

SET 证书申请协议在 SPV 下的自动化验证及改进

肖茵茵¹⁾ 苏开乐^{1),2)} 岳伟亚¹⁾ 陈清亮³⁾ 吕关锋⁴⁾ 杨晋吉^{1),5)}

¹⁾(中山大学信息科学与技术学院广东省信息安全重点实验室 广州 510275)

²⁾(北京大学信息科学技术学院教育部高可信软件技术重点实验室 北京 100871)

³⁾(暨南大学计算机科学系 广州 510632)

⁴⁾(北京工业大学计算机学院 北京 100022)

⁵⁾(华南师范大学计算机学院 广州 510631)

摘 要 基于实例化空间逻辑理论,使用知识推理方法,在 SPV(Security Protocol Verifier)下对完整 SET 证书申请协议的秘密性、认证性等安全性质进行了完全自动化证明,并对协议进行了改进. SPV 调用工业级 SAT 求解器,能够高效验证安全协议是否满足 CAPSL(Common Authentication Protocol Specification Language)协议规范及单层、多层认知规范. 应用一个逻辑或工具对协议进行验证首先必须对该协议进行简化,而 SET 协议作为当前最复杂的工业级协议,其原始文档有上千页,因此简化过程相当困难,相关研究较少,已有的一些简化模型也不够完整. 因此,文章针对 SET 证书申请协议,给出了比以往更贴近原协议的简化模型,并详细阐述了该模型在 SPV 下的形式化描述及验证过程. 验证结果,分析了由于协议不满足某些认知规范所带来的安全隐患,从而对协议进行改进,最后证明了改进后协议的有效性. 该工作也充分说明了 SPV 足以处理复杂的工业级协议.

关键词 SET 证书申请协议;自动化验证;SPV;认证性;秘密性

中图法分类号 TP309

The Automatic Verification and Improvement of SET Certificate Registration Protocols with SPV

XIAO Yin-Yin¹⁾ SU Kai-Le^{1),2)} YUE Wei-Ya¹⁾ CHEN Qing-Liang³⁾
LU Guan-Feng⁴⁾ YANG Jin-Ji^{1),5)}

¹⁾(Key Laboratory for Information Security of Guangdong Province,

School of Information Science & Technology, Sun Yat-Sen University, Guangzhou 510275)

²⁾(Key Laboratory for High Confidence Software Technologies of Ministry of Education,

School of Electronics Engineering and Computer Science, Peking University, Beijing 100871)

³⁾(Department of Computer Science, Jinan University, Guangzhou 510632)

⁴⁾(College of Computer Science, Beijing University of Technology, Beijing 100022)

⁵⁾(School of Computer Science, South China Normal University, Guangzhou 510631)

Abstract Based on the Instantiation Space Logic theory and knowledge reasoning, the authors implement the totally automatic verification on the complete SET certificate registration protocols' authentication and secrecy properties using SPV, and improve the protocols. SPV can efficiently verify whether the security protocol satisfies the goals in CAPSL(Common Authentication Protocol Specification Language) as well as multi-level epistemic specifications using modern SAT solvers. All protocols should be simplified before being verified by logics or tools. As to the SET protocols, it is the most complex industrial protocol at present, which has the document of over

收稿日期:2007-07-12;最终修改稿收到日期:2008-01-22. 本课题得到国家“九七三”重点基础研究发展规划项目基金(2005CB321902)、国家自然科学基金(60496327,10410638,60473004)、广东省自然科学基金(06023195)和广东省自然科学基金团队项目(04205407)资助. 肖茵茵,女,1983年生,博士研究生,研究兴趣包括模型检测、模态逻辑、知识推理、安全协议验证等. E-mail: xyycx1983@163.com. 苏开乐,男,1964年生,博士,教授,博士生导师,研究兴趣包括模型检测、知识推理、非单调推理、模态逻辑、安全协议验证等. 岳伟亚,男,1985年生,博士研究生,研究兴趣包括模态逻辑、安全协议验证和逻辑程序设计等. 陈清亮,男,1980年生,博士,助教,研究兴趣包括模型检测、模态逻辑、安全协议验证和符号化算法等. 吕关锋,男,1973年生,博士,讲师,研究兴趣包括信息安全、算法分析与设计. 杨晋吉,男,1968年生,博士,副教授,研究兴趣包括网络协议的形式化验证与多媒体设计.

1000 pages. Therefore, it is very difficult to simplify and there are few research works about it. Besides, some existent simplified models are not complete enough. Consequently, the paper gives a simplified model which is more close to the original SET certificate registration protocols, and introduces the model's formal description in SPV with the verification process and results. Moreover, according to the hidden danger of the protocols brought by the unsatisfied epistemic specification, the authors improve the protocols and show the effectiveness. The work also justifies that SPV has the ability to deal with complex industrial protocols.

Keywords SET certificate registration protocols; automatic verification; SPV; authentication; secrecy

1 引 言

安全协议是在开放网络中借助密码体制达到密钥分配、身份认证、信息保密等特定目标的通信协议,其正确性对网络应用的安全至关重要.安全协议的手工分析十分困难,容易出错,所以研制高效、可靠的自动验证工具是当前安全协议研究的热点.

从协议分析的目的划分,安全协议的形式化验证方法可分为证伪法和证明法:前者的目标在于寻找协议的漏洞和潜在攻击的路径,后者用于验证协议是否能够满足某些安全性质以及证明协议的正确性.实例化空间逻辑是一个在 Dolev-Yao 模型下对安全协议进行形式化分析的基于证明的新方法^[1],该方法足以验证大规模工业级复杂协议的认证性、秘密性等相关安全性质.更重要的是,该逻辑中的公理集在算法上可完全实现,其相应的自动化验证工具为 SPV(Security Protocol Verifier).SPV 使用知识推理方法,调用 SAT 求解器,能够高效验证安全协议是否满足协议规范.

安全电子交易(Secure Electronic Transaction, SET)协议是 VISA 国际组织、MasterCard 国际组织联合开发,结合 GTE、IBM、Microsoft、Netscape、RSA、HP 等公司制定的电子商务中安全电子交易的一个国际标准,是目前最复杂的电子支付系统规范^[1].SET 协议是一个协议簇,其主要部分为证书申请协议和支付协议.SET 证书申请协议的目标是使持卡人、商家和支付网关分别获得由可信任的认证中心认证的证书.证书绑定了交易实体与其公钥,在稍后的支付阶段中使用证书能够加强认证性.

由于 SET 协议具有很高的复杂性,因此能否验证该协议成为衡量一个安全协议验证理论或工具能否处理复杂工业级协议的标准.该协议已通过模型检测的分析^[3-5]或通过半自动的方式如定理证明器

Isabelle^[6-9]得到证明,但首先实现对完整 SET 协议的秘密性、认证性等安全性质的完全自动化证明的工具是 SPV.一般而言,验证复杂工业级协议的步骤为抽象简化协议步,形式化描述协议,人工/自动验证协议,根据结果对协议进行分析或改进,即简化协议,它是协议验证的首要步骤.而 SET 协议的原始文档多达上千页^[2],因此简化过程相当困难,相关研究较少,已有的一些简化模型也不够理想,例如提出的攻击在实际中不存在^[4],未直接描述异或操作^[10],没有引入与异或原语相关的定理^[6-9]等.因此,我们针对 SET 证书申请协议的简化做了大量工作.本文中,我们给出了比以往更完整、更贴近原协议的简化模型,详细介绍了该协议在 SPV 下的形式化描述及验证过程、验证结果,分析了由于协议不满足某些认知规范所带来的安全隐患,从而改进协议,并用 SPV 证明了改进后协议的有效性(SET 支付协议的验证将在另外的文章中介绍).我们之前的文章中^[1,11]并未详细讨论 SPV 对大型协议的验证过程,作为补充,本文工作正充分说明 SPV 足以处理复杂的工业级协议.

本文第 2 节首先给出实例化空间逻辑和 SPV 工具的简单介绍;第 3 节介绍了建立协议模型时的化简规则;第 4、5 节分别阐述了 SET 持卡人证书申请协议和商家/支付网关证书申请协议简化模型在 SPV 下的描述、验证和改进;第 6 节为 SPV 验证这两个协议的效率分析;第 7 节为相关工作的比较;第 8 节为结论.

2 实例化空间逻辑与 SPV

为便于理解,本节将对实例化空间逻辑与 SPV 作简单介绍,关于本节内容的详细论述可参见文献^[1],本文未特别说明的符号和术语均与文献^[1]一致.

2.1 实例化空间逻辑

安全协议中的一切数据都可以看成消息. 实例化空间的消息代数 (M, K) 归纳定义了消息的概念和特性. 在消息代数的基础上, 又定义了一个加密消息交换 (CME) 模型 $\Sigma = (M, K, e, Ag, Pk, Sk, Stamp, Nonce, Init, Recv, Sent)$, 用于说明智能体之间如何进行加密消息的交换. 另一方面, 还需要对协议进行形式化描述. 原子消息符号集描述了协议中的所需信息, 安全协议 P 则表示为由原子消息符号集和协议体构成的多元组. P 中所有消息符号用 MSG_P 来表示. 协议中的各个角色都有自己的局部协议, 用于刻画与自身有关的行为.

协议角色的行为与具体智能体的动作通过实例化函数联系起来. 对于一个协议 P 和 CME 模型 Σ , 二元组 (ρ, c) 表示以随机数或时戳 c 为标识消息的智能体 ρ 的局部运行. 对于每个局部运行 (ρ, c) , 可以定义一个消息赋值函数: $f: MSG_P \rightarrow M$. 对于每个 $M \in MSG_P$, $f(M)$ 是在 P 中的局部运行 (ρ, c) 中扮演协议所定义的 M 的具体消息. 若 f 描述了局部运行 (ρ, c) 中智能体 ρ 的动作与角色 A 的行为间的对应关系, 则 f 为 A 的实例化函数.

实例化空间是一个基于实例化函数和 CME 模型的安全协议验证逻辑语义模型. 一个实例化空间是一个多元组 $\Omega = (\Sigma, F, S)$: Σ 是 CME 模型, F 是实例化函数集合, S 是关于智能体 Ag 行为的假设集.

实例化空间逻辑是以实例化空间为语义模型的逻辑理论 Θ_P . Θ_P 提供了一组尽可能完备的纯命题逻辑的公理模式, 其中最重要的公理为角色假设定理和 $(n, 1)$ -Secrecy 定理. 这些公理比现有的一些验证逻辑刻画了更一般的情形, 可有效地对协议安全性质进行验证.

2.2 SPV 工具

验证协议所用工具 SPV 是本研究组基于上述理论开发出来的自动化安全协议工具, 可验证复杂的工业级的安全协议性质. 其中, 秘密性被转化为 CAPSL^[12] 的“SECRET”规范; 认证性被转化为 CAPSL 语言的“PRECEDES”规范及各种单层和多层认知规范.

SPV 的语法和语义将在另外的文章中介绍 (参阅 <http://www.cs.sysu.edu.cn/~skl/spv.htm>). 这里为叙述方便, 简单介绍其主要组成部分:

macro (宏定义部分): 用户可以根据消息的结构定义宏, 方便输入大型协议.

variable (协议常规变量定义部分): 定义了 CME 模型的具体消息集 M 中的变量以及协议 P 的

消息符号集 MSG_P 中的变量. 例如: “agent: ρ ” 表示 ρ 为智能体类型; “agent_term: A ” 表示 A 为主体消息符号类型, 即协议角色.

initialize (实例化部分): 定义了实例化函数, 将 # variable 部分的消息符号变量实例化成具体消息. 例如: “name(ρ, A)” 表示将智能体 ρ 实例化为 A , 即 ρ 将扮演协议角色 A .

protocol (协议主体部分): 刻画了协议执行步骤. 其中 $cryp(k, (m))$ 表示用 k 对 m 加密, 这里 k 可以是公钥、私钥、共享密钥、动态密钥、Hash 函数和 Xor 函数.

role_assumption (角色假设部分): 描述了角色假设定理, 刻画智能体在协议中扮演角色的条件假设. 例如: “sees(ρ, c) + said(ρ, c) > role(ρ, c, A)” 表示若智能体 ρ 看到或说过标识消息 c , 则可推出 ρ 在局部运行 (ρ, c) 中扮演了角色 A (符号 + 表示析取, > 表示蕴含).

define (假设集定义部分): 定义实例化空间 Ω 的假设集 F , 不同的假设下可能会有不同的验证结果.

goal (CAPSL 规范定义部分): 定义 CAPSL 规范. 如 “secret N ” 表示消息符号 N 是秘密的, 若 N 由角色 A 产生, 则该规范在实例化空间逻辑中可表示为

$$(reach(\rho, c, A, l_A) \wedge (\bar{P}_1^{\rho, c} = \rho_1) \wedge \cdots \wedge (\bar{P}_n^{\rho, c} = \rho_n) \wedge (\bar{N}^{\rho, c} = c)) \Rightarrow secr(\rho, \rho_1, \dots, \rho_n, \bar{N}^{\rho, c}).$$

“precedes $P: Q | N, M$ ” 表示在角色 Q 的最后状态, 若有扮演 Q 的智能体拥有 P, N, M , 则也有一个扮演角色 P 的智能体拥有同样值的 Q, N, M . 该规范在实例化空间逻辑中可表示为

$$(reach(\tau, c_2, Q, l_Q) \wedge (\bar{P}^{\tau, c_2} = \rho) \wedge (\bar{N}^{\tau, c_2} = c_1)) \Rightarrow (role(\rho, c_1, P) \wedge (\bar{Q}^{\rho, c_1} = \tau) \wedge (\bar{N}^{\rho, c_1} = c_1) \wedge (\bar{M}^{\rho, c_1} = \bar{M}^{\tau, c_2})).$$

specification (认知规范定义部分): 定义单层或多层认知规范. 例如 “know($\rho, said(\tau, m)$)” 表示智能体 ρ 知道智能体 τ 说过消息 m . 用户可以在 # goal 和本部分定义需要验证的安全性质.

验证协议时, SPV 首先根据变量、实例化函数和假设集, 生成实例化空间, 再根据协议步骤生成实例化空间逻辑中的所有公理集, 最后将公理集与要验证的规范转化成可满足性问题 (SAT), 调用快速高效的工业级 SAT 求解器求解, 最后输出结果.

3 SET 证书申请协议抽象规则

SET 协议是当前最复杂的工业级协议, 例如为

保证安全性,协议使用了层层嵌套的各种加密技术:对称和非对称加密体制保证了协议的秘密性;数字签名体制保证了协议的认证性;Hash 函数与数字信封体制保证了消息的完整性^[13]. 因此,要验证 SET 证书申请协议,首先要对其进行合理的抽象简化.

3.1 加密消息简化规则

SET 协议中,EXH 加密函数 $EXH(r, M, m) = \{\{M, H(m)\}_K, \{K, m, H(M)\}_{pubEK_r}\}$ 表示主体 r 使用对称密钥 K 对消息 M 、消息 m 的 Hash 值 $H(M)$ 进行加密,再用其公钥 $pubEK_r$ 对 K 、 m 、 M 的 Hash 值 $H(M)$ 进行加密,从而保证了 M 、 m 的秘密性和完整性. 在 Dolev-Yao 模型下,有所有加密都为完美加密(perfect encryption)且长期密钥安全的基本假设,而实例化空间逻辑基于 Dolev-Yao 模型,因此有命题 1.

命题 1. \forall 安全协议 P , 设 P' 为用 $\{M, m\}_{pubEK_r}$ 替换 P 中所有形如 $\{\{M, H(m)\}_K, \{K, m, H(M)\}_{pubEK_r}\}$ 的消息得到的协议, Ω, Ω' 分别为 P, P' 的实例化空间, 则 $(\Omega \models \text{secret}(M, m)) \Rightarrow (\Omega' \models \text{secret}(M, m))$. 其中 secret 为 SPV 定义下的 CAPSL 规范.

命题 1 说明经过消息替换后的协议仍能保持同样的秘密性. 这一命题的合理性是由 Dolev-Yao 模型的上述基本假设保证的^[6-9], 根据文献[1]中的定理不难验证该命题的正确性, 由于篇幅所限, 这里不再赘述. SPV 主要用于验证协议的秘密性和认证性, 因此根据命题 1 可将协议描述中所有形如 $\{\{M, H(m)\}_K, \{K, m, H(M)\}_{pubEK_r}\}$ 的消息简化为 $\{M, m\}_{pubEK_r}$.

3.2 证书内容简化规则

协议运行过程中,为持卡人、商家和支付网关颁发证书的认证中心需要使用由根认证中心签名的加密证书和签名证书证明自己的身份. 另外,在实际中证书通常包括了证书版本号、有效期限等辅助内容. 实际上,加密证书和签名证书的区分以及证书的辅助内容在分析协议的认证性、秘密性时并不重要,因此在本文的证书描述中,合并了认证中心的加密密钥对(证书)和签名密钥对(证书),省略了证书中的辅助内容,并根据命题 1 简化了证书.

3.3 异或原语保留规则

与文献[1]比较,本文采用的理论与工具增加了对异或原语 XOR 的处理. 设 $M_1 \oplus M_2 \in \text{Recg}(Q, l)$, 则与 XOR 相关的部分主要定理如下.

命题 2(poss 命题).

$$\models_p \text{reach}(\tau, c, Q, l) \wedge \text{poss}(\rho, \overline{M_1 \oplus M_2}^{\tau, c}) \wedge$$

$$\text{poss}(\rho, \overline{M_2}^{\tau, c}) \Rightarrow \text{poss}(\rho, \overline{M_2}^{\tau, c}).$$

命题 3(seeing 命题).

$$\models_p \text{reach}(\tau, c, Q, l) \wedge \text{sees}(\rho, \overline{M_1 \oplus M_2}^{\tau, c}) \wedge \text{poss}(\rho, \overline{M_2}^{\tau, c}) \Rightarrow \text{sees}(\rho, \overline{M_1}^{\tau, c}).$$

命题 4(saying 命题).

$$\models_p \text{reach}(\tau, c, Q, l) \wedge \text{said}(\rho, \overline{M_1 \oplus M_2}^{\tau, c}) \wedge \text{poss}(\rho, \overline{M_2}^{\tau, c}) \Rightarrow \text{said}(\rho, \overline{M_1}^{\tau, c}).$$

命题 2 描述了智能体 ρ 如何从异或消息 $M_1 \oplus M_2$ 出发拥有消息 M_1 ; 命题 3、命题 4 分别描述了 ρ 如果看到或说过了 $M_1 \oplus M_2$, 则它也看到或说过了 M_1 . 对 M_2 也有类似的命题.

$M_1 \oplus M_2$ 在 SPV 下描述为 $\text{cryp}(\text{xor}, (M_1, M_2))$. 因为能够直接处理异或原语, 所以本文在描述 SET 证书申请协议时采取保留异或原语的规则.

4 SET 持卡人证书申请协议的验证

4.1 协议主要步骤

本协议目标是持卡人 C 从认证中心 CCA 处获得签名证书. 首先, C 将证书申请初始请求 $CardCInitReq$ 发送给 CCA , 并得到 CCA 的应答 $CardCInitRes$; C 再发送注册表请求 $RegFoemReq$ 给 CCA , CCA 将包含注册表模板的 $RegFoemRes$ 发回给 C ; 最后, C 将正确填写的注册表以及新公钥放入 $CertReq$, 发送给 CCA , CCA 生成该公钥的证书并放入 $CertRes$, 发送给 C .

4.2 SPV 下的形式化描述

4.2.1 变量定义

本协议在 SPV 中的部分变量定义如下:

```
# variable
agent: cardholder, authority, rootauthority;
agent_term: C, CCA, RCA;
nonce: ..., cardholder_secret, authority_secret;
nonce_term: ..., CardSecret, CASecret;
publicKey_term: kca, kc, krca;
privateKey_term: _kca, _kc, _krca;
dynamicKey_term: kcca;
generalMessage_term: PAN;
```

其中, 智能体 $cardholder$ 、 $authority$ 、 $rootauthority$ 将在协议中分别扮演持卡人 C 、持卡人认证中心 CCA 、根认证中心 RCA 的角色; 除了协议通信中所需的随机数以外, 为保证新鲜性, 生成证书时所需的秘密变量 $CardSecret$ 、 $CASecret$ 也被设为 nonce 类型; kca 、 kc 、 $krca$ 与 $_kca$ 、 $_kc$ 、 $_krca$ 分别为 CCA 、 C 、 RCA 的公钥、私钥符号, 其中 kc 即为持卡人要绑定

在证书中的公钥符号; $kcca$ 为持卡人动态生成的密钥符号,用于加密协议最后一步中的秘密变量;持卡人帐号 PAN 是长期有效的消息符号,并且可能为组合消息符号,因此在 SPV 中被设为普通消息符号.

注 1. 这里无需显式地对攻击者进行描述,因为在实例化空间逻辑中攻击者和不诚实智能体被归入协议运行环境 e .

4.2.2 实例化

实例化部分给出了协议角色行为与具体智能体动作的映射关系. 协议的部分实例化过程如下:

```
# initialize
name(cardholder, C);
name(cardholder_secret, CardSecret);
nonce(C, CardSecret);
inverse_key(C, kc, _kc);
inverse_key(CCA, kca, _kca);
inverse_key(RCA, krca, _krca);
dynamic_key(C, kcca);
initial_general_message(PAN, C);
...
```

注 2. SET 证书申请协议的目标是为实体的新公钥颁发证书,所以与普通协议不同,该协议中除 RCA 的非对称密钥外,其他实体的非对称密钥可能在协议运行过程中动态建立;每个实体还可能有多 个密钥对,不管这些密钥是否经过认证. 因此,文献[9]中没有在初始化时绑定智能体(除了 RCA)和其密钥对,而是动态生成公钥并发送. 但是,要认证的公钥与其对应的私钥本质上是长期密钥,即使是动态生成,实体在协议本次执行时仍认定它们为当前的非对称密钥对,因此 SPV 仍然在实例化时绑定智能体及其密钥对. 文献[9]的后继版本文献[6-7]中,也采用了绑定的方法.

4.2.3 证书

在 SPV 下,证书都处理为宏形式.

(1) 根据证书内容化简规则,可得 CCA 的证书:

$$CertCA=cryp(_krca,(CCA,kca));$$

(2) 持卡人申请的证书是签名证书. 为保证持卡人帐号 PAN 的秘密性, CCA 签名的证书中包含的是 PAN 与秘密变量 $PANSecret$ 的 Hash 值,而 $PANSecret=CardSecret\oplus CASecret$. $CardSecret$ 、 $CASecret$ 分别为 C 、 CCA 生成的秘密变量. 经简化, C 的签名证书为

$$CertC=cryp(_kca,(cryp(hash,(PAN,cryp(xor,(CardSecret,CASecret))))),kc));$$

注 3. $CertCA$ 和 $CertC$ 中直接对明文进行签名,而不是对其摘要进行签名的原因是在实际中明

文通常更复杂,这将使证书更难被破解.

4.2.4 协议体

经简化,SET 持卡人证书申请协议在 SPV 中可描述为以下 6 步:

```
# protocol
C,CCA: C,Chall_C1;
CCA,C: cryp(\_kca,(C,Chall_C1)),CertCA;
C,CCA: cryp(kca,(C,Chall_C2,PAN));
CCA,C: cryp(\_kca,(C,Chall_C2,Chall_CA)),
CertCA;
C,CCA: cryp(kca,(C,Chall_C3,kcca,kc,PAN,
CardSecret,cryp(\_kc,cryp(hash,(C,
Chall_C3,kcca,kc,PAN,CardSecret)))));
CCA,C: cryp(kcca,(cryp(\_kca,(C,Chall_C3,CCA,
CASecret)),CertC,CertCA));
```

其中, CCA 向 C 发送消息时都会出示 $CertCA$ 证书表明身份. 前 4 步为初始化与注册表的请求应答,第 5、第 6 步为协议的核心部分: C 填写注册表后,动态生成 $kcca$,将 PAN 、 $CardSecret$ 、 kc 、 $kcca$ 签名加密,发回给 CCA ; CCA 再生成认证 kc 的 $CertC$,并对 $CASecret$ 签名,与证书一起用 $kcca$ 加密后发回给 C . 这样 C 就能用 $CASecret$ 检验收到的证书是否有效. 第 6 步中使用 $kcca$ 加密,而不用 C 的公钥 kc 加密的原因是在协议本次运行结束前 kc 还未获得认证.

4.2.5 角色假设

本协议的部分角色假设描述如下:

```
# role_assumption
sees(cardholder,cardholder_secret)+said(cardholder,
cardholder_secret)>role(cardholder,cardholder_secret,C);
sees(authority,cardholder_secret)+said(authority,
cardholder_secret)>role(authority,cardholder_secret,CCA);
...
```

4.2.6 安全性质

在描述与验证安全性质前,可根据需要为实例化空间语义模型定义不同的智能体行为假设. 在本协议的验证中,我们设定 $Supp_3^{\rho,P}$ 假设和原子表达式 $norm$ 成立,即假设扮演角色 P 的智能体 ρ 的局部运行都能完成,而且这是协议中所有通信智能体的公共知识^[1]. 这一假设的 SPV 语言描述如下:

```
# define
normal_state=1;
(1) 秘密性
```

本协议需要保证持卡人帐号 PAN 和 $PANSecret$ 的秘密性,而 $PANSecret$ 的秘密性又由 $CardSecret$ 和 $CASecret$ 的秘密性保证. 这一性质在 SPV 中描述为

```
# goal
secret PAN;
secret CardSecret;
secret CASecret;
```

(2) 认证性

使用 CAPSL 的 PRECEDES 规范与单层、多层等认知规范,该协议的认证性在 SPV 中的部分描述如下:

```
# goal
precedes C: CCA|Chall_C1,PAN;
precedes CCA: C|Chall_C1,PAN;
...

# specification
know(cardholder,(role(authority,chall_authority,CCA)));
know(cardholder,(equal(local(authority,chall_authority,PAN),local(cardholder,chall_authority,PAN))));
know(cardholder,known(authority,(said(cardholder,authority_secret))));
...
```

其中,“precedes C: CCA | Chall_C1, PAN”表示在 CCA 的最后状态,若有扮演 CCA 的智能体拥有 C、Chall_C1、PAN,那么也有一个扮演 C 的智能体拥有同样值的 CCA、Chall_C1、PAN;形如“know(cardholder,(role(authority,chall_authority,CCA)))”的单层认知规范则表示在局部运行(chall_authority,authority)下,cardholder 知道 authority

在协议中扮演了角色 CCA;而形如“know(cardholder,(equal(local(authority,⋯))))”的规范表示 cardholder 知道在局部运行(chall_authority,authority)与(chall_authority,cardholder)中的 PAN 相同,这类规范更直观地描述了消息匹配,对认证性十分重要;形如“know(cardholder,known(authority,⋯))”的多层认知规范表示 cardholder 知道 authority 知道 cardholder 说过消息 authority_secret,因为涉及到不同智能体间的知识推理,所以这种嵌套的认知规范具有更强的认证性.

注 4. 在 SET 证书申请协议中,同一个 CA 颁发的证书与被认证的密钥是一一对应的,因此为了验证证书的唯一性,文献[6-7,9]中将 CA 发出的所有对同一个密钥进行认证的证书视为同一个消息.在本文的分析中,我们认为证书唯一性的判别是 CA 内部数据库检测和管理的责任,与协议本身不直接相关,因此省略了这一性质的描述和验证.

4.3 验证结果

实验运行在 2.00GHz CPU,1.00GB DDR 内存,Redhat Linux 7.0(gcc 3.2.2)的 PC 上.原持卡人证书申请协议的部分验证结果如表 1 所示.

为方便起见,表 1 中用形如“K_{card}said(auth,⋯)”的记法表示“cardholder 知道⋯”的单层认知规范;“K_{card}(⋯=⋯)”表示“cardholder 知道⋯与⋯相同”的消息匹配规范;“K_{card}K_{auth}⋯”表示“cardholder 知道 authority 知道⋯”的多层认知规范.

表 1 持卡人证书申请协议与改进后协议的验证结果

安全性质	原验证结果(时间/s)	改进验证结果(时间/s)
K _{card} said(auth,chall_card1)	Yes (2.03)	Yes (1.16)
K _{auth} said(card,chall_auth)	No (2.05)	Yes (1.18)
K _{card} role(auth,chall_auth,CCA)	Yes (2.04)	Yes (1.16)
K _{auth} role(card,chall_auth,C)	No (2.04)	Yes (1.17)
K _{card} (local(auth,chall_auth,PAN)=local(card,chall_auth,PAN))	Yes (2.04)	Yes (1.17)
K _{auth} (local(auth,chall_auth,PAN)=local(card,chall_auth,PAN))	No (2.04)	No (1.16)
K _{card} (local(auth,chall_auth,CardSecret)=local(card,chall_auth,CardSecret))	No (2.04)	Yes (1.17)
K _{auth} (local(auth,chall_auth,CardSecret)=local(card,chall_auth,CardSecret))	No (2.07)	Yes (1.18)
K _{card} (local(auth,chall_auth,CASecret)=local(card,chall_auth,CASecret))	No (2.03)	Yes (1.16)
K _{auth} (local(auth,chall_auth,CASecret)=local(card,chall_auth,CASecret))	No (2.03)	No (1.17)
K _{card} K _{auth} said(card,chall_card1)	No (114.15)	No (48.45)
K _{auth} K _{card} said(auth,chall_auth)	No (109.88)	No (47.33)
secret PAN	No (382.81)	No (197.03)
secret CardSecret	Yes (476.48)	Yes (238.91)
secret CASecret	Yes (594.14)	—
precedes C: CCA Chall_CA,PAN	No (2.04)	No (1.15)
precedes CCA: C Chall_CA,PAN	Yes (2.03)	Yes (1.17)
precedes C: CCA Chall_CA,CardSecret	No (2.03)	No (1.14)
precedes CCA: C Chall_CA,CardSecret	Yes (2.04)	Yes (1.14)
precedes C: CCA Chall_CA,CASecret	No (2.05)	—
precedes CCA: C Chall_CA,CASecret	Yes (2.05)	—

表 1 的原协议验证结果显示 SPV 证明了 *CardSecret* 和 *CASecret* 的秘密性,但未证明 *PAN* 的秘密性.在 SPV 下,安全性质未被证明的原因有两种:(1)协议本身存在潜在的攻击,导致安全性质不能被满足;(2)实例化空间逻辑的公理系统未足够完备来证明该性质,而不是系统有错误,此时只需增加相应公理即可.在目前的协议形式化模型下,我们尚未发现能够破坏 *PAN* 秘密性的潜在攻击;因此为实例化空间逻辑的公理系统增加保持秘密性的相关定理,从而证明 *PAN* 的秘密性将是我们下一步的工作.

表中还显示 SET 持卡人证书申请协议的认证性很难保证.这是因为该协议与普通协议不同,在 *CCA* 收到 *C* 发送的公钥之前,*C* 不能对消息签名,因为此时 *CCA* 无法用公钥对 *C* 的签名消息进行解密:例如协议第 3 步就不是一个签名消息,无法保证消息由 *C* 发出.另外,主体应答时一些参数是否包含在消息中是可选的^[2],造成了某些认证性的难以确定.这与证书申请协议的设计目的相关:SET 协议假定申请证书的主体都是诚实的,主体发送注册表,通过注册表中的个人信息向 *CCA* 表明身份,而 *CCA* 在协议外验证主体身份;协议不排斥持卡人重复发出请求或运行次数的不匹配,只要攻击者无法将自己的密钥与持卡人帐号绑定,或盗取持卡人信息即可.

在其他相关研究中,同样给出 SET 证书申请协议实际验证结果的工作主要有文献[5]和文献[6-9].其中,文献[5]使用 AVISS 模型检测工具验证出协议的认证性不足,但其并未讨论协议中 *CardSecret* 等关键消息的秘密性;文献[6-9]使用定理证明器 Isabelle 证明了协议满足秘密性要求,也提出了协议在认证性方面存在问题,但他们并未给出关于认证性的具体验证结果.而从表 1(以及下文中的表 2)可以看出,我们比较完整地分析了 SET 证书申请协议的秘密性和认证性,并且该验证过程是全自动的.

4.4 协议改进

4.4.1 问题 1

无论协议的目的如何,加强协议的认证性总能在实际中加强协议的安全性.例如在持卡人证书申请协议中, $K_{auth}role(card, chall_auth, C)$ 规范不被满足,将导致协议第 5 步中 *CCA* 不知道 *C* 是之前与之通信的 *C*,因此在第 5 步可能有其他 *C'* 插入运行协议,取代 *C* 最后获得证书:

$CCA, C: cryp_kca, (C, Chall_C2, Chall_CA), CertCA;$

$C', CCA: cryp(kca, (C', Chall_C3', kcca', kc', PAN', CardSecret', cryp_kc', cryp(hash, (C', Chall_C3', kcca', kc', PAN', CardSecret'))))));$

...

4.4.2 问题 2

原协议中 *PANSecret* 由异或 \oplus 产生,异或的特性可能使不诚实的 *CCA* 为所有帐户生成同一个 *PANSecret*,从而失去秘密性:若 $CASecret = CardSecret \oplus N$,则 $PANSecret = CardSecret \oplus CardSecret \oplus N = N$.另外,协议第 6 步使用动态密钥 *kcca* 加密消息,这种短期密钥一旦泄漏,将使 *CASecret* 失去秘密性^[6-7].

4.4.3 改进

若在第 5 步中,*C* 将第 4 步中收到的 *Chall_CA* 一并发送给 *CCA*,*CCA* 即可确认 *C* 的身份,解决问题 1.SET 原协议中,*Chall_CA* 是否要发回给 *CA* 其实是可选的.由上面的分析可看到 SET 的参数可选择性可能会带来一些安全性的问题.另外,在协议第 2,3 步中也可类似增加应答机制加强认证性,这里将其省略.

问题 2 的一个解决方法是省略 *CASecret*,用 *hash* 代替异或操作,直接对 *CardSecret* 加密生成 *PANSecret*.这样在协议第 6 步中,*CCA* 不必传输 *CASecret* 给 *C*,还可省略外层的 *kcca* 加密以及第 5 步中动态生成的 *kcca*,简化了协议.

综上所述,改进后的 *CertC* 证书为

$CertC = cryp_kca, (cryp(hash, (PAN, cryp(hash, CardSecret))), kc));$

改进后协议的第 5、6 步为

$C, CCA: cryp(kca, (C, Chall_C3, Chall_CA, kc, PAN, CardSecret, cryp_kc, cryp(hash, (C, Chall_C3, Chall_CA, kc, PAN, CardSecret)))));$
 $CCA, C: cryp_kca, (C, Chall_C3, CCA), CertC, CertCA;$

改进后的持卡人证书申请协议部分验证结果如表 1 所示.在秘密性方面,“secret *CardSecret*”等安全性质仍被满足,说明协议改进后不影响秘密性,同时避免了问题 2;在认证性方面,一些原先不被满足的单层认证规范在改进后的协议中被满足,说明协议改进后加强了认证性.例如,“ $K_{auth}role(card, chall_auth, C)$ ”为真表示 *authority* 知道是 *cardholder* 在整个协议运行中扮演了角色 *C*,因此由于认证性不足产生的问题 2 将不再存在.但要指出的是,由于协议本身设计目标的原因,协议改进后仍不能完全满足双层认证规范等强认证性^[9].

5 SET 商家/支付网关证书 申请协议的验证

5.1 协议主要步骤

SET 商家/支付网关证书申请协议比持卡人证书申请协议简单,以商家为例,其目标是商家 M 从商家认证中心 MCA 处获得加密证书和签名证书.首先, M 发送申请获得证书注册表的初始请求 $Me-AqCInitReq$ 给 MCA ,并得到包含注册表模板的应答 $Me-AqCInitRes$;之后 M 将正确填写的注册表单以及新公钥(包括加密公钥和验证签名的公钥)放入 $CertReq$,发送给 MCA , MCA 对公钥生成加密证书和签名证书,放入 $CertRes$ 发回给 M .

5.2 SPV 下的形式化描述

该协议在 SPV 下的描述与 4.2 节类似.由于篇幅所限,这里只介绍部分描述.

智能体 $merchant$ 、 $authority$ 、 $rootauthority$ 在协议中分别扮演商家 M 、商家认证中心 MCA 、根认证中心 RCA 的角色; kca 、 $krca$ 与 $_kca$ 、 $_krca$ 分别为 MCA 、 RCA 的密钥符号, ksm 、 kem 与 $_ksm$ 、 $_kem$ 分别为 M 要绑定在证书中的加密公钥和验证签名

公钥符号;注册表单 $Form$ 是普通消息符号.由于商家的签名和加密采用了不同的密钥对,所以需要分别申请加密证书 $CertEM$ 和签名证书 $CertSM$,而且证书中不含帐号等秘密消息:

```
CertSM=cryp(_kca,(M,ksm));
CertEM=cryp(_kca,(M,kem));
经简化,协议在 SPV 中可以描述为以下 4 步:
# protocol
M, MCA: M, Chall_M1;
MCA, M: cryp(_kca,(M, Chall_M1, Chall_CA,
Form)), CertCA;
M, MCA: cryp(kca,(M, Chall_M2, ksm, kem,
cryp(_ksm, cryp(hash,(M, Chall_M2,
ksm, kem)))));
MCA, M: cryp(_kca,(M, Chall_M2, MCA)),
CertSM, CertEM, CertCA;
```

由于 MCA 颁发的证书不含秘密消息,所以协议第 4 步无需用动态密钥加密^[2].

5.3 验证结果

原商家/支付网关证书申请协议的部分验证结果如表 2 所示.结果显示注册表 $Form$ 不满足秘密性,因为 $Form$ 传输时未被加密.另外,与持卡人证书申请协议类似,本协议的认证性也很难保证.

表 2 商家/支付网关证书申请协议与改进后协议的验证结果

安全性质	原验证结果(时间/s)	改进验证结果(时间/s)
$K_{mer}said(auth, chall_mer2)$	Yes (0.24)	Yes (0.24)
$K_{auth}said(mer, chall_auth)$	No (0.24)	Yes (0.24)
$K_{mer}role(auth, chall_auth, MCA)$	Yes (0.24)	Yes (0.24)
$K_{auth}role(mer, chall_auth, M)$	No (0.24)	Yes (0.24)
$K_{mer}(local(auth, chall_mer2, Form)=local(mer, chall_mer2, Form))$	No (0.24)	Yes (0.24)
$K_{auth}(local(auth, chall_mer2, Form)=local(mer, chall_mer2, Form))$	No (0.24)	No (0.24)
$K_{mer}K_{auth}said(mer, chall_mer2)$	No (4.69)	No (4.8)
$K_{auth}K_{mer}said(auth, chall_auth)$	No (4.73)	No (4.76)
secret $Form$	No (28.17)	No (29.13)
precedes $M; MCA Chall_M1, Form$	No (0.24)	No (0.24)
precedes $MCA; M Chall_M1, Form$	No (0.23)	Yes (0.24)

5.4 协议改进

5.4.1 问 题

与 4.4.1 节的问题 1 类似,协议规范 $K_{mer}role(mer, chall_auth, M)$ 在商家/支付网关证书申请协议中不被满足,将导致协议第 3 步中 MCA 不知道 M 是之前与之通信的 M . 商家的证书无需与帐号绑定,而且注册表未加密,所以攻击者 M' 可用自己的公钥填写注册表,获得假证书,在支付协议的交易中假扮商家 M 而获利:

```
M, MCA: M, Chall_M1;
MCA, M: cryp(_kca,(M, Chall_M1, Chall_CA,
Form)), CertCA;
```

```
M', MCA: cryp(kca,(M, Chall_M2', ksm', kem',
cryp(_ksm', cryp(hash,(M, Chall_M2',
ksm', kem')))));
MCA, M': cryp(_kca,(M, Chall_M2', MCA)),
CertSM', CertEM', CertCA;
```

其中,

```
CertSM'=cryp(_kca,(M,ksm'));
CertEM'=cryp(_kca,(M,kem'));
```

5.4.2 改 进

若在第 3 步中, M 将第 2 步中收到的 $Chall_CA$ 一并发送给 MCA , MCA 即可确认 C 的身份,解决上述问题.改进后协议的第 3 步为

$M, MCA; \text{cryp}(kca, (M, Chall_M2, Chall_CA, ksm, \\ kem, \text{cryp}(ksm, \text{cryp}(\text{hash}, (M, Chall_M2, \\ Chall_CA, ksm, kem)))));$

改进后的协议部分验证结果如表 2 所示:协议改进后在一定程度上加强了认证性。

6 验证效率分析

SET 证书申请协议在 SPV 下的验证效率见表 3. 验证时间以秒为单位。

表 3 SET 证书申请协议在 SPV 下的验证效率

协议名称	生成 变量数	生成 定理数	生成 时间
原协议(持卡人)	196038	415740	408447
改进协议(持卡人)	121975	237141	135628
原协议(商家/支付网关)	33630	47874	5319.13
改进协议(商家/支付网关)	33630	48111	5065.77

从表 1~表 3 中可以看出,SPV 验证一个协议时,大部分时间用于产生变量和定理,而验证安全性质只需要很少时间,有些甚至不用 1 秒. 另外,改进后的持卡人证书申请协议验证效率大幅提高,而商家证书申请协议的验证效率更高. 其主要原因是实例化空间逻辑的变量和定理与智能体的局部运行(ρ, c)相关,每减少一个标识消息 c 时生成的变量和定理将大幅减少。

7 相关工作

文献[14]提出了一种专门描述 SET 支付协议的语言,但并未对协议进行验证. 文献[3]首次对 SET 支付协议建立了简化的形式化模型并使用 FDR 对该模型进行模型检测,证明了 SET 满足可终止性等五个性质,但文中并未对协议的秘密性、认证性进行讨论. 文献[4]用符号化模型检测工具 NuSMV 验证文献[3]中模型的认证性、保密性和数据完整性,发现了两个攻击,但该攻击需要在一定的假设下才存在,对完整的 SET 协议不起作用. 但他们均无讨论 SET 证书申请协议. 而我们的工作使用知识推理的方法,给出了更完整的 SET 协议简化模型,并对其秘密性、认证性等安全性质进行了验证,指出由于协议不满足某些认知规范,可能在实际中产生安全隐患。

Bella、Massacci 和 Paulson^[6-9] 为分析 SET 协议做了大量工作,并首次对 SET 证书申请协议和支

付协议建立了完整的形式化模型,用定理证明器 Isabelle 验证并证明了协议的秘密性等安全性质,但他们没有具体分析协议的认证性. 而且 Isabelle 是半自动的,验证过程需要用户干预,并且用户还要有比较深入的专业领域知识. 相比较而言,SPV 对 SET 协议的验证是完全自动化的,而且由于 SPV 所依赖的实例化空间协议验证逻辑的语法语义十分自然,因此 SPV 的输入语言也接近协议的自然描述,简明清晰,可供用户方便使用。

文献[5]用 AVISS 模型检测工具分析了文献[9]中建立的 SET 持卡人证书申请协议模型的认证性,指出协议认证性的不足可能导致 CA 收到重复的证书申请请求,并提出可通过增加应答标志增强认证性,但文中没有提出改进的具体操作方法,实际上 CA 重复收到请求也并不会影响双方的正常通信. 而我们针对原协议存在的实质性安全问题,对协议进行改进,并用 SPV 证明了改进后协议的有效性. 与本文工作较为类似的是文献[10],该作者讨论了 SET 证书申请协议,特别是商家/支付网关证书申请协议在认证性上的不足导致的隐患,但文中结论没有经过形式化证明或工具验证。

与我们之前的工作^[1,11] 比较,本文使用的 SPV 版本和相应理论添加了对异或算子 xor 的处理。

8 结 论

能否验证 SET 协议是衡量一个安全协议验证理论或工具是否能够处理复杂工业级协议的标准. 实例化空间理论和 SPV 工具首先实现了对完整 SET 协议的秘密性、认证性等安全性质的完全自动证明. 本文对 SET 证书申请协议做出了比以往更完整、更贴近原协议的简化,给出了协议在 SPV 下的形式化描述与验证结果,并针对原协议的安全问题,对协议做了有效的改进. 这一成果充分说明 SPV 可以处理复杂的工业级协议。

在本文和已有研究工作^[1,11] 的基础上,进一步提高 SPV 的验证效率,完善 SPV 的理论基础,使之能处理更多的密码原语,如 Diffie-Hellman 函数以及各种新型的安全协议,如电子投票协议和匿名通信协议等是下一步研究工作的重点。

参 考 文 献

[1] Su Kai-Le, Yue Wei-Ya, Chen Qing-Liang et al. Instantia-

- tion space: A new modal for security. Chinese Journal of Computers, 2006, 29(9): 1657-1665(in Chinese)
(苏开乐, 岳伟亚, 陈清亮等. 实例化空间: 一种新的安全协议验证逻辑的语义模型. 计算机学报, 2006, 29(9): 1657-1665)
- [2] MasterCard, VISA. Secure electronic transactions. TMA Lomas and Computer Security Group, Computer Laboratory, University of Cambridge, 1999
- [3] Lu S, Smolka S. Model checking the secure electronic transaction (SET) protocol//Proceedings of the 7th International Symposium on Modeling, Analysis and simulation of Computer and Telecommunication Systems. Washington, D. C., 1999: 358-364
- [4] Panti M, Spalazzi L, Tacconi S et al. Automatic verification of security in payment protocols for electronic commerce//Proceedings of the 4th International Conference on Enterprise Information Systems. Ciudad-Real, Spain, 2002, 4: 968-974
- [5] Armando A, Basin D et al. The AVISS security protocol analysis tool//Proceedings of the 14th Computer-Aided Verification (CAV). Springer LNCS, Copenhagen, Denmark, 2002: 349-354
- [6] Bella Giampaolo, Massacci Fabio, Paulson L C. An overview of the verification of SET. International Journal of Information Security, 2005, 4(1-2): 17-28
- [7] Bella Giampaolo, Massacci Fabio, Paulson L C. Verifying the SET registration protocols. IEEE Journal on Selected Areas in Communications, 2003, 21(1): 77-87
- [8] Bella Giampaolo, Massacci Fabio, Paulson L C. The verification of an industrial payment protocol: The SET purchase phase//Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, D. C.: ACM Press, 2002: 12-20
- [9] Bella Giampaolo, Massacci Fabio, Paulson L C, Tramontano Piero. Formal verification of cardholder registration in SET//Proceedings of the Computer Security-ESORICS 2000. Toulouse, France, 2000: 159-174
- [10] Brlek S, Hamadou S, Mullins J. Some remarks on the certificates registration of the electronic commerce protocol SET//Proceedings of the International Conference on Internet and Web Applications and Services (ICIW06). Guadeloupe, 2006: 119-124
- [11] Su Kai-Le, Lu Guan-Feng, Chen Qing-Liang. Knowledge structure approach to verification of authentication protocols. Science in China(Series E: Information Science), 2005, 35(4): 337-351(in Chinese)
(苏开乐, 吕关锋, 陈清亮. 基于知识结构的认证协议验证. 中国科学(E辑), 2005, 35(4): 337-351)
- [12] Millen J K. Common Authentication Protocol Specification Language (CAPSL). Computer Science Laboratory, SKI International, 2003
- [13] Fan Hong, Feng Deng-Guo. Security Protocol Theory and Method. Beijing: Science Press, 2003(in Chinese)
(范红, 冯登国. 安全协议理论与方法. 北京: 科学出版社, 2003)
- [14] Meadows C, Syverson P. A formal specification of requirements for payment transactions in the SET protocol//Proceedings of the Financial Cryptography 98. Anguilla, British West Indies, 1998: 122-140



XIAO Yin-Yin, born in 1983, Ph. D. candidate. Her research interests include model checking, modal logic, reasoning about knowledge, verification of security protocol.

SU Kai-Le, born in 1964, professor, Ph. D. supervisor. His research interests include model checking, reasoning about knowledge, non-monotonic reasoning, modal logic, verification of security protocol.

YUE Wei-Ya, born in 1985, Ph. D. candidate. His re-

search interests include model checking, verification of security protocol, logic programming.

CHEN Qing-Liang, born in 1980, Ph. D., assistant. His research interests include model checking, modal logic, verification of security protocol, symbolic algorithm.

LU Guan-Feng, born in 1973, Ph. D., lecturer. His research interests include information security, design and analysis of algorithms.

YANG Jin-Ji, born in 1968, Ph. D., associate professor. His research interests include verification of security protocol and design of multimedia.

Background

This research is supported by the National Basic Research 973 Program of China under grant No.2005CB321902, the National Natural Science Foundation of China under grant Nos.60496327, 10410638, 60473004, the Natural Science

Foundation of Guangdong under grant No.06023195 and the Natural Science Foundation Team Collaboration Project of Guangdong under grant No.04205407.

It is widely acknowledged that logical flaws in security

protocols, especially in complex industrial protocols, are hard to analyze. Instantiation Space Logic is a new justification-oriented security protocol logic under Dolev-Yao model, which can prove whether a protocol satisfies concerned security properties. The tool of this logic SPV(Security Protocol Verifier) is designed and implemented, which can efficiently verify whether the security protocol satisfies the goals in CAPSL(Common Authentication Protocol Specification Language) as well as multi-level epistemic specifications using modern SAT solvers.

All protocols should be simplified before being verified by logics or tools. SET(Secure Electronic Transaction) protocol is an e-commerce protocol devised by Visa and MasterCard. At present, it is the most complex industrial protocols, which has the document of over 1000 pages. Therefore, it is very difficult to simplify and there are few research works about it. Besides, some existent simplified models are not complete enough. For example, some models do not describe the XOR calculus, while the attacks in some others are not realistic.

In this paper, based on the Instantiation Space Logic theory and knowledge reasoning, the authors give a simplified model which is more close to the original SET certificate registration protocols than before, and introduce the model's formal description in SPV with the verification process and results. Moreover, according to the hidden danger of the protocols brought by the unsatisfied epistemic specification, the authors improve the protocols and show the effectiveness.

Actually, whether a theory or tool can verify SET protocol has become a standard to demonstrate whether the verification technology is mature enough to cope with the complex industrial protocols. Some parts of this protocol have been verified by model checkers or semi-automatic proves such as Paulson's Isabelle. However, this work is the first one to implement the totally automatic verification on the complete SET certificate registration protocols' authentication and secrecy properties, so it justifies that SPV has the ability to deal with complex industrial protocols.