pqNTRUSign: update and recent results

Jeff Hoffstein, Jill Pipher, William Whyte and Zhenfei Zhang
- You may know us as **Security Innovation** …
  - who owns IP of NTRU
- NTRUEncrypt patent released to public domain – March 2017
- Security Innovation (Embed business unit)
Modular lattice signature scheme

- For a given $L$ and a document $m$, its signature is a vector $v$
  - $v \in L$ can be generated efficiently with a trapdoor of $L$
  - $v = \text{hash}(m|L) \mod p$ for some $p$
  - Forgery = solving approx.-SVP for $L$

- pqNTRUSign is a modular lattice signature with $L = \text{NTRU lattice}$
  - Easy construction of trapdoors
  - Fast implementation
pqNTRUSign: Sign

- Input a hash function, \( m, (pf, g), h \)
  - \((s_p, t_p) = \text{hash}(m|h)\)  \# hash the message and PK into a mod \( p \) vector
  - \( r \leftarrow \text{Sampler} \)  \# generate a mask vector from certain sampler
  - \( s_0 = pr + s_p \)  \# \( s_0 \equiv s_p \mod p \)
  - \( t_0 = s_0h \)  \# \((s_0, t_0)\) is a lattice vector
  - \( a = (t_p - t_0)g^{-1} \mod p \)
  - \((s_1, t_1) = a(pf, g)\)  \# \( t_0 + t_1 \equiv t_p \mod p \)
  - \((s, t) = (s_0, t_0) + (s_1, t_1)\)

- Repeat above steps with rejection sampling

- Output \((s, t)\)
pqNTRUSign: verify

- Input \((s, t), m, h\)
  - Check \((s, t) = \text{hash}(m|h) \mod p\)
  - Check \(||(s, t)||_\infty\) is within some bound
  - Check \(t = sh\)
pqNTRUSign: rejection sampling

- **Uniform distribution:**
  - Reject \((s, t)\) when \(\| (s, t) \|_\infty > \frac{q}{2} - B\) for some bound \(B\)
  - High rejection rate, large sig. size \(\approx n\log_2 q\)

- **(bimodal) Gaussian distribution:**
  - Reject \(s\) with probability \(e^{\left(\frac{-2(r+af)af+\|af\|_2}{2\sigma^2}\right)}\)
  - Reject \(t\) when \(\|t\|_\infty > \frac{q}{2} - B\) for some bound \(B\)
  - Low rejection rate, small sig. size \(\approx n\left(\frac{\log_2 q}{2} + 2\right)\) with compression
pqNTRUSign: signature aggregation

- Store $t$ as the signature, compute $s = t h^{-1}$ during verification
- $s$ follows Gaussian $\rightarrow$ Sum of $s$ will not cause wraparound $\rightarrow$ sum of $s = \text{sum of } s_p \mod p$
- Verify $k = (q/2\sigma)^2$ signatures in a single ring multiplication
- In practice verify $k \sim 2000$ signatures in 0.3 ms
- At a cost of increasing signature size
  - Gaussian $s$ (4608 bits) vs uniform $t$ (8196 bits)
NTRUEncrypt

- Constant time implementation for NTRU-743
  - 128 bits quantum security
  - AVX2
  - Combination of Karatsuba, Toom-3 and Toom-4
  - 2.23x faster than reference implementation
Thank you!

- https://github.com/NTRUOpenSourceProject