浅谈后量子公钥密码的发展

● 李益发[1]　索敏杰[1]　姜　放[2]

[1]解放军信息工程大学　[2]国家保密科学技术研究所

【摘要】本文简要介绍了近年来后量子密码的发展状况，包括基于纠错编码、基于格、基于hash等多种方式的抗量子公钥体制，重点介绍了基于多变量二次多项式的公钥密码算法的进展。

【关键词】量子计算；后量子密码；QPKC

1 引言

熟知，密码体制是保护信息系统安全的核心技术。密码体制通常分为对称密码与非对称密码（也称公钥密码）。而公钥密码体制有其独特的优势。目前几乎所有的信息安全系统，都使用了公钥密码体制，其中绝大部分使用了RSA、ElGamal和ECC等几个最为著名的公钥体制，以实现密钥交换、数字签名和身份认证等。

然而，基于量子计算机的特殊计算能力，Shor等人给出了模幂运算的量子求阶算法，即著名的Shor算法[1]，依赖于合适的能用量子计算机实现的量子傅立叶变换，可成功解决大数分解和离散对数等困难问题，而这些问题是几大著名公钥体制——RSA、ElGamal[2]和ECC[3、4]的理论基础。这意味着，量子计算机可以对这几大著名的公钥体制形成致命的攻击。换言之，一旦量子计算机付诸应用，所有使用RSA、ElGamal或ECC算法的信息安全系统都将面临崩溃。另外，Grover等也给出了Grover量子搜索算法，可以将对密钥空间的搜索效率极大的提高，达到“指数减半”的效果。比如，用Grover量子搜索算法对128位密钥（密钥空间为2^{128}）的AES算法进行密钥搜索，则其效果可使得密钥空间缩小到64位（即密钥空间为2^{64}），接近DES的水平。这对于对称算法也形成了有力的攻击。而对量子计算机的一般估计是，10~15年时间即可投入应用。但最近公布的结果表明，美国目前已经成功研制了128位的量子存贮器，这已经接近实用水平。而其所用的“贴磁砖”的方法，可能极易用于研制更高位的量子存贮器。这表明，也许不到十年，实用的量子计算机就会问世。因此，构造能够抵抗量子计算机攻击的密码算法，成了近年来密码学领域的一个研究热点。一般，把这类能够抵抗量子计算机攻击的密码算法称为后量子（Post-Quantum）密码[5]或抗量子（计算的）密码。

尽管Grover量子搜索算法对于对称算法的安全性有一定的影响，但并不是致命的，因为适当增加密钥的长度，仍能抵抗量子计算机的攻击。但对上述几大著名公钥算法的攻击则是致命的。因此，后量子公钥算法的研究显得尤为重要和迫切。

2 后量子公钥密码算法概述

抵抗量子计算攻击的公钥密码，可以依据计算环境分为两大类，一类基于量子计算和量子通信环境，属于量子密码。量子密码的优势在于确能抗量子计算机的攻击，安全性很高，但建立量子密码系统需要昂贵的量子信道，在量子通信尚未普及的时候，应用范围受到极大限制，所以至少在量子通信问题解决之前并不能大范围适用。

另一类基于经典计算（即非量子计算）环境，属于经典抗量子密码。通常，当人们说到后量子公钥密码时，更多的是指这一类密码。

除量子公钥密码外，后量子公钥密码都是基于不能转换成离散傅立叶变换的数学难题而建立，主要有以下几种类型。

（1）基于hash算法构造的Merkle型签名算法

基于hash算法构造的签名体制，最经典的是Merkle hash树签名体制[6]，由传统的hash函数和任意的一次性签名算法，共同构造出一个完全二叉树来实现数字签名。由于该体制不依赖于大整数分解和离散对数等难解问题，所以被认为可以抵抗量子密码分析。尽管Merkle hash树签名体制在签名效率方面具有RSA等签名体制不可比拟的优势，但因为签名数量和签名大小的限制，Merkle hash树数字签名并没有得到很好的应用。事实上，这类签名都是一次性签名（一次一密），况且不能用于公钥加密，也无法实现原有系统中的许多密钥交换功能，因而难以在开放环境下大量使用。

（2）基于编码的公钥算法

基于编码理论构造的公钥体制，其理论基础是解码问题的困难性，即仅在已知生成矩阵的情况下，在码空间中寻找一个码字与已知码的Hamming距离最短。如果已知码为0，则问题就是最小权重问题。Berlekamp、McEliece和Tilborg证明，最小权重问题是NP-完全问题[7]。McEliece于1978年提出了基于Goppa码（一种代数编码）的加密算法[8]，但该算法的密钥空间太大，不能用于数字签名，且安全性近年来也一直受到挑战，2008年荷兰的研究人员就宣称，已经能成功破译该算法。尽管对该算法的改进可以用于数字签名，但总的来说，基于编码理论的许多签名算法的安全性一直受到质疑（许多签名算法相继被破译）。到目前为止，尚具有较好安全性的基于编码理论的公钥签名体制只有由Courtois等人提出的CFS签名体制[9]。

（3）基于格的公钥算法

基于格的公钥密码是指在大维数的格上，基于最短向量问题（SVP）和最近向量问题（CVP）等数学难题而构造的公钥密码体制。SVP是指在大维数格中寻找长度最短的非零向量，而CVP是指在大维数格中寻找和固定向量距离最短的向量，这两个问题都是NP难问题。比较著名的有Goldreich、Goldwasser和Halevi在1996年提出的GGH密码体制[10]，Ajtai和Dwork在1996年提出的Ajtai-Dwork密码体制[11]等，但最有代表性的算法是由美国数学家Hoffstein、Pipher和Silverman于1996年提出，并在以后作了修改的NTRU公钥密码系统[12]，它既可用于加密，也可用于签名。基于格上的难解问题设计的公钥加密算法，由于没有大整数的运算，运算速度和RSA相比要快得多。更重要的是，目前还没有针对基于格中密码体制的量子算法。目前NTRU算法由NTRU公司（资本雄厚且有美国政府支持）拥有，其理论和工程指标都日趋成熟。NTRU公司不仅在多国注册了NTRU算法的基础性专利，还开发了一系列示范性产品（IC卡、手机、3G、无线互联网、电子商务、可信计算等），并试图就该算法建立相应的国际标准。不过，由于算法的安全性还没有获得充分认可，特别是其签名的安全性远低于加密的安全性，不太适用于建立网络信任体系，加之知识产权的障碍，所以该算法并没有得到广泛应用。

（4）基于多变量的公钥算法

多变量公钥密码体制（Multivariate-quadratic-polynomials Public Key Cryptosystem，简称MQ或MPKC）是一大类各具特色的公钥密码算法的统称，也是近年来后量子公钥密码的研究热点。这类体制主要基于有限域上的多元二次多项式方程组的难解性。与RSA、DH、ECC相比，多变量公钥密码的安全性很难被证明等价于一个已知的可简单表述的数学难题，因而也被认为是很难找到相应量子攻击算法的难题，从而被看成具有抗量子计算的性能。最早提出的多变量密码体制是在1988年，但因其很快就被攻破，并且很多变型也没有达到安全的标准，使得这个体制一直不受重视。直到2000年以后，

出于抗量子算法攻击的考虑，对多变量的研究才重新受到重视。

1988年Matsumoto和Imai提出了著名的MI[13]密码体制，这是多变量公钥密码史上的一个里程碑。在随后的20多年里，许多密码学家在该领域做了很多出色的工作，提出了多种多变量公钥体制及其变型，其中最著名的体制类型有隐域方程（HFE）[14]、不平衡油醋（UOV）[15]、三角体制[16]等，变型方法有减、加[17]、子域[18]、分支[19]、醋变量[15]、内部扰动[20、21]以及固定、隐藏[22、23]等方法。然而很多方法都因为安全性或代价因素被否定，只保留了少数几种，比较著名的加密体制有PMI+、HFEv、彩虹体制等。在对MPKC的研究中，以丁津泰、杨柏因、王立中等年轻数学家为主体的中国人也做了很多出色的工作。

值得一提的是，除了上述几种公钥算法外，国内也由管海明、张焕国等在多变量体制的基础上自主提出了基于有理分式的公钥算法。

3 后量子公钥密码研究新的特点

目前，国际上关于后量子公钥密码的研究趋势有以下几个明显的特点。

一是研究步伐逐步加快。这从近几年召开的后量子密码会议可见一斑。2006年，在比利时的Leuven召开了第一届国际后量子密码学会议，2008年在美国的Cincinnati召开了第二届，2010年在德国的Darmstadt召开了第三届，基本上是两年一届。但今年，将在中国台北召开第四届，且以后将每年一届，时间节奏明显加快。

二是更加注重相关基础研究。例如对近年提出的后量子算法的数学理论基础有了更多的探讨，加强了对算法的安全性分析，对与抗量子性能相关的量子复杂性理论的研究也越来越多。

三是更加注重算法的有效性与可用性。因为可实用的量子计算机的问世已越来越迫近，可用性与效率都是无法回避的问题。

四是各国政府的支持力度也越来越大。表面上看，后量子密码的研究属于学术领域，但背后往往有政府的参与，因为这是涉及未来若干年国家安全的重大学术问题。BMS

参考文献：

[1] Rivest R,Shamir A, Adelman L.A method for obtaining digital signatures and public-key cryptosystems[C].Communications of the ACM,February 1978,21(02):120-126.

[2] ElGamal T.A public key cryptosystem and a signature scheme based on discrete logarithms[C]. IEEE Transactions on Information Theory, 31(1985): 469-472.

[3] Koblitz N.A course in number theory and cryptography[C].Springer-Verlag New York, Inc.,New York, NY, 1987.

[4] Miller V S.Use of elliptic curves in cryptography[C]. LNCS218 on Advances in cryptology(CRYPTO'85). Santa Barbara,California,United States,June 986:417-426.

[5] Bernstein D J.Post-quantum cryptography[M]. Springer Verlag,2009.

[6] Merkle R C.Secrecy,authentication,and public key systems[M].UMI Research Press,1982.

[7] Berlekamp E R, McEliece R J,van Tilborg HCA. On the inherent intractability of certain coding problems[C].IEEE Trans.Information Theory IT-24,1978,24(03):384-386

[8] McEliece R J.A public-key system based on algebraic coding theory[R].DSN Progress Reprot 42～44.JPL,Pasadena,1978:114-116.

[9] Courtois N,Finiasz M, Sendrier N.How to achieve a McEliece-based digital signature scheme[C]. Advances in Cryptology - ASIACRYPT,LNCS2248. Springer-Verlag,2001:157-174.

[10] Goldreich O,Goldwasser S,Halevi S.Public-key cryptosystems from lattice reduction problems[C]. Advances in Cryptology－CRYPTO'97, LNCS1294. Springer-Verlag,1997: 112-131.

[11] Ajtai M,Dwork C.A public-key cryptosystem with worst-case/ average-case equivalence[C]. Proc.of 29th Annual ACM Symposium on Theory of Computing (STOC'97).ACM Press,1997:284-293

[12] Hoffstein J， Pipher J， Silverrnan J H.NTRU: a ring based public key cryptosystem[C].Proc.

of ANTS III, First presented at the rump session of Crypto'96.LNCS 1423.Springer-Verlag, 1998:267-288.
[13] Imai H,Matsumoto T.Algebraic methods for constructing asymmetric cryptosystems[C]. Algebraic Algorithms and Error-Correcting Codes,3rd International Conference,LNCS 229. Springer, 1985:108～119.
[14] Partarin J. Hidden fields equations(HFE) and isomorphisms of polynomials(IP):tow new families of asymmetrc algorithms[C].Advances in Cryptology-Eurocrypt 96.Berlin:Springer-Verlag, 1996:33-48.
[15] Kipnis,A,Patarin J,Goubin L.Unbalanced oil and vinegar signature schemes[C].Advances in Cryptology -EUROCRYPT '99.LNCS1592. Springer 1999:206-222.
[16] Shamir A.Efficient signature schemes based on birational permutations[C].Proceeding CRYPTO '93 Proceedings of the 13th annual international cryptology conference on Advances in cryptology. Springer 1993:1-12.
[17] Patarin,J.Asymmetric Cryptography With a Hidden Monomial[C]. Advances in Cryptology-Crypt 96.Berlin:Springer-Verlag,1996:45-60
[18] Sidorenko A V,Gabidulin E M.The weak keys for HFE[C].Proceedings of the 7th International Symposium onCommunication Theory and Applications.2003:239－244.
[19] Felke,P.On the affine transformations of HFE-cryptosystems and systems with branches[C]. Coding and Cryptography:LNCS 3969.Springer 2006:229-241.
[20] Ding,J.A new variant of the Matsumoto-Imai cryptosystem through perturbation[C].Public Key Cryptography(CPKC'04):305-318.
[21] Ding J, Schmidt D.Cryptanalysis of HFEv and internal perturbation of HFE[C].Public Key Cryptography(CPKC’05):288-301.
[22] Courtois,N.The security of hidden field equations (HFE) [C].Topics in Cryptology CT-RSA 2001:266-281.
[23] Wolf C.Hidden field equations (HFE)-variations and attacks [D].Diplom thesis,Universit t Ulm,2002.

（上接第 44 页）

6 管理体系应能够自我改进

涉密信息系统的安全保密管理不是一成不变的，而是随着技术的发展、网络结构的变化、用户的增减、人员安全保密认识的不断深入等情况动态变化的。涉密信息系统的安全保密管理体系只有具备了随着来自内部或外部的变化，不断自我适应、自我完善的能力，才能实现保护国家秘密这一最终目标。国家保密标准中也指出要通过分析异常事件、定期自评估和检查评估等手段，发现安全保密管理的薄弱环节并不断改进完善。因此，在测评实践中，要分析被测涉密信息系统的安全保密管理体系是否具备自我改进的能力，以防止在涉密信息系统开通运行一段时间后，出现安全保密管理体系与实际的管理需求不相适应的情况。

7 结语

本文根据作者参与涉密信息系统测评工作的经验和认识，就如何把握涉密信息系统安全保密管理的测评要点进行了讨论。由于在实际测评工作中，安全保密管理体系的评价存在较大的主观色彩，往往与测评人员的工作经历、对标准的认识深度、分析问题的能力以及对被测单位的了解程度等人为因素有关，为正确贯彻标准、促进涉密信息系统建设使用单位改进安全保密管理体系、确保国家秘密安全，有必要针对涉密信息系统安全保密管理体系的评价方法和要点进行深入研究。BMS