

Compact implementations of pairings

Anthony Van Herrewege

Day. sup.: Dr. Lejla Batina, Miroslav Knezevic, Dr. Ir. Nele Mentens

Prom.: Prof. Dr. Ir. Ingrid Verbauwhede, Prof. Dr. Ir. Bart Preneel

Ass.: Prof. Dr. Ir. Wim Dehaene, Dr. Ir. Frederik Vercauteren

22 May 2009

Outline

1 Pairings

2 Implementation

3 Results

Outline

1 Pairings

2 Implementation

3 Results

Overview

- Several available pairings:

Weil, Tate, η_T , Ate, ...

Overview

- Several available pairings:

Weil, Tate, η_T , Ate, ...

- Bilinearity property:

$$e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

Overview

- Several available pairings:

Weil, Tate, η_T , Ate, ...

- Bilinearity property:

$$e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

- *Optimized* Tate pairing:

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

$$\mu_l = \text{group of } l\text{th roots of } \mathbb{F}_{q^k}^*$$

Possibilities

- Identity-based encryption

Possibilities

- Identity-based encryption
- Short signatures

Possibilities

- Identity-based encryption
- Short signatures
- Non-interactive key agreement

Possibilities

- Identity-based encryption
- Short signatures
- Non-interactive key agreement
- Tripartite key agreement in 1 round

Possibilities

- Identity-based encryption
- Short signatures
- Non-interactive key agreement
- Tripartite key agreement in 1 round
- ...

Outline

1 Pairings

2 Implementation

3 Results

Restrictions

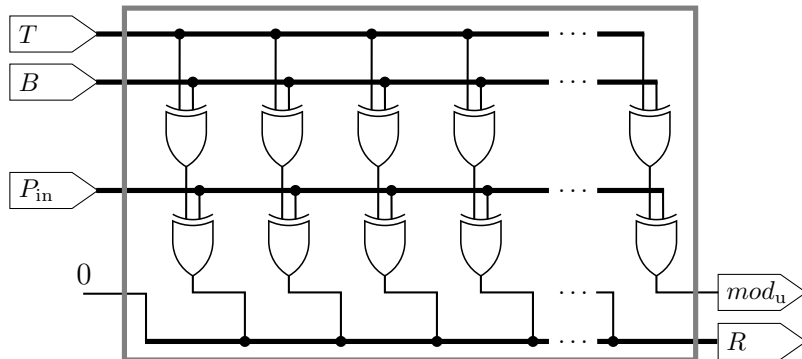
Avoid the use of flip-flops and muxes:

Cell	Area $\left[\frac{\text{gate}}{\text{bit}} \right]$
D flip-flop (reset)	6
D flip-flop (no reset)	5.5
D latch	4.25
3 input MUX	4
2 input XOR	3.75
2 input MUX	2.25
2 input NAND	1
NOT	0.75

MALU - Addition & Reduction in \mathbb{F}_{2^m}

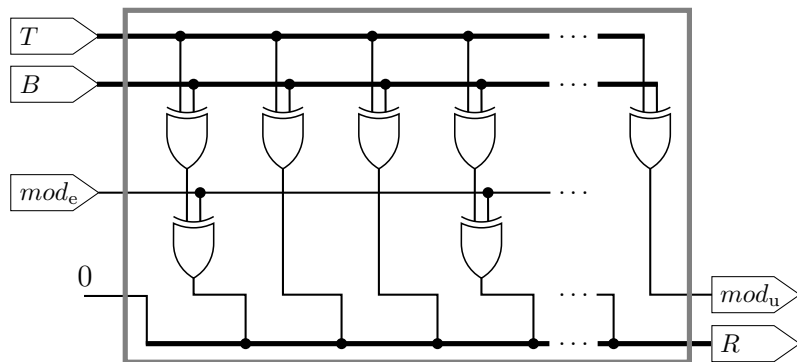
$$R = (T + B \pmod{P_{\text{in}}})_{0:m-2} \ll 1$$

$$\text{mod}_u = (T + B \pmod{P_{\text{in}}})_{m-1}$$

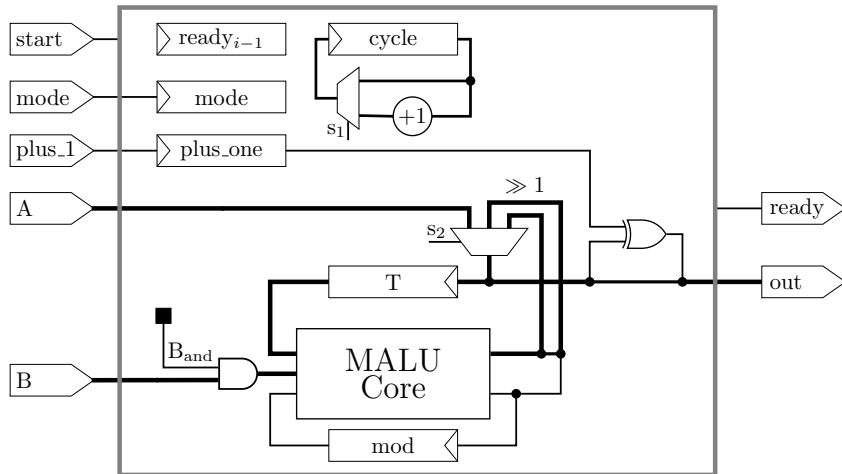


MALU - Addition & Reduction in \mathbb{F}_{2^m}

Optimized MALU needs $\Delta = m - (\text{Hamm}(P) - 1)$ less XORs:

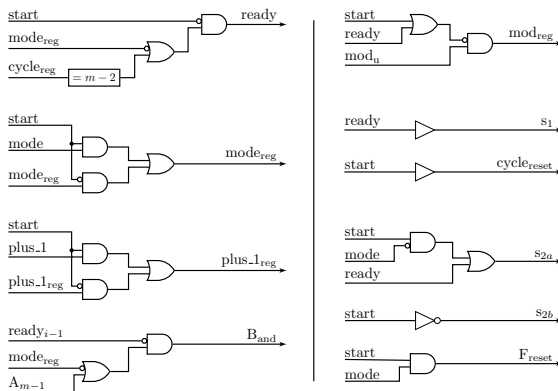


\mathbb{F}_{2^m} Multiplication & Addition



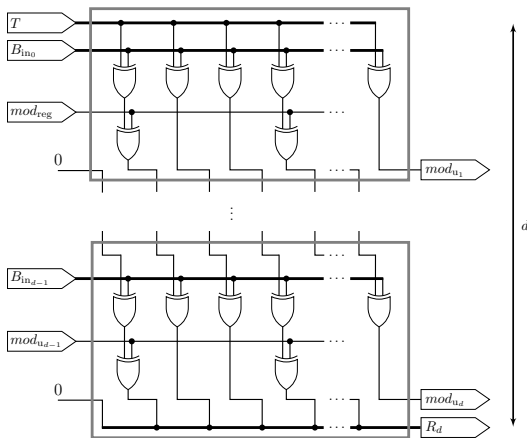
\mathbb{F}_{2^m} Multiplication & Addition

No FSM needed, simple logic:

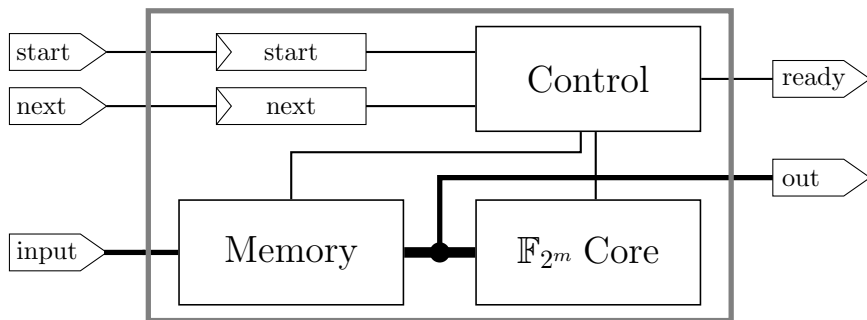


\mathbb{F}_{2^m} Multiplication & Addition

Speed up calculation by daisy-chaining MALUs ($m \bmod d!$):



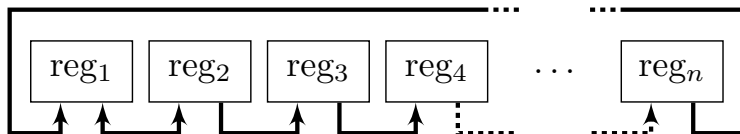
Controller for Miller's algorithm



Memory design

Initial design:

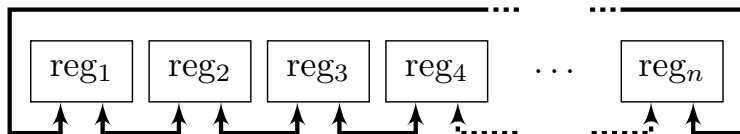
$$\bar{t} = O\left(\frac{n^2}{3}\right) \quad \bar{w} = O\left(\frac{n^3}{3}\right)$$



Memory design

Final design:

$$\bar{t} = O\left(\frac{n}{4}\right) \quad \bar{w} = O(n)$$



Optimizations

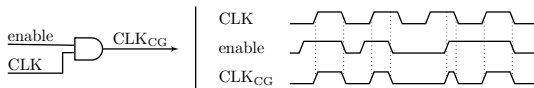
- Remove reset from registers ($-0.5 \frac{\text{gate}}{\text{bit}}$)

Optimizations

- Remove reset from registers ($-0.5 \frac{\text{gate}}{\text{bit}}$)
- Implement clock gating:

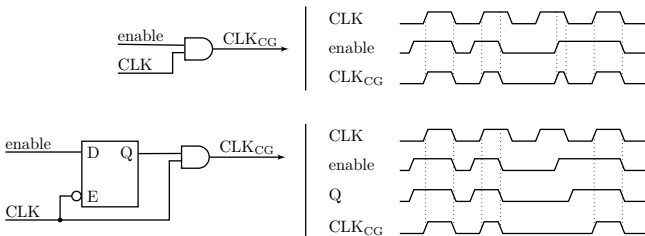
Optimizations

- Remove reset from registers ($-0.5 \frac{\text{gate}}{\text{bit}}$)
- Implement clock gating:



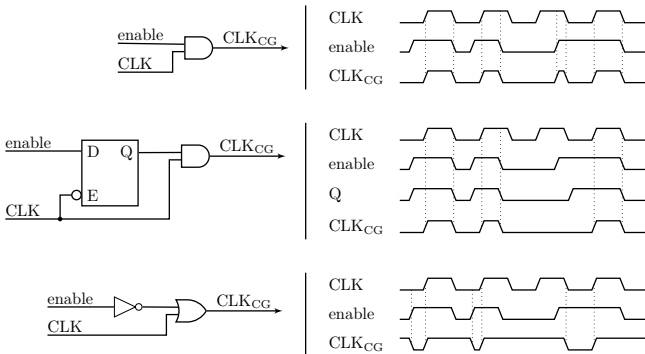
Optimizations

- Remove reset from registers ($-0.5 \frac{\text{gate}}{\text{bit}}$)
- Implement clock gating:



Optimizations

- Remove reset from registers ($-0.5 \frac{\text{gate}}{\text{bit}}$)
- Implement clock gating:



Outline

1 Pairings

2 Implementation

3 Results

Runtime

- FSM with 553 states

Runtime

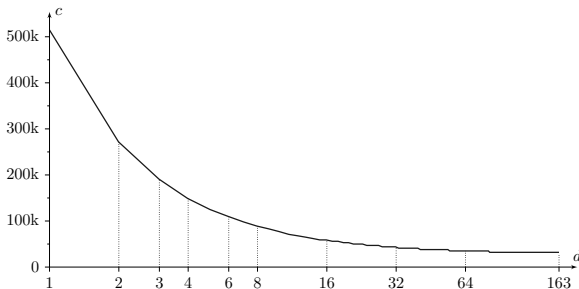
- FSM with 553 states
- Total n° of clock cycles c for one pairing:

$$c = 21681 + 4322 + 2998 \cdot \left\lceil \frac{m}{d} \right\rceil$$

Runtime

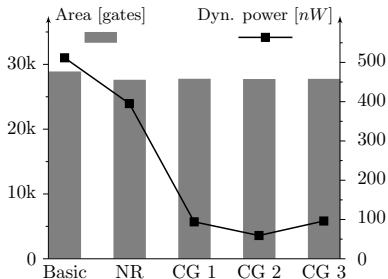
- FSM with 553 states
- Total n° of clock cycles c for one pairing:

$$c = 21681 + 4322 + 2998 \cdot \left\lceil \frac{m}{d} \right\rceil$$



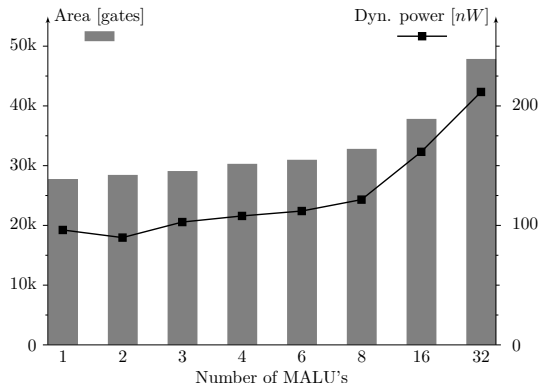
Synthesis

Implementation	Area [gates]		Power @ 10 kHz [<i>nW</i>]			
			Dynamic		Leakage	
Basic	28 876		512		117	
No Reset	27 596	96%	395	77%	107	92%
CG 1	27 751	96%	94	18%	109	94%
CG 2	27 713	96%	59	12%	102	88%
CG 3	27 734	96%	96	19%	110	94%



Synthesis - Continued

Component	Opp. [gates]	
MALU	458	1.7%
\mathbb{F}_{2^m} core		
Logic	783	2.8%
Registers	962	3.5%
Controller		
Logic	13 044	47%
Registers	12 487	45%
Total	27 734	100%



Comparison

	This work		Beuchat <i>et al.</i>
	1 MALU	2 MALUs	
Field	$\mathbb{F}_{2^{163}}$	$\mathbb{F}_{2^{163}}$	$\mathbb{F}_{3^{97}}$
Pairing	Tate	Tate	η_T
Security [bit]	652	652	922
Technology [μm]	0.13	0.13	0.18
Area [gates]	27 430	28 155	193 765
f [MHz]	10.3	5.44	200
Calc. time [μs]	$50 \cdot 10^3$	$50 \cdot 10^3$	46.7
Power [mW]	$98.3 \cdot 10^{-3}$	$48.6 \cdot 10^{-3}$	672
Efficiency [$\frac{nJ}{bit}$]	7.54	3.73	34.0

$$\text{Efficiency} = \frac{\text{power} \times \text{calc. time}}{\text{bits security}}$$

Conclusion

- Very small: $< 30k$ gates

Conclusion

- Very small: $< 30k$ gates
- Extremely low power: < 220 nA

Conclusion

- Very small: $< 30k$ gates
- Extremely low power: < 220 nA
- Energy efficiency improvement up to more than $25\times$ possible

Conclusion

- Very small: $< 30\text{k}$ gates
- Extremely low power: $< 220\text{ nA}$
- Energy efficiency improvement up to more than $25\times$ possible

Definitely possible to use in constrained environments

Conclusion

- Very small: $< 30\text{k}$ gates
- Extremely low power: $< 220\text{ nA}$
- Energy efficiency improvement up to more than $25\times$ possible

Definitely possible to use in constrained environments

- Example with 3 MALUs:

Area = 29k gates

$f = 9.70\text{ Mhz}$

Power = $100\text{ }\mu\text{A}$

Time = 19.6 ms

The end

Questions?