后量子可证明安全研究

江浩东 [1,2], 刘亚敏 [3]

[1] 数学工程与先进计算国家重点实验室 郑州 中国 450001
[2] 中国科学院软件研究所可信计算与信息保障实验室 北京 中国 100190
[3] 中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093

摘要 后量子密码经过数十年的发展, 其效率已经趋于实用化, 其标准化工作也正在开展中。与此同时, 对量子环境中的密码方案的可证明安全理论的研究在近十年也备受关注。本文将介绍近年来后量子可证明安全领域的发展和研究现状, 包括经典密码方案在量子环境中的安全模型建立、安全概念定义, 以及经典环境和量子环境中的安全性的分离结论和蕴含结论, 并重点介绍量子随机谕言模型中的安全性证明。对后量子可证明安全理论的研究, 对于合理评估密码算法在量子环境中的安全性、实现到后量子密码算法的安全平稳过渡具有重要意义。

关键词 后量子密码学; 可证明安全; 量子随机谕言模型
中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.03.02

On Post-Quantum Provable Security

JIANG Haodong [1, 2], LIU Yamin [3]

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
[2] Trusted Computing and Information Assurance Laboratory, Chinese Academy of Sciences, Beijing 100190, China
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract Post-quantum cryptosystems are becoming more and more practical in efficiency after decades of development, and the standardization of them is also in progress. In the meantime, the research on the provable security theory of cryptosystems in the quantum setting attracts much attention in the past decade. In this paper we give a survey on the development and state-of-art of the field of post-quantum provable security, including the establishing of security models and the defining of security notions for classical cryptosystems in the quantum setting, and the separation and the implication results of security in the classical setting and the quantum settings. Especially, security proofs in the quantum random oracle model are introduced. The research on the post-quantum provable security theory, is of significance for appropriately evaluating the security of cryptographic algorithms in the quantum setting and realizing a safe and smooth transition to post-quantum cryptographic algorithms.

Key words post-quantum cryptography; provable security; quantum random oracle model

1 绪论

后量子密码指面对量子敌手时仍然安全的经典密码。这个领域的研究包括探索抗量子的基础困难问题、设计对量子敌手免疫的密码方案, 以及后量子环境下的可证明安全理论等。目前, 对抗量子的基础困难问题的研究已经很丰富, 例如格上的最短向量问题、有限距离解码问题, 多变量方程的求解问题, 随机线性码解码问题等, 都被认为是抗量子的。后量子密码方案的构造也已经趋于成熟, 尤其基于散列函数的签名、基于格的加密和签名等方案, 效率与传统的公钥密码方案相当。而后量子环境中的可证明安全理论, 在近十年也处于蓬勃发展状态[1]。

可证明安全方法[2]使用归约, 将密码方案的安全性和数学问题的困难性联系起来, 为方案的安全性提供理论依据, 也为方案实施时的参数选取提供参考。因此在公钥密码领域, 可证明安全是设计方案时的基本指导思想; 在对称密码领域, 可证明安全

通讯作者: 刘亚敏, 博士, 助理研究员, Email: ymliu@is.ac.cn。
本课题得到国家自然科学基金面上项目“公钥密码的后量子可证安全理论研究”(No. 61772515), 以及国家自然科学基金青年项目“可证明安全的确定性公钥加密体制研究”(No. 61502480)资助。
收稿日期: 2018-11-08; 修改日期: 2019-02-18; 定稿日期: 2019-02-26

也有许多应用, 例如散列函数的安全性质证明、分组密码的工作模式等。

经典环境中, 经典密码算法在经典计算机上实现, 敌手也只拥有经典计算机。量子环境中主要考虑的仍然是在经典计算机上实现经典密码算法, 而敌手拥有量子计算机, 使用量子态的相干叠加性可以实现计算的量子并行; 对于密码算法中的一些公开组件, 例如散列函数, 敌手可以自行用量子电路实现, 这反映在安全性归约中便是敌手可以对这些组件相关的谕言使用叠加态询问。更为超前的是考虑在量子计算机上实现经典密码算法, 敌手可以对算法的一些私有组件相关的谕言使用叠加态询问, 例如允许敌手进行叠加态的解密询问等。这些情形都是经典可证明安全理论不足以刻画的; 并且在经典环境中成立的安全性证明、使用的证明技术在量子环境中不一定继续生效。如何合理地为量子环境中的经典方案建立安全模型和定义安全概念, 以及经典安全性能否蕴含量子安全性, 这些问题引出对后量子可证明安全理论的研究。这对于合理评估密码算法在量子环境中的安全性、实现到后量子密码算法的安全平稳过渡具有重要意义。例如在美国标准化组织 NIST 的后量子公钥密码算法标准征集项目中, 许多候选算法都考虑了量子环境中的安全性证明。

本文将介绍近年来后量子可证明安全领域的发展和研究现状, 包括经典密码方案在量子环境中的安全模型建立、安全概念定义, 以及经典环境和量子环境中的安全性的分离结论和蕴含结论, 并重点介绍量子随机谕言模型中的安全性证明。

2 量子环境中的安全模型和安全概念

在经典可证明安全理论中, 为了刻画密码算法的安全性, 研究者提出了多种安全模型和安全概念。在量子环境中, 这些模型和概念的重新定义和可满足性成为一个问题。本节将介绍量子环境中的安全模型和安全概念定义, 以及对应的方案构造。

2.1 量子随机谕言模型

随机谕言(Random Oracle, RO)模型[3]是一个理想化模型。在 RO 模型中, 散列函数被理想化为一个公开可访问的随机谕言, 散列函数的计算通过询问随机谕言来实现。在实际密码学应用中, 高效的可证明安全的密码方案往往是基于 RO 模型设计, 如 RSA-OAEP 加密[4], Fujisaki-Okamoto(FO)转换[5]等。许多高效后量子密码方案也产生于 RO 模型, 如文献[6]中的签名方案, 文献[6-8]中基于身份的加密(identity- based encryption, IBE)等。

在后量子时代, 量子敌手可以在量子计算机上离线量子叠加计算散列函数。因此, 为了更好地刻画量子敌手能力, Boneh 等人[9]提出量子 RO 模型(quantum random oracle model, QROM), 并论证了在考虑密码学方案后量子安全性时, 需要考虑量子 RO 模型。不同于经典 RO 模型, 量子 RO 模型中敌手可以使用叠加态询问随机谕言。因此, 经典 RO 模型中的理想性质在量子 RO 模型中不一定存在, 如自适应可编程、询问提取等; 归约算法甚至难以为敌手模拟 RO; 识别在量子 RO 模型中继续成立的安全归约也很复杂。特别地, Boneh 等人[9]通过构造一个区分实例说明了经典 RO 模型下可证明安全的方案在量子 RO 模型下并不一定是安全的。研究如何在量子 RO 模型下证明密码方案的安全性成为一个有趣的问题。

2.2 密码系统的量子安全性

通常, 安全性定义中刻画了密码方案期望达到的安全目标和可能遇到的攻击, 以“游戏”的形式描述密码方案的诚实用户和敌手之间的交互。在经典环境中, 这些交互都是通过发送经典信息来进行的。而在量子环境中, 有些交互可能是以量子态进行的, 例如当一个经典密码算法在量子计算机上实现时, 敌手能够以量子态与诚实用户交互。这样, 经典环境和量子环境中的安全性定义的强度和可满足性可能会有所不同。在这一动机驱使下, 出现了一系列对量子安全性定义的研究。

2.2.1 量子通用可复合性

Canetti 提出的通用可复合性[10](universal composability, UC)是一种基于模拟的安全性定义。在 UC 的定义框架下, 称一个协议安全地实现了给定的理想函数(functionality), 如果对任意现实世界的敌手, 都存在一个理想世界的模拟器, 使得区分器(称为环境)无法区分协议是在有敌手的现实世界运行还是在有模拟器的理想世界运行; 这也意味着现实世界的协议运行并未向敌手泄露更多信息。按照区分器的计算能力, UC 可以分为统计 UC 安全和计算 UC 安全。UC 的定义框架十分强大, 它以统一的方式表达了多种协议的安全性, 并且 UC 安全保证了协议可以安全地复合。

Ben-Or 和 Mayers[11], Unruh[12]分别独立地在量子环境中定义了 UC 安全性, 并应用到对量子协议的研究中。为了研究量子不经意传输协议(oblivious transfer, OT)的构造, 2010 年 Unruh 给出了新的更简单的量子 UC 安全性的定义[13], 并且对经典协议和量子协议都适用。与经典的 UC 框架相比, 文献[13]

中的量子 UC 框架定义的主要改变在于允许所有参与方进行量子计算以及发送量子态的消息。Unruh 证明了经典意义下的统计 UC 安全性便蕴含了量子统计 UC 安全性。

随后, Hallgren, Smith 和宋方[14]提出了两方协议的量子独立安全性(stand-alone security), 这可以视为 Unruh 的量子 UC 安全性的弱化, 即协议的安全模型中, 充当区分器的环境是非交互的; 此外, 文献[14]中还证明了一些满足经典意义下的计算 UC 安全性的方案, 也可以满足量子计算 UC 安全性。在文献[15]中, Fehr 等人继续研究了在 UC 框架下实现函数的可能性。

2.2.2 量子安全的伪随机函数

伪随机函数[16](pseudorandom function)是各类密码算法(如分组密码、消息认证码等)构造中的重要基础模块。伪随机函数的安全性定义要求, 对于任意具有多项式次访问谕言的能力的敌手, 区分其与真随机函数的优势是可忽略的。在经典环境中, 敌手的谕言访问方式自然是经典的。这一定义也被沿用到量子环境中, 称为“标准安全性”: 量子敌手进行经典询问, 但是敌手自身的计算可以是量子的。2012 年 Zhandry 提出了伪随机函数的量子安全性定义[17], 允许敌手进行量子询问。在这种安全模型下, 伪随机函数已经在量子电路中运行。

Zhandry 指出, 伪随机函数的量子安全性是强于其标准安全性的, 并给出了在量子环境下满足标准安全性但是不满足量子安全性的 PRF 的构造。随后, Zhandry 证明了 Goldreich, Goldwasser 和 Micali 于 1986 年提出的基于伪随机生成器构造的伪随机函数[16]可以满足量子安全性。文献[16]中的构造在经典环境中的证明并不能直接在量子环境中成立。Zhandry 使用了新的技术来证明其量子安全性。为了实现这一点, Zhandry 定义了分布的谕言不可区分性质(oracle-indistinguishability)。给定两个分布, 在不可区分性定义中, 量子区分器可以得到它们的采样; 而谕言不可区分性质中, 量子区分器能够以量子询问方式访问一个谕言, 并判断谕言所实现的是哪一个分布。Zhandry 证明了两个分布的不可区分性质和它们的谕言不可区分性质是等价的。这样, 以文献[16]中基于伪随机生成器(pseudorandom generator)的伪随机函数构造的证明为例, Zhandry 先将伪随机生成器的谕言不可区分性质归约为伪随机函数的量子安全性, 而伪随机生成器的谕言不可区分性质又由其输出分布与均匀分布的不可区分性质而来。

使用类似的证明思路, 文献[17]中还证明了 Naor 和 Reingold 基于伪随机合成器[18](pseudorandom synthesizer)的构造, 以及 Banerjee, Peikert 和 Rosen 基于带取整的学习问题(learning with rounding)的构造[19]都是量子安全的。2017 年, 宋方和 Yun 证明了 NMAC,HMAC,AMAC 等构造都是量子安全的伪随机函数[20]。

2.2.3 量子安全的消息认证码

消息认证码(message authentication code, MAC)是用于提供数据完整性的工具, 通常基于伪随机函数构造。与伪随机函数的情形类似, Boneh 和 Zhandry 也研究了消息认证码的量子安全性[21]。

消息认证码在选择消息攻击下的存在性不可伪造性(existentially unforgeable under chosen message attack, EUF-CMA)定义中, 敌手可以访问一个 MAC 谕言, 为敌手选定的消息产生标签。如果敌手最终不能为一个它未曾询问过 MAC 谕言的消息产生合法的标签, 则称这个消息验证码方案是 EUF-CMA 安全的。在经典环境中, 敌手对 MAC 谕言的访问是经典的。类似伪随机函数的情形, 也可以将这一定义直接沿用到量子环境中, 使量子敌手也只能提交经典询问。Boneh 和 Zhandry 指出[21], 如果允许敌手对 MAC 谕言提交量子询问, 即可得到对量子选择消息攻击的存在性不可伪造性定义(EUF-qCMA): 称消息认证码方案 MAC 是对量子选择消息攻击存在性不可伪造安全的, 如果没有敌手能够在 k 次量子选择消息询问后, 产生 k+1 个合法的经典消息-标签对。

与伪随机函数的两种安全性定义的强弱类似, EUF-qCMA 也是严格强于 EUF-CMA 的。Boneh 和 Zhandry[21]基于量子安全的伪随机函数构造了具有 EUF-qCMA 安全性的 MAC 方案; 此外, 他们还证明, 将 Carter-Wegman 的 MAC 构造稍作变形, 即可证明其 EUF-qCMA 安全性。经典环境中, 使用 2-wise 独立的函数族即可构造一次性 MAC; 但 Boneh 和 Zhandry 证明了在量子环境中 2-wise 独立是不够的, 对于一次性 MAC, 需要 4-wise 独立的散列函数族, 才能保证其量子安全性。

2.2.4 量子安全的签名

对于签名方案, Boneh 和 Zhandry 定义了对量子选择消息攻击的存在性不可伪造性[22](EUF-qCMA)。这个定义和消息认证码的量子安全性的定义方式非常相似: 如果敌手以量子询问方式访问签名谕言 q 次后, 不能产生 q+1 个合法且通过签名验证的消息-签名对, 则称签名方案满足 EUF-qCMA。签名方案的 EUF-qCMA 也是严格强于只使用经典询问的 EUF-CMA 定义的。

Boneh 和 Zhandry 给出了两种方法, 可将满足经典安全性定义的签名方案转化为满足量子安全性定义。其一是对于满足经典 EUF-CMA 定义的签名, 使用变色龙散列函数(chameleon hash function)来处理原签名方案的消息, 然后对散列函数值签名, 这样得到的新签名方案就能满足 EUF-qCMA 安全性。这样, 他们证明了一些基于格上的小整数解问题(small integer solution, SIS)构造的签名方案, 都可以变形为 EUF-qCMA 安全的, 例如 Cash 等在文献[8]中构造的签名, 以及 Agrawal 等在文献[7]中构造的签名。其二是对于在经典意义下满足较弱的对随机消息攻击的通用不可伪造性(universally unforgeable under random message attack, UUF-RMA)的签名方案, 使用刻画为随机谕言的散列函数来处理消息, 然后对散列函数值签名。这样可以得到在量子随机谕言模型下满足 EUF-qCMA 安全性的签名方案。

2014 年宋方[23]也证明了基于散列树的签名, 例如文献[24]中提出的签名方案是量子安全的。

2.2.5 量子选择密文安全的加密

对自适应选择密文攻击的不可区分性(indistinguishability against adaptive chosen ciphertext attack, IND-CCA2)[25]是公钥加密方案的标准安全准则。经典 IND-CCA2 游戏分成两个阶段, 寻找阶段, 其中敌手自由选择两个明文; 以及猜测阶段, 其中敌手得到两个密文之一的加密, 称为挑战密文, 并输出对于其所加密的明文的猜测。在寻找阶段和猜测阶段敌手都可以访问解密谕言, 只是在猜测阶段它不能请求挑战密文的解密。

IND-CCA2 的概念也被引入到了对称加密中, 其定义形式与公钥加密的情形类似, 只是在寻找阶段和猜测阶段, 敌手都可以访问一个加密谕言, 为敌手提供加密服务。

一个加密方案是 IND-CCA2 安全的, 如果任意敌手在其 IND-CCA2 游戏中的猜测优势可忽略。比 IND-CCA2 弱一些的安全概念还有对非自适应性选择密文攻击的不可区分性(IND-CCA1), 在其中不允许敌手在猜测阶段访问解密谕言; 以及更弱的对选择明文攻击的不可区分性(IND-CPA), 其中敌手的寻找阶段和猜测阶段都不可以访问解密谕言。

Boneh 和 Zhandry 定义了量子选择密文攻击安全性[22](IND-qCCA2)。无论是公钥加密还是对称加密, 它们的 IND-qCCA2 定义中都允许敌手使用叠加态的密文访问解密谕言, 并得到叠加态的明文; 只是在猜测阶段如果叠加态密文中有挑战密文, 解密谕言仍然会拒绝提供其明文。对于对称加密方案, IND-qCCA2 的加密谕言也可以接收量子态的询问: 在收到对叠加态明文的加密请求时, 选择一个随机数, 并用其加密叠加态中所有明文, 返回叠加态的密文。加密的 IND-qCCA2 定义也是严格强于经典环境中的 IND-CCA2 的。类似的定义方式也可以应用到 IND-CCA1 和 IND-CPA, 得到 IND-qCCA1 和 IND-qCPA。

Boneh 和 Zhandry 基于量子安全的伪随机函数构造了具有 IND-qCCA2 安全性的对称加密方案; 而经典环境中将 IBE 方案转化为 IND-CCA2 安全的公钥加密的 CHK 转换[26], 也可以类似地用来构造 IND-qCCA2 安全的公钥加密方案, 只要 IBE 方案对于量子选择身份攻击是安全的, 例如文献[7]中基于格上带错误的学习问题构造的 IBE 方案。

2.2.6 承诺方案和散列函数的量子安全性

在经典环境中承诺方案的安全性包括绑定(binding)和隐藏(hiding), 并且这二者不能同时在统计意义下成立。量子环境对隐藏性质的定义影响不大, 但是对于绑定性质, 沿用经典定义并不合适, 尤其是在计算绑定(computationally-binding)的情形下。Unruh 为承诺方案定义了坍缩绑定(collapse-binding)性质[27], 可视为量子环境中的计算绑定。

在经典环境中, 承诺方案的计算绑定性通常基于散列函数的抗碰撞性。虽然散列函数的抗碰撞性在量子环境中所受影响较小, 但是抗碰撞性不足以保证坍缩绑定性。因此, Unruh 为散列函数在量子环境中定义了更强的坍缩(collapsing)性质[27], 能够蕴含抗碰撞性。从坍缩的散列函数可以构造具有坍缩绑定性质的承诺方案。因此, 寻找具有坍缩性质的散列函数也成为一个有趣的研究问题。在文献[28]中, Unruh 研究了基于 Merkle-Damgård 构造的散列函数例如 SHA2 的坍缩性; 在文献[29]中 Czajkowski 等人研究了海绵(sponge)结构的坍缩性。

3 经典环境和量子环境中安全性证明的关系

量子环境中敌手拥有更多的计算资源, 其对密码方案的攻击能力也更为强大。量子攻击不仅可针对方案所基于的困难问题, 也可体现在通信和计算的多个环节。这使得经典环境中定义的安全模型、安全概念与它们的量子版本之间可能存在差距(gap), 从而对应的安全性证明在量子环境中失效; 但是也存在具有良好可移植性的安全性证明, 其在经典环境中成立, 在量子环境中也继续成立。本节将介绍经典环境和量子环境中的一些分离(separation)结论和蕴含结论。

3.1 分离结论

Boneh 等人[9]证明了经典 RO 模型中的安全性并不意味着量子 RO 模型中的安全性。在文献[9]中给出了一个身份认证协议, 其在经典 RO 模型中对经典敌手安全, 在有量子敌手但是 RO 以经典方式访问的环境中依然安全, 但是在量子 RO 模型中不安全。该协议的构造利用了量子算法和经典算法在寻找散列函数的碰撞上有明显的算力差这一前提[30-31], 修改身份认证协议中证明者通过验证的条件为“成功伪造证明, 或者成功在特定时间内找到足够多的散列碰撞”。这样, 如果敌手能够以量子叠加态询问访问实现散列函数的谕言, 就能够比只有经典询问时找到更多的碰撞, 从而通过验证。

在为伪随机函数定义量子安全性时, Zhandry 也证明了文献[17]其量子安全性严格强于标准安全性。给定一个满足经典环境中的标准安全性的伪随机函数, Zhandry 构造了一个具有大周期的新函数。由于量子算法和经典算法在找周期问题上具有明显的算力差[32], 当敌手可以使用量子叠加态询问时, 它可以找到新函数的周期, 从而攻破其量子伪随机性质; 而敌手只能使用经典询问时无法找到周期, 因此新函数对敌手来说仍然是伪随机的。类似的方法可以用来证明消息认证码、签名、加密等原语的量子安全性和标准安全性之间的差距。

3.2 蕴含结论

Boneh 等人[9]为签名算法定义了无历史归约(history-free reduction)。如果签名算法在经典 RO 模型中的安全性归约以无历史的方式模拟 RO, 归约算法对 RO 询问的回答不依赖于以往的询问, 也不依赖于询问次数, 则称该归约是无历史的。只需要使用量子安全的伪随机函数来模拟量子 RO, 则无历史归约可以直接移植到量子 RO 模型中, 从而使方案的安全性证明在量子 RO 模型中成立。

宋方提出了量子友好的安全性归约(quantum-friendly security reduction)的框架[14]。在文献[23]中将安全性归约分为两类, 一类称为游戏保持(game-preserving), 另一类称为游戏更新(game-updating)。对于游戏保持的归约, 只要其满足一些准则, 例如可扩展(extendible), 直线型(straight-line)等, 就可以对量子敌手继续成立。而对于游戏更新的归约, 如果其是可译的(translatable), 则可构造一个解释器(interpreter), 将其转换为游戏保持的类型。

4 量子随机谕言模型中的安全性证明

研究密码方案在量子 RO 模型中的安全性证明在近年来颇受关注。在本节我们将介绍对于公钥加密、密钥封装、签名以及 IBE 等密码方案在量子 RO 模型中的证明进展。

4.1 公钥加密算法和密钥封装机制

2011 年, Boneh 等人[9]证明了文献[3]中的混合加密方案在量子 RO 模型下是可证明安全的, 其安全归约损失是二次的。基于 Unruh 在文献[33]中提出的 oneway- to-hiding(OW2H)引理, 以及文献[34]中提出的在线可提取(on-line extractability)技术, 2016 年, Targhi 等人[35]修改了 Fujisaki-Okamoto 变换[5]和 OAEP 方案[4], 在密文中增加了额外的 Targhi-Unruh 散列组件, 提出变形的 FO 变换和 OAEP 变换。额外的散列组件使得安全性证明中的解密模拟器可以提取到敌手对量子 RO 的询问, 从而可以在量子 RO 模型证明变形的 FO 变换和 OAEP 方案的安全性, 其安全归约损失分别是四次和八次的。

2017 年, Hofheinz 等人[36]提出 FO 变换的一系列密钥封装机制(key encapsulation mechanism, KEM)版本(FO-KEM), 并根据文献[35]的技术, 增加 Targhi-Unruh 散列组件, 在量子 RO 模型下证明 FO-KEM 安全性, 其安全归约损失是四次的。实际上, 对于密钥封装方案, 其解密模拟并不需要提取敌手的量子 RO 询问。因此, 2018 年, Saito 等人[37] 和 Jiang 等人[38]移除 Targhi-Unruh 散列组件, 证明了 FO-KEM 的安全性, 且给出了更紧致的安全归约。特别地, 如果基础 PKE 满足标准 CPA 安全性, 则安全归约损失是二次的; 如果基础 PKE 满足非标准的 DS(disjoint simulatability)安全性, 则安全归约是紧的。

4.2 数字签名

在 RO 模型中构造数字签名主要有两种方法, 其一是基于单向陷门函数/原像可采样函数, 例如 FDH 签名[3]和 GPV 签名[6]; 其二是基于 Fiat-Shamir 变换[39]。对这两种方法在量子 RO 模型中的安全性的研究目前已经较为完善。Boneh 等人[9]和 Zhandry[40]在量子 RO 模型下证明了基于格的 GPV 签名算法[6]的安全性和应用更为一般的 FDH[3]框架的安全性。2013 年, Dagdelen 等人[41]使用元归约(meta-reduction)技术, 在量子 RO 模型下论证了 Fiat- Shamir 变换的安全性, 阐述了一般证明的困难性, 给出了一些 Fiat- Shamir 变换的变形在量子 RO 模型中满足可证明安全性的一些条件。2014 年, Andris 等人[42]使用谕言分离(oracle separation)技术证明了一般情形下 Fiat-Shamir 变换在量子 RO 模型下是不安全的, 并针对一个特殊的构造, 给出了具体量子攻击算法。2017 年, Unruh[43]进一步研究了 Fiat- Shamir 变换在量子 RO

模型下可证明安全的条件。Kiltz 等人[44]在更为特殊的 Lossy 假设下, 完成 Fiat- Shamir 变换的安全证明, 并将其应用于具体的基于格的签名算法。

4.3 基于身份的加密

2012 年, Zhandry[40]证明了量子算法不能区分随机谕言和半常数(semi-constant)分布谕言, 从而证明文献[6]中的 IBE 方案在量子 RO 模型下是安全的。使用将半常数分布嵌入挑战的方法, 文献[40]中还证明了文献[8]和文献[7]中的分层 IBE 在量子 RO 模型中的安全性。2018 年, Katsumata 等人[45]改进了 Zhandry 的结果, 给出了更紧致的安全归约。

5 总结与展望

综上, 量子环境下的公钥密码可证明安全是近年来的新兴研究方向, 在后量子密码适用的基础原语、安全模型、安全概念、安全归约和方案构造等方面都有了较快发展, 也存在大量的开放问题。很多基础原语在量子环境中的存在性与构造还是未知的; 研究者们也正在将更多安全性定义扩展到量子环境中, 例如对量子不可分辨性[46]的最新研究[47-48]; 在量子 RO 模型中关于加密方案和密钥交换协议的安全性证明还相对较少; 识别在量子环境中继续适用的安全归约类型, 这一问题还需要更多探索。

参考文献

[1] T. Kan. A Survey on Quantum-Secure Cryptographic Systems. https://www.boazbarak.org/cs127/Projects/tomoka_kan.pdf

[2] S. Goldwasser and S. Micali. Probabilistic Encryption. Special issue of *Journal of Computer and Systems Sciences*, 28(2):270-299, 1984.

[3] M. Bellare and P. Rogaway. Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. *ACM CCS* 1993, pp. 62-73, 1993.

[4] M. Bellare and P. Rogaway. Optimal Asymmetric Encryption: How to Encrypt with RSA. *Eurocrypt 1994, LNCS* 950, pp. 92-111, 1995.

[5] E. Fujisaki, and T. Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. *CRYPTO* 1999, LNCS 1666, 537-554, 1999.

[6] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. *STOC* 2008, 197-206, 2008.

[7] S. Agrawal, D. Boneh, and X. Boyen. Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE. *CRYPTO* 2010, LNCS 6223, 98-115, 2010.

[8] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai Trees, or How to Delegate a Lattice Basis. *Eurocrypt* 2010, 523-552, 2010.

[9] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random Oracles in a Quantum World. *Asiacrypt* 2011, LNCS 7073, 41-69, 2011.

[10] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. *FOCS* 2001, 136-145, 2001.

[11] M. Ben-Or, and D. Mayers. General Security Definition and Composability for Quantum & Classical Protocols. arXiv:quant-ph/0409062v2

[12] D. Unruh. Simulatable Security for Quantum Protocols. arXiv:quant-ph/0409125v2

[13] D. Unruh. Universally Composable Quantum Multi-Party Computation. *Eurocrypt* 2010, LNCS 6110, 1484-1509, 1997.

[14] S. Hallgren, A. Smith, and F. Song. Classical Cryptographic Protocols in a Quantum World. *CRYPTO* 2011, LNCS 6841, 411-428, 2011.

[15] S. Fehr, J. Katz, F. Song, H. Zhou, and V. Zikas. Feasibility and Completeness of Cryptographic Tasks in the Quantum World. *TCC* 2013, LNCS 7785, 281-296, 2013.

[16] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. J*ournal of the ACM (JACM)*, 33(4): 792-807, 1986.

[17] M. Zhandry. How to Construct Quantum Random Functions. *FOCS* 2012, 679-687, 2012.

[18] M. Naor, and O. Reingold. Synthesizers and Their Application to the Parallel Construction of Pseudo-Random Functions. *FOCS* 1995, 170-181, 1995.

[19] A. Banerjee, C. Peikert, and A. Rosen. Pseudorandom Functions and Lattices. *Eurocrypt* 2012, LNCS 7237, 1-26, 2012.

[20] F. Song, and A. Yun. Quantum Security of NMAC and Related Constructions – PRF domain extension against quantum attacks. *CRYPTO* 2017, LNCS 10402, 283-309, 2017.

[21] D. Boneh, and M. Zhandry. Quantum-Secure Message Authentication Codes. *Eurocrypt* 2013, LNCS 7881, 592-608, 2013.

[22] D. Boneh, and M. Zhandry. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. *CRYPTO* 2013, Part II, LNCS 8043, 361-379, 2013.

[23] F. Song. A Note on Quantum Security for Post-Quantum Cryptography. *PQCrypto* 2014, LNCS 8772, 246-265, 2014.

[24] J. A. Buchmann, E. Dahmen, A. Hülsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. *PQCrypto 2011*: 117-129.

[25] C. Rackoff and D. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. *Crypto* 1991, LNCS 576, pp. 433-444, Springer, 1991.

[26] R. Canetti, S. Halevi, and J. Katz. Chosen-Ciphertext Security from Identity-based Encryption. *Eurocrypt* 2004, LNCS 3027, 207-222, 2004.

[27] D. Unruh. Computationally Binding Quantum Commitments. *Eurocrypt* 2016, Part II, LNCS 9666, 497-527, 2016.

[28] D. Unruh. Collapse-Binding Quantum Commitments without Random Oracles. *Asiacrypt* 2016, Part II, LNCS 10032, pp. 166-195, 2016.

[29] J. Czajkowski, L. G. Bruinderink, A. Hülsing, C. Schaffner, D. Unruh. Post-Quantum Security of the Sponge Construction. *PQCrypto* 2018, LNCS 10786, 185-204, 2018.

[30] L.K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. *STOC* 1996, 212-219, 1996.

[31] L.K. Grover. Quantum Search on Structured Problems. *QCQC* 1998, LNCS 1509, 126-139, 1999.

[32] D. Boneh and R.J. Lipton. Quantum Cryptanalysis of Hidden Linear Functions. *CRYPTO* 1995, LNCS 963, 424-437, 1995.

[33] D. Unruh. Revocable Quantum Timed-release Encryption. *Eurocrypt*

2014, LNCS 8441, 129-146, 2014.

[34] D. Unruh. Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model. *Eurocrypt* 2015, Part II, LNCS 9057, 755-784, 2015.

[35] E.E. Targhi, and D. Unruh. Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms. *TCC* 2016-B, Part II, LNCS 9986, 192-216, 2016.

[36] D. Hofheinz, K. Hövelmanns, and E. Kiltz. A Modular Analysis of the Fujisaki-Okamoto Transformation. *TCC* 2017, LNCS 10677, 341-371, 2017.

[37] T. Saito, K. Xagawa, and T. Yamakawa. Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model. *Eurocrypt* 2018, LNCS 10822, 520-551, 2018.

[38] H. Jiang, Z. Zhang, L. Chen, H. Wang and Z. Ma. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. *CRYPTO* 2018, LNCS 10993, 96-125, 2018.

[39] A. Fiat, and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. *CRYPTO* 1986, LNCS 263, 186-194, 1987.

[40] M. Zhandry. Secure Identity-Based Encryption in the Quantum Random Oracle Model. *CRYPTO* 2012, LNCS 7417, 758-775, 2012.

[41] Ö. Dagdelen, M. Fischlin, and T. Gagliardoni. The Fiat-Shamir Transformation in a Quantum World. *Asiacrypt* 2013, Part II, LNCS 8270, 62-81, 2013.

[42] A. Ambainis, A. Rosmanis, and D. Unruh. Quantum Attacks on Classical Proof Systems: the Hardness of Quantum Rewinding. *FOCS* 2014, 474-483, 2014.

[43] D. Unruh. Post-quantum security of Fiat-Shamir. *Asiacrypt* 2017, LNCS 10624, 65-95, 2017.

[44] E. Kiltz, V. Lyubashevsky, and C. Schaffner. A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. In *Eurocrypt* 2018, volume 10822 of LNCS, pages 552–586. Springer, 2018.

[45] S. Katsumata and S. Yamada and T. Yamakawa, Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model. *Asiacrypt* 2018, part II, LNCS 11273, 253-282, 2018.

[46] U. Maurer, R. Renner, and C. Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. *TCC* 2004, LNCS 2951, pp. 21-39, 2004.

[47] T.V. Carstens, E. Ebrahimi, G.N. Tabia, and D. Unruh. On Quantum Indifferentiability. Cryptology ePrint Archive, Report 2018/257, 2018.

[48] M. Zhandry. How to Record Quantum Queries, and Applications to Quantum Indifferentiability. Cryptology ePrint Archive, Report 2018/276, 2018.

江浩东 数学工程与先进计算国家重点实验室密码学专业博士研究生。目前在中科院软件研究所可信计算与信息保障实验室进行访问交流。研究领域为抗量子密码研究。研究兴趣包括量子可证明安全理论、格密码学设计与分析，量子算法与量子查询复杂度理论。Email: hdjiang13@gmail.com

刘亚敏 于 2011 年在中国科学院大学信息安全专业获得工学博士学位。现任中国科学院信息工程研究所助理研究员。研究领域为公钥密码学。研究兴趣包括: 可证明安全理论、基于格的公钥密码算法设计。Email: ymliu@is.ac.cn