Compact implementations of pairings

Anthony Van Herrewege

Lejla Batina & Miroslav Knezevic
Prof. Dr. Ir. I. Verbauwhede & Prof. Dr. Ir. B. Preneel

22 May 2009

Outline

Symmetric cryptography

- Pro:
  - High security per bit
  - Very fast implementations
- Contra:
  - How to establish the key?

Asymmetric cryptography

- Pro:
  - No key establishment necessary
  - Central location with everyone's key
- Contra:
  - Need for certificate authorities, ...

Identity-based cryptography

- Pro:
  - Public key deduced from ID
  - No need for certificates
- Contra:
  - How to issue new keys, . . . ?
- Extra's:
  - Non-interactive key establishment
  - Date-stamped encryption

What?

- Mathematical construction discovered in the 40's
- Allow implementation of ID-based cryptography
- Strength based on discrete logarithm problem

How?

Several available pairings:

Weil, Tate, ate, eta, ...

Tate pairing:

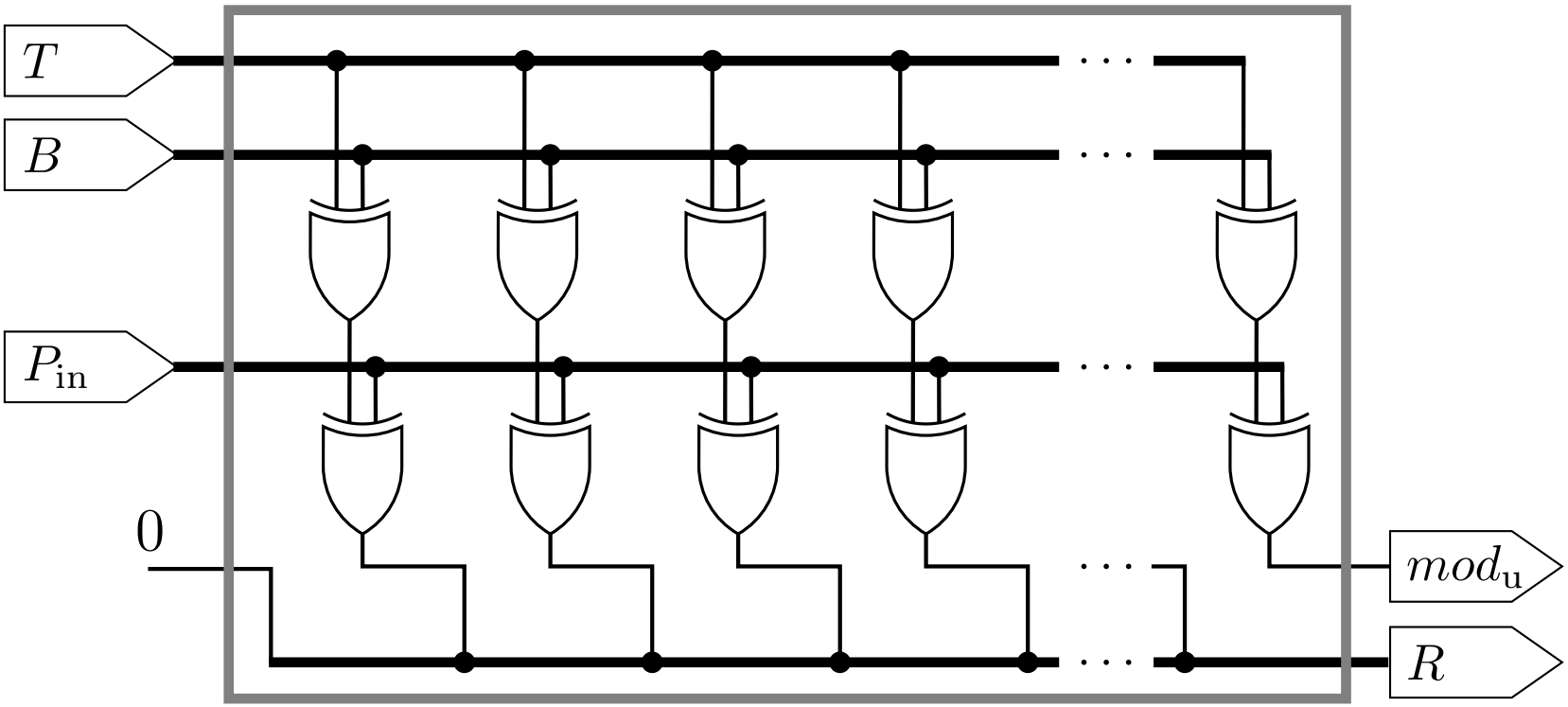
$$\hat{e}(P,Q) : E(\mathbb{F}_q)[l] \times E(\mathbb{F}_q)[l] \mapsto \mu_l$$

Mapping needs to be:

- Bilinear: $\hat{e}(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$
- Non-degenerate: $\hat{e}(P, P) \neq 1$
- Efficiently computable

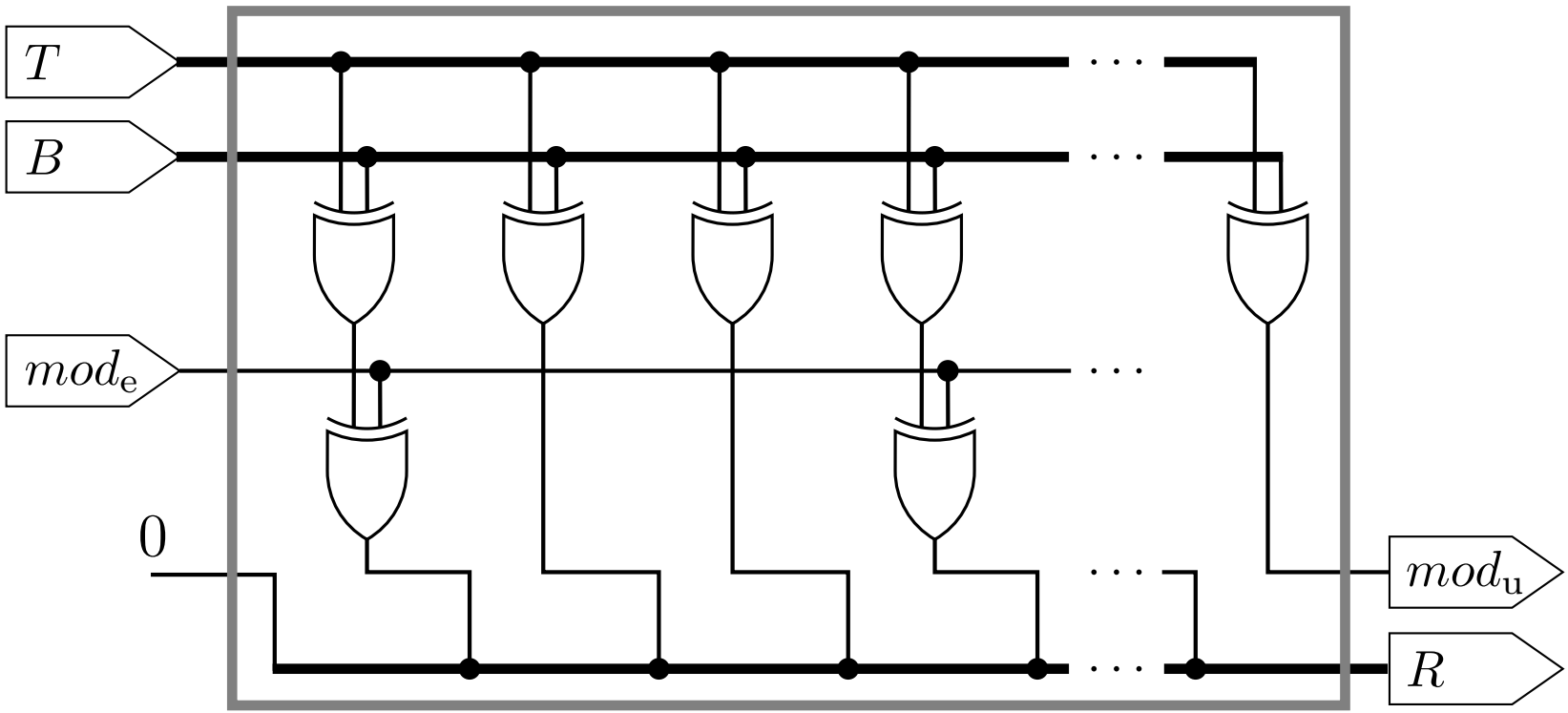
MALU

Modulo Arithmetic Logical Unit [general]:



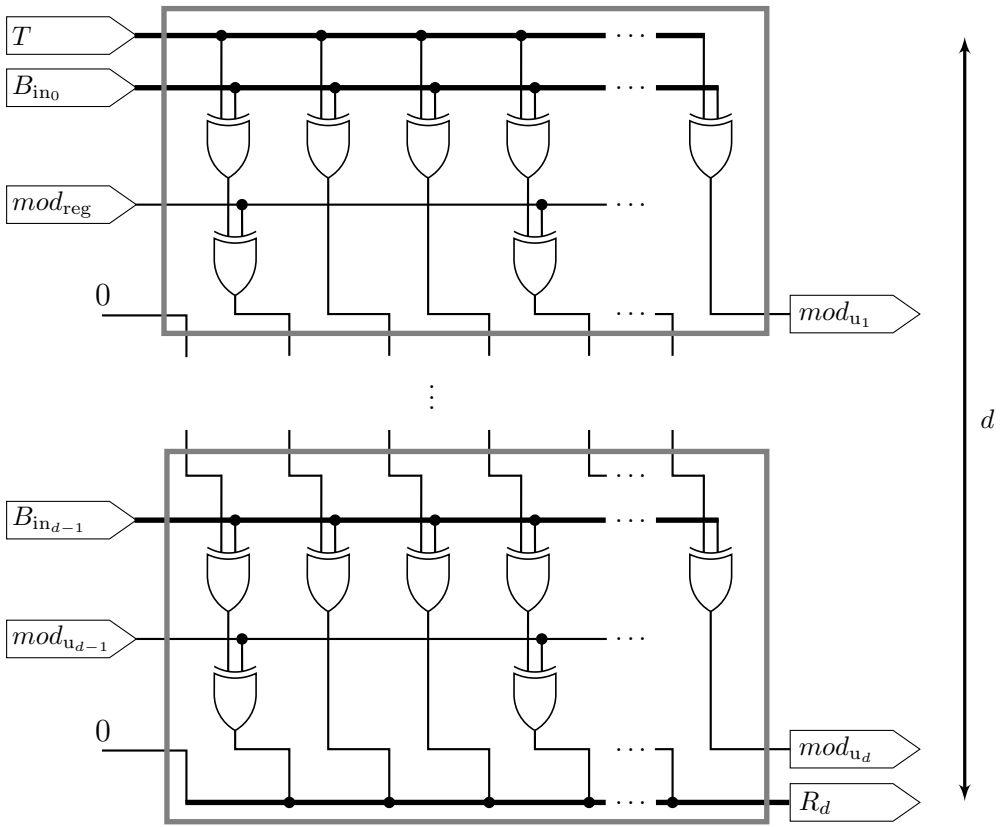
MALU

Modulo Arithmetic Logical Unit [optimized]:



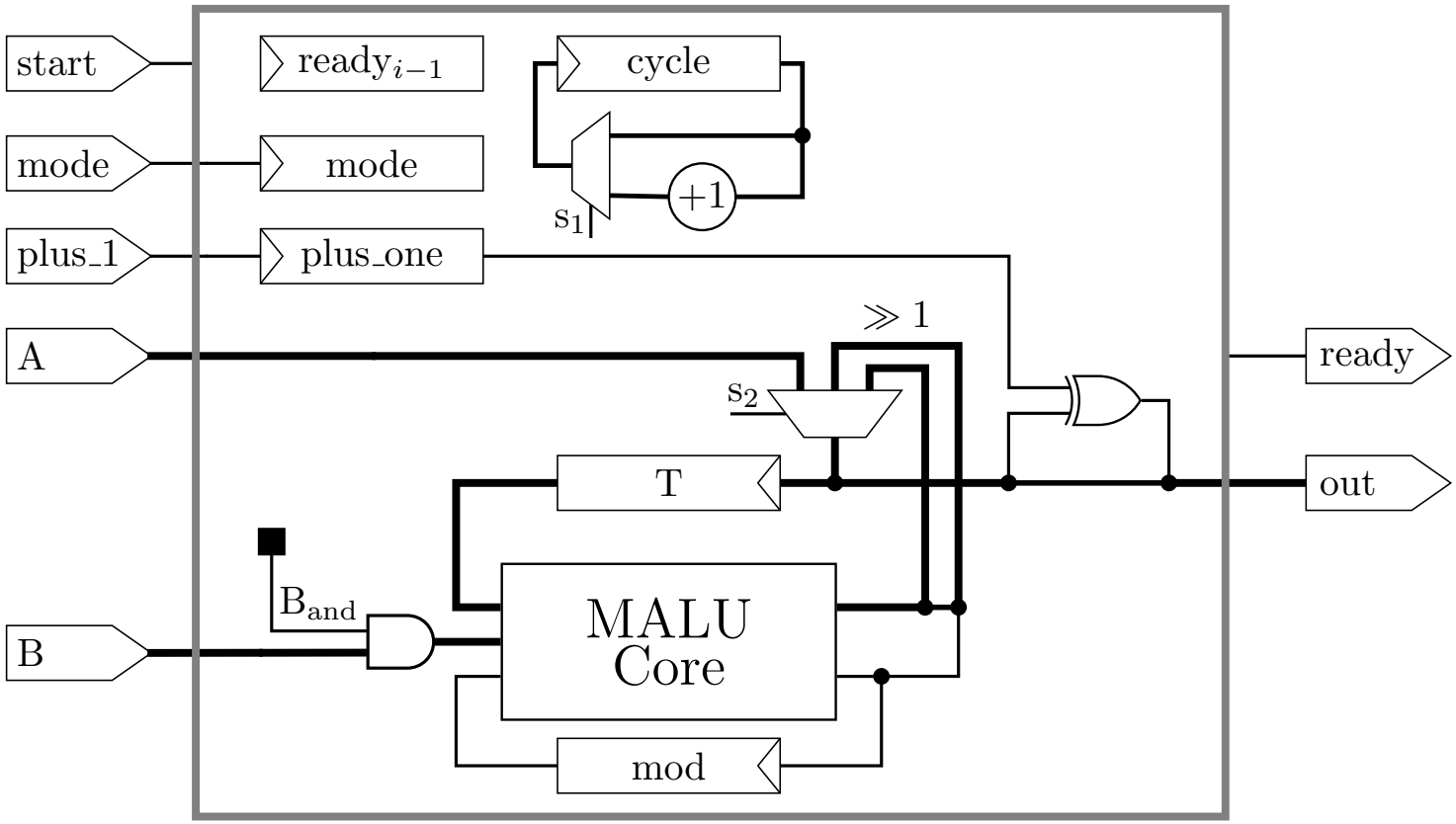
MALU

Modulo Arithmetic Logical Unit [optimized; d-bits wide]:

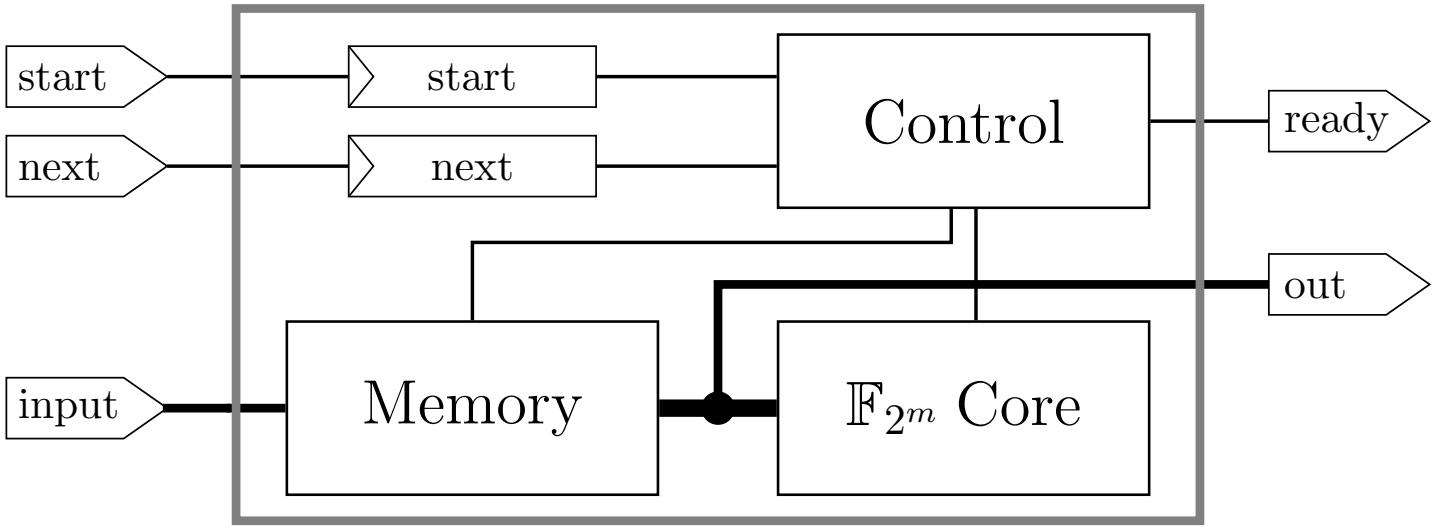


Wrappers - GF_{2^m}

GF_{2^m} Multiplication/Addition:



Controller - Miller's algorithm



State of the art

Some currently available implementations:

Name	Platform	Field	Speed
TinyTate	ATMega128L [7.4Mhz]	$\mathbb{F}_{2^{256}}$	30.2s
TinyPBC	ATMega128L [7.4Mhz]	$\mathbb{F}_{2^{256}}$	5.45s
Hankerson	P4 [2.8Ghz]	$\mathbb{F}_{2^{1223}}$	0.07s
Hankerson	P4 [2.8Ghz] (SSE)	$\mathbb{F}_{2^{1223}}$	0.03s

Progress so far

- MALU
- GF_{2^m} functions
- ECC functions
- Pairing functions (partial)

To do

- Complete pairing functions
- Bugfixing
- Optimization (VHDL)
- Write thesis text

The end

Questions?