软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(1):140−151 [doi: 10.3724/SP.J.1001.2012.04092]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

随机谕言模型*

贾小英, 李 宝, 刘亚敏+

(中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

Random Oracle Model

JIA Xiao-Ying, LI Bao, LIU Ya-Min+

(State Key Laboratory of Information Security, Graduate University, The Chinese Academy of Sciences, Being 100049, China)

+ Corresponding author: E-mail: ymliu@is.ac.cn, http://www.lois.cn

Jia XY, Li B, Liu YM. Random oracle model. *Journal of Software*, 2012,23(1):140−151. http://www.jos.org.cn/1000-9825/4092.htm

Abstract: This paper gives a survey of the random oracle model, which is an important tool in provable security. The random oracle model is introduced on several aspects, including its origin and development, basic properties and methodology, representative schemes, plaintext awareness, random oracle instantiation, the uninstantiable properties and related negative results, and the research of weakened random oracle models. Besides, other ideal models are compared with the random oracle model, and the construction of encryption schemes in the standard model is also referred.

Key words: public-key cryptography; provable security; random oracle model; random oracle instantiation; uninstantiability of random oracle; weakened random oracle model

摘 要: 介绍了可证明安全理论中的重要工具——随机谕言模型,包括随机谕言模型的起源、基本性质和方法、随机谕言模型中的代表方案、明文知晓性质、随机谕言的实例化、随机谕言不可实例化的性质和相关负面结论以及对弱化的随机谕言模型的研究.此外,比较了随机谕言模型和其他理想模型,简介了标准模型中的方案设计状况.

关键词: 公钥密码学;可证明安全;随机谕言模型;随机谕言实例化;随机谕言的不可实例化性质;弱化的随机谕言模型

中图法分类号: TP309 **文献标识码**: A

随机谕言模型(random oracle model,简称 ROM)[1],亦可翻译为随机谕示模型、随机预言模型或随机预言机模型等,是可证明安全理论中的重要工具.可证明安全是指将密码方案的安全性归约为某些问题的难解性(intractability),从而使方案的安全性有具体的度量标准的理论和方法.自 Goldwasser 和 Micali 建立可证明安全理论以来[2,3],寻找高效率并且可证明安全的方案就成为公钥密码学领域的首要问题.

起初的安全性证明模型中只有对某些数学问题的难解性假设,而没有对密码学原语的理想化假设.这种模型称为标准模型(standard model),并被认为是最接近现实状况的模型.然而,最初在标准模型中设计的具有可证明安全性的密码方案的效率并不理想.为了提高效率,理想化的随机谕言模型成为平衡效率和安全性的一种方

* 基金项目: 国家自然科学基金(61070171); 国家重点基础研究发展计划(973)(2007CB311201)
收稿时间: 2010-10-15; 定稿时间: 2011-07-08; jos 在线出版时间: 2011-09-09
CNKI 网络优先出版: 2011-09-09 13:54, http://www.cnki.net/kcms/detail/11.2560.TP.20110909.1354.003.html

式,也成为可证明安全领域的一大争议问题:一方面是层出不穷的在随机谕言模型下设计的密码协议,另一方面是对随机谕言模型特殊性质的探讨和各种负面结论.因此,对随机谕言模型的研究已经成为可证明安全领域的重要部分.

本文将介绍随机谕言模型的起源与发展、基本性质与方法、应用实例以及关于随机谕言模型的热点研究问题.此外,本文还简介了与随机谕言模型相关的其他理想模型以及标准模型中的加密方案设计现状.

1 随机谕言模型

1.1 起 源

1986 年,Fiat 和 Shamir 提出一种将 3 轮身份验证协议转换为签名方案的方法,称为“Fiat-Shamir 转换”[4].图 1 给出了一个标准 3 轮身份验证协议[5],其中,发送者 S 需要使接收者 R 确信其身份,$sig_{sk}(\cdot)$是 S 使用的签名算法.

给定如图 1 所示的标准 3 轮身份验证协议,Fiat-Shamir 转换将第 2 轮中 R 发送的消息$\beta=r_R$用一个杂凑函数(hash function)h^{FS} 来替代,其中的 FS 是 Fiat-Shamir 的缩写.给定需要签名的消息 m,则对消息 m 的签名就是(α,β,γ).Fiat-Shamir 转换如图 2 所示.

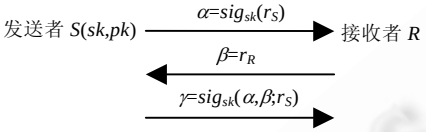

Fig.1 A canonical 3-round identification protocol

图 1 标准 3 轮身份验证协议

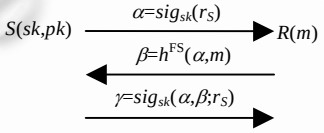

Fig.2 Fiat-Shamir transformation

图 2 Fiat-Shamir 转换

在证明 Fiat-Shamir 转换的安全性时,Fiat 和 Shamir 假设其中使用的杂凑函数 h^{FS} 是理想化的随机函数.这一方法被视为随机谕言模型思想的雏形.随后在 1993 年,Bellare 和 Rogaway 指出,如果承认这种假设合理,则可以构造出高效率的且可证明安全的加密方案[1].Bellare 和 Rogaway 正式提出了随机谕言方法,并在随机谕言模型中给出了几个高效率的加密方案的构造,例如:IND-CPA 安全的$\mathcal{E}_{pk}(m;r)=f(r)\|G(r)\oplus m$,其中,杂凑函数 G 在安全性证明中被视为随机谕言;以及 IND-CCA2 安全的$\mathcal{E}_{pk}(m;r)=f(r)\|G(r)\oplus m\|H(m,r)$,其中的杂凑函数 G,H 均为随机谕言.自此,随机谕言模型成为设计高效率的密码协议的重要工具.

1.2 基本性质和方法

随机谕言模型中假设协议各方都能够访问一个公开的随机函数,即“随机谕言”.随机谕言必须满足如下基本性质:(1) 确定性:对于相同的谕言询问 q,总是给出相同的回答;(2) 有效性:对于任意随机谕言询问 q,总是在多项式时间内给出回答;(3) 随机性:谕言的输出分布均匀、随机.

应用随机谕言方法构造密码方案则包括以下几个步骤:(1) 在随机谕言模型中构造方案,并建立方案的安全性;(2) 用合适的函数代替方案中使用的随机谕言,即随机谕言的实例化.

由于随机谕言的输出熵大于它的输入熵,即,它的确定性和随机性要求是矛盾的,这一点表明,随机谕言只是理想存在的原语[6].因此,随机谕言模型中建立的方案安全性并不等同于实例化之后的方案实际安全性,这一点也成为随机谕言模型受到质疑的原因.

当在随机谕言模型中证明方案的安全性时,需要模拟随机谕言.这一点通常使用“查表法”来实现,即,保持一个动态增长的列表 L.对于询问 q,首先在 L 中查找是否已有项(q,y)存在.如果是,则输出 y 作为回答;否则,均匀随机地选择 y,输出 y,并将(q,y)添加到表 L 中.这种模拟方法得到的随机谕言完全满足它的 3 种基本性质,并且能够简化方案的安全性证明.

2 随机谕言模型中的方案和概念

随机谕言模型自提出以来便成为构造高效率密码方案的重要工具,并且一些密码概念都是先在随机谕言

模型下构造出可行的方案,再在标准模型中实现.可以说,随机谕言模型也是方案构造的一个“实验台”.本节将介绍两个成功的随机谕言模型方案,即 *f*-OAEP 公钥加密方案[7]和 Fujisaki-Okamoto 变换[8],以及起源于随机谕言模型的安全概念、明文知晓性质[7].

2.1 *f*-OAEP方案

1994 年,Bellare 和 Rogaway 在随机谕言模型下构造了具有密文比特最优性质的公钥加密方案——*f*-OAEP 方案.随后,RSA-OAEP,即 *f* 为 RSA 函数时得到的公钥加密方案,成为了 PKCS#1 V2.0 中的加密标准.

2.1.1 方案描述

约定方案的安全参数为 1^k,k_0,k_1,n 为正整数. $G:\{0,1\}^{k_0}\mapsto\{0,1\}^{n+k_1}$ 和 $H:\{0,1\}^{n+k_1}\mapsto\{0,1\}^{k_0}$ 是随机谕言,$\mathcal{F}$是一个陷门置换生成器.

1) 密钥生成:运行$\mathcal{F}(1^k)$得到(f,f^{-1}).f 是公钥,f^{-1} 是私钥;

2) 加密:*f*-OAEP 方案首先使用随机谕言 G 和 H 对明文消息 m 进行填充变换,即 OAEP(optimal asymmetric encryption padding)变换.OAEP 算法是一个不对称的两轮 Feistel 结构,其中,随机谕言 G 和 H 的作用与 Feistel 结构中的轮函数类似.对于消息 $m\in\{0,1\}^n$,均匀、随机地选择随机数 $r\in\{0,1\}^{k_0}$,并计算:

$$s=m\|0^{k_1}\oplus G(r),t=r\oplus H(s),u=s\|t.$$

将填充后的消息 u 应用单向陷门置换 f,便得到密文 $y=f(u)$.

3) 解密:对于密文 y,首先计算 $u=f^{-1}(y)$.将 u 解析为 $s\|t$,并计算:

$$r=t\oplus H(s),\hat{m}=s\oplus G(r).$$

将 $\hat{m}$ 解析为 $m\in\{0,1\}^n$ 和 $z\in\{0,1\}^{k_0}$, 若 z 是全 0 串,则表示 y 是合法密文,输出明文 m;否则,输出错误符号$\perp$.

2.1.2 效率和安全性

f-OAEP 方案的主要开销为 f 函数的计算.与 f 函数的计算开销相比,算法中的消息填充、随机谕言询问以及异或运算的开销微乎其微.因此,*f*-OAEP 在计算上具有高效率.此外,*f*-OAEP 方案中的明、密文长度之比,较之此前的其他加密方案也是最优的.

f-OAEP 方案的安全性证明却是一波三折.起初在提出 *f*-OAEP 时,Bellare 和 Rogaway 声称对于任何单向陷门置换 f,*f*-OAEP 在随机谕言模型中都能达到 IND-CCA2 安全.然而 2001 年,Shoup 指出[9],若仅要求 f 具有单向性还无法保证 *f*-OAEP 的 IND-CCA2 安全性,并给出了若 f 具有异或可延展性质(XOR-malleability),则 *f*-OAEP 无法达到 IND-CCA2 安全性的证明.幸运的是,Fujisaki 等人发现,若 f 具有部分定义域单向性(partial domain one-wayness),则 *f*-OAEP 在随机谕言模型下仍然能够达到 IND-CCA2 安全性[10].而 RSA 函数便具有这种性质,因此 RSA-OAEP 在随机谕言模型下仍然是 IND-CCA2 安全的.

2.2 Fujisaki-Okamoto变换

1999 年,Fujisaki 和 Okamoto 提出了一种利用随机谕言将具有弱安全性的公钥加密方案转化为具有强安全性的公钥加密方案的变换方法[8],称为 Fujisaki-Okamoto 变换(FO 变换).下面介绍 FO 变换的一种简化形式.

2.2.1 方案描述和安全性

令$\mathcal{E}_{pk}$为一个概率公钥加密方案,G,H 是两个随机谕言.对$\mathcal{E}_{pk}$应用 FO 变换,可以得到一个混合形式的公钥加密方案 $\mathcal{E}_{pk}^{hy}$.$\mathcal{E}_{pk}^{hy}$ 的密钥生成算法与$\mathcal{E}_{pk}$的密钥生成算法相同,在加密时,对于消息 m, $\mathcal{E}_{pk}^{hy}$ 选择随机数σ并计算:

$$\mathcal{E}_{pk}^{hy}(m)=\mathcal{E}_{pk}(\sigma;H(\sigma,m))\|G(\sigma)\oplus m.$$

对于密文 $y=(C,U)$,其中,C 是密文中来自$\mathcal{E}_{pk}$加密的部分,U 是随机谕言 G 的对应值和明文的异或部分.使用$\mathcal{E}_{pk}$的私钥便可对 C 密文解密得到σ,再计算 $m=U\oplus G(\sigma)$并验证是否有 $C=\mathcal{E}_{pk}(\sigma;H(\sigma;m))$:如果是,则输出明文 m;否则,输出错误符号$\perp$.

只要公钥加密方案$\mathcal{E}_{pk}$具有 IND-CPA 安全性,经过 FO 变换后得到的 $\mathcal{E}_{pk}^{hy}$ 的公钥加密在随机谕言模型下便能达到 IND-CCA2 安全.而具有 IND-CPA 安全性的公钥加密方案比具有 IND-CCA2 安全性的方案更容易构造,

因此,FO 变换可以方便地将弱安全的公钥加密方案转化为强安全的公钥加密方案.

FO 变换的一个著名应用便是 Boneh-Franklin 的基于身份的加密方案(BF-IBE 方案)[11].自 1984 年 Shamir 提出基于身份的加密方案(identity-based encryption,简称 IBE)的构想以来[12],构造高效率 IBE 方案的问题一直悬而未决;直到 2001 年,Boneh 和 Franklin 利用 Weil 对子(Weil pairing)和 FO 变换构造了在随机谕言模型下达到 IND-ID-CCA2 安全的 BF IBE 方案.BF IBE 方案是第一个现实的 IBE 方案,并且已经进入 2009 年公布的 IEEE P1363.3 关于基于身份的公钥密码协议的标准草案中.

2.3 明文知晓性(plaintext awareness)

在随机谕言模型中产生的不只是高效率的密码方案,还有新的安全概念.明文知晓性便是起源于随机谕言模型然后被推广到标准模型下的一个强安全性概念.明文知晓性是 1994 年 Bellare 和 Rogaway 为了方便证明 *f*-OAEP 方案的 IND-CCA2 安全性而提出来的,它的直观含义是指,如果敌手产生了一个有效密文,则它一定已经知道对应的明文,这样,CCA 模型中的解密谕言对敌手就没有用处了.随后,Bellare 等人又细化了明文知晓性的概念,为敌手增加了窃听密文的能力[13],将概念推广到标准模型下,并细分为 PA0,PA1,PA2 等不同难度等级[14].PA0,PA1,PA2 与标准的安全性定义存在对应关系,即 IND-CPA+PA0⇒IND-CPA,IND-CPA+PA1⇒IND-CCA1,IND-CPA+PA2⇒IND-CCA2.

为了使 PA 在随机谕言模型与标准模型中的定义兼容,Bellare 和 Palacio 推荐将随机谕言模型中的 PA 定义也区分成 PA0-RO,PA1-RO 和 PA2-RO.以下是 PA1-RO 和 PA2-RO 的定义,其中的敌手$\mathcal{A}$称为密文生成器,解密模拟器$\mathcal{A}^*$称为明文提取器.

定义 1(PA1-RO). 一个公钥加密方案,如果对任意密文生成器$\mathcal{A}$都存在明文提取器$\mathcal{A}^*$,只给定公钥和$\mathcal{A}$的随机谕言询问列表 $R[\mathcal{A}]$,$\mathcal{A}^*$与真实解密算法的输出分布不可区分,则称此方案满足 PA1.

PA0 的定义与 PA1 相似,只是在 PA0 中,敌手$\mathcal{A}$只被允许询问一次明文提取器$\mathcal{A}^*$,而在 PA1 中,$\mathcal{A}$可以向$\mathcal{A}^*$发送多项式次解密询问.

PA1 中的敌手并没有窃听密文的能力.在 PA2 中增加了明文生成器$\mathcal{P}$用以刻画$\mathcal{A}$的窃听密文能力,也就是说,$\mathcal{P}$能够为$\mathcal{A}$提供$\mathcal{A}$不知道对应明文的密文.$\mathcal{A}$从$\mathcal{P}$得到的密文存放在密文列表 *CLIST* 中.$\mathcal{A}$不允许用 *CLIST* 中的密文询问$\mathcal{A}^*$.

定义 2(PA2-RO). 一个公钥加密方案,如果对访问任意明文生成器$\mathcal{P}$的任意密文生成器$\mathcal{A}$都存在明文提取器$\mathcal{A}^*$,只给定公钥和$\mathcal{A}$的随机谕言询问列表 $R[\mathcal{A}]$以及密文列表 *CLIST*,$\mathcal{A}^*$与真实解密算法的输出分布不可区分,则称此方案满足 PA2.

标准模型中没有随机谕言询问,因而在标准模型的明文知晓性定义中,$R[\mathcal{A}]$是$\mathcal{A}$的随机数列表.实际上,标准模型中的明文知晓性比 IND-CCA2 安全性更难证明.但是,对标准模型中的明文知晓性的研究仍然是可证明安全中有趣的研究方向,因为它还有着实际应用的需求.例如,Raimondo 等人发现,SKEME 密钥交换协议的可否认性的证明就需要使用加密方案的明文知晓性[15].

3 随机谕言实例化

随机谕言基本性质中的确定性和随机性是矛盾的,因此随机谕言只是理想化的原语,实际计算时需要用现实函数来替代.随机谕言的实例化即指在实际应用中通过使用合适的杂凑函数的计算来代替对随机谕言的访问.究竟采用具有何种性质的杂凑函数来实例化随机谕言,才能够使在随机谕言模型下安全的方案在标准模型中也能建立起至少经得起现实考验的安全性,是研究随机谕言模型的一个热点方向.本节将介绍一些用于实例化随机谕言的密码学原语以及对 *f*-OAEP 的实例化结论.

3.1 完美单向杂凑函数

1997 年,Canetti 提出了用于随机谕言实例化的谕言杂凑技术(oracle hashing)[16].之后,在 1998 年,Canetti 等人为其更名为完美单向杂凑函数(perfectly one-way hash function,简称 POWHF)[17].完美单向杂凑函数是一类概

率杂凑函数,它能够隐藏关于其自变量的所有部分信息,并且具有完整性、抗碰撞性与完美单向性.以下是完美单向杂凑函数的形式化定义.

定义 3(完美单向杂凑函数). 约定安全参数为 1^k.算法$\mathcal{H}$为对于输入 x 和随机数 $r\in R_k$,返回杂凑值 y.算法$\mathcal{V}$能够有效地验证 y 是否是输入 x 的杂凑值,并输出一个判定比特.如果满足如下性质,则函数对$(\mathcal{H},\mathcal{V})$被称为完美单向杂凑函数:

I. 完整性:对所有足够大的 k,任意 $r\in R_k$ 和任意输入 x,有$\mathcal{V}(x,\mathcal{H}(x,r))=1$;

II. 抗碰撞性:对任意概率多项式时间的敌手$\mathcal{A}$,令$(x,x'y)\leftarrow\mathcal{A}(1^k)$,那么以下概率 $Pr[\mathcal{V}(x,y)=1\wedge\mathcal{V}(x',y)=1\wedge x\neq x']$ 是可忽略的;

III. 完美单向性:对任意概率多项式时间的敌手$\mathcal{A}$,有$\langle x,\mathcal{A}(\mathcal{H}(x,r))\rangle\overset{c}{=}\langle x,\mathcal{A}(\mathcal{H}(x',r))\rangle$, x 的杂凑值与 x'的杂凑值计算不可区分,即$\mathcal{H}(x,r)$隐藏了 x 的所有部分信息.

3.1.1 强完美单向杂凑函数

在实例化随机谕言时,通常需要杂凑函数具有强完美单向性,即对于不可逆函数 f,有

$$\langle x,\mathcal{A}(f(x),\mathcal{H}(x,r))\rangle\overset{c}{=}\langle x,\mathcal{A}(f(x),\mathcal{H}(x',r))\rangle.$$

使用强完美单向杂凑函数实例化随机谕言,已经出现了一些正面结论.例如,此前所述的 Bellare 和 Rogaway 的在随机谕言模型下达到 IND-CPA 安全性的加密方案[1],$\mathcal{E}_{pk}(m;r)=f(r)\|G(r)\oplus m$,用关于 f 的强完美单向杂凑函数代替 G 后,该方案仍然保持 IND-CPA 安全性[16].此外,Boldyreva 和 Fischilin 证明了用强完美单向杂凑函数实例化 Fujisaki-Okamoto 变换中的任意一个随机谕言,所得到的部分实例化后的方案在随机谕言模型中仍然保持安全性[18].但是,Fujisaki-Okamoto 变换的完全实例化仍然是一个开放问题.

3.1.2 完美单向杂凑函数的构造

Canetti 等人提出了几个构造(强)完美单向杂凑函数的方法[16,17].由于完美单向杂凑函数要求杂凑值可验证,因此计算杂凑值所使用的随机数通常是公开的,这种“公开随机数”的方法在目前的随机谕言实例化结论中普遍使用.以下是 Canetti 等人提出的两种(强)完美单向杂凑函数的构造:

构造 1:$H(x,r)=(r,r^{h(x)})$,其中,h 是一个抗碰撞的杂凑函数.令 G 为模 p 的 q 阶子群,$g\in G$.H 的完整性很明显,其抗碰撞性质基于 h 的抗碰撞性质.

在判定性 Diffie-Hellman(DDH)假设下(即对于 $a,b,c\in\mathbb{Z}_q^*, c\neq ab$ 有 $(g^a,g^b,g^{ab})\overset{c}{=}(g^a,g^b,g^c)$),可以将区分 $(r,r^{h(x)})$和$(r,r^{h(x')})$的问题归约为区分(g^a,g^b,g^{ab})和(g^a,g^b,g^c)问题,从而证明 H 的完美单向性质.此外,类似地,基于更强的假设 $(f(a),g^b,g^{ab})\overset{c}{=}(f(a),g^b,g^c)$,可以归约证明 H 的强完美单向性质.

构造 2: $H_l(x,r)=(r,f_x^l(r))$,其中,$f^l(\cdot)$来自于一个抗碰撞的伪随机函数部落$\{\{F_t^{(n)}\}_{t\in\{T_n\}}\}_{n\in N}$.$H_l$ 的完整性是明显的,其抗碰撞性质来自于 $f^l(\cdot)$的抗碰撞,H_l 的完美单向性来自于 $f^l(\cdot)$的伪随机性质.故 H_l 是完美单向杂凑函数.

3.2 增强的完美单向杂凑函数

此后的文献中也提出了一些强原语,这些强原语的性质可以增强完美单向杂凑函数的性质.下面介绍自适应完美单向杂凑函数[19]和可提取的完美单向杂凑函数[20].

3.2.1 自适应完美单向杂凑函数

2008 年,Pandey,Pass 和 Vaikuntanathan 提出了自适应单向函数的概念[19].

给定一个族函数$\mathcal{F}_n=\{f_{tag}:\{0,1\}^n\mapsto\{0,1\}^n\}$,其中,$tag$ 是函数 f_{tag} 的下标.如果对于每个 tag 和随机的 r,即使敌手能够访问 $tag'\neq tag$ 的其他函数 $f_{tag'}$的求逆谕言,$f_{tag}(r)$都难以求逆,则称函数族$\mathcal{F}_n$ 是自适应单向的.

将自适应性质加诸完美单向杂凑函数,得到的强原语、自适应的完美单向杂凑函数,可以适用于更复杂的随机谕言模型方案的实例化.例如 Bellare 和 Rogaway 于 1993 年提出的在随机谕言模型下达到 IND-CCA2 安全性的加密方案[1],$\mathcal{E}_{pk}(m;r)=f(r)\|G(r)\oplus m\|H(m\|r)$,若 G,H 均用自适应的强完美单向杂凑函数实例化,则该方案仍然保持 IND-CCA2 安全性.

3.2.2 可提取的完美单向杂凑函数

可提取的完美单向函数是 Canetti 和 Dakdouk 于 2008 年提出的又一个强原语[20].由于随机谕言本身具有可提取性质,即,如果有一种算法知道函数值,则说明它已经知道原像.这种性质使得随机谕言模型下的安全性证明十分便利.如果用具有可提取性质的函数来实例化随机谕言,则原来在随机谕言模型中的证明可以直接移植过来,加密方案$\mathcal{E}_{pk}(m;r)=f(r)||G(r)\oplus m||H(m||r)$中的随机谕言 G,H 也可以用可提取的强完美单向杂凑函数安全地实例化.

Canetti 和 Dakdouk 给出了一些基于强假设构造可提取的单向函数的方法[20],但是可提取的(强)完美单向杂凑函数的构造仍然是未知的.如果能构造出可提取的(强)完美单向杂凑函数,即使是基于强假设,也将是随机谕言实例化问题的重要进展.

3.3 对OAEP的实例化

f-OAEP 是随机谕言模型中最成功的方案之一.虽然 Bellare 和 Rogaway 推荐基于 SHA 和 MD5 杂凑函数来构造 *f*-OAEP 方案中的两个随机谕言 G,H 的替代函数,并且在 PKCS#1 V2.1 标准中也类似地推荐了 MD 系列和 SHA 系列的杂凑函数来构造对 G,H 的替代,但是这种替代的安全性仅仅基于“经验”,并没有得到严格证明.因此,从可证明安全的角度研究对 *f*-OAEP 方案的实例化意义重大.下面介绍一些对 *f*-OAEP 方案实例化的已有结论.

2005 年,Boldyreva 和 Fischilin 证明了 OAEP 中的两个随机谕言 G,H 都不能用强完美单向杂凑函数来实例化[18].随后在 2006 年,Boldyreva 和 Fischilin 细致分析了 OAEP 中的随机谕言对方案的安全性所起的作用,并为 *f*-OAEP 方案的部分实例化“定制”了具有某些特定性质的杂凑函数[21].适合随机谕言 G 的是近似抗碰撞的伪随机生成器(near-collision resistant pseudorandom generator,简称 NCRPRG).用 NCRPRG 实例化 G 后得到的方案在随机谕言模型中保持了 IND-CCA2 安全性;适合随机谕言 H 的是不可延展的伪随机生成器(non-malleable pseudorandom generator,简称 NMPRG),用 NMPRG 实例化 H 后得到的方案在随机谕言模型中是 NM-CPA 安全的.如果同时实例化 G,H,则得到的完全实例化的 *f*-OAEP 方案在标准模型中是$NM-CPA 安全的.

由于$NM-CPA 是 NM-CPA 的较弱的变形,并非标准的安全性定义,因此 Boldyreva 和 Fischilin 提出了一个开放问题,即,能否使 *f*-OAEP 的完全实例化满足一个标准的安全性定义.2010 年,Kiltz,O'Neil 和 Smith 解决了这个开放问题,证明了 *f*-OAEP 可以满足标准的 IND-CPA 安全性定义[22].这是对 *f*-OAEP 实例化的最新正面结论.

4 随机谕言的不可实例化性质

如果说对随机谕言模型实例化的研究表现出对随机谕言方法的支持,那么反对随机谕言方法的声音主要表现在对随机谕言的不可实例化性质的研究上.虽然在随机谕言模型中构造的密码方案具有高效率,但是在随机谕言模型中的安全性证明并不能保证方案的实际安全性,这是因为随机谕言模型的一些理想化的性质是现实的原语都不具有的.以下介绍一些关于随机谕言模型的负面结果.

4.1 相关难解性质

1998 年,Canetti,Halevi 和 Goldreich 首次构造了在随机谕言模型中安全但在标准模型中却无法安全实例化的方案[23].这种方案的存在,正是由于随机谕言独特的相关难解性质(correlation intractability)所致.

为了刻画相关难解性质,Canetti 等人首先定义了模糊二元关系(evasive binary relation)这一概念.

定义 4(模糊二元关系). 给定一个二元关系 R,如果对于任何概率多项式时间的谕言机$\mathcal{M}$,以下概率 $\Pr[x\leftarrow\mathcal{M}^{\mathcal{O}}(1^k),(x,\mathcal{O}(x))\in R]$ 可忽略,则称 R 为模糊二元关系,其中,$\mathcal{O}$是随机谕言.

由于随机谕言$\mathcal{O}$的输出分布均匀、随机,因此,$\mathcal{O}(x)$与 x 之间并不存在明显的非平凡关系,故而模糊二元关系很容易找到.相关难解性正是随机谕言的理想随机性的体现.

定义 5(相关难解性). 给定一个函数 $f:\{0,1\}^*\mapsto\{0,1\}^{poly(k)}$,其函数描述为 s.如果对于任意模糊二元关系 R 以及任意概率多项式时间图灵机$\mathcal{M}$,以下概率 $\Pr_{s\in\{0,1\}^k}[x\leftarrow\mathcal{M}(s),(x,f(x))\in R]$ 可忽略,则称 f 具有相关难解性.

函数的变量和自变量之间的映射关系由其描述决定.随机谕言的描述一般被视为多项式时间内不可计算

的,而现实中使用的函数,其描述都是公开的并且是多项式时间内可计算的.因此,总是能够根据其描述构造出一个模糊二元关系 R,使得$(x,f(x))\in R$,例如关系 $R^{\mathcal{F}}=\bigcup_k\{(s,f_s(s)):s\in\{0,1\}^k\}$,其中,$\mathcal{F}=\{f_s\}_{s\in\{0,1\}^*}$ 是所有下标为 s 的函数的集合.故而,现实中的函数都不具备相关难解性.

利用这一点,Canetti,Halevi 和 Goldreich 能够由任意安全的签名方案构造在随机谕言模型下安全,但用任意现实中使用的函数都无法安全实例化的签名方案[22].给定一个能够抵抗存在性伪造攻击的签名方案 $S=(\mathcal{G},\mathcal{S},\mathcal{V})$,可以构造随机谕言模型中的关于模糊二元关系 R 的签名方案 $S_R^{\mathcal{O}}=(\mathcal{G},\mathcal{S}_R^{\mathcal{O}},\mathcal{V}_R^{\mathcal{O}})$ 如下,其中,$\mathcal{O}$是随机谕言:

1) 签名算法 $\mathcal{S}_R^{\mathcal{O}}$:

$$\mathcal{S}_R^{\mathcal{O}}(sk,m)=\begin{cases}(sk,m), & (m,\mathcal{O}(m))\in R\\ \mathcal{S}(sk,m), & (m,\mathcal{O}(m))\notin R\end{cases}.$$

2) 验证算法 $\mathcal{V}_R^{\mathcal{O}}$:

$$\mathcal{V}_R^{\mathcal{O}}(vk,m,\sigma)=\begin{cases}\text{接受}, & (m,\mathcal{O}(m))\in R\\ \mathcal{V}(vk,m,\sigma), & (m,\mathcal{O}(m))\notin R\end{cases}.$$

可以看出,在随机谕言模型下,签名方案 $S_R^{\mathcal{O}}=(\mathcal{G},\mathcal{S}_R^{\mathcal{O}},\mathcal{V}_R^{\mathcal{O}})$ 的安全性仍然与方案 $S=(\mathcal{G},\mathcal{S},\mathcal{V})$一样,因为 $(m,\mathcal{O}(m))\in R$ 的概率可以忽略.然而,当$\mathcal{O}$被描述为 s 的现实函数 f_s 所替代时,很容易构造关系 R 使得$(m,f_s(m))\in R$,从而使方案输出其签名密钥.

4.2 其他负面结论

2002 年,Nielsen 指出[24],在随机谕言模型中很容易构造的一类密码方案——非交互非承诺的加密方案(non-interactive non-committing encryption,简称 NINCE),在标准模型中是无法构造的.这是由于随机谕言模型具有的理想可编程性质(ideal programmability),现实函数并不具有.简而言之,随机谕言模型的理想可编程性质是指其在某些点的值可以预先设置而不被察觉.与相关难解性一样,理想可编程性质也是随机谕言的随机性的体现,它与相关难解性之间的关系很可能是等价的.验证这一点将是一个有趣的问题,有助于理解随机谕言模型的基本性质.探讨现实中的原语的可编程性质也是有意义的,如 2008 年,Hofheinz 和 Kiltz 还尝试了在标准模型中构造具有可编程性质的杂凑函数[25]的研究工作.

2003 年,Goldwasser 和 Taumann 对 Fiat-Shamir 变换[5]的分析类似于 Canetti 等人的结论.Goldwasser 和 Taumann 证明,对于某些 3 轮身份验证协议,应用 Fiat-Shamir 变换可以得到在随机谕言模型下可证明安全,但却无法安全实例化的签名方案.

2004 年,Bellare 等人研究了公钥密码学当前的一个热点研究方向——密钥封装机制(key encapsulation mechanism,简称 KEM)的构造,并证明,同时具有密钥可验证性质、密文可验证性质以及 IND-CCA 保持性质的 KEM 只能在随机谕言模型中存在[26].Bellare 等人的结论与此前的负面结论大不一样,因为他们的着眼点不在于现实中的函数不具备随机谕言模型的理想随机性上,而在于随机谕言的公开可访问性质并非总是存在.即,两个随机谕言模型中的密码系统,它们各自使用的随机谕言是独立的,并不能在这两个密码系统分别的参与方之间共享.而现实中,函数的描述总是公开的,因此不具有这种性质.

2004 年,Maurer,Renner 和 Holenstein 研究了密码系统之间的可归约性[27].他们将两个密码系统的不可区分性质一般化成不可分辨性质(indifferentiability),并重新定义了可归约性.若$\mathcal{A}$和$\mathcal{B}$不可分辨,则将系统$\mathcal{C}(\mathcal{B})$中的组件$\mathcal{B}$替换成$\mathcal{A}$后,$\mathcal{C}(\mathcal{B})$的安全性并不受影响;而系统$\mathcal{U}$能够归约为系统$\mathcal{V}$,是指从$\mathcal{V}$可以构造与$\mathcal{U}$不可分辨的系统$\mathcal{B}(\mathcal{V})$.Maurer 等人证明了随机谕言不能归约为一个较弱的原语:异步信标(asynchronous beacon),而异步信标亦不能归约为有限长度的随机串.这说明存在随机谕言模型中的密码系统,其中的随机谕言并不能用现实中的函数来替代.Maurer 等人关于随机谕言模型的负面结论并不针对具体的密码方案和构造,并蕴涵了此前 Canetti 等人的结论[23].

虽然以上这些负面结论已经触及了一些现实的密码学目标,如 KEM 的构造等,但是尚未涉及像 RSA-OAEP

这种已经成为加密标准的方案.然而在 2006 年,Brown 提出,实例化 RSA-OAEP 中的随机谕言后,可能无法将其 IND-CCA2 安全性归约为 RSA 的单向性[28].2009 年,Kiltz 和 Pietrzak 对基于填充的加密方案的随机谕言实例化给出了一个负面结论[29].基于填充的加密方案(padding-based encryption)是指像 *f*-OAEP 这种首先用一个公开的单射变换 π(如 OAEP)对明文消息和随机数进行填充变换,再对变换结果应用陷门置换 f 的加密方案.Kiltz 和 Pietrzak 证明,即使假设理想的陷门置换存在,基于填充的加密方案的 IND-CCA2 安全性,甚至 IND-CCA1 安全性,也都无法黑箱归约到 f 的"理想单向性".但是,Kiltz 和 Pietrzak 的结论也没有排除用非黑箱归约的方法建立 *f*-OAEP 在标准模型中的安全性的可能.

如果说大部分关于随机谕言模型实例化的负面结论在直观上可以归咎于真实杂凑函数并不具有随机谕言的理想随机性的话,那么 2009 年,Leurent 和 Nguyen 的实例化负面结论则可以归咎于真实杂凑函数不那么理想的抗碰撞性.Leurent 和 Nguyen 的分析更为精细[30],在他们的结论中,此前多种随机谕言实例化建议,例如 Bellare 和 Rogaway 早期关于随机谕言模型的文献中所提出的方法[1,7],都是不安全的.

综合对随机谕言模型的实例化和不可实例化的结论来看,随机谕言模型实例化进展甚微而困难重重,是一个极具挑战性的研究方向.目前的情形是,实例化方法大多效率不高,并且在完全实例化的情形下,大都不能保持在随机谕言模型中建立的安全性;而对随机谕言不可实例化性质的研究,虽然结论众多,但是也大都停留在定义层面,并没有产生对一般随机谕言模型中的方案的现实攻击.

5 弱化的随机谕言模型

随机谕言模型中的假设过于强大,使得它在密码方案的证明中几乎具有无所不能的性质.如果能够弱化随机谕言模型,那么在弱化的模型中建立的安全性可能会更加接近方案的实际安全性.因此,近年来对弱化随机谕言模型的研究也逐渐成为热点.下面给出简单介绍.

5.1 弱化的随机谕言模型(weakened random oracle model)

Liskov 在 2006 年提出了弱理想压缩函数(weak ideal compression function)的概念,并基于弱理想压缩函数构造了与理想杂凑函数不可分辨的杂凑函数[31].弱理想压缩函数是带攻击谕言的随机谕言,以下描述了弱理想压缩函数的一些常见弱点:(1) 碰撞易解(collision tractable);(2) 第二原像易解(second pre-image tractable);(3) 原像易解(first pre-image tractable).

弱化的随机谕言模型即指带有相应的攻击谕言的随机谕言模型,例如碰撞易解的随机谕言模型(CT-ROM)、第二原像易解的随机谕言模型(SPT-ROM)和原像易解的随机谕言模型(FPT-ROM).它们的强度依次减弱,FPT-ROM 中的安全性蕴涵着 SPT-ROM 中的安全性.

2010 年,Kawachi 等人在弱化的随机谕言模型中分析了 *f*-OAEP 和 Fujisaki-Okamoto 转换在这些弱化的随机谕言模型中的安全性[32],并得出如下结论:

1) *f*-OAEP 在所有这些弱化的随机谕言模型中都是 IND-CCA2 安全的,其中,f 为部分定义域单向的陷门单向函数;
2) Fujisaki-Okamoto 转换在 SPT-ROM 中是安全的,但是有些从 Fujisaki-Okamoto 转换得到的方案在 FPT-ROM 中并不安全.

5.2 其他对随机谕言模型的弱化

2002 年,Nielsen 提出了不可编程的随机谕言模型(non-programmable random oracle model,简称 NPROM)[24].随后,NOROM 也被视为一种弱化的随机谕言模型.在 NPROM 中,随机谕言的值不能够被预先设置和改变.2009 年,Wee 在分析随机谕言模型中的零知识协议时也分析了 NPROM 对零知识协议的影响[33].此外,在 2007 年,Unruh 还提出了带辅助输入的随机谕言,其中的辅助输入可以依赖于谕言;并且,Unruh 证明了 RSA-OAEP 在带辅助输入的随机谕言模型中仍然是 IND-CCA2 安全的[34].

研究弱化的随机谕言模型的意义在于,可以藉此分析随机谕言模型的哪些性质对于方案的安全性必不可

少,从而去除方案安全性证明对理想化性质的依赖.理论上,在弱化的随机谕言模型中建立的方案,其安全性更为接近现实模型中的安全性.

6 其他理想模型

理想化的密码模型能够简化问题,因而在密码方案的设计和安全性证明中广泛地得以应用.本节简介另外两种与随机谕言模型关联密切的理想模型,即理想密码模型(ideal cipher model)和一般群模型(generic group model).

6.1 理想密码模型

理想密码模型来源于 1949 年 Shannon 提出的“随机密码”,因此亦被称为“Shannon 模型”[35].通常,分组密码被视为伪随机置换.而在理想密码模型中,分组密码被理想化为所有的协议参与方都可以访问的随机置换,称为“理想密码”.这种方法类似于随机谕言模型中将杂凑函数视为随机函数的假设.

2005 年,Coron 等人证明了随机谕言模型下建立的安全性蕴涵了理想密码模型中的安全性[36].即,用理想分组密码代替方案中的随机谕言后,方案在理想密码模型中仍然安全.2008 年,Coron,Patarin 和 Seurin 证明了随机谕言模型与理想密码模型是等价的[37].

6.2 一般群模型

1997 年,为了分析群上的离散对数问题和 Diffie-Hellman 问题的难解性,Shoup 提出了一般群模型[38].随后,一般群模型广泛应用于基于 Diffie-Hellman 问题的密码协议的安全性分析.例如,通常用来分析公钥加密方案在标准模型下的 PA 性质的 Diffie-Hellman 知识(DHK)问题的难解性便是在一般群模型中建立的[39].

令 p 为 k 比特的素数,G 为模 p 的加法群,$S=\{0,1\}^{l(k)}$是一个比特串集合,其中,$l(k)\geqslant k$.令 $\sigma:G\mapsto S$ 为一个 1-1 映射.对σ的要求是,从$\sigma(x)$恢复 x 的困难性等同于群 G 上的离散对数问题.即,从$\sigma(x)$恢复 x 的概率可以忽略.敌手不能直接得到群 G 中的元素,而只能得到群元素在σ作用下的像.敌手可以通过询问一个加法谕言$\mathcal{O}:S\times S\mapsto S$ 来完成两个群元素的相加操作.

一般群模型中,假设群的描述不会向敌手泄露任何信息.即,将映射σ理想化.而现实中的编码并不具有如此良好的性质,因此,一般群模型有着与随机谕言模型相同的弱点.2002 年,Dent 提出[40],存在一些在一般群模型中证明安全但是在现实中易于攻破的方案.Dent 的方法与 Canetti,Halevi 和 Goldreich 的方法[23]类似,即先定义了与模糊二元关系相似的模糊群关系以及相关难解性,然后证明在现实中并不存在相关难解的编码函数族.

7 标准模型中的加密方案构造

与几类理想化的密码模型相比,标准模型更接近于现实模型,因此,在标准模型中设计高效率的加密方案是公钥密码学领域内的重要目标.1998 年,Cramer 和 Shoup 提出的基于 DDH 假设的公钥加密方案[41]是第一个在标准模型中达到 IND-CCA2 安全且高效率的加密方案.

随后,Cramer 和 Shoup 将这种加密方案的设计方法发展为通用杂凑证明系统(universal hash proof system,简称 UHPS)框架[42].UHPS 框架能够将一类困难假设、子集成员问题(subset membership problems)假设,例如 DDH 假设,转化为具有 IND-CCA2 安全性的公钥加密方案.

通用杂凑证明系统不是唯一的“IND-CCA2 公式”.2008 年,Peikert 和 Waters 提出新的密码学原语,称为损耗陷门函数(lossy TDF,简称 LTDF)[43].Peikert 和 Waters 提出的从 LTDF 构造具有 IND-CCA2 安全性的公钥加密方案的通用方法,成为近年来的研究热点.损耗陷门函数也可以基于 DDH 假设来构造.实际上,基于 DDH 假设构造损耗陷门函数,然后构造出具有 IND-CCA2 安全性的加密方案,该方法很有可能也蕴含在通用杂凑证明系统中.

诸如 DDH 假设的子集成员问题假设是一类比较强的判定性困难性假设,降低假设的强度能够使方案的安全性证明更可信.近年来,也出现了在标准模型下基于更弱的计算性假设,如 CDH 假设(computational Diffie-Hellman problem)的公钥加密方案.例如,2008 年,Cash,Kiltz 和 Shoup 提出了新的计算性困难问题——孪生 DH

问题(twin Diffie-Hellman problem,简称 2DH),并证明了 2DH 问题的难度至少与 CDH 问题的难度一样[44].从 2DH 问题也可以构造高效率的加密方案.

DDH,CDH,2DH 假设等都属于 Diffie-Hellman 问题类.2009 年,Hoefheinz 与 Kiltz 基于因子分解假设构造的具有 IND-CCA2 安全性的加密方案[45],其效率远胜于标准模型中基于因子分解假设的 IND-CCA2 安全的其他方案,引起了研究者们的关注.而后,在 2010 年,Wee 将近年来的许多基于计算性假设构造的公钥加密方案统一在可提取杂凑证明系统(extractable hash proof system)之下[46].可提取杂凑证明系统蕴涵了 Cash 等人的 2DH 构造框架[44]以及 Hoefheinz 等人的基于因子分解假设的构造框架[45].

总体来说,目前标准模型中加密方案的效率还没有超越随机谕言模型中的方案,但是较之以前已经有了长足进步.在标准模型中研究方案构造和密码学原语,都能够推进对随机谕言模型的实例化和弱化的研究;而随机谕言模型中的方案设计思想对标准模型的加密方案构造也有所启发.

8 结束语

随机谕言模型的提出,是为了实现安全性和效率的平衡:一方面,需要构造能够满足实际应用需求的高效率的密码方案;另一方面,还需要尽量建立方案的可证明安全性.由于随机谕言模型中的可证明安全性并不等同于标准模型中的安全性,而后者被认为更接近于现实模型,因此,随机谕言方法引起了学术界的质疑.然而,随机谕言方法仍然在工业界取得了成功,在大量关于随机谕言模型的负面结论产生之后,在随机谕言模型中构造的高效率的密码方案仍然成为工业标准,或者进入了工业标准草案.随机谕言模型只有在两种情况下才会终结:一是产生了与随机谕言模型相关的现实攻击,二是在标准模型中构造的方案的效率可以与随机谕言模型中的方案的效率相匹敌.这样看来,在一段时间里,随机谕言模型的支持者和反对者仍然将会同行.因此,本文试图全面地介绍随机谕言模型的起源、发展、基本性质和当前研究热点,并将随机谕言模型与标准模型以及其他理想模型进行比较说明,以期对这方面的研究者有所帮助.

References:

[1] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Denning DE, Pyle R, Ganesan R, Sandhu RS, Ashby V, eds. Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62−67. [doi: 10.1145/168588.168596]

[2] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Science, 1984,28(2):270−299. [doi: 10.1016/0022-0000(84)90070-9]

[3] Feng DG. Research on Theory and Approach of Provable Security. Journal of Software, 2005,16(10):1743−1756 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1743.htm [doi: 10.1360/jos161743]

[4] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko A, ed. Proc. of the Advances in Cryptology—Crypto'86. LNCS 263, Berlin, Heidelberg: Springer-Verlag, 1986. 186−194. [doi: 10.1007/3-540-47721-7_12]

[5] Goldwasser S, Taumann YT. On the (in) security of the Fiat-Shamir paradigm. In: Proc. of the 44th Symp. on Foundations of Computer Sciences. Washington: IEEE Computer Society, 2003. 102−115. [doi: 10.1109/SFCS.2003.1238185]

[6] Mao W, Wrote; Wang JL, Trans. Modern Cryptography: Theory and Practice. Beijing: Publishing House of Electronics Industry, 2004 (in Chinese).

[7] Bellare M, Rogaway P. Optimal asymmetric encryption. In: Santis AD, ed. Proc. of the Advances in Cryptology—EUROCRYPT'94. LNCS 950, Berlin, Heidelberg: Springer-Verlag, 1995. 92−111.

[8] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. In: Wiener MJ, ed. Proc. of the Advances in Cryptology—CRYPTO'99. LNCS 1666, London: Springer-Verlag, 1999. 537−554. [doi: 10.1007/3-540-48405-1_34]

[9] Shoup V. OAEP reconsidered. In: Kilian J, ed. Proc. of the Advances in Cryptology—Crypto 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 239−259. [doi: 10.1007/3-540-44647-8_15]

[10] Fujisaki E, Okamoto T, Pointcheval D, Stern J. RSA-OAEP is secure under the RSA assumption. In: Kilian J, ed. Proc. of the Advances in Cryptology—Crypto 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 260−274. [doi: 10.1007/s00145-002-0204-y]

[11] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Proc. of the Advances in Cryptology—Crypto 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[12] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, Chaum D, eds. Proc. of the Advances in Cryptology—Crypto'84. LNCS 196, Berlin, Heidelberg: Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[13] Bellare M, Desai A, Pointcheval D, Rogaway P. Relations among notions of security for public-key encryption schemes. In: Krawczyk H, ed. Proc of the Advances in Cryptology—Crypto'98. LNCS 1462, Berlin, Heidelberg: Springer-Verlag, 1998. 26−46. [doi: 10.1007/BFb0055718]

[14] Bellare M, Palacio A. Towards plaintext-aware public-key encryption without random oracles. In: Lee PJ, ed. Proc. of the Advances in Cryptology—Asiacrypt 2004. LNCS 3494, Berlin, Heidelberg: Springer-Verlag, 2004. 440−456. [doi: 10.1007/978-3-540-30539-2_4]

[15] Di Raimondo M, Gennaro R, Krawczyk H. Deniable authentication and key exchange. In: Juels A, Wright RN, De Capitani di Vimercati S, eds. Proc. of the ACMCCS 2006. New York: ACM Press, 2006. 400−409. [doi: 10.1145/1180405.1180454]

[16] Canetti R. Towards realizing random oracles: Hash functions that hide all partial information. In: Kaliski BS Jr, ed. Proc. of the Advances in Cryptology—Crypto'97. LNCS 1294, Berlin, Heidelberg: Springer-Verlag, 1997. 455−469.

[17] Canetti R, Micciancio D, Reingold O. Perfectly one-way probabilistic hash functions. In: Vitter JS, ed. Proc. of the STOC'98. New York: ACM Press, 1998. 131−140. [doi: 10.1145/276698.276721]

[18] Boldyreva A, Fischlin M. Analysis of random oracle instantiation scenarios for OAEP and other practical schemes. In: Shoup V, ed. Proc. of the Advances in Cryptology—Crypto 2005. LNCS 3621, Berlin, Heidelberg: Springer-Verlag, 2005. 412−429. [doi: 10.1007/11535218_25]

[19] Pandey O, Pass R, Vaikuntanathan V. Adaptive one-way functions and applications. In: Wagner D, ed. Proc. of the Advances in Cryptology—Crypto 2008. LNCS 5157, Berlin, Heidelberg: Springer-Verlag, 2008. 57−44. [doi: 10.1007/978-3-540-85174-5_4]

[20] Canetti R, Dakdouk RR. Extractable perfectly one-way functions. In: Aceto L, Damgard I, Goldberg LA, Halldórsson MM, Ingólfsdóttir A, Walukiewicz I, eds. Proc. of the ICALP 2008. LNCS 5126, Berlin, Heidelberg: Springer-Verlag, 2008. 449−460. [doi: 10.1007/978-3-540-70583-3_37]

[21] Boldyreva A, Fischlin M. On the security of OAEP. In: Lai X, Chen K, eds. Proc. of the Advances in Cryptology—Asiacrypt 2006. LNCS 4284, Berlin, Heidelberg: Springer-Verlag, 2006. 210−225.

[22] Kiltz E, O'Neil A, Smith A. Instantiability of RSA-OAEP under chosen-plaintext attack. In: Rabin T, ed. Proc. of the Advances in Cryptology—Crypto 2010. LNCS 6223, Berlin, Heidelberg: Springer-Verlag, 2010. 295−313. [doi: 10.1007/978-3-642-14623-7_16]

[23] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004,51(4):557−594. [doi: 10.1145/1008731.1008734]

[24] Nielsen JB. Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In: Yung M, ed. Proc. of the Advances in Cryptology—Crypto 2002. LNCS 2442, Berlin, Heidelberg: Springer-Verlag, 2002. 111−126. [doi: 10.1007/3-540-45708-9_8]

[25] Hofheinz D, Kiltz E. Programmable Hash functions and their applications. In: Wagner D, ed. Proc. of the Advances in Cryptology—Crypto 2008. LNCS 5157, Berlin, Heidelberg: Springer-Verlag, 2008. 21−38. [doi: 10.1007/978-3-540-85174-5_2]

[26] Bellare M, Boldyreva A, Palacio A. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In: Cachin C, Camenisch J, eds. Proc. of the Advances in Cryptology—EUROCRYPT 2004. LNCS 3027, Berlin, Heidelberg: Springer-Verlag, 2004. 171−188. [doi: 10.1007/978-3-540-24676-3_11]

[27] Maurer U, Renner R, Holenstein C. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor M, ed. Proc. of the TCC 2004. LNCS 2951, Berlin, Heidelberg: Springer-Verlag, 2004. 21−39.

[28] Brown DRL. Unprovable security of RSA-OAEP in the standard model. Report 2006/223. Cryptology ePrint Archive, 2006.

[29] Kiltz E, Pietrzak K. On the security of padding-based encryption schemes. In: Joux A, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2009. LNCS 5479, Berlin, Heidelberg: Springer-Verlag, 2009. 389−406. [doi: 10.1007/978-3-642-01001-9_23]

[30] Leurent G, Nguyen PQ. How risky is the random-oracle model. In: Halevi S, ed. Proc. of the Advances in Cryptology—CRYPTO 2009. LNCS 5677, Berlin, Heidelberg: Springer-Verlag, 2009. 445−464. [doi: 10.1007/978-3-642-03356-8_26]

[31] Liskov M. Constructing an ideal hash function from weak ideal compression functions. In: Haddad H, ed. Proc. of the SAC 2006. LNCS 4356, Berlin, Heidelberg: Springer-Verlag, 2007. 358−375. [doi: 10.1007/978-3-540-74462-7_25]

[32] Kawachi A, Numayama A, Tanaka K, Xagawa K. Security of encryption schemes in weakened random oracle models. In: Nguyen PQ, Pointcheval D, eds. Proc. of the PKC 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 403−419. [doi: 10.1007/978-3-642-13013-7_24]

[33] Wee H. Zero knowledge in the random oracle model, revisited. In: Matsui M, ed. Proc. of the Advances in Cryptology—ASIACRYPT 2009. LNCS 5912, Berlin, Heidelberg: Springer-Verlag, 2009. 417−434. [doi: 10.1007/978-3-642-10366-7_25]

[34] Unruh D. Random oracles and auxiliary input. In: Menezes A, ed. Proc. of the Advances in Cryptology—CRYPTO 2007. LNCS 4622, Berlin, Heidelberg: Springer-Verlag, 2007. 205−223. [doi: 10.1007/978-3-540-74143-5_12]

[35] Shannon CE. Communication theory of secrecy systems. Bell Systems Technical Journal, 1949,28(4):656−715.

[36] Coron JS, Dodis Y, Malinaud C, Puniya P. Merkle-Damgård revisited: How to construct a hash function. In: Shoup V, ed. Proc. of the Advances in Cryptology—Crypto 2005. LNCS 3621, Berlin, Heidelberg: Springer-Verlag, 2005. 430−448.

[37] Coron JS, Patarin J, Seurin Y. The random oracle model and the ideal cipher model are equivalent. In: Wagner D, ed. Proc. of the Advances in Cryptology—Crypto 2008. LNCS 5157, Berlin, Heidelberg: Springer-Verlag, 2008. 1−20. [doi: 10.1007/978-3-540-85174-5_1]

[38] Shoup V. Lower bounds for discrete logarithms and related problems. In: Fumy W, ed. Proc of the Advances in Cryptology—Eurocrypt'97. LNCS 1233, Berlin, Heidelberg: Springer-Verlag, 1997. 256−266. [doi: 10.1007/3-540-69053-0_18]

[39] Dent AW. The hardness of the DHK problem in the generic group model. Technical Report, 2006/156, 2006.

[40] Dent AW. Adapting the weaknesses of the random oracle model to the generic group model. In: Zheng Y, ed. Proc. of the Advances in Cryptology—Asiacrypt 2002. LNCS 2501, Berlin, Heidelberg: Springer-Verlag, 2002. 100−109. [doi: 10.1007/3-540-36178-2_6]

[41] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H, ed. Proc of the Advances in Cryptology—Crypto'98. LNCS 1462, Berlin, Heidelberg: Springer-Verlag, 1998. 13−25. [doi: 10.1007/BFb0055717]

[42] Cramer R, Shoup V. Universal Hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen LR, ed. Proc. of the Advances in Cryptology—Eurocrypt 2002. LNCS 2332, Berlin, Heidelberg: Springer-Verlag, 2002. 45−64. [doi: 10.1007/3-540-46035-7_4]

[43] Peikert C, Waters B. Lossy trapdoor functions and their applications. In: Dwork C, ed. Proc. of the STOC 2008. New York: ACM Press, 2008. 187−196. [doi: 10.1145/1374376.1374406]

[44] Cash D, Kiltz E, Shoup V. The twin Diffie-Hellman problem and applications. In: Smart N, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2008. LNCS 4965, Berlin, Heidelberg: Springer-Verlag, 2008. 127−145. [doi: 10.1007/978-3-540-78967-3_8]

[45] Hofheinz D, Kiltz E. Practical chosen ciphertext secure encryption from factoring. In: Joux A, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2009. LNCS 5479, Berlin, Heidelberg: Springer-Verlag, 2009. 313−332. [doi: 10.1007/978-3-642-01001-9_18]

[46] Wee H. Efficient chosen-ciphertext security via extractable Hash proofs. In: Rabin T, ed. Proc. of the Advances in Cryptology—Crypto 2010. LNCS 6223, Berlin, Heidelberg: Springer-Verlag, 2010. 314−332. [doi: 10.1007/978-3-642-14623-7_17]

附中文参考文献:

[3] 冯登国.可证明安全性理论与方法研究.软件学报,2005,16(10):1743−1756. http://www.jos.org.cn/1000-9825/16/1743.htm [doi: 10.1360/jos161743]

[6] Mao W,著;王继林,译.现代密码学理论与实践.北京:电子工业出版社,2004.

贾小英(1978－),女,湖北襄阳人,博士生,主要研究领域为可证明安全.

刘亚敏(1983－),女,博士,主要研究领域为公钥加密.

李宝(1962－),男,博士,研究员,博士生导师,主要研究领域为密码学基础.