A Quantum Algorithm for a Variant of LWE

Pierre Karpman

Totally not the DGSE

Jérôme Plût

Totally not the DGSE
(Really!!)

Hanoi
2016–12–06

Learning With Errors: the medium-characteristic case

- **Question: how to give practical LWE parameters?**

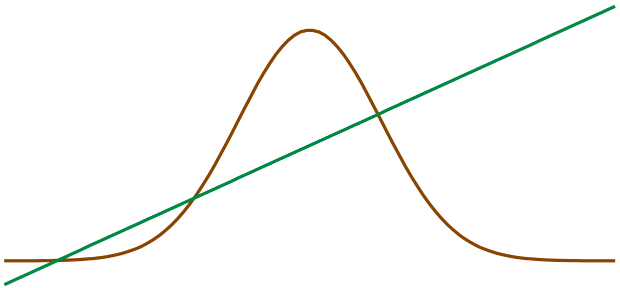
- We give a new parametrization of the Learning With Errors problem.
- Interesting parameters are:
  - dimension n;
  - real noise parameter σ;
  - prime modulus p (also called the *characteristic*).
  - the volume $q = p^n$.
- The **medium-characteristic cases** of LWE correspond to the moduli such that

$$p \approx \exp q^{1/3} (\log q)^{2/3}.$$

- We now repair the Eldar-Shor quantum LWE solver in the medium-characteristic cases.
  - We needed **slightly more** than the allowed 10 frames to prove this; we hope that Steven did not cut anything too important...

Use the (Well-known) Group Law over a Gaussian

- Add a point at infinity $\mathscr{O}$ to a Gaussian.
- Derive a group law using a chord-and-tangent process:



- $\Rightarrow$ The Gaussian cycles at ∞
- $\Rightarrow$ Can use Shor's order-finding algorithm

A Fundamental Lemma (17/17)

... Combining (12) with the smoothness of 24 we get:

$$\frac{1}{2} + \Re(\langle \psi \mid [2i]P \oplus e^{2i\pi\langle P[7], s+\widehat{e}=2.7\rangle} \mid \psi' \rangle - \frac{3}{4}$$

$$\leq$$

$$\sum_{\infty} \sum_{\eta \in \mathbb{F}_1} \langle \mathscr{G}(\sigma, \eta + \infty) \times \mathbb{Z} \rangle \cdot \sqrt{1 + [H_n < 5]} \cdot \frac{1}{n} \cdot \sqrt{s^2 - e_{[3i]}(\psi^t, \phi)}$$

$$\leq$$

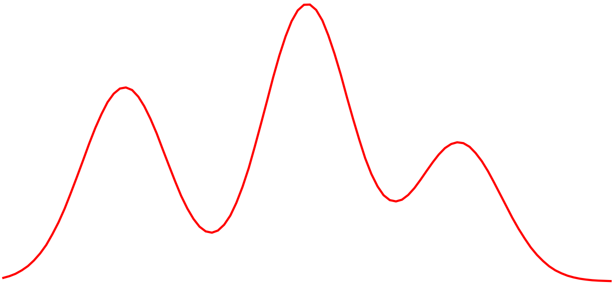
$$2\pi r$$

□

(r: radius of the fundamental circle)

Immediate Corollary

- The attack also works for Gaussian varieties of higher genus.



A simple proof of a useful inequality

- **Lemma:** $\frac{1}{4} > 0$.
  - Proof: $\frac{1}{4} = \left(\frac{1}{2}\right)^2$, which is a square.
  - Also, there is a field with 4 elements, and no field with 0 elements, so that $4 \neq 0$, so that $\frac{1}{4}$ exists (and is $\neq 0$).
  - (this non-constructive proof of existence of $\frac{1}{4}$ is enough for us).
- From the Lemma we deduce that, for any integer n, $\left(\frac{1}{4}\right)^n > 0$.
- Summing the geometric series we obtain:

$$\sum_{n \geqslant 1} \frac{1}{4^n} = \frac{\frac{1}{4}}{1 - \frac{1}{4}} = \frac{1}{3} > 0.$$

- We obtain the following:

Proposition

The following inequality is true: $\frac{1}{3} > 0$.

A proof of the Goldbach conjecture

- Up to now, the best known result on Goldbach is due to [Ramaré 95]:

  every even number is the sum of at most six primes.

- Dividing by three, we see that one third of every even number is the sum of at most one third of six primes.
- But one third of six is exactly two! *←factorial*
- In other words, the probability that an even n is the sum of two primes is $\geqslant \frac{1}{3}$.
- Since $\frac{1}{3} > 0$ (as was proved previously), we can rewind and replay the proof enough times until this eventually happens.

- We just proved the Goldbach theorem!

Solving TWE in any dimension

Put together, frames #14, #17 and #29 solve the "Teaching With Errors" problem when the dimension is prime. We now generalize the proof to any dimension n.

- **(Easy case).** Assume n is even. Then, by Euler-Goldbach, we can write $n = p + p'$.
  - By the extension theorem (Karatsuba-Strassen: we can trade expensive composites for cheaper primes assuming), we can combine a solution for p and one for p' into a solution for n.
- **(Hard case).** Now assume that n is odd.
  - It is possible, in probabilistic polynomial time, to find some $n' \geqslant n$ which is even.
  - (for example, pick $n' \geqslant n$ uniformly random until n' is even).
  - The inclusion principle allows us to pull back a solution for n' to a solution for n.

Final summary (1/2)

- From LWE in mid-characteristic to Goldbach's strong theorem back to TWE in even and odd prime cases and then any natural
- Subsumes much of 21st+ century computer science & mathematics

- The proof can be made very compact (≈ 1 frame) using notation from frame #278, as follows:

And the job is done!

- TWE $\Rightarrow$ P = NP (Thm. 7.α) $\Rightarrow$...