基于混淆的广播多重签名方案

李 磊 贾惠文 班学华 何宇帆
(综合业务网理论及关键技术国家重点实验室(西安电子科技大学) 西安 710071)
(西安电子科技大学通信工程学院 西安 710071)

摘 要 基于Lin等人于2016年提出的不可区分混淆,提出了一个新的广播多重签名方案,其使用混淆后的验证电路作为验证密钥,对部分签名和多重签名进行验证。在本方案中,每个签名成员生成自己的部分签名,签名收集方只需要将每个成员的部分签名进行模乘,即可得到多重签名。每个签名方的部分签名的长度、签名算法和验证算法的复杂度不随签名人数的多少而变化。本方案满足不可伪造性和不可否认性等性质,同时可以抵抗外部量子攻击。

关键词 不可区分混淆,数字签名,广播多重签名,抗量子攻击,安全性证明
中图法分类号 TP309 **文献标识码** A

Obfuscation-based Broadcasting Multi-signature Scheme

LI Lei JIA Hui-wen BAN Xue-hua HE Yu-fan
(State Key Laboratory of Integrated Services Networks (Xidian University), Xi'an 710071, China)
(School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)

Abstract Based on the indistinguishability obfuscation, this paper proposed a new broadcast Multi-signature scheme. By using the confused verification circuit as verification key, the part signature and the multi-signature can be verified. In this scheme, after generating the part signature by each signer, multi-signature is obtained by the modulation of the part signature which is collected by signature collector. The length of the part signatures, the complicacy of its algorithm and the complicacy of the verification algorithm are independent when the number of the signers changes. The properties of against external attack, non-forgery and non-disavowal are obtained in this scheme. Its securities are proved in the random oracle model.

Keywords Indistinguishability obfuscation, Digital signature, Broadcasting multi-signature, Against quantum attack, Security proof

1 引言

现实生活中,很多时候需要多人对同一文件进行签字,例如在车载网络中,每个车载通信单元都需要对同一个事件进行签名;在电子商务中,需要若干个机构部门对同一个文件进行签名等,这些应用场景中需要的签名就是多重签名。多重签名最早由Itakura和Nakamur[1]提出。在多重签名中,由多个签名人对同一个明文做出部分签名,再由签名收集人把部分签名整合成一个多重签名。根据部分签名方签名时是否按照一定的顺序,将在签名方有一定顺序的多重签名称为有序多重签名[2-4],将无一定签名顺序的多重签名称为广播多重签名[5-6]。

近年来对多重签名的应用研究成为了热点,多重签名被认为可以应用到电子合同签署[7]、教务管理系统[8]、成绩管理系统[9]及专家会诊[10]等多个领域。大量基于不同的困难性问题的多重签名方案正在被不断提出和逐步改进,最早被提出的多重签名方案是基于离散对数的,此类方案被提出之后,得到了不断的改进,例如文献[11-12]中的方案都属于此类型的多重签名方案。随着椭圆曲线技术在密码学中的应用,基于椭圆曲线的多重签名方案被提出[6];为了增强方案的安全性和实用性,随后又对其进行了不断改进[14-15]。Zeng等人[16]于2001年首次将量子相关的技术应用到签名方案中,并提出量子签名方案。Wen等人[17]于2007年以后将量子签名扩展,并提出量子多重签名方案。相比于基于其他困难性问题的多重签名具,量子多重签名体制有高效且安全的性质。在以上基于不同密码学难题的多重签名体制中,只有量子多重签名体制可以抗量子攻击。

广播多重签名是多重签名的一种形式,其特点是每个签名方把自己的部分签名传递给签名收集方,签名收集方收集到部分签名后依次进行验证,若所有的签名都验证通过,则合成多重签名,否则不进行整理合成。基于不同的困难性问题,广播多重签名方案多种多样,Harn[18-19]于1994年最早提出了基于离散对数的广播多重签名,之后有学者不断提出基于此类困难性问题的广播多重签名方案,但是这些方案的参与

本文受国家自然科学基金(61472309)资助。

李 磊(1992-),男,硕士生,主要研究方向为格公钥密码、混淆、多重签名,E-mail:chan_yi@live.cn(通信作者);贾惠文(1990-),男,博士生,主要研究方向为公钥密码、多线性映射与混淆;班学华(1991-),女,硕士生,主要研究方向为格公钥密码、混淆、可搜索加密;何宇帆(1991-),男,硕士生,主要研究方向为格公钥密码、混淆。

方都需要彼此之间进行多次数据交换，从而增大了系统的通信量，而且易受到攻击[20]。文献[21]对此问题进行了研究，并给出了一种解决方案。虽然基于各种困难性问题的广播多重签名较多，但是能够抗量子攻击的多重签名只有基于量子的多重签名体制，还没有非量子广播多重签名体制可以抵抗量子攻击。考虑到量子密码体系存在着抗干扰性差、无法远距离发送消息、窃听方的攻击可能造成量子态的丢失和信道衰减等还需继续研究的问题，本文引入了混淆技术，采用混淆技术与多重签名构造相结合的思路，提出一种新型的基于混淆技术且抗量子攻击的多重签名方案。

最早提出混淆的目的是在不影响软件功能的情况下将其代码进行掩盖，它在软件保护等领域有着很重要的应用价值，但是早期的混淆缺乏严格的形式化定义及安全性证明[23-24]。Barak 等人[25]于 2001 年首次给出混淆的形式化定义，所给出的混淆满足虚拟黑盒混淆性质，即混淆后的程序被认为是一个黑盒，其内部的任何信息无法被知晓；他们同时提出了混淆领域的众多成果，但这个定义过强，被证明是无法构造出任意函数的通用混淆。随后，研究者们不断尝试构造定义相对弱化的混淆方案，期间提出了很多满足不同性质的混淆方案。Garg 等人[26]于 2013 年构造出安全性较低但可以适用于任何多项式时间电路的不可区分混淆，随后不可区分混淆相继被应用到全域哈希、一轮多方密钥协商协议和可否认加密方案等密码学方案中。

随着安全混淆方案的提出，很多密码方案变得易于构造且安全可靠。本文基于不可区分混淆，提出一种新的广播多重数字签名。

2 预备知识

2.1 广播多重签名

设 Alice 是消息的发送方，$U_i(i=1,2,\cdots,t)$表示 t 个签名方，Charlie 表示签名的收集方，则广播多重签名的基本过程是：Alice 将消息 m 通过广播的方式发送给签名方 $U_i(i=1,2,\cdots,t)$，签名方 $U_i(i=1,2,\cdots,t)$对 m 进行签名后将签名发送给签名收集方 Charlie，Charlie 收到签名后对每个签名的有效性进行验证，如果每个签名都有效，则对签名进行整理生成多重签名，再发送给验证方 Bob，否则舍弃签名，如图 1 所示。

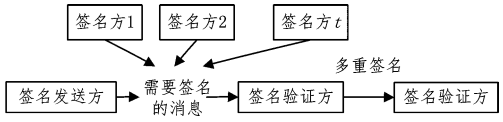

图 1 广播多重签名的过程

2.1.1 多重签名的定义

多重签名包括以下几个步骤：

(1)系统初始化(Setup)：系统为每个签名方生成公私钥对(sk_i,vk_i)，将私钥 sk_i 通过安全通道发送给签名各方。

(2)部分签名(Sign)：签名用户对需要签名的明文 m 进行签名，将完成的部分签名 $\sigma_i(i=1,\cdots,t)$广播出去。

(3)签名收集(MSign)：签名收集方 Charlie 收集各个签名用户的签名并进行验证，若验证不通过，则终止多重签名过程；若签名全部通过验证，则签名收集方 Charlie 将部分签名合并成多重签名 σ，然后将多重签名发送给签名接收方。

(4)多重签名验证过程(MVf)：签名接收方接收到签名收集方 Charlie 发来的多重签名并进行验证，若验证通过则接受签名，即为有效的多重签名；若验证失败，则拒绝签名。

2.1.2 安全性模型

广播多重签名方案需要满足密钥的安全性、多重签名的不可伪造性及部分签名的不可否认性等多个性质。

针对多重签名的不可伪造性，下面描述一个选择明文攻击下的攻击方 $\mathcal{A}$ 和挑战方之间的 Game。将攻击方 $\mathcal{A}$ 和挑战方之间的交互过程记$\Pi=(\text{Setup},\text{Sign},\text{MSign},\text{MVf})$。

初始化：挑战方运行 Setup 算法来获得公共参数和公私钥对(sk_i,vk_i)，敌手 $\mathcal{A}$ 将会获得公共参数及公钥；

询问：$\mathcal{A}$ 选择明文 m_i 要求签名，得到明文 m_i 的多重签名 σ_i；

回答：询问多项式时间 q 次后，攻击方 $\mathcal{A}$ 利用 q 对明文签名对$(m_i,\sigma_i)(i=1,\cdots,q)$来伪造明文 m^* 的签名 σ^*；然后使用多重签名的验证程序 MVf，得到输出 $b\in\{0,1\}$。定义攻击方 $\mathcal{A}$ 在 Game 中的优势为 $Adv_{\mathcal{A}}=\Pr[b=1]-\frac{1}{2}$。

定理 1 如果攻击方 $\mathcal{A}$ 在 Game 中的优势是可忽略的，那么广播多重签名方案在选择明文攻击下是不可伪造的。

2.2 混淆

混淆发展至今，从虚拟黑盒性质到不可区分性质，关于它的多种不同性质被提出。其具体形式化的定义[26]如下：

定义 1(虚拟黑盒混淆) 对于一个多项式时间的算法 $\mathcal{O}(\cdot)$，如果满足以下 3 个性质，那么称 $\mathcal{O}(\cdot)$是满足虚拟黑盒混淆。

(1)功能性：对于每个电路 C，输出 $\mathcal{O}(C)$表示与原电路 C 计算同样功能的电路。

(2)效率性：存在一个多项式 P，满足对于所有电路 C，$|\mathcal{O}(C)|\leqslant p(|C|)$。

(3)虚拟黑盒性质：对所有 PPT A 和所有电路 C，存在一个 PPT S 和一个可忽略的函数 α 满足不等式$|\Pr[A(\mathcal{O}(C))=1]-\Pr[S^C(1^{|C|})=1]|\leqslant\alpha(|C|)$。

虽然 Barak 等人给出了形式化的混淆定义，但是一个适合于通用电路且满足虚拟黑盒性质的混淆被证明是不存在的。随后，相对较弱的不可区分性混淆的概念又被提出，Garg 等人于 2013 年基于多线性映射构造出了第一个不可区分性混淆，并利用不可区分混淆器实现了功能加密(functional encryption)。

定义 2(不可区分性混淆) 如果可以满足如下条件，那么一个一致性 PPT 算法 $\mathcal{IO}$ 对于一类电路$\{C_\lambda\}$而言被称为不可区分性混淆。

(1)对所有安全参数 $\lambda\in\mathbb{N}$，$c\in C_\lambda$，对所有输入 x，有：

$\Pr[C'(x)=C(x):C'\leftarrow i\mathcal{O}(\lambda,C)]=1$

(2)对任意 PPT 区分器 D(不必是一致性的)，存在一个可忽略的函数 α 使得如下条件成立：对于所有安全参数 $\lambda\in\mathbb{N}$，以及所有电路对 $C_0,C_1\in C_\lambda$，如果对所有输入 x，$C_0(x)=C_1(x)$，那么：

$|\Pr[D(\mathcal{IO}(\lambda,C_0))=1]-\Pr[D(\mathcal{IO}(\lambda,C_1))=1]|\leqslant\alpha(\lambda)$

但是随着 GGH 多线性映射方案被 Hu 和 Jia 攻击之后[35]，基于 GGH 多线性映射的不可区分混淆方案也变得不安全，Miles 等[36]于 2016 年提出一种攻击方案，致使 Gary 等人提出的不可区分混淆可以被攻击。之后，新的满足不可区

分性质的混淆方案又不断被提出。同年，Lin[37] 根据常数阶分级加密方案提出一个不可区分混淆，并将此不可区分混淆的安全性规约到格上的带错误学习困难性（Learning With Errors，LWE）问题上。本文用于构造广播多重签名方案的不可区分混淆器就是采用 Lin 提出的方案进行设计的。

2.3 伪随机函数（PRF）

伪随机函数（PRF）是密码学中的一个基本概念，具有广泛的应用。PRF 是一个确定的多项式时间的算法，由 $\mathcal{K}\times\mathcal{X}\to\mathcal{Y}$ 映射，其中 $\mathcal{K}$ 是密钥空间，$\mathcal{X}$ 是定义域，$\mathcal{Y}$ 是值域。伪随机函数 F 的输入为 $(k,x)\in(\mathcal{K}\times\mathcal{X})$，输出为 $F(k,x)\in\mathcal{Y}$，对于密钥 $k\in\mathcal{K}$，伪随机函数 $F(k,\cdot)$ 可以有效计算出所有满足 $x\in\mathcal{X}$ 的值。Boneh 等[31] 于 2013 年提出 Constrained PRF 的概念。与 PRF 不同的是，在 Constrained PRF 中限制密钥 k_S 来自于主密钥 k，而限制密钥可以计算出 PRF 在定义域的某个确定子集合中的伪随机函数值，不在这个子集合中的值无法被求出。形式化表示如下。

定义 3　如果在伪随机函数系统中增加密钥空间 $\mathcal{K}_s$ 和两个算法 $F.constrain$ 和 $F.eval$，那么一个伪随机函数 PRF 就是限制伪随机函数（Constrained PRF），即伪随机函数 $F:(\mathcal{K}\times\mathcal{X})\to\mathcal{Y}$ 被限制在集合 $\mathcal{S}\subseteq 2^{\mathcal{X}}$。算法 $F.constrain$ 和 $F.eval$ 如下：

（1）$F.constrain(k,S)$ 是一个随机多项式时间算法，其输入为伪随机函数的密钥 $k\in\mathcal{K}$ 和集合 $S\in\mathcal{S}$（也即 $S\subseteq\mathcal{X}$），输出为限制密钥 $k_S\in\mathcal{K}_c$，此限制密钥 k_S 可以计算出伪随机函数 $F(k,x)$ 在 $x\in S$ 中的所有函数值，但是不能求出此外的函数值。

（2）$F.eval(k_S,x)$ 是一个确定的多项式时间算法，其输入为限制密钥 $k_S\in\mathcal{K}_c$ 和值 $x\in\mathcal{X}$。如果 k_S 是 $F.constrain(k,S)$ 在某个确定的 PRF 中的主密钥 $k\in\mathcal{K}$ 的输出，那么：

$$F.eval(k_S,x)=\begin{cases}F(k,x), & \text{if } x\in S\\ \perp, & \text{otherwise}\end{cases}$$

其中，$\perp\notin\mathcal{Y}$。

自从 Boneh 等人提出 Constrained PRF 概念以来，其他学者又提出了不同的 Constrained PRF 的变形体，如刺穿 PRF（puncturable PRF）[29]、功能 PRF（Functional PRF）[32] 和代理 PRF（Delegatable PRF）[33]。其中，刺穿 PRF（puncturable PRF）和不可区分性混淆组合后，可以构造出多个密码学方案。

文献[29]中给出了刺穿 PRF 的形式化定义。

定义 4　对于一个可刺穿的伪随机函数族（puncturable PRFs）F，给定 3 个图灵机（Key_F，$Puncture_F$，$Eval_F$）和一对可计算函数（$n(\cdot)$ 和 $m(\cdot)$），满足如下条件：

（1）刺穿情况下的功能保持性：对于任意 PPT 敌手 $\mathcal{A}$，$\mathcal{A}(1^\lambda)$ 输出一个集合 $S\subseteq\{0,1\}^{n(\lambda)}$，且对所有的 $x\in\{0,1\}^{n(\lambda)}$，$x\notin S$，有：

$$\Pr[Eval_F(K,x)=Eval_F(K_S,x):K\leftarrow Key_F(1^\lambda),K_S=Puncture_F(K,S)]=1$$

（2）刺穿点的伪随机性：对于每个 PPT 敌手，$(\mathcal{A}_1,\mathcal{A}_2)$ 使得 $\mathcal{A}_1(1^\lambda)$ 输出一个集合 $S\subseteq\{0,1\}^{n(\lambda)}$ 和状态 σ，在 $K\leftarrow Key_F(1^\lambda)$，$K_S=Puncture_F(K,S)$ 时，有：

$$|\Pr[\mathcal{A}_2(\sigma,K_S,S,Eval_F(K,S))=1]-\Pr[\mathcal{A}_2(\sigma,K_S,S,U_{m(\lambda)\cdot|S|})=1]|=negl(\lambda)$$

其中：$Eval_F(K,S)$ 表示 $Eval_F(K,x_1),\cdots,Eval_F(K,x_k)$ 的串联，$S=\{x_1,\cdots,x_k\}$ 是 S 内元素的字典序排列，$negl(\lambda)$ 是可忽略函数，U_l 表示 l 比特的均匀分布。

3　基于混淆的广播多重签名

3.1 具体方案

广播多重签名方案具有很广泛的应用，而最新提出的功能强大的不可区分混淆也可以在广播多重签名中得到应用，这可以使得广播多重签名方案的实现变得很简洁。以下是具体实现方案。

系统初始化 $Setup(\cdot)$：输入安全参数 1^λ，输出系统参数 sp。

签名参数生成 $SKG(\cdot)$：系统选取一个大素数 N，选择 t 个不同的随机数作为签名方 U_i 的密钥 sk_i（$i=1,\cdots,t$）（$sk_i\ll N$），并计算 $sk=\sum_{i=1}^{t}sk_i$（$sk<N$）。同时，系统为每个签名方 U_i（$i=1,2,\cdots,t$）生成各自的伪随机函数 $PRF(sk_i,\cdot)$，记为 PRF_i。其中，PRF_i 是可刺穿伪随机函数，输入为 l 比特，输出 λ 比特。选择单向函数为 $f(\cdot)$，明文空间为 $M=\{0,1\}^l$。系统将 t 个不同的 sk_i 和 PRF_i 分别通过安全通道发送给每个签名方 U_i（$i=1,2,\cdots,t$），并公布签名方集合 $U=\{U_i\}_{i=1}^t$、混淆后的签名验证程序和多重签名验证程序。

部分签名 $Sign(\cdot)$：Alice 通过广播信道广播明文 m 并发送给要签名的用户 U_i，用户 U_i 选择一个随机数 s_i，计算 $x_i=PRF(sk_i,s_i)$，然后 U_i 进行签名操作 $m^{sk_i}\cdot x_i=\sigma_i(\mathrm{mod}\ N)$，$\sigma_i$ 表示用户 U_i 对明文的签名。部分签验证程序 p_i 如图 1 所示。

验证签名
常数：签名密钥 sk_i 和 PRF_i
输入：明文 m、签名 σ_i 和随机数 s_i
判断是否
$f(m^{sk_i}\cdot PRF(sk_i,s_i)(\mathrm{mod}\ N))=f(\sigma_i)$
如果相等则输出 1，如果不等则输出 0。

图 1　部分签名验证程序

对以上的验证程序混淆后的程序记为 $i\mathcal{O}(p_i)$。签名方 U_i 将签名 σ_i、明文 m、选择的随机数 s_i 和混淆后的验证程序 $i\mathcal{O}(p_i)$ 发送给签名收集方 Charlie。

签名收集 $Comp(\cdot)$：签名收集方 Charlie 将每个用户 U_i 发给自己的签名 σ_i、明文 m 和随机数 s_i 输入混淆程序 $i\mathcal{O}(p_i)$ 进行一一验证。若程序 $i\mathcal{O}(p_i)$ 输出 1，则 U_i 的签名有效，合并多重签名；若程序 $i\mathcal{O}(p_i)$ 输出 0，则无效，协议终止。若每个用户 U_i 的签名都正确，则 Charlie 计算多重签名 $\sigma=\prod_{i=1}^{t}\sigma_i(\mathrm{mod}\ N)$。多重签名验证程序 p 如下算法 2 所示。

验证多重签名
常数：收集签名方私钥 sk 和 $PRF_i(i=1,\cdots,t)$
输入：多重签名 σ、明文 m 和签名用户所拥有随机数 $s_i(i=1,\cdots,t)$
判断是否
$f(\sigma)=f(m^{sk}\cdot PRF(sk_1,s_1)\cdot PRF(sk_2,s_2)\cdot\cdots\cdot PRF(sk_t,s_t))(\mathrm{mod}\ N)$
如果相等则输出 1，如果不等则输出 0。

图 2　多重签名验证程序

将以上的多重签名验证程序混淆后的程序记为 $i\mathcal{O}(p)$。签名收集方将多重签名 σ、明文 m、每个签名用户选择的随机

数 $s_i(i=1,\cdots,t)$以及混淆后的多重签名验证程序 $i\mathcal{O}(p)$发送给验证方 Bob。

多重签名验证过程 $MVerif(\cdot)$:Bob 收到多重签名 σ、明文 m 和混淆后的多重签名验证程序 $i\mathcal{O}(p)$后,将明文 m、多重签名 σ 和每个签名用户选择的随机数 $s_i(i=1,\cdots,t)$输入验证程序 $i\mathcal{O}(p)$中。若程序 $i\mathcal{O}(p)$输出 1,则 Bob 接受多重签名;若程序 $i\mathcal{O}(p)$输出 0,则终止协议。

3.2 安全性分析

3.2.1 抗量子特性

量子攻击算法主要指 1994 年 Shor 提出的 Short 算法和 1996 年 Grover 提出的 Grover 算法。Shor 算法是一种针对大数分解和离散对数问题的有效求解方案;Shor 算法可以将原来是 NP 问题的以上两个困难性问题变为容易解决的问题,所以以上两种困难性问题在量子计算条件下变成了可以求解的问题,基于此两种困难性问题的方案的安全性也将无法保证。Grover 算法没有具体针对某一个特定的困难性,而是对通用的计算效率的提高。虽然量子密码可以攻击一部分困难性问题,但是仍然有一些困难性问题是现有的量子计算算法无法求解的。密码学中的格公钥密码就可以抵抗现有的量子攻击,在量子计算的条件下,格上带错误学习的困难性(LWE)问题仍然是难解的。

本文提供的基于不可区分混淆的广播多重签名方案若能抵抗以上的两种算法,即可表明本文方案具有抗量子攻击性。在基于不可区分混淆的广播多重签名方案中,签名方的私钥秘密保存,若要证明本文方案具有抗量子计算攻击性,只需要证明具有量子计算能力的攻击方获取到本方案的验证公钥之后无法获取到签名私钥即可。又因为本文所给出的验证公钥为一个经过不可区分混淆器混淆后的程序,所以下面只需要证明:具有量子计算能力的攻击方即使获取到混淆后的验证公钥程序,也依然无法得到签名私钥。详细的证明过程如下。

定理 2 如果文中使用的 Lin 等人提出的混淆器满足不可区分混淆性,那么基于此不可区分混淆的广播多重签名方案具有抗量子计算攻击性。

证明:首先构造如下的模拟程序 p'。

模拟程序 p′
常数:随机数 k、PRF
输入:明文 m、签名 σ 和随机数 s
判断是否
$f(m^k \cdot PRF(k,s)(\mathrm{mod}\ N))=f(\sigma)$。
如果相等则输出 0,如果不等则输出 1。

假设存在一个算法 $\mathcal{B}$ 可以通过模拟程序 p' 和混淆后的多重签名验证程序 $i\mathcal{O}(p)$的输出获取到程序 $i\mathcal{O}(p)$内隐含的私钥 sk,如果获取成功,则算法输出 1,否则输出 0。首先,攻击方执行 $Setup()$操作,获取到系统所用的参数。攻击方选择一个明文 m 发送给挑战方,挑战方执行整个签名过程,将多重签名发动给攻击方 $\mathcal{A}$。

具有量子计算能力的攻击方 $\mathcal{A}$ 和挑战方之间的密码学实验如下:

1)攻击方 $\mathcal{A}$ 选择一个随机数 k 发给挑战方。

2)挑战方构造如上的一个模拟程序 p' 和多重签名验证程序 $i\mathcal{O}(p)$发给攻击方。

3)攻击方接收到两个程序 p' 和 $i\mathcal{O}(p)$,调用算法 $\mathcal{B}$,输入两个程序,获取输出。

攻击方和挑战方进行如上的密码学实验多项式次,如果在多项式次内攻击得到的输出为 1,则攻击成功;否则攻击失败。

如果攻击方得到的输出为 1,那么将此时选取的随机数 k 分别输入两个程序中,输出 0 的程序为模拟程序 p',而输出 1 的程序为多重签名验证程序 $i\mathcal{O}(p)$。按此即可区分两个程序,这与本方案所使用的基于格上 LWE 困难性问题的混淆器具有不可区分性相矛盾。因为格上的 LWE 困难性问题在量子计算下是不容易求解的,所以不存在这样的算法 $\mathcal{B}$,即在量子计算条件下无法通过签名验证公钥程序获取到签名私钥。

证明完毕。

3.2.2 不可伪造性

首先构造一个验证程序 2,如图 3 所示。

部分签名验证签名 2
常数:签名密钥 sk、PRF、(m^*,s^*)和 z^*
输入:明文 m、签名 σ_i 和随机数 s_i
1. 判断(m,s)与(m^*,s^*)是否相等,若相等,再检测 σ_i 与 z^*,若是则输出 1,若不是则输出 0。
2. 若不相等,再判断 $f(m^{sk} \cdot PRF(sk,s)(\mathrm{mod}N))$与 $f(\sigma)$是否相等。如果相等则输出 1,如果不等则输出 0。

图 3 验证签名 2

将原来的验证签名程序使用随机字符串填充,使得其与验证签名 2 具有相同的长度,并记为验证签名程序 1。

定理 3 如果文中使用的不可区分混淆程序是安全的,使用的 PRF 是安全的约束伪随机函数,单向函数 $f(\cdot)$是安全的单向函数,那么签名方案在抵抗明文攻击下是不可伪造的。

证明:使用一系列的 Game 来证明。可以证明依次相邻的两个 Game 之间具有可忽略的不同优势,通过最终的 Game 可以说明文中的签名方案如果是可伪造的,那么可以攻破安全的单向函数。

Game0:具体过程如下:

1)攻击方选择一个明文(m^*,s^*)发给挑战方。

2)挑战方选择 PRF 的密钥 sk,将混淆后的签名验证程序 VK 公布。

3)攻击方使用不同于(m^*,s^*)的明文向签名 $Oracle$ 询问多项式次,得到 $m^{sk} \cdot PRF(sk,s)(\mathrm{mod}\ N)$。

4)攻击方伪造一个签名 σ^*,并与(m^*,s^*)一起输入签名验证程序,如果输出 1,则伪造成功。

Game1:设置 $z^*=f(m^{*sk} \cdot PRF(sk,s^*)(\mathrm{mod}\ N))$,令 VK 是签名验证程序 2 的混淆。其他过程与 Game0 相同。

Game2:设置 $z^*=f(t)$,t 随机选取。

首先证明对于任何多项式时间的攻击方,Game0 和 Game1 之间的不同优势是可忽略的。可以发现,除了 Game1 中增加了 m^* 和 z^* 之外,它在其他方面都与 Game0 相同。如果存在多项式时间的攻击方 $\mathcal{A}$ 可以找出 Game0 和 Game1 之间的不同优势为不可忽略的,那么就可以创建一个算法 $\mathcal{B}$,它能够区分不可区分混淆器。发送签名验证程序 1 和签名验证程序 2 给 $\mathcal{IO}$ 挑战方,$\mathcal{IO}$ 混淆后传回验证程序 VK,调用 $\mathcal{A}$,如果在进行 Game0,则说明 $\mathcal{IO}$ 挑战方选择了签名验证程序 1,反之则选择了签名验证程序 2。如此,便可以区分 $\mathcal{IO}$ 挑战方对两个混淆后的程序。

然后证明对于多项式时间的攻击方，Game1 和 Game2 之间的不同优势是可忽略的。经过讨论发现，除了 Game2 中改变 $z^*=f(t)$ 之外，它在其他方面都与 Game1 相同。如果存在多项式时间的攻击方 $\mathcal{A}$ 可以找出 Game1 和 Game2 之间的不同优势为不可忽略的，那么在假设离散对数难题易解的情况下，就可以创建一个算法 $\mathcal{B}$，它能够攻破安全的伪随机函数 PRF。选择随机数 s^*，发送不同于 s^* 的随机数 s 给 PRF 挑战方，PRF 挑战方选择对应的 PRF 的密钥 sk，并输出 PRF 作用后的值，记为 a，将多项式次询问后计算出的值记为 a^*。如果 a^* 是 PRF 在点 s^* 的输出，那么这个过程在 Game1 里；如果是随机的，则这个过程在 Game2 里。那么当算法 $\mathcal{B}$ 输出 1 时，伪造成功。因为算法 $\mathcal{B}$ 在多项式时间内可以完成，所以它可以破坏伪随机函数的安全性。

最后，证明如果攻击方可以攻击 Game2，那么就可以攻破单向函数的安全性。攻击方 $\mathcal{A}$ 可以攻击 Game2，即可伪造出一个 σ 使得 $f(\sigma)=f(t)$。构造一个归约算法 $\mathcal{B}$，给出一个 y 使得 $z^*=y$，调用攻击算法 $\mathcal{A}$，多项式次询问后计算出伪造签名 σ，判断 $f(\sigma)=z^*$ 是否成立。如果程序输出 1，那么 y 就是 σ 在作用于单向函数后的值，如此便可攻破单向函数的安全性。因此，如果单向函数是安全的，那么攻击方无法在多项式时间内成功攻击 Game2，而且 Game 之间都是优势可忽略的，因此攻击方无法在多项式时间内成功攻击 Game0，即无法在多项式时间内伪造出签名。

4　讨论

对本文所给出的方案与王晓峰等人的方案[22]（记为方案一）及杨亚涛等人的方案[34]（记为方案二）进行比较，结果如表 1 所列。

表 1　方案比较结果

	部分及多重签名不随人数增加而增加	不受签名人数限制	签名及验证算法不随人数增加而增加	抗量子攻击
方案一	√	√	√	×
方案二	√	√	×	√
本方案	√	√	√	√

方案一代表传统上基于各种不同密码学困难问题的多重签名方案，方案二代表采用新型量子技术构造的多重签名方案。方案一是王晓峰等人[22]根据因数分解和二次剩余困难性假设而提出的一类具有代表性的多重数字签名方案；在方案一中，作者对方案满足的部分及多重签名不随人数增加而增加、不受签名人数限制、签名及验证算法不随人数增加而增加等性质做了具体的说明，但是这类方案由于本身基于的困难性难题在量子计算下是可解的，因此并不具有抵抗量子攻击的性质。考虑方案二，杨亚涛等人[34]提出的广播多重签名被证明满足不可伪造和不可否认等基本性质，但文献所提出的方案中使用到的幺正变换 W 随着签名人数的增多而变得复杂，所以它无法实现签名及验证算法不随人数增加而增加。因此，与两种对比方案相比，基于混淆的多重签名方案具有多种优势。

本方案的不足是计算效率比较低，采用混淆是为了保证良好的性质，但构造过程复杂，必然导致计算效率较低。Garg 等人于 2013 年提出的基于多线性映射的混淆的计算效率为 $\mathrm{poly}(|C|,\lambda)\cdot 2^n$，其中 C 是被混淆电路，λ 是安全参数，n 是输入电路 C 的长度；2016 年 Lin 等人考虑到了其效率低下的问题，但是也只能将计算效率保持在指数级别，而其他两种方案则都可以在多项式时间内完成。

结束语　最近安全的不可区分混淆器的构造方案被提出，使用混淆构造多种应用已经被大家追捧，因为应用混淆的各种方案可以很容易地提高方案的安全性。文中给出了应用混淆的广播多重签名方案，此方案利用混淆的性质，不仅可以满足不可伪造性等多种性质，还可以抵抗量子攻击。但因为混淆的实用性比较低，所以构造一个实用的混淆方案将是一个值得继续研究的课题。

参 考 文 献

[1] ITAKURA K, NAKAMURA K. A public-key cryptosystem suitable for digital multisignatures[J]. NEC Research & Development, 1983(71): 1-8.

[2] 韩亚宁，王彩芬. 无证书广义指定多个验证者有序多重签名[J]. 计算机应用，2009，29(6)：1643-1645.

[3] WEN X, LIU Y. A realizable quantum sequential multi-signature scheme[J]. Acta Electronica Sinica, 2007, 35(6): 1079-1083.

[4] LUN W J, LI C Y. A Certificateless Sequential Multi-Signature Scheme without Pairings[J]. International Journal of Advancements in Computing Technology, 2012, 4(9): 193-199.

[5] WEN X, LIU Y, ZHOU N. Realizable quantum broadcasting multi-signature scheme[J]. International Journal of Modern Physics B, 2008, 22(24): 4251-4259.

[6] 匡宏波，李霞. 基于椭圆曲线的多重数字签名方案及其监控[J]. 计算机工程与应用，2000，36(12)：55-56.

[7] 雷琼. 电子合同签署中有序多重数字签名的应用[J]. 计算机与现代化，2016(2)：72-74.

[8] 饶静，王元华. 多重数字签名在教务管理系统中的应用研究[J]. 兴义民族师范学院学报，2013(5)：105-109.

[9] 张丽萍，葛福鸿. 多重数字签名在成绩管理系统中的应用研究[J]. 中国教育信息化，2016(9)：56-59.

[10] 王玉叶，邵美芹，常玲霞，等. 多重数字签名在专家会诊中的应用[J]. 山东理工大学学报(自然科学版)，2016(1)：29-32.

[11] HARN L, KRELER T. New scheme for digital multisignatures[J]. Electronics Letters, 1989, 25(15): 1002-1003.

[12] JIA H J, REN J Z. Digital multi-signature based on Schnorr scheme[C]// Proceedings of the CHINACRYPT. 1996: 170-176.

[13] 陆浪如，曾俊杰，张白愚，等. 基于离散对数多重签名体制的改进[J]. 通信学报，2002，23(6)：1-5.

[14] 吕皖丽. 基于椭圆曲线密码体制的多重数字签名技术研究[D]. 南宁：广西大学，2003.

[15] 姜岸. 基于椭圆曲线的多重数字签名方案的研究[D]. 长沙：长沙理工大学，2010.

[16] ZENG G, MA W, WANG X, et al. Signature scheme based on quantum cryptography[J]. Acta Electronica Sinica, 2001, 29(8): 1098-1100.

[17] WEN X, TIAN Y, JI L, et al. A group signature scheme based on quantum teleportation[J]. Physica Scripta, 2010, 81(5): 055001.

（下转第 352 页）

3)对生成的符号约束进行优化,消除冗余的括号及运算;
4)将该方法应用于实际的工业级 PLC 程序。

参 考 文 献

[1] 陈钢,宋晓宇,顾明. COQ 定理证明器辅助 PLC 程序验证和分析[J]. 北京大学学报(自然科学版),2010,46(1):30-34.

[2] 肖力田,顾明,孙家广. 一种 PLC 程序语言指称语义及函数的形式化定义方法[C]// 中国智能自动化会议. 2011.

[3] 陈雪琨. PLC 程序的 Petri 网建模与分析方法研究[D]. 泉州:华侨大学,2013.

[4] BIALLAS S,BRAUER J,ARCADE K S. PLC:A verification platform for programmable logic controllers[C]// Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering. ACM,2012:338-341.

[5] DARVAS D,APIEGO B F,VINUELA E B. PLCverif:a tool to verify PLC programs based on model checking techniques[C]// International Conference on Accelerator and Large Experimental Physics Control Systems. 2015:911-914.

[6] ADIEGO B F,DARVAS D,VINUELA E B,et al. Applying model checking to industrial-sized PLC programs[J]. IEEE Transactions on Industrial Informatics,2015,11(6):1400-1410.

[7] MCLAUGHLIN S E,ZONOUZ S A,POHLY D J,et al. A Trusted Safety Verifier for Process Controller Code[C]// NDSS. 2014:14.

[8] OULD BIHA S. A Formal Semantics of PLC Programs in Coq[C]// IEEE International Computer Software and Applications Conference,COMPSAC 2011. Munich,Germany,DBLP,2011:118-127.

[9] BLECH J O,BIHA S O. On Formal Reasoning on the Semantics of PLC using Coq[J]. axXiv:2013. 1301:3047.

[10] IEC (International Electrotechnical Commission). IEC Standard 61131-3:Programmable controllers-Part 3[S]. 1993.

[11] CYTRON R,FERRANTE J,ROSEN B K,et al. Efficiently Computing Static Single Assignment Form and the Control Dependence Graph[J]. ACM Transactions on Programming Languages & Systems,1991,13(4):451-490.

[12] 西门子股份有限公司. SIMATIC S7-300 和 S7-400 语句表(STL)编程:参考手册[M]. 西门子股份有限公司,2002.

(上接第 333 页)

[18] HARN L,XU Y. Design of generalized ElGamal type digital signature schemes based on discrete logarithm[J]. Electronics letters,1994,30(24):2025-2026.

[19] HARN L. New digital signature scheme based on discrete logarithm[J]. Electronics Letters,1994,30(5):396-398.

[20] 韩小西,王贵林,鲍丰,等. 针对基于离散对数多重签名方案的一种攻击[J]. 计算机学报,2004,27(8):1147-1152.

[21] 杜海涛,张青坡,杨义先. 新的 ElGamal 型广播多重数字签名方案[J]. 计算机工程,2007,33(12):10-11.

[22] 王晓峰,张璟,王尚平. 多重数字签名方案及其安全性证明[J]. 计算机学报,2008,31(1):176-183.

[23] WROBLEWSKI G. General method of program code obfuscation[C]// International Conference on Software Engineering Research and Practice. 2002.

[24] LINN C,DEBRAY S. Obfuscation of executable code to improve resistance to static disassembly[C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. ACM,2003:290-299.

[25] BARAK B,GOLDREICH O,IMPAGLIAZZO R,et al. On the (im) possibility of obfuscating programs[C]// Advances in cryptology—CRYPTO 2001. Springer Berlin Heidelberg,2001:1-18.

[26] GARG S,GENTRY C,HALEVI S,et al. Candidate indistinguishability obfuscation and functional encryption for all circuits[C]// 2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS). IEEE,2013:40-49.

[27] HOHENBERGER S,SAHAI A,WATERS B. Replacing a random oracle:Full domain hash from indistinguishability obfuscation[C]// Advances in Cryptology-EUROCRYPT 2014. Springer Berlin Heidelberg,2014:201-220.

[28] BONEH D,ZHANDRY M. Multiparty key exchange,efficient traitor tracing,and more from indistinguishability obfuscation[C]// Advances in Cryptology-CRYPTO 2014. Springer Berlin Heidelberg,2014:480-499.

[29] SHAAI A,WATERS B. How to use indistinguishability obfuscation:deniable encryption,and more[C]// Proceedings of the 46th Annual ACM Symposium on Theory of Computing. ACM,2014:475-484.

[30] HARN L,KRESLER T. New scheme for digital multisignatures[J]. Electronics Letters,1989,25(15):1002-1003.

[31] BONEH D,WATER B. Constrained pseudorandom functions and their applications[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg,2013:280-300.

[32] BOYLE E,GOLDWASSER S,IVAN I. Functional signatures and pseudorandom functions[M]// International Workshop on Public Key Cryptography. Springer Berlin Heidelberg,2014:501-519.

[33] KIAYIAS A,PAPADOPOULOS S,TRIANDOPOULOS N,et al. Delegatable pseudorandom functions and applications[C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM,2013:669-684.

[34] 杨亚涛,薛霆,李子臣. 广播多重量子数字签名方案的设计与分析[J]. 中国科学技术大学学报,2011,41(10):924-927.

[35] HU Y,JIA H. Cryptanalysis of GGH map[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg,2016:537-565.

[36] MILES E,SAHAI A,ZHANDRY M. Annihilation attacks for multilinear maps:Cryptanalysis of indistinguishability obfuscation over GGH13[C]// Annual Cryptology Conference. Springer Berlin Heidelberg,2016:629-658.

[37] LIN H. Indistinguishability obfuscation from constant-degree graded encoding schemes[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg,2016:28-57.