# 一种分析 Timed-Release 公钥协议的扩展逻辑

范 红 冯登国

(中国科学院研究生院信息安全国家重点实验室 北京 100039)

**摘 要** 在 Coffey 和 Saidha 提出的 CS 逻辑(CS 逻辑将时间与逻辑结构相结合,可用于形式化分析 Timed-release 公钥协议的时间相关性秘密的安全性)的基础上,提出了 CS 逻辑的扩展逻辑,它更好地反映了 Timed-release 公钥协议的特性,并对一个协议实例进行了有效的形式化分析.

**关键词** Timed-release 公钥协议; CS 扩展逻辑; 形式化分析

**中图法分类号** TP309

# An Extension Logic of Timed-Release Public Key Protocols Analysis

FAN Hong FENG Deng-Guo

(*State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing* 100039)

**Abstract** Timed-release public key protocol can provide time-dependent secrets by using public key cryptographic system through standard time provided by the trusted third party. The formal analysis of this kind of protocols needs special logic system which can reflect its properties. Coffey & Saidha have proposed a logic system to formally analyze the timed-release public key protocols, which is called CS logic. CS logic adds the time into logic structure, so it can be used to analyze the security of time-dependent secrets of timed-release public key cryptographic protocols. This paper presents an extension of CS logic which reflects the properties of timed-release public key protocols better, and gives a good formal analysis of a concrete protocol.

**Keywords** timed-release public key protocol; CS extension logic; formal analysis

## 1 引 言

Rivest, Shamir 和 Wagner 在文献[1]中提出了 Timed-release 的概念用于解决与时间相关的安全性问题. 根据他们的提法, Timed-release 秘密是在向未来发送消息,即通过一个可信的第三方提供标准的时间参照,使得秘密只能在某个未来时间公开. Timed-release 公钥协议就是使用公钥密码体制提供时间相关性秘密的协议. 由于 BAN 及 BAN 类逻辑的推证结构中并没有考虑协议的时间因素,因此不能用于此类协议的分析. Coffey 和 Saidha 在文献[2]中提出了一种将时间与逻辑结构相结合的逻辑(称为 CS 逻辑),并且 CS 逻辑中的一些定理还对协议的秘密性进行了推证,如明确指出主体对某些解密消息的不可知性等. 因此,如果将 CS 逻辑进行适当扩展,则可对 Timed-release 类公钥协议进行有效的形式化分析.

本文第 2 节给出了 CS 逻辑框架;第 3 节对 CS 逻辑进行了扩展,增强了其协议分析的能力;第 4 节利用扩展逻辑对一个 Timed-release 公钥协议实例进行了形式化分析;第 5 节给出了结论.

收稿日期:2002-01-07;修改稿收到日期:2002-06-12. 本课题得到国家重点基础研究规划项目(G1999035802)和国家杰出青年科学基金(60025205)资助.**范 红**,女,1969 年生,博士研究生,讲师,主要研究方向为计算机网络信息安全. E-mail: pkfanhong@sina.com.cn. **冯登国**,男,1965 年生,博士,研究员,博士生导师,研究方向为信息安全.

## 2 CS 逻辑

CS 逻辑是由 Coffey 和 Saidha 提出的,它结合了传统的谓词逻辑和模态逻辑的特点[3],并在逻辑结构中引入时间的因素使之可用于分析与时间相关的协议秘密的安全性.

### 2.1 逻辑结构

CS 逻辑提供了两种不同的运算符 $K$ 和 $B$,$K$ 表示主体的知识,$B$ 表示主体的信仰.运算符都以时间作下标索引,用于标识主体获得知识和信仰的时间性.

$K_{\Sigma,t}\phi$:主体 $\Sigma$ 在 $t$ 时知道语句 $\phi$.

$B_{\Sigma,t}\phi$:主体 $\Sigma$ 在 $t$ 时相信语句 $\phi$.

主体 $\Sigma$ 的公钥记为 $K_\Sigma$,相应的私钥记为 $K_\Sigma^{-1}$,$e()$和 $d()$分别表示用公钥和私钥对消息进行密码运算.

$e(x,K_\Sigma)$:用公钥对 $x$ 进行加密运算.

$d(x,K_\Sigma^{-1})$:用对应的私钥对 $x$ 进行签名运算.

$S$ 和 $R$ 分别表示消息的发送与接收.

$S(\Sigma,t,x)$:主体 $\Sigma$ 在 $t$ 时发送消息 $x$.

$R(\Sigma,t,x)$:主体 $\Sigma$ 在 $t$ 时接收消息 $x$.

CS 逻辑中另一个较重要的运算符是 $C$,用于表示消息直接或间接地包含在另一消息中.

$C(x,y)$:消息 $x$ 包含消息 $y$($y$ 可能是明文或密文).

### 2.2 推理规则

系统中的所有主体的集合记为 $PRI$.

(1) 知识与信仰规则

I1 (a) $K_{\Sigma,t}p \wedge K_{\Sigma,t}(p\rightarrow q)\rightarrow K_{\Sigma,t}q$.

(b) $B_{\Sigma,t}p \wedge B_{\Sigma,t}(p\rightarrow q)\rightarrow B_{\Sigma,t}q$.

I1 表明:如果主体 $\Sigma$ 在 $t$ 时知道或相信 $p$,并且由 $p$ 可推知 $q$,那么 $\Sigma$ 在 $t$ 时知道或相信 $q$.

(2)时间单调性规则

I2 (a) $K_{i,t}x\rightarrow \forall t'\geq t\ K_{i,t'}x$ .

(b) $B_{i,t}x \rightarrow \forall t'\geq t\ B_{i,t'}x$ .

I2 表明:CS 逻辑运算符 $K$,$B$ 与时间相关的单调增长性.

(3)包含规则

I3 $K_{i,t}y \wedge C(y,x)\rightarrow \exists j\in PRI\ K_{j,t}x$ .

(4)发送与接收规则

I4 $S(\Sigma,t,x)\rightarrow K_{\Sigma,t}x \wedge \exists i\in PRI\backslash\{\Sigma\}\ \exists t'>t\ R(i,t',x)$.

I5 $R(\Sigma,t,x)\rightarrow K_{\Sigma,t}x \wedge \exists i\in PRI\backslash\{\Sigma\}\ \exists t'<t\ S(i,t',x)$.

这组规则表明:如果一个主体在某时发送了一个消息,那么在此之后会有某一个主体收到此消息;或者如果一个主体在某时接收了一个消息,那么在此之前一定有某一个主体发送了此消息.

(5)密钥规则

I6 $K_{i,t}x \wedge K_{i,t}K_\Sigma\rightarrow K_{i,t}(e(x,K_\Sigma))$.

I7 $K_{i,t}x \wedge K_{i,t}K_\Sigma^{-1}\rightarrow K_{i,t}(d(x,K_\Sigma^{-1}))$.

I8 $K_{i,t}K_i^{-1} \wedge \forall j\in PRI\backslash\{i\}\rightarrow \neg K_{j,t}K_i^{-1}$.

I9 $K_{i,t}(d(x,K_\Sigma^{-1}))\rightarrow K_{\Sigma,t}x$.

这组规则表明:主体只有知道公钥及其对应的私钥才能进行加密操作或对密文进行相应的解密操作,而且私钥只为主体独自持有,公钥则是公开的.

(6)消息获取规则

I10(a) $\neg K_{i,t}K_\Sigma \wedge \forall t'<t\ \neg K_{i,t'}(e(x,K_\Sigma)) \wedge \neg(\exists y(R(i,t,y)\wedge C(y,e(x,K_\Sigma))))\rightarrow \neg K_{i,t}(e(x,K_\Sigma))$.

(b) $\neg K_{i,t}K_\Sigma^{-1} \wedge \forall t'<t\ \neg K_{i,t'}(d(x,K_\Sigma^{-1})) \wedge \neg(\exists y(R(i,t,y)\wedge C(y,d(x,K_\Sigma^{-1}))))\rightarrow \neg K_{i,t}(d(x,K_\Sigma^{-1}))$.

这组规则表明了主体对密文消息的获取能力.

## 3 CS 逻辑扩展

CS 逻辑将主体的知识和信仰与时间相关联,从而可对 Timed-release 公钥协议进行形式化分析.但原有的 CS 逻辑存在着不足,在具体应用时须作扩展.

### 3.1 时间单调性规则的扩展

单调性规则表示了 CS 逻辑运算符 $K$,$B$ 与时间相关的单调增长性,存在的不足是(1)未对 $K$,$B$ 与时间相关的不可知性进行描述;(2)未对时间段的合并与拆分操作前后知识与信仰的变化进行描述.故对原时间单调性规则扩展如下:

I2 (a1) $K_{i,t}x \rightarrow \forall t'\geq t\ K_{i,t'}x$.

(a2) $\neg K_{i,t}x \rightarrow \forall t'\leq t\ \neg K_{i,t'}x$.

(b1) $B_{i,t}x \rightarrow \forall t'\geq t\ B_{i,t'}x$ .

(b2) $\neg B_{i,t}x\rightarrow \forall t'\leq t\ \neg B_{i,t'}x$ .

(c1) $\forall tn\leq t'\leq tm\ K(B)_{i,t'}x \wedge \forall tm\leq t''\leq ts\ K(B)_{i,t''}x\rightarrow \forall tn\leq t\leq ts\ K(B)_{i,t}x$.

(c2) $\forall tn\leq t\leq ts\ K(B)_{i,t}x\rightarrow \forall tn\leq t'\leq tm\ K(B)_{i,t'}x \wedge \forall tm\leq t''\leq ts\ K(B)_{i,t''}x$.

这组扩展规则表明:主体如果在 $t$ 时知道 $x$,则

此后一直知道;如果主体在 $t$ 时不知道 $x$,则在此之前也不知道 $x$. 并且 $K,B$ 的时间单调性满足时间段的合并与拆分操作.

### 3.2　包含规则的扩展

在对具体的协议消息进行分析时,我们不仅要了解消息的包含关系,更要考虑主体是否能够真实获取所包含的消息. 对于有些被包含的密文消息,如果主体不持有相应的解密密钥,那么即使主体能够得到包含的消息也无法知道消息的内容. 例如在这种情况下:$K_{i,t}y \wedge C(y,y') \wedge C(y',e(z,K_\phi))$ 就只能得出十分有限的结论 $C(y,z)$,而不一定能够得出 $K_{i,t}z$,这将取决于主体是否持有 $K_\phi^{-1}$. 可见由于 $C$ 操作符的局限性,使得 CS 逻辑对主体消息获取能力描述乏力. 因此在原有的包含操作基础上增加获取操作 possess,记为 $P_{i,t}(x,y)$,表示主体 $i$ 在 $t$ 时能够获取包含在 $x$ 中的消息 $y$. 当 $y$ 为明文时,除增加了时间因素外,获取操作与包含操作同义;当 $y$ 为密文或包含有加密的子消息时,获取操作与包含操作的含义是不相同的,形式化描述为

$$K_{i,t}y \wedge C(y,y') \wedge \exists Y \in sub\text{-}y', \exists Z \in Msg,$$
$$k \in KEY \cdot Y = \{Z\}_K \wedge K_{i,t}k^{-1} \rightarrow P_{i,t}(y,Z).$$

获取操作更加突显了协议消息的密码属性,从而增强了其分析密码协议的能力. 在此基础上对原有的包含规则扩展如下:

I3(b) $K_{i,t}y \wedge C(y,y') \wedge P_{i,t}(y,y') \rightarrow K_{i,t}y'$.

显然 $P$ 具有传递性:

(c) $P_{i,t}(x,y) \wedge P_{i,t}(y,z) \rightarrow P_{i,t}(x,z)$.

并且 $P$ 满足于消息的级联与分离操作:

(d1) $P_{i,t}(x,y1) \wedge P_{i,t}(x,y2) \rightarrow P_{i,t}(x,y1|y2)$.

(d2) $P_{i,t}(x,y1|y2) \rightarrow P_{i,t}(x,y1) \wedge P_{i,t}(x,y2)$.

前面所述的时间单调性扩展规则同样适用于获取操作:

(e1) $P_{i,t}(x,y) \rightarrow \forall t' \geq t\ P_{i,t'}(x,y)$.

(e2) $\neg P_{i,t}(x,y) \rightarrow \forall t' \leq t \neg P_{i,t'}(x,y)$.

这组扩展规则表明了消息的获取随时间的单调增长性.

### 3.3　发送与接收规则的扩展

主体通过消息的发送与接收可以建立或使其它主体建立起有关的知识与信仰,原有的发送与接收规则未能反映出这一特性.

I4(a) $S(\Sigma,t,x) \rightarrow B_{\Sigma,t}x \wedge B_{i \in PRI\setminus\{\Sigma\},t'>t}R(i,t',x)$.

I5(a) $R(\Sigma,t,x) \rightarrow B_{\Sigma,t}x \wedge B_{i \in PRI\setminus\{\Sigma\},t'<t}S(i,t',x)$.

这组扩展规则表明:当主体发送或接收一个消息时,它相信此消息且相信另一个主体在此之后接收或在此之前发送了此消息. 进一步而言,如果将接收规则(I5)与密钥规则相结合,则可得到十分有用的通过加密消息判定主体身份的信仰.

(b1) $R(\Sigma,t,e(x,K_i^{-1})) \rightarrow B_{\Sigma,t}S(i,t' \mid t' \leq t,x) \wedge \exists j \in PRI\setminus\{i\} \rightarrow K_{j,t'}x$.

(b2) $S(\Sigma,t,e(x,K_i)) \rightarrow B_{i,t'>t} \exists j \in PRI\setminus\{\Sigma,i\} \rightarrow K(j,t',x)$.

这组扩展规则表明:如果主体接收到一个某主体的签名消息,那么它相信在此之前有一个主体发送了此消息,且仅此主体知道这个消息;如果主体发送了一个用另一个主体公钥加密的消息,那么它相信在此后只有它和那个主体知道此消息(假设消息是由主体生成的新鲜消息).

### 3.4　消息获取规则的扩展

在获取操作的基础上,对消息获取规则可做进一步的修订与扩展. 原有的消息获取规则的第 1 条与主体公钥的性质是相矛盾的;第 2 条由于原有 $C$ 操作符的局限性不能对消息的获取给出确切的定义,提出的条件过于严格. 现修订与扩展如下

I10(a) $\exists y(R(i,t,y) \wedge C(y,d(x,K_\Sigma^{-1})) \wedge P_{i,t}(y,d(x,K_\Sigma^{-1}))) \wedge \exists sub\text{-}y(P_{i,t}(y,sub\text{-}y) \wedge \forall Q \in PRI\setminus\{\Sigma\} \rightarrow K_{Q,t}sub\text{-}y) \rightarrow \forall\ t' < t \forall j \in PRI\setminus\{\Sigma\} \rightarrow K_{j,t'}x$.

这条扩展规则表明:如果主体在 $t$ 时直接或间接收到另一个主体的一个签名消息,且此消息中至少包含一个消息部分仅为发送主体所知(可能是一个 Hash 值,或者是一个新的随机数),则意味着在此之前只有该主体知道此消息. 这里 $x$ 为明文或密文.

如果结合特定的秘密释放时间的性质,还可对消息获取规则做如下扩展:

(b1) $\forall j \in PRI\setminus\{T\}\ \forall t < Time\ K_{j,t}y \wedge C(y,e(x,tk_{Tim})) \rightarrow \neg P_{i,t}(y,x)$.

(b2) $\forall j \in PRI\ \forall t \geq Time\ K_{j,t}y \wedge P_{i,t}(y,e(x,tk_{Time})) \rightarrow \forall j \in PRI\ K_{j,t}x$.

这组扩展规则表明:如果在秘密释放时间前除了 $T$ 任何主体无法获知 $x$($x$ 为一个时间相关的秘密数据项);而在秘密释放时间后每个人都可获知 $x$.

## 4　实例分析

### 4.1　一个 Timed-release 公钥协议

Kudo & Mathuria 提出了一个 Timed-release 公钥协议实例,它包括 3 个主体:$A$,$B$ 和 $T$. 其中 $A$

是一个发送与未来某个时间相关的秘密消息的主体，$B$ 是密文的意定接受者，$T$ 是一个可信第三方并假设其知道准确的时间，且可运用适当的密码体制生成非对称密钥对，并将之与 $A$ 所规定的未来特定秘密释放时间进行绑定. 协议描述如下：

(1) $A->T$: "$ek$", $Time$.

(2) $T->A$: $\{$"$ek$", $Time$, $tk_{Time}\}\ k_T^{-1}$.

(3) $A->B$: $A$.

(4) $B->A$: $Nb$.

(5) $A->B$: $\{\{Xa, Na, A\}tk_{Time}, A, B, Time, Nb, tk_{Time}\}k_A^{-1}$, $\{$"$enc$", $Time$, $tk_{Time}\}\ k_T^{-1}$.

(6) $B->A$: $\{\{\{Xa, Na, A\}\ tk_{Time}, A, B, Time, Nb, tk_{Time}\}k_A^{-1}\}\ k_B^{-1}$.

(7) $B->T$: "$dk$", $Time$.

(8) $T->B$: if current time$\geq Time$, $\{\{$"$dk$", $Time$, $tk_{Time}^{-1}\}\ k_T^{-1}\}k_B$.

首先 $A$ 发送消息给 $T$，请求 $T$ 为某个未来时间 $Time$ 生成一个时间密钥对(消息 1)，并要求 $T$ 返回时间公钥. 收到此消息后，$T$ 生成时间密钥对 $tk_{Time}$ 和 $tk_{Time}^{-1}$，并对其中的 $tk_{Time}$ 签名后发给 $A$(消息 2). $T$ 在时间 $Time$ 之前持有解密密钥 $tk_{Time}^{-1}$. $A$ 验证 $T$ 的签名并向 $B$ 发送包含 $A$ 名字的挑战消息(消息 3). $B$ 回应一个随机数 $Nb$(消息 4). 接下来 $A$ 生成一个随机数 $Na$，与秘密数据 $Xa$ 以及 $A$ 的名字一起用时间公钥 $tk_{Time}$ 加密. $Na$ 在这里可抗重放攻击. 加密结果附加上 $A$，$B$，$Time$，$Nb$ 和 $tk_{Time}$，$A$ 对整条消息签名，并级联消息 2 一起发给 $B$(消息 5). $Nb$ 在这里的作用是抗重放攻击. $B$ 验证 $A$ 的签名，将消息 5 中的消息 2 部分留下，对其余部分签名后返回给 $A$(消息 6). $B$ 向 $T$ 申请时间私钥以获得 $Xa$(消息 7). 如果 $T$ 的时钟表明当前时间已大于或等于 $Time$，则 $T$ 向 $B$ 返回一个包含 $tk_{Time}^{-1}$ 的消息(消息 8)，否则不做出响应. $B$ 最终可用 $tk_{Time}^{-1}$ 解密出 $Xa$. 显然，此类协议的主要目的并不是像其它协议一样通过一个意定接收者以保证 $Xa$ 的秘密性，而是用一个特定的时间点，在特定时间点之后，$B$ 可从 $T$ 处得到解密密钥进而得到秘密.

### 4.2 协议分析

CS 扩展逻辑对 Timed-release 公钥协议的形式化分析包括以下 4 步：

将 Timed-release 公钥协议的过程语言进行时间标注；

提出 Timed-release 公钥协议所基于的假设或前提；

形式化说明协议将达成的目标；

运用 CS 扩展逻辑推理规则和协议会话事实及假设从协议初始状态开始推证直至验证协议是否达成其最终执行目标.

分析流程如图 1 所示.

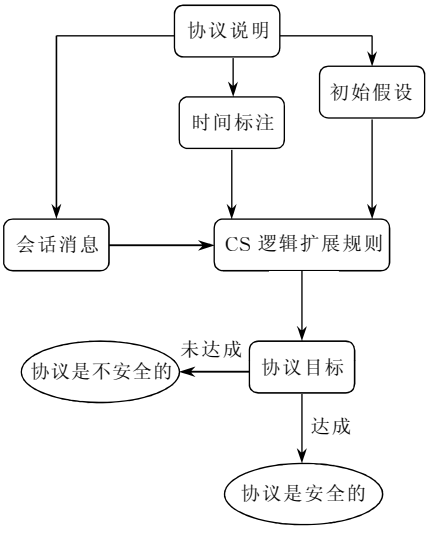


图1 CS 扩展逻辑协议形式化分析流程框图

(1) 时间标注

为协议标注几个关键的时间点. 令 $t0$ 为协议的初始时间，即协议从 $t0$ 时开始执行，$tn$ 为协议结束时间. 则 $\forall t<t0$ 或者 $\forall t>tn$ 表示非本轮的协议执行. $tg$ 为可信中心 $T$ 生成时间密钥对的时间，$tb$ 为 $B$ 向 $T$ 申请解密密钥的时间，$Time$ 为允许秘密释放的时间. 除上述特别说明的时间点以外，如果忽略主体的消息处理的时间延迟，我们还可对某些对于协议分析较为重要的消息进行时间标注，可在一定程度上反映协议的时间相关的执行顺序. 标记规则为：$ti\ (mi)ti+1$ 表示发送消息 $mi$ 的时间是 $ti$，对方收到此条消息的时间是 $ti+1$，并且消息 $mi+1$ 的发送时间等于消息 $mi$ 的接收时间. 为保证协议的完整执行，我们假设 $tb>Time$，即 $B$ 在允许的秘密释放时间之后向 $T$ 申请解密密钥. 本协议的消息交换与关键时间点的关系分三部分进行标注，具体如图 2 所示.

对协议消息进行时间标注是由 Timed-release 公钥协议的特点决定的. 因为此类协议目标达成的关键在于协议中定义的时间点，而不是像其它协议是通过协议消息的传递来保证秘密的不泄露或主体双方某种信仰共识的达成.

(2)假设条件

①有关密钥的假设：

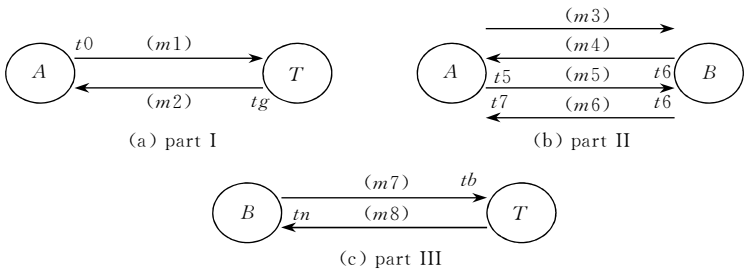


图 2　协议消息时间标注示意图

A1: $\forall \Sigma, i \in \{A, B, T\}\ \forall t \geq t0\ K_{\Sigma,t} k_\Sigma \wedge K_{\Sigma,t} k_i$.

协议主体 $A, B, T$ 在协议开始运行后知道自己及对方的公钥.

A2: $\forall \Sigma \in \{PRI \backslash \Sigma\}\ \forall t \geq t0 \rightarrow K_{\Sigma,t} k_\Sigma^{-1}$.

协议主体 $A, B, T$ 的私钥在协议开始运行后仅为主体自己知道.

A3: $\forall \Sigma \in \{PRI \backslash T\}\ \forall tg < t < Time \rightarrow K_{\Sigma,t}\ tk_{Time}^{-1}$.

$tk_{Time}^{-1}$ 在 $Time$ 之前只有可信中心 $T$ 知道.

②有关随机数的假设:

A4: $\forall i \in ENY\ \forall t < t0 \rightarrow K_{I,t} Na \wedge \rightarrow K_{I,t} Nb$ .

主体的随机数 $Na, Nb$ 是本轮协议产生的.

A5: $\forall i \in ENY \backslash \{A\}\ \forall t > t0 \rightarrow K_{I,t} Na$ .

只有主体 $A$ 知道 $Na$.

③协议假设主体都是诚实的,$T$ 为可信中心,并且所用密码算法是完美的.

(3) 协议目标

协议目标形式化表示为

G1: $B$ 在时间 $Time$ 之后能够解密秘密消息.

$\forall t \geq Time\ K_{B,t} Xa$ .

G2: $B$ 相信 $Xa$ 是由 $A$(而不是其它主体)在当前协议轮中发送的.

$\forall t \geq t0\ B_{B,t} S(A, t, Xa)$ .

G3: $A$ 相信 $B$ 收到了加密的秘密消息.

$B_{A,t} R(B, t, \{\{Xa, Na, A\} tk_{Time}, A, B, Time, Nb, tk_{Time}\} k_A^{-1})$ .

(4) 逻辑推证

证明.

令 $M = \{Xa, Na, A\}\ tk_{Time}, A, B, Time, tk_{Time}$,

$\forall t \geq tg\ R(A, t, \{\text{“}ek\text{”}, Time, tk_{Time}\}\ k_T^{-1})$ (1)

由 I6 和式(1)得

$$\forall t \geq tg\ K_{A,t} S(T, tg, tk_{Time}) \rightarrow \forall t \geq tg\ K_{A,t} tk_{Time} \quad (2)$$

$T$ 在 $tg$ 时为秘密消息生成密钥对,$A$ 在此后收到 $T$ 签名的消息,其中包含用于对秘密消息加密的密钥.

由消息 5 得

$$R(B, t6, \{M, Nb\} k_A^{-1}) \wedge R(B, t6, \{\text{“}enc\text{”}, Time, tk_{Time}\}\ k_T^{-1} \quad (3)$$

由 I5 和式(3)得

$$K_{B,t6}\{M, Nb\} k_A^{-1} \wedge \exists i \in PRI \backslash \{B\}\ \exists t < t6\ S(i, t, \{M, Nb\} k_A^{-1}) \quad (4)$$

由式(4)和 A2 得

$$K_{B,t6}(M, Nb) \rightarrow K_{B,t6} M \quad (5)$$

根据时间标定,$T$ 在 $tb$ 时收到 $B$ 的申请,要求 $T$ 为其提供秘密消息的解密密钥. 由时间假设 $tb > Time$,故 $T$ 在消息 8 中将解密密钥提供给 $B$,由 I5 得

$$K_{B,tn}(\{\{\text{“}dk\text{”}, Time, tk_{Time}^{-1}\}\ k_T^{-1}\}\ k_B) \rightarrow K_{B,tn}(\text{“}dk\text{”}, Time, tk_{Time}^{-1}) \rightarrow K_{B,tn} tk_{Time}^{-1} \quad (6)$$

由式(5)和 I2(a)及 $tn > t6$ 得

$$K_{B,tn} M \quad (7)$$

由式(6),(7)得

$$K_{B,tn} d(M, tk_{Time}^{-1}) \rightarrow \forall t \geq Time\ K_{B,tn} Xa \quad (8)$$

$B$ 在 $Time$ 之后知道秘密消息. 证明了 G1.

由式(3)得

$$B_{B,t6}(S(\exists j,\ \forall t < t6,\ \{M, Nb\} k_A^{-1})) \quad (9)$$

$B$ 在 $t6$ 时相信在此之前有一个主体曾发送了一个包含秘密消息的消息.

如果 $B$ 欲证明在 $t6$ 之前是主体 $A$ 而不是其它主体向其发送了加密的秘密消息,那么必须满足消息获取扩展规则 I10(a). 即 $B$ 收到了由 $A$ 签名的消息(式(9))并且消息中包含仅为 $A$ 所知的子消息.

由 A3 及包含规则得

$$\forall j \in PRI \backslash \{A\}\ \forall t < Time \rightarrow K_{j,t}(\{Xa, Na, A\} tk_{Time}) \quad (10)$$

由式(9)和式(10)及消息获取扩展规则得

$$B_{t6}(S(A, \forall t < t6, \{M, Nb\} k_A^{-1})) \quad (11)$$

所以虽然消息 5 可被除 $B$ 以外的任何人截获,但由于 $\{Xa, Na, A\} tk_{Time}$ 的特殊性任何非 $A$ 的人冒充 $A$ 是没有任何意义的,并不能构成现实攻击,故 G2 得到满足. 但由于 $tk_{Time}$ 的时间性,真正的验证应在 $Time$ 之后可信中心 $T$ 颁发了 $tk_{Time}^{-1}$ 时完成.

由消息 6 得

$$R(A,t7,\{\{\{Xa,Na,A\}tk_{Time},A,B,Time,Nb,tk_{Time}\}k_A^{-1}\}k_B^{-1}) \quad (12)$$

由式(12)及扩展规则 I5(b1)得

$$B_{A,t}S(B,t' \mid t' \leq t7,\{\{Xa,Na,A\}tk_{Time},A,B,Time,Nb,tk_{Time}\}k_A^{-1}\}) \wedge \exists j \in PRI\backslash\{B\} \neg K_{j,t'}\{\{Xa,Na,A\}tk_{Time},A,B,Time,Nb,tk_{Time}\}k_A^{-1}\} \quad (13)$$

由式(13)及包含扩展规则,得

$$B_{A,t}S(B,t' \mid t' \leq t7,\{Xa,Na,A\}tk_{Time}) \quad (14)$$

即 $A$ 相信 $B$ 在 $t7$ 前收到了秘密消息. 证明了 G3.

## 5 结束语

与 BAN 及 BAN 类逻辑相比,CS 逻辑的特点是[4]:在逻辑框架中引入时间因素从而可分析密码协议的时间相关秘密的安全性. 本文对原有的 CS 逻辑进行了扩展,使之能够更好地反映主体知识和信仰与时间之间的关系,因而能有效地应用于极具实用价值的 Timed-release 公钥协议的形式化分析中. 更加严格规范逻辑语义及协议假设,使之可应用于更多的密码协议分析中是进一步要做的工作[5].

## 参 考 文 献


1 Rivest R L, Shamir A, Wagner D A. Timed-lock puzzles and timed-release cryptographic protocol. MIT Laboratory for Computer Science. 1996

2 Coffey T, Saidha P. Logic for verifying public-key cryptographic protocols. IEEE Proceedings of Computers and Digital Techniques, 1997, 144(1):28～32

3 Syverson P, van Oorschot P. On unifying some cryptographic protocol logics. In:Proceedings of IEEE Symposium on Security and Privacy, 1994. 14～28

4 Fan Hong, Feng Deng-Guo. Carrent states of security protocal formal analysis. Net Security Technologies and Application, 2001,1(8):12～15(in Chinese)
(范 红,冯登国. 安全协议形式化分析的研究现状与有关问题. 网络安全技术与应用,2001, 1(8):12～15)

5 Feng Deng-Guo. Information security research and development. Net Security Technologies and Application, 2001,1(1):4～10(in Chinese)
(冯登国. 国内外信息安全研究现状及其发展趋势. 网络安全技术与应用,2001, 1(1):4～10)

6 Feng Deng-Guo, Pei Ding-Yi. The Guidance of Cryptograph. Beijing: Science Press,1999(in Chinese)
(冯登国,裴定一. 密码学导引. 北京:科学出版社, 1999)



**FAN Hong**, born in 1969, Ph. D. candidate, lecturer. Her research interests include computer network information security.

**FENG Deng-Guo**, born in 1965, Ph. D., professor, doctoral supervisor. His current research areas focus on information security.