ZAMA

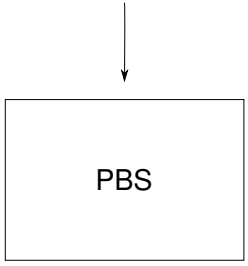
LIBERATING TFHE

Programmable Bootstrapping with General Quotient Polynomials

Marc Joye Michael Walter

PBS IN TFHE

$(a, b = \langle a, s \rangle + \Delta m + e)$



$(a', b' = \langle a', s \rangle + \Delta f(m) + e')$

- $a, s \in \mathbb{Z}_q^n$, $b \in \mathbb{Z}_q$
- $m \in \mathbb{Z}_p$
- $\Delta = \frac{q}{p}$
- $e, e' \in \mathbb{Z}$, $\|e'\| < \|e\|$

PBS: BUILDING BLOCKS

RLWE

$m(X)$ $\quad m(X) \in R_q = \mathbb{Z}_q[X]/(X^N + 1)$

$m(X)$ $\xrightarrow{\cdot X^z}$ $X^z \cdot m(X)$

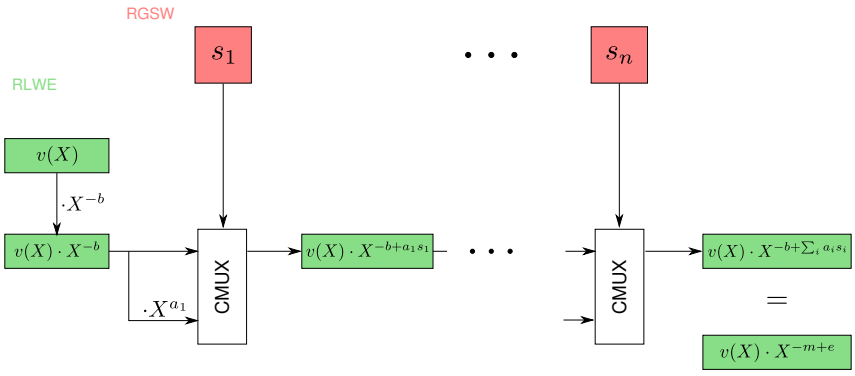
RGSW

b $\quad b \in \{0, 1\}$

$m_0(X)$ → CMUX → $m_b(X)$

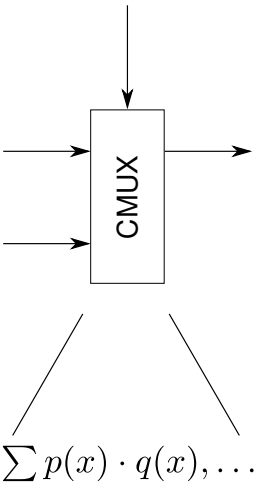
$m_1(X)$ → CMUX

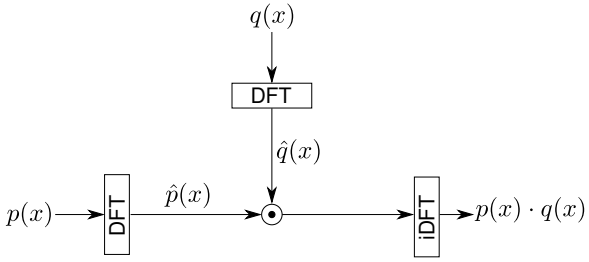
PBS DETAILS



$$v(X) = \sum_i v_i X^i \in \mathbb{Z}_q[X]/(X^N + 1) \implies v(X) \cdot X^{-j} = v_j + \dots$$

CMUX





DFT in $R[X]/(X^M - 1)$ (or in $R[X]/(X^{M/2} + 1)$) requires primitive M-th root of untiy ω in R.

- NTT over $\mathbb{Z}_q$: primitive M-th root $\omega \in \mathbb{Z}_q$
  - e.g. $M = 2^k$ and q prime s.t. $q \equiv 1 \mod M$
- FFT over $\mathbb{C}$: $\omega = e^{2\pi i/M}$

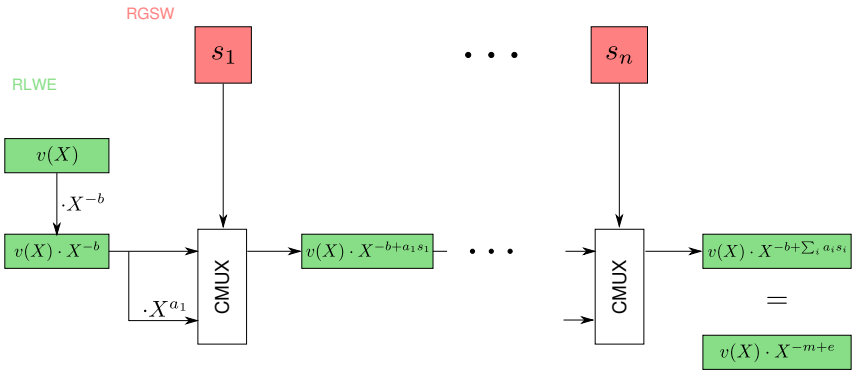
NUSSBAUMER

$$\mathbb{Z}_q[X]/(X^N+1) \mapsto (\mathbb{Z}_q[Y]/(Y^m+1))\,[X]/(X^t-Y)$$

where $N = M/2 = mt$.

- $R := \mathbb{Z}_q[Y]/(Y^m+1)$
- $R[X]/(X^t-Y) \mapsto R[X]/(X^{2t}-1)$
- $\omega = Y^{m/t}$ is a $2t$-th primitive root in R
- Apply DFT, recurse for multiplications in R
- Remaining condition: $M \in \mathbb{Z}_q^*$ (for iDFT)
- Generalizes to higher radices, e.g. $M = 3^k$ and $\Phi_M(X) = X^N + X^{N/2} + 1$, (with $N = \varphi(M)$)
- Allows for $M = 3^k$, $q = 2^n$

GENERAL PBS



$$v(X) = \sum_i v_i X^i \in \mathbb{Z}_q[X]/(\Phi_M(X)) \quad \Longrightarrow \quad v(X) \cdot X^{-j} = ???$$

PROGRAMMING THE TEST POLYNOMIAL

THEOREM (SPECIALIZED/SIMPLIFIED)

Let $M = 3^k$, $N = \varphi(M)$, $\Phi_M(X) = X^N + X^{N/2} + 1$ and $\{K_i \in \mathbb{Z}_q\}_{i=0}^{N-1}$. If

$$v_i = \begin{cases} K_i & \text{if } i < N/2 \\ K_i + K_{i-N/2} & \text{else} \end{cases}$$

then $X^{-t}v(X) = K_t + \cdots \in \mathbb{Z}_q[X]/(\Phi_M(X))$. [1]

[1] Generalization in paper: 1) More general quotient polynomials and 2) embed result in other coefficients.

NOISE ANALYSIS

$$
\begin{aligned}
&X^{-t}\left[a(X)\cdot s(X)+\Delta\cdot v(X)+e(X)\right]\\
&\quad=\left[X^{-t}a(X)\right]\cdot s(X)+\Delta\left[X^{-t}\cdot v(X)\right]+X^{-t}e(X)
\end{aligned}
$$

- $\in \mathbb{Z}_q[X]/(X^N+1) \implies \left|X^{-t}e(X)\right| = |e(X)|$
- $\in \mathbb{Z}_q[X]/p(X)$:
  - assume $p(X) \mid (X^M-1)$ for some M
  - by CRT: $\mathbb{Z}_q[X]/p(X) \simeq \mathbb{Z}_q[X]/(X^M-1) + \mod p(X)$

Let $e(X) \in \mathbb{Z}_q[X]/(X^M-1)$. Then

$$
\left|e(X) \mod (X^N+X^{N/2}+1)\right| \leq 2\,|e(X)|
$$

PADDING

- embed LWE sample in $\langle X \rangle \subset \mathbb{Z}_q/(\Phi_M(X))$
- $|\langle X \rangle| = M$
- $\deg(v(X)) < N$
- solution: ensure $b - \langle a, s \rangle < N$
- fraction of usable plaintext space: $\varphi(M)/M$

PBS-FRIENDLY FUNCTIONS

- $\Phi_M(X) = X^N + 1$ and $f = [a \mid -a] \longrightarrow$ no padding required
  - e.g., sign function
- $\Phi_M(X) = X^N + X^{N/2} + 1$ and $f = [a \mid b \mid -(a+b)] \longrightarrow$ no padding required
  - e.g., step activation function $[1 \mid 0 \mid -1]$

SUMMARY

- PBS involves many polynomial multiplications
- For NTT
  - plain NTT: change modulus q to NTT-friendly
  - Nussbaumer/Schönhage: change quotient polynomial
- Change of quotient polynomial $\longrightarrow$ General PBS
- Side effect: Less padding required