列表译码在密码中的应用综述

张卓然 张 煌 张方国*

(中山大学数据科学与计算机学院 广州 510006)

(广东省信息安全技术重点实验室 广州 510006)

摘 要：列表译码自上世纪50年代提出以来，不仅在通信与编码等方面得到了广泛应用，也在计算复杂性理论和密码学领域有着广泛的应用。近年来，随着量子计算的发展，基于整数分解等传统困难问题设计的密码方案受到了巨大的威胁。由于编码理论中一些计算问题的NP困难性被广泛认为是量子概率多项式时间不可攻克的，建立在其上的基于纠错码的密码体制得到了越来越多的重视，列表译码也越来越引起人们的关注。该文系统梳理了列表译码在密码学中的应用，包括早期在证明任何单向函数都存在硬核谓词、设计叛徒追踪方案、以多项式重建作为密码原语设计公钥方案、改进传统基于纠错码的密码方案和求解离散对数问题(DLP)等方面的应用，以及近期，列表译码在设计安全通信协议、求解椭圆曲线离散对数问题、设计新的基于纠错码的密码方案等方面的应用。该文对列表译码的算法改进及其在密码协议设计和密码分析中的应用、新应用场景探索等方面的发展趋势进行了探讨。

关键词：公钥密码；列表译码；离散对数；后量子密码

中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2020)05-1049-12

DOI: 10.11999/JEIT190851

Survey on Applications of List Decoding to Cryptography

ZHANG Zhuoran ZHANG Huang ZHANG Fangguo

(*School of Data and Computer Science*, *Sun Yat-sen University*, *Guangzhou* 510006, *China*)

(*Guangdong Key Laboratory of Information Security*, *Guangzhou* 510006, *China*)

Abstract: Since the conception of list decoding is proposed in the 1950s, list decoding not only is applied to communication and coding theory, but also plays a significant role in computational complexity and cryptography. In recent years, with the rapid development of quantum computing, the traditional cryptographic schemes based on factorization and other difficult problems are greatly threatened. The code-based cryptosystems, whose security relies on the NP-hard problems in coding theory, are attracting more and more attention as a candidate of the post-quantum cryptography, and so does the list decoding algorithm. This paper systematically reviews the applications of list decoding to cryptography, including early applications in proving that any one-way function has hard-core bits, designing traitor tracing schemes, designing public key schemes using polynomial reconstruction as cryptographic primitives, improving the traditional code-based cryptosystems and solving Discrete Logarithm Problems (DLP), and recent applications to designing secure communication interactive protocols, solving the elliptic curve discrete logarithm problem, and designs new cryptographic schemes based on error correction codes. Finally, the new research issues of the algorithm improvement of list decoding, its application to the design of cryptographic protocol and cryptoanalysis, and the exploration of new application scenarios are discussed.

Key words: Public key cryptography; List decoding; Discrete logarithm; Post-quantum cryptography

收稿日期：2019-11-01；改回日期：2020-02-25；网络出版：2020-03-19

*通信作者： 张方国 isszhfg@mail.sysu.edu.cn

基金项目：国家自然科学基金(61672550, 61972429)，国家重点研发计划(2017YFB0802503)

Foundation Items: The National Natural Science Foundation of China (61672550, 61972429), The National Key R & D Program of China (2017YFB0802503)

1 引言

纠错码理论在密码学中的应用与研究已经有了很长的历史。1978 年Berlekamp等人[1]证明了一般线性码的译码问题是NP完全问题，受到这一事实而启发出的第1个基于纠错码的McEliece公钥加密方案[2]，开启了纠错码理论在密码学中的应用前景。基于纠错码理论构造的公钥体制，其理论基础是译码问题的困难性，即仅在已知生成矩阵的情况下，在码空间中寻找与给定接收向量Hamming距离最短的码字。纠错码可以被用于构造公钥加密和签名算法、设计对称方案等，在现代密码学中发挥着重要的作用。

列表译码是纠错码理论中一类特殊的译码算法，它可以输出与接收向量在给定Hamming距离内的全部合法码字，并且它的纠错能力超过了传统的唯一译码(unique decoding)算法。对列表译码的研究最早可以追溯到上世纪50年代的Elias[3]，但当时只是提出了列表译码的概念，并没有给出可行的算法。目前，比较经典的算法有对Hadamard码的列表译码算法[4]、对Reed-Solomon(RS)码的译码算法[5]、对代数几何码的译码算法[6,7]、对Reed-Muller(RM)码的译码算法[8]等。Sudan[9]在2000年曾给出过一个关于列表译码的综述，但该综述仅着眼于列表译码在计算复杂性理论中的应用。

列表译码在密码学领域也有着广泛的应用。Goldreich和Levin[4]通过Hadamard码的列表译码算法，提出了对任意单向函数构造硬核谓词的方法，引出了硬核谓词与列表译码间的微妙联系，启发了大量的工作[10–18]，列表译码成为了硬核谓词研究中的重要技术之一。列表译码比传统纠错算法更强大的能力，在提高叛徒追踪方案的效率[19–25]、降低传统基于纠错码的密码方案的参数规模和密钥长度[26]等方面都发挥了独特的作用。另一方面，列表译码算法和某些特殊问题之间的关联，使其在密码学中得到了更加广泛的应用。如RS码的列表译码问题，本质上就是通过某些点和对应函数值来恢复赋值多项式，因此又被称为多项式重建(Polynomial Reconstruction, PR)问题，基于该问题及相关子问题，可以设计许多有趣的密码方案和协议[27–30]。而有限域上离散对数问题的求解[31,32]，也和RS码的列表译码有着深刻的联系。

近几年，列表译码技术在密码学中得到了进一步的应用。在设计能够抵抗量子计算攻击和主动敌手攻击的安全通信协议时，RS码由于具有高效列表译码算法，可以提高信道传输能力和纠错能力，被用来对传递的消息进行编码[33]。代数几何码作为RS在高亏格曲线上的推广，也有着有效的列表译码算法，受到用列表译码求解有限域上离散对数问题的研究思路的启发，椭圆码的列表译码被用来对椭圆曲线上离散对数进行求解[34]。在后量子密码的方案设计中，列表译码不仅被用来减小密钥规模，还被用来保护码族的结构，为代数几何码在密码中的应用创造了可能[35–37]。列表译码技术的强大功能，正在成为密码学飞速发展的助推剂。探究列表译码技术在密码学中的新应用，具有重要的理论意义和实用价值。

本文将对列表译码在密码中的应用进行较为细致的综述。首先将以硬核谓词、叛徒追踪、构造公钥方案、求解离散对数问题和缩短密钥尺寸为例，介绍列表译码在密码学中的早期应用。然后重点介绍列表译码近些年来在密码学中的新应用，如在构造安全通信协议、求解椭圆曲线上离散对数问题、设计新的基于代数几何码的密码方案等方面。

文章组织如下：第2节介绍线性纠错码和代数几何码的基本定义与性质。第3节介绍现有的列表译码算法，主要是RS码和代数几何码的列表译码算法。第4节和第5节分别介绍列表译码技术在密码学中的早期应用和新应用。最后，第6节对全文进行总结，并对未来的发展趋势进行探讨。

2 纠错码与代数几何码

定义在有限域$\mathbb{F}_q$上码长为n，维数为k的$[n,k]$线性码$\mathcal{C}$是n维线性空间$\mathbb{F}_q^n$的一个k维子空间，$\mathcal{C}$中的向量称为码字(codeword)。$\mathcal{C}$的生成矩阵$\boldsymbol{G}$是满秩的$k\times n$矩阵，$\boldsymbol{G}$的行向量构成了$\mathcal{C}$的一组基，因此一个线性码的生成矩阵不是唯一的，各个生成矩阵之间可以通过初等行变换相互转化。形式化地，码$\mathcal{C}$的定义是$\mathcal{C}=\{\boldsymbol{x}\boldsymbol{G}|\boldsymbol{x}\in\mathbb{F}_q^k\}$。给定一个码字$\boldsymbol{c}=(c_1,c_2,\cdots,c_n)\in\mathcal{C}\subseteq\mathbb{F}_q^n$，它的汉明重量(Hamming weight)是指码字中非零分量的个数，即$\mathrm{wt}(\boldsymbol{c})=|\{i|c_i\neq 0,1\le i\le n\}|$。两个码字$\boldsymbol{c}_1$和$\boldsymbol{c}_2$之间的汉明距离$d(\boldsymbol{c}_1,\boldsymbol{c}_2)$，是指两个码字中不同分量的个数，而线性码$\mathcal{C}$的最小距离$d(\mathcal{C})$是$\mathcal{C}$中任意两个码字之间汉明距离的最小值。由纠错码的线性性质，有$d(\mathcal{C})$就是$\mathcal{C}$中所有非零码字重量的最小值，即$d(\mathcal{C})=\min\{\mathrm{wt}(\boldsymbol{c})|\boldsymbol{c}\in\mathcal{C}\backslash\{0\}\}$。如果$[n,k]$码的最小距离是$d$，那么$\mathcal{C}$就是一个$[n,k,d]$线性码。

代数几何码作为RS码的一般推广，由Goppa[38]在1977年首先提出，并由Janwa和Moreno[39]在1996年引入密码学。代数几何码是一类定义在代数曲线上的线性码。设$\mathcal{X}$是有限域$\mathbb{F}_q$上的一条不可约曲线，亏格为g，记$\mathcal{X}$上的函数域为$\mathbb{F}_q(\mathcal{X})$。曲线上的除子$D$是曲线$\mathcal{X}$上的点的形式和，即$D=\sum_P n_P P$，

其中$n_P \in \mathbb{Z}\backslash\{0\}$仅在有限个点成立。这些系数非零的点组成的集合被称为除子D的支座，记作$\mathrm{supp}(D)$。除子D的次数是n_P的和，即$\deg(D)=\sum_P n_P$。对任意$P\in\mathcal{X}$和$f\in\mathbb{F}_q(\mathcal{X})\backslash\{0\}$，定义$f$在点$P$的赋值$v_P$是从$\mathbb{F}_q(\mathcal{X})$到$\mathbb{Z}\cup\{\infty\}$的映射。如果$v_P(f)=m>0$，则称$P$是$m$重零点；如果$v_P(f)=m<0$，则称$P$是$-m$重极点。任意函数$f\in\mathbb{F}_q(\mathcal{X})\backslash\{0\}$可以与主除子相对应。$f$的主除子的定义为$\mathrm{div}(f)=\sum_P v_P(f)Pv_P(f)P$，主除子的次数总是0。设$G=\sum_P n_P$是曲线$\mathcal{X}$上任一个$\alpha$次除子。用$\mathcal{L}(G)$表示所有非负有理函数构成的集合，即$\mathcal{L}(G)=\{f|\mathrm{div}(f)+G\succ 0\}\cup\{0\}$。由Riemann-Roch定理，$\mathcal{L}(G)$是$\mathbb{F}_q$上维数有限的向量空间，它的维数为$\dim(\mathcal{L}(G))=\alpha-g+1$，其中$g$是曲线$\mathcal{X}$的亏格。给定一条不可约曲线$\mathcal{X}$和$\mathcal{X}$上的函数域$\mathbb{F}_q(\mathcal{X})$，设$P_1,P_2,\cdots,P_n$是$\mathcal{X}$上互不相同的有理点。由这$n$个点定义除子$D=P_1+P_2+\cdots+P_n$。设$G$是$\mathcal{X}$上任意满足$\{P_1,P_2,\cdots,P_n\}\cap\mathrm{supp}(G)=\varnothing$的除子，则代数几何码$\mathcal{C}(D,G)$由映射$\mathrm{ev}:\mathcal{L}(G)\to\mathbb{F}_q^n$定义，其中$\mathrm{ev}(f)=(f(P_1),f(P_2),\cdots,f(P_n))$。因此，$\mathcal{C}(D,G)=\mathrm{image}(\mathrm{ev})$。如果$G=\sum_P n_P P$是一个$\alpha$次除子，那么$\mathcal{C}(D,G)$就是$\mathbb{F}_q$上的一个$[n,k=\alpha+g-1,d]$码，且有$d\le n-k+1$。更多代数几何码的性质可以参阅文献[40]。

3　列表译码技术

码字在信道上传送的过程中可能出现错误。如果$\boldsymbol{c}$是一个码字，而$\boldsymbol{r}=\boldsymbol{c}+\boldsymbol{e}$是接收到的向量，称$\boldsymbol{r}$为接收向量(或受损码字)，$\boldsymbol{e}$为错误向量，$\{i|e_i\neq 0\}$为错误位置，$\mathrm{wt}(\boldsymbol{e})$为错误重量。如果$\mathrm{wt}(\boldsymbol{e})<d/2$，那么在码字空间里可以找到与该接收向量对应的唯一码字$\boldsymbol{c}'$，且一定有$\boldsymbol{c}=\boldsymbol{c}'$。这种译码方式叫做唯一译码。但研究者们很早就注意到，从接收向量恢复码字并不是只有唯一译码能完成的。上世纪50年代，Elias[3]首先提出了列表译码的概念，在列表译码中，输出结果不再是某个特定的码字，而是到接收向量的距离在给定范围内的全部码字的列表。显然，列表译码可以纠正重量更大的错误，有着比唯一译码更强的纠错能力。第1个具体的列表译码算法是由Goldreich和Levin等人[4]在1989年提出的关于Hadamard码的一种随机译码算法，针对二元域上的Hadamard码，可以在$\mathrm{poly}\left(\lg n,\frac{1}{\gamma}\right)$的时间内，给出到接收向量的距离在$\left(\frac{1}{2}-\gamma\right)n$的所有码字。目前在实际中应用较多的代数几何码及其列表译码，将在下面做出详细介绍。

1996年，Sudan[5]给出了RS码的列表译码算法，该算法可以纠正接收向量中重量不超过$n-\sqrt{2nk}$的错误。随后，Shokrollahi和Wasserman[41]将这一算法进行了推广，从而可以对任意代数几何码进行译码，但可以纠正的错误上界仍然是$n-\sqrt{2nk}$。1999年，Guruswami和Sudan[6,7]对之前的算法进行了优化，将RS码和代数几何码可以纠正的错误上界提高到了$n-\sqrt{nk}$，即该算法可以有效地输出一个表单，该表单包含所有以接收向量为中心，半径不超过$t=n-\sqrt{nk}$的码字。进一步地，列表译码算法ListDecode$(\mathcal{C},\boldsymbol{r},t)$以一个$[n,k]$线性码$\mathcal{C}$，一个接收向量$\boldsymbol{r}$和参数$t\le n-\sqrt{nk}$为输入，输出一个码字表单，该表单里的码字到$\boldsymbol{r}$的汉明距离不超过$t$。表1给出该算法的一个简短描述，更多信息请参考文献[6,7]。

目前为止，列表译码是对代数几何码最有效的译码算法之一。文献[6,7]中给出的插值和求根算法实现效率比较低，后续有大量的工作给出了更有效的算法，如文献[42,43]等。Muralidhara等人[44]给出了纠错能力超过$n-\sqrt{nk}$的RS码的列表译码算法，他们证明了对任何常数c，以$n-\sqrt{nk}+\mathrm{c}$为半径的汉明球中，有至多$\mathcal{O}\left(n^{2\mathrm{c}\sqrt{\alpha}/(1-\sqrt{\alpha})^2+\mathrm{c}+2}\right)$个合法码字。Guruswami和Xing在文献[45]中利用蒙特卡洛算法，给出了对任意固定$\epsilon>0$，可以在$\mathcal{O}(1/\epsilon)$时间内，纠正$(1-R-\epsilon)$比例的错误的列表译码算法，其中$R=k/n$，该算法不仅适用于RS码，也适用于秩度量的Gabidulin码，是第一个可以纠正超过$d/2$个秩错误的列表译码算法。

4　列表译码在密码学中的早期应用

列表译码在密码中早期的应用起源于单向函数硬核谓词的构造，之后在叛徒追踪、构造基于多项式重构的密码体制，及减少基于纠错码的密钥尺寸等方面均有所应用。

4.1　硬核谓词

函数f的硬核谓词是一个布尔函数h，它代表着与函数f原像相关的信息中，最不容易被求逆的某一比特。故而当f被普遍认为是单向函数后，h的像便展现出优秀的伪随机性。这使得它在伪随机数生成器、伪随机函数等密码学理论中具有重要作用。1982年Blum和Micali[10]首次发现硬核谓词的存在后，探讨这一有趣现象的工作陆续出现。Goldreich和Levin[4]发现对任意单向函数$f(x)$，容易构造新的单向函数$g(x,r)$及其硬核谓词$h(x,r)$。证明思路是将硬核谓词转换成Hadamard码的码字集合，将与待求逆的单向函数值$g(x,r)$相关的硬核谓

表 1 Guruswami-Sudan列表译码算法 ListDecode$(\mathcal{C},\boldsymbol{r},t)$

输入：有限域$\mathbb{F}_q$，曲线$\mathcal{X}$，除子$G=\alpha Q$和D，接受向量$\boldsymbol{r}=(r_1,r_2,\cdots,r_n)$ 以及错误重量上界t。

初始化：

(1) 设置表单$\Omega_r:=\varnothing$；

(2) 由n,k,t计算译码参数l，要求$l>\alpha$；一般地，设

$$r=1+\frac{(2g+\alpha)n-2gt+\sqrt{((2g+\alpha)n-2gt)^2-4(g^2-1)((n-t)^2-\alpha n)}}{2(n-t)^2-\alpha n},\ l=r(n-t)-1;$$

(3) 固定$\mathcal{L}(lQ)$的一组极基$\{\phi_{j_1}:1\le j_1\le l-g+1\}$，使得$Q$最多为$\phi_{j_1}$的$j_1+g-1$次极点；

(4) 对任意$P_i,1\le i\le n$，找$\mathcal{L}(lQ)$的一组零基$\{\psi_{j_3}:1\le j_3\le l-g+1\}$，使得$P_i$为$\psi_{j_3,P_i}$重数(至少)为$j_3-1$的零点；

(5) 计算集合$\{a_{P_i,j_1,j_3}\in\mathbb{F}_q:1\le i\le n,1\le j_1,j_3\le l-g+1\}$，使得对任意i和$j_1$，都有$\phi_{j_1}=\Sigma_{j_3}a_{P_i,j_1,j_3}\psi_{j_3,P_i}$。

插值：

令$s=\dfrac{l-g}{\alpha}$，找非零多项式$H\in\mathcal{L}(lQ)[T]$，它具有以下形式：$H[T]=\sum\limits_{j_2=0}^{s}\sum\limits_{j_1=1}^{l-g+1-\alpha j_2}h_{j_1,j_2}\phi_{j_1}T^{j_2}$；

其中，系数$h_{j_1,j_2}\in\mathbb{F}_q$满足：至少有一个$h_{j_1,j_2}$是非零的，且对任意$i\in[n]$，和满足$j_3+j_4\le r$的$j_3\ge 1,j_4\ge 0$，有

$$h_{j_3,j_4}^{(i)}=\sum_{j_2=j_4}^{s}\sum_{j_1=1}^{l-g+1-\alpha j_2}\binom{j_2}{j_4}r_i^{j_2-j_4}\cdot h_{j_1,j_2}\alpha_{x_i,j_1,j_3}=0$$

求根：

找到$H[T]$的所有根$h\in\mathcal{L}(\alpha Q)\subseteq\mathcal{L}(lQ)$。对每一个$h$，检查是否对至少$n-t$个$i\in\{1,2,\cdots,n\}$有$h(P_i)=r_i$，即$d(\boldsymbol{r},\boldsymbol{c})\le t$。如果成立，将$h$加入$\Omega_r$。

输出：码字列表Ω_r。

词值$h(x,r)$转成受损码字，再通过寻找与受损码字距离最为接近的一批码字来对$g(x,r)$求逆。这种对任意单向函数构造硬核谓词的方式，本质上是一个对Hadamard码的多项式时间列表译码算法。

2003年，Akavia 等人[11]中给出了一套对于任意抽象群上单向函数的硬核谓词的构造和证明方法，首次明确地展示了列表译码技术在硬核谓词研究中的作用。该方法中的关键一步是寻找任意函数的坐标所对应的傅里叶基，可保证整个规约算法能在多项式时间执行。王明强等人[12]在此基础上提出了基于列表译码方法在查询访问模型下含错学习问题的求解算法，其结果也可以理解为建立了一类单向函数的困难比特。2009年，Morillo等人[13]扩展了Akavia的工作，证明了对于定义在N阶循环群上可以乘法访问的任意函数而言，其所有的比特都是安全的。之后，谢小荣等人[14]证明了$ax+b \bmod p$的任意比特位是p阶循环群上积性码可接近的单向函数的硬核谓词。Duc等人[15]在2012年用列表译码技术证明了有限域$\mathbb{F}_q$上椭圆曲线的单向函数，其输入的任意一比特都是硬核的。同年，Fazio等人[16]给出进一步成果，他们在有限域$\mathbb{F}_{p^2}$上定义了一个Diffie-Hellman(DH)问题的变体，并利用列表译码技术证明了秘密DH值的其中一个坐标的任意比特位是无法预测的。2016年，Wang等人[17]在文献[16]的基础上，进一步给出了如下结论：在$\mathbb{F}_{p^2}$上的计算性DH问题的秘密值的所有单独的比特位都是硬核的，而对于在$\mathbb{F}_{p^t}$上的计算DH问题而言，几乎所有的单独比特位都是硬核的。2006年，Kawachi等人[18]提出了对于任意量子单向函数的3个量子硬核函数。通过提出主要技术为对经典纠错码的量子列表解码方法，他们证明了伪随机数生成器的的量子硬核特性，给出了一个简单但强大的标准用以将多项式时间可计算码转化为量子单向函数的量子硬核谓词。

4.2 叛徒追踪

叛徒追踪方案考虑的是数字资源通过网络广播的手段发送给各个订阅者的场景。在付费电视和网络等应用中，服务提供者以公钥将资源加密，并给予订阅者内置私钥的硬件或软件实现的解码器用于解密，从而仅有付费用户能够获得服务。然而，合法的订阅者可以通过复制解码器或提取解码器中的私钥，制作更多的解码器分发给未被授权的用户。“叛徒”就是指进行上述行为的授权用户。叛徒追踪方案希望通过提升授权用户进行叛徒行为的代价来减少或阻止这种行为的发生。具体来讲，如果多个用户合谋生成非授权的解码器，那么至少其中一个合谋者会被检测出来。由于合谋者均不希望自己成为被追踪的一个，上述特性已经对于非授权行为造成可观的警示。早期的叛徒追踪策略通过分发不同的私钥组合给授权用户，在定位其身份的同时给予其解密的能力，然而这种策略仅能概率性地追踪叛徒。

为了给出确定性的追踪策略，Boneh等人[19]首次尝试使用了代数方法来设计方案。该叛徒追踪方案的追踪性与安全分别基于离散对数问题(Discrete

Logarithm Problems, DLP)和判定性DH问题，并且需要借助一种线性空间追踪码。如果由这种码产生的$2k$个密钥是线性无关的，那么叛徒们在生成新的私钥时，任何k个密钥的凸组合是可以被唯一追踪的(尽管不一定高效)，其中k是叛徒个数上界。作者进一步指出，如果使用RS码，并以适当的方式从其中产生私钥，那么利用RS码的列表译码算法，可以实现更有效的追踪。Fernandez等人[20]提出了以代数几何码及其列表译码算法找出所有非诚实用户的方法。随后的一系列工作，如文献[21–23]等，均体现出列表译码技术在以纠错码为基础的叛徒追踪策略中有诸多潜在的用途。2001年，Silverberg等人[24,25]利用列表译码技术构造了一个叛徒追踪方案，该方案可以高效地列举出所有可能的叛徒。

4.3 构造密码协议

RS码的列表译码问题又被称为PR问题，即给定参数k,t和n个点(x_i,y_i)，求全部次数不超过k的多项式$P(x)$，使得在至少对t个i的值有$y_i=P(x_i)$。Naor和Pinkas在文献[46]中利用PR问题构造了多种实用的加密应用，但当时并没有对方案的安全性进行严格的证明。Kiayias和Yung[28]研究了PR问题的困难性，证明了PR及其相关子问题，指标PR(Index-PR)问题在密码学意义上具有很强的鲁棒性，非常值得在密码学中被进一步研究和应用。他们提出了判定版本的PR问题，并证明了该判定问题中部分信息的提取是困难的，即在新的点上预测某些可计算函数的值是困难的；此外，PR实例是伪随机的，它们与随机点集不可区分。这些结果表明PR问题在密码学意义上是非常健壮的，适合在密码构造中使用。多样本多项式重建问题(Multisample - PR, MPR)作为PR问题的自然推广，在文献[27]中被第1次提出，并在文献[47]中得到了进一步的研究。MPR问题具有与PR问题相似的鲁棒性。Kiayias和Yung[28]对相应的指标MPR问题做了研究。基于MPR问题的困难性，他们在文献[30]中给出了两种类型的多项式表示的安全游戏模型，并在此基础上设计了一系列密码协议。他们设计的私有信息检索协议能保证检索结果正确，且仅有对数级的复杂度。此外，他们还给出了列表交集预测、不经意协商等多种具体协议，这些协议可以被用于安全计算、结算托管等，从而在电子商务中发挥作用。

利用PR和MPR问题还可以设计对称加密方案，产生的流(块)密码体制具有许多良好的性质[30]，如语义安全、纠错解密(error-correcting decryption)、超短密钥、在有限域上具有乘法有解的全同态性等。而在公钥体制方面，Augot和Finiasz[48]利用PR问题构造了一种公钥加密方案，该方案的公钥是一个困难PR问题实例，而私钥是对应的错误位置。加密时，由公钥和随机数作标量乘的结果与明文相加，再添加额外错误扰动，得到密文；解密时，先由私钥去除部分错误，再由译码算法去除剩余的错误。该方案与McEliece方案相比有着更小的密钥尺寸，但方案的部分参数被Coron[49]攻破，Kiayias和Yung[29]进一步证明了利用列表译码技术可以构造对该方案的通用攻击。

4.4 $\mathbb{F}_q$上DLP求解

Justesen和Hoholdt[50]指出，对于任意整数$g<n$，存在至少一个半径为$n-g$的汉明球，包含了至少$\binom{n}{g}/q^{g-k}$个码字。但是当g的值从k逐渐提高到n时，$\binom{n}{g}/q^{g-k}$会下降到低于1的值，此时g的值是小于$\sqrt{nk}$的。即如果用$\hat{g}(n,k,q)$表示使得$\binom{n}{g}/q^{g-k}$小于1的最小整数，$\hat{g}(n,k,q)$和$\sqrt{nk}$之间存在一个间隙。那么，当错误重量为$n-\hat{g}(n,k,q)$时，列表译码究竟有多困难呢？Cheng和Wan在文献[31]中对此问题进行了研究，并发现该问题和有限域上的DLP有着密切的联系。

DLP是数论中的经典困难问题之一，目前已知的最优算法仍然是亚指数级的计算复杂度，因此在密码学中被广泛应用于构造密码方案。DLP的一个实例$(\mathbb{Z}_p{}^*,g,y)$是，给定乘法群$\mathbb{Z}_p{}^*$和其中一个生成元g，对$\mathbb{Z}_p{}^*$中的元素y，求整数a, $0\le a\le p-1$，使得$g^a=y$。如何提高DLP的求解效率、是否存在一些特殊参数使得相应的DLP是容易的，都是密码学中的研究热点。

Cheng和Wan在文献[31]通过建立到接收向量的距离为$n-g$的码字和$\mathbb{F}_q$上g次多项式环的一一映射，证明了如果列表译码可以纠正$n-\hat{g}(n,k,q)$个错误，那么有限域$\mathbb{F}_{q^{\hat{g}(n,k,q)-k}}$上的DLP是容易的。另外，若$h$和$g$分别是对任意$\epsilon>0$满足$q\ge\max(g^2,(h-1)^{2+\epsilon})$和$g\ge(4/\epsilon+2)(h+1)$的正整数，求解$\mathbb{F}_{q^h}$上的以$b(\alpha)$为基的$t(\alpha)$的离散对数时，通过构造赋值点集为$\{(a,-f(a)/h(a)-a^{g-h})|a\in\mathbb{F}_q\}$的RS码，并以类似于指数演算法的方式，重复运行错误界为$q-g$的列表译码来收集方程，再分解因式，最终能以$1-1/2n$的概率求得DLP的解。

同年，Cheng还在文献[32]中提出了一种算法，在满足一些特定条件的情况下，利用RS码的列表译码技术，可以在关于$\lg(q^n)$的多项式时间内，对给定的有限域$\mathbb{F}_{q^n}$上的g和g^e，找到离散对数e从而给出了$\mathbb{F}_{q^n}$上有界数字和形式的DLP更有效的求解算法。Cheng给出的算法[38]以指数演算法为基础，是一种随机算法，适用于对有限域$\mathbb{F}_q$的

Kummer扩张$\mathbb{F}_{q^n}$上的DLP的求解。该算法以有限域$\mathbb{F}_{q^n}=\mathbb{F}_q[x]/(x^n-a)$及其生成元$g$和求解目标$y=g^e$为输入，希望输出求解结果$e$。算法对参数的要求是：(1) $n|q-1$; (2) $0\le e\le q^n$且$S_q(e)\le n$; (3) $g=\alpha+b$，其中$\mathbb{F}_q(\alpha)=\mathbb{F}_{q^n}$, $b\in\mathbb{F}_q{}^*$且$\alpha^n\in\mathbb{F}_q$。算法的核心思想是将y表示为$f(\alpha)$的形式，其中$f\in\mathbb{F}_q[x]$且$\deg(f)\le n$，并将该多项式分解为$f(x)=(x+b)^{e_1}(h^2x+b)^{e_2}\cdots(h^{n-1}x+b)^{e_{n-1}}$的形式，其中分解得到的幂次指数就是$e$的$q$元分解表示的系数，即$e=e_0+e_1q+\cdots+e_{n-1}q^{n-1}$。这一步骤几乎与RS码的列表译码算法相同，因此利用Guruswami-Sudan的列表译码算法，就可以对DLP求解算法进行有效的实现。

4.5 减小公钥尺寸

目前公认的抗量子密码主要是基于格、基于纠错码、基于多变量和基于哈希的方案。美国国家标准技术局 NIST已经于2018年开始对抗量子密码方案的征集，在他们收到的69个草案中有20个是利用纠错码设计的，而进入第2轮筛选的26个方案中有7个是基于纠错码的，基于纠错码的密码体制在量子计算时代的地位可见一斑。McEliece方案[2]是经典的基于纠错码的公钥加密方案，其安全性依赖于线性码的一般译码问题和Goppa码的区分问题，被认为是可以抵抗量子计算攻击的公钥加密方案。McEliece方案加解密算法都非常高效，但过大的公钥规模限制了其实用性，因此许多工作围绕着缩减McEliece体制的密钥尺寸进行。目前，比较主流的减小密钥长度的方法有使用准循环(Quasi-Cyclic, QC)码、准并矢(Quasi-Dyadic, QD)码，或转用基于秩度量(rank metric)的编码等。这些方法都使用了具有特殊结构的码族，在某些参数或码族选择不合适的情况下，可能会导致攻击。

Barbier和Barreto在文献[26]中提出，将传统基于编码的密码体制中调用的译码算法，从唯一译码变为列表译码，从而在加密时可以引入重量超过最小距离d的一半的错误向量。上述改变将增加一般译码问题的难度，可以选用长度和维数更小的码。进一步地，上述改变不会给使用的原始码增加额外的结构特点，或减小原始码的空间，从而不会带来新的安全隐患。与此同时，对所有基于编码的密码方案的通用攻击，信息集译码攻击，有着和错误重量密切相关的算法复杂度[51]，随着错误重量的增加，ISD的算法复杂度是呈亚指数级增加的。因此，和使用唯一译码的方案相比，采用列表译码技术能够用更小的参数来抵抗同样级别的ISD攻击，从而达到减小密钥存储空间的效果。他们指出，使用二元Goppa码的列表译码来改进标准McEliece加密方案，可以减少4%的密钥存储空间，如果将Goppa码换成QD码，可以减少21%的密钥存储空间。虽然他们提出的使用QD码的方案并不能完全避免文献[52]提出的攻击，但使用列表译码来减小参数规模进而减小密钥尺寸的思想，为提高McEliece方案的实用性提供了思路。

5 列表译码在密码学中的新应用

5.1 安全通信

物联网的不断普及和量子计算的飞速发展，对当今网络物理世界的长期信息安全保障提出了巨大的挑战。当前通讯网络的极端连通性意味着对数据的保护必须是端到端的，并且保护必须要落实在网络的所有层，而量子计算的发展前景还要求算法和协议在量子计算时代仍然保持安全。能否在物理层假设上构建端到端的安全通信成为了一个值得关注的问题。

Wang等人在文献[33]中，提出了一种能够抵抗敌手的包括窃听、在被窃听的部分码字上添加噪声扰动等攻击行为的交互协议。该协议建立在Wyner第2类窃听模型[53]下，即通信双方所用的信道，被拥有无限计算能力的敌手监听，且敌手可以选择查看并修改固定比例的通信内容，而通信仍然达到信息论安全，是一种特殊的对抗窃听信道(AWTP channel)。该协议可以分为两步：首先通过密钥协议(Key Agreement Protocol)步骤在通信双方之间建立共享密钥，该密钥被用来计算消息的MAC，从而接收方可以判断敌手是否对信道上的消息进行了篡改。在第2步中，双方将进行多个回合的前向传输和重复请求，确保接收方可以得到正确的消息，而敌手得不到任何有用的信息。在重复请求中，接收者会要求重传一些前一轮中的符号。在协议中，信道上传送的所有消息都使用RS码编码，直到接收方得到了足够译码的正确分量。在前向信道编码时，首先对消息用特定长度的随机数进行填充，再添加删余错误，从而保障对敌手不能从对码字的观察中获得额外的信息。而在后向信道中，同样采用RS码进行编码来保障消息的可靠性。该方案选用RS码作为主要编码方法的主要原因，就是它有着高效的列表译码算法，从而能够纠正包括噪声和删余的更多错误，有更强大的容错能力，从而可以提高通信效率。可否利用具有更好的代数性质并且能够列表译码的其他纠错码，构造更有效或性能更好的此类协议是这个方向值得深入探讨的内容。

此外，随着5G技术的发展和推广，极化码的列表译码技术引起了国内外的关注[54–56]。目前，已经有将极化码应用于设计密码方案的研究[57,58]，但这些的方案的安全性均受到了挑战[59]。如何将极化码及其列表译码应用于密码方案的设计和安全通信协议的设计，为5G通信的安全护航，也是很有意义的研究方向。

5.2 椭圆曲线上离散对数问题的求解

上世纪80年代，基于椭圆曲线的密码体制(ECC)开始发展。由于在椭圆曲线上实现的公钥加密、数字签名、密钥交换等密码原语，在和传统方案达到相同安全级别的要求下，所需要的密钥更小，实现速度更快，已经在过去的几十年中被广泛的使用到各种应用和程序之中。而ECC安全性的关键，就在于椭圆曲线上离散对数问题(ECDLP)的困难性。ECDLP问题的一个实例$(\mathbb{F}_q,\mathcal{E}(\mathbb{F}_q),p,Q,P)$是：定义在有限域$\mathbb{F}_q$上的椭圆曲线$\mathcal{E}(\mathbb{F}_q)$，$P\in\mathcal{E}(\mathbb{F}_q)$为其上的一个$p$阶点，$\langle P\rangle$为以点$P$为生成点构成的$p$阶子群，对$Q\in\langle P\rangle$，求$0\le s<p$使得$Q=sP$。目前为止，除了一些特殊的曲线，ECDLP求解算法的计算复杂度仍然是$O(\sqrt{p})$。

Goppa在1977年提出了代数几何码的概念[38]，而定义在椭圆曲线上的代数几何码就是椭圆码。对于$[n,k]$椭圆码来说，它的最小距离一定是$n-k$或$n-k+1$，这取决于是否存在$\{P_{i_1},P_{i_2},\cdots,P_{i_k}\}\subseteq\{P_1,P_2,\cdots,P_n\}$使得$P_{i_1}+P_{i_2}+\cdots+P_{i_k}-G$是一个主除子。而文献[60]和文献[61]先后关注到，曲线$\mathcal{E}$上的ECDLP的解和定义在$\mathcal{E}$的椭圆码的最小距离有着密切的关联，这就为求解ECDLP问题提供了新的思路。通过寻找椭圆码的最小重量码字，就有可能解决相应的ECDLP。虽然椭圆码的最小距离问题在文献[61]中被证明了是NP困难问题(从而寻找最小重量码字也是NP困难问题)，但理论上还是有可能构造出比穷搜索更有效率的算法。

Zhang和Liu在文献[34]中提出了一种解决ECDLP问题的新方法。对于任何ECDLP，首先构造一个对应的椭圆码，然后利用列表译码技术来寻找最小重量码字，再通过这个码字解决ECDLP问题。具体来说，对一个ECDLP问题的实例$(\mathbb{F}_q,\mathcal{E}(\mathbb{F}_q),p,Q,P)$，假设$P$的阶是素数$p$。令$\theta=\lceil\log_2 p\rceil$，$n=2\theta$，$k=\lfloor(\theta+1)/2\rfloor$。定义$P_i=2^{i-1}P$，选取$\mathbb{Z}_p$上的随机数$r_2,r_3,\cdots,r_{n-\theta}$，定义$P_{\theta+j}=r_jQ$，其中$j=1,2,\cdots,n-\theta$。由除子$G=k\mathcal{O}$和$D=\sum_{i=1}^{n}P_i$构造椭圆码$\mathcal{C}(G,D)$。调用列表译码算法，直到对一个接收向量译出两个码字，就找到了$\mathcal{C}(G,D)$的最小重量码字$\boldsymbol{c}=(c_1,c_2,\cdots,c_n)$，设其中的非零分量为$c_{i_1},c_{i_2},\cdots,c_{i_k}$。假设$i_{j-1}\le\theta$且$i_j>\theta$，则计算$s'\equiv-\left(\sum_{k=j}^{\theta}r_{i_k-\theta}\right)^{-1}\sum_{k=1}^{j-1}2^{i_k-1}\bmod p$，若验证有$Q=s'P$，则找到了相应ECDLP的解。

可以发现，对ECDLP的求解和有限域上DLP的求解，其实有很大的不同。对DLP的求解[31,32]主要基于对有限域结构的观察，只适用于某些特殊的有限域，对素域上的DLP问题是无法求解的。而Zhang等人的结果，是一种求解ECDLP的通用解法，不受有限域类型和大小限制。虽然目前文献[34]中算法的成功概率并不是很高，却是第1个通过列表译码技术解决ECDLP的算法，具有深刻的理论意义。

5.3 设计新的基于代数几何码的公钥加密方案

随着量子计算的快速发展，目前使用的基于整数分解、离散对数等数学问题困难性假设构造的公钥方案的安全性受到了极大的挑战。基于编码技术的密码方案作为能够抵抗量子攻击的方案，引起了研究者的关注。基于编码的密码方案主要有3种形式，分别是以一般译码问题为困难假设的McEliece体制、以校验子译码问题为困难假设的Niederreiter体制，和以LWE问题为困难性假设的密码体制。其中，一般译码问题和校验子译码问题已经被证明是等价的，并且都是NP完全的[1]。而椭圆码的最小距离判定问题和最大似然译码问题也是NP困难的[61]。

代数几何码的概念在1996年被Janwa和Moreno引入密码学领域[39]。代数几何码一方面将存储码的方式从生成矩阵转化为曲线上的除子和有理点集，减小了传统的McEliece方案的密钥尺寸；另一方面能够提供更多的参数选择空间，从而使得方案的应用更加灵活。然而其结构过于特殊，遭到了大量的攻击。1992年，Sidelnikov和Shestakov[62]攻破了使用亏格为0的代数几何码，也就是RS码的Niederreiter方案；Minder等人[63,64]结合ISD对亏格小于等于2的曲线上定义的代数几何码进行了攻击；Couvreur等人[65]证明了对高亏格曲线上定义的代数几何码，存在多项式时间的攻击算法，随后在文献[66]中，他们又结合ECP译码技术[67,68]对任意亏格的代数几何码给出了多项式时间的攻击。至此，代数几何码几乎已经被认为不适用于构造密码体制了。

2016年，Marquez-Corbella等人[35]提出利用RS码构造广义$(U|U+V)$码，进而设计公钥加密方案的思路。使用广义$(U|U+V)$码可以有效隐藏RS码的结构信息，从而可以抵抗针对RS码的结构攻击，进而利用RS码的特殊结构来减小私钥尺寸；而RS码具有有效的列表译码算法，和$(U|U+V)$

码的译码算法相结合，可以进一步提高译码算法的纠错能力，减小公钥尺寸。

Zhang等人[36]构造了一种能抵抗已知攻击的基于椭圆码的方案ECC^2，该方案使用了列表译码技术，从而可以纠正超过码字最小距离1/2的错误，这正是抵抗针对代数几何码的已知攻击的关键。该方案的第1个版本[36]中，所采用的McEliece方案的变种并不能达到IND-CPA安全，已经在新的版本[37]中进行了更正，即将加在消息上的随机向量由第1部分密文中被编码的向量，变成了错误中的非零位组成的新向量。为了抵抗文献[63]针对椭圆码的结构攻击，利用文献[61]中证明椭圆码最小距离问题是NP完全问题的思路，通过将一个背包问题实例转化成椭圆码，构造出赋值点远少于曲线上有理点的椭圆码，从而难以找到这样的椭圆码上的最小重量码字，这就打破了文献[63]中攻击方法的假设前提。而针对ECP攻击，利用ECP存在当且仅当错误重量不超过码的最小距离1/2的结论，添加超过限制重量的错误，从而ECP译码方法失效，无法直接攻击。同时保证从接收向量中寻找额外错误的位置也是不可行的，即先剔除超过码的最小距离1/2的错误，再使用ECP译码也是不可行的。在解码时，通过列表译码技术，直接纠正接收向量中的全部错误，译得码字，再进行解密步骤。该方案的安全性在标准模型下归结到椭圆码的校验子译码问题上。在此基础上，能否考虑利用其他代数几何码来构造安全实用的，抵抗量子攻击的密码体制，是非常值得研究的问题。

6 结束语

列表译码自诞生起，便成为了纠错码译码研究方面的一个关注点。尽管通讯领域非常需要其强大的抗噪声能力，但广义上，列表译码的功能与研究意义绝不仅限于此。从当前的情形看，列表译码的思想与底蕴深厚的纠错码理论还为其它学科中一些繁琐的现象提供了自然、严谨、相对简单的描述或解释方法。熟悉Goldreich-Levin硬核谓词的读者应当能更加容易地体会这一观点。随着纠错码与密码学的融合，前者成为了后量子密码体制中一个独具特色的计算困难性提供源。可以说，当前的纠错码理论已可以系统化地为密码学家诠释出基于纠错码的候选单向陷门函数的原理与结构。这种看似平凡的诠释却在计算复杂性的观点下证实了基于纠错码的密码体制的存在性。然而，存在性与实用性往往还存在着较大的间隙。为了缩小这个间隙，众多理论或技术上的屏障成为了亟待解决的问题。鉴于译码算法与求逆前述单向陷门函数的紧密联系，与列表译码相关的内容无疑将成为攻克这些屏障的道路上，最值得研究的课题之一。

首先来看列表译码算法本身。无论是从编码学还是密码学的角度，更少的计算资源、更强的纠错能力和更广的码族覆盖面必定是其最终追求的目标。因此，从提高运行效率与纠错能力的角度提高和改进现有算法，或是针对码族的特征结构完成其列表译码从无到有的转变均是十分有意义的研发工作。具体来看，当前使用的列表译码主要还是Guruswami-Sudan算法。如果尝试将其应用于代数几何码，那么需要寻找对应除子空间中的一组零基和一组极基。一般而言，极基容易得到，但零基并非如此。目前数学界普遍认为，对于由任意一条代数曲线上任意除子生成的Riemann-Roch空间而言，构造其一组零基是一个非常困难的计算问题；仅在某些特殊曲线上，有效的零基构造方法是已知的。既然密码方案中使用的代数几何码只能在素域上的低亏格曲线上构造，一个自然的想法便是如何针对这类特殊的曲线，改进已知的零基构造算法，使之能够服务于密码中的代数几何码，进而使列表译码成为可能。另一方面，还可以探究如何充分地运用循环码和准循环码等编码的特殊结构，用以提高其现有列表译码算法的效率。这些问题的解决将为列表译码在密码学中的应用前景提供可观的促进作用。

然后来看与列表译码相关的密码方案与协议。毋庸置疑，列表译码技术本身的提升对上层的方案与协议有正面的影响，但针对特定方案的具体特点，给出适宜的修改策略亦是对其进行优化和改进的思路。细化来看，既然当前常用的PR，也即RS码的列表译码问题，能够被用于多种密码方案和协议设计，而且多元多项式重建与列表译码存在着微妙的联系，一个直观的设想为是否能利用多元多项式重建问题以及与PR相关的设计思路，提出功能相同但性能更为优越的方案。与此同时，目前存在多个利用列表译码技术减小密钥存储空间或者保护码的特殊结构的方案，可见以列表译码为基于纠错码的方案进行减负提速的研究很可能是大有文章可做的。遗憾的是，在使用列表译码强大纠错能力的同时，付出的代价是更长的计算时间。故而为了使得上述方案更为贴近实际使用，往往还需要在密钥存储空间与解密效率或密钥安全性等方面做出权衡。除此之外，基于编码的签名等技术需要相应的校验子译码算法，而利用编码构造基于身份的加密系统时，更是需要一类对任意向量都能进行校验子译码的码族。这些问题使得寻找合适的码族与相应的列表译码算法变得有意义起来。

接下来考虑以列表译码求解DLP等问题的密码分析类研究。DLP是一个跟循环群有关的跨度相对很广的计算问题。由此，研究思路呈现两个方面：一是尝试能否将一些目前不太常用的有限域上的DLP，进行放宽限制条件的处理，然后将现有的方法扩展到其上；二是对这些不常用类型的有限域结构进行观察和分析，随后利用列表译码技术设计新的DLP求解方法。与此同时，对ECDLP问题的攻击算法的改进中，很可能会遇到缺乏合适的纠错码及其列表译码算法的情况。由于不同参数下的纠错码体现出来的纠错性能不同，于是能否在设计列表译码时借助这些现象来提速最小重量码字的寻找算法，从而提速ECDLP计算，是一个有潜力的研究课题。另外，如果能够提高Guruswami-Sudan的列表译码界，那么其很显然有助于ECDLP攻击的效率提升，但这已被认为是编码界的疑难问题。可见，在椭圆码，或者利用 ECDLP实例构造的椭圆码，甚至是具有某些特殊性质的椭圆码上，寻找相对于传统办法而言具有更高译码界和更有效的列表译码算法将是一个值得重点研究的问题。

最后，改进与提高现有的理论与方案只是为了列表译码在密码学领域深度的扩充，想要赢得更宽更广的发展，我们必须重视其在密码学新应用中的作用，尤其是全同态加密、混淆等近十年取得突飞猛进的领域。一个显而易见的难点是，尽管纠错码与格存在诸多的相似点，但上述这几种功能异常优秀的密码应用最初却是在一类特殊格，也即理想格上构造的。理想格在结构上更近似于循环码或者准循环码，拥有节省存储，具有环特性等一般格不具备的优点。因此，该方向的攻坚问题大概率集中在了寻找具有特殊结构的纠错码及其列表译码算法上，其中列表译码的作用主要体现在于解密算法与安全证明中。

随着研究的深入，密码学中的新问题和新研究方向会不断出现。鉴于效率的提高，列表译码理论与技术的实用性将不断增强，进而延伸到密码学的各分支中，为新密码方案与协议的设计以及疑难问题的解决提供更为夯实的工具与基础。

参 考 文 献

[1] BERLEKAMP E R, MCELIECE R J, and VAN TILBORG H C A. On the inherent intractability of certain coding problems (Corresp.)[J]. *IEEE Transactions on Information Theory*, 1978, 24(3): 384–386. doi: 10.1109/TIT.1978.1055873.

[2] MCELIECE R J. A public-key cryptosystem based on algebraic coding theory[R]. DSN Progress Report 42–44, 1978: 114–116.

[3] ELIAS P. List decoding for noisy channels[R]. Technical Report 335, 1957: 94–104.

[4] GOLDREICH O and LEVIN L A. A hard-core predicate for all one-way functions[C]. The 21st Annual ACM Symposium on Theory of Computing, Seattle, USA, 1989: 25–32. doi: 10.1145/73007.73010.

[5] SUDAN M. Decoding of Reed Solomon codes beyond the error-correction bound[J]. *Journal of Complexity*, 1997, 13(1): 180–193. doi: 10.1006/jcom.1997.0439.

[6] GURUSWAMI V and SUDAN M. Improved decoding of Reed-Solomon and algebraic-geometry codes[J]. *IEEE Transactions on Information Theory*, 1999, 45(6): 1757–1767. doi: 10.1109/18.782097.

[7] GURUSWAMI V and SUDAN M. On representations of algebraic-geometric codes for list decoding[C]. The 8th Annual European Symposium, Saarbrücken, Germany, 2000: 244–255. doi: 10.1007/3-540-45253-2_23.

[8] GOPALAN P, KLIVANS A R, and ZUCKERMAN D. List-decoding Reed-Muller codes over small fields[C]. The 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, 2008: 265–274. doi: 10.1145/1374376.1374417.

[9] SUDAN M. List decoding: Algorithms and applications[C]. International Conference IFIP TCS 2000 Sendai, Japan, 2000: 25–41. doi: 10.1007/3-540-44929-9_3.

[10] BLUM M and MICALI S. How to generate cryptographically strong sequences of pseudo random bits[C]. The 23rd Annual Symposium on Foundations of Computer Science, Chicago, USA, 1982: 112–117. doi: 10.1109/SFCS.1982.72.

[11] AKAVIA A, GOLDWASSER S, and SAFRA S. Proving hard-core predicates using list decoding[C]. The 44th Annual IEEE Symposium on Foundations of Computer Science, Cambridge, USA, 2003: 146–157. doi: 10.1109/SFCS.2003.1238189.

[12] 王明强, 庄金成. 基于列表译码方法在查询访问模型下含错学习问题的分析[J]. 电子与信息学报, 2020, 42(2): 322–326. doi: 10.11999/JEIT190624.

WANG Mingqiang and ZHUANG Jincheng. Analysis of learning with errors in query access model: A list decoding approach[J]. *Journal of Electronics & Information Technology*, 2020, 42(2): 322–326. doi: 10.11999/JEIT190624.

[13] MORILLO P and RÀFOLS C. The security of all bits using list decoding[C]. The 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, USA, 2009: 15–33.

[14] 谢小容, 吕克伟, 王鲲鹏. $ax+b \bmod p$比特安全的列表译码证明[J]. 系统科学与数学, 2012, 32(11): 1366–1376.

XIE Xiaorong, LÜ Kewei, and WANG Kunpeng. Proving the security of all bits of $ax + b \bmod p$ using list decoding[J]. *Journal of Systems Science and Mathematical Sciences*, 2012, 32(11): 1366–1376.

[15] DUC A and JETCHEV D. Hardness of computing individual bits for one-way functions on elliptic curves[C]. The 32nd Annual Cryptology Conference, Santa Barbara, USA, 2012: 832–849. doi: 10.1007/978-3-642-32009-5_48.

[16] FAZIO N, GENNARO R, PERERA I M, *et al*. Hard-core predicates for a Diffie-Hellman problem over finite fields[C]. The 33rd Annual Cryptology Conference, Santa Barbara, USA, 2013: 148–165. doi: 10.1007/978-3-642-40084-1_9.

[17] WANG Mingqiang, ZHAN Tao, and ZHANG Haibin. Bit security of the CDH problems over finite fields[C]. The 22nd International Conference on Selected Areas in Cryptography, Sackville, 2015: 441–461.

[18] KAWACHI A and YAMAKAMI T. Quantum hardcore functions by complexity-theoretical quantum list decoding[C]. The 33rd International Colloquium on Automata, Languages and Programming, Venice, 2006: 216–227.

[19] BONEH D and FRANKLIN M. An efficient public key traitor tracing scheme[C]. The 19th Annual International Cryptology Conference Santa Barbara, Santa Barbara, USA, 1999: 338–353. doi: 10.1007/3-540-48405-1_22.

[20] FERNANDEZ M and SORIANO M. Identification of traitors in algebraic-geometric traceability codes[J]. *IEEE Transactions on Signal Processing*, 2004, 52(10): 3073–3077. doi: 10.1109/TSP.2004.833858.

[21] FAZIO N, NICOLOSI A, and PHAN D H. Traitor tracing with optimal transmission rate[C]. The 10th International Conference on Information Security, Valparaíso, Chile, 2007: 71–88. doi: 10.1007/978-3-540-75496-1_5.

[22] PHAN D H. Traitor tracing for stateful pirate decoders with constant ciphertext rate[C]. The 1st International Conference on Cryptology in Vietnam, Hanoi, Vietnam, 2006: 354–365. doi: 10.1007/11958239_24.

[23] SIRVENT T. Traitor tracing scheme with constant ciphertext rate against powerful pirates[EB/OL]. https://eprint.iacr.org/2006/383, 2019.

[24] SILVERBERG A, STADDON J, and WALKER J L. Efficient traitor tracing algorithms using list decoding[C]. The 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Gold Coast, Australia, 2001: 175–192. doi: 10.1007/3-540-45682-1_11.

[25] SILVERBERG A, STADDON J, and WALKER J L. Applications of list decoding to tracing traitors[J]. *IEEE Transactions on Information Theory*, 2003, 49(5): 1312–1318. doi: 10.1109/TIT.2003.810630.

[26] BARBIER M and BARRETO P S L M. Key reduction of McEliece's cryptosystem using list decoding[C]. 2011 IEEE International Symposium on Information Theory Proceedings, St. Petersburg, Russia, 2011: 2681–2685. doi: 10.1109/ISIT.2011.6034058.

[27] KIAYIAS A and YUNG M. Secure games with polynomial expressions[C]. The 28th International Colloquium on Automata, Languages, and Programming, Crete, Greece, 2001: 939–950. doi: 10.1007/3-540-48224-5_76.

[28] KIAYIAS A and YUNG M. Polynomial reconstruction based cryptography[C]. The 8th Annual International Workshop on Selected Areas in Cryptography, Toronto, Canada, 2001: 129–133. doi: 10.1007/3-540-45537-X_10.

[29] KIAYIAS A and YUNG M. Cryptanalyzing the polynomial-reconstruction based public-key system under optimal parameter choice[C]. The 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, 2004: 401–416. doi: 10.1007/978-3-540-30539-2_28.

[30] KIAYIAS A and YUNG M. Cryptographic hardness based on the decoding of Reed-Solomon codes[J]. *IEEE Transactions on Information Theory*, 2008, 54(6): 2752–2769. doi: 10.1109/TIT.2008.921876.

[31] CHENG Qi and WAN Daqing. On the list and bounded distance decodibility of Reed-Solomon codes[C]. The 45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, 2004: 335–341. doi: 10.1109/FOCS.2004.46.

[32] CHENG Qi. On the bounded sum-of-digits discrete logarithm problem in finite fields[C]. The 24th Annual International Cryptology Conference, Santa Barbara, USA, 1999: 201–212. doi: 10.1007/978-3-540-28628-8_12.

[33] WANG Pengwei and SAFAVI-NAINI R. Interactive message transmission over adversarial wiretap channel Ⅱ[C]. IEEE INFOCOM 2017-IEEE Conference on Computer Communications, Atlanta, USA, 2017: 1–9. doi: 10.1109/INFOCOM.2017.8057120.

[34] ZHANG Fangguo and LIU Shengli. Solving ECDLP via list decoding[EB/OL]. https://eprint.iacr.org/2018/795.pdf, 2019.

[35] MÁRQUEZ-CORBELLA I and TILLICH J P. Using Reed-Solomon codes in the (U|U+V) construction and an application to cryptography[C]. 2016 IEEE International Symposium on Information Theory, Barcelona, Spain, 2016: 930–934. doi: 10.1109/ISIT.2016.7541435.

[36] ZHANG Fangguo and ZHANG Zhuoran. ECC^2: Error correcting code and elliptic curve based cryptosystem[C]. The 11th International Symposium Cyberspace Safety and

Security, Guangzhou, China, 2019: 214–229.

[37] ZHANG F, ZHANG Z, and GUAN P. ECC^2: Error correcting code and elliptic curve based cryptosystem (full version)[J]. Submit to Information Science.

[38] GOPPA V D. Codes on algebraic curves[J]. *Soviet Math Dokl*, 1981, 24: 170–172.

[39] JANWA H and MORENO O. McEliece public key cryptosystems using algebraic-geometric codes[J]. *Designs, Codes and Cryptography*, 1996, 8(3): 293–307. doi: 10.1023/A:1027351723034.

[40] HØHOLDT T, VAN LINT J H, and PELLIKAAN R. Algebraic Geometry Codes[M]. LUISA B. Handbook of Coding Theory. Amsterdam: Elsevier Science Inc., 1998: 871–961.

[41] SHOKROLLAHI M A and WASSERMAN H. List decoding of algebraic-geometric codes[J]. *IEEE Transactions on Information Theory*, 1999, 45(2): 432–437. doi: 10.1109/18.748993.

[42] WU Xinwen and SIEGEL P H. Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes[J]. *IEEE Transactions on Information Theory*, 2001, 47(6): 2579–2587. doi: 10.1109/18.945273.

[43] TRIFONOV P. On the root finding step in list decoding of folded Reed-Solomon codes[EB/OL]. http://arxiv.org/abs/1103.1958v3, 2019.

[44] MURALIDHARA V N and SEN S. Improvements on the Johnson bound for Reed-Solomon codes[J]. *Discrete Applied Mathematics*, 2009, 157(4): 812–818. doi: 10.1016/j.dam.2008.06.014.

[45] GURUSWAMI V and XING Chaoping. List decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the singleton bound[C]. The 45th Annual ACM Symposium on Theory of Computing, Palo Alto, USA, 2013: 843–852. doi: 10.1145/2488608.2488715.

[46] NAOR M and PINKAS B. Oblivious transfer and polynomial evaluation[C]. The 21st Annual ACM Symposium on Theory of Computing, Atlanta, USA, 1999: 245–254. doi: 10.1145/301250.301312.

[47] BLEICHENBACHER D, KIAYIAS A, and YUNG M. Decoding of interleaved Reed Solomon codes over noisy data[C]. The 30th International Colloquium on Automata, Languages, and Programming, Eindhoven, The Netherlands, 2003: 97–108. doi: 10.1007/3-540-45061-0_9.

[48] AUGOT D and FINIASZ M. A public key encryption scheme based on the polynomial reconstruction problem[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003: 229–240. doi: 10.1007/3-540-39200-9_14.

[49] CORON J S. Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem[C]. The 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, 2004: 14–27. doi: 10.1007/978-3-540-24632-9_2.

[50] JUSTESEN J and HOHOLDT T. Bounds on list decoding of MDS codes[J]. *IEEE Transactions on Information Theory*, 2001, 47(4): 1604–1609. doi: 10.1109/18.923744.

[51] NIEBUHR R, CAYREL P L, BULYGIN S, *et al*. On lower bounds for information set decoding over F_q[C]. The 2nd International Conference on Symbolic Computation and Cryptography - SCC 2010, Egham, UK, 2010: 143–157.

[52] FAUGÈRE J C, OTMANI A, PERRET L, *et al*. Algebraic cryptanalysis of mcEliece variants with compact keys[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 2010: 279–298. doi: 10.1007/978-3-642-13190-5_14.

[53] OZAROW L H and WYNER A D. Wire-tap channel Ⅱ[C]. EUROCRYPT 1984 A Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, 1984: 33–50. doi: 10.1007/3-540-39757-4_5.

[54] TAL I and VARDY A. List decoding of polar codes[J]. *IEEE Transactions on Information Theory*, 2015, 61(5): 2212–2216. doi: 10.1109/TIT.2015.2410251.

[55] 王琼, 罗亚洁, 李思舫. 基于分段循环冗余校验的极化码自适应连续取消列表译码算法[J]. 电子与信息学报, 2019, 41(7): 1572–1578. doi: 10.11999/JEIT180716.

WANG Qiong, LUO Yajie, and LI Sifang. Polar adaptive successive cancellation list decoding based on segmentation cyclic redundancy check[J]. *Journal of Electronics & Information Technology*, 2019, 41(7): 1572–1578. doi: 10.11999/JEIT180716.

[56] 王美洁, 郭锐. 极化码低时延列表连续删除译码算法[J]. 通信技术, 2016, 49(3): 270–273. doi: 10.3969/j.issn.1002-0802.2016.03.004.

WANG Meijie and GUO Rui. Reduced-latency successive cancellation list decoding for polar code[J]. *Communications Technology*, 2016, 49(3): 270–273. doi: 10.3969/j.issn.1002-0802.2016.03.004.

[57] HOOSHMAND R, SHOOSHTARI M K, EGHLIDO T, *et al*. Reducing the key length of McEliece cryptosystem using polar codes[C]. The 11th International ISC Conference on Information Security and Cryptology, Tehran, Iran, 2014: 104–108. doi: 10.1109/ISCISC.2014.6994031.

[58] SHRESTHA S R and KIM Y S. New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography[C]. The 14th International Symposium on Communications and Information Technologies, Incheon, South Korea, 2014: 368–372. doi:

10.1109/ISCIT.2014.7011934.

[59] BARDET M, CHAULET J, DRAGOI V, *et al*. Cryptanalysis of the McEliece public key cryptosystem based on polar codes[C]. The 7th International Workshop, Fukuoka, Japan, 2016: 118–143. doi: 10.1007/978-3-319-29360-8_9.

[60] DRIENCOURT Y and MICHON J F. Elliptic codes over fields of characteristics 2[J]. *Journal of Pure and Applied Algebra*, 1987, 45(1): 15–39. doi: 10.1016/0022-4049(87)90081-8.

[61] CHENG Qi. Hard problems of algebraic geometry codes[J]. *IEEE Transactions on Information Theory*, 2008, 54(1): 402–406. doi: 10.1109/TIT.2007.911213.

[62] SIDELNIKOV V M and SHESTAKOV S O. On insecurity of cryptosystems based on generalized Reed-Solomon codes[J]. *Discrete Mathematics and Applications*, 1992, 2(4): 439–444.

[63] MINDER L. Cryptography based on error correcting codes[D]. [Ph.D. dissertation], EPFL, 2007.

[64] FAURE C and MINDER L. Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes[C]. The 11th international workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, 2008: 99–107.

[65] COUVREUR A, MÁRQUEZ-CORBELLA I, and PELLIKAAN R. A polynomial time attack against algebraic geometry code based public key cryptosystems[C]. 2014 IEEE International Symposium on Information Theory, Honolulu, USA, 2014: 1446–1450. doi: 10.1109/ISIT.2014.6875072.

[66] COUVREUR A, MÁRQUEZ-CORBELLA I, and PELLIKAAN R. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes[J]. *IEEE Transactions on Information Theory*, 2017, 63(8): 5404–5418. doi: 10.1109/TIT.2017.2712636.

[67] PELLIKAAN R. On decoding by error location and dependent sets of error positions[J]. *Discrete Mathematics*, 1992, 106-107: 369–381. doi: 10.1016/0012-365X(92)90567-Y.

[68] PELLIKAAN R. On the existence of error-correcting pairs[J]. *Journal of Statistical Planning and Inference*, 1996, 51(2): 229–242. doi: 10.1016/0378-3758(95)00088-7.

张卓然：女，1995年生，博士生，研究方向为基于纠错码的密码学.

张 煌：男，1988年生，博士生，研究方向为格密码和零知识.

张方国：男，1972年生，教授，研究方向为密码学理论及其应用，特别是椭圆曲线密码体制、安全多方计算、可证明安全性等.