Digital signature from I-PLWE

Table of Contents

Ring LWE

Ring LWE

- RLWE is introduced by Lyubashevsky, Peikert and Regev [LPR'10].

Let $R = \mathbb{Z}[X]/(X^d + 1)$, where $d = 2^k$ for some $k \geq 0$. For an integer q, let $R_q = R/qR$. The following two distributions are hard to distinguish:

$$\boxed{\begin{array}{ll} a_1 \leftarrow R_q; & b_1 = a_1 \cdot s + e_1 \mod q \\ a_2 \leftarrow R_q; & b_2 = a_2 \cdot s + e_2 \mod q \\ & \vdots \\ a_m \leftarrow R_q; & b_m = a_m \cdot s + e_m \mod q \end{array}}$$

$$\boxed{\begin{array}{ll} a_1 \leftarrow R_q; & b_1 \leftarrow R_q \\ a_2 \leftarrow R_q; & b_2 \leftarrow R_q \\ & \vdots \\ a_m \leftarrow R_q; & b_m \leftarrow R_q \end{array}}$$

Where $s \leftarrow R_q$, and $e_i \leftarrow \chi$ over R. $\|e_i\|_\infty \leq \beta \ll q$.

Ring LWE

[LyubashevskyPeikertRegev'10]

If there exists a PPT algorithm solves RLWE problem, then there exists a PPT *quantum* algorithm solves some hard lattice problems for *all* d-dimensional *ideal lattices*.

Commitment scheme

Commitment scheme

The message space is R_q^ℓ. Let χ be a β-bounded distribution over R.

- KeyGen(1^λ) : Sample $\mathbf{a}_1 \leftarrow R_q^m$ and $\mathbf{A}_2 \leftarrow R_q^{m\times\ell}$, output $\mathbf{A} = [\mathbf{a}_1|\mathbf{A}_2] \in R_q^{m\times(\ell+1)}$.
- Com$(\mathbf{A}, \mathbf{m} \in R_q^\ell)$: Sample $s \leftarrow R_q$ and $\mathbf{e} \leftarrow \chi^m$, output $\mathbf{c} = \mathbf{A}[s|\mathbf{m}] + \mathbf{e} \in R_q^m$.
- Ver$(\mathbf{A}, \mathbf{c}, (s, \mathbf{m}))$: Accept iff $\|\mathbf{c} - \mathbf{A}[s|\mathbf{m}]\|_\infty \leq \beta$.

Is e going to be β bounded when we replace e with $e(q)$?

Commitment scheme

The message space is R_q^ℓ. Let χ be a β-bounded distribution over R.

- KeyGen(1^λ) : Sample $\mathbf{a}_1 \leftarrow R_q^m$ and $\mathbf{A}_2 \leftarrow R_q^{m\times\ell}$, output $\mathbf{A} = [\mathbf{a}_1|\mathbf{A}_2] \in R_q^{m\times(\ell+1)}$.
- Com$(\mathbf{A}, \mathbf{m} \in R_q^\ell)$: Sample $s \leftarrow R_q$ and $\mathbf{e} \leftarrow \chi^m$, output $\mathbf{c} = \mathbf{A}[s|\mathbf{m}] + \mathbf{e} \in R_q^m$.
- Ver$(\mathbf{A}, \mathbf{c}, (s, \mathbf{m}))$: Accept iff $\|\mathbf{c} - \mathbf{A}[s|\mathbf{m}]\|_\infty \leq \beta$.

Security:

- Computational hiding:

$$\mathbf{c} = \mathbf{A}[s|\mathbf{m}] + \mathbf{e} = \boxed{\mathbf{a}_1 \cdot s + \mathbf{e}} + \mathbf{A}_2\mathbf{m}$$

- Perfect binding: For uniformly random $\mathbf{A}$,

$$\Pr[\|\mathbf{y}\|_\infty \leq 2\beta : \mathbf{y} = \mathbf{A}\mathbf{x}, \mathbf{x} \neq \mathbf{0}] \leq \mathsf{negl}(\lambda).$$

issues

Lemma 1 ([19] Lemma 21). *Let n, m, d, q be positive integers with $n \leq m$. We have:* $\Pr_{\mathbf{A} \leftarrow R_q^{m \times n}}[\lambda_1^{\infty}(\Lambda_q(\mathbf{A})) \geq \frac{1}{8\sqrt{d}} q^{1-\frac{n}{m}}] \geq 1 - (\frac{1}{2\sqrt{d}})^{nd}$.

Is this lemma true when we replace a polynomial with a value?

Zero knowledge proof

Zero knowledge proof

Relation:

$$\mathcal{R}_{\mathsf{RLWE}} = \{((\mathbf{A}, \mathbf{c}), (s, \mathbf{m}, \mathbf{e})) \ : \ \mathbf{c} = \mathbf{A}(s \| \mathbf{m}) + \mathbf{e} \mod q \wedge \|\mathbf{e}\|_\infty \leq \beta\}.$$

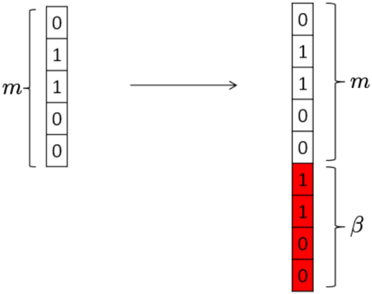
- Extend Stern's ZKP for syndrome decoding problem. Similar to [JainKrennPietrzakTentes'12] and [LingNguyenStehléWang'13].
- The challenge set $\mathcal{C} = \{1, 2, 3\}$. The first two openings prove $\mathbf{A}, \mathbf{c}$ have the form $\mathbf{c} = \mathbf{A}[s|\mathbf{m}] + \mathbf{e}$.
- Obstacle: How to prove $\mathbf{e}$ is "short" without revealing anything else?

Zero knowledge proof

- If $\mathbf{e} \in \{0,1\}^m$ and $\|\mathbf{e}\|_1 = \beta$: Prover sends $\pi(\mathbf{e})$ for a uniformly random permutation π. $\pi(\mathbf{e})$ only reveals the Hamming weight of $\mathbf{e}$.

Zero knowledge proof

- If $\mathbf{e} \in \{0,1\}^m$ and $\|\mathbf{e}\|_1 = \beta$: Prover sends $\pi(\mathbf{e})$ for a uniformly random permutation π. $\pi(\mathbf{e})$ only reveals the Hamming weight of $\mathbf{e}$.
- If $\mathbf{e} \in \{0,1\}^m$ and $\|\mathbf{e}\|_1 \leq \beta$: Extend $\mathbf{e} \in \{0,1\}^m$ to $\mathbf{e}' \in \{0,1\}^{m+\beta}$ by padding, such that $\|\mathbf{e}'\|_1 = \beta$. Prover sends $\pi(\mathbf{e}')$.

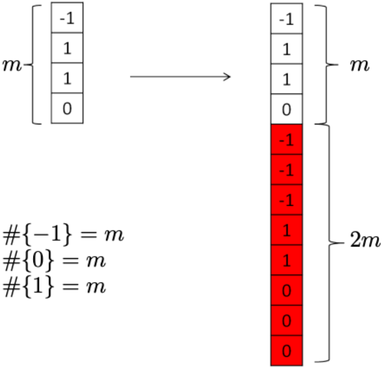


Zero knowledge proof

- If $\mathbf{e} \in \mathbb{Z}^m$ and $\|\mathbf{e}\|_\infty \leq \beta$: Decompose $\mathbf{e}$:

$$\mathbf{e} = \sum_{i=0}^{k-1} 2^i \cdot \tilde{\mathbf{e}}_i, \; k = \lfloor \log \beta \rfloor + 1, \; \tilde{\mathbf{e}}_i \in \{-1, 0, 1\}^m$$

Extend $\tilde{\mathbf{e}}_i \in \{-1, 0, 1\}^m$ to $\mathbf{e}_i \in \{-1, 0, 1\}^{3m}$. Prover sends $\pi_i(\mathbf{e}_i)$.



$$\#\{-1\} = m$$
$$\#\{0\} = m$$
$$\#\{1\} = m$$

Zero knowledge proof

- If $\mathbf{e} \in R^m$ and $\|\mathbf{e}\|_\infty \leq \beta$. View $\mathbf{e} \in \mathbb{Z}^{dm}$ by the coefficient representation. The same as above.

Zero knowledge proof

Relation:

$$\mathcal{R}_{\text{RLWE}} = \{((\mathbf{A}, \mathbf{c}), (s, \mathbf{m}, \mathbf{e})) \ : \ \mathbf{c} = \mathbf{A}(s \| \mathbf{m}) + \mathbf{e} \mod q \wedge \|\mathbf{e}\|_\infty \leq \beta\}.$$

- Prover first decomposes $\mathbf{e} \in R^m$ to $\mathbf{e}_i \in R^{3m}$ according the method above.
- Define matrix $\hat{\mathbf{I}} = [\mathbf{I}_m | \mathbf{0}_m | \mathbf{0}_m] \in R^{m \times 3m}$.

Note that :

$$\mathbf{c} = \mathbf{A}(s|\mathbf{m}) + \mathbf{e} \Leftrightarrow \mathbf{c} = \mathbf{A}(s|\mathbf{m}) + \hat{\mathbf{I}}(\sum_{i=0}^{k-1} 2^i \cdot \mathbf{e}_i)$$

Zero knowledge proof

- Prover samples $(\mathbf{r}_0, ..., \mathbf{r}_{k-1}) \leftarrow (R_q^{3m})^k$, $\mathbf{v} \leftarrow R_q^{1+\ell}$, and k random permutations $(\pi_0, ..., \pi_{k-1})$. Sends:

$$\begin{cases} C_1 = & \mathsf{Com}\left(\{\pi_i\}_{i=0}^{k-1}, \mathbf{t}_1 = \mathbf{A}\mathbf{v} + \hat{\mathbf{I}}(\sum_{i=0}^{k-1} 2^i \cdot \mathbf{r}_i)\right) \\ C_2 = & \mathsf{Com}\left(\{\mathbf{t}_{2i} = \pi_i(\mathbf{r}_i)\}_{i=0}^{k-1}\right) \\ C_3 = & \mathsf{Com}\left(\{\mathbf{t}_{3i} = \pi_i(\mathbf{r}_i + \mathbf{e}_i)\}_{i=0}^{k-1}\right) \end{cases}$$

Zero knowledge proof

- Prover samples $(\mathbf{r}_0, ..., \mathbf{r}_{k-1}) \leftarrow (R_q^{3m})^k$, $\mathbf{v} \leftarrow R_q^{1+\ell}$, and k random permutations $(\pi_0, ..., \pi_{k-1})$. Sends:

$$\begin{cases} C_1 = & \mathsf{Com}\left(\{\pi_i\}_{i=0}^{k-1}, \mathbf{t}_1 = \mathbf{A}\mathbf{v} + \hat{\mathbf{I}}(\sum_{i=0}^{k-1} 2^i \cdot \mathbf{r}_i)\right) \\ C_2 = & \mathsf{Com}\left(\{\mathbf{t}_{2i} = \pi_i(\mathbf{r}_i)\}_{i=0}^{k-1}\right) \\ C_3 = & \mathsf{Com}\left(\{\mathbf{t}_{3i} = \pi_i(\mathbf{r}_i + \mathbf{e}_i)\}_{i=0}^{k-1}\right) \end{cases}$$

- Verifier chooses $Ch \leftarrow \{1, 2, 3\}$ and sends to Prover.

Zero knowledge proof

- Prover samples $(\mathbf{r}_0, \ldots, \mathbf{r}_{k-1}) \leftarrow (R_q^{3m})^k$, $\mathbf{v} \leftarrow R_q^{1+\ell}$, and k random permutations $(\pi_0, \ldots, \pi_{k-1})$. Sends:

$$\begin{cases} C_1 = & \mathsf{Com}\left(\{\pi_i\}_{i=0}^{k-1}, \mathbf{t}_1 = \mathbf{A}\mathbf{v} + \hat{\mathbf{I}}(\sum_{i=0}^{k-1} 2^i \cdot \mathbf{r}_i)\right) \\ C_2 = & \mathsf{Com}\left(\{\mathbf{t}_{2i} = \pi_i(\mathbf{r}_i)\}_{i=0}^{k-1}\right) \\ C_3 = & \mathsf{Com}\left(\{\mathbf{t}_{3i} = \pi_i(\mathbf{r}_i + \mathbf{e}_i)\}_{i=0}^{k-1}\right) \end{cases}$$

- Verifier chooses $Ch \leftarrow \{1, 2, 3\}$ and sends to Prover.
- According to Ch, Prover does the following:

$$\begin{cases} Ch = 1, & \text{open } C_1, C_2; \\ Ch = 2, & \text{open } C_1, C_3; \\ Ch = 3, & \text{open } C_2, C_3. \end{cases}$$

Zero knowledge proof

- Prover samples $(\mathbf{r}_0, ..., \mathbf{r}_{k-1}) \leftarrow (R_q^{3m})^k$, $\mathbf{v} \leftarrow R_q^{1+\ell}$, and k random permutations $(\pi_0, ..., \pi_{k-1})$. Sends:

$$\begin{cases} C_1 = & \mathsf{Com}\left(\{\pi_i\}_{i=0}^{k-1}, \mathbf{t}_1 = \mathbf{A}\mathbf{v} + \hat{\mathbf{I}}(\sum_{i=0}^{k-1} 2^i \cdot \mathbf{r}_i)\right) \\ C_2 = & \mathsf{Com}\left(\{\mathbf{t}_{2i} = \pi_i(\mathbf{r}_i)\}_{i=0}^{k-1}\right) \\ C_3 = & \mathsf{Com}\left(\{\mathbf{t}_{3i} = \pi_i(\mathbf{r}_i + \mathbf{e}_i)\}_{i=0}^{k-1}\right) \end{cases}$$

- Verifier chooses $Ch \leftarrow \{1, 2, 3\}$ and sends to Prover.
- According to Ch, Prover does the following:

$$\begin{cases} Ch = 1, & \text{open } C_1, C_2; \\ Ch = 2, & \text{open } C_1, C_3; \\ Ch = 3, & \text{open } C_2, C_3. \end{cases}$$

- Verifier checks the following:

$$\begin{cases} Ch = 1, & \text{check } \mathbf{t}_1 - \hat{\mathbf{I}} \cdot \left(\sum_{i=0}^{k-1} 2^i \cdot \pi_i^{-1}(\mathbf{t}_{2i})\right) \in \mathsf{Img}(\mathbf{A}); \\ Ch = 2, & \text{check } \mathbf{t}_1 + \mathbf{c} - \hat{\mathbf{I}} \cdot \left(\sum_{i=0}^{k-1} 2^i \cdot \pi_i^{-1}(\mathbf{t}_{3i})\right) \in \mathsf{Img}(\mathbf{A}); \\ Ch = 3, & \text{check } \mathbf{t}_{3i} - \mathbf{t}_{2i} \in \{-1, 0, 1\}^{3md}. \end{cases}$$