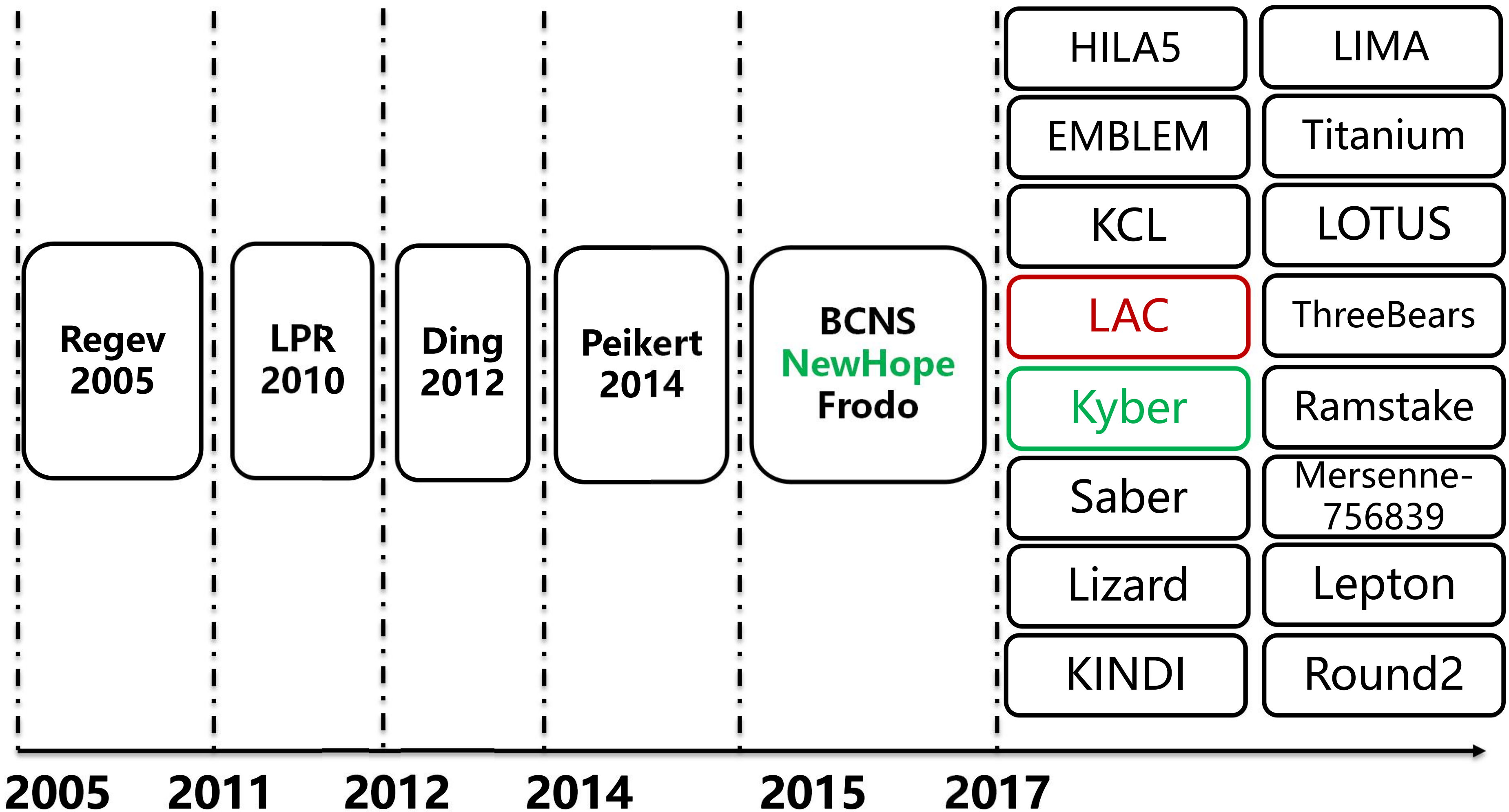
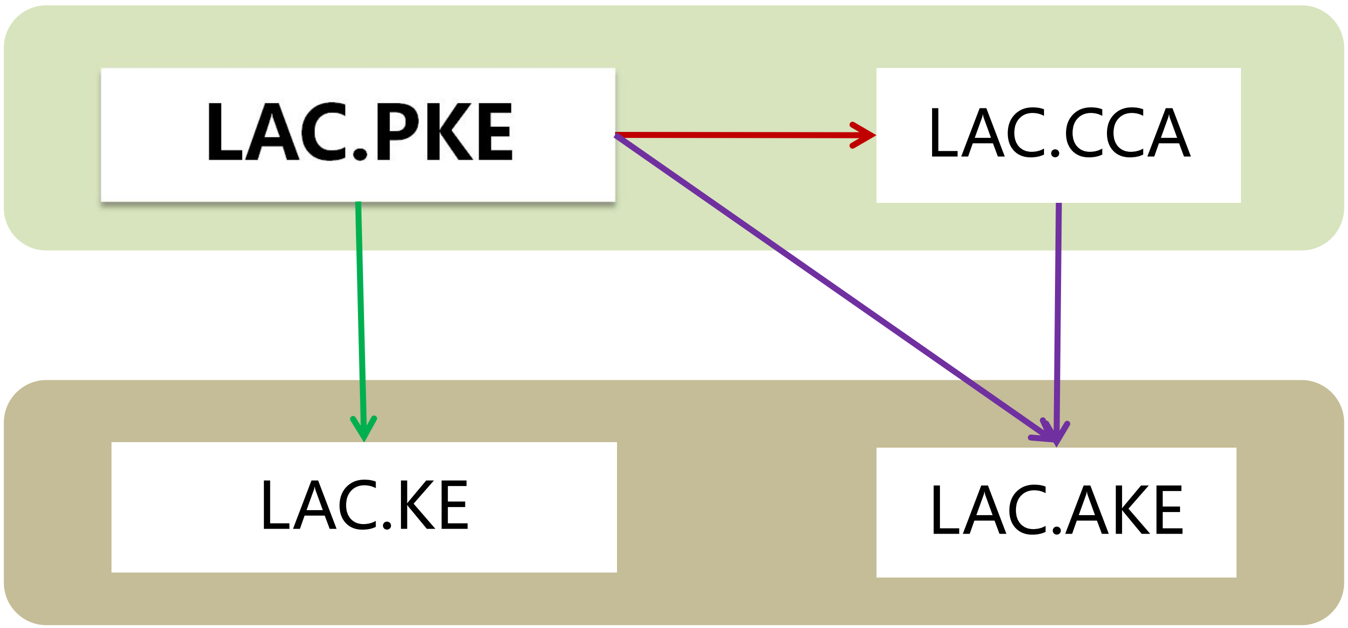
The Design of LAC

Xianhui Lu, Yamin Liu, Dingding Jia
Haiyang Xue, Jingnan He, Zhenfei Zhang

Overview of LAC



Overview of LAC



Main Features of LAC

$$pk = (\mathbf{a}, \mathbf{b} = \mathbf{a}\mathbf{s} + \mathbf{e}), sk = \mathbf{s}$$

$$\mathbf{a} \in Z_q[X]/X^n + 1,$$

$$q = 251(257), n = 512/1024, \mathbf{e}, \mathbf{s} \in \psi_1 \text{ or } \psi_{1/2}$$

$$\psi_1 : \Pr[x=0] = \frac{1}{2}, \Pr[x=-1] = \frac{1}{4}, \Pr[x=1] = \frac{1}{4}; \psi_{1/2} : \Pr[x=0] = \frac{3}{4}, \Pr[x=-1] = \frac{1}{8}, \Pr[x=1] = \frac{1}{8}$$

$$\mathbf{r} \leftarrow \mathrm{bch\_enc}(\mathbf{m})$$

$$\mathbf{c}_1 = \mathbf{s}'\mathbf{a} + \mathbf{e}', \mathbf{c}_2 = \mathbf{s}'\mathbf{b} + \tilde{\mathbf{e}} + \mathbf{r} \cdot q/2$$

small modulus q & large-block error correction code

Design Rationale of LAC: q<2^8

Target / Param	Security	Error Rate	Size	Performance
n	$n \log q$		As small as possible	As small as possible
q	$\frac{\sigma}{q}$	$\sigma^2\sqrt{2n} < \frac{q}{4}$	As small as possible	NTT q=c*n+1
σ			As small as possible	Gaussian Centre Binomial {-1,0,1}

Selection of q=251: largest prime<2^8

NewHope: $n=1024, \sigma=\sqrt{8}, q=12289$

Kyber: $n=256*3, \sigma=2, q=7681$

LAC: $n=512, \sigma=1/\sqrt{2}, q=251$

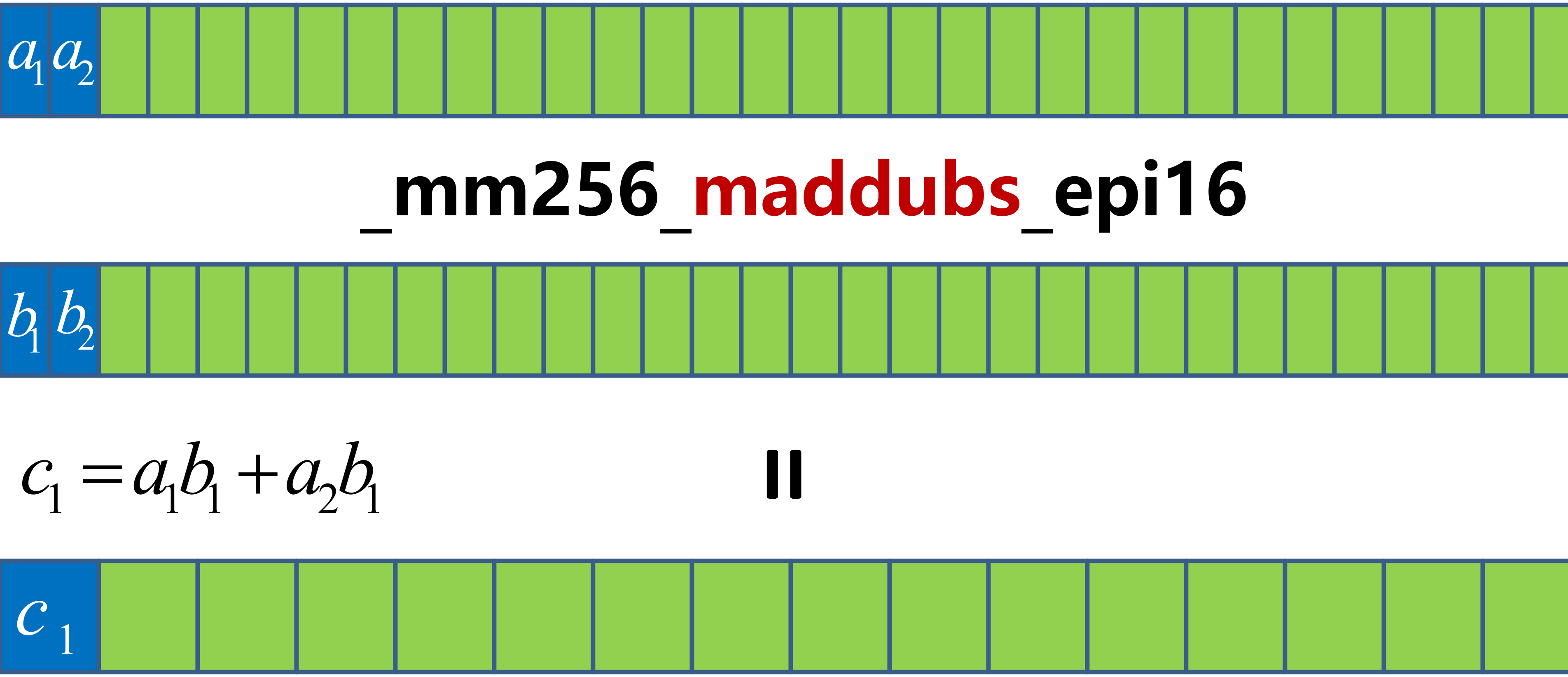
Security and Error Rate of q=251

q	**n**	σ	**Classical Security**	**Quantum security**	**Error rate (single bit)**
12289	1024	sqrt(8)	282	256	2^(-54)
12289	1024	1	218	198	negligible
12289	1024	1/sqrt(2)	201	182	negligible
251	**512**	1/sqrt(2)	**148**	**134**	**2^(-13.2)**
251	**1024**	1/sqrt(2)	**321**	**292**	**2^(-7.35)**

Decrease Error Rate with BCH

Categories	Parameters	Error correction
LAC-128	n=512,q=251 \psi_{1}	BCH(511,256,35) 2^-13.2->2^-128
LAC-192	n=1024,q=251 \psi_{1/2}	BCH(511,384,15) 2^-25->2^-143
LAC-256	n=1024,q=251 \psi_{1}	BCH(1023,512,115) 2^-7.35->2^-109

Multiplication without NTT



30 times speed up:
150 microseconds to 5 microseconds

Security Categories

	q	n	σ	Classical Security	Quantum security	claimed security
LAC-128	251	512	ψ_{1}	147	133	1,2
LAC-192	251	1024	$\psi_{1/2}$	286	259	3,4
LAC-256	251	1024	ψ_{1}	320	290	5

Performance (AVX2)

Intel Core-i7-4770S (Haswell) @ 3.10GHz, memory 7.6GB.

	performance (μs /cpu cycles)			Size	
	KeyGen	Enc	Dec	PK	Ciphertext
LAC128 CPA	**12.56** **38957**	**17.21** **53357**	**8.79** **27259**	**544**	**1024(768)**
LAC128 CCA	**12.53** **38847**	**19.66** **60952**	**24.13** **74812**	**544**	**1024(768)**
LAC192 CPA	**37.02** **114753**	**37.98** **117749**	**17.52** **54313**	**1056**	**1536(1280)**
LAC192 CCA	**36.92** **114461**	**42.61** **132087**	**73.89** **229054**	**1056**	**1536(1280)**
LAC256 CPA	**25.38** **78678**	**44.28** **137258**	**43.03** **133379**	**1056**	**2048(1536)**
LAC256 CCA	**25.23** **78214**	**51.77** **160489**	**94.56** **293128**	**1056**	**2048(1536)**

Comments(1): Subfield Attack

$$x^n + 1 = \left(x^{n/2} + 91x^{n/4} - 1\right)\left(x^{n/2} - 91x^{n/4} - 1\right) \bmod 251$$

$$g = x^{n/2} + 91x^{n/4} - 1$$

$$\mathbf{A} = \left[\mathbf{a} \bmod \mathbf{g} \mid \mathbf{1} \mid 11 * \mathbf{b} \bmod \mathbf{g}\right],$$

$$z = \left(11 * s \bmod g, 11 * e \bmod g, -1\right)$$

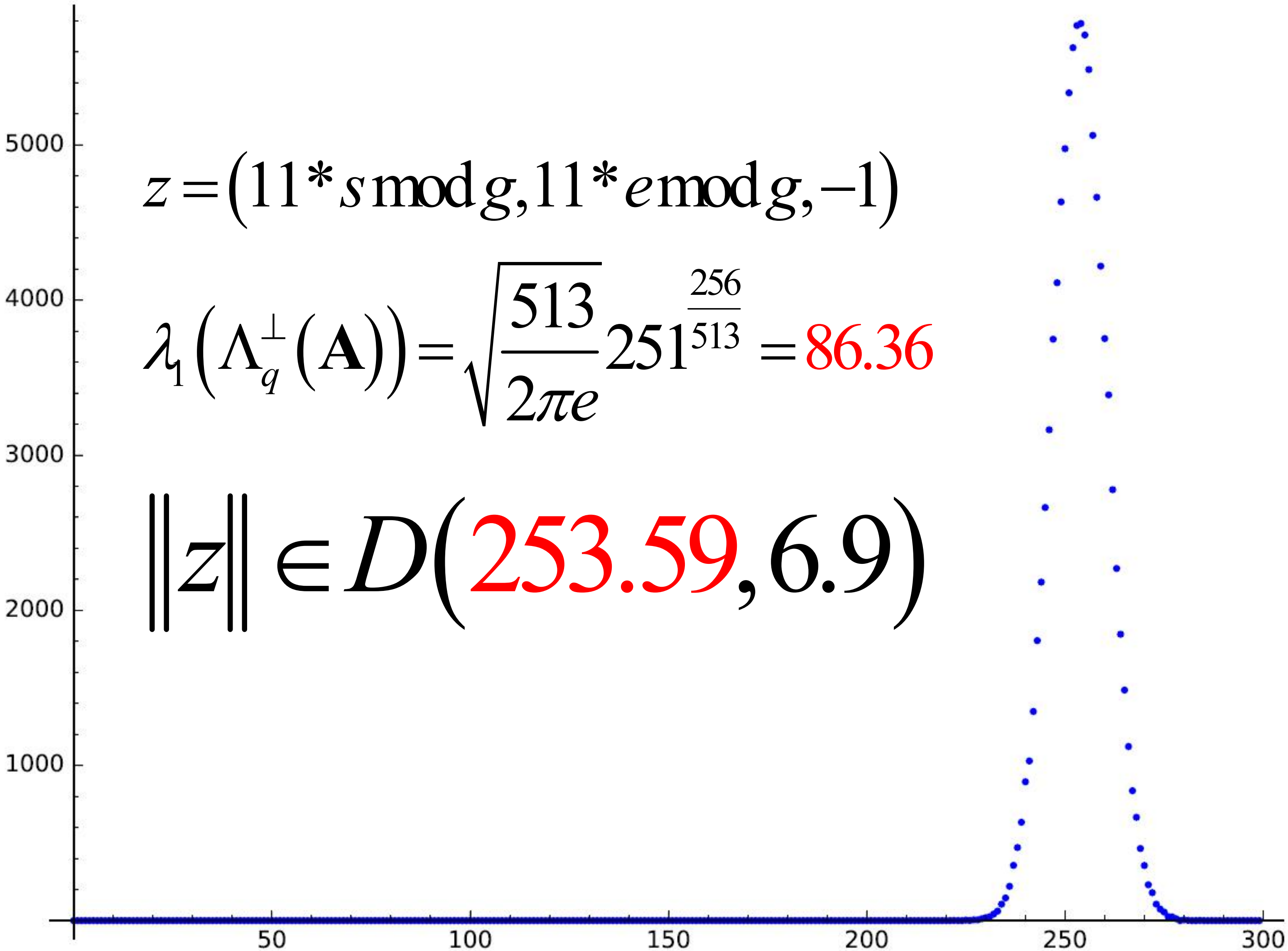
find $\mathbf{z}$ from lattice $\mathbf{Az}=0$ by using BKZ?

Comments(1): Subfield Attack

$$z = (11 * s \bmod g, 11 * e \bmod g, -1)$$

$$\lambda_1\left(\Lambda_q^{\perp}(\mathbf{A})\right) = \sqrt{\frac{513}{2\pi e}} 251^{\frac{256}{513}} = 86.36$$

$$\|z\| \in D(253.59, 6.9)$$



Comments(2): Worst case hardness

$$\psi_1 : \Pr[x=0]=\frac{1}{2}, \Pr[x=-1]=\frac{1}{4}, \Pr[x=1]=\frac{1}{4}, \sigma_1 = 1/\sqrt{2}$$

$$\psi_{1/2} : \Pr[x=0]=\frac{3}{4}, \Pr[x=-1]=\frac{1}{8}, \Pr[x=1]=\frac{1}{8}, \sigma_2 = 1/2$$

$$\text{Regev Reduction:} \alpha q \approx \sqrt{n}, \sigma = \frac{\alpha q}{\sqrt{2\pi}} \approx 9$$

$$\text{MP2013 Reduction:} e \leftarrow \{0,1\}, m = n\left(1+\Omega\left(1/\log n\right)\right)$$

Daniele Micciancio, Chris Peikert: Hardness of SIS and LWE with Small Parameters. CRYPTO (1) 2013: 21-39.

Comments(2): Worst case hardness

Broader perspective. As a byproduct of the proof of Theorem 1.1, we obtain several results that shed new light on the hardness of LWE. Most notably, our modulus reduction result in Section 3 is actually far more general, and can be used to show a "modulus expansion/dimension reduction" tradeoff. Namely, it shows a reduction from LWE in dimension n and modulus p to LWE in dimension n/k and modulus p^k (see Corollary 3.4). Combined with our modulus reduction, this has the following interesting consequence: the hardness of n-dimensional LWE with modulus q is a function of the quantity $n \log_2 q$. In other words, varying n and q individually while keeping $n \log_2 q$ fixed essentially preserves the hardness of LWE.

q=251,n=512, sigma=1/sqrt(2):	q=251*251, n=256, sigma= 1/sqrt(2) * 251:
primal attack:	primal attack:
classical cost= 148	classical cost= 156
quantum cost= 135	quantum cost= 141
dual attack:	dual attack:
classical cost= 147	classical cost= 154
quantum cost= 133	quantum cost= 139

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, Damien Stehlé: Classical hardness of learning with errors. STOC 2013: 575-584

Comments(3): CCA security

Main Idea: Find enough ciphertexts with Hamming weights of (r,e_1) of 1024+310, to cause decryption failure probability about 2^{-50.51}. Recover s as in https://eprint.iacr.org/2016/085.pdf.

Difficulty1: Any changes of the error-reconciliation vector will be rejected by the re-encryption process in the decryption algorithm.

Difficulty2: (r,e_1) are generated by the hash function, can not be set as special vectors used in https://eprint.iacr.org/2016/085.pdf.

Comments(4): error correction code

BCH, Goppa,……

Martin Tomlinson: One significant advantage is that you can benefit from the extensive research in the last decade that has been applied to the McEliece system to avoid side channel information leakage in the syndrome calculation, Berlekamp-Massey and root finding algorithms.

Thanks