优化的匿名电子现金支付协议及其形式化验证 *

陈 莉, 刘 军
(河南财经学院 计算中心, 郑州 450002)

摘 要: 针对匿名电子现金支付协议存在的缺陷,提出了一种能够满足多种安全属性的优化协议。将会话密钥的协商与使用分为两个阶段进行,确保协议密钥保密性的实现;引入电子证书证明交易主体的身份,确保协议非否认性的实现;借助可信方传递付款收据,避免交易主体不诚实所导致的公平性缺失;引入 FTP 传输方式传送电子货币和付款收据,确保实现可追究性与公平性,进一步增强协议的鲁棒性。对优化协议进行形式化验证,结果表明,优化协议满足密钥保密性、非否认性、公平性、可追究性、原子性等安全属性。

关键词: 安全属性; 形式化验证; 密钥保密性; 非否认性; 公平性; 原子性
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)08-3053-05
doi:10.3969/j.issn.1001-3695.2010.08.064

Optimization of anonymous e-cash payment protocol and its formal verification

CHEN Li, LIU Jun
(*Computer Center*, *Henan University of Finance & Economics*, *Zhengzhou* 450002, *China*)

Abstract: In response on the existing problems of anonymous e-cash payment protocol, the paper proposed an optimal protocol, which could meet a variety of security properties. To ensure the realization of its key confidentiality, the agreement and use of the session key were divided into two stages. To realize its non-repudiation, the certificates were used to prove the identities of the transaction entities. To avoid unfairness arisen by the dishonest transaction entities, the transmission of payment receipt was achieved by the trusted party. The proposed protocol used FTP to transmit electronic cashes and payment receipts, which ensured achievement of accountability and fairness, and enhanced the robustness of the protocol. Formal verification results indicate that the optimal protocol satisfies key confidentiality, non-repudiation, accountability, fairness and atomicity.

Key words: security property; formal verification; key confidentiality; non-repudiation; fairness; atomicity

电子商务安全协议[1~4]是保障电子商务安全、顺利开展的关键技术。然而,电子商务安全协议自身的缺陷和安全漏洞,可能导致诸多问题,如协议异常中断、不诚实交易方否认自己的行为以及无法追究不诚实交易方的责任等,都将使诚实交易主体的利益受到严重损害。因此,电子商务安全协议应该具有更全面的安全属性,即不仅要满足一般安全协议具有的认证性、密钥保密性、密钥新鲜性、密钥专有性和完整性等安全属性,而且还要满足原子性、公平性、非否认性、匿名性、可追究性、时限性、不可滥用性等安全属性。现有的大多数电子商务安全协议安全目标单一,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,文献[5]使用改进的 SVO 逻辑、文献[6]使用所提出的周—卿—逻辑、文献[7]使用串空间方法分别对匿名电子现金支付协议 ISI[1] 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 ISI 协议的改进方案。

本文研究发现 ISI 协议不满足密钥保密性,因此本文针对上述问题,提出一种优化的匿名电子现金支付协议,并通过文献[8]提出的逻辑方法对优化协议进行了形式化验证,该协议能够满足密钥保密性、非否认性、公平性、可追究性、原子性等安全属性。

1 优化的匿名电子现金支付协议

1.1 匿名电子现金支付协议

匿名电子现金支付协议 ISI[1](表 1)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。

表 1 匿名电子现金支付协议 ISI

(1) $A\rightarrow B$:	K_{AB}
(2) $B\rightarrow A$:	$\{K_B\}K_{AB}$
(3) $A\rightarrow B$:	$\{\{\text{coins}\}K_{CS}^{-1}, SK_A, K_{\_SES}, S_{\_ID}\}K_B$
(4) $B\rightarrow CS$:	$\{\{\text{coins}\}K_{CS}^{-1}, SK_B, \text{transaction}\}K_{CS}$
(5) $CS\rightarrow B$:	$\{\{\text{new\_coins}\}K_{CS}^{-1}\}SK_B$
(6) $B\rightarrow A$:	$\{\{\text{amount}, \text{Tid}, \text{date}\}K_B^{-1}\}SK_A$

在 ISI 协议中,K_{AB} 表示 A 和 B 之间的会话密钥;K_A、K_B、K_{CS}、K_{CS}^{-1} 分别表示客户 A、商家 B 的公钥以及货币服务方 CS 的公钥和私钥;$\{\text{coins}\}K_{CS}^{-1}$ 表示 A 的电子货币(货币均由 CS 签发);SK_A、SK_B 分别表示 A 与 B 共享的密钥;$K_{\_SES}$ 表示想要获得的服务的密钥;$S_{\_ID}$ 表示想要获得的服务的标志符;transaction

收稿日期: 2010-01-16; **修回日期**: 2010-03-19 **基金项目**: 国家"863"计划资助项目(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(072102210029);河南省科技攻关项目(0624260017);河南省教育厅自然科学研究计划项目(2010A520004)

作者简介:陈莉(1968-),女,副教授,博士,主要研究方向为信息安全、安全协议和电子商务(chlit123@yahoo.com.cn);刘军(1963-),男,副教授,主要研究方向为信息安全理论与技术.

表示具体事务处理。

文献[5~7]对匿名电子现金支付协议 ISI 进行分析,发现该协议不能实现其预期的安全目标,存在以下安全漏洞和缺陷:a)商家提供的公钥不能作为其身份证明,导致 ISI 协议无法实现非否认性;b)在以下两种情况下,ISI 协议无法满足公平性、可追究性,即通信信道不可靠与商家 B 企图恶意欺骗;c)在一般情况下,ISI 协议不能实现原子性。但是上述文献都没有提出改进方案。

1.2 优化协议的提出

本文研究发现,ISI 协议的第一条消息以明文方式传递 A 和 B 之间的会话密钥 K_{AB},这样将无法确保密钥的保密性。针对文献[5~7]以及本文研究发现的 ISI 协议的缺陷,本文提出以下改进:

改进 1 针对该协议不能满足密钥保密性的缺陷,本文提出的优化协议将会话密钥的协商与使用分为两个阶段进行,即会话密钥安全协商在交易主体身份认证阶段进行,其使用则在认证之后的交易中进行。从而有效解决了此安全缺陷。交易主体实现身份认证和会话密钥协商,可采用文献[9]提出的下述方案:

a) $A \rightarrow TTP$: ID_A, ID_B, Nonce_A

b) $TTP \rightarrow A$: $\{\mathrm{Nonce}_A,\ \mathrm{ID}_B, K_{A\_B}, \{\mathrm{ID}_A, T_B, K_{A\_B}\}K_{B\_TTP}\}K_{A\_TTP}$

c) $A \rightarrow B$: $\{\mathrm{ID}_A,\ T_{TTP}, K_{A\_B}\}K_{B\_TTP}, \{\mathrm{ID}_A, T_A\}K_{A\_B}$

d) $\mathrm{B} \rightarrow A$: $\{\mathrm{ID}_B, T_A - 1\}K_{A\_B}$

如果兼顾认证效率和安全性,也可以采用文献[10]提出的基于令牌的认证协议实现身份认证和会话密钥协商。协议描述如下:

a) $A \rightarrow B$: ID_A, B, Token_A^{n-2}, $\{\mathrm{TS}, \mathrm{Token}_A^{n-1}, \{K_{A\_B}\}K_{\mathrm{MAC1}}\}K_{TTP}$, MAC1

b) $B \rightarrow TTP$: ID_A, B, Token_A^{n-2}, $\{\mathrm{TS}, \mathrm{Token}_A^{n-1}, \{K_{A\_B}\}K_{\mathrm{MAC1}}\}K_{TTP}$, MAC2

c) $TTP \rightarrow B$: ID_A, B, $\{\mathrm{TS}, \mathrm{SUCC}, \{K_{A\_B}\}K_{\mathrm{MAC1}}\}K_{B\_TTP\_1}$, MAC3

d) $B \rightarrow A$: ID_A, B, $\{\mathrm{TS}, \mathrm{SUCC}\}K_{A\_B}$, MAC4

由于在上述认证协议中实现了会话密钥的协商,根据协议执行的时序关系,可以省略原 ISI 协议的第 a)步。

改进 2 在原协议语句(2)中,商家向客户提供的公钥不能作为其身份的证明,因此本方案改为:商家 B 向客户 A 提供由 TTP 为其签发的电子证书 $\{k_B, B\}K_{TTP}^{-1}$ 证明自己的身份。

改进 3 为了防止原协议商家的恶意欺骗行为,即收到付款后,不向客户提供付款收据,本方案改变了付款收据的交递方式,即将原协议中由商家自己发送付款收据的方式改为由货币服务方 CS 转交的方式。

改进 4 将协议语句(4)和(5)中的消息传送方式改为 FTP 方式,通过多次传输使 B 和 A 得到他们各自应得的付款和支付收据。防止了由于通信信道出现故障所导致的协议语句执行被中断情况的发生。

优化的匿名电子现金支付协议如表 2 所示。

表 2 优化的匿名电子现金支付协议

(1) $B \rightarrow A$: $\{\{k_B, B\}K_{TTP}^{-1}\}K_{A\_B}$

(2) $A \rightarrow B$: $\{\{\mathrm{coins}\}K_{CS}^{-1}, SK_A, K_{\_\mathrm{SES}}, S_{\_\mathrm{ID}}\}K_B$

(3) $B \rightarrow CS$: $\{\{\mathrm{coins}\}K_{CS}^{-1}, SK_B, \mathrm{transaction}, \mathrm{ID}_A\}K_{CS}, \{\{\mathrm{amount}, \mathrm{Tid}, \mathrm{date}\}K_B^{-1}\}SK_A$

(4) $B \leftrightarrow CS$: $\{\{\mathrm{new\_coins}\}K_{CS}^{-1}\}SK_B$

(5) $A \leftrightarrow CS$: $\{\{\mathrm{amount}, \mathrm{Tid}, \mathrm{date}\}K_B^{-1}\}SK_A$

1.3 优化协议的目标

通过改进匿名电子现金支付协议 ISI 提出的优化协议,拟实现下述安全目标:

a)密钥保密性。攻击者无法得到合法协议主体之间共享的密钥信息。

b)非否认性。A 不能否认自己的付款行为,B 不能否认自己所开具的付款收据(作为 A 的提货凭证)。

c)可追究性。即满足以下两个子目标:

(a) A 和 B 都可向第三方证明对方必须对自己行为负责;

(b) A 和 B 必须得到对方的非否认证据。

d)公平性。即满足以下两个子目标:

(a)协议正常结束时,A 和 B 必须得到对方的非否认证据;

(b)协议异常终止时,A 和 B 中的任何一方都不占优势。

e)原子性。协议结束时,要么 A 和 B 都得到了所交换的信息,要么双方都没有得到。

2 优化协议的形式化验证

本章将使用文献[8]中提出的逻辑方法(本文称为 C 逻辑)对优化协议的密钥保密性、非否认性、可追究性、公平性、原子性进行验证。

由于篇幅有限,本文只给出验证过程中所需的 C 逻辑公理及推理规则。C 逻辑内容详见文献[8]。

信任公理 AB1

$\mathrm{believe}(P,x) \wedge \mathrm{believe}(P,y) \leftrightarrow \mathrm{believe}(P, x \wedge y)$

消息接收公理 AMR

$\mathrm{receive}(P,(x_1,\cdots,x_n)) \rightarrow \mathrm{receive}(P,x_i)$

密文理解公理 ACC1

$\mathrm{receive}(P,E(x,k)) \wedge \mathrm{possess}(P,k^{-1}) \rightarrow \mathrm{receive}(P,x)$

必然规则 NER

$\mathrm{true}(x) \rightarrow \mathrm{true}(\mathrm{believe}(P,x))$

签名规则 SR1

$\mathrm{possess}(P,S(x,k^{-1})) \wedge \mathrm{canprove}(P,\mathrm{authenticate}(k,Q)) \rightarrow \mathrm{canprove}(P,\ \mathrm{claims}(Q,x))$

签名规则 SR2

$\mathrm{believe}(P,\mathrm{receive}(P,S(m,k^{-1}))) \wedge \mathrm{believe}(P,\mathrm{authenticate}(k,Q)) \rightarrow \mathrm{believe}(P,\mathrm{send}(Q,m))$

密文理解规则 CCR1

$\mathrm{canprove}(P,\mathrm{claim}(Q,E(x,k))) \wedge \mathrm{canprove}(P,\mathrm{possess}(Q,k)) \wedge \mathrm{canprove}(P,\mathrm{verify}(x,k,E(x,k))) \rightarrow \mathrm{canprove}(P,\mathrm{claim}(Q,k))$

身份证明规则 IAR2

$\mathrm{canprove}(P,\mathrm{authenticate}(k_{TTP},TTP)) \wedge \mathrm{possess}(P,S((k_Q,Q),k_{TTP}^{-1})) \wedge \mathrm{possess}(P,k_{TTP}) \rightarrow \mathrm{canprove}(P,\mathrm{authenticate}(k_Q,Q))$

身份证明规则 IAR3

$\mathrm{believe}(P,\mathrm{possess}(P,S((k_Q,Q),k_{TTP}^{-1})) \wedge \mathrm{possess}(P,k_{TTP}) \rightarrow \mathrm{believe}(P,\mathrm{authenticate}(k_Q,Q))$

协议形式化验证的准备工作:

任务 1 给出协议的形式化描述。

使用 C 逻辑对优化协议进行形式化描述(表 3)。

表 3　优化协议的形式化描述

(1) receive(A,$E(S((k_B,B),K_{TTP}^{-1}),K_{A\_B})$)
(2) receive(B,$E((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B)$)
(3) receive(CS,$(E((S(\text{coins},K_{CS}^{-1}),SK_B,\text{transaction},ID_A),K_{CS}),E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A))$
(4) receive(B,$E(S(\text{new\_coins},K_{CS}^{-1}),SK_B)$)
(5) receive(A,$E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A)$)

任务 2　列举协议的初始化集合。

根据协议运行环境和协议运行的初始状态,分别列举协议主体的初始假设集合、拥有集合以及接收消息集合。

设协议主体 A、B、攻击者 I 和仲裁方 ADJ 的初始假设集合分别为 INI_S_A、INI_S_B、INI_S_I 和 INI_S_{ADJ},他们的初始拥有集合分别为 POS_A^0、POS_B^0、POS_I^0 和 POS_{ADJ}^0,A 和 B 的接收消息集合分别为 REV_A 和 REV_B。

$INI\_S_A = \{\text{canprove}(A,\text{authenticate}(K_{CS},CS)),\text{canprove}(A,\text{authenticate}(K_{TTP},TTP))\}$

$POS_A^0 = \{SK_A,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_A^{-1}\}$,$REV_A = \{\}$

$INI\_S_B = \{\text{believe}(B,\text{authenticate}(K_{CS},CS)),\text{canprove}(B,\text{authenticate}(K_{CS},CS))\}$,$POS_B^0 = \{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1}\}$

$\text{REV}_B = \{\}$

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

$POS_I^0 = \{K_{CS},K_A,K_B,K_{TTP}\}$

$INI\_S_{ADJ} = \{\text{believe}(ADJ,\text{authenticate}(K_{CS},CS))\}$

$POS_{ADJ}^0 = \{S((k_B,B),K_{TTP}^{-1}),K_{TTP},K_{CS},K_A,K_B\}$

任务 3　列举发方非否认证据 EOO 和收方非否认证据 EOR。

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

$EOR = S((\text{amount},\text{Tid},\text{date}),K_B^{-1})$

2.1　密钥保密性验证

步骤 1　给出密钥保密性的形式化定义。

使用 C 逻辑可以将密钥保密性目标形式化定义为

G　$\neg(\text{in}(K_{A\_B},POS_I) \wedge \text{in}(SK_B,POS_I) \wedge \text{in}(SK_A,POS_I) \wedge \text{in}(K_{\_SES},POS_I) \wedge \text{in}(K_{CS}^{-1},POS_I)) \wedge \text{in}(K_{TTP}^{-1},POS_I) \wedge \text{in}(K_A^{-1},POS_I) \wedge \text{in}(K_B^{-1},POS_I))$

步骤 2　验证密钥保密性目标。

使用 C 逻辑的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,并以此判断密钥保密性目标是否满足。

证明　电子商务交易的网络环境是开放的,所以在协议执行过程中,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)成立。

$$\text{receive}(I,(E(S((k_B,B),K_{TTP}^{-1}),K_{A\_B})) \tag{1}$$

由攻击者初始拥有集合 POS_I^0 可知

$$\neg(\text{in}(K_{A\_B},PO_{SI})) \tag{2}$$

由式(1)(2)和 C 逻辑密文理解公理 ACC1 可得

$$\neg\ \text{in}(S((k_B,B),K_{TTP}^{-1}),POS_I) \tag{3}$$

接下来,分析协议第(2)条语句。对攻击者而言,该语句执行后式(4)成立。

$$\text{receive}(I,E((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B)) \tag{4}$$

由攻击者初始假设集合 $INI\_S_I^0$ 可知

$$\neg(\text{in}(K_B^{-1},POS_I)) \tag{5}$$

由式(4)(5)和 C 逻辑密文理解公理 ACC1 可得

$$\text{in}((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),POS_I) \tag{6}$$

由式(6)可得

$$\neg(\text{in}(K_{\_SES},POS_I) \wedge \text{in}(SK_A,POS_I)) \tag{7}$$

由攻击者初始假设集合 $INI\_S_I^0$ 可知

$$\neg(\text{in}(K_B^{-1},POS_I)) \tag{8}$$

由式(7)(8)和 C 逻辑密文理解公理 ACC1 可得

$$\neg\ \text{in}((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),POS_I) \tag{9}$$

下面分析协议第(3)条语句。对攻击者而言,该语句执行后式(10)成立。

$$\text{receive}(I,(E((S(\text{coins},K_{CS}^{-1}),SK_B,\text{transaction},\text{ID}_A),K_{CS}),E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A))) \tag{10}$$

由式(10)和 C 逻辑消息接收公理 AMR 可得

$$\text{receive}(I,E((S(\text{coins},K_{CS}^{-1}),SK_B,\text{transaction},\text{ID}_A),K_{CS})) \tag{11}$$

$$\text{receive}(I,E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A)) \tag{12}$$

由攻击者初始假设集合 $INI\_S_I^0$ 可知

$$\neg(\text{in}(K_{CS}^{-1},POS_I) \wedge (SK_A,POS_I)) \tag{13}$$

由式(11)(13)和 C 逻辑密文理解公理 ACC1 可得

$$\neg\ \text{in}((S(\text{coins},K_{CS}^{-1}),SK_B,\text{transaction},\text{ID}_A),POS_I) \tag{14}$$

由式(14)和 C 逻辑消息接收公理 AMR 可得

$$\neg\ \text{in}(SK_B,POS_I) \tag{15}$$

由式(12)(13)和 C 逻辑密文理解公理 ACC1 可得

$$\neg\ \text{in}((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),POS_I) \tag{16}$$

同理分析后两条语句,攻击者无法得到密钥信息。

由式(2)(5)(8)(13)(15)和密钥保密性形式化定义可以得出,优化协议满足密钥保密性目标。证毕。

2.2　非否认性验证

步骤 1　给出非否认性的形式化定义。

使用 C 逻辑可以将非否认性目标形式化定义为

G1　$\text{believe}(ADJ,\text{send}(A,EOO))$

G2　$\text{believe}(ADJ,\text{send}(B,EOR))$

步骤 2　验证非否认性目标。

利用 C 逻辑的公理和推理规则验证优化协议是否满足上述所给的非否认性目标 G1 和 G2。

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

$$\text{believe}(ADJ,\text{receive}(ADJ,EOO)) \tag{17}$$

即

$$\text{believe}(ADJ,\text{receive}(ADJ,S(\text{new\_coins},K_{CS}^{-1}))) \tag{18}$$

根据 ADJ 的初始假设集合 INI_{ADJ}_S 可知

$$\text{believe}(ADJ,\text{authenticate}(K_{CS},CS)) \tag{19}$$

由式(18)(19)和 C 逻辑的信任公理 AB1 可得

$$\text{believe}(ADJ,\text{receive}(ADJ,S(\text{new\_coins},K_{CS}^{-1})) \wedge \text{authenticate}(K_{CS},CS)) \tag{20}$$

由式(20)和 C 逻辑的签名规则 SR2,可得

$$\text{believe}(ADJ,\text{send}(CS,\text{new\_coins})) \tag{21}$$

综上即得,电子货币 $S(\text{new\_coins},K_{CS}^{-1})$ 是有效的。由于优化协议是匿名支付协议,而且协议主体不可能进行不利于自己的欺骗,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 收到了发方非否认证据 EOR,可

知

$$\text{believe}(ADJ,\text{receive}(ADJ,EOR)) \tag{22}$$

即

$$\text{believe}(ADJ,\text{receive}(ADJ,S((\text{amount},\text{Tid},\text{date}),K_B^{-1}))) \tag{23}$$

根据 ADJ 的初始拥有集合 POS_{ADJ}^0 可知

$$\text{possess}(ADJ,S((k_B,B),K_{TTP}^{-1}))\wedge\text{possess}(ADJ,k_{TTP}) \tag{24}$$

由式(24)和 C 逻辑的必然规则 NER 可得,

$$\text{believe}(ADJ,\text{possess}(ADJ,S((k_B,B),K_{TTP}^{-1}))\wedge \text{possess}(ADJ,k_{TTP})) \tag{25}$$

由式(25)和 C 逻辑的身份证明规则 IAR2 可得

$$\text{believe}(ADJ,\text{authenticate}(k_B,B)) \tag{26}$$

由式(23)(26)和 C 逻辑的信任公理 AB1 可得

$$\text{believe}(ADJ,\text{receive}(ADJ,S((\text{amount},\text{Tid},\text{date}),K_B^{-1}))\wedge\text{authenticate}(k_B,B)) \tag{27}$$

由式(27)和 C 逻辑的签名规则 SR2,可得

$$\text{believe}(ADJ,\text{send}(B,(\text{amount},\text{Tid},\text{date}))) \tag{28}$$

综合 1)和 2)的证明可得,优化协议满足非否认性目标。证毕。

2.3　可追究性验证

步骤 1　给出可追究性的形式化定义。

使用 C 逻辑可以将可追究性目标形式化定义为

G1　$\text{canprove}(B,\text{claim}(A,\text{new-coins}))$

G2　$\text{canprove}(A,\text{claim}(B,(\text{amount},\text{Tid},\text{date})))$

G3　$\text{in}(EOO,POS_B)$

G4　$\text{in}(EOR,POS_A)$

步骤 2　验证可追究性目标。

1)假定 $\text{in}(EOO,POS_B)$ 和 $\text{in}(EOR,POS_A)$ 成立,验证 G1 和 G2 是否成立

证明　假定 $\text{in}(EOO,POS_B)$ 成立,即得

$$\text{in}(S(\text{new\_coins},K_{CS}^{-1}),POS_B) \tag{29}$$

由式(29)可知

$$\text{possess}(B,S(\text{new\_coins},K_{CS}^{-1})) \tag{30}$$

由初始假设集合 INI_S_B 可知

$$\text{canprove}(B,\text{authenticate}(K_{CS},CS)) \tag{31}$$

由式(30)(31)和 C 逻辑的签名规则 SR2,可得

$$\text{canprove}(B,\text{claims}(CS,\text{new\_coins})) \tag{32}$$

由于优化协议是匿名支付协议,对于收款方 B 而言,只需证明付款有效,即可认为可追性目标 G1 达到。

假定 $\text{in}(EOR,POS_A)$ 成立,即

$$\text{in}(S((\text{amount},\text{Tid},\text{date}),K_B^{-1})) \tag{33}$$

由式(33)可知

$$\text{possess}(A,S((\text{amount},\text{Tid},\text{date}),K_B^{-1})) \tag{34}$$

由初始假设集合 INI_S_A 可知

$$\text{canprove}(A,\text{authenticate}(K_{TTP},TTP)) \tag{35}$$

由拥有集合 $POS_A^1=POS_A^0\cup\{S((k_B,B),K_{TTP}^{-1})\}$ 可知

$$\text{possess}(A,S((k_B,B),K_{TTP}^{-1}))\wedge\text{possess}(A,K_{TTP}) \tag{36}$$

由式(35)(36)和 C 逻辑的身份证明规则 IAR2,可得

$$\text{canprove}(A,\text{authenticate}(k_B,B)) \tag{37}$$

由式(34)(37)和 C 逻辑的签名规则 SR1,可得

$$\text{canprove}(A,\text{claim}(B,(\text{amount},\text{Tid},\text{date}))) \tag{38}$$

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。

$$POS_B \xrightarrow{\text{初始拥有}} POS_B^0\cup POS_B^4 \xrightarrow{\text{接收消息(4)}} \{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1}\}\cup POS_B^3\cup\{E(S(\text{new\_coins},K_{CS}^{-1}),SK_B)\} \xrightarrow{\text{解密}} \{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1}\}\cup POS_B^2\cup\{E((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B)\}\cup\{E(S(\text{new\_coins},K_{cs}^{-1}),SK_B)\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1}E((S(\text{coins},K_{CS}^{-1})SK_A,K_{\_SES},S_{\_ID}),K_B),E(S(\text{new\_coins},K_{CS}^{-1}),SK_B)\} \xrightarrow{\text{解密}} \{SK_B,K_{CS},K_{\text{TTP}},K_{A\_B},K_A,K_B,K_B^{-1},S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID},S(\text{new\_coins},K_{CS}^{-1}),SK_B\} \tag{39}$$

由式(39)可得,$\text{in}(S(\text{new\_coins},K_{CS}{}^{-1}),POS_B{}^5)$,即

$$\text{in}(EOO,POS_B{}^5) \quad (G3)$$

$$POS_A \xrightarrow[\text{初始拥有}]{\text{接收消息(5)}} POS_A^0\cup POS_A^1\cup\{E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A)\} \xrightarrow[\text{接收消息(1)}]{} \{SK_A,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_A^{-1}\}\cup\{E(S((k_B,B),K_{\text{TTP}}^{-1}),K_{A\_B})\}\cup\{E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A)\}=\{SK_A,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_A^{-1},E(S((k_B,B),K_{\text{TTP}}^{-1}),K_{A\_B}),E((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A)\} \xrightarrow{\text{解密}} \{SK_A,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},S((k_B,B),K_{TTP}^{-1}),S((\text{amount},\text{Tid},\text{date}),K_B^{-1})\} \tag{40}$$

由式(40)可得,$\text{in}((S(\text{amount},\text{Tid},\text{date}),K_B^{-1}),POS_A^5)$,即

$$\text{in}(EOR,POS_A^5) \quad (G4)$$

综上即得,可追究性目标 G1 ~ G4 均成立。证毕。

2.4　公平性验证

步骤 1　给出公平性的形式化定义。

1)协议正常结束时,使用 C 逻辑可以将公平性目标形式化定义为

G1　$\text{in}(EOO,POS_B)$; G2　$\text{in}(EOR,POS_A)$

2)协议第 i 条语句中断执行时,使用 C 逻辑可以将公平性目标形式化定义为

G3　$\neg\ \text{in}(EOO,POS_B^{i-1})(i=1,2,3,4)$

G4　$\neg\ \text{in}(EOR,POS_A^{i-1})(i=1,2,3,4)$

步骤 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,可以得知,协议正常结束时,公平性目标满足。

2)协议异常终止

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 B 而言,当前三条语句执行中断时,即

当 $i=1$ 时,$POS_B^1=POS_B^0=\{SK_B,K_{CS},K_{TTP},K_{A\_B}\}$

当 $i=2$ 时,$POS_B^2=POS_B^1\cup\{E((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B)\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B^{-1},K_B\}\cup\{E((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B)\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},E((S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}),K_B)\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}\}$

当 $i=3$ 时,$POS_B^3=POS_B^2=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},S(\text{coins},K_{CS}^{-1}),SK_A,K_{\_SES},S_{\_ID}\}$

因此,当 $i=1,2,3$ 时,可得

$$\neg\ \text{in}(EOO,POS_B^i) \tag{41}$$

对 A 而言,当前三条语句执行中断时,即

当 $i=1$ 时,$POS_A^1=POS_A^0\cup\{E(S((k_B,B),K_{TTP}^{-1}),K_{A\_B})\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1}\}\cup\{E(S((k_B,B),K_{TTP}^{-1}),K_{A\_B})\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},E(S((k_B,B),K_{TTP}^{-1}),K_{A\_B})\}=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},S((k_B,B),$

$K_{TTP}^{-1})\}$

当 $i=2,3$ 时,$POS_A^2=POS_A^3=POS_A^1=\{SK_B,K_{CS},K_{TTP},K_{A\_B},K_A,K_B,K_B^{-1},S((k_B,B),K_{TTP}^{-1})\}$

因此,当 $i=1,2,3$ 时,可得

$$\neg\ \mathrm{in}(EOR,POS_A^i) \tag{42}$$

由式(41)和(42)得出,协议前三条语句中断时,公平性目标 G3 和 G4 均成立。即 *A* 和 *B* 都不占优势。证毕。

2.5　原子性验证

步骤 1　给出原子性的形式化定义。

使用 C 逻辑可以将原子性目标形式化定义为

GA1 ∨ A2

A1　$\neg\ \mathrm{in}(\text{new-coins},REV_B)\wedge\neg\ \mathrm{in}((\text{amount},\text{Tid},\text{date}),REV_A)$(当协议异常终止时)

A2　$\mathrm{in}(\text{new-coins},REV_B)\wedge\mathrm{in}((\text{amount},\text{Tid},\text{date}),REV_A)$(当协议正常结束时)

步骤 2　验证原子性目标。

利用 C 逻辑公理和推理规则,分析协议每条语句执行之后 *A* 和 *B* 接收消息的情况,用以验证原子性目标。

证明　协议前三条语句不含原子性目标中所含的内容,因此,只需要分析第(4)(5)条语句。

a)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。

b)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)。

$$\mathrm{believe}(B,\mathrm{receive}(B,E(S(\text{new\_coins},K_{CS}^{-1}),SK_B))) \tag{43}$$

由初始拥有集合 $POS_B^0=\{SK_B,K_{CS},K_{TTP},K_{A\_B}\}$ 可知

$$\mathrm{possess}(B,SK_B) \tag{44}$$

$$\mathrm{possess}(B,K_{CS}) \tag{45}$$

由式(43)(44)和 C 逻辑的密文理解规则 CCR1 可得

$$\mathrm{believe}(B,\mathrm{receive}(B,S(\text{new\_coins},K_{CS}^{-1}))) \tag{46}$$

由式(45)(46)和 C 逻辑的签名规则 SR1 可得

$$\mathrm{believe}(B,\mathrm{receive}(B,\text{new\_coins})) \tag{47}$$

即

$$\mathrm{in}(\text{new-coins},REV_B) \tag{48}$$

接下来,分析协议语句(5)。

$$\mathrm{believe}(A,\mathrm{receive}(A,E(S((\text{amount},\text{Tid},\text{date}),K_B^{-1}),SK_A))) \tag{49}$$

由初始拥有集合 $POS_A^0=\{SK_A,K_{CS},K_{TTP},K_{A\_B}\}$ 可知

$$\mathrm{possess}(A,SK_A) \tag{50}$$

由式(49)(50)和 C 逻辑的密文理解规则 CCR1 可得

$$\mathrm{believe}(A,\mathrm{receive}(A,S((\text{amount},\text{Tid},\text{date}),K_B^{-1}))) \tag{51}$$

由初始拥有集合 $POS_A^1=POS_A^0\cup\{S((k_B,B),K_{TTP}^{-1})\}$ 可知

$$\mathrm{believe}(A,\mathrm{possess}(A,S((k_B,B),k_{TTP}^{-1}))) \tag{52}$$

由初始拥有集合 $POS_A^0=\{SK_A,K_{CS},K_{TTP},K_{A\_B}\}$ 可知

$$\mathrm{possess}(A,K_{TTP}) \tag{53}$$

由(52)(53)和 C 逻辑的身份证明规则 IAR3 可得

$$\mathrm{believe}(A,\mathrm{authenticate}((k_B,B))) \tag{54}$$

由(51)(54)和 C 逻辑的签名规则 SR2 可得

$$\mathrm{believe}(A,\mathrm{receive}(A,(\text{amount},\text{Tid},\text{date}))) \tag{55}$$

即

$$\mathrm{in}((\text{amount},\text{Tid},\text{date}),REV_A) \tag{56}$$

由(48)和(56)可得出,原子性目标的子目标 A2 成立。

综合情况 a)和 b)可得出,协议满足原子性。证毕。

3　优化协议的性能分析

1)安全性讨论

本文 2.2 节给出了优化协议的形式化验证,验证表明,优化协议能够满足非否认性、可追究性、公平性和原子性目标。该协议与匿名电子现金支付协议 ISI 的比较表 4 所示。

表 4　优化协议与协议 ISI 的比较

协议	安全属性						
	密钥保密性	非否认性		可追究性	公平性		原子性
		EOO	*EOR*		*A*	*B*	
ISI 协议	否	是	否	否	否/劣势	否/优势	否
优化协议	是	是	是	是	是	是	是

2)鲁棒性分析

对 ISI 协议的分析[5~7]可以得出,当协议异常终止时,*B* 占据优势,而 *A* 处于劣势。优化的匿名电子现金支付协议引入 FTP 传输方式传送交易主体 *A* 和 *B* 的电子货币和付款收据,不仅确保了协议可追究性、公平性的实现,而且进一步增强了协议的鲁棒性。

4　结束语

针对现有文献指出的匿名电子现金支付协议 ISI 的缺陷,以及本文研究发现的缺陷,本文提出了该协议的优化协议,解决了上述缺陷。然而本文没有讨论协议其他安全属性的形式化验证,例如匿名性、时限性等。此问题可以通过提高 C 逻辑的分析能力加以解决。对协议更多的安全属性进行形式化验证是下一步的研究重点。

参考文献:

[1] 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 ComAnications Security. USA: ACM Press, 1993: 102-106.

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

[3] HERNANDEZ-ARDIETA J, GONZALEZ-TABLASA A, ALVAREZA B R. An optimistic fair exchange protocol based on signature policies [J]. Computers & Security,2008,27(7/8):309-322.

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

[5] 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.

[6] 周典苹,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.

[7] 刘义春, 张焕国. 电子商务协议的串空间分析[J]. 计算机科学, 2008,35(2):109-114.

[8] 陈莉. 电子商务安全协议的设计与分析[D]. 郑州:信息工程大学, 2009.

[9] CHEN Li, LI Xiang-dong. A novel micro-payment scheme for m-commerce based on self-renewal hash chains[C]//Proc of International Conference on Communications, Circuits and Systems Proc. Chengdu: UESTC Press, 2007.

[10] CHEN Li, JIANG Zhi-jun. Design and logical analysis of authenticated key exchange protocol[C]//Proc of the 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing. [S.l.]: IEEE Communications Society Press, 2008.