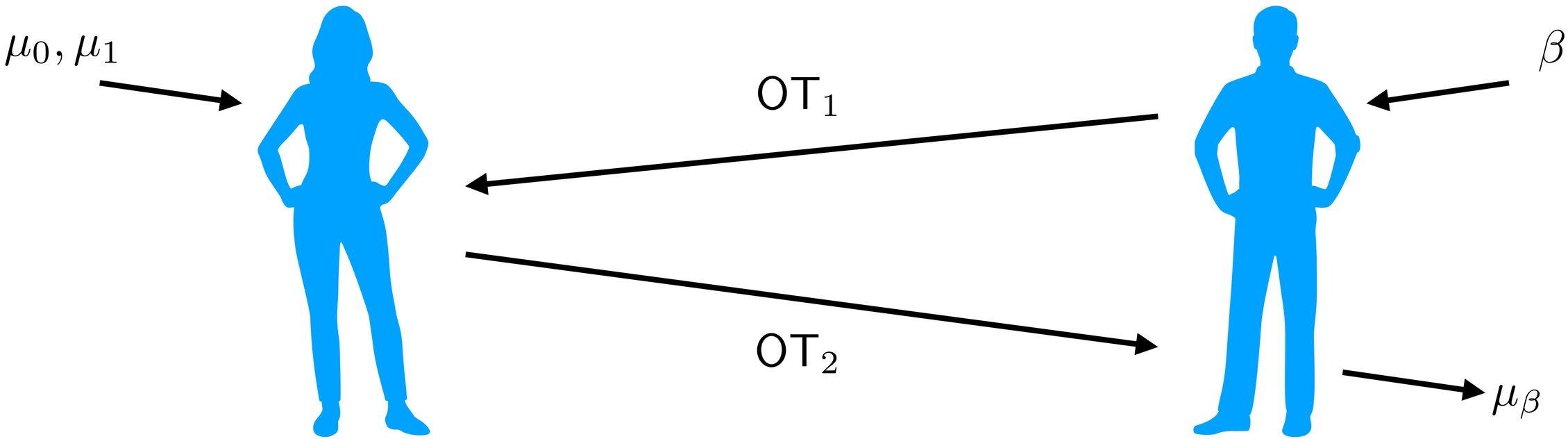
# Two-Message Statistically Sender-Private OT from LWE

Zvika Brakerski* and Nico Döttling†
*Weizmann Institute of Science
†~~FAU Erlangen-Nürnberg~~ —> Cispa Helmholtz Center

# 2-Message Oblivious Transfer



# 2-Message Oblivious Transfer: Security

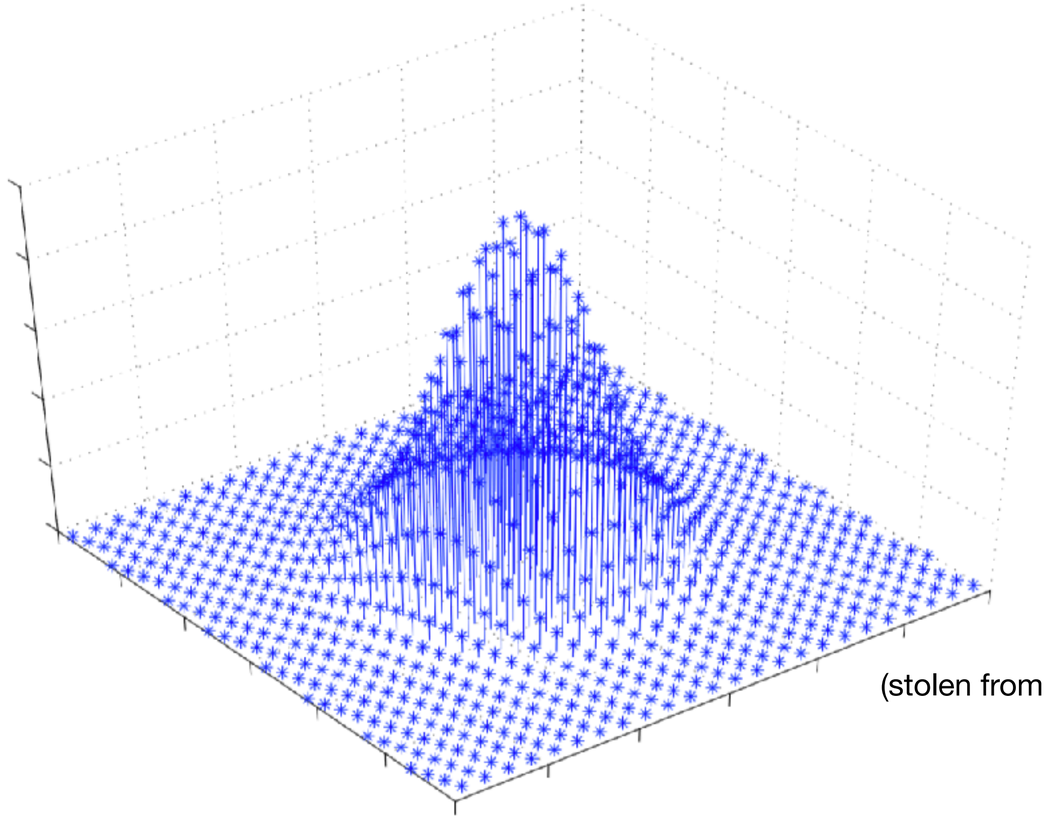
- Computational Receiver Security (best-possible): $ot_1$ computationally hides choice bit $\beta$
- Statistical Sender Security: There exists an unbounded extractor OTExt such that Sender($ot_1, \boldsymbol{\mu}_0, \boldsymbol{\mu}_1$) $\approx_s$ Sender($ot_1, \boldsymbol{\mu}_{\beta'}, \boldsymbol{\mu}_{\beta'}$) where $\beta'$ = OTExt($ot_1$)

# Maliciously Secure 2-round OT

- Useful primitive: 2-message WI proofs [BGI+17,JKKR17,KKS18], maliciously circuit-private FHE [GHV10,OPP14],…
- First instantiation: [NP01,AIR01] from DDH
- Also known from Hash-Proof Systems (e.g. QR/DCR) [Kal05,HK12,…]
- 0/1-nature of number-theoretic languages in these constructions is essential

# Discrete Gaussians on $\mathbb{Z}^m$

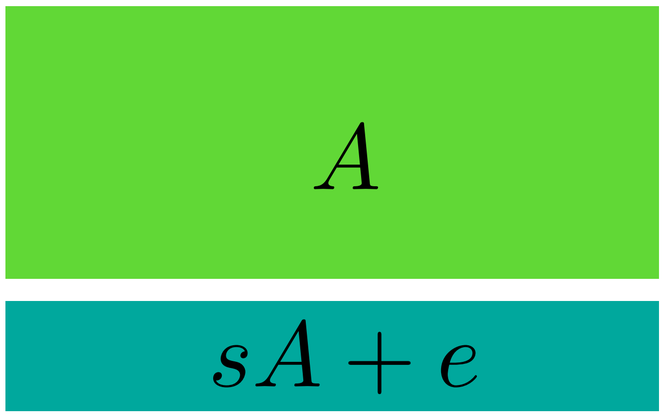
$$\rho_s(x) = e^{-\pi \cdot \frac{\|x\|^2}{s^2}}$$



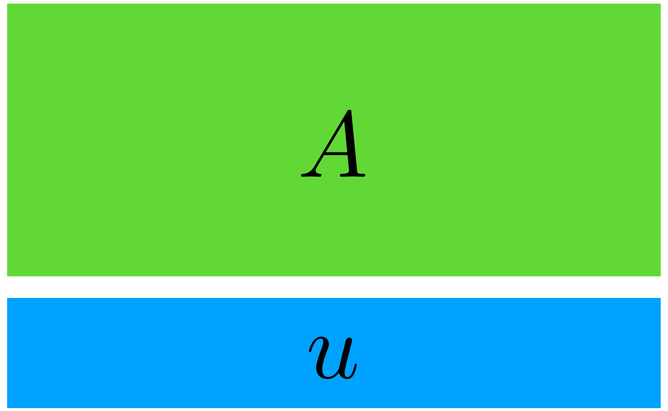
(stolen from MR04)

$$X \sim D_{\mathbb{Z}^m, s} \qquad \text{has pmf} \qquad \Pr[X = x] = \frac{\rho_s(x)}{\rho_s(\mathbb{Z}^m)}$$

# Learning With Errors




$\approx_c$




where

$$A \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$$
$$s \leftarrow_{\$} \mathbb{Z}_q^{n}$$
$$e \leftarrow_{\$} \chi$$
$$u \leftarrow_{\$} \mathbb{Z}_q^{m}$$

$\chi$ is B-bounded

# Primal Regev Encryption, GPV08 version

pk $A = \begin{array}{|c|}\hline A' \\ \hline a' = sA + e \\ \hline \end{array}$

sk $\begin{array}{|c|c|}\hline -s & 1 \\ \hline \end{array}$

Enc $c \leftarrow A \cdot x + \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hat{\mu} \end{pmatrix}}_{ECC(\mu)}$

where

$x \leftarrow_{\$} D_{\mathbb{Z}^m, \sigma_0}$

$\hat{\mu} \leftarrow \frac{q}{2} \cdot \mu$

# Decryption

$$\begin{bmatrix} -s & 1 \end{bmatrix} \begin{bmatrix} c \end{bmatrix} = -sAx + sAx + ex + \frac{q}{2}\mu = \frac{q}{2}\mu + ex$$

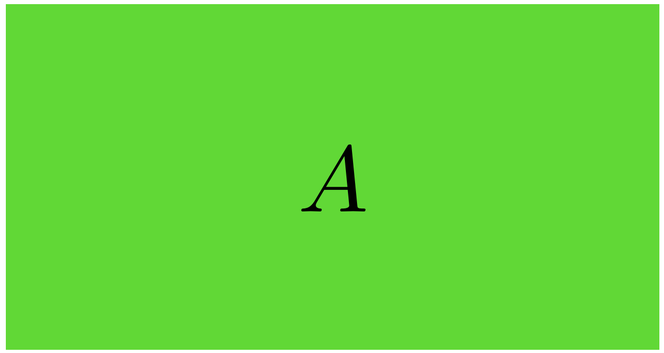
e*x smaller than q/4 ⇒ msb is $\boldsymbol{\mu}$

Cauchy-Schwarz $|e \cdot x| \leq \|e\| \cdot \|x\| \leq B \cdot \sigma_0 \cdot m$

⇒ Scheme correct if $\sigma_0 \leq \frac{q}{4Bm}$

# Dual Regev Trapdoor Function [GPV08]

pk




td

[Ajt99,MP12]: A statistically close to uniform over $\mathbb{Z}_q^{(n+1)\times m}$

Eval(A,r,$\eta$): $y \leftarrow rA + \eta$

where $r \leftarrow_\$ \mathbb{Z}_q^{n+1}$

$\eta \leftarrow_\$ D_{\mathbb{Z}^m,\sigma_1}$

Trapdoor Inversion:

$s \leftarrow \mathsf{Decode}(td, y)$

Correct if $\|\eta\| \leq \frac{q}{\tilde{\Omega}(\sqrt{m})} \Leftrightarrow \sigma_1 \leq \frac{q}{\tilde{\Omega}(m)}$

# A simple Idea

- What happens if we us one and the same matrix A as public key in primal Regev encryption and the dual Regev TDF?

- Given a key A, compute two “ciphertexts”:
  - c = Enc(A, $\mu$)
  - y= Eval(A,r,$\eta$)

- Clearly, if A is a public key for primal Regev, we can recover $\mu$

- Likewise, if A is a public key for dual Regev, we can recover r

# A simple idea

- What happens in the other cases?
- Consider the lattice

$$\Lambda_q(A) = \{z \in \mathbb{Z}^m : \exists v \in \mathbb{Z}_q^n \text{ s.t. } z = vA \ (mod\ q)\}$$

- Observervation: If A is an honestly generated primal Regev key, then $\boldsymbol{\Lambda}_q$(A) contains an unusually short vector
- Conversely, if A is an honestly generated dual Regev key, then $\boldsymbol{\Lambda}_q$(A) does not have short vectors (e.g. via transference, counting argument etc.)

# Smoothing [MR04]

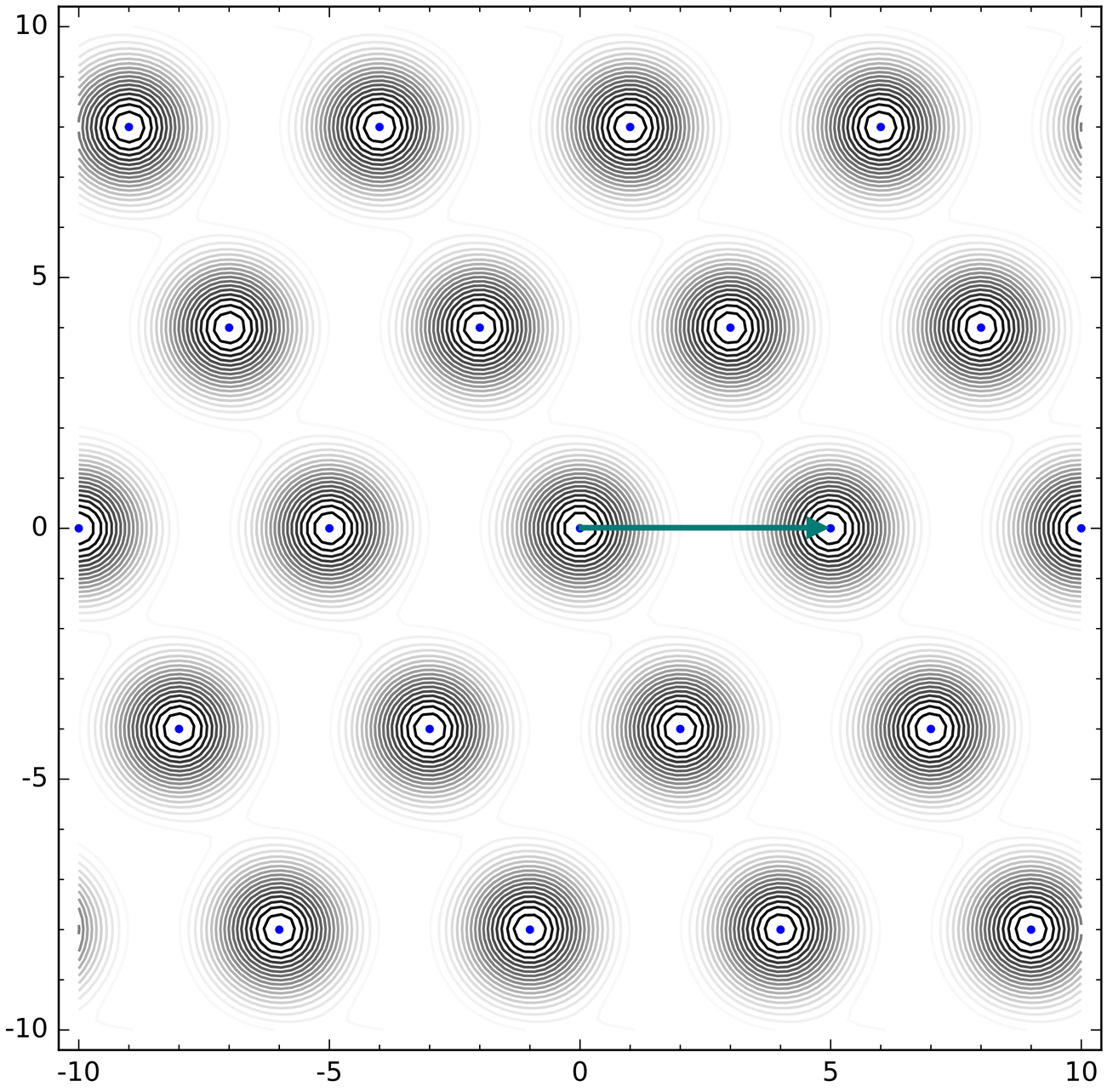
If $\sigma_0 > \frac{q \cdot \sqrt{m}}{\lambda_1(\Lambda_q(A))} \geq \eta_\epsilon(\Lambda_q^\perp(A))$

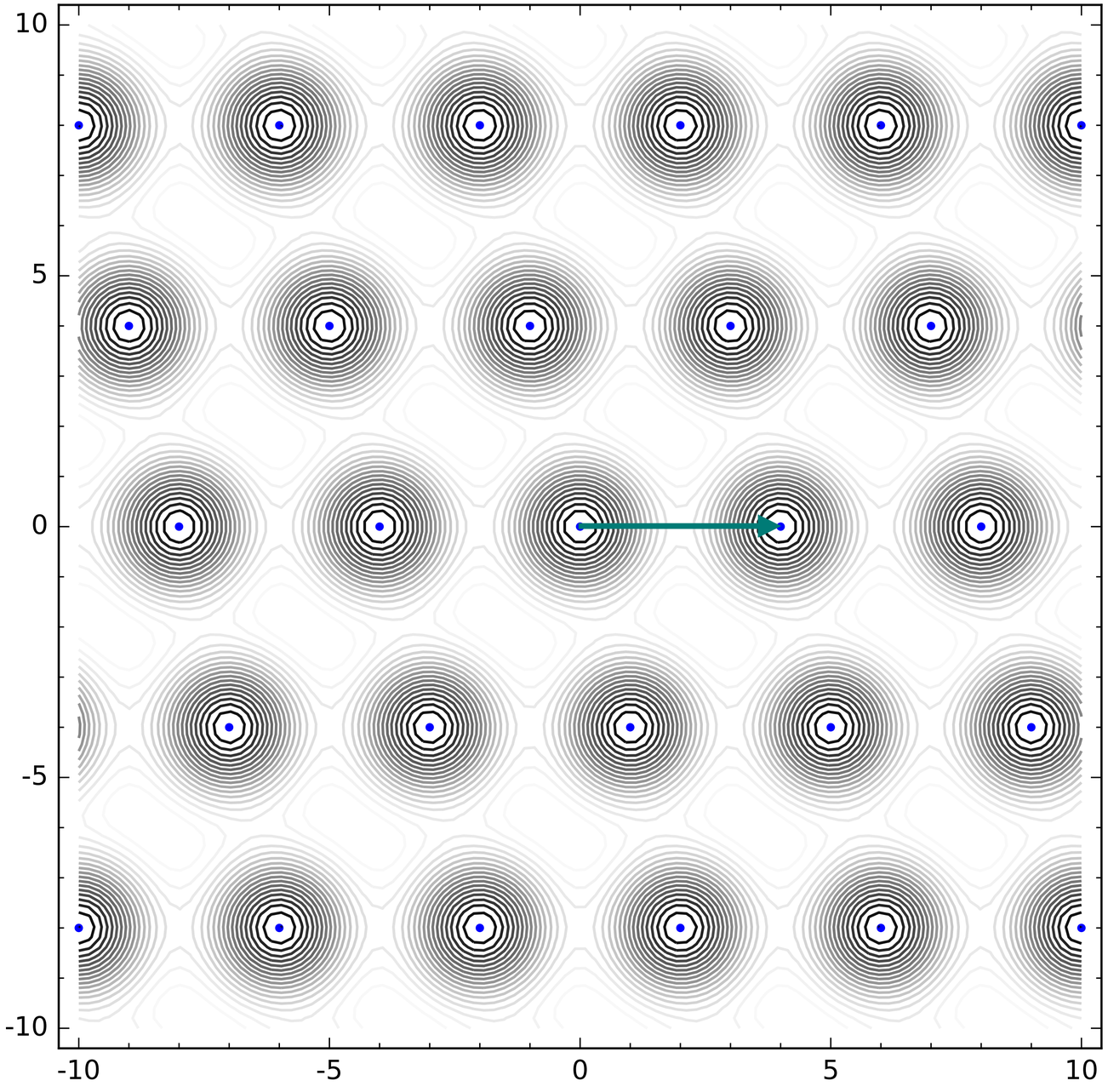
then $A \cdot x \approx_\epsilon u \ (mod\ q)$

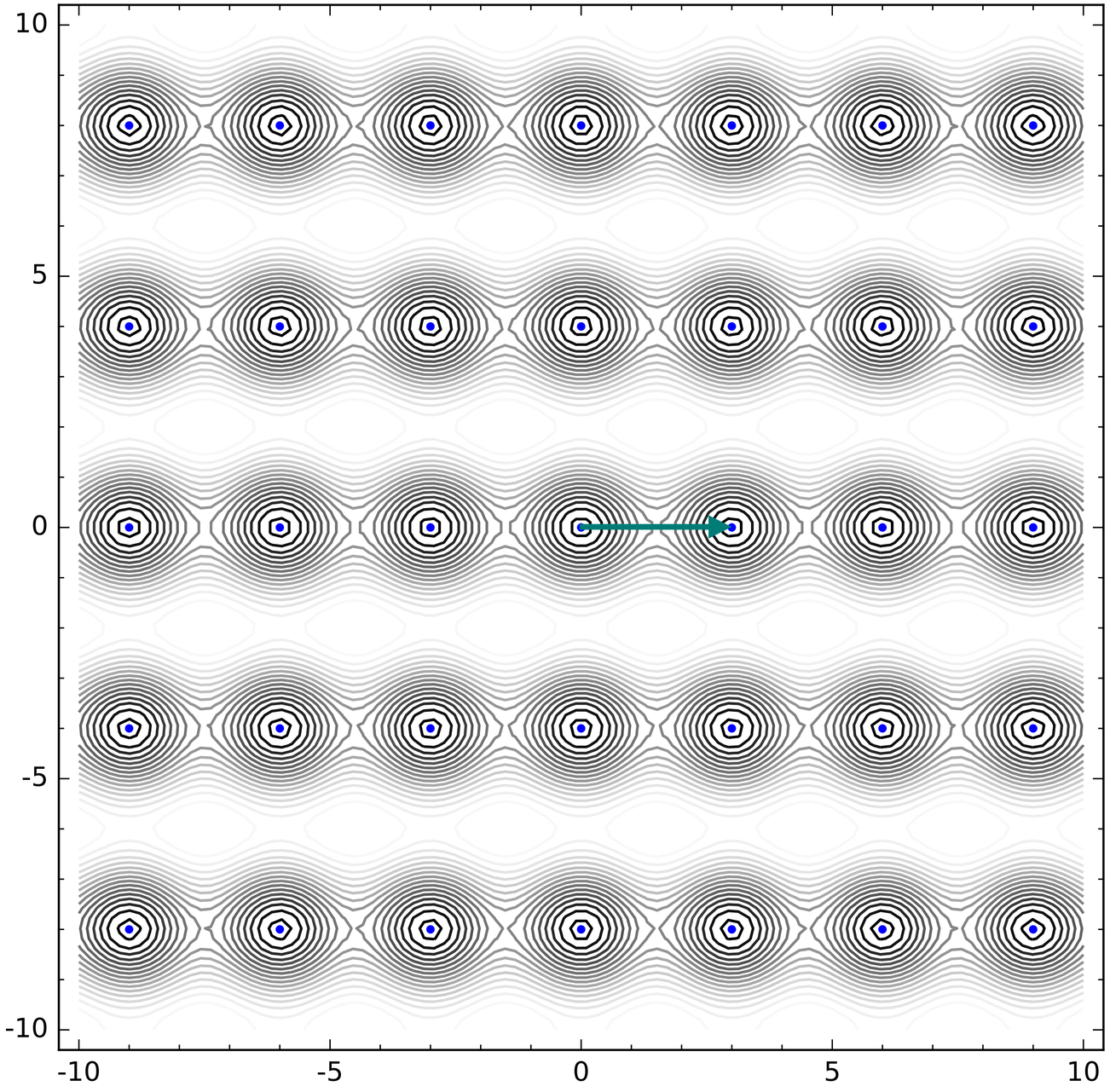
thus $c = Ax + ECC(\mu)$ statistically hides $\boldsymbol{\mu}$

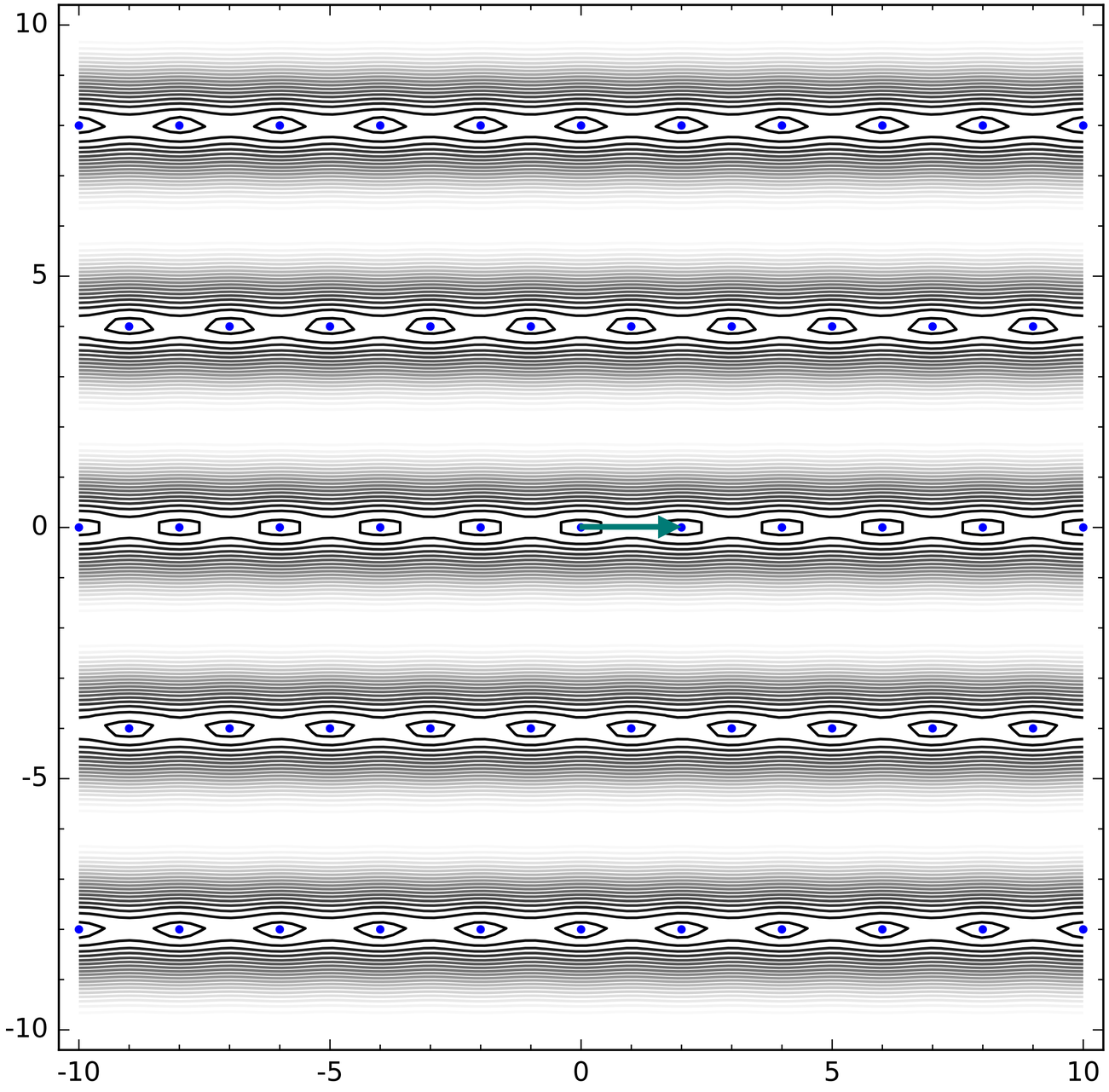
# Lossiness

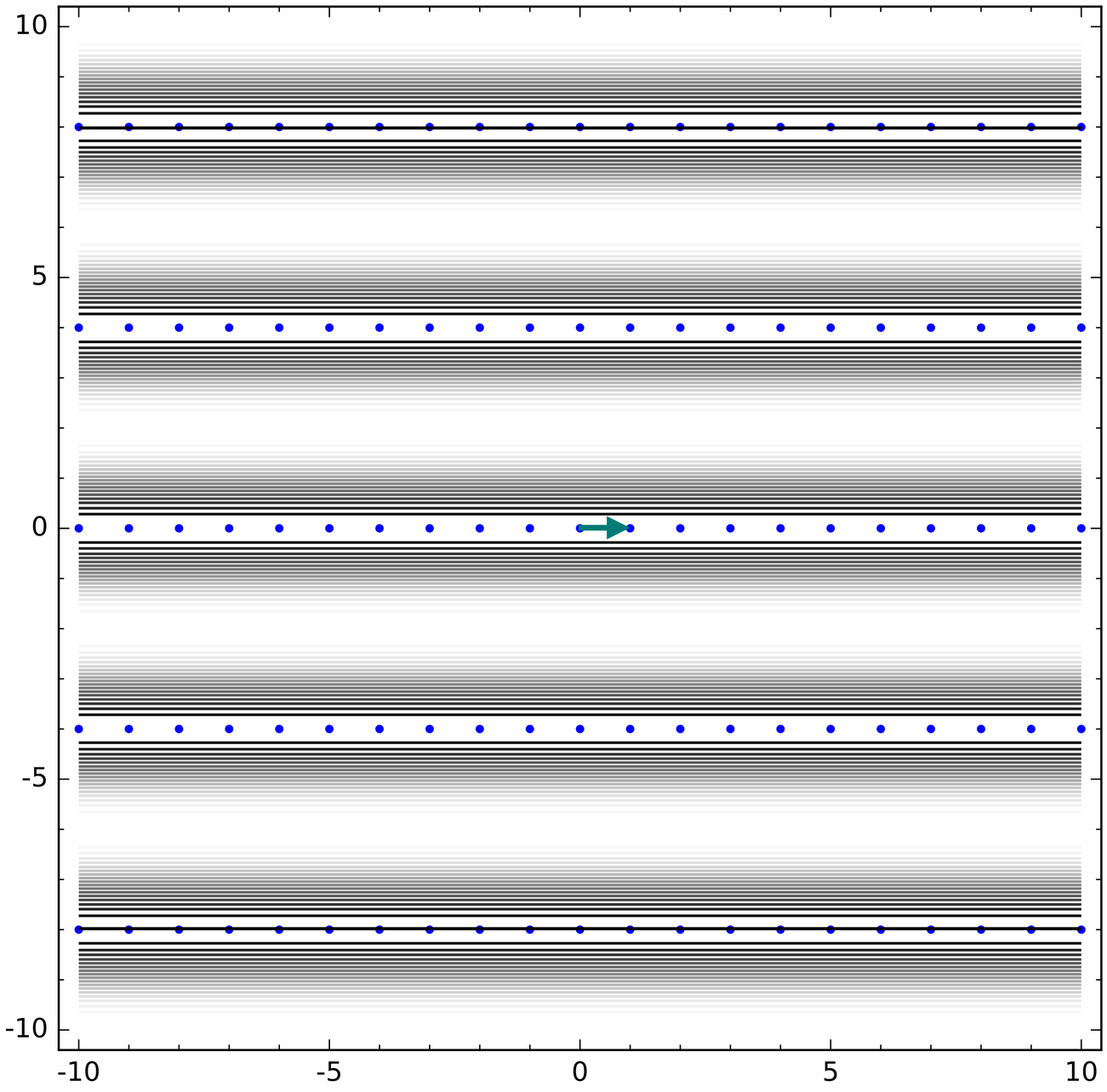
- [GG98,CDLP13]: AM protocols for gap-SVP
- Idea: If Lattice contains a short vector, then adding a sufficiently wide gaussian to a “random” lattice point is lossy
- Can turn this into lossiness argument for dual Regev


10
5
0
-5
-10
-10
-5
0
5
10


10
5
0
-5
-10
-10
-5
0
5
10


10
5
0
-5
-10
-10
-5
0
5
10


10
5
0
-5
-10
-10
-5
0
5
10


10
5
0
-5
-10
-10
-5
0
5
10

# Lossiness of Dual Regev

## (using techniques from [CDLP13])

If $\sigma_1 > 2 \cdot \lambda_1(\Lambda_q(A))$

then $\tilde{H}_\infty(r \mid rA + \eta) > 1 - \text{negl}$

Thus

$$\tilde{H}_\infty((r_1, \ldots, r_\ell) \mid r_1 A + \eta_1, \ldots, r_\ell A + \eta_\ell) > \ell - \text{negl}$$

# Making the cases overlap

Smoothing: $\lambda_1(\Lambda_q(A)) > \dfrac{q \cdot \sqrt{m}}{\sigma_0}$

Lossiness: $\lambda_1(\Lambda_q(A)) < \dfrac{\sigma_1}{2}$

One of the cases must occur if $\dfrac{\sigma_1}{2} > \dfrac{q \cdot \sqrt{m}}{\sigma_0}$

i.e. $\sigma_0 \cdot \sigma_1 > 2q\sqrt{m}$

# A simple scheme

A

B

If $\beta = 0$:

$(A, s) \leftarrow \mathsf{PR.KeyGen}(1^\lambda)$

If $\beta = 1$:

$(A, td) \leftarrow \mathsf{DR.KeyGen}(1^\lambda)$

$A$

$c_0 \leftarrow \mathsf{PR.Enc}(A, \mu_0)$

$\forall i \in [\ell] : y_i \leftarrow r_i A + \eta_i$

$c_1^* \leftarrow Ext(r_1, \ldots, r_\ell) \oplus \mu_1$

$c_1 \leftarrow (y_1, \ldots, y_\ell, c_1^*)$

$(c_0, c_1)$

If $\beta = 0$:

$\mu_0' \leftarrow \mathsf{PR.Dec}(s, c_0)$

If $\beta = 1$:

$\forall I \in [\ell] : \; r_i \leftarrow \mathsf{DR.Decode}(td, y_i)$

$\mu_1 \leftarrow c_1^* \oplus Ext(r_1, \ldots, r_\ell)$

# Correctness

- Primal Regev correct given $\sigma_0 \leq \frac{q}{4Bm}$
- Dual Regev correct given $\sigma_1 \leq \frac{q}{\tilde{\Omega}(m)}$

# Security

- Receiver Security: LWE
- Sender Security: Statistical by the above reasoning: $\sigma_0 \cdot \sigma_1 > 2q\sqrt{m}$
- $\lambda_1(\boldsymbol{\Lambda}_q(A))$ is very short ⇒ dual Regev is lossy ⇒ Ext($s_1$,…,$s_l$) is statistically close to uniform and hides $\boldsymbol{\mu}_1$
- $\lambda_1(\boldsymbol{\Lambda}_q(A))$ is not short ⇒ primal Regev statistically hides $\boldsymbol{\mu}_0$

# Instantiation

$q = \tilde{O}(n^3)$

$m = \tilde{O}(n)$

$\sigma_0 = \tilde{O}(n^{2.5})$

$\sigma_1 = \tilde{O}(n)$

This yields worst-case approximation factor $\tilde{O}(n/\alpha) = \tilde{O}(n^{3.5})$

# Drawbacks

- Scheme has very poor rate (1/poly) due to amplification for case $\beta = 1$
- Security is *very unbalanced*: $\beta = 0$ has very good security right away whereas $\beta = 1$ needs to be amplified via parallel repetition and extractors?
- Can we balance things such that both cases need to be a little bit amplified?

# A more efficient scheme (Teaser only)

Ideas

- $\beta = 0$ : Packed primal Regev encryption
- $\beta = 1$: Single instance of dual Regev TDF
- Use extractors in both cases

# A more efficient scheme

- Lossiness argument in case $\beta = 1$ generalizes robustly to lattices $\boldsymbol{\Lambda}_q(A)$ with many linearly independent short vectors

$$\tilde{H}_\infty(r \mid rA + \eta) \approx \log(\rho_{\sigma_1}(\Lambda_q(A)))$$

- similar to [DM13]
- Smoothing argument requires some refinement
- We obtain a scheme of rate $\tilde{\Omega}(1)$

# Partial Smoothing

- Cannot guarantee uniformity of Ax mod q if $\boldsymbol{\Lambda}_q(A)$ contains short vectors
- However: If $\boldsymbol{\Lambda}_q(A)$ contains sufficiently few linearly independent short vectors, then Ax mod q is uniformly random in a subspace

**Corollary 4.2.** *Let $q > 0$ be an integer and let $\gamma > 0$. Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and let $\sigma > 0$ and $\epsilon > 0$ be such that $\rho_{q/\sigma}(\Lambda_q(\mathbf{A}) \backslash \gamma\mathcal{B}) \leq \epsilon$. Let $\mathbf{D} \in \mathbb{Z}_q^{k \times m}$ be a full-rank (and therefore minimal) matrix with $\Lambda_q^{\perp}(\mathbf{D}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \forall \mathbf{y} \in \Lambda_q(\mathbf{A}) \cap \gamma\mathcal{B} : \langle \mathbf{x}, \mathbf{y} \rangle = 0 \pmod q\}$. Let $\mathbf{x} \xleftarrow{\$} D_{\mathbb{Z}^m,\sigma}$ and $\mathbf{u} \xleftarrow{\$} \Lambda_q^{\perp}(\mathbf{D}) \bmod q$. Then it holds that*

$$\mathbf{A}\mathbf{x} \bmod q \approx_{\epsilon} \mathbf{A} \cdot (\mathbf{x} + \mathbf{u}) \bmod q.$$

# Summary

- First two-round malicious OT scheme w/o setup from non-numbertheoretic assumptions
- Standard LWE with poly approximation factor
- Optimized scheme with rate $\tilde{\Omega}(1)$

# Thanks!

*Coming soon to an eprint server near you!*