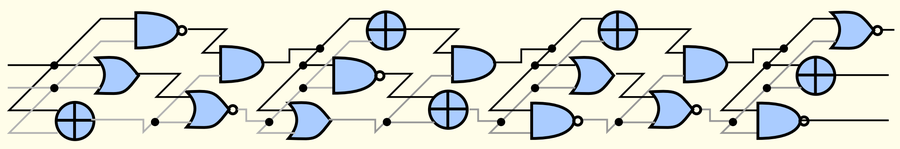
Toward a generic geometric API for FHE

N. Gama and M. Georgieva https://tfhe.github.io

inpher

Model of computations

1 Binary, circuit computations

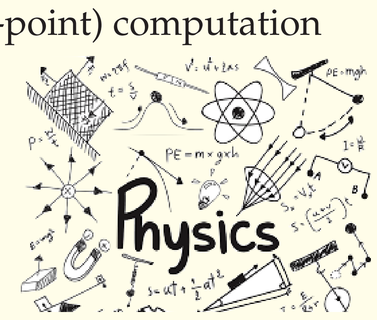


2 Integer arithmetic computation

decimal

```
  0 0 1 1  ← carries
  4 5 6 7
    3 6 6
  -------
  4 9 3 3
```

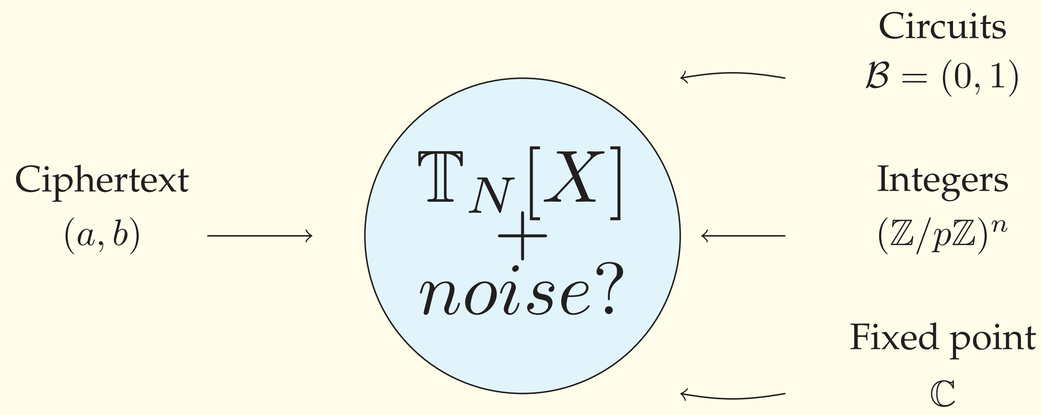
3 Approximated (fixed-point) computation



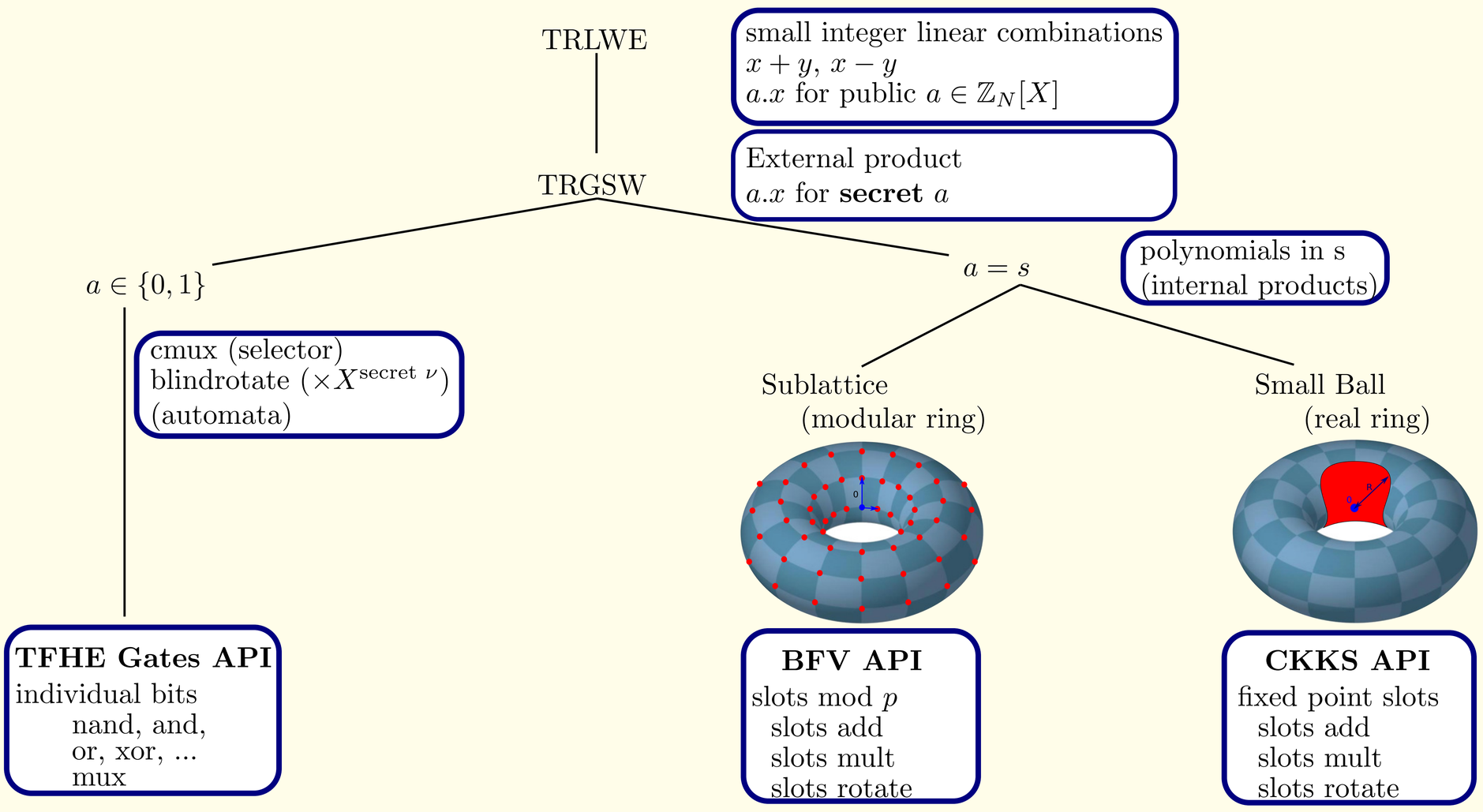
Some HE libraries and their strength

- BGV (Helib): massively parallel, finite field arithmetic
- BFV (Seal, Palisade): massively parallel, small depth polynomials
- CKKS (HEAAN): massively parallel, floating point arithmetic
- TFHE, FHEW: single eval, boolean logic, comparison, threshold

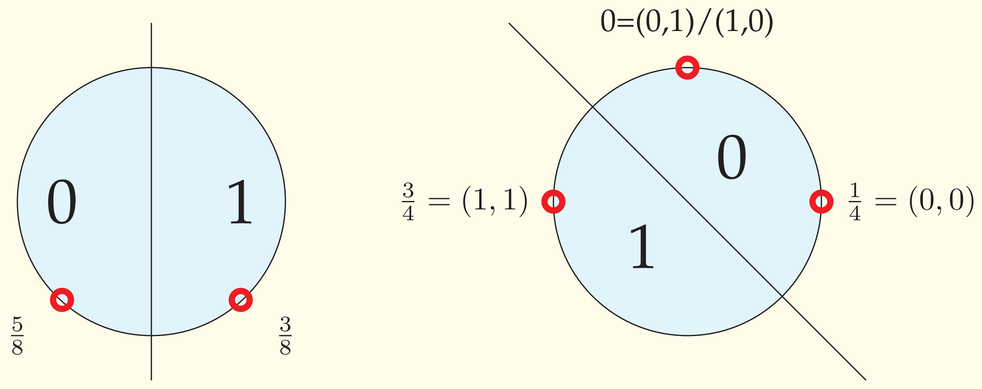
How we can represent all plaintexts over the $\mathbb{T}_N[X]$



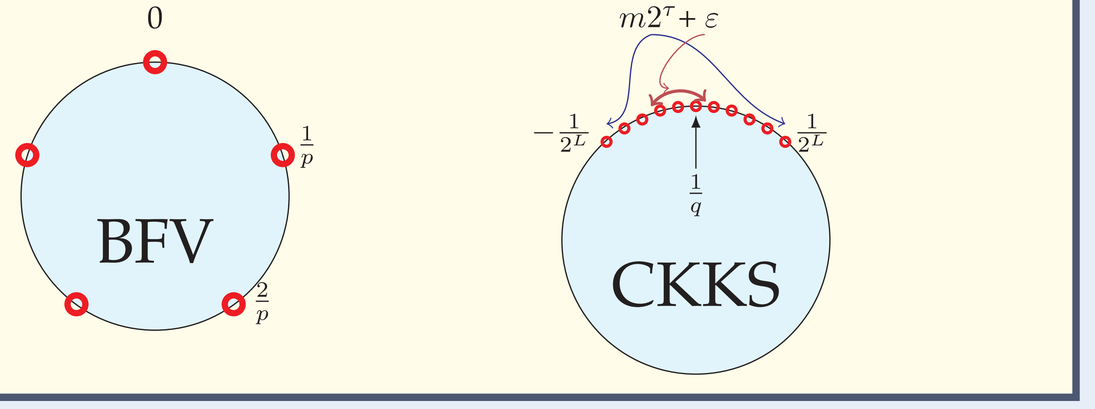
Homomorphic operations hierarchy



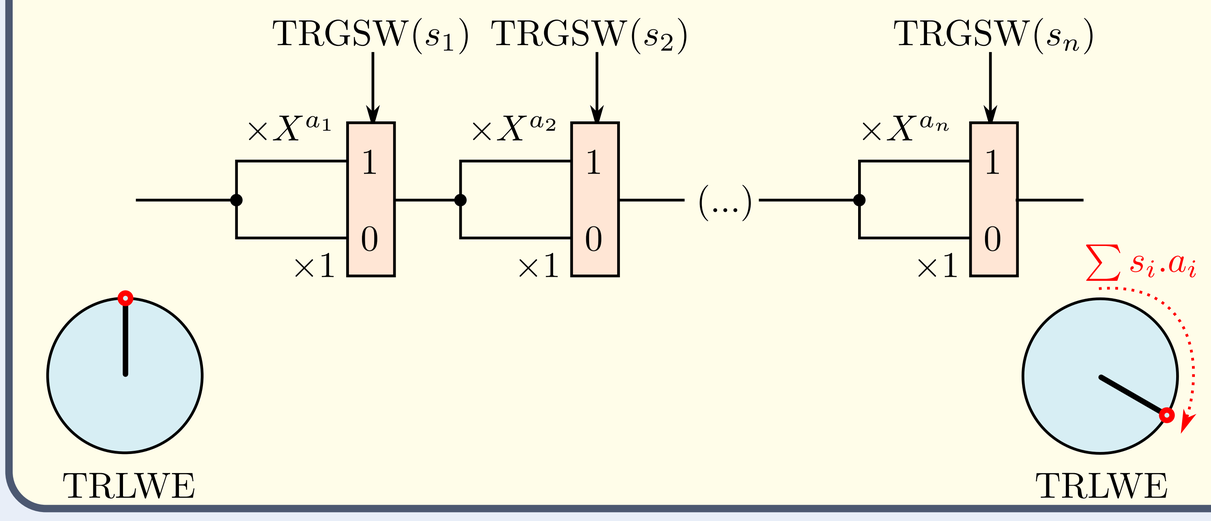
Circuits over $\mathbb{T}_N[X]$ (AND)



Integers and fixed-point over $\mathbb{T}_N[X]$



Linear combination with secret coefficients $(0,1)$



Linear combination with secret coefficient s

Internal product requires to evaluate a polynomial in s : $(b_1 - sa_1)(b_2 - sa_2)$

HowTo: evaluate a polynomial in s?

- dedicated relinearization/keyswitch techniques (2011, ...)
- But in fact, TRGSW provides multiplication by s !

$$C_1 \boxtimes_{P,\alpha} C_2 = (C_1, C_0) - TRGSW(s) \boxdot_\alpha (C_2, 0)$$