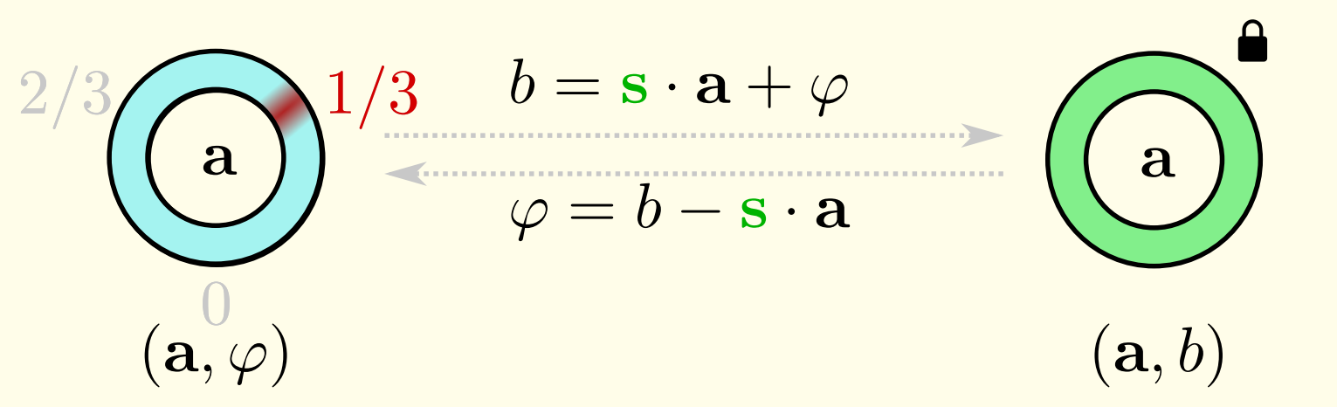
TFHE: Fully Homomorphic Encryption over the Torus

I. Chillotti, N. Gama, M. Georgieva and M. Izabachène.

https://tfhe.github.io

TLWE Encryption over the torus

secret key: $\mathbf{s} \in \{0,1\}^n$



2/3
1/3
0
a
$b = \mathbf{s} \cdot \mathbf{a} + \varphi$
$\varphi = b - \mathbf{s} \cdot \mathbf{a}$
$(\mathbf{a}, \varphi)$
$(\mathbf{a}, b)$

Example: $\mathcal{M} = \{0, 1/3, 2/3\}$ *mod* 1
$\mu = 1/3$ *mod* $1 \in \mathcal{M}$

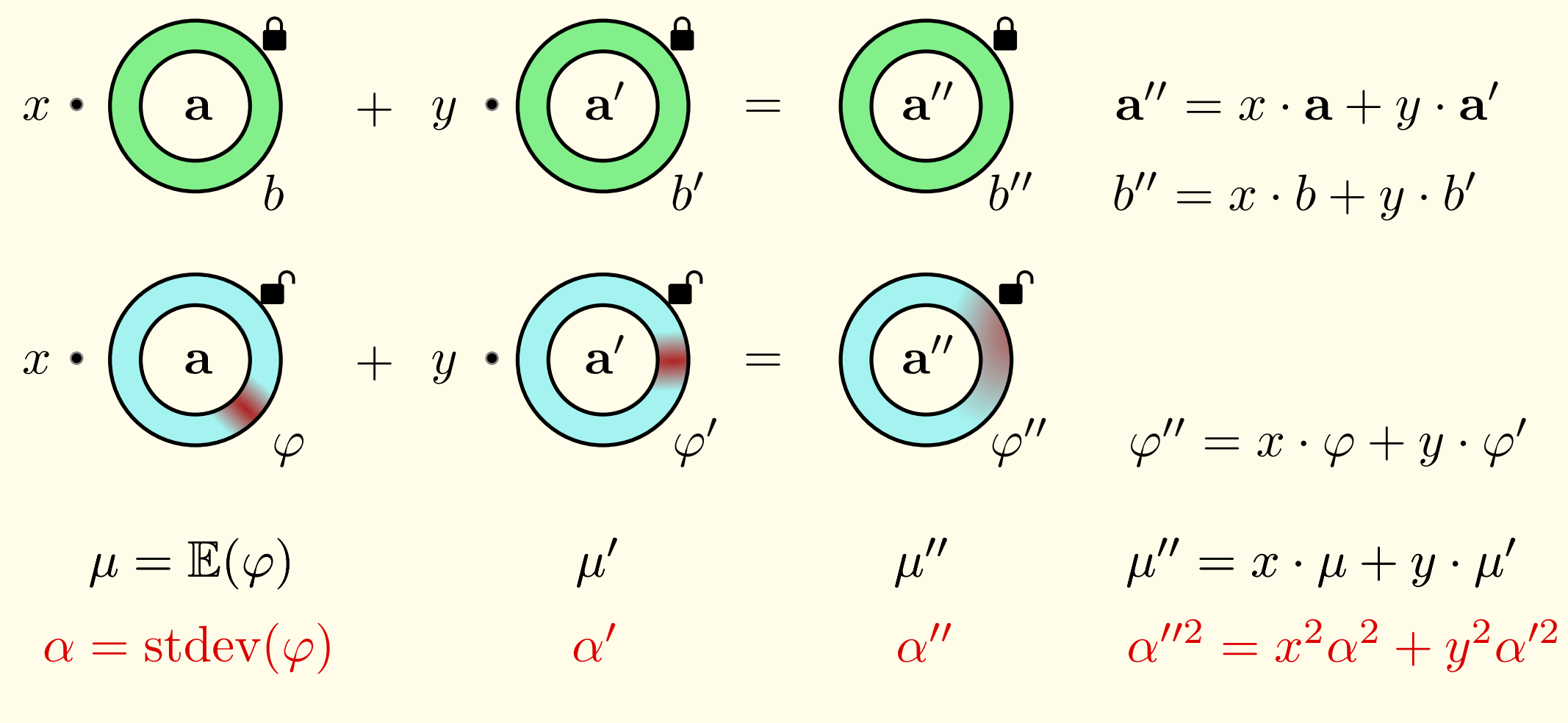
TLWE Encryption

- $\varphi = \mu +$ *Gaussian Error*
- Random mask $\mathbf{a} \in \mathbb{T}^{\mathbf{n}}$

TLWE Decryption

- Unlock the representation $(\mathbf{a}, \varphi)$
- Round φ to the nearest message $\mu \in \mathcal{M}$

TLWE/TRLWE Linear Operations



$\mathbf{a}'' = x \cdot \mathbf{a} + y \cdot \mathbf{a}'$
$b'' = x \cdot b + y \cdot b'$

$\varphi'' = x \cdot \varphi + y \cdot \varphi'$

$\mu = \mathbb{E}(\varphi)$ μ' μ'' $\mu'' = x \cdot \mu + y \cdot \mu'$

$\alpha = \mathrm{stdev}(\varphi)$ α' α'' $\alpha''^2 = x^2\alpha^2 + y^2\alpha'^2$

Sublinear noise propagation

TRGSW Ciphertexts

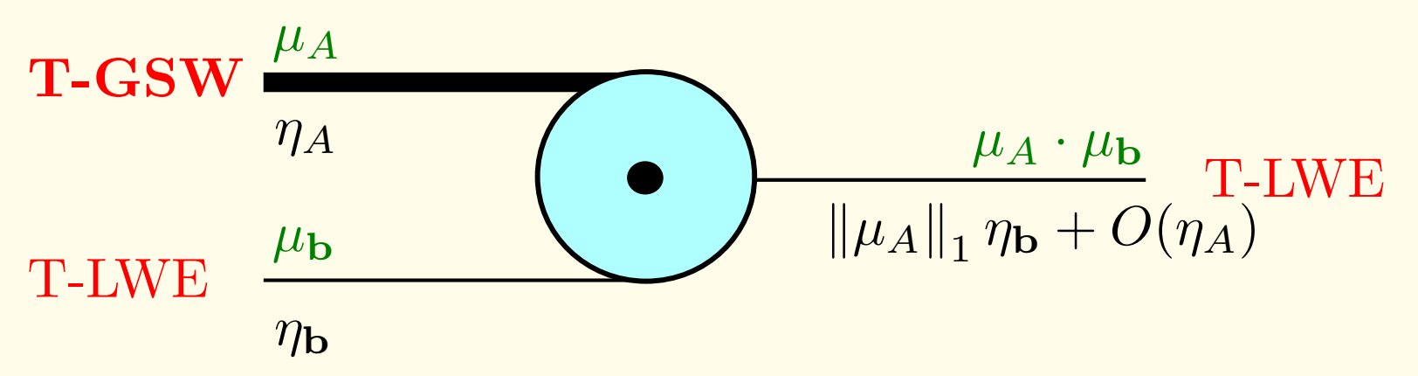
TRGSW: $C = Z + \mu H$
with $\mu \in \mathbb{Z}_N[X]$

$$\mathsf{TRGSW}(\mu) = \left(\begin{array}{c} \mathsf{TRLWE}_K(K \cdot \frac{\mu}{2}) \\ \mathsf{TRLWE}_K(K \cdot \frac{\mu}{4}) \\ \mathsf{TRLWE}_K(K \cdot \frac{\mu}{8}) \\ \hline \mathsf{TRLWE}_K(1 \cdot \frac{\mu}{2}) \\ \mathsf{TRLWE}_K(1 \cdot \frac{\mu}{4}) \\ \mathsf{TRLWE}_K(1 \cdot \frac{\mu}{8}) \end{array}\right)$$

Homomorphic ops.

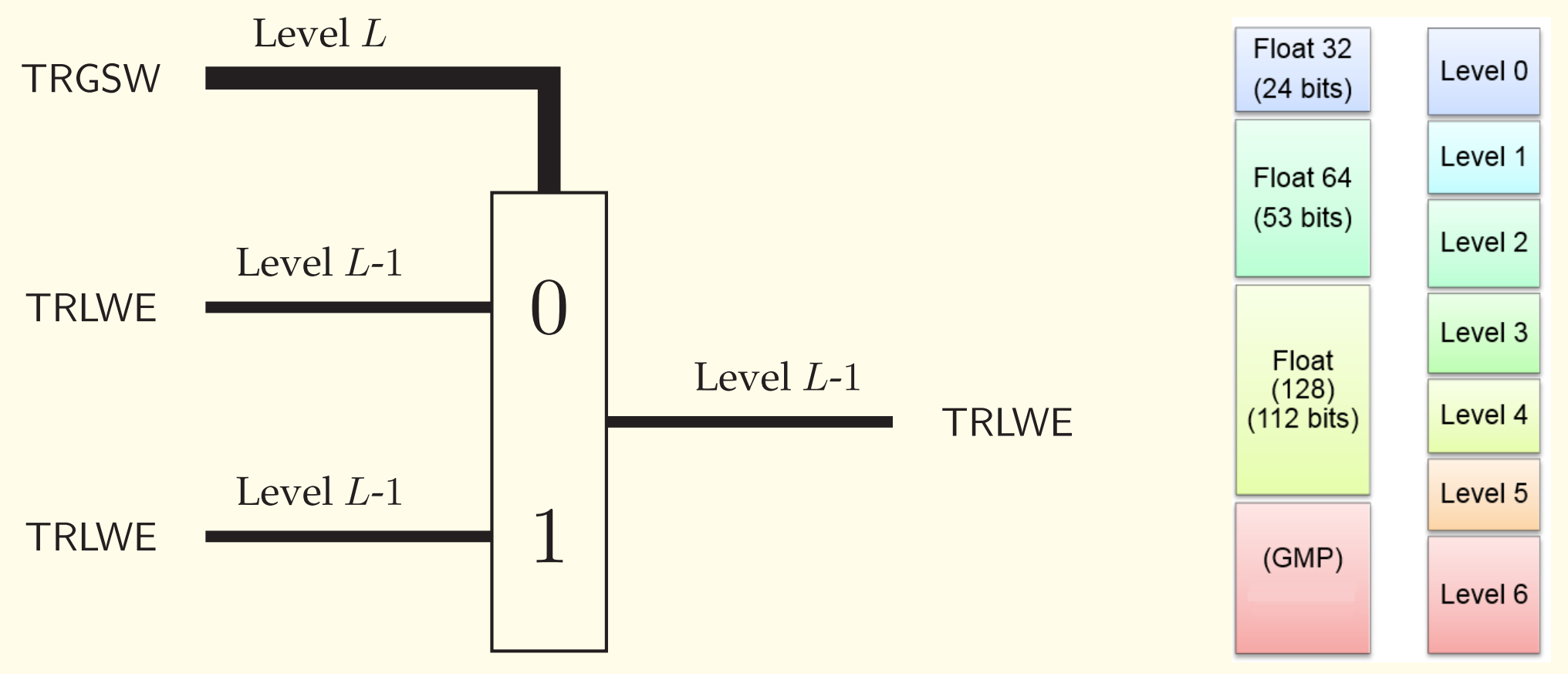
- Additions
- Public Linear combinations
  Sublinear noise propagation
- Internal products
- External products
  Unbalanced noise propagation

External Product

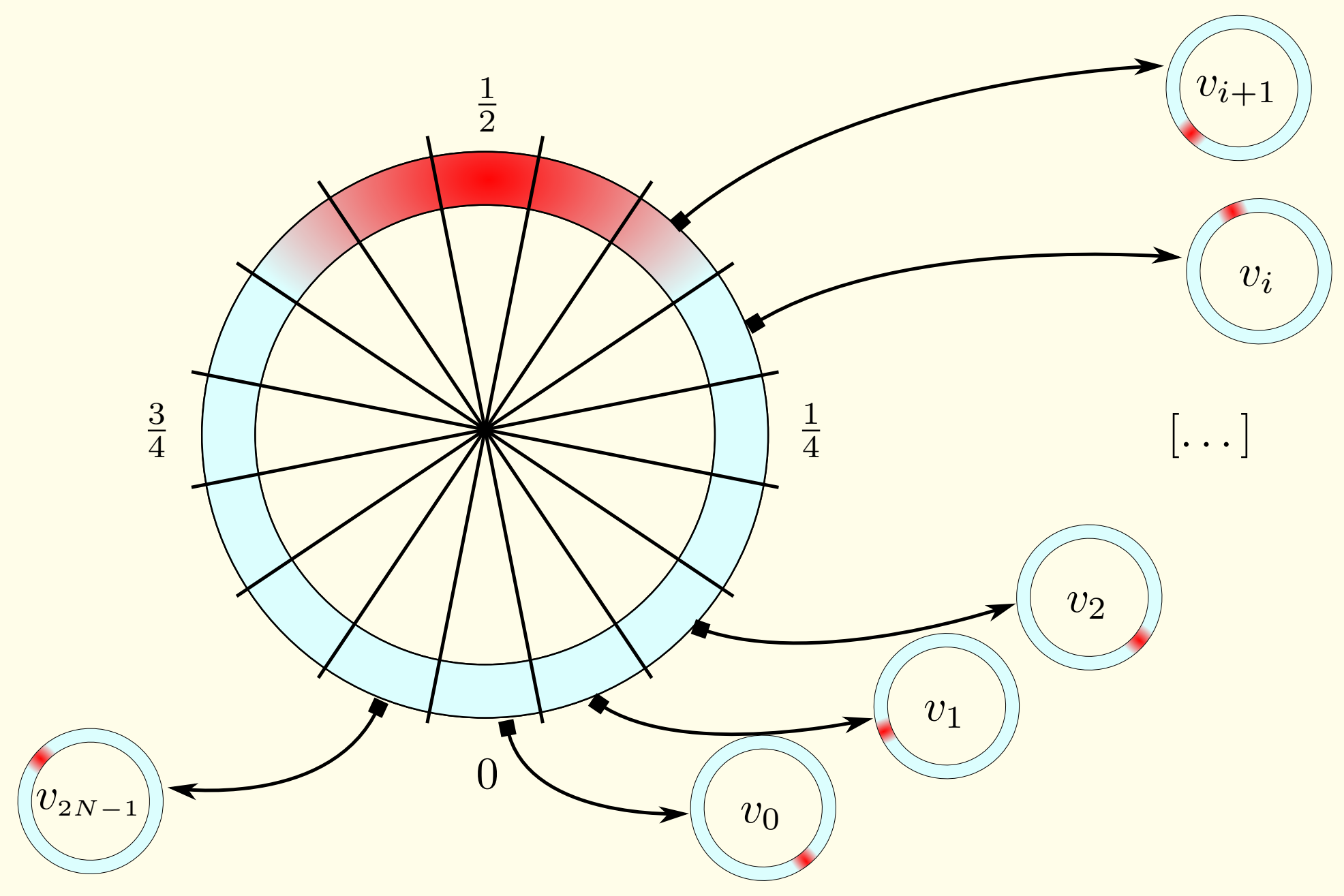


T-GSW
μ_A
η_A
T-LWE
$\mu_{\mathbf{b}}$
$\eta_{\mathbf{b}}$
$\mu_A \cdot \mu_{\mathbf{b}}$
$\|\mu_A\|_1 \eta_{\mathbf{b}} + O(\eta_A)$
T-LWE

Homomorphic MUX



Gate Bootstrapping

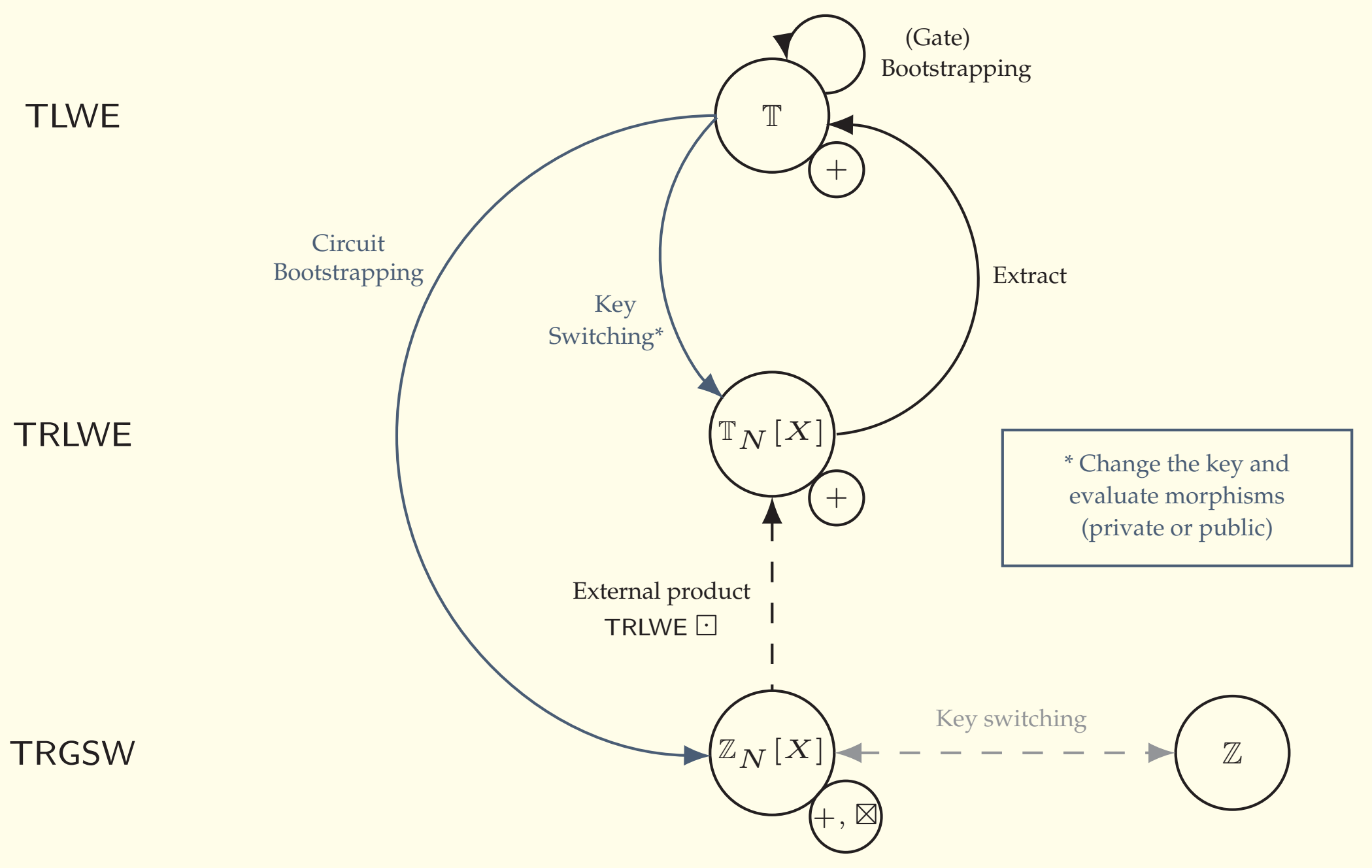


Bootstrapping algorithm of $(\mathbf{a}, b)$

1. Start from (a trivial) TRLWE ciphertext of message $v_0 + v_1 X + \cdots + v_{N-1} X^{N-1}$
   N coefs mod $X^N + 1$ can be viewed as $2N$ coefs mod $X^{2N} - 1$ s.t. $v_{N+i} = -v_i$
2. Rotate it by $p = -\varphi_s(\mathbf{a}, b)$ positions using external product.
3. Extract the constant term (which encrypts v_p).

TFHE Morphisms

	message	ciphertext	key	lin. com.	prod.
TLWE	$\mathbb{T}$	$\mathbb{T}^{n+1}$	$\mathbb{B}^n$	✓	✗
TRLWE	$\mathbb{T}_N[X]$	$\mathbb{T}_N[X]^{k+1}$	$\mathbb{B}_N[X]^k$	✓	✗
TRGSW	$\mathbb{Z}_N[X]$	ℓ-vect. of TRLWE	$\mathbb{B}_N[X]^k$	✓	✓



* Change the key and evaluate morphisms (private or public)

Batching and Vertical Packing

TRLWE: messages $\mathbf{m} = \sum_{i=0}^{N-1} m_i \cdot X^i \in \mathbb{T}_N[X]$

m_0	m_1	m_2	$\cdots$	m_{N-1}

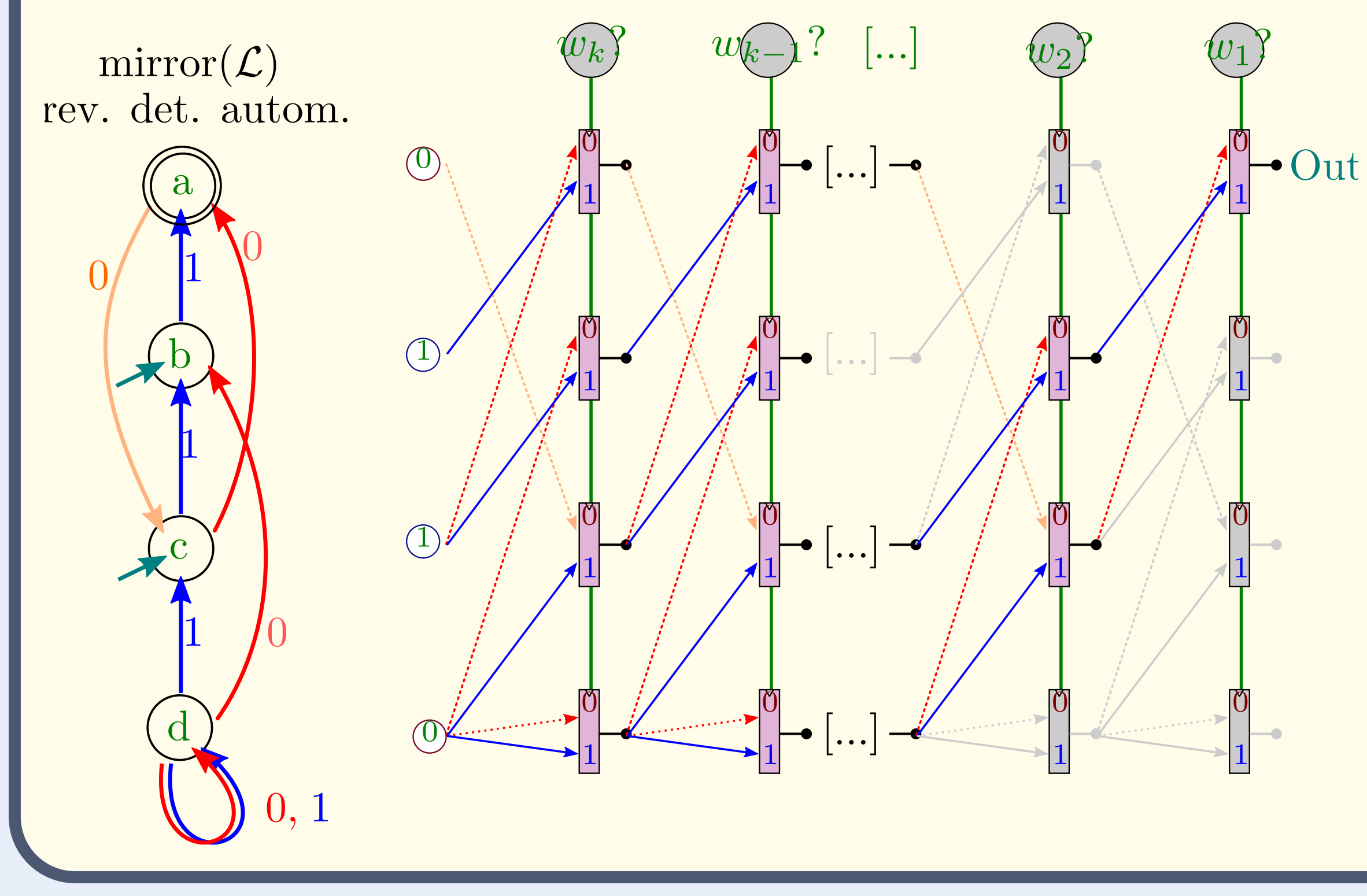
LookUp Tables to evaluate arbitrary functions:

$$f : \mathbb{B}^d \longrightarrow \mathbb{T}^s$$

$$x = (x_0, \ldots, x_{d-1}) \longmapsto f(x) = (f_0(x), \ldots, f_{s-1}(x))$$

x_0	$\cdots$	x_{d-1}	f_0	$\cdots$	f_{s-1}
0	$\cdots$	0	$\sigma_{0,0}$	$\cdots$	$\sigma_{s-1,0}$
1	$\cdots$	0	$\sigma_{0,1}$	$\cdots$	$\sigma_{s-1,1}$
0	$\cdots$	0	$\sigma_{0,2}$	$\cdots$	$\sigma_{s-1,2}$
1	$\cdots$	0	$\sigma_{0,3}$	$\cdots$	$\sigma_{s-1,3}$
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\cdots$	1	$\sigma_{0,2^d-2}$	$\cdots$	$\sigma_{s-1,2^d-2}$
1	$\cdots$	1	$\sigma_{0,2^d-1}$	$\cdots$	$\sigma_{s-1,2^d-1}$

Automata



DFA (deterministic finite automata)

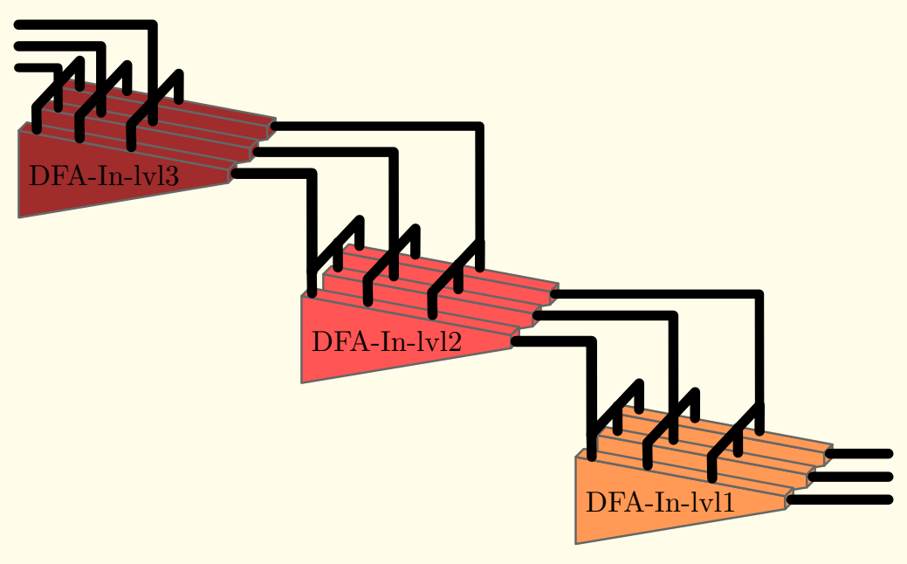
- Decisional: returns **accepted** (1) or **rejected** (0)

det-WFA (deterministic weighted automata)

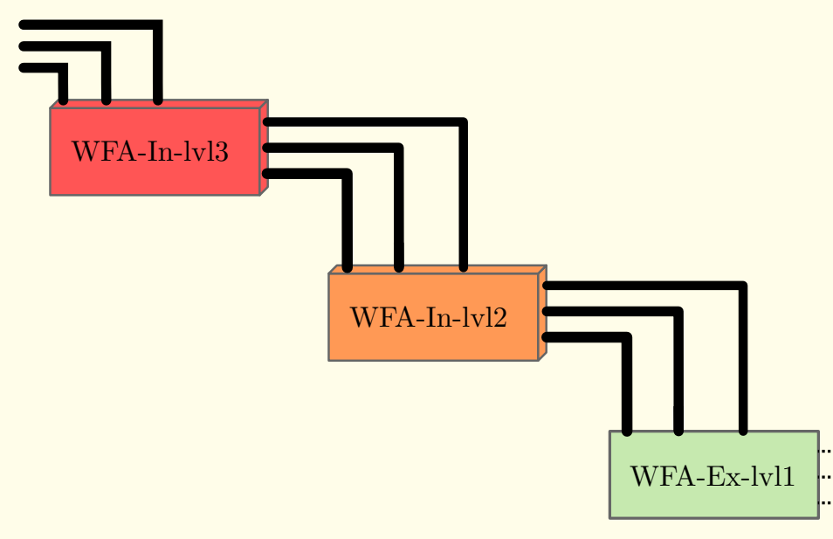
- Computational: returns a **weight** in $\mathbb{T}_N[X]$

Weights act like a "memory" that stores the result all along the evaluation

Compositions



Composition of DFA



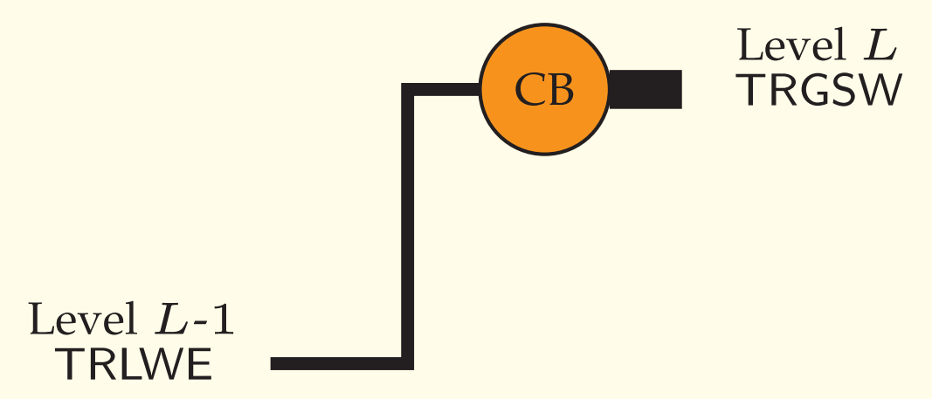
Composition of det-WFA

Levels = composition depth
colors: very slow, slow, ..., very fast

Circuit Bootstrapping

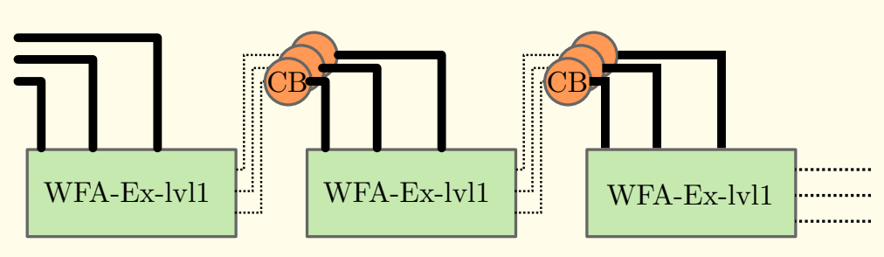
Permits composition of automata and run everything in levels 0,1 and 2 (*i.e.* native floats).

Reconstruct a TRGSW encryption directly from its internal structure.



Gate/Circuit Bootstrapping

TFHE in Circuit Bootstrap mode
Bootstrap after many gates



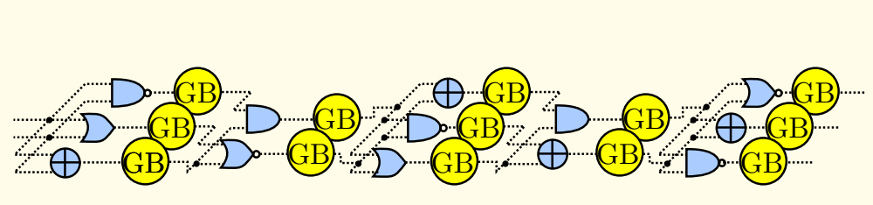
Input/Output

Plaintext (TLWE) → Ciphertext (TRGSW)
Bit Overhead: 262144

- Very fast : transition in 34 μs
- No so fast: circuit bootstrapped in 134 ms but after many gates
- Composition : LUT, (W)DFA

TFHE in Circuit bootstrap mode can evaluate LUT 16 to 8 in 1 sec

TFHE in Gate Bootstrap mode
Bootstrap between each gate



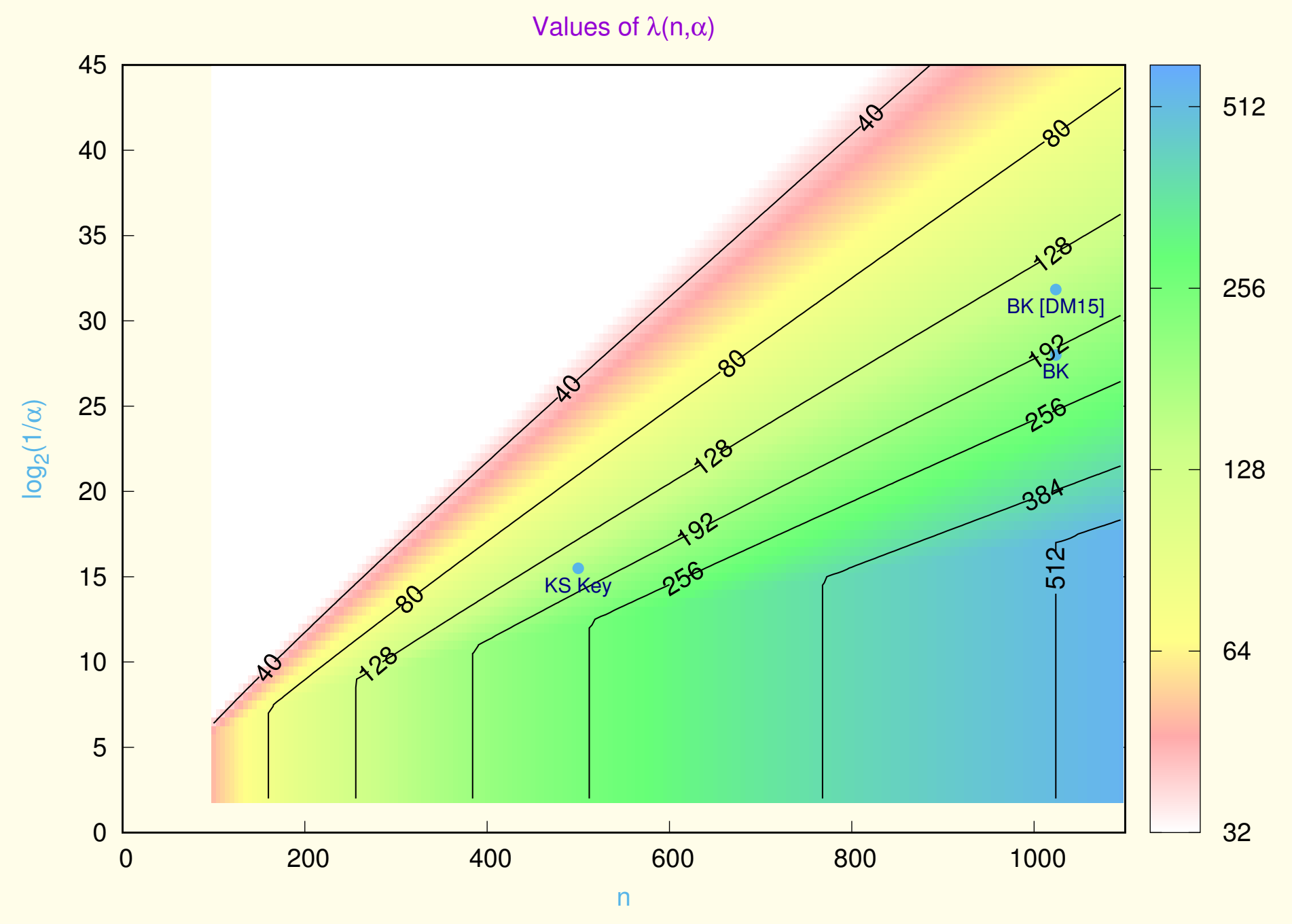
Input/Output

Plaintext (TLWE) → Ciphertext (TLWE)
Bit Overhead: 8000

- No so fast: bootstrapped binary gate runs in 13 ms
- All gates have the same cost
- Composable: between each gate

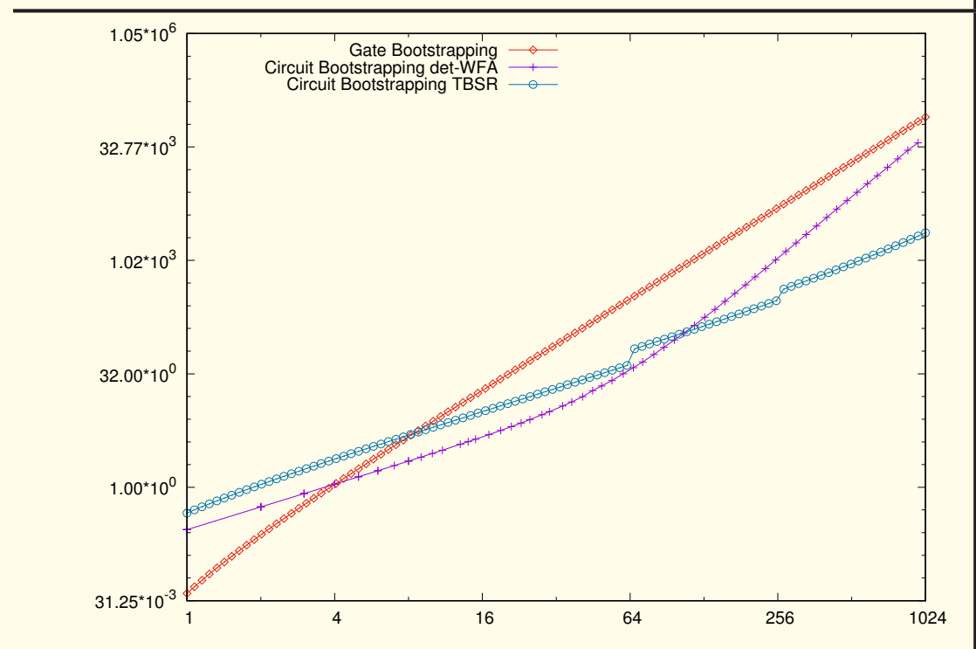
With TFHE we can compute 76 gates per second, for any circuit.

Security



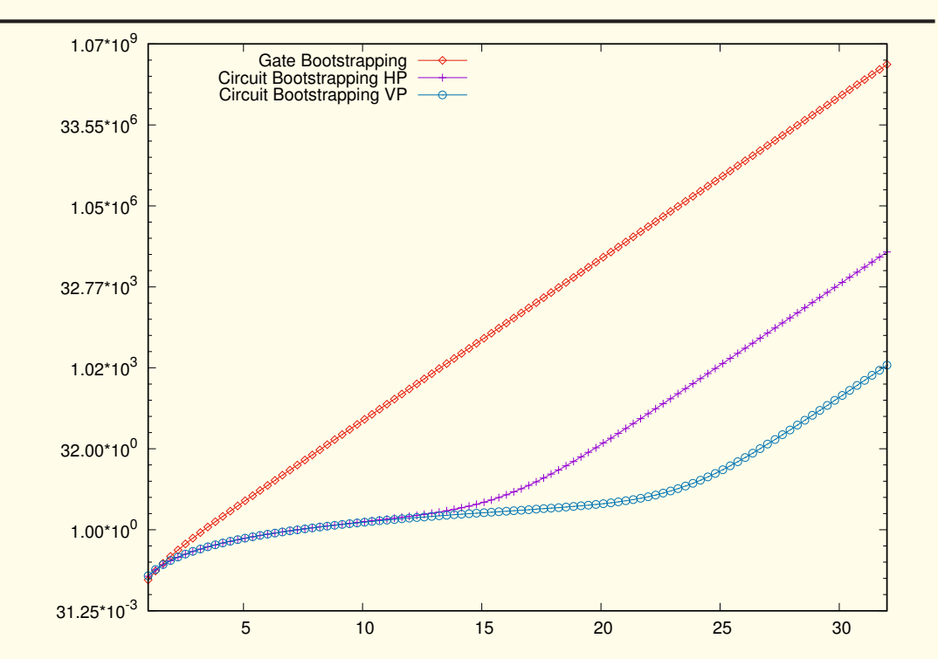
Timings (seconds)

Multiplication



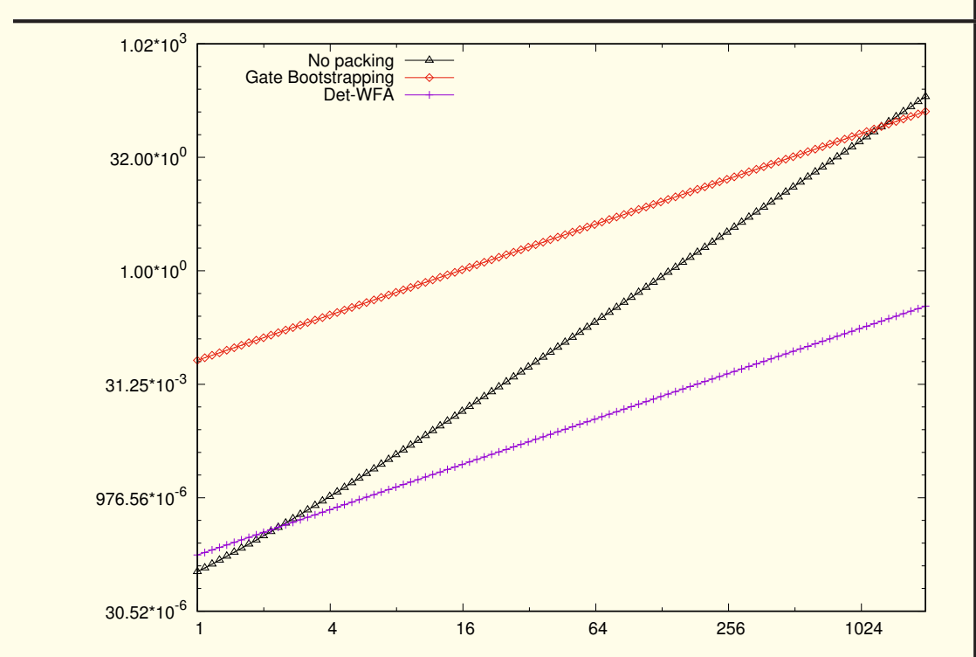
Multiplication (2 inputs of d-bits each)
- Gate bootst.: $(6d^2 - 3d)t_{\mathsf{GB}}$
- Circuit bootst with Det WFA.: $2dt_{\mathsf{CB}} + \Theta(d^3)t_{\mathsf{XP}}$
(computed by optimization program)
- Circuit bootst with TBSR:
(computed by optimization program)

n to 8-bit LUT



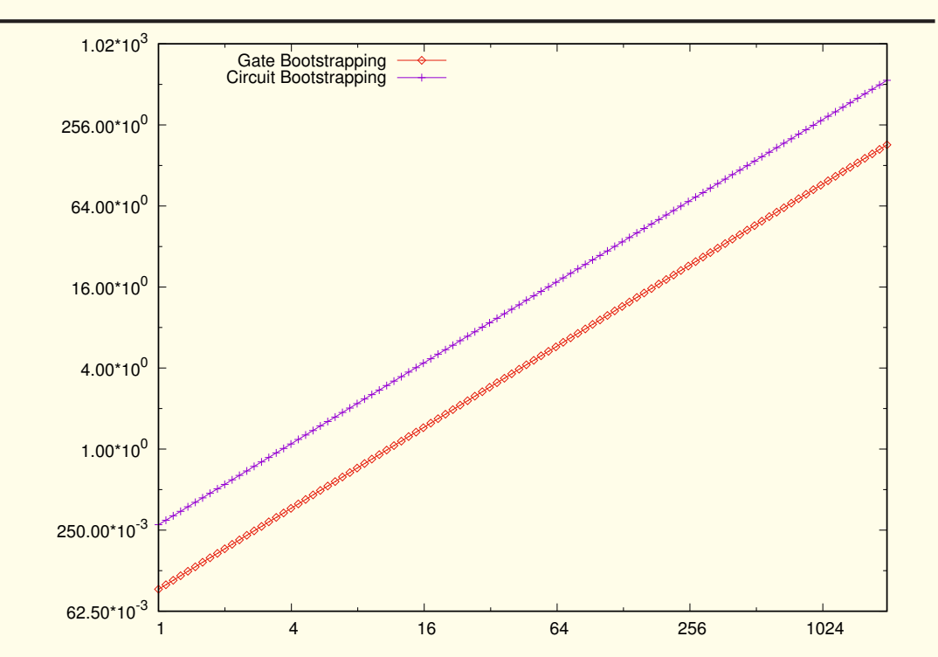
LUT (d-bits input and $s = $ 8-bits output)
- Gate bootst.: $(d + s(2^d - 1))t_{\mathsf{GB}}$
- Circuit bootst. with HP: $dt_{\mathsf{CB}} + (2^d - 1)t_{\mathsf{XP}}$
- Circuit bootst. with VP: $dt_{\mathsf{CB}} + s(2^d/N - 1 + \log N)t_{\mathsf{XP}}$.

Leveled HE MAX



Leveled Max (2 inputs of d-bits each)
- No packing: $3(d(d+1)/2)t_{\mathsf{XP}}$
- Gate bootst.: $5dt_{\mathsf{GB}}$
- Det Weighted automata (Det WFA): $5dt_{\mathsf{XP}}$

FHE MAX



Max (2 inputs of d-bits each)
- Gate bootst.: $7dt_{\mathsf{GB}}$
- Circuit bootst. with VP: $2dt_{\mathsf{CB}} + 5dt_{\mathsf{XP}}$