Boosting the Hybrid Attack on NTRU: Torus LSH, Permuted HNF and Boxed Sphere

Phong Nguyễn

Inria
INVENTORS FOR THE DIGITAL WORLD

1794
ENS
ÉCOLE NORMALE SUPÉRIEURE

erc
European Research Council
Established by the European Commission

Targets

- NTRU
- Any lattice cryptosystem using q-ary lattices with very short vectors: binary LWE, etc.

The Hybrid Attack

- Introduced by [HG-2007] to combine Odlyzko's meet-in-the-middle attack with lattice reduction.
- Sometimes the best attack on NTRU, e.g. some settings of NTRU-HSS.
- Arguably ``poorly" understood.

Our Results

- Improve the hybrid attack and its analysis
  - Easier to implement, more efficient
  - Less heuristic analysis
  - Bigger experiments
- Probabilistic analysis of Babai's nearest plane algorithm

Application to NTRU

- NTRU's security estimates for the hybrid attack are wrong: overestimating both the success probability and the MITM cost.

	hps2048509	hps2048677	hps4096821
MITM cost overestimate	2^{8}	2^{16}	2^{3}
Proba overestimate	$[2^{46},2^{76}]$	$[2^{55},2^{89}]$	$[2^{72},2^{115}]$

NTRU Submission Issues

- Inconsistency with NTRU scripts: different values of s; swap of f and g.
- No rationale for several conditions
  - $||b_d^*|| \geq 2s$ is not justified: it looks arbitrary.

Randomizing the Hybrid Attack

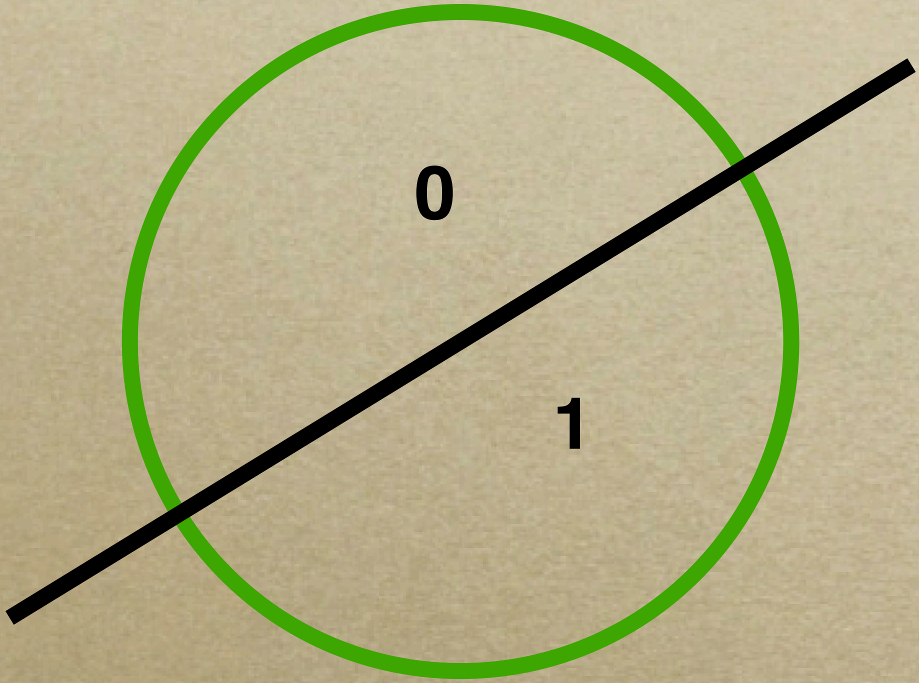
Randomization

- The hybrid attack is essentially deterministic: only the lattice reduction part brings randomness.
- We add randomization to improve the analysis and the success probability.
  - Torus Locality-Sensitive-Hashing (LSH)
  - Permuted HNF

Odlyzko's Attack

- $g=hf \bmod (q,X^N-1)$ where f,g ternary
- If $f=f_1-f_2$ then $g=hf_1-hf_2 \bmod (q,X^N-1)$ so hf_1 and hf_2 are close mod q: near-collisions detected with a **variable-output-size** function.
- **Torus-LSH** uses a **random** hash function H such that $H(hf_1)=H(hf_2)$ with high probability.

Halving a Torus



Integers mod q

The Hybrid Attack

- Replace the decomposition $f=f_1-f_2$ by a partial decomposition f_1-f_2 over the last k coordinates of f.
- Lattice reduction can combine it with Torus-LSH if a certain condition holds.

Permuted HNF

- Instead of the last k coordinates of f, target any k coordinates of (f,g): much more efficient if g is sparser than f, e.g. NTRU-HSS.
  - Permute the coordinates
  - Extract the HNF
  - Repermute the coordinates

Cleaning Up the Success Probability

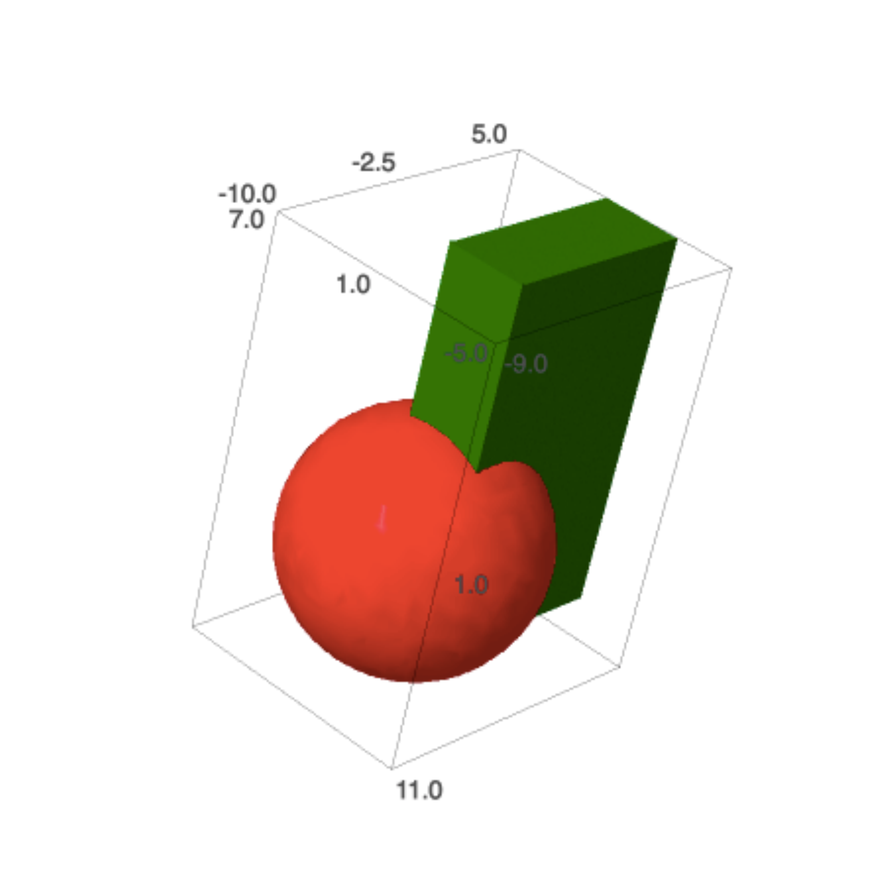
Success Probability

- It depends on the so-called admissibility condition [HG07].
  - Only heuristic estimates proposed: assume independence of coordinates.
  - Very limited experiments.
  - Ignored by the NTRU submission.

Geometric Insights

- Analyze the success probability of Babai's nearest plane algorithm to solve BDD with a spherical noise.
- Generalization to admissibility.

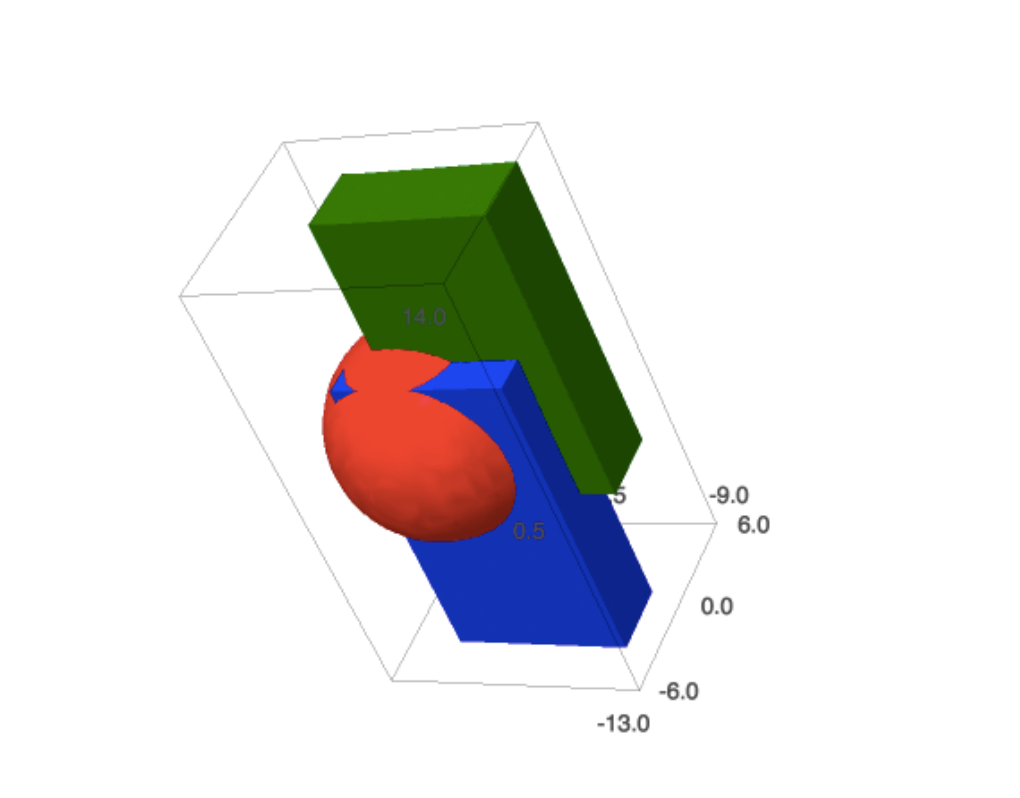
Sphere Fraction in a Box



- box = Gram-Schmidt parallelepiped of the reduced basis
- sphere = noise

- The worst-case analysis is not tight: Most of the unit-sphere is inside a cube $[-c,c]^n$ for some $c \sim 2\log(n)/\sqrt{n}$

Random Sphere Fraction



- Success probability obtained by shifting the centered box by a random point in the box: significantly decreases the fraction.

Our results

- Fast rigorous bounds on the sphere/box fraction
- A polynomial-time approximation based on Fourier series, expanding [AN17]
- Simpler and faster heuristic estimates

Conclusion

- Faster and cleaner hybrid attack
  - Larger experiments, e.g. NTRU-107 with BKZ-20.
- NTRU's security estimates for the hybrid attack should be ignored: actual figures don't compete with the primal attack.