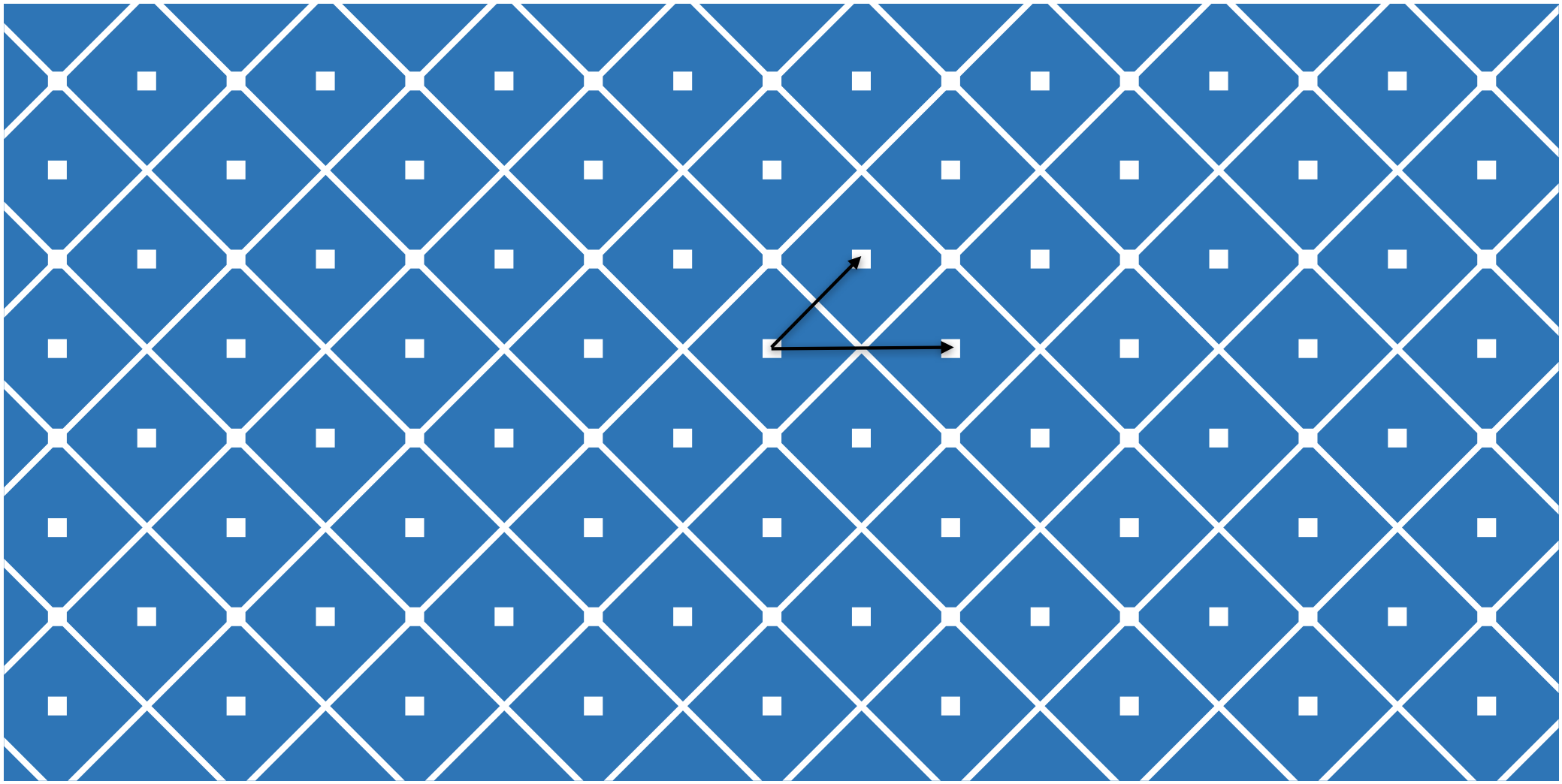

RING LEARNING WITH ERRORS DIGITAL SIGNATURE

Adam Ibrahim CS293G

WHY R-LWE ?

- Most signature schemes currently in use depend on the difficulty of factoring or of the DLP
- Shor (1994): A quantum computer can efficiently (i.e. in polynomial time) deal with both factoring and the DLP
- Grover (1996): Speed-up on quantum computers against symmetric ciphers
- We therefore need quantum-resistant algorithms !

WHY R-LWE ?

- Post-quantum schemes:
  - Lattice-based: R-LWE, NTRU, GRH, …
  - Multivariate: Rainbow
  - Hash-based: Merkle, XMSS, …
  - Code-based: Niederreiter, McEliece, …
  - Supersingular EC isogeny
  - AES with large key sizes

WHY R-LWE ?

- At 128 bit of post-quantum security (source:Wikipedia)

Algorithm	Type	Public Key	Private Key	Signature
NTRU Encrypt	Lattice	6130 B	6743 B	
Streamlined NTRU Prime	Lattice	1232 B		
Rainbow		124 KB	95 KB	
SPHINCS	Hash Signature	1 KB	1 KB	41 KB
BLISS-II	lattice	2 KB	7 KB	5 KB
New Hope	Ring-LWE	2 KB	2 KB	
Goppa-based McEliece		1 MB	11.5 KB	
Quasi-cyclic MDPC-based McEliece		8 KB	4384 B	
SIDH	Isogeny	564 B	48 B	
SIDH (compressed keys)	Isogeny	330 B	48 B	
3072-bit Discrete Log (not PQC)		384 B	32 B	
256-bit Elliptic Curve (not PQC)		32 B	32 B	

WHY R-LWE ?

- R-LWE is efficient and several improvements have reduced the key sizes and number of computations even further (e.g. Zhang 2015 for the key exchange)

- The average case complexity of solving the lattice problem on which R-LWE is based is related to the worst case complexity of the shortest vector problem, which is NP-hard (Ajtai 1996, 1998)

- Pedro covered the key exchange last week; R-LWE can also be used for digital signature

R-LWE GLP DIGITAL SIGNATURE

- We follow the GLP scheme by Güneysu T., Lyubashevsky V., Pöppelmann T. (2012)

- As with the key-exchange, we work in the ring ideal $\frac{\mathbb{Z}_q[X]}{\Phi(X)}$ where Φ is the cyclotomic polynomial $x^n + 1$, q is a prime number and n a power of 2

- We work in the least magnitude representation, i.e. $\mathbb{Z}_q = \{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$

R-LWE GLP DIGITAL SIGNATURE

- "Small" polynomial: infinity norm (i.e. max of the coefficients in $\mathbb{Z}$) is bounded
- Uniform sampling: the coefficients are all chosen uniformly in $\{-b, \ldots, b\}$ where $b \ll q$
- One can also use discrete Gaussians in $\mathbb{Z}_q^n$ in which case solving the R-LWE problem is as hard as the worst-case lattice problem with quantum algorithms (Lyubashevsky 2010)
- The private key is composed of two polynomials $\boldsymbol{s_1}$ and $\boldsymbol{s_2}$ with coefficients in $\{-1, 0, 1\}$

R-LWE GLP DIGITAL SIGNATURE

- As with DSA, a hash function is required. The hash function maps bit strings to small polynomials
- It is possible to choose a hash function such that exactly k coefficients are equal to 1 or -1, and the others to 0
- An upper bound β on the infinity norm (i.e. max of the coefficients) of certain vectors is fixed in advance to be equal to $\beta = b - k$, in order to avoid leaking information about the secret key

R-LWE GLP DIGITAL SIGNATURE

- Example of the $k = 32, n = 512$ hash function presented in the GLP paper:
  - H maps $\{0,1\}^*$ to a 160-bit string r, which is then mapped injectively to the set of polynomials of degree $n - 1$ with all coefficients equal to 0 except for 32 of them, equal to either 1 or -1
  - Read r 5 bits at a time, e.g. $r_1 r_2 r_3 r_4 r_5$, and create a 16-digit string. If $r_1 = 0$, put a -1 at index $r_2 r_3 r_4 r_5$ (read as a binary between 0 and 15) of the 16-digit string. If $r_1 = 1$, put a 1 at index $r_2 r_3 r_4 r_5$
  - E.g. if we are reading in r (01101), the 16-digit string for those 5 bits is $(0\ \ 000\ \ 000\ \ 000\ \ 000\ \ (-1)00)$
  - This gives a $\frac{160}{5} * 16 = 512$ bit string which we read as a poly

R-LWE GLP DIGITAL SIGNATURE – PUBLIC KEY GENERATION

- $q, n, b, k, \Phi(X)$ are known by the signer and the verifier
- The private key consists in two polynomials s_0 and s_1 chosen uniformly randomly from $\{-1, 0, 1\}^n$ by the signer
- The public key consists in a polynomial a chosen in a uniformly randomly from $\frac{\mathbb{Z}_q[X]}{\Phi(X)}$ and $t = as_0 + s_1$

R-LWE GLP DIGITAL SIGNATURE – SIGNATURE

1. Two polynomials y_0, y_1 are selected by sampling uniformly their coefficients from $\{-b, \dots, b\}$
2. Compute $w = ay_0 + y_1$ and compute $c = H(w, m)$
3. Compute $z_0 = s_0 c + y_0$ and $z_1 = s_1 c + y_1$ (no reduction mod q necessary in this step given the "small coefficients" condition)
4. If $||z_0||_\infty$ or $||z_1||_\infty > \beta$, restart at 1.
5. The signature is (c, z_0, z_1)

R-LWE GLP DIGITAL SIGNATURE – VERIFICATION

1. If $||z_0||_\infty$ or $||z_1||_\infty > \beta$, reject
2. Compute $w' = az_0 + z_1 - tc$
3. If $c = H(w', m)$, accept

R-LWE GLP DIGITAL SIGNATURE – VERIFICATION PROOF

- Proof:

$$\begin{aligned} w' &= az_0 + z_1 - tc \\ &= a(s_0 c + y_0) + z_1 - (as_0 + s_1)c \\ &= ay_0 + (s_1 c + y_1) - s_1 c \\ &= ay_0 + y_1 = w \end{aligned}$$

- Note: while a smaller β is more secure, it increases the likelihood of having to resample the y_i
- For $k = 32$ the likelihood of $||z_i||_\infty \leq \beta$ can be shown to be equal to $\left(1 - \frac{64}{2b+1}\right)^{2n}$

R-LWE GLP DIGITAL SIGNATURE

- R-LWE can be used for quantum-resistant asymmetric key encryption/decryption and digital signature with a speed comparable to current methods (RSA, ECDSA)
- The GLP algorithm with $n = 512, q = 8383489, b = 2^{14}$ has a signature size of ~1KB, a secret key size of ~200B, and a public key size of ~1.5KB and provides a security equivalent to ~100 bits
- The GLP algorithm can be implemented on embedded systems and was tested to be 1.5x faster than RSA

CONCLUSION

- Other algorithms based on R-LWE exist for signature, such as BLISS
- Akleylek & al. (2016): ring-TESLA: most secure implementation to date, 20% faster than GLP at the cost of larger keys / signature, smaller key sizes than BLISS but 1.45x slower, although BLISS may be vulnerable to timing attacks
- Relatively new subfield of crypto, expect to see a lot of development in the next few years due to the proven security of R-LWE !