满足多种安全属性的复合型支付协议及其逻辑分析*

陈 莉，袁开银
（河南财经政法大学 现代教育技术中心，郑州 450002）

摘 要：针对典型电子支付协议存在的安全目标单一，不能满足日益提高的安全需求等问题，提出了一种能够满足认证性、密钥新鲜性、密钥秘密性、非否认性、公平性、可追究性和原子性等多种安全属性的复合型安全支付协议，该协议的认证子协议基于令牌概念设计，能够实现高效认证及会话密钥协商。通过引入公钥证书证明协议主体的身份、借助可信方传递付款收据以及采用 FTP 方式传送电子货币和付款收据等方式提出了支付子协议。使用逻辑分析方法对该协议进行严格逻辑推理验证，结果表明该协议能够满足多种安全属性。

关键词：复合型支付协议；密钥新鲜性；密钥秘密性；原子性
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2012)07-2672-06
doi:10.3969/j.issn.1001-3695.2012.07.074

Design and logical analysis of compound payment protocol satisfying a variety of security properties

CHEN Li, YUAN Kai-yin
(*Center of Modern Educational Technology, Henan University of Economics & Law, Zhengzhou* 450002, *China*)

Abstract: In view of the existing problems of the payment protocols, e.g. security goal is single, increasing security requires are not been satisfied. This paper proposed a compound payment protocol, which satisfies a variety of security properties, such as authenticity, freshness of key, secrecy of key, non-repudiation, accountability, fairness and atomicity. The authentication sub-protocol of the new protocol can authenticate identities of the important entities in the foremost time, and the session keys used for transaction are negotiated efficiently. The payment sub-protocol is designed by using the following improvements. The first improvement is introducing certificates to prove the identities of the protocol entities. The second is transmitting the payment receipts by the trusted party. The third is using FTP to transport electronic cashes and payment receipts. The new protocol is proven to satisfy a variety of security properties by the logical analysis.

Key words: compound payment protocol; freshness of key; secrecy of key; atomicity

0 引言

现有大多数电子支付协议[1~3]安全目标单一，即协议设计通常只考虑满足部分安全属性，甚至有些协议还不能达到其预期的安全目标。例如，针对匿名电子现金支付协议 ISI[3]，文献[4]使用改进的 SVO 逻辑、文献[5]使用所提出的电子商务安全协议分析工具、文献[6]使用串空间方法均进行了分析，指出了该协议存在的缺陷，但这些文献都没有给出对协议 ISI 的改进方案。

针对上述问题，本文提出一种新的能够满足多种安全属性的复合型安全支付协议。该协议包括认证子协议和支付子协议两部分。其中基于令牌的认证子协议(token-based authenticated key exchange protocol, TAKEP)能够实现对移动商务交易主体身份的高效认证和交易会话密钥的协商。支付子协议(anonymous e-cash payment protocol, AECPP)是通过融合认证子协议 TAKEP、改进协议 ISI 设计而成的。本文还使用逻辑分析方法[7]对新协议的安全目标进行了严格的逻辑推理验证。

1 满足多种安全属性的支付协议

本章提出能够满足多种安全属性的复合型支付协议，该协议包括五个参与实体：移动用户 MU、网络信息服务提供商 SP、攻击者 I 以及 MU 和 SP 都信任的货币服务方 CS 与仲裁方 ADJ。

1.1 认证子协议

1.1.1 令牌构造

基于令牌概念设计认证协议，能够实现对交易实体 MU 的第一时间显性认证，令牌基于 hash 链技术构造，利用 hash 函数的单向性实现对令牌持有者的验证。

MU 构造一个 hash 链，首先确定安全的 hash 函数 h，安全参数记为 k，$h:\{0,1\}^* \mapsto \{0,1\}^k$，随机选择一个秘密种子 s，迭代执行 hash 函数 n 次，得到如下 hash 链：

$$T_0 = h^n(s) = h(h^{n-1}(s)) = \underbrace{h(h(h(\cdots h(s))))}_{n}$$

收稿日期：2011-12-03；**修回日期**：2012-01-04　　**基金项目**：国家“863”计划基金资助项目(2007AA01Z471)；国家自然科学基金资助项目(60473021)；河南省重点科技攻关项目(112102210015,072102210029)；河南省基础与前沿技术研究计划项目(122300410175)

作者简介：陈莉(1968-)，女，江苏如皋人，副教授，博士，主要研究方向为信息安全理论与技术(chlit123@yahoo.com.cn)；袁开银(1972-)，男，河南信阳人，讲师，主要研究方向为网络技术和信息安全.

Hash 链中的节点构成顺序的验证材料(称为令牌,表示为 token)集合,T_0 作为 hash 链验证锚用于验证 hash 链节点即令牌的有效性,每次 MU 登录 SP 网站出示一个(或多个)令牌,MU 第 i 次(i 从 1 到 n)出示自己的认证令牌,记为$\text{token}_{MU}^{i} = h^{n-i}(s)$。

CS 接收到 SP 转发的 MU 认证请求消息,包含 MU 出示的令牌,CS 计算 $h^i(\text{token}_{MU}{}^i)$,并与其验证锚 T_0 比较,相等表示该令牌有效,并更新链节指针为当前 i 值。

1.1.2　基于令牌的认证子协议

基于令牌的认证子协议 TAKEP 描述如下:

a) MU → SP: ID_{MU}, SP, $\text{Token}_{MU}{}^{n-2}$, {TS, $\text{Token}_{MU}{}^{n-1}$, $\{K_{MU\_SP}\}K_{MAC_1}\}K_{CS}$, MAC_1。

b) SP → CS: ID_{MU}, SP, $\text{Token}_{MU}{}^{n-2}$, {TS, $\text{Token}_{MU}{}^{n-1}$, $\{K_{MU\_SP}\}K_{MAC_1}\}K_{CS}$, MAC_2。

c) CS→SP: ID_{MU}, SP, {TS, SUCC, $\{K_{MU\_SP}\}K_{MAC_1}\}K_{SP\_CS\_1}$, MAC_3。

d) SP→MU: ID_{MU}, SP, {TS, SUCC}K_{MU_SP}, MAC_4。

协议约定及说明如下:

a) SP 表示主体 SP 的身份标志符。

b) ID_{MU}表示 MU 的匿名身份标志符,MU 真实身份对除 CS 之外的协议主体来说是保密的。

c) TS 表示协议主体产生的时间戳,协议中包含的令牌产生方式为:$\text{token}_{MU}{}^{n} = h^{n+1}(s)$, $\text{token}_{MU}^{n+1} = h^{n+2}(s)$。

d) K_{CS}表示 CS 的公钥,SUCC 表示认证成功的标志。

e) 会话密钥 K_{MU_SP}由 MU 产生,使用共享密钥 K_{MAC1} 和 K_{CS} 双重加密后,通过 CS 安全传递给 SP。K_{MU_SP}用于 MU 与 SP 安全的交易。其生成方式如下:K_{MU_SP} = PRF-128(I_{MU}, I_{SP}, N_{MU}),这里,N_{MU}表示由 MU 产生的随机数。

f) PRF-128 表示输出长度为 128 bit 的伪随机数生成函数。

g) K_{MAC_1}和 K_{MAC_2}分别表示 MU 与 SP 共享的、SP 与 CS 共享的、用于加密 hash 函数的密钥。

h) $K_{SP_CS_1}$和 $K_{SP_CS_2}$分别表示 SP 与 CS 的两个共享子密钥。$K_{SP_CS_1}$用于加密两者之间传递的数据,$K_{SP_CS_2}$用于构造两者传递消息的 MAC。

i) 消息完整性认证码 MAC_1 ~ MAC_4 定义如下:

MAC_1 = HMAC(ID_{MU}, SP, $\text{token}_{MU}{}^{n-2}$, {TS, $\text{token}_{MU}{}^{n-1}$, $\{K_{MU\_SP}\}K_{MAC_1}\}K_{CS}$, K_{MAC_1});

MAC_2 = HMAC($K_{SP\_CS\_2}$, ID_{MU}, SP, $\text{token}_{MU}{}^{n-2}$, {TS, $\text{token}_{MU}{}^{n-1}$, $\{K_{MU\_SP}\}K_{MAC_1}\}K_{CS}$, K_{MAC_2});

MAC_3 = HMAC($K_{SP\_CS\_2}$, ID_{MU}, SP, {TS, SUCC, $\{K_{MU\_SP}\}K_{MAC1}\}K_{SP\_CS\_1}$, K_{MAC_2});

MAC_4 = HMAC(ID_{MU}, SP, {TS, SUCC}K_{MU_SP}, K_{MAC_1});

HMAC 表示加密的 hash 函数。

1.2　支付子协议

匿名电子现金支付协议 ISI[3] 涉及三个参与者:客户 A、商家 B 以及双方都信任的货币服务方 CS,付款人 A 向收款人 B 付款,整个付款过程中付款人 A 保持匿名。

a) A→B: K_{AB}。

b) B→A: $\{K_B\}K_{AB}$。

c) A→B: $\{\{\text{coins}\}K_{CS}^{-1}, SK_A, K_{\_SES}, S_{\_ID}\}K_B$。

d) B→CS: $\{\{\text{coins}\}K_{CS}^{-1}, SK_B, \text{transaction}\}K_{CS}$。

e) CS→B: $\{\{\text{new\_coins}\}K_{CS}^{-1}\}SK_B$。

f) B→A: $\{\{\text{amount}, \text{Tid}, \text{date}\}K_B{}^{-1}\}SK_A$。

文献[4~6]对匿名电子现金支付协议 ISI 进行了分析,发现该协议存在以下安全漏洞和缺陷:

a) 使用商家提供的公钥作为其身份证明,将导致该协议无法实现非否认性。

b) 在以下两种情况下,该协议无法满足公平性、可追究性:一是通信信道不可靠,二是商家 B 企图恶意欺骗。

c) 在一般情况下,该协议不能实现原子性。但是上述文献都没有提出改进方案。

本文研究发现,协议 ISI 的第一条消息以明文方式传递交易主体之间的会话密钥 K_{AB},将导致密钥的秘密性无法确保。针对上述缺陷,本文提出的复合型协议将作以下改进:

a) 改进 1。由于认证子协议 TAKEP 实现了会话密钥的协商,所以根据协议执行的时序关系,原 ISI 协议的第 a) 步可省略。

b) 改进 2。由于在原协议语句 b) 中,商家提供的公钥不能作为其身份的证明,因此本协议改为:SP 向 MU 提供由 TTP 为其签发的公钥证书$\{k_{SP}, SP\}K_{TTP}^{-1}$证明自己的身份。

c) 改进 3。为了防止原协议商家 SP 的恶意欺骗,本协议将发送付款收据的方式改为由货币服务方 CS 转交的方式。

d) 改进 4。将协议语句 d) 和 e) 中的消息传送方式改为 FTP 方式,通过多次传输使 SP 和 MU 得到他们各自应得的付款和支付收据。防止由于信道出现故障所导致的协议执行被中断情况的发生。

ISI 的改进法方案即支付子协议 AECPP 描述如下:

a) SP→MU: $\{\{k_{SP}, \text{SP}\}K_{TTP}^{-1}\}K_{MU\_SP}$。

b) MU→SP: $\{\{\text{coins}\}K_{CS}^{-1}, SK_{MU}, K_{\_SES}, S_{\_ID}\}K_{SP}$。

c) SP→CS: $\{\{\text{coins}\}K_{CS}^{-1}, SK_{SP}, \text{transaction}, ID_{MU}\}K_{CS}$, $\{\{\text{amount}, \text{Tid}, \text{date}\}K_{SP}^{-1}\}SK_{MU}$。

d) SP↔CS: $\{\{\text{new\_coins}\}K_{CS}^{-1}\}SK_{SP}$。

e) MU↔CS: $\{\{\text{amount}, \text{Tid}, \text{date}\}K_{SP}^{-1}\}SK_{MU}$。

2　协议安全属性分析

本章使用逻辑分析方法[7]对复合型支付协议的安全属性进行严格的逻辑推理验证。鉴于篇幅有限,逻辑分析方法不在此赘述。

2.1　认证性和密钥新鲜性分析

1) 给出主体 MU 认证性和密钥新鲜性的形式化定义

G1: belie(MU, share(MU, SP, K_{MU_SP} +))

G2: belie(MU, fresh(K_{MU_SP}))

G3: belie(MU, belie(SP, share(SP, MU, K_{MU_SP}-)))

G4: belie(MU, belie(SP, fresh (K_{MU_SP})))

2) 列出主体 MU 的初始假设

P1: belie(MU, posse(MU, K_{MU_SP}))

P2: belie(MU, fresh(K_{MU_SP}))

P3: belie(MU, fresh(TS))

P4: belie(MU, share(MU, SP, K_{MAC1}))

P5: recei (MU, (ID_{MU}, SP, E ((TS, SUCC), K_{MU_SP}), H

((ID$_{MU}$,SP, E((TS,SUCC),K_{MU_SP})),K_{MAC1})))

P6: belie(MU, recei(MU, (ID$_{MU}$, SP, E((TS, SUCC), K_{MU_SP}), H((ID$_{MU}$,SP,E((TS,SUCC),K_{MU_SP})),K_{MAC1}))))

P7: belie(MU, send(SP, E((TS,SUCC),K_{MU_SP})) ∧ recei(MU, E((TS, SUCC),K_{MU_SP})) → belie(SP, share(SP, MU, K_{MU_SP}-)) ∧ belie(SP, fresh(K_{MU_SP}))

3)对主体 MU 的认证性和密钥新鲜性进行逻辑验证

(1) recei(MU, (ID$_{MU}$, SP, E((TS, SUCC), K_{MU_SP}), H((ID$_{MU}$,SP, E((TS,SUCC),K_{MU_SP})),K_{MAC1}))) → belie(MU, recei(MU,(ID$_{MU}$,SP, E((TS,SUCC),K_{MU_SP}),H((ID$_{MU}$,SP,E((TS,SUCC),K_{MU_SP})),K_{MAC1})))) AB1,P5,NER

(2) belie(MU, recei(MU, (ID$_{MU}$, SP, E((TS, SUCC), K_{MU_SP}), H((ID$_{MU}$,SP,E((TS,SUCC),K_{MU_SP})),K_{MAC1})))) AB2,P6,MPR,(1)

(3)belie(MU,recei(MU,E((TS,SUCC),K_{MU_SP}))) AB1,AMR,(2)

(4)belie(MU,send(SP,E((TS,SUCC),K_{MU_SP})) AB1,AB2,P4,MPR,(2)

(5)belie(MU,belie(SP,share(SP,MU,K_{MU_SP}-))) belie(MU,belie(SP,fresh(K_{MU_SP}))) AB1,P7,(3),(4)

(6)belie(MU,share(MU,SP,K_{MU_SP}-)) AB1,P1,(3),(4)

(7)belie(MU, posse(SP, share(MU,SP,K_{MU_SP}))) ∧ send(SP, (TS, SUCC)) AB1,ASA1,P1,(3)

(8)belie(MU,recei(MU,(TS,SUCC))) AB1,ACC1,P1,(3)

(9)belie(MU,fresh(E((TS,SUCC),K_{MU_SP}))) AB1,AMF1,P3,(7)

(10)belie(MU,send(SP,E((TS,SUCC),K_{MU_SP})) AB1,ANV,(6),(9)

(11)belie(MU,share(MU,SP,K_{MU_SP} +)) AB1,(6),(7),(10)

根据上述逻辑推理得到的结论(5)、(11)和 P2,可以得出协议能够满足关于 MU 的认证性和密钥新鲜性目标。

4)给出主体 SP 认证性和密钥新鲜性的形式化定义

G5:belie(SP,share(SP,MU,K_{MU_SP} +))

G6:belie(SP,fresh(K_{MU_SP}))

G7:belie(SP,belie(MU,share(MU,SP, K_{MU_SP}-)))

G8:belie(SP,belie(MU,fresh(K_{MU_SP})))

5)列出主体 SP 的初始假设

P1:bbelie(SP,posse(MU,K_{MU_SP}))

P2:belie(SP,fresh(TS))

P3:belie(SP,share(SP,CS,K_{MAC_2}))

P4:belie(SP,share(SP,CS,$K_{CS\_SP\_1}$))

P5:belie(SP,share(SP,MU,K_{MAC_1}))

P6:recei(SP,(ID$_{MU}$,SP,E((TS,SUCC,E(K$_{MU_SP}$,K_{MAC1})),$K_{SP\_CS\_1}$), H((($K_{SP\_CS\_2}$, ID$_{MU}$, SP, E((TS, SUCC, E(K_{MU_SP}, K_{MAC_1})), $K_{SP\_CS\_1}$)),K_{MAC_2}))

P7:belie(SP,recei(SP,(ID$_{MU}$,SP,E((TS,SUCC,E(K_{MU_SP}, K_{MAC_1})), $K_{SP\_CS\_1}$), H(($K_{SP\_CS\_2}$, ID$_{MU}$, SP, E((TS, SUCC, E(K_{MU_SP}, K_{MAC_1})), $K_{SP\_CS\_1}$)),K_{MAC_2}))) → belie(SP,recei(SP,(ID$_{MU}$,SP,E((TS,SUCC, E(K_{MU_SP},K_{MAC1})),$K_{SP\_CS\_1}$),H(($K_{SP\_CS\_2}$,ID$_{MU}$, SP,E((TS,SUCC, E(K_{MU_SP},K_{MAC1})),$K_{SP\_CS\_1}$)),K_{MAC_2}))) AB1,P6,NER

(2) belie(SP, recei(SP, (ID$_{MU}$, SP, E((TS, SUCC, E(K_{MU_SP}, K_{MAC_1})), $K_{SP\_CS\_1}$), H(($K_{SP\_CS\_2}$, ID$_{MU}$, SP, E((TS, SUCC,E(K_{MU_SP},K_{MAC1})),$K_{SP\_CS\_1}$)),K_{MAC_2}))) AB1,AB2,P7,MPR,(1)

(3)belie(SP,send(CS,E((TS,SUCC,E(K_{MU_SP},K_{MAC_1})), $K_{SP\_CS\_1}$))) AB1,AB2,P3,MPR,(2)

(4)belie(SP,recei(SP,E((TS,SUCC,E(K_{MU_SP},K_{MAC_1})), $K_{SP\_CS\_1}$))) AB1,AMR,(2)

(5)belie(SP,recei(SP,(TS,SUCC,E(K_{MU_SP},K_{MAC_1})))) AB1,ACC1,P4,(4)

(6)belie(SP,recei(SP,E(K_{MU_SP},K_{MAC_1}))) AB1,AMR,(5)

(7)belie(SP,send(MU,share(SP,MU,K_{MU_SP}))) AB1,ASA1,P5,(6)

(8)belie(SP,belie(MU,share(MU,SP,K_{MU_SP}))) belie(SP,belie(MU,fresh(K_{MU_SP}))) AB1,P8,(7)

(9)belie(SP,belie(MU,share(MU,SP,K_{MU_SP}-))) AB1,P1,(8)

(10)belie(SP,recei(SP,share(SP,MU,K_{MU_SP}))) AB1,ACC1,P5,(6)

(11)belie(SP,share(SP,MU,K_{MU_SP})) AB1,(7),(10)

(12)belie(SP,posse(SP,share(SP,MU,K_{MU_SP}))) AB1,AMP1,(10)

(13)belie(SP,share(SP,MU,K_{MU_SP})) AB1,P1,(6),(7)

(14)belie(SP,fresh(K_{MU_SP})) AB1,AMF1,P5,(5)

通过上述逻辑推理,可以得出协议满足关于 SP 的认证性和密钥新鲜性目标。

2.2 密钥秘密性分析

协议分析的准备工作。

1)任务 1 给出支付子协议的形式化描述。

(1)recei(MU,E(S((K$_{SP}$,SP),K_{TTP}^{-1}),K_{MU_SP}))

(2)recei(SP,E((S(coins,K_{CS}^{-1}),SK$_{MU}$,$K_{\_SES}$,S$_{_ID}$),K_{SP}))

(3) recei(CS, (E((S(coins, K_{CS}^{-1}), SK$_{SP}$, transaction, ID$_{MU}$),K_{CS}), E((S(amount,Tid,date),K_{SP}^{-1}),SK$_{MU}$))

(4)recei(SP,E(S(new_coins,K_{CS}^{-1}),SK$_{SP}$))

(5)recei(MU,E((S(amount,Tid,date),K_{SP}^{-1}),SK$_{MU}$))

2)任务 2 列举协议的初始化集合。

列举协议主体 MU、SP、攻击者 I 和仲裁方 ADJ 的初始假设集合、初始拥有集合,MU 和 SP 接收消息集合。

INI_S$_{MU}$ = {canpr(MU,authe(K_{CS},CS)),canpr(MU,authe

$(K_{TTP},TTP))\}$,

$INI\_S_{SP}=\{belie(SP,authe(K_{CS},CS)),canpr(SP,authe(K_{CS},CS))\}$,

$INI\_S_I=\{\neg(in(K_{CS}^{-1},POS_I)\wedge in(K_{TTP}^{-1},POS_I)\wedge in(K_{MU}^{-1},POS_I)\wedge in(K_{SP}^{-1},POS_I))\}$,

$INI\_S_{ADJ}=\{belie(ADJ,authe(K_{CS},CS))\}$,

$POS_{MU}^0=\{SK_{MU},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{MU}^{-1}\}$,

$POS_{SP}^0=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1}\}$,

$POS_I^0=\{K_{CS},K_{MU},K_{SP},K_{TTP}\}$,

$POS_{ADJ}^0=\{S((K_{SP},SP),K_{TTP}^{-1}),K_{TTP},K_{CS},K_{MU},K_{SP}\}$

$REV_{MU}=\{\}$,$REV_{SP}=\{\}$。

3)任务 3　列举发方、收方非否认证据 EOO 和 EOR。

$EOO=S(new\_coins,K_{CS}^{-1})$

$EOR=S((amount,Tid,date),K_{SP}^{-1})$

(1)给出密钥秘密性的形式化定义

$G\neg(in(K_{MU\_SP},POS_I)\wedge in(SK_{SP},POS_I)\wedge in(SK_{MU},POS_I)\wedge in(K_{\_SES},POS_I)\wedge in(K_{CS}^{-1},POS_I))\wedge in(K_{TTP}^{-1},POS_I)\wedge in(K_{MU}^{-1},POS_I)\wedge in(K_{SP}^{-1},POS_I))$。

(2)验证密钥秘密性目标

使用逻辑公理和推理规则,分析在每一条协议语句执行之后,攻击者获取合法协议主体密钥信息的情况。以此判断密钥秘密性目标是否满足。

证明　由于移动商务交易的网络环境是开放的,所以攻击者能够截获、窃听、窜改协议消息。首先,分析协议第(1)条语句。对攻击者而言,该语句执行后式(1.1)成立:

$$recei(I,(E(S((K_{SP},SP),K_{TTP}^{-1}),K_{MU\_SP})) \tag{1.1}$$

由攻击者初始拥有集合 POS_I^0 可知

$$\neg(in(K_{MU\_SP},POS_I)) \tag{1.2}$$

由式(1.1)(1.2)和密文理解公理 ACC1 可得

$$\neg in(S((K_{SP},SP),K_{TTP}^{-1}),POS_I) \tag{1.3}$$

第(2)条语句执行后,对攻击者而言,式(1.4)成立。

$$recei(I,E((S(coins,K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),K_{SP})) \tag{1.4}$$

由攻击者初始假设集合 $INI\_S_I^0$ 可知

$$\neg(in(K_{SP}^{-1},POS_I)) \tag{1.5}$$

由式(1.4)(1.5)和密文理解公理 ACC1 可得

$$\neg in((S(coins,K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),POS_I) \tag{1.6}$$

由上式可得

$$(in(K_{\_SES},POS_I)\wedge in(SK_{MU},POS_I)) \tag{1.7}$$

由攻击者初始假设集合 $INI\_S_I^0$ 可知

$$\neg(in(K_{SP}^{-1},POS_I)) \tag{1.8}$$

由式(1.7)(1.8)和密文理解公理 ACC1 可得

$$\neg in((S(coins,K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),POS_I) \tag{1.9}$$

第(3)条语句执行后,对攻击者而言,式(1.10)成立:

$$recei(I,(E((S(coins,K_{CS}^{-1}),SK_{SP},transaction,ID_{MU}),K_{CS}),E((S(amount,Tid,date),K_{SP}^{-1}),SK_{MU})) \tag{1.10}$$

由上式和消息接收公理 AMR 可得

$$recei(I,E((S(coins,K_{CS}^{-1}),SK_{SP},transaction,ID_{MU}),K_{CS})) \tag{1.11}$$

$$recei(I,E((S(amount,Tid,date),K_{SP}^{-1}),SK_{MU})) \tag{1.12}$$

由攻击者初始假设集合 $INI\_S_I^0$ 可知

$$\neg(in(K_{CS}^{-1},POS_I)\wedge(SK_{MU},POS_I)) \tag{1.13}$$

由式(1.11)(1.13)和密文理解公理 ACC1 可得

$$\neg in((S(coins,K_{CS}^{-1}),SK_{SP},transaction,ID_{MU}),POS_I) \tag{1.14}$$

由式(1.14)和消息接收公理 AMR 可得

$$\neg in(SK_{SP},POS_I) \tag{1.15}$$

由式(1.12)(1.13)和密文理解公理 ACC1 可得

$$\neg in((S(amount,Tid,date),K_{SP}^{-1}),POS_I) \tag{1.16}$$

同理分析后两条语句,攻击者无法得到密钥信息。

由式(1.2)(1.5)(1.8)(1.13)(1.15)和密钥秘密性定义可以得出,支付子协议满足密钥秘密性目标。证毕。

2.3　非否认性分析

1)给出非否认性的形式化定义

G1:belie(ADJ,send(MU,EOO))

G2:belie(ADJ,send(SP,EOR))

2)验证非否认性目标

(1)验证发方非否认性。

证明　假设仲裁方 ADJ 收到了发方非否认证据 EOO,可知

$$belie(ADJ,recei(ADJ,EOO)) \tag{2.1}$$

即

$$belie(ADJ,recei(ADJ,S(new\_coins,K_{CS}^{-1}))) \tag{2.2}$$

根据 ADJ 的初始假设集合 INI_{ADJ}_S 可知

$$belie(ADJ,authe(K_{CS},CS)) \tag{2.3}$$

由式(2.2)(2.3)和信任公理 AB1 可得

$$belie(ADJ,recei(ADJ,S(new\_coins,K_{CS}^{-1}))\wedge authe(K_{CS},CS)) \tag{2.4}$$

由式(2.4)和签名规则 SR2 可得

$$belie(ADJ,send(CS,new\_coins)) \tag{2.5}$$

综上即得,电子货币 $S(new\_coins,K_{CS}^{-1})$ 是有效的。由于支付子协议 AECPP 是匿名支付协议,而且通常协议主体不可能进行不利于自己的欺骗,因此,对于仲裁方来说,只需要证明付款有效即可认为目标达到。证毕。

(2)验证收方非否认性。

证明　假设仲裁方 ADJ 收到了收方非否认证据 EOR,可知

$$belie(ADJ,recei(ADJ,EOR)) \tag{2.1}$$

即

$$belie(ADJ,recei(ADJ,S((amount,Tid,date),K_{SP}^{-1}))) \tag{2.2}$$

根据 ADJ 的初始拥有集合 POS_{ADJ}^0 可知

$$posse(ADJ,S((K_{SP},SP),K_{TTP}^{-1}))\wedge posse(ADJ,K_{TTP}) \tag{2.3}$$

由式(2.3)和必然规则 NER 可得

$$belie(ADJ,posse(ADJ,S((K_{SP},SP),K_{TTP}^{-1}))\wedge posse(ADJ,K_{TTP})) \tag{2.4}$$

由式(2.4)和身份证明规则 IAR2 可得

$$belie(ADJ,authe(K_{SP},SP)) \tag{2.5}$$

由式(2.2)(2.5)和信任公理 AB1 可得

$$belie(ADJ,recei(ADJ,S((amount,Tid,date),K_{SP}^{-1}))\wedge authe(K_{SP},SP)) \tag{2.6}$$

由式(2.6)和签名规则 SR2 可得

$$belie(ADJ,send(SP,(amount,Tid,date))) \tag{2.7}$$

综合(1)和(2)的证明可知,支付子协议满足非否认性。证毕。

2.4 可追究性分析

1)给出可追究性的形式化定义

G1:canpr(SP,claim(MU,new-coins))

G2:canpr(MU,claim(SP,(amount,Tid,date)))

G3:in(EOO,POS_{SP})

G4:in(EOR,POS_{MU})

2)验证可追究性目标

(1)假定 in(EOO,POS_{SP})和 in(EOR,POS_{MU})成立,验证 G1 和 G2 是否成立;

证明 假定 in(EOO,POS_{SP})成立,即得

$$\text{in}(S(\text{new\_coins},K_{CS}^{-1}),POS_{SP}) \tag{3.1}$$

由式(3.1)可知

$$\text{posse}(SP,S(\text{new\_coins},K_{CS}^{-1})) \tag{3.2}$$

由 SP 初始假设集合 INI_S_{SP}可知

$$\text{canpr}(SP,\text{authe}(K_{CS},CS)) \tag{3.3}$$

由式(3.2)(3.3)和签名规则 SR2 可得

$$\text{canpr}(SP,\text{claims}(CS,\text{new\_coins})) \tag{3.4}$$

由于支付子协议 AECPP 是匿名支付协议,因此,对于收款方 SP 而言,只需证明付款有效,即可认为可追性目标 G1 成立。

假定 in(EOR,POS_{MU})成立,即

$$\text{in}(S((\text{amount},\text{Tid},\text{date}),K_{SP}^{-1})) \tag{3.5}$$

由式(3.5)可知

$$\text{posse}(MU,S((\text{amount},\text{Tid},\text{date}),K_{SP}^{-1})) \tag{3.6}$$

由 MU 初始假设集合 INI_S_{MU}可知

$$\text{canpr}(MU,\text{authe}(K_{TTP},TTP)) \tag{3.7}$$

由 MU 的拥有集合 $POS_{MU}1$ 可知

$$\text{posse}(MU,S((K_{SP},SP),K_{TTP}^{-1}))\wedge\text{posse}(MU,K_{TTP}) \tag{3.8}$$

由式(3.7)(3.8)和身份证明规则 IAR2 可得

$$\text{canpr}(MU,\text{authe}(K_{SP},SP)) \tag{3.9}$$

由式(3.6)(3.9)和签名规则 SR1 可得

$$\text{canpr}(MU,\text{claim}(SP,(\text{amount},\text{Tid},\text{date}))) \tag{3.10}$$

综上即得,可追究性目标 G2 得证。

(2)验证协议运行结束时,G3 和 G4 是否成立。

$$POS_{SP}\xrightarrow{\text{初始拥有}}POS_{SP}^{0}\cup POS_{SP}^{4}\xrightarrow{\text{接收消息(4)}}\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1}\}\cup POS_{SP}3\cup\{E(S(\text{new\_coins},K_{CS}^{-1}),SK_{SP})\}\xrightarrow{\text{解密}}\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1}\}\cup POS_{SP}2\cup\{E((S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),K_{SP})\}\cup\{E(S(\text{new\_coins},K_{CS}^{-1}),SK_{SP})\}\xrightarrow{\text{解密}}\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID},S(\text{new\_coins},K_{CS}^{-1}),SK_{SP}\} \tag{3.1}$$

由式(3.1)可得

$$\text{in}(S(\text{new\_coins},K_{CS}^{-1}),POS_{SP}5)$$

即

$$\text{in}(EOO,POS_{SP}5) \tag{G3}$$

$$POS_{MU}\xrightarrow{\text{初始拥有,接收消息(5)}}POS_{MU}^{0}\cup POS_{MU}1\cup\{E((S(\text{amount},\text{Tid},\text{date}),K_{SP}^{-1}),SK_{MU})\}\xrightarrow{\text{接收消息(1)}}\{SK_{MU},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{MU}^{-1}\}\cup\{E(S((K_{SP},SP),K_{TTP}^{-1}),K_{MU\_SP})\}\cup E((S(\text{amount},\text{Tid},\text{date}),K_{SP}^{-1}),SK_{MU})\}\xrightarrow{\text{解密}}\{SK_{MU},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},S((K_{SP},SP),K_{TTP}^{-1}),S(\text{amount},\text{Tid},\text{date}),K_{SP}^{-1}))\} \tag{3.2}$$

由式(3.2)可得

$$\text{in}(S(\text{amount},\text{Tid},\text{date}),K_{SP}^{-1})),POS_{MU}5)$$

即

$$\text{in}(EOR,POS_{MU}5) \tag{G4}$$

综上即得,可追究性目标 G1 ~ G4 均成立。证毕。

2.5 公平性分析

1)给出公平性的形式化定义

(1)协议正常结束时,公平性目标定义为

G1:in(EOO, POS_{SP})

G2:in(EOR, POS_{MU})

(2)协议第 i 条语句中断执行时,公平性定义为:

G3:¬ in(EOO, POS_{SP}^{i-1}) (这里 $i=1,2,3,4$)

G4:¬ in(EOR, POS_{MU}^{i-1}) (这里 $i=1,2,3,4$)

2)验证公平性目标

证明 (1)协议正常结束。根据 2.3 节中的分析结果,协议正常结束时,公平性目标满足。

(2)协议异常终止。由于协议语句(4)和(5)中的消息采用 FTP 方式传输,所以语句不会中断。

对 SP 而言,当前三条语句执行中断时,即

当 $i=1$ 时,$POS_{SP}^{1}=POS_{SP}^{0}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP}\}$

当 $i=2$ 时,$POS_{SP}^{2}=POS_{SP}1\cup\{E((S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),K_{SP})\}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1}\}\cup\{E((S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),K_{SP})\}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},E((S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}),K_{SP})\}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}\}$

当 $i=3$ 时,$POS_{SP}^{3}=POS_{SP}^{2}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},S(\text{coins},K_{CS}^{-1}),SK_{MU},K_{\_SES},S_{\_ID}\}$

因此当 $i=1,2,3$ 时,可得¬ in(EOO,$POS_{SP}i$) (4.1)

对 MU 而言,当前三条语句执行中断时,即

当 $i=1$ 时,$POS_{MU}^{1}=POS_{MU}^{0}\cup\{E(S((K_{SP},SP),K_{TTP}^{-1}),K_{MU\_SP})\}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1}\}\cup\{E(S((K_{SP},SP),K_{TTP}^{-1}),K_{MU\_SP})\}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},E(S((K_{SP},SP),K_{TTP}^{-1}),K_{MU\_SP})\}=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},S((K_{SP},SP),K_{TTP}^{-1})\}$

当 $i=2,3$ 时,$POS_{MU}^{2}=POS_{MU}^{3}=POS_{MU}1=\{SK_{SP},K_{CS},K_{TTP},K_{MU\_SP},K_{MU},K_{SP},K_{SP}^{-1},S((K_{SP},SP),K_{TTP}^{-1})\}$

因此当

$i=1,2,3$ 时,可得 in(EOR,$POS_{MU}i$) (4.2)

由式(4.1)(4.2)得出,协议前三条语句中断时,公平性目标 G3 和 G4 均成立。即 MU 和 SP 都不占优势。证毕。

2.6 原子性分析

1)给出原子性的形式化定义

G:A1 ∨ A2

A1:¬ in(new-coins,REV_{SP}) ∧ ¬ in((amount,Tid,date),REV_{MU}) (当协议异常终止时)

A2:in(new-coins,REV_{SP}) ∧ in((amount,Tid,date),REV_{MU}) (当协议正常结束时)

2)验证原子性目标

利用逻辑公理和推理规则,分析协议每条语句执行之后,

MU 和 SP 接收消息的情况,以此验证原子性目标。

证明　(1)在通信信道不可靠的情况下,当协议前三条语句中的任何一条语句中断时,都不会执行协议语句(4)和(5),因此可得出,原子性目标的子目标 A1 成立。

(2)在通信信道可靠的情况下,协议正常结束。只需对协议语句(4)和(5)进行分析。

首先,分析协议语句(4)。

$$\text{belie}(\text{SP},\text{recei}(\text{SP},\text{E}(\text{S}(\text{new\_coins},K_{\text{CS}}^{-1}),\text{SK}_{\text{SP}}))) \quad (5.1)$$

由 SP 的初始拥有集合 $\text{POS}_{\text{SP}}^{0}$ 可知

$$\text{posse}(\text{SP},\text{SK}_{\text{SP}}) \quad (5.2)$$

由式(5.1)(5.2)和密文理解规则 CCR1 可得

$$\text{belie}(\text{SP},\text{recei}(\text{SP},\text{S}(\text{new\_coins},K_{\text{CS}}^{-1}))) \quad (5.3)$$

由 SP 的初始拥有集合 $\text{POS}_{\text{SP}}^{0}$ 可知

$$\text{posse}(\text{SP},K_{\text{CS}}) \quad (5.4)$$

由式(5.3)(5.4)和签名规则 SR1 可得

$$\text{belie}(\text{SP},\text{recei}(\text{SP},\text{new\_coins})) \quad (5.5)$$

即

$$\text{in}(\text{new-coins},\text{REV}_{\text{SP}}) \quad (5.6)$$

接下来,分析协议语句(5)。

$$\text{belie}(\text{MU},\text{recei}(\text{MU},\text{E}(\text{S}((\text{amount},\text{Tid},\text{date}),K_{\text{SP}}^{-1}),\text{SK}_{\text{MU}}))) \quad (5.7)$$

由 MU 的初始拥有集合 $\text{POS}_{\text{MU}}^{0}$ 可知

$$\text{posse}(\text{MU},\text{SK}_{\text{MU}}) \quad (5.8)$$

由式(5.7)(5.8)和密文理解规则 CCR1 可得

$$\text{belie}(\text{MU},\text{recei}(\text{MU},\text{S}((\text{amount},\text{Tid},\text{date}),K_{\text{SP}}^{-1}))) \quad (5.9)$$

由 MU 的初始拥有集合 $\text{POS}_{\text{MU}}1$ 可知

$$\text{belie}(\text{MU},\text{posse}(\text{MU},\text{S}((K_{\text{SP}},\text{SP}),K_{\text{TTP}}{}^{-1}))) \quad (5.10)$$

由 MU 的初始拥有集合 $\text{POS}_{\text{MU}}^{0}$ 可知

$$\text{posse}(\text{MU},K_{\text{TTP}}) \quad (5.11)$$

由式(5.10)(5.11)和身份证明规则 IAR3 可得

$$\text{belie}(\text{MU},\text{authe}((K_{\text{SP}},\text{SP}))) \quad (5.12)$$

由式(5.9)(5.12)和签名规则 SR2 可得

$$\text{belie}(\text{MU},\text{recei}(\text{MU},(\text{amount},\text{Tid},\text{date}))) \quad (5.13)$$

即

$$\text{in}((\text{amount},\text{Tid},\text{date}),\text{REV}_{\text{MU}}) \quad (5.14)$$

由式(5.6)(5.14)可得出,原子性的子目标 A2 成立。

结合情况(1)和(2),可得协议满足原子性目标。证毕。

3　协议性能分析

3.1　认证子协议效率分析

比较协议 TAKEP 与协议 P1[8] 耗费资源的情况可以得出,P1 没有充分考虑 MU 资源受限以及 SP 和 CS 在线资源占用问题,需要执行两次签名、三次验证操作。此外由于 P1 采用传统 hash 链机制,所以每次交易 MU 都必须签名、传递新的验证锚。交易频繁时,将导致消耗 MU 有限的计算资源。而 TAKEP 协议只有 MU 首次交易需要签名、加密传递验证锚,后续交易时,由于 MU 在使用旧 hash 链的同时,已将新链的验证锚可验证地传递给 SP,所以 MU 只需支持公钥加密操作,而无须支持解密以及签名/验证操作。当配置加密效率高的算法时(如 RSA 公钥加密算法),MU 的计算消耗非常小。

比较 TAKEP 与协议 FWAI[9] 耗费资源的情况可以得出,两者都不执行签名及验证操作,FWAI 中 MU 与 CS 分别需要支持解密和加密操作。而 TAKEP 中 MU 不需要执行解密操作,CS 不需要执行加密操作。

将这三种协议的消息流数量进行比较,可以发现 TAKEP 包含比 P1 和 FWAI 更少的协议消息流,如表 1 所示。

综上分析可知,协议 TAKEP 具有更高的认证效率。

表 1　认证子协议 TAKEP 与典型协议计算资源及通信资源比较

协议	消息流	签名/验证			公钥加/解密		
		MU	SP	TTP	MU	SP	TTP
P1	6	1/1	0/2	1/0	0/0	0/0	0/0
FWAI	5	0/0	0/0	0/0	1/1	0/0	1/1
TAKEP	4	0/0	0/0	0/0	1/0	0/0	0/1

3.2　支付子协议鲁棒性分析

根据文献[4~7]对协议 ISI 的分析以及本文第 2 节对支付子协议 AECPP 的逻辑验证结果,可以得到表 2 中的数据。由此得出,支付子协议不仅确保了非否认性、可追究性、公平性的实现,而且实现了原子性和密钥秘密性,进一步增强了协议的鲁棒性。

表 2　支付子协议 AECPP 与协议 ISI 的比较

协议	安全属性						
	密钥秘密性	非否认性		可追究性	公平性		原子性
		EOO	EOR		MU	SP	
ISI[3]	×	√	×	×	×/劣势	×/优势	×
AECPP	√	√	√	√	√	√	√

4　结束语

本文提出了一种适用于移动商务交易的复合型安全支付协议,并且使用逻辑分析方法对该协议进行严格的逻辑推理验证,结果表明该协议能够满足多种安全属性。

随着移动商务和网络信息技术的发展,对电子支付的安全需求会不断提高,因此,需要设计出能够满足更多种安全属性的电子支付协议。与此同时,对电子支付安全协议形式化分析方法的研究也提出了更高的要求。

参考文献:

[1] DESPOINA P, PETROS D, KOSMAS P. A novel peer-to-peer payment protocol[J]. International Journal of Network Security, 2007, 4(1): 107-120.

[2] SHAO Jun, FENG Min, ZHU Bin, *et al*. An efficient certified email protocol[C]//Proc of Information Security Conference. Berlin: Springer, 2007: 145-157.

[3] MEDVINSKY G, NEUMAN B C. Netcash: a design of practical electronic currency on the Internet [C]//Proc of the 1st ACM Conference on Computer and Communications Security. New York: ACM Press, 1993: 102-106.

[4] 王茜, 杨德礼. 一种基于 SVO 逻辑的新形式化验证方法[J]. 计算机集成制造系统, 2004, 10(3): 342-351.

[5] 周典萃, 卿斯汉, 周展飞. 一种分析电子商务安全协议的新工具[J]. 软件学报, 2001, 12(9): 1318-1328.

[6] 刘义春, 张焕国. 电子商务协议的串空间分析[J]. 计算机科学, 2008(2): 109-114.

[7] CHEN Li, LI Xiao-xue. Verification method of security protocols and its application[C]//Proc of IEEE International Conference on Intelligent Computing and Intelligent Systems. 2010: 483-486.

[8] 姬东耀, 王育民. 基于 PayWord 的小额电子支付协议[J]. 电子学报, 2002, 30(2): 301-303.

[9] ZHANG Hao-jun, ZHU Yue-fei. A new authentication and key management scheme of WLAN[C]//Proc of the 1st International Conference on Communications and Networking in China. 2006: 1-5.