Fully Homomorphic Encryption for Cyclotomic Prime Moduli

The Generalized BFV scheme

Robin Geelen
Frederik Vercauteren

COSIC, KU Leuven

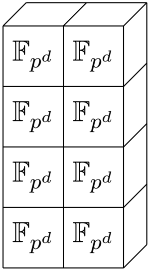
Eurocrypt 2025

BFV versus CLPX

- BFV scheme
  - Computations over $\mathbb{F}_{p^d}$ for small p and d
- CLPX scheme
  - Computations over $\mathbb{Z}_p$ for huge p

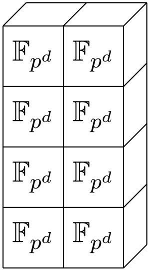
BFV versus CLPX

- BFV scheme
  - Computations over $\mathbb{F}_{p^d}$ for small p and d
  - Pack full hypercube in a ciphertext: ℓ slots
- CLPX scheme
  - Computations over $\mathbb{Z}_p$ for huge p
  - No packing



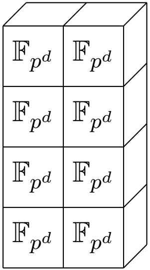
BFV versus CLPX

- BFV scheme
  - Computations over $\mathbb{F}_{p^d}$ for small p and d
  - Pack full hypercube in a ciphertext: ℓ slots
  - Arbitrary computations via bootstrapping
- CLPX scheme
  - Computations over $\mathbb{Z}_p$ for huge p
  - No packing
  - No bootstrapping



BFV versus CLPX

- BFV scheme
  - Computations over $\mathbb{F}_{p^d}$ for small p and d
  - Pack full hypercube in a ciphertext: ℓ slots
  - Arbitrary computations via bootstrapping
  - Example: $p^d = 2^{20}$ and $\ell = 1200$



- CLPX scheme
  - Computations over $\mathbb{Z}_p$ for huge p
  - No packing
  - No bootstrapping
  - Example: $p = 2^{2^{14}} + 1$

Research questions

- Can we define something in between BFV and CLPX?
  - Computations over $\mathbb{F}_{p^d}$ with large p and small d
  - Possibility of packing
  - Bootstrapping

Notations

- We use the m-th cyclotomic polynomial $\Phi_m(x)$
  - The corresponding cyclotomic field is $\mathcal{K} = \mathbb{Q}[x]/(\Phi_m(x))$
  - Its ring of integers is $\mathcal{R} = \mathbb{Z}[x]/(\Phi_m(x))$

Notations

- We use the m-th cyclotomic polynomial $\Phi_m(x)$
  - The corresponding cyclotomic field is $\mathcal{K} = \mathbb{Q}[x]/(\Phi_m(x))$
  - Its ring of integers is $\mathcal{R} = \mathbb{Z}[x]/(\Phi_m(x))$
- Take non-zero **plaintext modulus** $t = t(x) \in \mathcal{R}$
  - Define **plaintext ring** $\mathcal{R}_t = \mathcal{R}/t\mathcal{R}$
  - So $\mathcal{R}_t = \mathcal{R}/t\mathcal{R} = \mathbb{Z}[x]/(\Phi_m(x), t(x))$

Notations

- We use the m-th cyclotomic polynomial $\Phi_m(x)$
  - The corresponding cyclotomic field is $\mathcal{K} = \mathbb{Q}[x]/(\Phi_m(x))$
  - Its ring of integers is $\mathcal{R} = \mathbb{Z}[x]/(\Phi_m(x))$
- Take non-zero **plaintext modulus** $t = t(x) \in \mathcal{R}$
  - Define **plaintext ring** $\mathcal{R}_t = \mathcal{R}/t\mathcal{R}$
  - So $\mathcal{R}_t = \mathcal{R}/t\mathcal{R} = \mathbb{Z}[x]/(\Phi_m(x), t(x))$
  - BFV uses integer t and CLPX uses $t(x) = x - b$

Generalized BFV (GBFV)

- Unification and generalization of BFV and CLPX

Generalized BFV (GBFV)

- Unification and generalization of BFV and CLPX
- We support arbitrary non-zero $t \in \mathcal{R}$ as the plaintext modulus:

$$(\boldsymbol{c}_0, \boldsymbol{c}_1) = \left(\left\lfloor \frac{q}{t} \cdot \boldsymbol{m} \right\rceil + \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e}, -\boldsymbol{a} \right) \pmod{q}$$

$=$ 

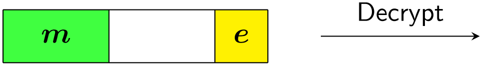
Generalized BFV (GBFV)

- Unification and generalization of BFV and CLPX
- We support arbitrary non-zero $t \in \mathcal{R}$ as the plaintext modulus:

$$(\boldsymbol{c}_0, \boldsymbol{c}_1) = \left(\left\lfloor \frac{q}{t} \cdot \boldsymbol{m} \right\rceil + \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e}, -\boldsymbol{a} \right) \pmod{q}$$

$=$

- Decryption via scale-and-round:



$$\boldsymbol{m} = \left\lfloor \frac{t}{q} \cdot (\boldsymbol{c}_0 + \boldsymbol{c}_1 \cdot \boldsymbol{s}) \right\rceil$$

The GBFV scheme: flattening

- New function to choose small representatives modulo t:

$$\mathsf{Flatten}_t\colon \mathcal{R}_t \to \mathcal{R}\colon \boldsymbol{m} \mapsto t \cdot \left[\frac{\boldsymbol{m}}{t}\right]_1$$

The GBFV scheme: flattening

- New function to choose small representatives modulo t:

$$\mathsf{Flatten}_t \colon \mathcal{R}_t \to \mathcal{R} \colon \boldsymbol{m} \mapsto t \cdot \left[\frac{\boldsymbol{m}}{t} \right]_1$$

- Resulting norm depends on $\Phi_m(x)$ and t: if $\hat{\boldsymbol{m}} = \mathsf{Flatten}_t(\boldsymbol{m})$ then

$$||\hat{\boldsymbol{m}}||_\infty^{\mathsf{can}} \leq (\varphi(m)/2) \cdot ||t||_\infty^{\mathsf{can}}$$

The GBFV scheme: flattening

- New function to choose small representatives modulo t:

$$\text{Flatten}_t \colon \mathcal{R}_t \to \mathcal{R} \colon \boldsymbol{m} \mapsto t \cdot \left[\frac{\boldsymbol{m}}{t}\right]_1$$

- Resulting norm depends on $\Phi_m(x)$ and t: if $\hat{\boldsymbol{m}} = \text{Flatten}_t(\boldsymbol{m})$ then

$$||\hat{\boldsymbol{m}}||_\infty^{\text{can}} \leq (\varphi(m)/2) \cdot ||t||_\infty^{\text{can}}$$

Examples for $\Phi_m(x) = x^8 + 1$

- $\text{Flatten}_5(51 \cdot x + 44) = x - 1$

The GBFV scheme: flattening

- New function to choose small representatives modulo t:

$$\mathsf{Flatten}_t \colon \mathcal{R}_t \to \mathcal{R} \colon \boldsymbol{m} \mapsto t \cdot \left[\frac{\boldsymbol{m}}{t}\right]_1$$

- Resulting norm depends on $\Phi_m(x)$ and t: if $\hat{\boldsymbol{m}} = \mathsf{Flatten}_t(\boldsymbol{m})$ then

$$||\hat{\boldsymbol{m}}||_\infty^{\mathsf{can}} \leq (\varphi(m)/2) \cdot ||t||_\infty^{\mathsf{can}}$$

Examples for $\Phi_m(x) = x^8 + 1$

- $\mathsf{Flatten}_5(51 \cdot x + 44) = x - 1$
- $\mathsf{Flatten}_{x-4}(4^3 - 2 \cdot 4^2 + 4) = x^3 - 2 \cdot x^2 + x$

The GBFV scheme: flattening

- New function to choose small representatives modulo t:

$$\text{Flatten}_t \colon \mathcal{R}_t \to \mathcal{R} \colon \boldsymbol{m} \mapsto t \cdot \left[\frac{\boldsymbol{m}}{t}\right]_1$$

- Resulting norm depends on $\Phi_m(x)$ and t: if $\hat{\boldsymbol{m}} = \text{Flatten}_t(\boldsymbol{m})$ then

$$||\hat{\boldsymbol{m}}||_\infty^{\text{can}} \leq (\varphi(m)/2) \cdot ||t||_\infty^{\text{can}}$$

Examples for $\Phi_m(x) = x^8 + 1$

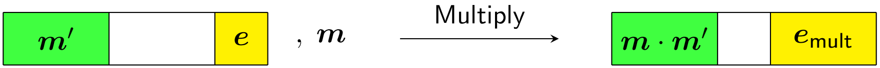
- $\text{Flatten}_5(51 \cdot x + 44) = x - 1$
- $\text{Flatten}_{x-4}(4^3 - 2 \cdot 4^2 + 4) = x^3 - 2 \cdot x^2 + x$
- $\text{Flatten}_{(x-4)^2}(256 \cdot x + 512) = -2 \cdot x^6 + 11 \cdot x^5 - 6 \cdot x^4$

The GBFV scheme: multiplication

- We want to multiply ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1)$ with plaintext $\boldsymbol{m}$
- Let $\hat{\boldsymbol{m}} = \mathsf{Flatten}_t(\boldsymbol{m})$ and output $([\hat{\boldsymbol{m}} \cdot \boldsymbol{c}_0]_q, [\hat{\boldsymbol{m}} \cdot \boldsymbol{c}_1]_q)$

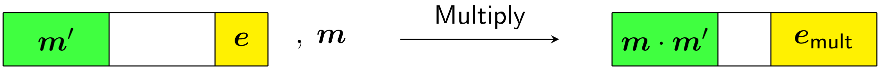
The GBFV scheme: multiplication

- We want to multiply ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1)$ with plaintext $\boldsymbol{m}$
- Let $\hat{\boldsymbol{m}} = \mathsf{Flatten}_t(\boldsymbol{m})$ and output $\left([\hat{\boldsymbol{m}} \cdot \boldsymbol{c}_0]_q, [\hat{\boldsymbol{m}} \cdot \boldsymbol{c}_1]_q\right)$



The GBFV scheme: multiplication

- We want to multiply ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1)$ with plaintext $\boldsymbol{m}$
- Let $\hat{\boldsymbol{m}} = \mathsf{Flatten}_t(\boldsymbol{m})$ and output $([\hat{\boldsymbol{m}} \cdot \boldsymbol{c}_0]_q, [\hat{\boldsymbol{m}} \cdot \boldsymbol{c}_1]_q)$



- New noise $\boldsymbol{e}_{\mathsf{mult}} = \hat{\boldsymbol{m}} \cdot \boldsymbol{e}$ satisfies

$$||\boldsymbol{e}_{\mathsf{mult}}||_\infty^{\mathsf{can}} \leq (\varphi(m)/2) \cdot ||t||_\infty^{\mathsf{can}} \cdot ||\boldsymbol{e}||_\infty^{\mathsf{can}}$$

The GBFV scheme: plaintext space

- Start from identity $\Phi_m(x) = \Phi_r(x^{m/r})$ where r is the radical of m

The GBFV scheme: plaintext space

- Start from identity $\Phi_m(x) = \Phi_r(x^{m/r})$ where r is the radical of m
- We take $t(x) = x^k - b$ where k divides m/r:

$$(\Phi_r(x^{m/r}), x^k - b) = (x^k - b, \Phi_r(b^{m/(rk)}))$$

The GBFV scheme: plaintext space

- Start from identity $\Phi_m(x) = \Phi_r(x^{m/r})$ where r is the radical of m
- We take $t(x) = x^k - b$ where k divides m/r:

$$(\Phi_r(x^{m/r}), x^k - b) = (x^k - b, \Phi_r(b^{m/(rk)}))$$

- Native arithmetic modulo an integer $p = \Phi_r(b^{m/(rk)})$
  - If p is a prime number then we call it a **cyclotomic prime**

Packing-noise trade-off: Fermat family

- Consider $m = 2^{15}$ and **Fermat prime** $p = \Phi_2(2^{16}) = 2^{16} + 1$
- Let $t(x) = x^k - b$ with $k = 2^{i+10}$ and $b = 2^{2^i}$

Packing-noise trade-off: Fermat family

- Consider $m = 2^{15}$ and **Fermat prime** $p = \Phi_2(2^{16}) = 2^{16} + 1$
- Let $t(x) = x^k - b$ with $k = 2^{i+10}$ and $b = 2^{2^i}$
- Trade-off between #slots and noise:
  - Number of slots: k
  - Noise: increases with b

i	0	1	2	3	BFV
Number of slots	1024	2048	4096	8192	16384
Mult noise (bits)	10.5	11.2	13.0	17.3	25.1

Packing-noise trade-off: Goldilocks family

- Consider $m = 3 \cdot 2^{14}$ and **Goldilocks prime** $p = \Phi_6(2^{32}) = 2^{64} - 2^{32} + 1$
- Let $t(x) = x^k - b$ with $k = 2^{i+8}$ and $b = 2^{2^i}$

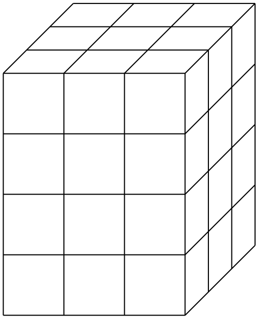
Packing-noise trade-off: Goldilocks family

- Consider $m = 3 \cdot 2^{14}$ and **Goldilocks prime** $p = \Phi_6(2^{32}) = 2^{64} - 2^{32} + 1$
- Let $t(x) = x^k - b$ with $k = 2^{i+8}$ and $b = 2^{2^i}$
- Trade-off between #slots and noise:
  - Number of slots: k
  - Noise: increases with b

i	0	1	2	3	4	5	BFV
Number of slots	256	512	1024	2048	4096	8192	16384
Mult noise (bits)	10.3	11.3	13.1	17.2	25.2	41.3	73.0

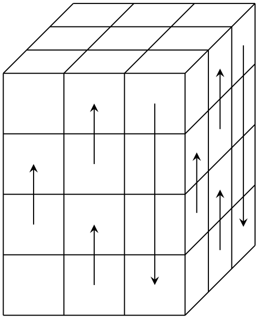
The BFV hypercube

- Slots of $\mathbb{F}_{p^d}$-elements are arranged in hypercube



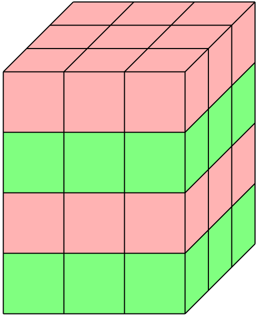
The BFV hypercube

- Slots of $\mathbb{F}_{p^d}$-elements are arranged in hypercube
- Circular rotations along one dimension



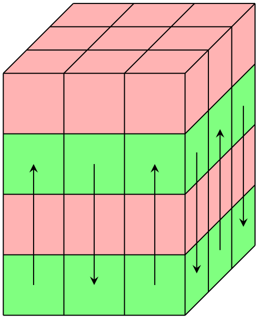
The GBFV hypercube

- Slots of $\mathbb{F}_{p^d}$-elements are arranged in hypercube



The GBFV hypercube

- Slots of $\mathbb{F}_{p^d}$-elements are arranged in hypercube
- Circular rotations along one dimension



Ring switching

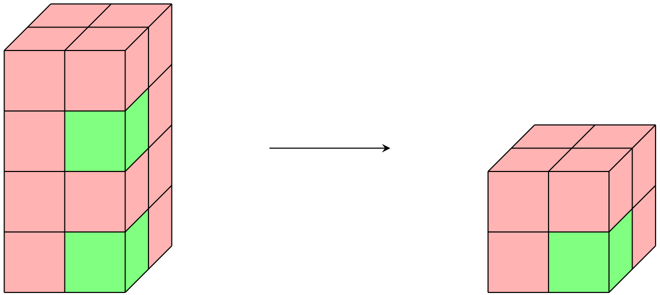
- Change cyclotomic ring *during computation* and select subset of the slots
  - Example for Goldilocks prime:

$$m = 3 \cdot 2^4,\ t(x) = x^2 - 256 \quad \longrightarrow \quad m' = 3 \cdot 2^{3},\ t'(x) = x^{1} - 256$$

Ring switching

- Change cyclotomic ring *during computation* and select subset of the slots
  - Example for Goldilocks prime:

$$m = 3 \cdot 2^4,\ t(x) = x^2 - 256 \quad \longrightarrow \quad m' = 3 \cdot 2^{3},\ t'(x) = x^{1} - 256$$



Conversion to BFV

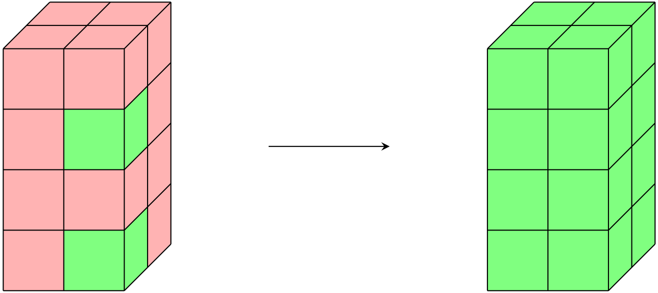
- GBFV ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1)$ satisfies $\boldsymbol{c}_0 + \boldsymbol{c}_1 \cdot \boldsymbol{s} = (q/t) \cdot (\boldsymbol{m} + t \cdot \boldsymbol{a} + \boldsymbol{v})$
  - Divide by $p/t \in \mathcal{R}$ and round:

$$\left\lfloor \frac{t}{p} \cdot \boldsymbol{c}_0 \right\rceil + \left\lfloor \frac{t}{p} \cdot \boldsymbol{c}_1 \right\rceil \cdot \boldsymbol{s} \approx \frac{q}{p} \cdot (\boldsymbol{m} + t \cdot \boldsymbol{a} + \boldsymbol{v})$$

Conversion to BFV

- GBFV ciphertext $(\boldsymbol{c}_0, \boldsymbol{c}_1)$ satisfies $\boldsymbol{c}_0 + \boldsymbol{c}_1 \cdot \boldsymbol{s} = (q/t) \cdot (\boldsymbol{m} + t \cdot \boldsymbol{a} + \boldsymbol{v})$
  - Divide by $p/t \in \mathcal{R}$ and round:

$$\left\lfloor \frac{t}{p} \cdot \boldsymbol{c}_0 \right\rceil + \left\lfloor \frac{t}{p} \cdot \boldsymbol{c}_1 \right\rceil \cdot \boldsymbol{s} \approx \frac{q}{p} \cdot (\boldsymbol{m} + t \cdot \boldsymbol{a} + \boldsymbol{v})$$

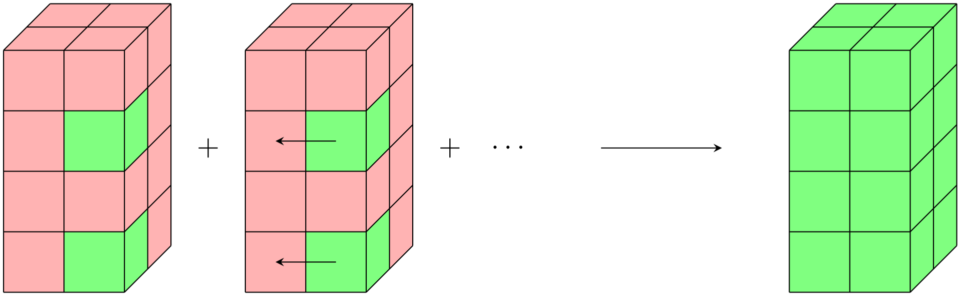


Packing to BFV

- Conversion uses available space inefficiently
- Pack multiple ciphertexts together using following steps:
  1. Convert GBFV to BFV and put zero in garbage slots
  2. Rotate each ciphertext with different offset and add results

Packing to BFV

- Conversion uses available space inefficiently
- Pack multiple ciphertexts together using following steps:
    1. Convert GBFV to BFV and put zero in garbage slots
    2. Rotate each ciphertext with different offset and add results



GBFV bootstrapping

$$\begin{array}{c}
\mathsf{Enc}_t(m_1, \ldots, m_{\ell'}) \\
\downarrow \text{GBFV to BFV} \\
\mathsf{Enc}_p(m_1, \ldots, m_{\ell'}, \ldots, m_\ell) \\
\downarrow \text{Noisy expansion} \\
\mathsf{Enc}_{p^2}(p \cdot m_1 + e_1, \ldots, p \cdot m_{\ell'} + e_{\ell'}, \ldots, p \cdot m_\ell + e_\ell) \\
\downarrow \text{BFV to GBFV} \\
\mathsf{Enc}_{t^2}(p \cdot m_1 + e_1, \ldots, p \cdot m_{\ell'} + e_{\ell'}) \\
\downarrow \text{Digit removal} \\
\mathsf{Enc}_t(m_1, \ldots, m_{\ell'})
\end{array}$$

Bootstrapping results

Table: results for $m = 2^{15}$ and $p = 2^{16} + 1$

Number of slots ℓ'		1024	2048	4096	8192
Bits per multiplicative level		11	12	14	18
Noise (bits)	Noisy expansion	111	111	114	118
	Digit removal	82	91	113	161
	Remaining	**124**	**115**	**90**	**38**
Execution time (sec)	Noisy expansion	1.41	1.44	1.44	1.46
	Digit removal	0.53	0.54	0.54	0.55
	Total	**1.94**	**1.98**	**1.98**	**2.01**

Conclusion

- Better FHE for large cyclotomic prime fields
  - Flexible packing-noise trade-off
  - Lower-latency bootstrapping

Conclusion

- Better FHE for large cyclotomic prime fields
  - Flexible packing-noise trade-off
  - Lower-latency bootstrapping
- Bootstrapping converts to regular BFV

Blog post:

Blog post:

Thank you for listening!