Computer Science and Application 计算机科学与应用, 2017, 7(11), 1089-1100
Published Online November 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.711123

Hans汉斯

Development Analysis of Post Quantum Cryptography

Qiang Li, Qingfeng Cheng, Hongxin Li, Junqi Zhang

Luoyang Campus, Strategic Support Force Information Engineering University, Luoyang Henan
Email: lihongxin830@163.com

Received: Nov. 6th, 2017; accepted: Nov. 18th, 2017; published: Nov. 23rd, 2017

Abstract

Since the rapid development of quantum computing brings great impacts to classical cryptography, people set their sights on the research of post quantum cryptography. Along with the approach of the quantum era, the pace of research on post quantum cryptography is accelerating. This paper reviews the development of four types of post quantum cryptography, which are multivariate public key cryptography, Hash-based digital signature, code-based cryptography and lattice-based cryptography. And then the latest progress of post quantum cryptography is presented based on all the eight International Workshops on Post-Quantum Cryptography. These are of great value as reference for future research on quantum cryptography.

Keywords

Multivariate Public Key Cryptography, Hash-Based Digital Signature, Code-Based Cryptography, Lattice-Based Cryptography, International Workshops on Post-Quantum Cryptography

抗量子密码体制发展研究

李　强，程庆丰，李宏欣，张军琪

战略支援部队信息工程大学洛阳校区，河南　洛阳
Email: lihongxin830@163.com

收稿日期：2017年11月6日；录用日期：2017年11月18日；发布日期：2017年11月23日

摘　要

量子计算的快速发展带给经典密码的巨大冲击使得人们将目光投向了抗量子密码体制的研究。随着量子时代的迫近，抗量子密码体制的研究步伐也在不断加快。本文回顾了以多变量公钥密码体制、基于Hash

文章引用: 李强, 程庆丰, 李宏欣, 张军琪. 抗量子密码体制发展研究[J]. 计算机科学与应用, 2017, 7(11): 1089-1100.
DOI: 10.12677/csa.2017.711123

函数的数字签名、基于编码的密码体制和基于格的密码四类抗量子密码的发展历程，并结合迄今为止的八届国际抗量子密码年会展示了抗量子密码体制的最新进展。这些对今后抗量子密码的研究具有重要的参考价值。

关键词

多变量公钥密码，基于Hash函数的数字签名，基于编码的密码，基于格的密码，国际抗量子密码年会

1. 引言

近三十年，以公钥密码体制为代表的加密方法成为全球化通讯数字基础设备的一个不可或缺的组成部分，在军事、政治、经济、生活等方面都有广泛的应用，在个人、企业和政府的安全通讯中发挥着至关重要的作用。可以说，RSA 加密体制、Diffie-Hellman 密钥交换、椭圆曲线加密体制、代数同态等等密码体制是近年信息安全领域最受学者青睐的一些加密和签名方案。

这一现状随着量子计算的兴起与快速发展而改变。

1994 年贝尔实验室的 Peter Shor 提出了量子质因数分解算法[1]，使得在 20 世纪 80 年代之前一直处于纸上谈兵状态的量子计算瞬间成为学者们关注的热点。Shor 算法展现了量子计算机可以高效地处理整数分解、离散对数等很多数学难题，这种利用物质和能量的物理性质进行计算的新技术使得一切公钥密码体系的假设不再成立。自 Shor 算法提出之后，近二十年里量子算法理论有了极大发展。在针对物理模仿、数论和拓扑结构相关的一些研究中，人们又发现了能够完成指数级提速的量子算法，包括在搜索成绩、查找碰撞和布尔公式的评价的相关多类成绩上有更多过度的提速计算的量子算法[2]。特别是，Grover 算法在非结构化的搜索上提供了平方的提速计算。虽然这种提速计算不会使得加密技术彻底无效，但为了保持原有的安全性水平，密码方案中就必须增大密钥的规模。因此，一个足够强大的量子计算机将使许多之前通讯方式处于风险之中，包括从加密过程的密钥交换阶段到数字认证阶段。

量子计算对于传统加密体制的威胁绝不仅仅是耸人听闻，庸人自扰。迄今为止，量子算法已经能够破译包括 RSA 公钥加密体制、Diffie-Hellman 密钥交换、椭圆曲线加密体制、Buchmann-Williams 密钥交换、代数同态在内的多类密码[3]。而且，随着近些年计算机技术和新型材料技术的飞速发展，量子计算机的研究正以不可阻挡的势头占领信息通讯和网络安全的高地。科学技术的发展尤其是量子科技的日新月异，使得学术界越来越相信，量子计算机的出现和实用化将只是时间问题。

此外，由于量子计算机对传统加密体制具有重大的威胁，许多国家政府已经认识到量子计算机的战略意义。美国政府在此领域率先行动，投入巨资启动了五个量子计算机研究计划：美国国防高级研究计划局的“量子信息科学与技术发展规划”、美国国家安全局的 ARDA5 计划、美国科学基金会的 QuBIC 计划、美国宇航局的 QCTG 计划和美国国家标准与技术研究院的 PLQI 计划。此后，日本、欧盟、加拿大等国家和地区也相继启动了量子计算机发展规划。我国也由中国科技大学潘建伟团队投入量子计算机的研发当中，在国际上首次利用光量子计算机实现了 Shor 量子分解算法，并且在 2016 年发射了国际上第一颗量子卫星。

量子计算对于传统密码的理论威胁、量子计算机相关技术的高速发展、各国政府量子战略和政策的

启动和推进，无不让密码学专家学者感受到一种前所未有的紧迫感。如果真如一些专家预测 20 年内将出现实用大型量子计算机，抗量子计算密码的研究将刻不容缓。

2. 抗量子计算密码

由于对抗量子计算密码的迫切需求，2006 年，国际上致力于抗量子计算密码研究的学者在比利时召开了第一届国际抗量子密码学会议(PQCrypto 2006)，在这次会议上，各国学者提出了多种抗量子计算密码体制，其中以多变量公钥密码体制类居多，也提出了基于格的密码体制、基于纠错码的体制和基于 Hash 函数的签名方案。此后，在历届国际抗量子密码会议上都会有所改进、拓展和创新，初步形成了以多变量公钥密码体制、基于 Hash 函数的数字签名方案、基于编码的密码体制和基于格的密码为主的四大类抗量子密码体制。

一个多变量公钥密码系统由有限域上一组二次多项式作为它的公钥映射。它的主要安全假设为求解有限域上非线性方程组是 NP 困难问题。最早的多变量公钥密码体制是 Tsuii 和 Imai 提出的，20 世纪 80 年代起他们就已经开始这个领域的研究。早期的多变量公钥密码体制研究成果主要在日本，1988 年，Matsumoto 和 Imai 提出了第一个现代化形式的多变量公钥密码形式[4]。随后的 20 多年里，多变量公钥密码体制受到了专家们的广泛关注。美国辛辛那提大学的 Jintai Ding、日本的 Kohtaro Tadaki、台湾的 Bo-Yin Yang 等很多知名学者在多变量公钥密码领域展开研究，并在历届抗量子密码会议上发表了多篇文章。此外，我国学者管海明引入单向函数链的概念，提出了有理分式公钥密码系统[5]；张焕国、王后珍等引入了 Hash 函数的认证机制构造了扩展多变量公钥密码算法[6]。基于抗量子计算的优势，未来多变量公钥密码的研究将进入一个新的高度。

基于 Hash 函数的数字签名主要指 Merkle 签名方案。1978 年 Rabin 首次提出了一次签名方案，验证签名时需要与签名者进行交互。次年，Lamport 提出了一个更有效的一次签名方案，该方案并不需要与签名者进行交互；Diffie 对 Lamport 的方案进行了推广来提高其效率，因此，该方案成称为 Lamport-Diffie 一次签名方案。Ralph Merkle 从一次性签名方案开始，借鉴了 Lamport 和 Diffie 的工作，发明了 Merkle 数字签名方案[7]。Merkle 的思想是用 Hash 树将多个一次性验证密钥(Hash 树的叶子)的有效性降低到一个公钥(Hash 树的根)的有效性。他最初的构造与 RSA 等方案相比并不够有效，然而由于 Merkle 签名方案的安全性是基于 Hash 函数的抗强碰撞性，并且理论计算表明最先进的 Hash 函数能确保 Merkle 签名方案的高安全性级别，抵御量子计算的攻击，因此，Merkle 签名方案仍然受到了学者们的青睐。Michael Szydlo、Johannes Buchmann、Erik Dahmen、Michael Schneider 等一大批学者对 Merkle 的方案进行了改进。目前，基于 Hash 函数的签名是代替 RSA 和椭圆曲线最有前途的签名方案。

基于编码的密码体制算法核心是应用了一种纠错码 C，主要特征是编码时添加一定数量的错误码字或根据码 C 的检验矩阵计算伴随式。基于纠错码的第一个密码体制是 1978 年 McEliece 提出的公钥加密方案。该方案安全性高且加密运算快，但为了安全它的公钥规模和签名代价太大[8]。1986 年 Niederreiter 提出了背包型基于编码的公钥密码体制。Niederreiter 的密码体制是基于 GRS 码而不是 McEliece 体制使用的 Goppa 码。1994 年李元兴、王新梅等人证明了这两种公钥方案在安全性上是等价的[9]。由于这两种加密方案都不能用于数字签名，1990 年王新梅提出了第一个基于编码的数字签名方案——Xinmei 方案[10]。1991 年李元兴构造了一类同时具有签名、加密和纠错能力的公钥体制[11]。随后，人们对 McEliece 体制进行了一系列的改进，最重要的是 2001 年由 Kobara 和 Imai 提出的改进方案。在抗量子计算密码被推上研究前沿之后，Bhaskar Biswas、Nicolas Sendrier、Stefan Heyse、Daniel J. Bernstein 等诸多专家学者在抗量子会议上展示了他们对 McEliece 体制的改进方案。由于基于数论的公钥密码体制容易受到量子计算的攻击，基于编码的公钥密码体制已然成为基于数论的公钥密码体制的一个很好的替代。

基于格的密码体制基础是格上面的一些困难问题，如最短向量问题(SVP)、最近向量问题(CVP)、最小基问题(SBP)等。在量子计算飞速发展的时代背景下，学者们对格密码对抗量子计算寄予厚望。自 1996 年 Ajtai 首次在格难题基础上提出一个具有里程碑意义的密码体制后，格理论的相关研究不断取得突破，已经逐步成为抵抗量子计算攻击的公钥密码体制理论的核心研究内容。基于格的公钥密码算法以其安全性高和效率高的优势受到研究者的持续关注。1996 年 Hoffstein、Pipher 和 Silverman 提出了 NTRU (Number Theory Research Unit)公钥密码体制，该体制具有抗量子攻击、安全性强、运行速度快、密钥生成快、所需内存小等优势[12]。由于基于 NTRU 体制的数字签名方案并不理想，2000 年，Hoffstein 等人利用 NTRU 提出了 NSS 签名体制，随后在 2001 年和 2003 年对签名方案进行了改进。在 2006 年抗量子会议召开之后，几乎每届抗量子会议都会提出新的或改进的格密码方案。

3. 抗量子密码的最新进展

由于对抗量子计算密码的迫切需求，2006 年，国际上致力于抗量子计算密码研究的学者在比利时召开了第一届国际抗量子密码学会议(PQCrypto 2006)，在这次会议上，各国学者提出了多种抗量子计算密码体制，其中以多变量公钥密码体制类居多，也提出了基于格的密码体制、基于纠错码的体制和基于 Hash 函数的签名方案。此后，在历届国际抗量子密码会议上都会有所改进、拓展和创新，初步形成了以多变量公钥密码体制、基于 Hash 函数的数字签名方案、基于编码的密码体制和基于格的密码为主的四大类抗量子密码体制。

2006 年至今，国际抗量子密码会议分别在比利时、美国、德国、中国台湾、法国、加拿大、日本和荷兰陆续召开，这也直接导致了近十年来抗量子密码体制的飞跃式发展。从这八届国际抗量子密码年会可以看出，无论抗量子密码种类的增加，还是同一类抗量子密码的不断改进、优化、拓展直至成熟，都充分展示了抗量子密码的时代性和生命力。

从图 1 可以看出，在诸多的抗量子密码体制中，多变量公钥密码体制是当前抗量子密码领域研究的重点、热点，也是成果最多的密码体制，基于编码的密码体制仅次。图上还显示，在这四类之外的会议论文也占有一席之地，约 14%的比重，这些成分是什么？我们后面会对这一部分进行分解和阐述。

3.1. 多变量密码体制

作为抗量子密码的最早成员之一，多变量公钥密码体制成为历届国际抗量子密码会议的主力和宠儿，每届会议论文集中多变量公钥密码体制相关的文章都有相当多的数量，如图 2 所示。

早期的多变量密码体制主要集中于基本理论的拓展、已知方案的安全性评估和常见的针对多变量体制的攻击方法。Jacques Stern 通过对现行的多变量方案进行攻击来评估当前方案的安全性水平，结果也展示了这些方案并没有为量子时代的到来做好足够的准备[13]。Aline Gouget 和 Jacques Patarin 讨论了概率性的多变量密码，在此基础上创建了很多新的签名方案，并揭示了概率性多变量密码对签名方案安全性水平有很好的提升[14]。2006 年，Jintai Ding 等人在提出了一种新的基本陷门，并且证明了它比 MIA 陷门方案快得多[15]。Christopher Wolf 和 Bart Preneel 讨论了多变量二次系统的等价密钥，并且展示了这样一个结果：对于所有的基本类型的方案，如隐域方程(HFE)，不平衡油醋方案，阶梯三角方案等，通过采取合适的策略有可能做到减小私钥和公钥的密钥空间[16]。2008 年，Anna Inn-Tung Chen 等人在多变量密码体制实际规模的实例基础上，加入了自己的设计，证实了在面对已知最好的攻击时，这些实例也能保持方案本身的特性[17]。密码分析方面，2006 年，Jintai Ding、Chia-Hsin Owen Chen 等学者给出了高阶线性化方程攻击、Gröbner 解算机和庄子算法等针对多变量密码的攻击算法[18] [19] [20]。2008 年，Jintai Ding 等人开发了一种新的 2R 转化方法和一些其他的新技术，用以找出一种原来有理方程的二维等价方

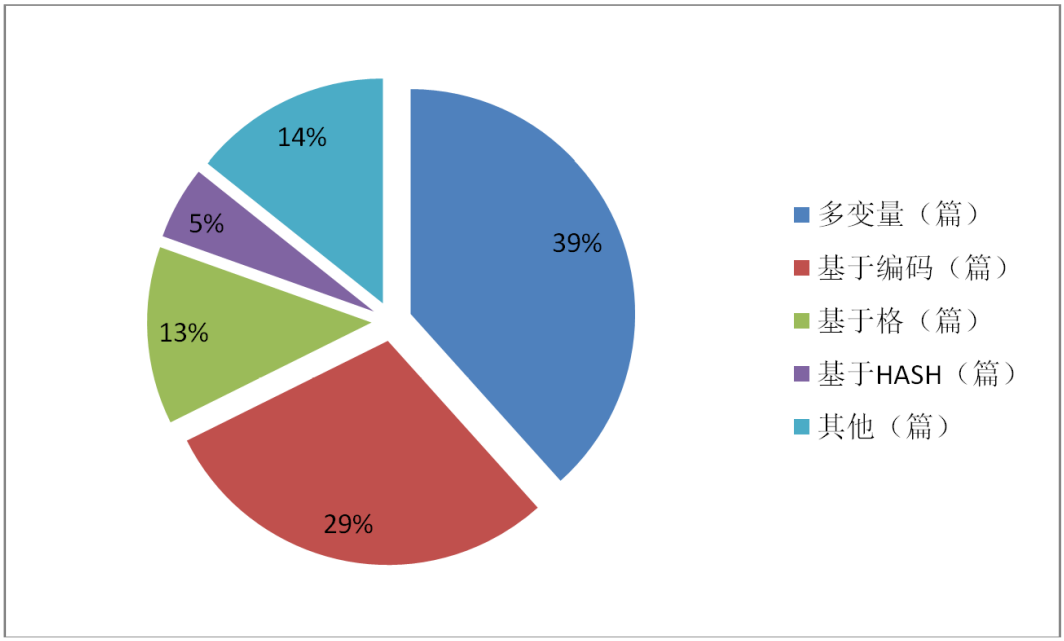

Figure 1. Distribution of different kinds of post quantum cryptography in all eight international conferences
图 1. 全八届国际抗量子会议各类抗量子密码体制分布

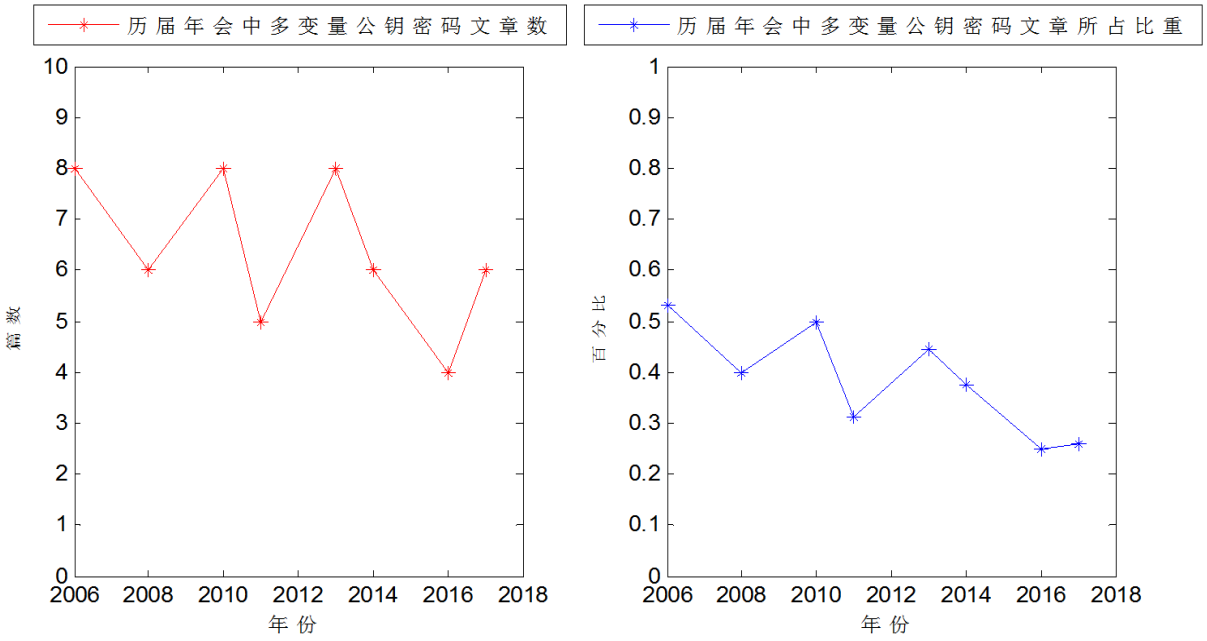

Figure 2. Papers of multivariate public key cryptography in annual conferences
图 2. 历届年会中多变量密码体制文章情况

程，从而彻底破坏多变量密码系统[21]。Mohamed Saied Emam Mohamed 等在 XL 与突变 XL 方法的基础上提出了 MXL2 的改进突变策略，并用该方法求解 GF(2)域上的多项式方程组，明显减小了矩阵的规模[22]。

2010 年以来，学者们对多变量公钥密码体制的研究持续深入，主要研究层面集中在三个方面：一是对基本理论的深入改进优化，包括加密、签名与分析；Crystal Lee Clough 等人对常规的平方加密机制进

行加法修正，提出了 Square+的构造设计[23]；Shigeo Tsujii 提出了一种新的基于 STS 陷门的数字签名方案，很好地解决了 STS 方案的脆弱性，并且在 Gröbner 基攻击和排名攻击保持很好的安全性水平[24]。Chen-Mou Cheng 等人提出了一种可以在多项式时间内解决多元二次方程(MQ)问题的扩展算法，并且通过与其他方案对比验证了算法的高效性[25]。二是对热点领域的重点攻关，比较有代表性的就是 HFE，仅仅最近五次国际抗量子密码会议就有 10 篇文章围绕 HFE 及其变种展开。比如 Taylor Daniels 等人对 HFE 密码系统的不同特性进行探究，并给出了该系统面对差分攻击时保持安全的参数集合[26]；Jaiberth Porras 等结合 HFE 和庄子算法提出了一种称为 ZHFE 的多变量公钥加密方案，展示了该方案在面对能威胁 HFE 方案的攻击面前是安全的[27]；Ray Perlner 对 Porras 设计的 ZHFE 进行了安全性分析并给出了修改方案，在保留其安全性和性能的基础上对其密钥尺寸进行了优化[28]；Albrecht Petzoldt 等提出了 HMFEv 签名方案，就存储和性能而言，该方案都比 HFE 族的其他方案更为有效[29]。三是进行全新的探索性尝试：Takanori Yasuda 等人利用二次型构造了一个签名方案，既能抵抗中心映射的攻击，同时与 Rainbow 方案相比，效率有 8~9 倍的提升[30]。

近些年多变量公钥密码体制的最新成果当然远远不止上面展示的这些，但通过这些成果足以看出后量子时代多变量公钥密码体制的地位和意义，它的发展值得我们关注和期待。

3.2. 基于 Hash 函数的密码体制

当Hash函数能抗强碰撞时，基于这样的Hash函数的数字签名能有效抵抗一直量子计算算法的攻击。因而，基于 Hash 函数的数字签名方案理所当然地成为学者们抵御量子计算威胁的重要武器。尽管不像多变量公钥密码体制那般火热，基于 Hash 函数的数字签名方案仍然成为人们不断去钻研、不断取得突破的课题。

图 3 展示了历届国际抗量子密码会议中基于 Hash 函数的密码文章数目，五届年会论文集中都有基于 Hash 函数的数字签名出现。基于 Hash 函数的数字签名方案的文章主要集中在对 Merkle 签名方案(MSS)的研究探讨。2006 年，Michael Szydlo 回顾了 Merkle 树的创建，聚焦于使得 Merkle 树创建更加有效和实用的最新进展。2008 年，Johannes Buchmann 提供了一种基于 Szydlo’s 算法的新算法来计算 Merkle 数字签名机制中的认证路径，并且实验证明了，与同类最好方法相比，他们的新算法大大减少了最坏情况的运行时间[31]。Erik Dahmen 等人对 Merkle 认证树提出了一种新的不再需要耐碰撞的 Hash 函数的结构，在所给的 Hash 函数抗二次原像时，由此产生的签名机制是不能伪造的，能产生更短的签名，并且能不被生日攻击和寻求碰撞算法的最新进展所影响[32]。2011 年 Johannes Buchmann 等人在 MSS 的基础上提出了一种称为 XMSS 的数字签名方案，指出了它的签名大小比已知最好的可证明安全的基于 Hash 函数的数字签名的签名大小减少了至少 25% [33]。

在 MSS 的钻研之外，2016 年，Ehsan Ebrahimi Targhi 等人研究了为一个函数寻找碰撞的量子查询复杂度问题，这种函数的输出选择时根据最小熵为 k 的分布，他们通过计算得出了量子查询复杂度至少为 $\Omega(2^{k/9})$的结论[34]。

尽管基于 Hash 函数的数字签名方案成果并不很多，但考虑到近些年研究带来的提升使之越发高效和实用，在量子时代山雨欲来的境况之下，学者们对于基于 Hash 函数的数字签名的前景充满信心。

3.3. 基于编码的密码体制

基于编码的密码体制也是近年来成果辈出的领域，McEliece 公钥密码体制及其改进版本等成为学者们最感兴趣的课题之一，各类基于编码的密码体制的安全性分析也成为近些年聚焦的热点。

图 4 展示了迄今为止 8 届国际抗量子密码年会中基于编码的密码体制的文章数。从图 4 可以看出，

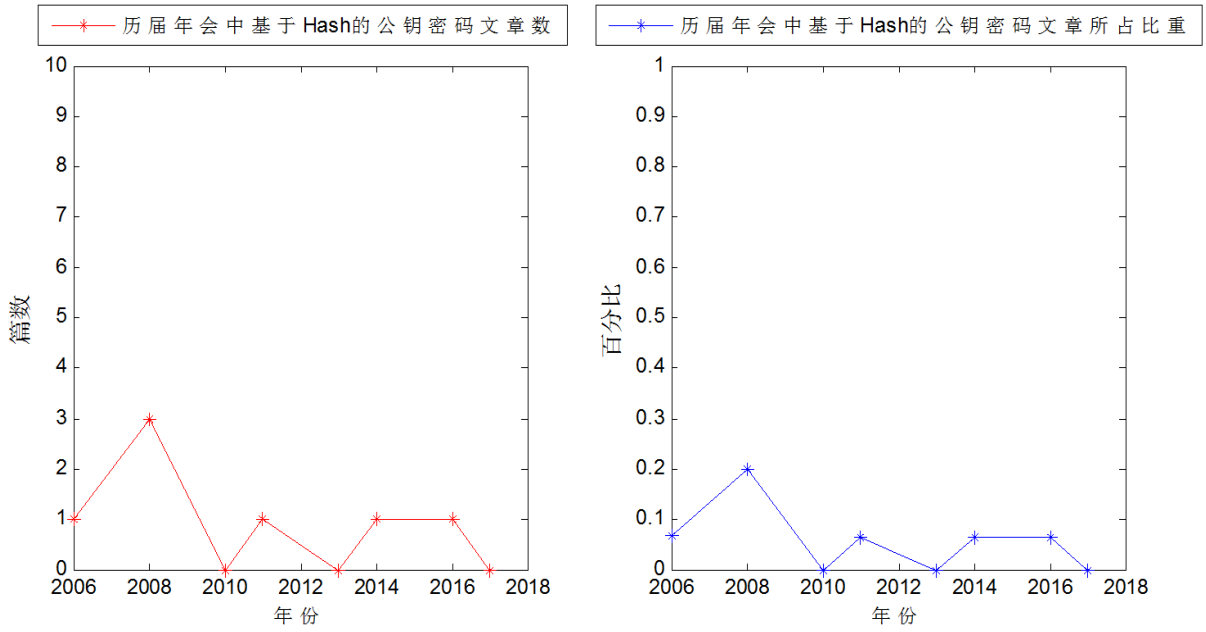

Figure 3. Papers of Hash-based digital signature in annual conferences
图 3. 历届年会中基于 Hash 函数的密码体制文章情况

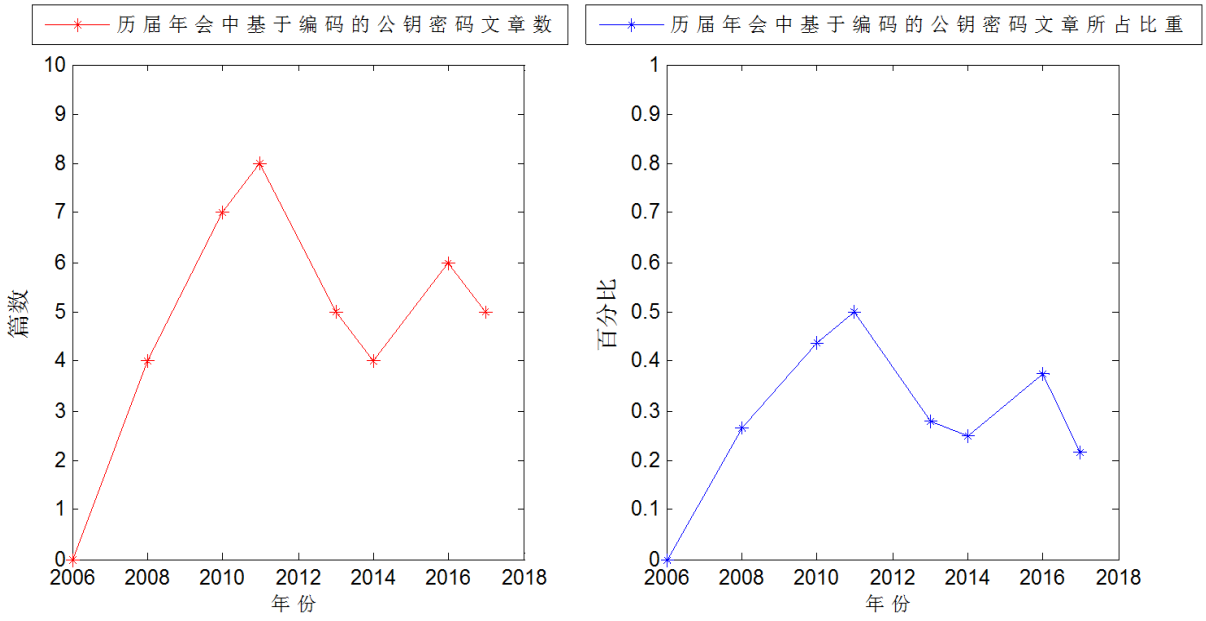

Figure 4. Papers of code-based cryptography in annual conferences
图 4. 历届年会中基于编码的密码体制文章情况

除了首届年会之外，之后每届抗量子密码年会都有至少 4 篇基于编码的密码体制的文章，充分展示了这一领域硕果累累。

基于编码的密码体制的文章绝大多数还是围绕着 McEliece 密码体制展开，其中既有 McEliece 密码方案的各类变种和修正，也有针对以 McEliece 密码体制为代表的基于编码的密码体制的多种攻击。密码体制方面，2008 年，Daniel J. Bernstein 等人提出了新的参数，使得 McEliece 和 Niederreiter 系统达到不被所有已知攻击攻破的安全水平，并且在满足同样安全条件下，使用新参数的系统公钥规模远小于使用之

前参数的系统[35]。Bhaskar Biswas 等人在他们的算法和参数选择基础上，提供了 McEliece 公钥加密机制的实施过程和完整描述，同时展示了密码分析的发展现状，并且证明了，与其他基于数论的公钥密码体制相比，他们的方案提速了至少 5~10 倍[36]。2011 年，Stefan Heyse 针对 McEliece 密码体制公钥大、非语义安全的缺点，提供了一个 McEliece 密码体制的实施方式——在嵌入式设备上实施，它在语义上是安全的，并同先前已发布的实现方案相比，它的公钥大小只有它们的 1/40，私钥大小只有它们的 1/5 [37]。攻击方面，信息集译码成为攻击基于编码的密码体制的主要手段。2010 年，Daniel J. Bernstein 通过实验展示了量子信息集译码比非量子信息集译码要快得多[38]。Christiane Peters 展示了 Stern 的信息集译码算法的一般化情形，用以解任意有限域上的线性编码和分析复杂度，这个结果使得计算最近提出的非二元域上的基于编码的系统的安全性成为可能[39]。Falko Strenzke 提出了一种新的针对 McEliece PKC 的时间攻击，它能利用 Patterson 算法的脆弱性使攻击者通过时间侧信道收集密钥交换的信息，从而显著地减少暴力攻击密钥所需要的时间[40]。Stefan Heyse 等人以 McEliece 方案在 8 bit 微处理器上的不同执行为基础，主要讨论了两种能量分析攻击，而这很可能是第一次对侧信道攻击进行实际评估[41]。2011 年，Nicolas Sendrier 考虑了攻击者可以利用很多密码系统但只能解码其中一个的情形，证明了如果攻击者能够获得无限数量的实例时，该攻击的复杂度将显著降低[42]。2013 年，Grćgory Landais 等人提出了一种对基于卷积码的 McEliece 密码变种的攻击，该攻击可以通过寻找公开码中的低重量码字成功攻击这种 McEliece 密码变种方案，解开卷积部分[43]。2016 年，Aurćlie Phesso 研究了 Baldi 等人提出的一种基于代码的签名方案，根据这个签名方案中一些比特的相关性提出了攻击方案，这种攻击方案能够恢复足够的基本密钥结构，从而伪造新的签名[44]。

除了对 McEliece 密码的探索，一些学者着眼于开辟新的基于编码的密码体制。2008 年，Carlos Aguilar Melchor 展示了从 Stern 的基于编码的认证机制到门限环签名的一般化过程，这种签名协议是第一个有效的基于编码的签名方案和第一个基于编码的门限环签名方案[45]。2011 年，Paulo S.L.M. Barreto 等人介绍了一种拟 monoidic 码，这种代码具有特殊的纠错能力，并且展示了基于这种代码的加密和签名方案如何实例化，同时给出了一些初步的参数[46]。2014 年，Philippe Gaborit 等人提出了一种称为 RankSign 的新的基于代码的数字签名方案，并且展示了如何使签名的不可伪造性归约为对公开矩阵的直接攻击，进而说明了这种签名方案没有信息泄露[47]。

基于编码的密码体制研究已经在不断深入，并将继续吸引着密码学专家们的广泛关注。随着其密钥尺寸的逐渐降低，加之其高安全性和高效率的优势，基于编码的密码体制势必在后量子时代大放异彩。

3.4. 基于格的密码体制

基于格的密码体制被广泛认为是量子计算最难攻破的密码。随着抗量子计算密码研究的不断深入，基于格的密码近年来也取得了飞速的发展和喜人的成果。

图 5 展示了八届国际抗量子密码会议中格密码的文章数量，可以看出，历届年会中都有关于格密码的文章，自 2013 年起格密码的研究成果明显增加。对于格密码的研究也呈现出几个特点：其一，基于格的加密和签名方案一直都是研究的重中之重，而且取得了相当不错的成果。2006 年，Jeff Hoffstein 等人回顾了 NTRU 加密和签名的算法，讨论了格密码算法的安全性现状，认为随着格密码算法和认证方面的不断进步，格密码势必会被学术界广泛接受和认可[48]。2008 年，Johannes Buchmann 等人在 Ajtai 的著名结果基础上，提出了一种维数增长的格基序列，这个格基序列有望成为 SVP 的困难实例，可以用来衡量格基规约算法[49]。2010 年，Markus Rückert 提出了“bonsai 树”标准签名方案的一个变种，这种变种拥有标准方案相同的效率，但又支持更强的强不可伪造性的概念，并且提供了标准模型中第一个没有树的数字签名方案以支持后量子时代的强不可伪造性[50]。2013 年，Slim Bettaieb 等人对 Cayrel 等人

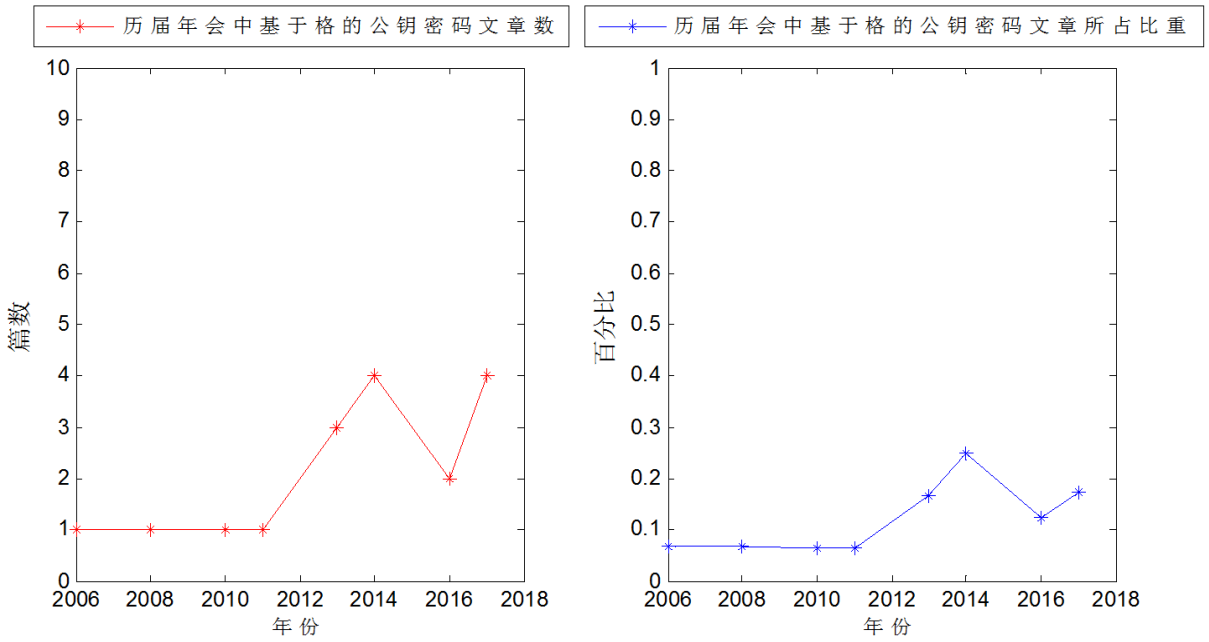

Figure 5. Papers of lattice-based cryptography in annual conferences
图 5. 历届年会中基于格的密码体制文章情况

的基于格上的门限环签名方案进行改进，将 CLRS 方案进行推广从而得到一个更有效的门限环签名方案，该方案在保持安全性的前提下减小了签名的规模，是当时最有效的基于格的环签名方案和门限签名方案[51]。2017 年，Charles Bouillaguet 等人回顾了前人提出的环上带舍入的子集积(SPRING)被用作伪随机数生成器时的安全性和有效性，在此基础上提出了一个新的变种，这种变种与在计数模式中与没有硬件加速的 AES 相比也有竞争力，并且通过执行证明了该变种高端台式电脑上有很好的性能[52]。其二，对于格密码的攻击方案的研究越来越受关注。2013 年，Thijs Laarhoven 等人通过将 Grover 量子搜索算法应用到 Micciancio 等人的格算法中，得到了改进的可解决最短向量问题的渐近量子结果，证明了利用量子计算机可以在 $2^{1.799n+o(n)}$ 时间内发现最短向量[53]。2017 年，Boru Gong 等人提出了一种针对 2015 年欧密会上提出的认证密钥交换方案中的其中一个变种 Π_1 的有效攻击，这种攻击利用环的代数结构进行攻击，而受害者一方很难发现这种攻击[54]。Florian Göpfert 等人提出了一种新的基于误差学习问题(LWE)的量子攻击，分析了这种攻击的运行时间复杂度，并且在所有可能的攻击参数选择下对它进行了优化，并且展示了他们的量子混合攻击较大地优于或至少与 Albrecht 等人在 2015 年展示的所有其他的攻击相当[55]。

不断增加的基于格的密码体制研究成果已经充分展示了这一领域所受到的关注，尽管格密码仍然处于发展阶段，但其强安全性基础仍然让业界对它充满兴趣和期待。

3.5. 其他抗量子密码体制

图 1 中显示，除了上面提到的四大类抗量子密码体制之外，还有 14%的文章不在此列。这里除了一些量子计算算法的文章外，还有一些其他的抗量子密码体制，主要就是量子密码和基于同源的密码体制。海森堡测不准原理及单量子不可复制定理保证了量子密码理论上的绝对安全，Elham Kashefi 等人提出的量子单向函数的候选[56]、Michele Mosca 等人讨论的经典认证密钥交换框架下量子密钥分配[57]等成果都充分展示了量子密码在后量子时代仍然扮演着重要的角色。基于同源的密码体制则是抗量子密码的新成员，David Jao 等人在椭圆曲线同源基础上提出了一个不可否认签名方案，并证明了在没有已知有效的量子算法的情况下，这类方案在一定合理的数论计算假设下是安全的[58]。Alexandre Gélin 等人和 Yan Bo

Ti 分别对超奇异同源密码系统的循环终止故障攻击和第一类故障攻击进行了讨论[59] [60]。

尽管目前主流的抗量子密码体制还是多变量公钥密码、基于 Hash 的密码、基于编码的密码和基于格的密码，但毫无疑问随着抗量子密码体制的深入研究，如基于同源的密码体制一样，新的抗量子密码体制一定会越来越多地登上后量子时代的舞台。

4. 研究展望

在量子时代不断向我们趋近的今天，量子计算已经不断侵蚀着曾经无数牢不可破的安全防线，对几乎所有涉及信息安全的领域构成了巨大的威胁。幸运的是，学者们在量子时代到来之前，已经前瞻性地展开了对抗量子密码体制的研究，并且已经取得了十分丰硕的成果。学术界不仅在多变量公钥密码、基于 Hash 函数的密码、基于编码的密码和基于格的密码方面不断取得突破，也在不断地开发新的抗量子密码体制，更为喜人的是，抗量子密码体制的标准化工作已经在如火如荼地开展。这些都让我们有足够的信心和理由相信，我们能够从容地面对量子时代的到来。

参考文献 (References)

[1] Shor, P.W. (1999) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Siam Review*, **41**, 303-332. https://doi.org/10.1137/S0036144598347011

[2] Chen, L., Liu, Y.-K., Jordan, S., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016) Report on Post-Quantum Cryptography. NISTIR 8105, Draft. https://doi.org/10.6028/NIST.IR.8105

[3] Bernstein, D.J., Buchmann, J. 抗量子计算密码[M]. 北京: 清华大学出版社, 2015.

[4] Matsumoto, T. and Imai, H. (1988) Public Quadratic Polynomial-Tuples for Efficient Signature Verification and Message-Encryption. *Advances in Cryptology—EUROCRYPT*'1988, 419-545.

[5] 管海明. 有理分式公钥密码体制[C]//第五届中国信息和通信安全学术会议论文集, 2007.

[6] 王后珍, 张焕国, 王张宜, 等. 一类具有安全加密功能的扩展 MQ 公钥密码体制[J]. 中国科学: 信息科学, 2011, 41(11): 1297-1309.

[7] Merkle, R.C. (1989) A Certified Digital Signature. *Advances in Cryptology—CRYPTO*'89 *Proceedings*, LNCS 435, Springer, Berlin, 218-238.

[8] Mceliece, R J. (1978) A Public-Key Cryptosystem Based on Algebraic Coding Theory. *Deep Space Network Progress Report*, 114-116.

[9] 王新梅, 李元兴. McEliece 公钥体制的修正[J]. 电子学报, 1994(4): 90-92.

[10] Xinmei, W. (1990) Digital Signature Scheme Based on Error-Correcting Codes. *Electronics Letters*, **26**, 898-899. https://doi.org/10.1049/el:19900586

[11] 李元兴, 成坚, 王新梅. 一种基于代数编码理论的签名, 加密和纠错公钥体制[J]. 电子与信息学报, 1991, 13(4): 359-364.

[12] Hoffstein, J., Pipher, J. and Silverman, J.H. (1996) NTRU: A High Speed Public Key Cryptosystem. PrePrint Presented at He Hump Session of Euro Crypt 96.

[13] Stern, J. (2006) Post-Quantum Multivariate-Quadratic Public Key Schemes. In: *International Workshop on Post-Quantum Cryptography*, Springer-Verlag, 25-26.

[14] Gouget, A. and Patarin, J. (2006) Probabilistic Multivariate Cryptography. In: *International Conference on Cryptology in Vietnam*. Springer-Verlag, 1-18.

[15] Ding, J., Wolf, C. and Yang, B.Y. (2007) Invertible Cycles for Multivariate Quadratic (MQ) Public Key Cryptography. In: *International Conference on Practice and Theory in Public-Key Cryptography*, Springer-Verlag, 266-281.

[16] Wolf, C. and Preneel, B. (2011) Equivalent Keys in Multivariate Quadratic Public Key Systems. *Journal of Mathematical Cryptology*, **2005**, 375-415.

[17] Chen, I.T., Chen, C.H.O., Chen, M.S., *et al*. (2008) Practical-Sized Instances of Multivariate PKCs: Rainbow, TTS, and ℓIC-Derivatives. In: *Post-Quantum Cryptography*, Springer Berlin Heidelberg, 95-108.

[18] Ding, J., Hu, L., Nie, X., *et al*. (2007) High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems. In: *International Workshop on Public Key Cryptography*, Springer, Berlin, Heidelberg, 233-248.

[19] Chia-Hsin, C., Bo-Yin, Y. and Jiun-Ming, C. (2006) The Limit of XL Implemented with Sparse Matrices. In: *International Conference on Cryptology in Vietnam*, Springer-Verlag, 215-225.

[20] Ding, J., Gower, J.E. and Schmidt, D. (2006) Zhuang-Zi: A New Algorithm for Solving Multivariate Polynomial Equations over a Finite Field. Iacr Cryptology Eprint Archive.

[21] Ding, J. and Wagner, J. (2007) Cryptanalysis of Rational Multivariate Public Key Cryptosystems. Vol. 5299, 124-136.

[22] Mohamed, M.S.E., Mohamed, W.S.A.E., Ding, J., *et al*. (2008) MXL2: Solving Polynomial Equations over GF(2) using an Improved Mutant Strategy. In: *Post-Quantum Cryptography*, Springer Berlin Heidelberg, 203-215.

[23] Clough, C.L. and Ding, J. (2010) Secure Variants of the Square Encryption Scheme. In: *International Conference on Post-Quantum Cryptography*, Springer-Verlag, 153-164.

[24] Tsujii, S., Gotaishi, M., Tadaki, K., *et al*. (2010) Proposal of a Signature Scheme Based on STS Trapdoor. In: *Post-Quantum Cryptography*, Springer Berlin Heidelberg, 201-217. https://doi.org/10.1007/978-3-642-12929-2_15

[25] Cheng, C.M., Hashimoto, Y., Miura, H., *et al*. (2014) A Polynomial-Time Algorithm for Solving a Class of Underdetermined Multivariate Quadratic Equations over Fields of Odd Characteristics. In: *Post-Quantum Cryptography*, Springer International Publishing, 40-58.

[26] Daniels, T. and Smith-Tone, D. (2014) Differential Properties of the HFE Cryptosystem. In: *Post-Quantum Cryptography*, Springer International Publishing, 59-75.

[27] Porras, J., Baena, J. and Ding, J. (2014) ZHFE, a New Multivariate Public Key Encryption Scheme. In: *Post-Quantum Cryptography*, 229-245. https://doi.org/10.1007/978-3-319-11659-4_14

[28] Perlner, R. and Smith-Tone, D. (2016) Security Analysis and Key Modification for ZHFE. In: *Post-Quantum Cryptography*, Springer International Publishing.

[29] Petzoldt, A., Chen, M.S., Ding, J., *et al*. (2017) HMFEv—An Efficient Multivariate Signature Scheme. In: *Post-Quantum Cryptography*. https://doi.org/10.1007/978-3-319-59879-6_12

[30] Yasuda, T., Takagi, T. and Sakurai, K. (2013) Multivariate Signature Scheme using Quadratic Forms. In: *Post-Quantum Cryptography*, Springer Berlin Heidelberg, 243-258. https://doi.org/10.1007/978-3-642-38616-9_17

[31] Buchmann, J., Dahmen, E. and Schneider, M. (2008) Merkle Tree Traversal Revisited. 2*nd International Workshop on Post-Quantum Cryptography*, Cincinnati, 17-19 October 2008, 63-78.

[32] Dahmen, E., Takagi, T., Takagi, T., *et al*. (2008) Digital Signatures Out of Second-Preimage Resistant Hash Functions. *International Workshop on Post-Quantum Cryptography*, Springer-Verlag, 109-123.

[33] Buchmann, J., Dahmen, E. and Hülsing, A. (2011) XMSS—A Practical forward Secure Signature Scheme Based on Minimal Security Assumptions. *Post-Quantum Cryptography*, Taipei, 29 November-2 December 2011, 17-129.

[34] Targhi, E.E., Tabia, G.N. and Unruh, D. (2016) Quantum Collision-Resistance of Non-Uniformly Distributed Functions. In: *International Workshop on Post-Quantum Cryptography*, Springer-Verlag, New York, 79-85.

[35] Bernstein, D.J., Lange, T. and Peters, C. (2008) Attacking and Defending the McEliece Cryptosystem. In: *Post-Quantum Cryptography*, Springer Berlin Heidelberg, 31-46. https://doi.org/10.1007/978-3-540-88403-3_3

[36] Biswas, B. and Sendrier, N. (2008) McEliece Cryptosystem Implementation: Theory and Practice. In: *International Workshop on Post-Quantum Cryptography*, Springer-Verlag, 47-62.

[37] Heyse, S. (2011) Implementation of McEliece Based on Quasi-Dyadic Goppa Codes for Embedded Devices. *International Workshop Post-Quantum Cryptography*, Taipei, 29 November-2 December 2011, 143-162.

[38] Bernstein, D.J. (2010) Grover vs. McEliece. In: *International Conference on Post-Quantum Cryptography*, Springer-Verlag, 73-80.

[39] Peters, C. (2002) Information-Set Decoding for Linear Codes over F, q. Introduction to Statistics for the Behavioral Sciences. Saunders, 3759-3763.

[40] Strenzke, F. (2010) A Timing Attack against the Secret Permutation in the McEliece PKC. Vol. 6061, 95-107.

[41] Heyse, S., Moradi, A. and Paar, C. (2010) Practical Power Analysis Attacks on Software Implementations of McEliece. In: 3*rd International Workshop Post-Quantum Cryptography*, Darmstadt, 25-28 May 2010, 108-125.

[42] Sendrier, N. (2011) Decoding One Out of Many.

[43] Landais, G. and Tillich, J.P. (2013) An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes. In: *International Workshop on Post-Quantum Cryptography*, Springer Berlin Heidelberg, 102-117.

[44] Phesso, A. and Tillich, J.P. (2016) An Efficient Attack on a Code-Based Signature Scheme. In: *Post-Quantum Cryptography*, Springer International Publishing.

[45] Aguilar Melchor, C., Cayrel, P., Gaborit, P., *et al*. (2008) A New Efficient Threshold Ring Signature Scheme Based on Coding Theory. In: *International Workshop on Post-Quantum Cryptography*, Springer Berlin Heidelberg, 1-16.

[46] Barreto, P.S.L.M., Lindner, R. and Misoczki, R. (2011) Monoidic Codes in Cryptography. In: *International Conference on Post-Quantum Cryptography*, Springer-Verlag, 179-199.

[47] Gaborit, P., Ruatta, O., Schrek, J., *et al*. (2014) Rank Sign: An Efficient Signature Algorithm Based on the Rank Metric. Vol. 8772, 88-107.

[48] Hoffstein, J., Howgrave-Graham, N., Pipher, J., *et al*. (2006) NTRUEncrypt and NTRUSign: Efficient Public Key Algorithms for a Post-Quantum World. *Proceedings of the International Workshop on Post-Quantum Cryptography*, 71-77.

[49] Buchmann, J., Lindner, R. and Rückert, M. (2008) Explicit Hard Instances of the Shortest Vector Problem. In: *International Workshop on Post-Quantum Cryptography*, Springer-Verlag, 79-94.

[50] Rückert, M. (2010) Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles. In: *Post-Quantum Cryptography*, Springer Berlin Heidelberg, 182-200. https://doi.org/10.1007/978-3-642-12929-2_14

[51] Bettaieb, S. and Schrek, J. (2013) Improved Lattice-Based Threshold Ring Signature Scheme. In: *International Workshop on Post-Quantum Cryptography*, Springer Berlin Heidelberg, 34-51.

[52] Bouillaguet, C., Delaplace, C., Fouque, P.A., *et al*. (2017) Fast Lattice-Based Encryption: Stretching Spring. In: *Post-Quantum Cryptography*.

[53] Laarhoven, T., Mosca, M. and Pol, J.V.D. (2013) Solving the Shortest Vector Problem in Lattices Faster using Quantum Search. In: *International Workshop on Post-Quantum Cryptography*, Springer, Berlin, Heidelberg, 83-101.

[54] Gong, B. and Zhao, Y. (2017) Cryptanalysis of RLWE-Based One-Pass Authenticated Key Exchange. In: *International Workshop on Post-Quantum Cryptography*, Springer, Cham, 163-183.

[55] Göpfert, F., Vredendaal, C.V. and Wunderer, T. (2017) A Hybrid Lattice Basis Reduction and Quantum Search Attack on LWE. In: *International Workshop on Post-Quantum Cryptography*, Springer, Cham, 184-202.

[56] Kashefia, E. and Kerenidisc, I. (2012) Statistical Zero Knowledge and Quantum One-Way Functions. *Theoretical Computer Science*, **378**, 101-116. https://doi.org/10.1016/j.tcs.2007.03.013

[57] Mosca, M., Stebila, D. and Ustaoğlu, B. (2012) Quantum Key Distribution in the Classical Authenticated Key Exchange Framework. *International Journal of Urban & Regional Research*, **7932**, 136-154.

[58] Jao, D. and Soukharev, V. (2014) Isogeny-Based Quantum-Resistant Undeniable Signatures. In: *Post-Quantum Cryptography*, Springer International Publishing, 160-179.

[59] Gélin, A. and Wesolowski, B. (2017) Loop-Abort Faults on Supersingular Isogeny Cryptosystems. In: *Post-Quantum Cryptography*. https://doi.org/10.1007/978-3-319-59879-6_6

[60] Yan, B.T. (2017) Fault Attack on Supersingular Isogeny Cryptosystems. In: *International Workshop on Post-Quantum Cryptography*, Springer, Cham, 107-122.