Arithmetic Operators for Pairing-Based Cryptography

J.-L. Beuchat[1] N. Brisebarre[2] J. Detrey[3] E. Okamoto[1]

[1]University of Tsukuba, Japan

[2]École Normale Supérieure de Lyon, France

[3]Cosec, b-it, Bonn, Germany

CHES 2007

Outline of the Talk

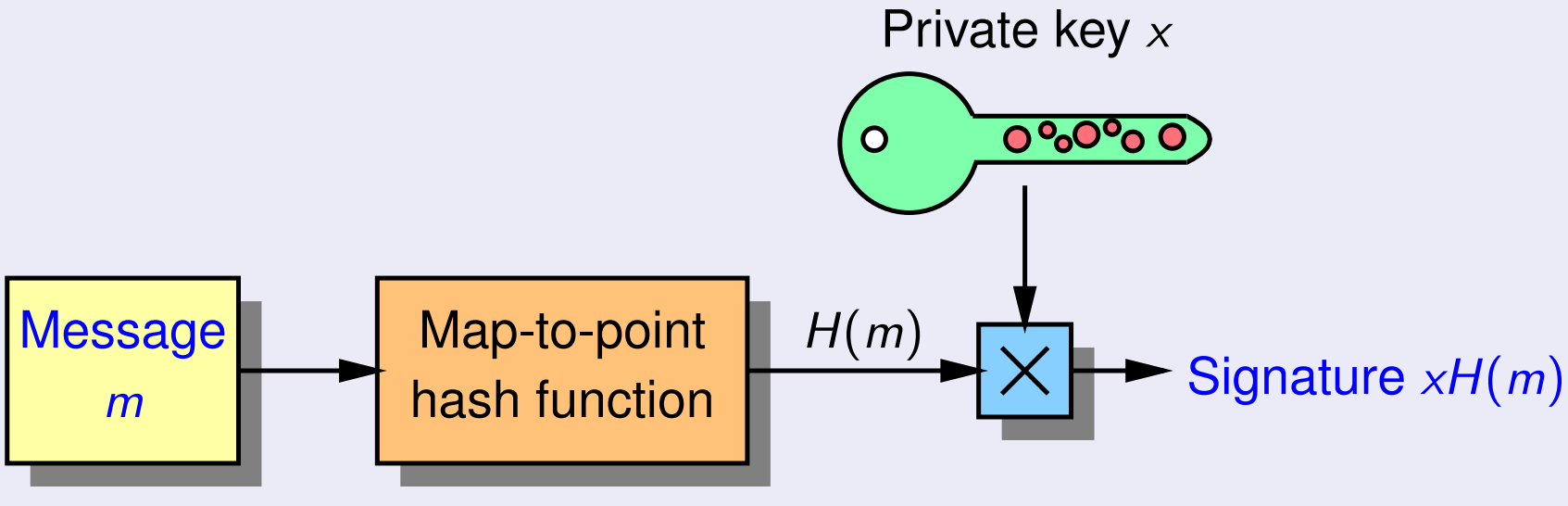
Example: BLS Short Signature Scheme

Key generation

- $G_1 = \langle P \rangle$: additively-written group of prime order q
- $H : \{0,1\}^* \to G_1$: map-to-point hash function
- Secret key: $x \in \{1, 2, \ldots, q-1\}$
- Public key: $xP \in G_1$

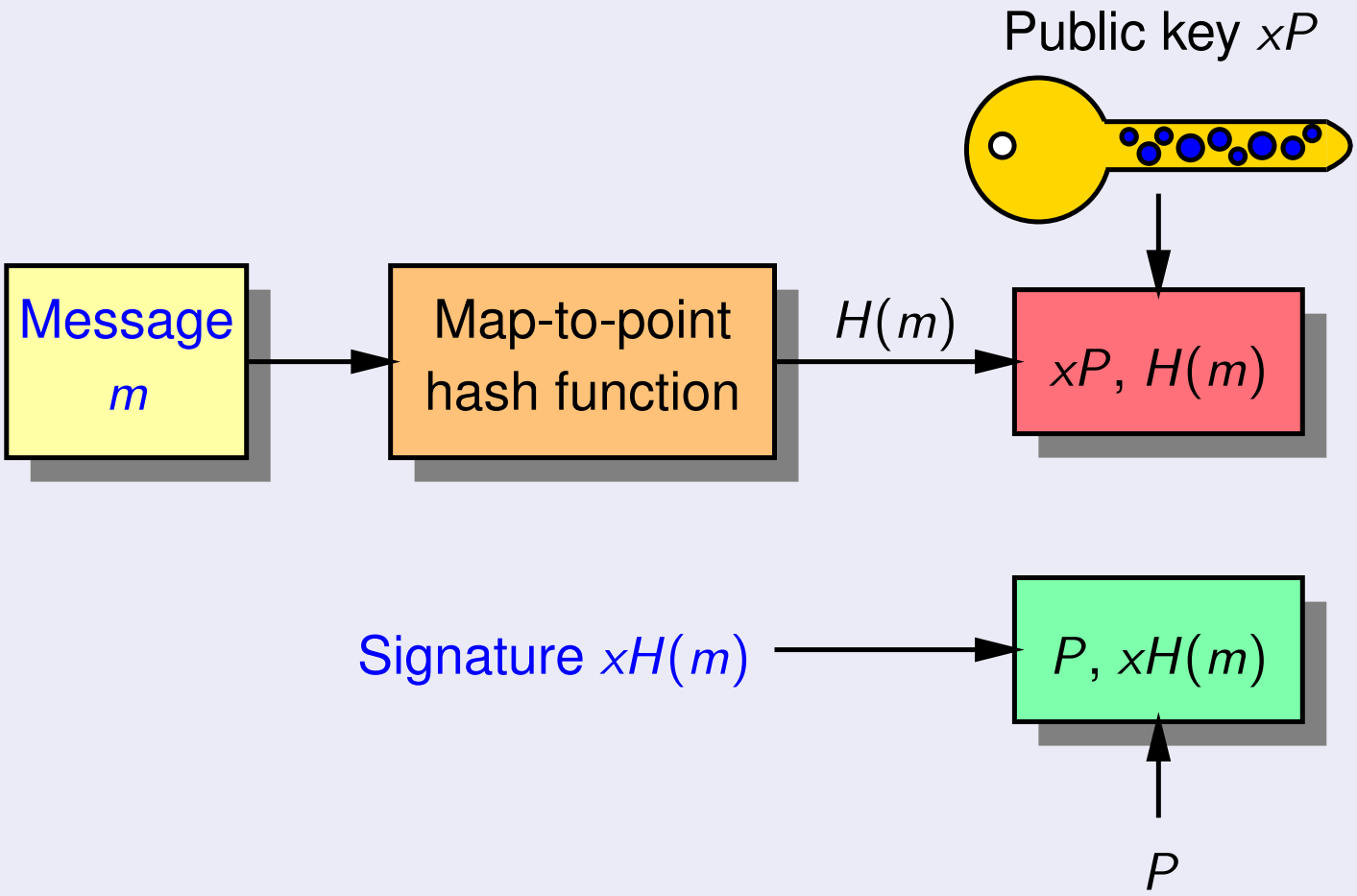
Example: BLS Short Signature Scheme

Sign



Example: BLS Short Signature Scheme

Verify



Example: BLS Short Signature Scheme

Bilinear pairing

- $G_1 = \langle P \rangle$: additively-written group
- G_2: multiplicatively-written group with identity 1
- A bilinear pairing on (G_1, G_2) is a map

$$\hat{e} : G_1 \times G_1 \to G_2$$

that satisfies the following conditions:

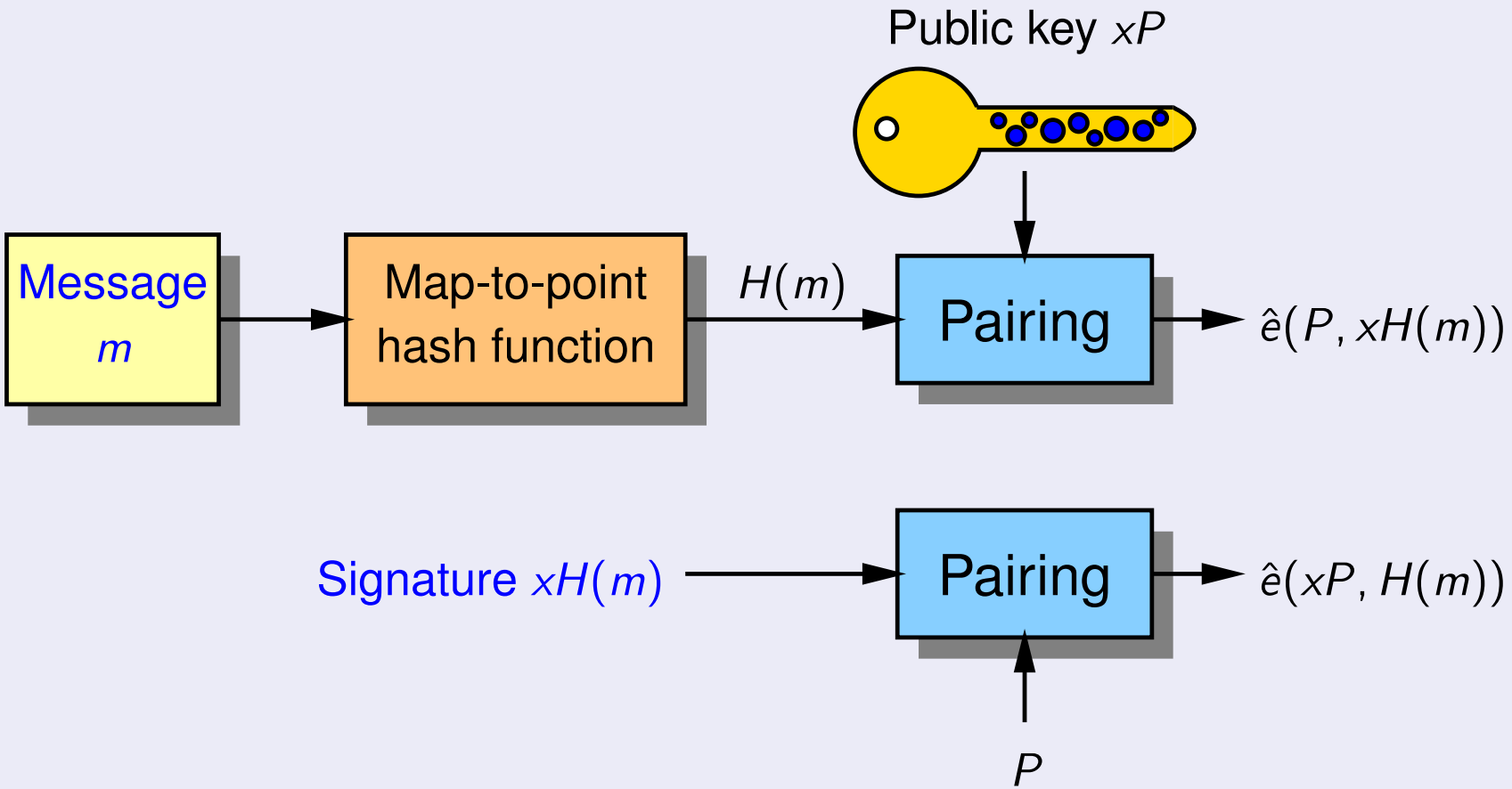
1. **Bilinearity.** For all Q, R, $S \in G_1$,

$$\hat{e}(Q + R, S) = \hat{e}(Q, S)\hat{e}(R, S) \quad \text{and} \quad \hat{e}(Q, R + S) = \hat{e}(Q, R)\hat{e}(Q, S).$$

2. **Non-degeneracy.** $\hat{e}(P, P) \neq 1$.
3. **Computability.** $\hat{e}$ can be efficiently computed.

Example: BLS Short Signature Scheme

Verify



$$\hat{e}(xP, H(m)) = \hat{e}(P, xH(m)) = \hat{e}(P, H(m))^x$$

Example: BLS Short Signature Scheme

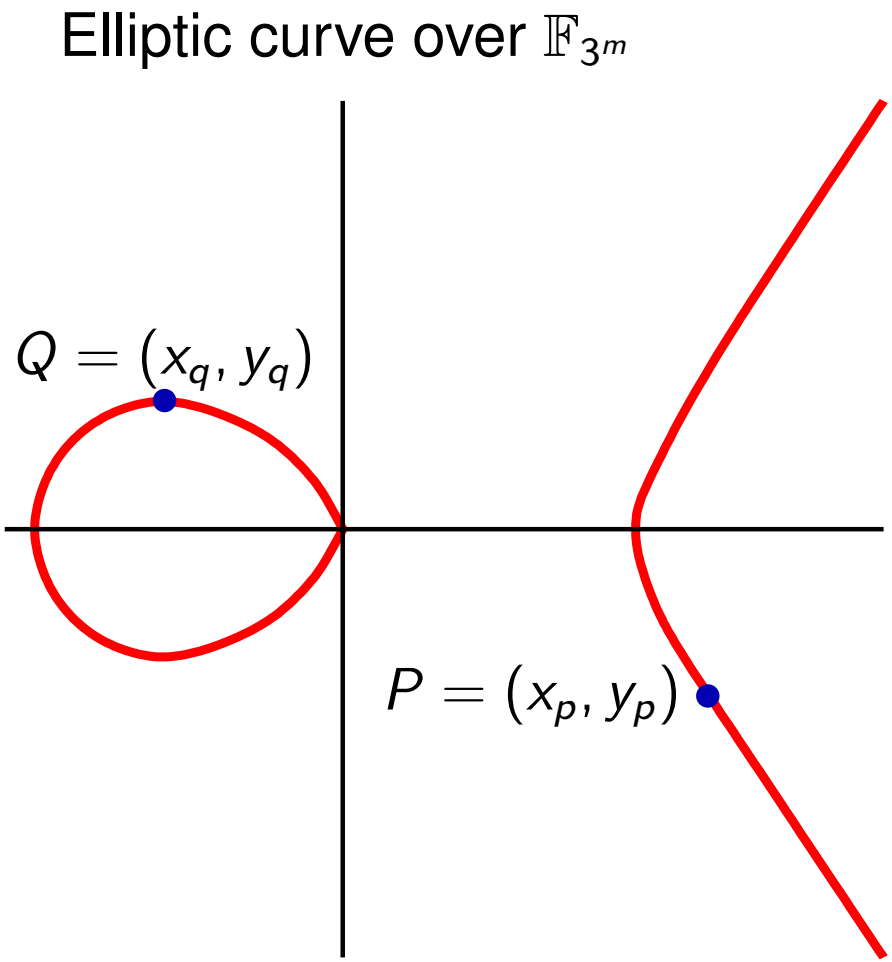
Examples of cryptographic bilinear maps

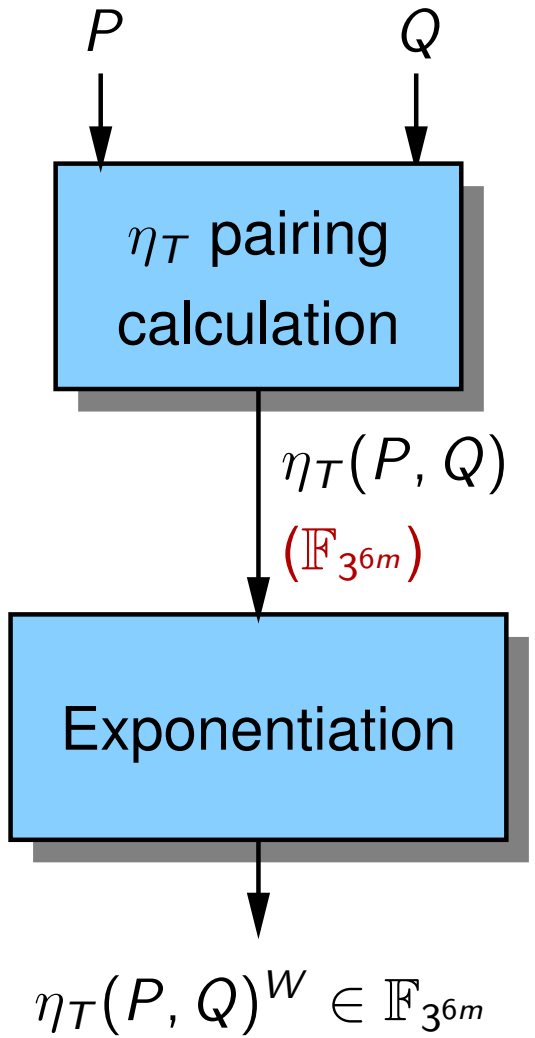
- Weil pairing
- Tate pairing
- η_T pairing (Barreto *et al.*)
- Ate pairing (Hess *et al.*)

Applications

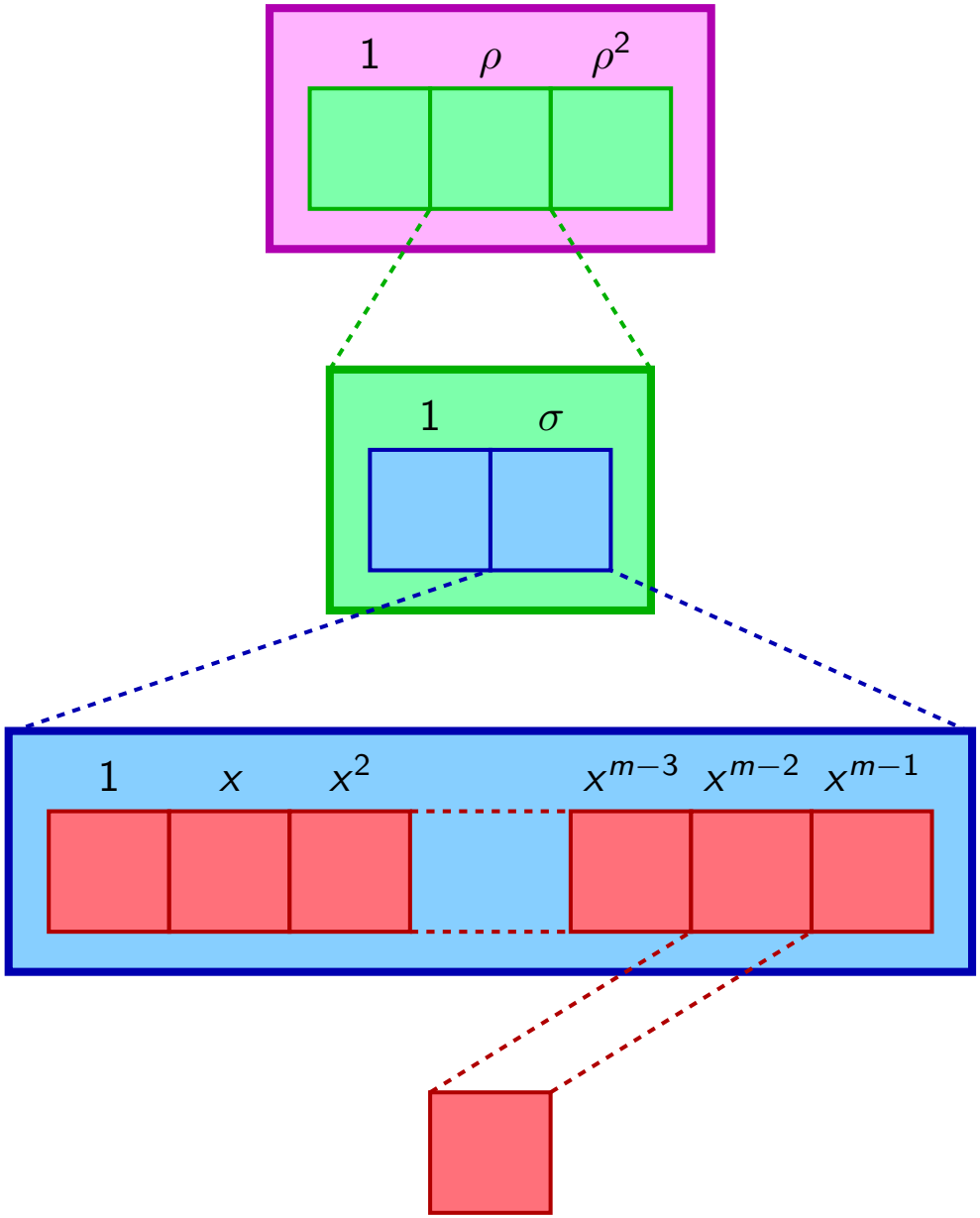
- Identity based encryption
- Short signature

Computation of the Full η_T Pairing





Computation of the Full η_T Pairing – Tower Field



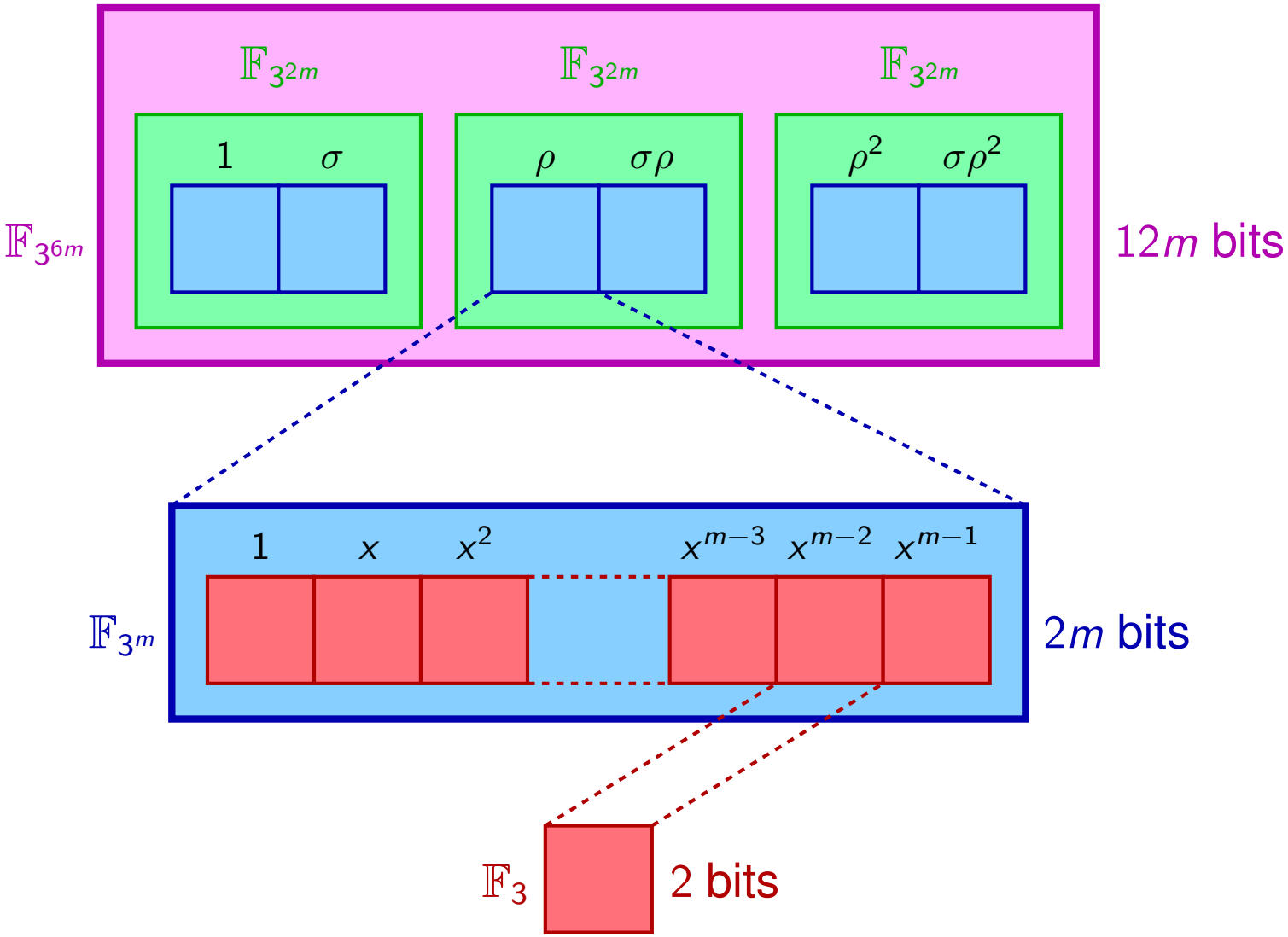
$$\mathbb{F}_{3^{6m}} = \mathbb{F}_{3^{2m}}[\rho]/(\rho^3 - \rho - 1)$$

$$\mathbb{F}_{3^{2m}} = \mathbb{F}_{3^m}[\sigma]/(\sigma^2 + 1)$$

$$\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(f(x))$$

$$\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$$

Computation of the Full η_T Pairing – Tower Field



Computation of the Full η_T Pairing

$\eta_T(P,Q)$

- Addition
- Multiplication
- Cubing
- Cube root

$\eta_T(P,Q)^{3^{\frac{m+1}{2}}}$ (Arith 18)

- Addition
- Multiplication
- Cubing

Bilinearity of $\eta_T(P,Q)^W$

$$\eta_T(P,Q)^W = \sqrt[3^m]{\left(\eta_T\left(\left[3^{\frac{m-1}{2}}\right]P,Q\right)^{3^{\frac{m+1}{2}}}\right)^W}$$

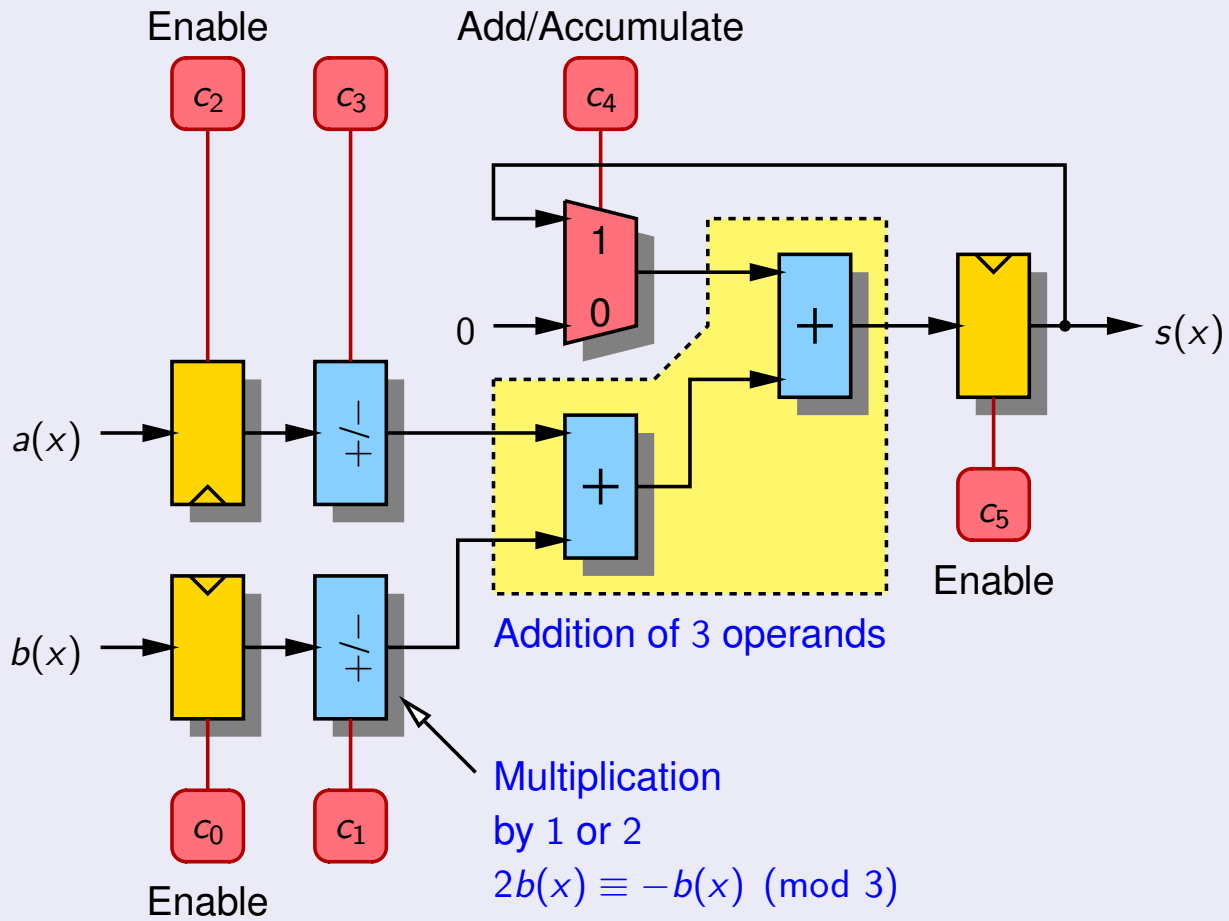
A Coprocessor for the Full Pairing Computation

Operations over $\mathbb{F}_{3^m}$

Additions	$51 \cdot \frac{m-1}{2} + 503$
Multiplications	$15 \cdot \frac{m-1}{2} + 86$
Cubings	$10m + 2$
Inversion	1

A Coprocessor for the Full Pairing Computation

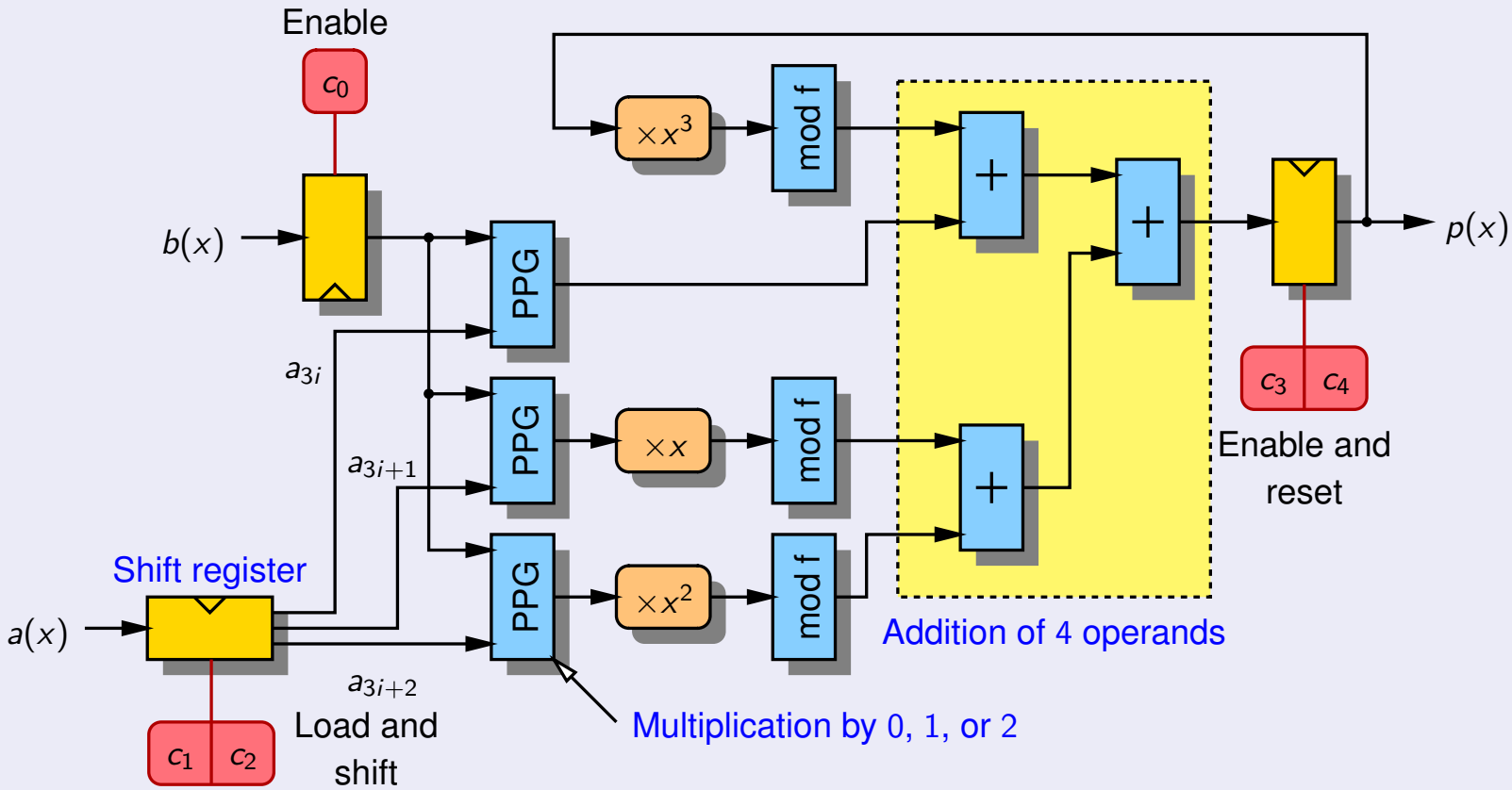
Addition, subtraction, and accumulation over $\mathbb{F}_{3^m}$



A Coprocessor for the Full Pairing Computation

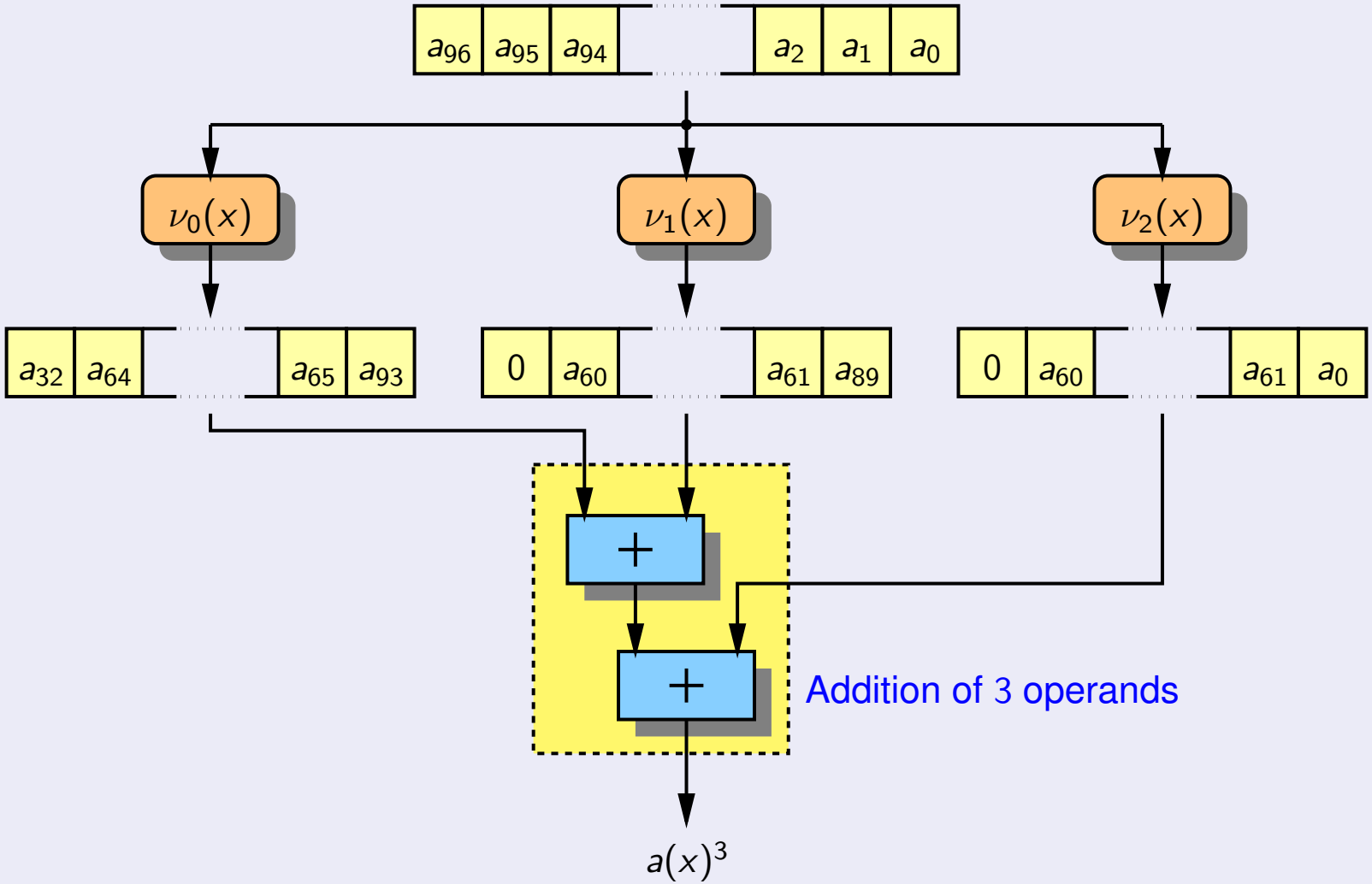
Multiplication over $\mathbb{F}_{3^m}$

- Array multiplier ($\lceil m/3 \rceil$ clock cycles)
- Most significant coefficient first (Horner's rule)



A Coprocessor for the Full Pairing Computation

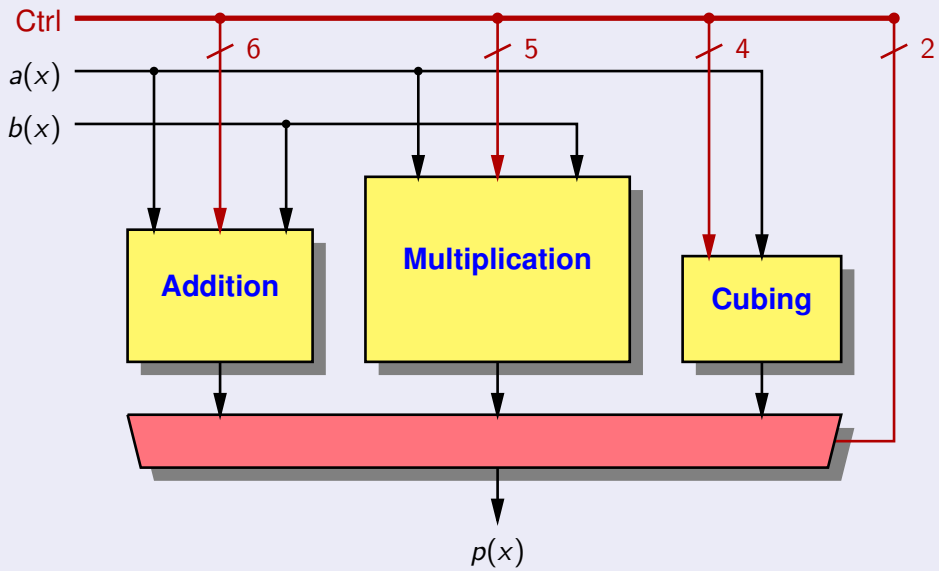
Cubing over $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$



A Coprocessor for the Full Pairing Computation

Arithmetic operators over $\mathbb{F}_{3^{97}}$ on a Cyclone II FPGA

Operation	Area [LEs]	Control [bits]
Add./sub.	970	6
Mult.	1375	5
Cubing	668	4
ALU	3308	17



A Coprocessor for the Full Pairing Computation

Unified arithmetic operator

- Operations
  - Addition
  - Subtraction
  - Accumulation
  - Multiplication
  - Cubing
- Area (Cyclone II): 2676 LEs (instead of 3308)
- Control bits: 11 (instead of 17)
- Inversion: Fermat's little theorem (96 cubings and 9 multiplications)

$$a^{3^m-2} = a^{-1}, \text{ where } a \in \mathbb{F}_{3^m}$$

A Coprocessor for the Full Pairing Computation

Results (CHES 2007)

- FPGA: Xilinx Virtex-II Pro 4
- $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$
- Area: 1888 slices + 6 memory blocks
- Clock frequency: 147 MHz
- Clock cycles for a full pairing: 32618
- Calculation time: 222 μs

A Coprocessor for the Full Pairing Computation

Results (CHES 2007)

- FPGA: Xilinx Virtex-II Pro 4
- $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$
- Area: 1888 slices + 6 memory blocks
- Clock frequency: 147 MHz
- Clock cycles for a full pairing: 32618
- Calculation time: 222 μs

Extended Euclidean algorithm (EEA)

- Area: 2210 additional slices
- Clock cycles for a full pairing: 32419 instead of 32618

A Coprocessor for the Full Pairing Computation

Results (new software for the CHES 2007 processor)

- FPGA: Xilinx Virtex-II Pro 4
- $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$
- Area: 1888 slices + 6 memory blocks
- Clock frequency: 147 MHz
- Clock cycles for a full pairing: 28201
- Calculation time: 192 μs

Results and Conclusion

Comparisons

Architecture	Area	Calculation time	FPGA
CHES 2007	1888 slices	222 μs	Virtex-II Pro
CHES 2007 (new software)	1888 slices	192 μs	Virtex-II Pro
Grabher and Page (CHES 2005)	4481 slices	432 μs	Virtex-II Pro
Ronan *et al.* (ITNG 2007)	10000 slices	178 μs	Virtex-II Pro

Results and Conclusion

Comparisons

Architecture	Area	Calculation time	FPGA
CHES 2007 (new software)	1888 slices	192 μs	Virtex-II Pro
CHES 2007 (new software)	1857 slices	141 μs	Virtex-4 LX
Kerins *et al.* (CHES 2005)	55616 slices	850 μs	Virtex-II Pro
η_T Pairing IP Core (synthesis)	74105 slices	8 μs	Virtex-4 LX
η_T Pairing IP Core (PAR)	–	20 μs	Virtex-4 LX
Arith 18 & Waifi 2007	18000 LEs	33 μs	Cyclone II

(1 slice $\approx$ 2 LEs)

Results and Conclusion

VHDL code generator

- Automatic generation of a unified operator according to $\mathbb{F}_{p^m} = \mathbb{F}_p/(f)$, where f is an irreducible degree-m polynomial
- Support for the following operations:
  - Addition
  - Multiplication
  - Frobenius ($a(x)^p \bmod f(x)$)
  - Inverse Frobenius ($\sqrt[p]{a(x)} \bmod f(x)$)

Results and Conclusion

VHDL code generator

- Automatic generation of a unified operator according to $\mathbb{F}_{p^m} = \mathbb{F}_p/(f)$, where f is an irreducible degree-m polynomial
- Support for the following operations:
  - Addition
  - Multiplication
  - Frobenius ($a(x)^p \bmod f(x)$)
  - Inverse Frobenius ($\sqrt[p]{a(x)} \bmod f(x)$)

Estimated area, frequency, and computation time (Virtex-II Pro)

Polynomial	**D = 3**	**D = 7**
$x^{97} + x^{12} + 2$	1402 slices – 147 MHz – 222 μs	2189 slices – 117 MHz – 146 μs
$x^{97} + x^{16} + 2$	1392 slices – 151 MHz – 216 μs	2246 slices – 116 MHz – 148 μs
$x^{193} + x^{64} + 2$	2811 slices – 126 MHz – 877 μs	4450 slices – 108 MHz – 495 μs

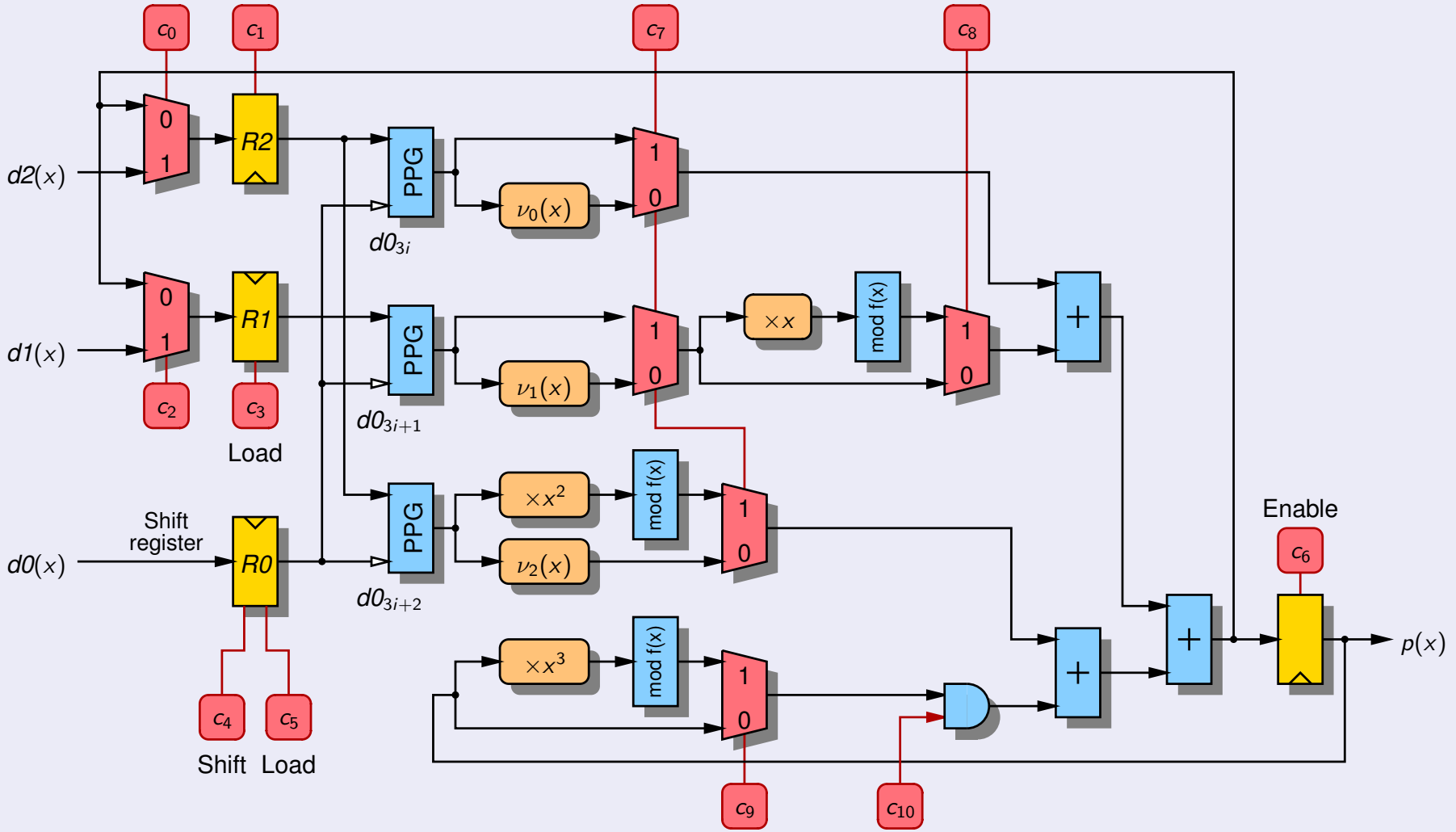
Results and Conclusion

Future work

- Automatic generation of the control unit
- New version of the software
- Application (*e.g.* short signature)
- Genus 2 curves
- Side-channel

A Coprocessor for the Full Pairing Computation

Unified arithmetic operator



A Coprocessor for the Full Pairing Computation