doi:10.3969/j.issn.1000-436x.2013.z1.006

基于 PUFS 的不经意传输协议

郭渊博，张紫楠，杨奎武
（解放军信息工程大学 网络空间安全学院，河南 郑州 450000）

摘 要：不经意传输(OT, oblivious transfer)协议是密码学中的一个基本协议。基于物理不可克隆函数（PUF, physical unclonable function）给出物理不可克隆函数系统（PUFS, physical unclonable function system）的概念，并在此基础上提出一个新的不经意传输协议（POT, PUFS based OT），最后在通用可组合（UC, universal composition）框架内给出 POT 协议抵抗静态敌手的安全性证明。相比于传统基于公钥加密的 OT 方案，POT 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，因此在很大程度上减小了计算和通信开销。
关键词：不经意传输；物理不可克隆函数（PUF）；物理不可克隆函数系统（PUFS）；UC 框架
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0038-06

Oblivious transfer based on physical unclonable function system

GUO Yuan-bo, ZHANG Zi-nan, YANG Kui-wu
(Institute of Cyberspace Security, the PLA Information Engineering University, Zhengzhou 450000,China)

Abstract: Oblivious transfer (OT) is a fundamental protocol in cryptography. According to the analysis of physical unclonable function, a physical unclonable function system framework was defined, and a novel oblivious transfer (POT, PUFS based OT) protocol was proposed based on this framework. Finally, a security analysis of this POT protocol in the universal composition framework was given in detail. Compared with the traditional public key encryption OT scheme, POT protocol does not use any computational assumptions but rather the secure property of PUFS, and thus this scheme needs less computation and communication cost.
Key words: oblivious transfer; physical unclonable function (PUF); physical unclonable function system(PUFS); universal composition framework

1 引言

不经意传输（OT, oblivious transfer）协议是密码学中的一个基本协议，可用于实现比特承诺[1]、安全多方计算[2]和在线交易[3]等协议。在 OT 协议初始阶段，发送者有2个秘密消息 s_0和 s_1，接收者有一个秘密选择 b。在执行 OT 协议之后，必须满足如下条件：1) 接收者得到其选择的秘密消息s_b；2) 接收者不能得到另一个秘密消息s_{1-b}；3) 发送者不能知道接收者的选择 b。自从 Rabin[4]提出 OT 之后，其在学术界得到了大量的关注。

目前提出的大部分 OT 协议是基于一些可计算假设实现的。基于判定 Diffie-Hellman 假设，Fischlin[5]设计一个由第三方辅助完成的 UC 安全 OT 协议。基于二次剩余和判定复合剩余假设，TaumanKalai[6]也提出了类似的协议。它们的主要问题是，辅助第三方的假设，增加了协议的交互次数，降低了协议的通信效率，从而限定了具体的应用场景。但是最近，基于物理不可克隆函数（PUF, physical unclonable function），Ruhrmair[7]利用交互散列实现了一个新的 OT 协议。该方案的主要缺点是，协议的计算开销比较大，因为交互散列要计算 m 轮才能实现一次协议交互，而且没有考虑在实际应用中 PUF 的激励响应行为受到噪音影响的情况。

本文基于物理不可克隆函数系统（PUFS, physical unclonable function system）提出了一个新的 OT 协

收稿日期：2013-06-29
基金项目：国家部委基金资助项目（9140C130103120C13062）
Foundation Item: The Foundation of National Department (9140C130103120C13062)

议。PUFS 包括一个 PUF 和一个相应的提取算法。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物理不可克隆的函数[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，并且这个响应是完全不可克隆的。它的主要优势是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。随着人们对 PUF 的理解逐步加深，人们提出越来越多的 PUF 实现方法（如涂层 PUF[9]）和 PUF 应用（如身份认证[10]、密钥生成[11]）。

自从 Pappu[8]提出物理不可克隆函数以来，凭借其具有良好的性质而受到广泛关注，并逐渐成为硬件安全领域研究中的一个热门话题。理想情况下，对 PUF 输入相同的激励，其会产生完全相同的响应，但是在实际中，由于噪音的影响，PUF 也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[11]。所以作者在 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、提取独立和顽健等属性。

作者的目标是基于 PUFS 设计一个 OT 协议 POT，该协议将作为应用中使用的子协议，或者和其他应用复合使用的协议。同时试图设计一个只需要分析一次就可以广泛应用的协议。为了实现这个目标，在协议的安全性分析中引入一个特殊的方法—通用可组合（UC, universal composition）框架[12]。

新的 UC 安全的 POT 协议具有如下功能和特点。1）POT 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，这大大减少了计算和通信开销。2）通过 PUFS 防止协议发送者和接收者的恶意行为。3）协议的交互简单，具有良好的计算效率，协议在一轮交互中实现 UC 安全的 string-OT 协议，与 bit-OT 相比，单轮通信效率提高了 $O(n)$ 倍。

2　物理不可克隆函数系统（PUFS）

2.1　物理不可克隆函数（PUF）

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物理不可克隆的函数[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，并且这个响应是完全不可克隆的。

PUF 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 也会产生不同的响应。

定义1　PUF。一个 PUF 是一个概率过程

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

其中，X 表示的激励集合，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

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

2.2　PUFS 框架

PUFS 主要包括一个 PUF 和一个提取算法（例如，Dodis[11]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 2 个：1) 通过提取算法设置阈值消除噪音的影响；2) 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 2 个不同模式执行：设置模式和重建模式。

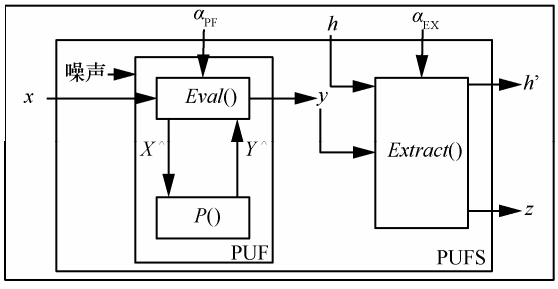

图 1　PUFS 一般框架

定义 3　PUFS。一个 PUFS 是一个概率过程

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

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 $h=\varepsilon$ 时，表示提取算法 Extract 在重建模式下利用激励 $x\in X$ 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

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

结论 1 根据对应于PUF的提取算法[11]的性质，一个 PUFS 具有如下属性。

广传播域属性。广传播域属性是在多项式时间内对于有限数量的激励 $x_1,\cdots,x_n$，与 x_k 的距离小于 $d_{\min}$ 的一个随机选择的激励 x 是可以忽略不计的。其中，$d_{\min}$ 是最小的汉明距离。

提取独立属性。对于所有的激励 $x_1,\cdots,x_n$，用一个 $dis(x_k,x)>d_{\min}$ 的激励 x 来评估 PUFS，那么提取算法会得出一个几乎平均的值 z。

顽健属性。提取算法设置阈值消除噪音的影响，即如果用激励 x 评估 PUF 两次得到 y 和 y'，那么提取算法返回相同的输出 z，即 $(z,h)\leftarrow Extract^{\mathrm{setup}}_{\alpha_{\mathrm{EX}}}(y,\varepsilon)$ 和 $(z,h)\leftarrow Extract^{\mathrm{reconstraction}}_{\alpha_{\mathrm{EX}}}(y',h)$。

3 POT 协议

本文基于 PUFS 提出了一个新的 OT 协议—POT。PUFS 不可克隆的激励响应行为以及 PUFS 的广传播、提取独立和顽健等属性使得 POT 协议可以完整地实现 OT 协议的基本功能。计算上不使用计算开销大的公钥加密体制，大大提高了计算效率。在通信开销上，POT 协议使用 3 次交互实现一轮 OT 协议，减少了通信开销。POT 协议如下。

前期准备

1) 分配接收者 P_j 一个物理不可克隆函数系统 PUFS。

2) 发送者 P_i 和接收者 P_j 已经同步一个加密方案 $E()$，其有如下性质。

① $E()$ 有效地加密有限个元组。

② $E()$ 可以被 $D()$ 解密即 $D(E(M))=M$。

3) 发送者 P_i 有 2 个接收者 P_j 不知道的秘密消息 s_0 和 s_1。

4) 接收者 P_j 有一个发送者 P_i 不知道的选择比特 b。

POT 协议

1) 注册阶段

① 给定接收者 P_j 一个物理不可克隆函数系统 PUFS，则相应的评估参数和提取参数是确定值。接收者 P_j 从 $\{0,1\}^{\lambda}$ 中随机选择 λ 长度的激励 x_k，其中，$1\leqslant k\leqslant N$。然后计算 $y_k\leftarrow Eval_p(\alpha_{\mathrm{PF}},x_k)$。把这些 N 对 (x_k,y_k) 存储到一个数据表 L 中。

② 接收者 P_j 把这个物理不可克隆函数系统PUFS传递给发送者 P_i。此时可以假定接收者 P_j 仍然具有这个固定提取参数的模糊提取算法。

2) 执行阶段

协议可以至多执行 N 次。

① 发送者 P_i 从 $\{0,1\}^{\lambda}$ 中随机选择 2 个字符串 r_0、r_1。然后把 $E(r_0,r_1)$ 传输给接收者 P_j。

② P_j 解密 $D(E(r_0,r_1))=r_0,r_1$。然后在 L 中随机选择一对 (x_k,y_k)，并把 $E(x_k\oplus r_b)$ 传送给发送者 P_i，这一对 (x_k,y_k) 在本次协议执行之后删除。

③ 发送者 P_i 解密得到 $x_k\oplus r_b$，然后计算 $y'_0\leftarrow Eval_p(\alpha_{\mathrm{PF}},x_k\oplus r_b\oplus r_0)$ 和 $y'_1\leftarrow Eval_p(\alpha_{\mathrm{PF}},x_k\oplus r_b\oplus r_1)$，接下来 P_i 利用提取算法计算得到：$(z_0,h_0)\leftarrow Extract^{\mathrm{setup}}_{\alpha_{\mathrm{EX}}}(y'_0,\varepsilon)$ 和 $(z_1,h_1)\leftarrow Extract^{\mathrm{setup}}_{\alpha_{\mathrm{EX}}}(y'_1,\varepsilon)$。最后计算 $S_0=s_0\oplus z_0$ 和 $S_1=s_1\oplus z_1$，然后传送 $E(S_0,h_0,S_1,h_1)$ 给接收者 P_j。

④ 接收者 P_j 首先解密得到 S_0、h_0、S_1、h_1，然后利用提取算法计算 $z'_b\leftarrow Extract^{\mathrm{reconstruction}}_{\alpha_{\mathrm{EX}}}(y_k,h_b)$，最后接收者 P_j 获得：$s_b=S_b\oplus z'_b$。

4 UC 框架下的 POT 协议

为了设计一个具有广泛适用性的通用协议，本文在协议的安全性分析中引入一个特殊的方法—通用可组合（UC, universal composition）框架[7]。

4.1 UC 框架

粗略地说，UC框架定义了2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，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Sim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Sim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，这在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 Sim，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和攻击者 $\overline{A}$ 控制的仿真器Sim以及理想功能 F 交互后的概率分布在计算上是不可区分的，则称协议 πUC 实现了理想功能 F。

4.2　不经意传输理想功能

OT 协议有2个参与方：发送者 P_i 和接收者 P_j。发送者 P_i 拥有2个秘密消息 s_0 和 s_1，接收者 P_j 拥有1个选择比特 b；执行 OT 协议后，接收者 P_j 获得选择秘密消息 s_b，但是不能获得秘密消息 s_{1-b}，并且发送者 P_i 不能知道接收者 P_j 的选择比特 b。通过 OT 理想功能 F_{OT} 可以实现这些需求，如图2所示。每个 PUFS 对应一个 ID。协议上下文对应一个会话标识 m。

F_{OT} 在一个发送者 P_i、一个接收者 P_j 和一个敌手仿真器 Sim 之间交互。

1) 每当从 P_i 接到消息 $(send, ID, m, P_i, (s_0, s_1))$，其中，$s_0$、$s_1 \in \{0,1\}^{\lambda}$，则 F_{OT} 存储 s_0, s_1，并发送 $(send, ID, m, P_i)$ 到 Sim。

2) 每当从 P_j 接到消息 $(choice, ID, m, P_j, b)$，其中，$b \in \{0,1\}$，则 F_{OT} 存储 b 并发送 $(choice, ID, m, P_j)$ 到 Sim。

3) 每当从 Sim 接到消息 $(transfer, ID, m)$，则 F_{OT} 检测是否已经存储元组 $(send, ID, m, P_i, (s_0, s_1))$ 和 $(choice, ID, m, P_j, b)$。如果是，则 F_{OT} 发送 $(transfer, ID, m, s_b)$ 到 P_i 并停机。如果不是，则不发送任何消息给 P_i（但继续运行）。

图 2　不经意传输理想功能 F_{OT}

4.3　安全性证明

POT 协议的安全性要求，在 POT 协议运行的最后：1）一个恶意发送者无法学习到比特 b；2）一个恶意接收者只能获得秘密消息 s_b 而不能获得秘密消息 s_{1-b}。

下面对以上两条性质进行详细讨论。

对于性质1），由于接收者随机选择激励 x_k，所以，$v = x_k \oplus r_b$ 信息理论上隐藏了信息 r_b，因而隐藏了 b。

对于性质2），为简单起见，假设 b=0，那么，发送者不能知道秘密消息 s_1。因为 PUFS 提取独立属性可以确保 z_1 均匀分布，所以对于发送者来说，s_1 在信息理论上被隐藏了。对于一个 PUFS 来说，由于其具有广传播域属性，接收者用 x_k 查询 PUF 的 $dis_{\mathrm{ham}}(x_k, v \oplus r_1) < d_{\min}$ 概率是微不足道的。所以在 L 中要么没有激励接近于 $v \oplus r_0$，要么没有激励接近于 $v \oplus r_1$。

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

证明　由于只考虑静态敌手腐化，所以可以利用腐化的一方来区分仿真。仿真器 Sim 模拟敌手 A 进行一次黑盒测试。如前所述，作者认为忠实地初始化一个 PUFS，并且当仿真器 Sim 拥有 PUFS 的时候，环境 Z 可以直接对其进行访问。

1）仿真双方都诚实的情况。①在理想世界中，每当 F_{OT} 发送 $(send, ID, m, P_i)$ 到 Sim，然后 Sim 提取2个随机值 (s_0', s_1') 作为假的秘密并将其发送到仿真的 P_i 上。然后仿真器 Sim 选择2个随机值 $r_0, r_1 \in \{0,1\}^{\lambda}$ 仿真真实的 P_i 并继续运行。②在理想世界中，每当 F_{OT} 发送 $(choice, ID, m, P_j)$ 到 Sim，然后 Sim 提取一个随机位 b' 并将其发送到仿真的 P_j 上。

如果 P_j 产生本地输出 s_b，那么 Sim 发送 $(transfer, ID, m)$ 到 F_{OT} 并被再次激活。

在注册阶段，A 和 Z 在协议中访问 PUF 作多项式数量的测量。对于敌手 A 有非常高的概率生成序列串 $(r_0, r_1, x_k \oplus r_b, s_0 \oplus z_0, s_1 \oplus z_1)$，该序列看起来是一个随机字符串的5元组：$r_0$ 和 r_1 是独立随机抽取的；通过随机获取 x_k 并异或 r_b 来定义 $x_k \oplus r_b$；$s_0 \oplus z_0$ 和 $s_1 \oplus z_1$ 看起来是随机串，因为提取算法可以保证响应具有高不相关性。因此，环境 Z 不能区分是在现实世界 A 和 POT 进行通信还是理想世界仿真的 A 和 F_{OT} 进行通信。

2) 发送者被腐化的情况

接下来假设发送者 P_i 是不诚实的而接收者 P_j 是诚实的。仿真器 Sim 将从不诚实的发送者中使用

其永久的 PUFS 访问权限来提取秘密(s_0,s_1)。仿真器 Sim 无顺序地等待满足 2 个条件：首先， A 指示恶意发送者 P_i 来发送 $(ID,m,P_i,(r_0,r_1))$ 到仿真中，其次， F_{OT} 发送 $(choice,ID,m,P_j)$ 到 Sim。然后 Sim 获得一个随机串 $v \leftarrow \{0,1\}^{\lambda}$ 并把它返回给 P_i。当 A 指示 P_i 来发送 $(ID,m,P_i,P_j,q_0,h_0,q_1,h_1)$ 到 P_j 时，Sim 发送 $(transfer,ID,m)$ 到 F_{OT} 并再次被激活。Sim 是通过运行 POT 协议提取秘密 s_0,s_1：$s_0 := z_0 \oplus q_0$ 和 $s_1 := z_1 \oplus q_1$。最后，Sim 发送 $(send,ID,m,P_i,(s_0,s_1))$ 到 F_{OT} 并继续仿真。

首先， P_i 在2个世界中收到的消息是一个均匀随机串。其次， P_i 的输出在2个世界中是一样的，所以 Z 不能区分仿真器仿真的是理想世界消息还是真实世界消息。

3) 接收者被腐化的情况

最后作者考虑的情况是，发送者 P_i 是诚实的而接收者 P_j 是不诚实的。在注册阶段，仿真器 Sim 观察腐化接收者的 PUF 查询（由 A 和 Z 实现）并存储激励响应对到一个 L 中。这些将在后来帮助仿真器在协议执行中提取秘密位。

每当 F_{OT} 发送 $(send,ID,m,P_i)$ 到 Sim，则 Sim 从 $\{0,1\}^{\lambda}$ 中提取一对随机值 (r_0,r_1) 并发送 $(ID,m,P_i,(r_0,r_1))$ 到仿真中。如果只存在激励 x_k 使得 $dis(r_0,v \oplus x_k) < d_{\min}$，则设置 $b := 0$。如果只存在激励 x_k 使得 $dis(r_1,v \oplus x_k) < d_{\min}$，那么设置 $b := 1$。如果没有这样的激励存在，那么随机选择 $b \leftarrow \{0,1\}$。然后 Sim 发送 $(send,ID,m,P_j,v)$ 到仿真中。由于 P_j 是腐化的，Sim 可以发送 $(choice,ID,m,P_i,b)$ 到 F_{OT}。当接收到消息 $(choice,ID,m,P_j)$ 时，Sim 发送 $(transfer,ID,m,s_b)$ 到被 A 控制的腐化用户 P_j。然后仿真器 Sim 选择一个随机值 $s_{1-b} \leftarrow \{0,1\}^{\lambda}$。最后仿真器 Sim 使用 PUFS 来确定 z_0、 h_0、 z_1 和 h_1。

分析表明，在协议执行中，Z 和 A 的共同看法与 Z 和理想过程用 S 仿真 A 的共同看法是不可区分的。2个执行唯一的区别是 P_j 收到的最后消息 $(s_0 \oplus z_0,h_0,s_1 \oplus z_1,h_1)$。假设敌手 A 不能用 $v \oplus x_{1-b}$ 小于 $d_{\min}$ 的任何激励查询 PUF，此时通过 PUFS 提取独立属性，z_{1-b} 是均匀分布的。因此，从 A 的角度来看，对于所有的值 z_{1-b}， $(s_{1-b} \oplus z_{1-b},h_{1-b})$ 是同分布的。所以环境 Z 不能区分仿真器仿真的理想世界消息和真实世界消息。

5 相关工作比较

基于判定 Diffie-Hellman（DDH）假设，Fischlin[5]设计了一个由第三方辅助完成的 UC 安全的 OT 协议。该方案在四步交互中利用特殊的辅助信息实现 bit-OT 功能。但是该方案存在以下问题：辅助第三方的假设，增加了协议的交互次数，降低了协议的通信效率，限定了具体的应用场景。基于二次剩余和判定复合剩余假设，TaumanKalai[6]也提出类似的协议。

最近，基于 PUF，Ruhrmair[7]利用交互散列实现了一个 OT 协议。该方案主要缺点是，协议的计算开销比较大，因为交互散列要计算 m 轮才能实现一次协议交互。

本文的 POT 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。新的 POT 协议直接实现了串的 OT 传输，与 bit-string 协议相比单轮通信效率提高了 $O(n)$倍，利用 PUFS 的广传播、提取独立和顽健等属性实现了理想世界和现实世界的不可区分性。计算上不使用计算开销大的公钥加密体制，大大提高了计算效率。在通信开销上，本文的 POT 协议使用3次交互实现一轮串 OT 协议，减少了通信开销。表1为 POT 协议和其他协议的比较。

表 1 POT 协议与其他协议的比较

OT 方案	安全假设	交互次数	一轮协议	每次交互计算量/轮
Fischlin's 方案	DDH	4	Bit-OT	1
Ruhrmair's 方案	PUF	3	String-OT	m
本文方案	PUFS 安全属性	3	String-OT	1

6 结束语

本文首先讨论了 PUFS 的一般框架，定义了其属性，然后基于这个框架，提出了一个新的 OT 协议（POT 协议）。和以往 OT 协议不同的是，POT 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，这大大减少了协议的计算和通信开销。最后在 UC 框架内详细讨论了这个协议，并给出了相应的安全性证明。

参考文献：

[1] KILIAN J. Founding cryptography on oblivious transfer[A]. Proceedings of the Twentieth Annual ACM Symposium on Theory of Com-

puting, STOC 1988[C]. Chicago, Illinois, 1988. 20-31.

[2] BEN-OR M, GOLDWASSER S, WIGDERSON A. Completeness theorems for non-cryptographic fault-tolerant distributed computation[A]. Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC 1988[C]. Chicago, Illinois, 1988. 1-10.

[3] CREPEAU C, VANDEGRAAF J, TAPP A. Committed oblivious transfer and private multiparty computation[A]. Computer Science Advances in Cryptology, Proceedings of Eurocrypt'95[C]. 1995. 110-123.

[4] RABIN M O. How to Exchange Secretes by Oblivious Transfer[R].Tech Rep TR-81, Harvard University, 1981.

[5] AIELLO W, ISHAI Y, REINGOLD O. Priced oblivious transfer: how to sell digital goods[A]. Advances in Cryptology2Eurocrypt 2001[C]. 2001. 119-135.

[6] KALAI Y T. Smooth projective hashing and two-message oblivious transfer[A]. Advances in Cryptology-Eurocrypt 2005[C]. 2005. 78-95.

[7] RUHRMAIR U. Oblivious transfer based on physical unclonable functions[J]. Lecture Notes in Computer Science, 2010, 6101:430-440.

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

[9] TUYLS P, SCHRIJEN G J, SKORIC B, *et al*. Read-proof hardware from protective coatings[A]. Cryptographic Hardware and Embedded Systems Workshop Lecture Notes in Computer Science[C]. New York, USA, 2006. 369-383.

[10] HAMMOURI G, OZTURK E, BIRAND B, *et al*. Unclonable light weight authentication scheme[A]. Proceedings of the 10th International Conference on Information and Communications Security (ICICS 2008)[C]. Springer, Heidelberg, 2008. 33-48.

[11] 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.

[12] CANETTI R. Universally composable security:a new paradigm for cryptographic protocols[A]. Proceedings of the 42nd IEEE Symposium on the FOCS[C]. New York, USA, 2001. 136-145.

作者简介：

郭渊博（1975-），男，陕西西安人，解放军信息工程大学副教授，主要研究方向为无线网络安全攻防、安全协议设计、系统可生存性等。

张紫楠（1987-），男，辽宁葫芦岛人，解放军信息工程大学硕士生，主要研究方向为基于 PUF 的安全协议设计。

杨奎武（1979-），男，吉林辽源人，解放军信息工程大学讲师，主要研究方向为无线网络安全。