The ABC of Symmetric Primitives over Integer Rings: Milk Before Meat

Tim Beyne[1] Lorenzo Grassi[2] Morten Øygarden[3] **Berenika Richterová**[2]
Arne Sandrib[4]

[1] KU Leuven, Belgium
[2] TU Eindhoven, Netherlands
[3] University of Bergen and Simula UiB, Norway
[4] University of Bergen and Nasjonal Sikkerhetsmyndighet, Norway

May 2026

Applications of Symmetric Primitives

Standard

- Data encryption
- Binary fields

Recent

- MPC, HE, ZK
- Prime fields
- Integer rings $\mathbb{Z}_q$
  - Efficiency
  - Elisabeth, FRAST and Rubato

Applications of Symmetric Primitives

Standard

- Data encryption
- Binary fields

Recent

- MPC, HE, ZK
- Prime fields
- Integer rings $\mathbb{Z}_q$
  - Efficiency
  - Elisabeth, FRAST and Rubato

Challenges over $\mathbb{Z}_{p^n}$

- Elements without a multiplicative inverse
- Not every function admits a polynomial representation
- Not clear how to design a secure cipher over $\mathbb{Z}_{p^n}$
  - Security reasoned for an equivalent version of the cipher over $\mathbb{F}_{p^n}$ or $\mathbb{F}_p^n$

Challenges over $\mathbb{Z}_{p^n}$

- Elements without a multiplicative inverse
- Not every function admits a polynomial representation
- Not clear how to design a secure cipher over $\mathbb{Z}_{p^n}$
  - Security reasoned for an equivalent version of the cipher over $\mathbb{F}_{p^n}$ or $\mathbb{F}_p^n$

Challenges over $\mathbb{Z}_{p^n}$

- Elements without a multiplicative inverse
- Not every function admits a polynomial representation
- Not clear how to design a secure cipher over $\mathbb{Z}_{p^n}$
  - Security reasoned for an equivalent version of the cipher over $\mathbb{F}_{p^n}$ or $\mathbb{F}_p^n$

Bridging the Gap

Focus: SPN cipher resembling SHARK/AES - layer of non-lineal S-boxes

Security of polynomial ciphers over $\mathbb{Z}_{p^n}^t$

- Polynomial representation $\rightarrow$ algebraic attacks modulo $p, p^2, p^3, \ldots$
- Cipher insecure if p^t small
- Polynomial S-box layer $\rightarrow$ easier analysis of statistical attacks

Bridging the Gap

Security of non-polynomial ciphers over $\mathbb{Z}_{p^n}^t$

- How close is it to polynomial function modulo p^ℓ ?
  $\rightarrow$ probabilistic algebraic attacks
- How often $x \equiv y \mod p^\ell$ implies $\mathsf{C}(x) \equiv \mathsf{C}(y) \mod p^\ell$?
  $\rightarrow$ new truncated differential attack

$\rightarrow$ Criteria when designing a cipher over $\mathbb{Z}_{p^n}$

& more!

Bridging the Gap

Security of non-polynomial ciphers over $\mathbb{Z}_{p^n}^t$

- How close is it to polynomial function modulo p^ℓ ?
  $\rightarrow$ probabilistic algebraic attacks
- How often $x \equiv y \mod p^\ell$ implies $\mathsf{C}(x) \equiv \mathsf{C}(y) \mod p^\ell$?
  $\rightarrow$ new truncated differential attack

$\rightarrow$ Criteria when designing a cipher over $\mathbb{Z}_{p^n}$

& more!

Where to find us?

- Soon on ePrint!
- Crypto 2026

Thanks for your attention!