物联网中移动节点抗克隆攻击的UC安全认证协议

宋生宇[1,2] 张紫楠[1] 王亚弟[1] 李俊峰[3]
(解放军信息工程大学 郑州 450001)[1] (总装备部装备论证中心九室 北京 100101)[2]
(太原卫星发射中心 太原 030000)[3]

摘 要 物联网中的感知网一般由计算、通信和存储能力极差的感知节点通过移动节点和静态节点相结合的方式构成,以采集信息;而传输网通常利用现有互联网的基础设施,提供强大的计算、通信和存储服务。为了满足物联网中移动节点漫游时实施接入认证的访问控制要求,同时兼顾实际应用中可行性与移动节点轻量级、抗物理克隆攻击等的安全性需求,基于物理不可克隆函数(Physical Unclonable Function,PUF),提出了移动节点抗克隆攻击的UC(Universally Composable)安全认证协议,其可实现移动节点漫游到其他区域时与接入基站之间的双向认证与密钥交换过程。分析表明,所提出的协议在UC安全模型下是可证明安全的。

关键词 物联网,物理不可克隆函数(PUF),物理不可克隆函数系统(PUFS),UC安全
中图法分类号 TP309.7 **文献标识码** A

Universally Composable Secure Authentication Protocol for Mobile Sensors Based on Physical Unclonable Function System

SONG Sheng-yu[1,2] ZHANG Zi-nan[1] WANG Ya-di[1] LI Jun-feng[3]
(PLA Information Engineering University, Zhengzhou 450001, China)[1]
(The Research Center, Equipment Demonstration of General Equipment Headquarter, Beijing 100101, China)[2]
(Taiyuan Satellite Launch Center, Taiyuan 030000, China)[3]

Abstract Internet of Things consists of sensor subnet and transmission network. For sensor subnet, it usually collects information by sensor node which has bad ability of computing, communication and storage implemented by combining mobile nodes and static nodes. But for transmission network, it commonly provides strong service of computing, communication and storage by making use of the existing internet infrastructure. To assure security control mechanics when the mobile sensors move from one cluster to another, whenever, to take into account both the security and feasibility of practical application, this paper presented an authentication and key exchange protocol based on Physical Unclonable Function(PUF). This protocol can achieve bidirectional authentication and key negotiation between mobile sensor and transmission network base station when the mobile sensor roams to other cluster. Analysis shows that the proposed protocol is universally composable secure.

Keywords Internet of things, Physical unclonable function(PUF), Physical unclonable function system(PUFS), Universal composition security

1 引言

物联网是典型的混合式异构网络,由感知网、传输网和应用网组成。感知网一般由计算、通信和存储能力极差的感知节点通过移动节点和静态节点相结合的方式构成。而传输网通常利用现有互联网的基础设施,提供强大的计算、通信和存储服务。

移动节点在初始区域A已经和传输网络的基站建立共享密钥,当移动节点从初始区域A进入另一个区域B进行相关信息采集时,它需要在区域A基站的帮助下与区域B的基站进行相互的认证和密钥交换。这种认证密钥交换有以下几个特点:1)移动节点的轻量级需求。物联网中的移动节点(如RFID标签、无线传感器节点和智能卡等)不具有强大的计算、存储和通信能力,所以需要设计计算复杂度较低的安全协议。2)移动节点的抗物理克隆攻击需求。物联网中的移动节点往往是克隆攻击的对象,一旦物理克隆攻击节点成功,就会对物联网造成严重的安全隐患。3)通用可组合性(Universal Composition,UC)[1-3]需求。移动节点与基站的交互协议不能够影响传输网中基站上其他协议的运行,即协议必须满足通用可组合特性。

本文基于物理不可克隆函数系统(Physical Unclonable Function System,PUFS)提出一个新的移动节点抗克隆攻击

到稿日期:2013-07-29 返修日期:2013-09-01 本文受国家部委基金资助项目(9140C130103120C13062)资助。
宋生宇(1978—),男,博士生,主要研究方向为物联网与移动互联网安全,E-mail:ssy_qj@sina.com;王亚弟(1953—),男,教授,博士生导师,主要研究方向为网络与信息安全。

的 UC 安全认证协议(称为 RAKP 协议)。PUFS 包括一个物理不可克隆函数(Physical Unclonable Function, PUF)[4-7] 和一个相应的提取算法[7]。PUF 是指对一个物理实体输入一个激励,利用其不可避免的内在物理构造的随机差异输出一个不可预测的响应这样一个抗克隆攻击的函数[8]。也就是说在理想情况下,对于一个确定的 PUF,输入相同的激励,其会输出相同的响应,并且这个响应具有物理不可克隆性。除了抵抗克隆攻击之外,PUF 的优势还包括这种不能被克隆的激励响应行为可以实现一些与传统公钥加密一样的功能,但是却大大减少了计算和通信开销。随着对 PUF 理解的逐步加深,人们提出越来越多的 PUF 实现方法(如光学 PUF[4] 和涂层 PUF[5])和 PUF 应用(如身份认证[6] 和密钥生成[7])。

新的移动节点抗克隆攻击的 UC 安全认证协议具有如下功能和特点:(1)PAKP 协议可以安全抵抗物理克隆攻击。(2)PAKP 协议不使用任何可计算的假设,而是基于 PUFS 的安全属性实现。相比于传统的公钥加密方案,它大大减少了计算和通信开销。(3)PAKP 协议满足通用可组合特性。

2 物理不可克隆函数

自从 Pappu[4] 提出物理不可克隆函数以来,其凭借物理不可克隆性、轻量级和不可预测性等良好的性质而受到广泛的关注,并逐渐成为硬件安全领域研究中的一个热门课题。但是在实际中,PUF 的激励响应行为会受到噪音的影响,即给定相同的激励,PUF 可能产生略有不同的响应,但是这些略有不同的响应是"相似"的,可以通过一个提取算法设置阈值来消除噪音的影响。所以在 PUF 中加入一个提取算法来实现一个物理不可克隆函数系统(PUFS),使得其具有广传播域、提取独立和鲁棒属性。

1)物理不可克隆函数(PUF)

PUF 是 PUFS 最主要的组件,它主要包括一个物理组件 $p()$ 和一个评估过程 $Eval()$。物理组件 p 是纯硬件实现的一部分,给定一些激励信号 $\bar{x}$,它会利用生产制造变化的不同输出一个响应信号 $\bar{y}$。而评估过程 $Eval()$ 的作用是将物理信号转换成数字信号。所以 PUF 的激励-响应行为主要依赖于物理组件 p 的属性,不可控的随机噪声(例如热噪声)和 PUF 制造商选择的一个评估参数 α_{PF}(例如量化因子)。也就是说,如果 3 个因素中有一个发生变化,PUF 的激励响应行为会表现出完全不同的结果,例如如果对于不同的物理组件 p,即使给定相同的激励,PUF 也会产生出不同的响应。

定义 1(PUF) 一个 PUF 是一个概率过程

$PUF_{p,\alpha_{PF}}: X \to Y$

其中,X 表示激励集合,Y 表示响应集合。

定义 2 在内部,一个 PUF 是一个物理组件 p 和评估过程 $Eval$ 的结合,即

$y \leftarrow PUF_{p,\alpha_{PF}}(x) = Eval(\alpha_{PF}, x)$

2)PUFS 框架

PUFS 主要包括一个 PUF 和一个提取算法(例如 Dodis[7] 等人提出的模糊提取算法),如图 1 所示。这里引入提取算法的目的有两个:第一是通过提取算法设置阈值消除噪音的影响,第二是通过提取算法使得响应具有高不相关性并使响应均匀分布。它利用辅助数据 h 在两个不同模式下执行:设置模式和重建模式。

定义 3(PUFS) 一个 PUFS 是一个概率过程

$PUFS_{p,\alpha_{PF},\alpha_{EX}}: X \times (H \cup \{\varepsilon\}) \to Z \times H$

其中,X 表示激励集合,H 表示辅助数据集合,ε 表示空字符串,Z 表示输出集合。当 $h=\varepsilon$ 时,表示提取算法 Extract 在设置模式下生成一个新的辅助数据 h。当 $h \neq \varepsilon$ 时,表示提取算法 Extract 在重建模式下利用激励 x 和辅助数据 h 来重建输出 z。

定义 4 在内部,一个 PUFS 是一个 PUF 和一个提取算法 Extract 的结合。即

$(z, h') \leftarrow PUFS_{p,\alpha_{PF},\alpha_{EX}}(x, h) = Extract_{\alpha_{EX}}(PUF_{p,\alpha_{PF}}(x), h)$

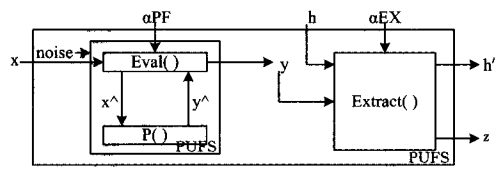

图 1 PUFS 一般框架

3 UC 框架和协议安全需求

3.1 通用可组合(UC)框架

粗略地说,UC 框架定义了两种协议运行模型:现实世界模型和理想世界模型。模型中的参与方都被抽象化为概率多项式时间交互式图灵机。

现实世界模型主要涉及 3 类抽象的参与方:被分析的协议 π;协议运行环境 Z,主要用于模型化系统中除被分析的协议之外的其他协议;现实攻击者 A,用来攻击协议消息和腐化协议参与方。理想世界模型中主要涉及的参与方包括环境 Z、理想攻击者 $\overline{A}$ 控制的仿真器 S 以及理想功能 F。其中,理想功能 F 模型化了密码学任务所应该实现的功能和可以允许的信息泄露,它可以通过虚拟用户与环境进行交互;理想攻击者 $\overline{A}$ 控制的仿真器 S 模型化了针对理想功能的特殊攻击者,它只能与理想功能进行交互,而不能与虚拟用户进行交互,这从形式上保证了理想世界模型中协议的安全性。最后,通过协议仿真保证现实世界模型中的协议具有和理想世界模型中的协议相同的功能,给出现实协议安全性的定义。

给定协议 π 以及理想功能 F,如果对任意的攻击者 A,都存在仿真器 S,使得对拥有任意输入的任何环境 Z,在和攻击者 A 以及协议 π 交互后的概率分布与在和攻击者 $\overline{A}$ 控制的仿真器 S 以及理想功能 F 交互后的概率分布是计算不可区分的,则称协议 π UC 安全地实现了理想功能 F。

3.2 PAKP 协议的安全需求

移动节点的安全无线漫游认证协议的主要需求和特征如下:

(1)轻量级。物联网中的移动节点(如 RFID 标签、无线传感器节点和智能卡等)不具有强大的计算、存储和通信能力,所以需要设计计算复杂度较低的安全协议。

(2)抵抗克隆攻击。移动节点的便携性使得节点容易受到敌手的物理克隆攻击,而目前设计的安全协议通常不具有抵抗物理克隆攻击的能力[8]。

(3)前向安全性[9]。当当前密钥受到威胁的时候,前向安全性保证了过去传输消息的安全。

(4)通用可组合性[10]。协议不仅在单独计算的条件下安

全，而且与其他协议并行执行也是安全的。

4 PAKP 协议

4.1 PAKP 协议设计

物联网中移动节点的相互认证和密钥交换通常需要经过两个阶段：1)移动节点在初始区域的注册阶段；2)将移动节点移动到其他区域后，在初始区域基站的协助下，完成移动节点与其他区域基站的相互认证和密钥交换。

注册阶段

在移动节点 SN_A 上，实现一个物理不可克隆函数系统 PUFS，其中相应的评估参数和提取参数是固定的值。对 PUFS 进行多项式次数的激励响应测量，其结果(x_k，h_k，y_k，z_k)存储到移动节点 SN_A 对应的激励响应对(CRP)数据表中，其中 $1 \leqslant k \leqslant N$。在移动节点 SN_A 和初始区域基站 BS_A 之间部署初始密钥 $k_{SN_A\text{-}BS_A}$。由于移动节点的轻量级限制，假定移动节点 SN_A 只可以具有 PUFS、哈希、异或和对称加密计算等简单运算功能。假定这种离线注册是安全的。

PAKP 协议

PAKP 协议的基本交互过程如图 2 所示。

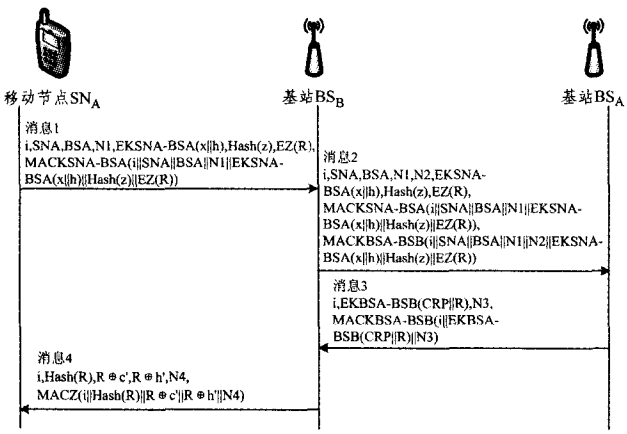

图 2 PAKP 协议交互过程

消息交互如下：

1)在 A 区域的移动节点 SN_A 移动到 B 区域时，向基站 BS_B 提出认证和密钥交换请求，并发起一个会话 i。向基站 BS_B 发送消息 1。其中 N_1 是一次性随机数，防止重放攻击。为了直观使用 SN_A、BS_B 和 BS_A 直接表示它们的 ID，会话标识 s 具有唯一性，在后面的实现过程中可以为 3 个随机数的级联表示。用基站 SN_A 和基站 BS_A 的密钥 $k_{SN_A\text{-}BS_A}$ 加密随机选择的激励 x 和辅助数据 h。利用 PUFS 计算出相应的响应 y 和输出 z。计算输出 z 的哈希值，并且用输出 z 加密一个随机数 R。MAC 是消息验证码，用密钥 $k_{SN_A\text{-}BS_A}$ 加密前面消息字段的总和，以实现消息完整性的验证。发送消息 1 之后，存储输出 z 和随机数 R 到会话 i 的条目中，并擦除激励 c 和辅助数据 h。

2)基站 BS_B 收到标识为 i 的会话消息 1 后，首先生成一次性随机数 N_2，防止重放攻击。然后用基站 BS_B 和基站 BS_A 的共享密钥 $k_{BS_A\text{-}BS_B}$ 生成前面消息字段总和的消息验证码。向基站 BS_A 发送消息 2。

3)基站 BS_A 收到标识为 i 的会话消息 2 后，首先使用密钥 $k_{BS_A\text{-}BS_B}$ 和 $k_{SN_A\text{-}BS_A}$ 对消息 2 中的两个消息验证码进行检验，若不满足则终止协议，否则得到激励 x、辅助数据 h、$Hash(z)$ 和 $E_z(R)$。找到对应于移动节点 SN_A 的激励响应对 CRP，查找对应于激励 x 和辅助数据 h 的数据条目，得到输出 z'，计算哈希值 $Hash(z')$，验证 $Hash(z)$ 和 $Hash(z')$ 是否相等，若不等则终止协议，否则实现对移动节点 SN_A 的认证。然后，向基站 BS_B 发送消息 3。其中 N_3 是一次性随机数，防止重放攻击；用密钥 $k_{BS_A\text{-}BS_B}$ 加密对应于移动节点 SN_A 的 CRP 和解密 $E_z(R)$得到 R。发送完成后，基站 BS_A 擦除对应于移动节点 SN_A 的 CRP、输出 z 和 R。

4)基站 BS_B 收到标识为 i 的会话消息 3 后，检验消息验证码，若不满足则终止协议，否则得到对应于移动节点 SN_A 的 CRP 和 R。从 CRP 中随机选择一个新的条目，得到激励 c'、辅助数据 h'和输出 z'，计算 $Hash(R)$、$R \oplus c'$和 $R \oplus h'$，并生成一个随机数 N_4，用 z 计算前面消息字段的消息验证码，最后向移动节点 SN_A 发送消息 4。发送消息之后，在 CRP 中擦除激励 c 和 c'对应的条目，设置基站 BS_B 接入结果为成功，使用 z'作为与移动节点 SN_A 的新会话密钥。

5)移动节点 SN_A 收到标识为 i 的会话消息 4 后，首先使用密钥 z 检验消息验证码的正确性，若不等则终止，否则实现初步认证，然后对会话 i 条目存储的 R 计算 $Hash(R)'$，验证发过来的 $Hash(R)$和 $Hash(R)'$是否相等，若不等则终止协议，否则实现对基站的认证。完成后擦除会话 i 的条目信息。使用 PUFS 计算出 x'和 h'对应的输出 z'，它就作为与基站 BS_B 新的会话密钥。至此，PAKP 协议交互完成。实现了移动节点的相互认证和密钥交换。

4.2 安全性分析

性质 1 协议能够抵抗物理克隆攻击。该协议在移动节点上实现一个物理不可克隆函数系统，根据 PUF 的本质属性：物理不可克隆性，任何试图物理克隆一个 PUF 电路的尝试是概率忽略不计的。所以任何试图通过物理克隆攻击移动节点而达到攻击协议的目的是不可能实现的。

性质 2 协议满足轻量级。物联网中的移动节点(如 RFID 标签、无线传感器节点和智能卡等)不具有强大的计算、存储和通信能力，该协议中的移动节点不使用公钥密码体制，而采用具有轻量级属性的 PUF 电路，同时，协议的交互过程中，移动节点只是计算对称加密、哈希和异或等运算，有效地满足移动节点的需求。

性质 3 协议具有前向安全性。攻击者即使获得了移动节点 SN_A 和基站 BS_A的会话密钥 $k_{SN_A\text{-}BS_A}$，也无法推导出之前的会话密钥。协议的相互认证和密钥交换过程是基于 PUF 的激励响应机制，其每一次的会话密钥是基于 CRP 中的一个条目，任何两个 CRP 中的条目没有任何关联，也就是说，获得一个条目对其他条目没有任何影响。通过上面分析，可知协议具有前向安全性。

性质 4 协议满足通用可组合性。该协议的通用可组合性证明参见下一节。

5 PAKP 协议的通用可组合安全性

在我们的协议中，基站 BS_A 的行为是可信的，并且基站 BS_B 和基站 BS_A 之间存在安全信道。略去一些不影响协议安全性的消息，给出 PAKP 协议的抽象描述 π，如图 3 所示。

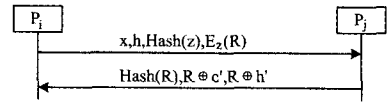

图 3 协议的抽象描述

5.1 PAKP 协议理想功能

PAKP 理想功能 F_{AKE} 的主要想法如下：如果双方是诚实的，PAKP 协议理想功能 F_{AKE} 提供它们一个共同的随机值，而这个随机值对于敌手是不可见的。如果其中的一个是腐化的，则敌手可完全决定会话密钥，所以建模一个腐化的参与方。PAKP 协议理想功能 F_{AKE} 如图 4 所示。

F_{AKE} 在各方 $P_1,\cdots,P_n$ 和敌手仿真器 S 之间交互，仅仅接收相同 sid 的消息：

· 每当从 P_i 接收到消息(establish, sid, ssid, P_i, P_j)的时候，F_{AKE} 存储消息(establish, sid, ssid, P_i, P_j)(并且拒绝建立，如果已经有一个消息(establish, sid, ssid, P_j, P_i)或者(establish, sid, ssid, P_i, P_j))，并且 F_{AKE} 发送(establish, sid, ssid, P_i, P_j)到仿真器 S。如果两个用户都是诚实的，则从 $\{0,1\}^\lambda$ 中选择一个随机值 k 并存储消息(send, sid, ssid, k, P_i)和(send, sid, ssid, k, P_j)。

· 每当从仿真器 S 接收到消息(choice, sid, ssid, P_i, P_j, k)的时候，F_{AKE} 检查是否有一个消息(establish, sid, ssid, P_j, P_i)或者一个消息(establish, sid, ssid, P_i, P_j)并且是否至少有一个用户 P_i 或 P_j 是腐化的。如果是，则存储消息(send, sid, ssid, k, P_i)和(send, sid, ssid, k, P_j)。

· 每当从仿真器 S 接收到消息(send, sid, ssid, P_i)的时候，F_{AKE} 检查是否有一个元组(send, sid, ssid, k, P_i)已经存储。如果是，发送(send, sid, ssid, k, P_i)到 P_i 并且删除消息(send, sid, ssid, k, P_i)。否者，什么也不做。

图 4 PAKP 协议理想功能

5.2 安全性证明

定理 1 假设 PUFS 是一个物理不可克隆函数系统，那么 PAKP 协议在静态敌方存在的情况下 UC 安全地实现了理想功能 F_{AKE}。

证明：由于只考虑静态的腐化，因此可以利用腐化的一方来区分仿真。

5.2.1 仿真器的 S 构造

a)仿真 P_i 和 P_j 都诚实的情况

每当理想功能 F_{AKE} 第一次发送消息(*establish*, *sid*, *ssid*, P_i, P_j)的时候，仿真器 S 初始化一个 PUF 并用 N 个随机激励 $x_1,\cdots,x_N$ 来查询它获得相应的响应 $y_1,\cdots,y_N$。接下来，仿真器 S 继续计算 $(z_k,h_k)\leftarrow Extract_{a_{EX}}^{setup}(y_k,\varepsilon)$，最后存储所有 N 个元组 (x_k,y_k,z_k,h_k) 到一个列表 CRP 中。仿真器 S 然后模拟一个物理不可克隆函数的移交并让敌手 A 查询物理不可克隆函数直到敌手 A 终止过渡阶段。设置阶段模拟结束。

每当接收一个消息(*establish*, *sid*, *ssid*, P_i, P_j)的时候，仿真器 S 发送(*send*, *sid*, *ssid*, P_i)到理想功能 F_{AKE}。

b)接收者 P_j 被腐化的情况

设置阶段的模拟与双方都诚实的情况是一样的。每当收到一个消息(*establish*, *sid*, *ssid*, P_i, P_j)的时候，仿真器 S 发送(*choice*, *sid*, *ssid*, P_i, P_j, z_k)到理想功能 F_{AKE}。然后仿真器 S 被再次激活并发送(*send*, *sid*, *ssid*, P_i)到理想功能 F_{AKE}。

c)发送者 P_i 被腐化的情况

仿真器 S 允许恶意用户 P_i 来实例化一个任意数量的物理不可克隆函数。接收者只能接受一个单一的物理不可克隆函数移交。每当一个敌手 A 通过认证发送(*sid*, *ssid*, (x_k, h_k))到 P_j 的时候，仿真器 S 用 x_k 查询物理不可克隆函数获得相应的响应 y_k 并且计算 $z_k\leftarrow Extract_{a_{EX}}^{reconstruction}(y_k,h_k)$。仿真器 S 让腐化虚拟用户 P_i 发送消息(*establish*, *sid*, *ssid*, P_i, P_j)到理想功能 F_{AKE}，接下来一并传送消息(*choice*, *sid*, *ssid*, P_i, P_j, z_k)和(*send*, *sid*, *ssid*, P_j)到理想功能 F_{AKE}。

5.2.2 不可区分性证明

由于 PUFS 中响应的广传播域和鲁棒属性，敌手 A 以压倒性的概率，在激励 x_k 没有比 $d_{\min}$ 更近的距离下查询物理不可克隆函数。由于 PUFS 中的响应独立属性，消息 (x_k,h_k) 对 z_k 是静态独立的。因此，仿真是完美的。在协议执行中环境 Z 和敌手 A 的共同看法与环境 Z 和在理想世界用仿真器 S 仿真的敌手 A 的共同看法是不可区分的。

结束语 文中首先讨论了 PUFS 的一般框架、定义及其属性，然后基于这个框架，提出了一个新的移动节点抗克隆攻击的通用可组合安全认证协议。与以往协议不同的是，PAKP 协议能够抵抗克隆攻击并且不使用任何可计算的假设，这大大减少了协议的计算和通信开销。最后详细讨论了这个协议的通用可组合特性，并给出相应的安全性证明。

参 考 文 献

[1] Canetti R. Universally composable security: A new paradigm for cryptographic protocols[C]// Proceedings of the 42nd IEEE Symposium on the FOCS. New York: IEEE Computer Society Press, 2001: 136-145

[2] Canetti R, Halevi S, Katz J, et al. Universally composable password-based key exchange[C]// Advances in Cryptology, Eurocrypt'05. LNCS. Vol. 3494, Berlin: Springer-Verlag, 2005: 404-421

[3] Moran T, Segev G. David and goliath commitments: UC computation for asymmetric parties using tamper-proof hardware[C]// EUROCRYPT, volume 4965 of Lecture Notes in Computer Science. Springer, 2008: 527-544

[4] Pappu R S. Physical One-Way Functions[D]. Massachusetts Institute of Technology, 2001

[5] Tuyls P, Schrijen G J, Škorić B, et al. Read-Proof Hardware from Protective Coatings. Cryptographic Hardware and Embedded Systems Workshop[C]// Lecture Notes in Computer Science. New York, NY: Springer, 2006, 4249: 369-383

[6] Hammouri G, Öztürk E, Birand B, et al. Unclonable Lightweight Authentication Scheme[C]// Proceedings of the 10th International Conference on Information and Communications Security (ICICS 2008). Heidelberg: Springer, 2008: 33-48

[7] Dodis Y, Ostrovsky R, Reyzin L, et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[J]. SIAM J. Comput., 2008, 38(1): 97-139

[8] 冯涛，李凤华，马建峰，等. UC 安全的并行可否认认证新方法[J]. 中国科学 E 辑：信息科学，2008，38：1220-1233

[9] Ben-Or M, Goldwasser S, Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation[C]// Proc. 20th STOC. ACM, 1988: 1-10

[10] Canetti R. Universally composable security: A new paradigm for cryptographic protocols [C]// Proceedings of the 42nd IEEE Symposium on the FOCS. New York: IEEE Computer Society Press, 2001: 136-145