ Claims } (h(E_{K_b}(m)), E_{K_{\text{sttp}}}(E_{K_b}(m)))) \tag{24}$$

由式(24)和C7有：

$$B \text{ CanProve } (A \text{ Has } E_{K_b}(m)) \tag{25}$$

由式(22)、式(24)、式(25)和C6可知：

$$B \text{ CanProve } (A \text{ Claims } E_{K_b}(m)) \tag{26}$$

即 $\Gamma_1' \vdash \phi_3[\text{Resolve}(A,B,\text{STTP})]_A\theta_2$ 成立，EOO的设计满足可追究性。

假定 $\text{EOR} \in O_A$，即 $E_{\text{SK}_{\text{sttp}}}(\text{receipt}_b) \in O_A$，故有：

$$A \text{ Has } E_{\text{SK}_{\text{sttp}}}(\text{receipt}_b) \tag{27}$$

由B3、签名公理和式(27)有：

$$A \text{ CanProve recover}(\text{receipt}_b, \text{Cert}_{tb}) \tag{28}$$

由式(28)、C8、T3以及管辖公理，有：

$$A \text{ CanProve recover}(\text{receipt}_b, \text{Cert}_{tb}) \tag{29}$$

由 O_A^0 可知：

$$A \text{ Has } \text{E}_{\text{sk}_b}(\text{Cert}_{tb}) \tag{30}$$

由式(30)，B1和签名公理，有：

$$A \text{ CanProve } (B \text{ Claims } \text{Cert}_{tb}) \tag{31}$$

由式(29)，式(31)和C9可知：

$$A \text{ CanProve } (B \text{ Claims receipt}_b) \tag{32}$$

成立。即公式 $\Gamma_1' \vdash \phi_3[\text{Resolve}(A,B,\text{STTP})]_A\theta_1$ 成立，EOR的设计满足可追究性。

综上所述，式(19)成立。

c. 分析协议是否达到可追究性目标。

以上证明针对协议已执行Resolve协议时的情况，在Resolve协议中，由R2、R3，有 $O_b^1 = O_b^0 \cup \text{EOO}$，$O_a^1 = O_a^0 \cup \text{EOR}$。因此有 $\text{EOO} \subseteq O_b \wedge \text{EOR} \subseteq O_a$ 成立，即协议在执行了Resolve协议的情况下可追究性得到满足。

由定理1、式(17)及式(32)可知式(16)成立，即此时协议满足可追究性。

通过对协议执行 Exchange[1](A,B,STTP) 和执行 Exchange[2](A,B,STTP) 的分析表明，协议的可追究性可以满足，即式(1)成立。

3.5 改进后协议的效率分析

改进后的协议采用文献[6]的签密方案，保持了原协议在对协议传输消息进行签名和加密时代价

小，执行效率高的特点。与文献[6]的方案比较，改进后的协议具有与原协议同样的协议体系结构和执行步骤。对原协议增加的操作如下：

1) 将原协议中所有明文传输的消息m用对称密钥算法加密为$E_{K_b}(m)$，同时对m的签名和摘要计算替换为对$E_{K_b}(m)$的签名和摘要。在整个协议中实际只增加了1次对m的加密，以后需要$E_{K_b}(m)$时直接调用即可。同时，消息中的签名和摘要只是内容改变，次数并未增加，因此没有对协议的整体执行效率带来影响。2) 在R1中，A传递的消息更改为$E_{\mathrm{sk}_b}(\mathrm{Cert}_{tb}, E_{K_{\mathrm{sttp}}}(E_{K_b}(m)), h(m)))$，该消息$A$直接从E2中获得，不需要增加任何计算，其时间复杂度和原协议一样。3) 在E2、E3中，各自增加了一次协议参与方对所传输消息的签名。在R2、R3中，增加了STTP对传输消息的一次签名。上述签名均只增加一次，并未对原协议增加过多的开销。

综上所述，改进后的协议并未大幅度增加原协议的执行开销。同时，如前文分析可以看出，增加的签名和加密过程均是克服文献[6]的缺陷所必须的。因此改进方案在没有大幅度增加原协议执行开销的同时，弥补了原协议中不满足保密性和可追究性的缺陷。

4　结 束 语

本文首先分析了文献[6]提出的协议所存在的3个安全性隐患，并采用文献[6]的签密方案，提出了一个基于离线半可信第三方的认证邮件协议。同时，针对Kailar逻辑以及组合协议分析方法在协议公平性及可追究性分析方面的不足，提出了在组合协议分析框架下利用Kailar逻辑进行协议分析的思路。最后，利用该方法对改进后的协议进行了形式化分析。

本文在利用Kailar逻辑分析离线第三方协议方面做出了有益的尝试，同时，将组合协议分析用于电子商务协议分析，扩大了其理论的应用范围。

参 考 文 献

[1] DENG R, GONG L, AUREL A, et al. Practical protocols for certified electronic mail[J]. Journal of Network and Systems Management, 1996, 4(3): 279-297.

[2] ASOKAN N, SHOUP V, WAIDNER M. Asynchronous protocols for optimistic fair exchange[C]//IEEE Symposium on Research in Security and Privacy. Oakland, USA: IEEE Computer Society, 1998: 86-99.

[3] ZHOU Jian-ying, DENG R H, BAO Feng. Some remarks on a fair exchange protocol[C]//International Workshop on Practice and Theory in Public Key Cryptography. Australia: Springer-Verlag, 2000: 46-57.

[4] SHAO Min-hua, WANG Gui-lin, ZHOU Jian-ying. Some common attacks against certified email protocols and the counter measures[J]. Computer Communications (Special Issue on Internet Communications Security), 2006, 29(15): 2759-2769.

[5] 崔军, 刘琦, 张振涛, 等. 可转换认证加密的安全邮件协议[J]. 电子科技大学学报学报, 2010, 39(4): 598-602.
CUI Jun, LIU Qi, ZHANG Zhen-tao, et al. A sec-email protocol based on the convertible authenticated encryption scheme[J]. Journal of University of Electronic Science and Technology of China, 2010, 39(4): 598-602.

[6] 张青, 张龙, 温巧燕, 等. 基于签密的认证邮件协议. 电子科技大学学报学报, 2008, 37(2): 282-284.
ZHANG Qing, ZHANG Long, WEN Qiao-yan, et al. A new certified e-mail protocol based on signcrytion[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(2): 282-284.

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

[8] 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 Dian-cui, QING Si-han, ZHOU Zhan-fei. A new approach for the analysis of electronic commerce protocolos [J]. Journal of Software of China, 2001, 12(9): 1318-1328.

[9] 卿斯汉. 一种电子商务协议形式化分析方法[J]. 软件学报, 2005, 16(10): 1757-1765.
QING Si-han. A formal method for analyzing electronic commerce protocols[J]. Journal of Software of China, 2005, 16(10): 1757-1765.

[10] DATTA A. Security analysis of network protocols: Compositional reasoning and complexity-theoretic foundations[D]. America: Stanford University, 2005.

[11] DATTA A, DEREK A, MITCHELL J C, et al. A derivation system for security protocols and its logical formalization[C]//Proceedings of 16th IEEE Computer Security Foundations Workshop. Washington DC, USA: IEEE, 2003.

[12] DATTA A, DEREK A, MITCHELL J C, et al. Secure protocol composition[C]//Proceedings of 19th Annual Conference on Mathematical Foundations of Programming Semantics. NewYork, USA: ACM, 2004.

[13] BACKES M, DATTA A, DEREK A, et al. Compositional Analysis of Contract-Signing Protocols[C]//Proceedings of 18th IEEE Computer Security Foundations Workshop. Washington DC, USA: IEEE, 2005.

编　辑　张　俊