7. Kryptotag – November 9th, 2007

Arithmetic operators for pairing-based cryptography

Jérémie Detrey

Cosec, B-IT, Bonn, Germany

jdetrey@bit.uni-bonn.de

Joint work with:

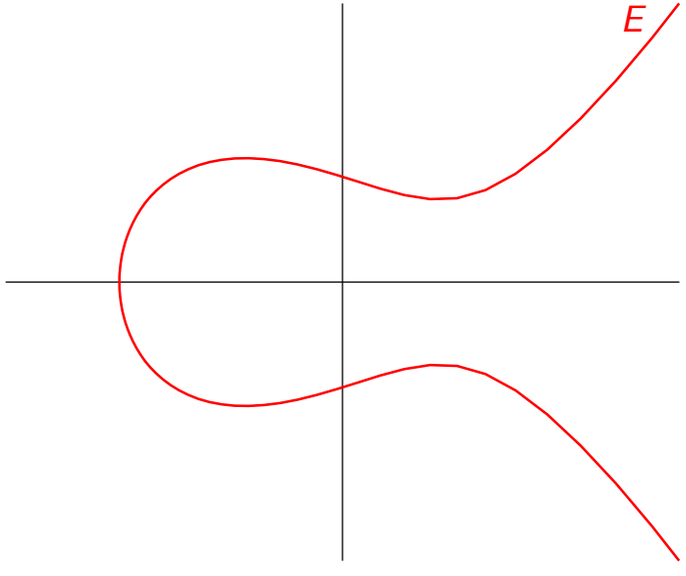
Jean-Luc Beuchat	LCIS, University of Tsukuba, Japan
Nicolas Brisebarre	LIP, École Normale Supérieure de Lyon, Lyon, France
Eiji Okamoto	LCIS, University of Tsukuba, Japan
Masaaki Shirase	IST Lab., Future University, Hakodate, Japan
Tsuyoshi Takagi	IST Lab., Future University, Hakodate, Japan

Outline of the talk

- Pairings?
- Arithmetic over $\mathbb{F}_{3^m}$
- Unified operator
- Results
- Final thoughts

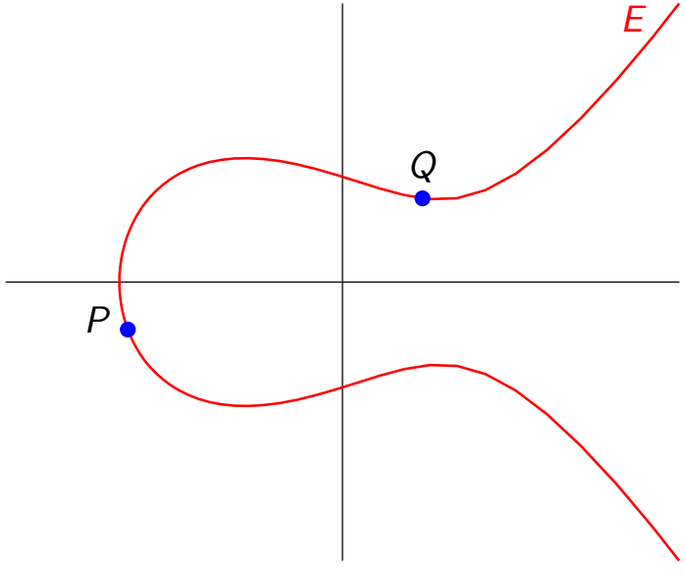
Elliptic curves

- E defined by an equation of the form
  $y^2 = x^3 + Ax + B$



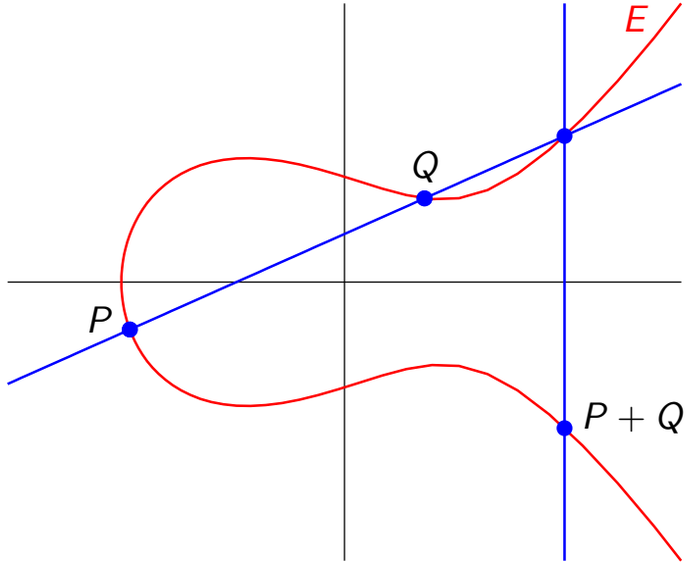
Elliptic curves

- E defined by an equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field K



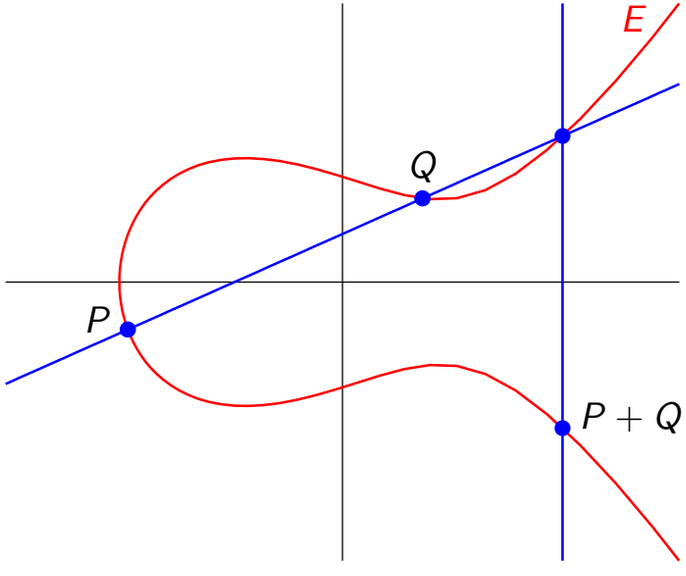
Elliptic curves

- E defined by an equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field K
- Additive group law over $E(K)$



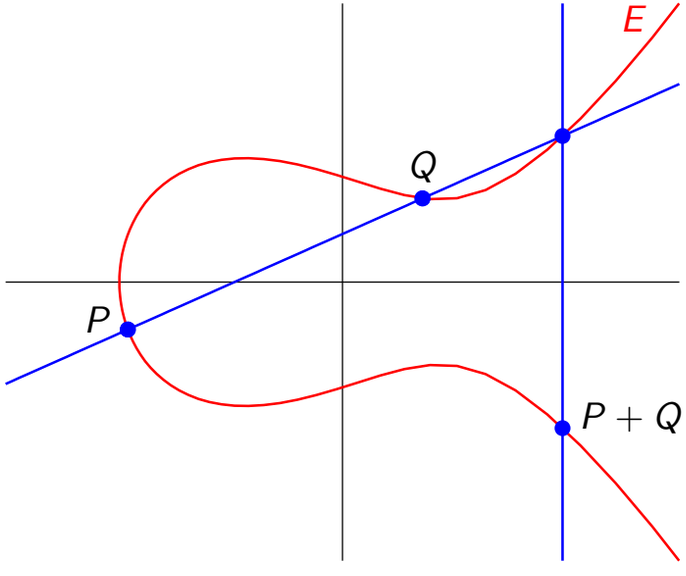
Elliptic curves

- E defined by an equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field K
- Additive group law over $E(K)$
- Many applications in cryptography
  - EC-based Diffie-Hellman key exchange
  - EC-based Digital Signature Algorithm
  - ...



Elliptic curves

- E defined by an equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field K
- Additive group law over $E(K)$
- Many applications in cryptography
  - EC-based Diffie-Hellman key exchange
  - EC-based Digital Signature Algorithm
  - ...
- But there's more: bilinear pairings



Bilinear pairings

- $G_1 = \langle P \rangle$ an additively-written group
- G_2 a multiplicatively-written group

Bilinear pairings

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

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

that satisfies the following conditions:

- computability: $\hat{e}$ can be efficiently computed
- non-degeneracy: $\hat{e}(P, P) \neq 1_{G_2}$
- bilinearity: for all Q_1, Q_2 and $R \in G_1$,

$$\hat{e}(Q_1 + Q_2, R) = \hat{e}(Q_1, R)\hat{e}(Q_2, R) \quad \text{and} \quad \hat{e}(R, Q_1 + Q_2) = \hat{e}(R, Q_1)\hat{e}(R, Q_2)$$

Bilinear pairings

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

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

that satisfies the following conditions:

- computability: $\hat{e}$ can be efficiently computed
- non-degeneracy: $\hat{e}(P, P) \neq 1_{G_2}$
- bilinearity: for all Q_1, Q_2 and $R \in G_1$,

$$\hat{e}(Q_1 + Q_2, R) = \hat{e}(Q_1, R)\hat{e}(Q_2, R) \quad \text{and} \quad \hat{e}(R, Q_1 + Q_2) = \hat{e}(R, Q_1)\hat{e}(R, Q_2)$$

- Immediate property: for any integer a,

$$\hat{e}(aP, P) = \hat{e}(P, aP) = \hat{e}(P, P)^a$$

Pairings in cryptography

- At first, used to reduce discrete logarithm problems to simpler instances
  - Menezes-Okamoto-Vanstone (MOV) attack, 1993

Pairings in cryptography

- At first, used to reduce discrete logarithm problems to simpler instances
  - Menezes-Okamoto-Vanstone (MOV) attack, 1993
- One-round three-party key agreement (Joux, 2000)
- Identity-based encryption
  - Boneh-Franklin, 2001
  - Sakai-Kasahara, 2001
  - ...
- Short signatures
  - Boneh-Lynn-Shacham (BLS), 2001
  - Zang-Safavi-Naini-Susilo (ZSS), 2004
  - ...

Pairings over elliptic curves

- E defined over a finite field $\mathbb{F}_{p^m}$, with p prime and $m \geq 1$
- An integer ℓ not divisible by p

Pairings over elliptic curves

- E defined over a finite field $\mathbb{F}_{p^m}$, with p prime and $m \geq 1$
- An integer ℓ not divisible by p
- Additive group, $\mathbb{F}_{p^m}$-rational ℓ-torsion points: $G_1 = E(\mathbb{F}_{p^m})[\ell]$
- Multiplicative group, ℓ-th roots of unity: $G_2 = \mu_\ell \subset \mathbb{F}^*_{p^{km}}$
- k is the embedding degree of the curve E

Pairings over elliptic curves

- E defined over a finite field $\mathbb{F}_{p^m}$, with p prime and $m \geq 1$
- An integer ℓ not divisible by p
- Additive group, $\mathbb{F}_{p^m}$-rational ℓ-torsion points: $G_1 = E(\mathbb{F}_{p^m})[\ell]$
- Multiplicative group, ℓ-th roots of unity: $G_2 = \mu_\ell \subset \mathbb{F}^*_{p^{km}}$
- k is the embedding degree of the curve E

$$\hat{e} : E(\mathbb{F}_{p^m})[\ell] \times E(\mathbb{F}_{p^m})[\ell] \longrightarrow \mu_\ell$$

Pairings over elliptic curves

- Which embedding degree?

Pairings over elliptic curves

- Which embedding degree?
  - ordinary curves? usually very large k

Pairings over elliptic curves

- Which embedding degree?
  - ordinary curves? usually very large k
  - supersingular curves?

Finite field $\mathbb{F}_{p^m}$	Maximal k
m even	3
m odd, $p = 2$	4
m odd, $p = 3$	6
m odd, $p > 3$	2

Pairings over elliptic curves

- Which embedding degree?
  - ordinary curves? usually very large k
  - supersingular curves?

Finite field $\mathbb{F}_{p^m}$	Maximal k
m even	3
m odd, $p = 2$	4
m odd, $p = 3$	6
m odd, $p > 3$	2

Pairings over elliptic curves

- Which embedding degree?
  - ordinary curves? usually very large k
  - supersingular curves?

Finite field $\mathbb{F}_{p^m}$	Maximal k
m even	3
m odd, $p = 2$	4
m odd, $p = 3$	6
m odd, $p > 3$	2

- Which pairing?
  - Weil pairing
  - Tate pairing
  - η_T pairing
  - Ate pairing

Pairings over elliptic curves

- Which embedding degree?
  - ordinary curves? usually very large k
  - supersingular curves?

Finite field $\mathbb{F}_{p^m}$	Maximal k
m even	3
m odd, $p = 2$	4
m odd, $p = 3$	6
m odd, $p > 3$	2

- Which pairing?
  - Weil pairing
  - Tate pairing
  - η_T pairing
  - Ate pairing

η_T pairing in characteristic 3

$$\hat{\eta_T} : E(\mathbb{F}_{3^m})[\ell] \times E(\mathbb{F}_{3^m})[\ell] \longrightarrow \mu_\ell \subset \mathbb{F}_{3^{6m}}$$

- Need for arithmetic over:
  - $\mathbb{F}_{3^m}$
  - $\mathbb{F}_{3^{6m}}$

η_T pairing in characteristic 3

$$\hat{\eta_T} : E(\mathbb{F}_{3^m})[\ell] \times E(\mathbb{F}_{3^m})[\ell] \longrightarrow \mu_\ell \subset \mathbb{F}_{3^{6m}}$$

- Need for arithmetic over:
  - $\mathbb{F}_{3^m}$
  - ~~$\mathbb{F}_{3^{6m}}$~~ arithmetic on the underlying field $\mathbb{F}_{3^m}$

η_T pairing in characteristic 3

$$\hat{\eta_T} : E(\mathbb{F}_{3^m})[\ell] \times E(\mathbb{F}_{3^m})[\ell] \longrightarrow \mu_\ell \subset \mathbb{F}_{3^{6m}}$$

- Need for arithmetic over:
  - $\mathbb{F}_{3^m}$
  - ~~$\mathbb{F}_{3^{6m}}$~~ arithmetic on the underlying field $\mathbb{F}_{3^m}$
- Operations over $\mathbb{F}_{3^m}$:

Operation	Count	$m = 97$
$+/-$	$121\lfloor\frac{m}{4}\rfloor + 186$	3090
$\times$	$25\lfloor\frac{m}{4}\rfloor + 79$	679
a^3	$17\lfloor\frac{m}{2}\rfloor + 9$	825
a^{-1}	1	1

η_T pairing in characteristic 3

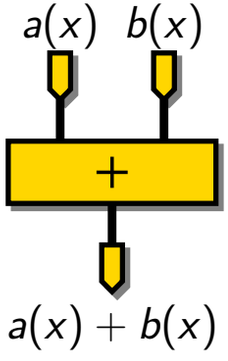
$$\hat{\eta_T} : E(\mathbb{F}_{3^m})[\ell] \times E(\mathbb{F}_{3^m})[\ell] \longrightarrow \mu_\ell \subset \mathbb{F}_{3^{6m}}$$

- Need for arithmetic over:
  - $\mathbb{F}_{3^m}$
  - ~~$\mathbb{F}_{3^{6m}}$~~ arithmetic on the underlying field $\mathbb{F}_{3^m}$
- Operations over $\mathbb{F}_{3^m}$:

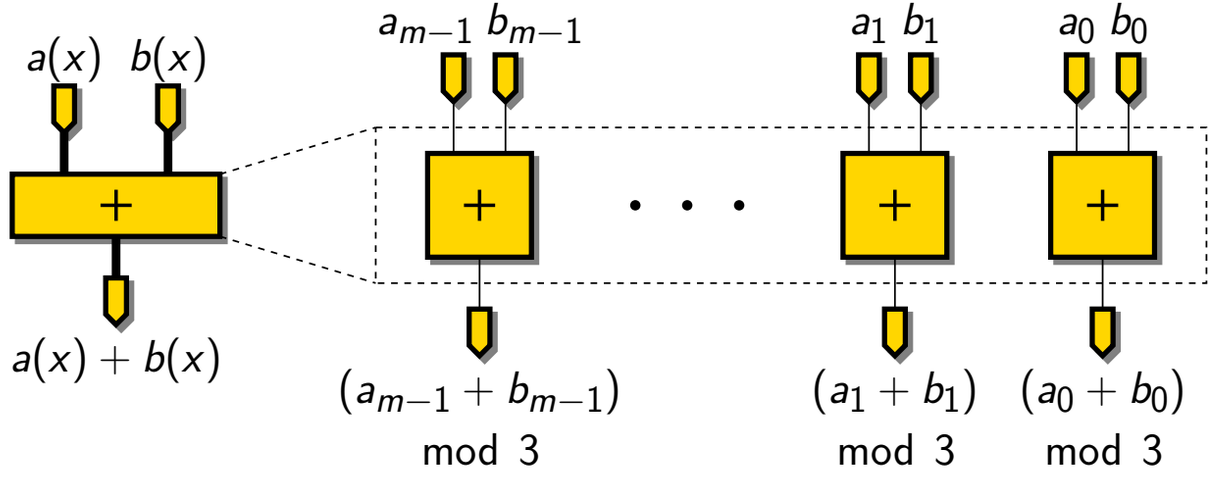
Operation	Count	$m = 97$
$+/-$	$121\lfloor\frac{m}{4}\rfloor + 186$	3090
$\times$	$25\lfloor\frac{m}{4}\rfloor + 79$	679
a^3	$17\lfloor\frac{m}{2}\rfloor + 9$	825
a^{-1}	1	1

- Arithmetic over $\mathbb{F}_{3^m}$:
  - Polynomial basis: $\mathbb{F}_{3^m} \cong \mathbb{F}_3[x]/(f(x))$
  - Degree-m irreducible polynomial $f(x)$ carefully chosen

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

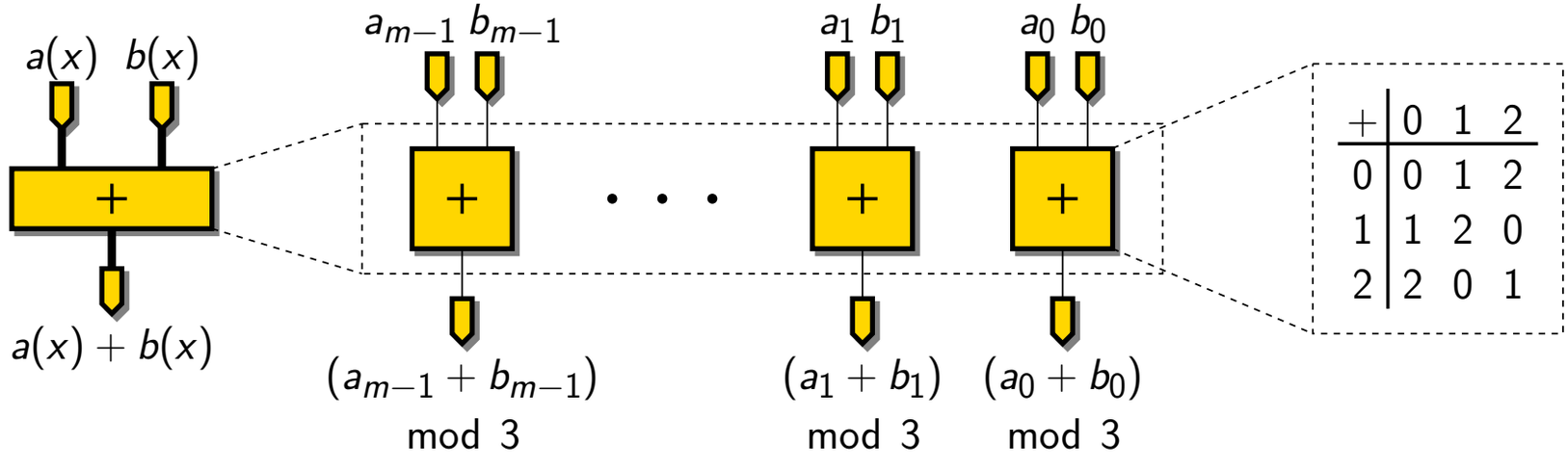


Addition over $\mathbb{F}_{3^m}$



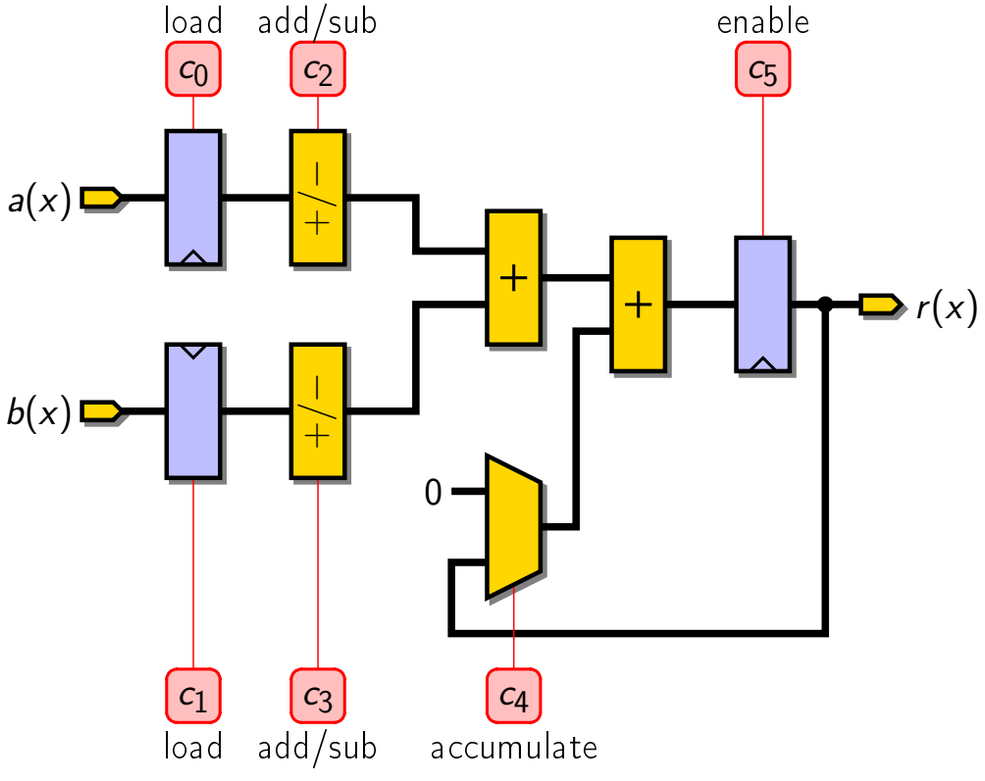
- coefficient-wise addition over $\mathbb{F}_3$

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



- coefficient-wise addition over $\mathbb{F}_3$
- addition over $\mathbb{F}_3$: small look-up table

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



- sign selection: multiplication by 1 or 2

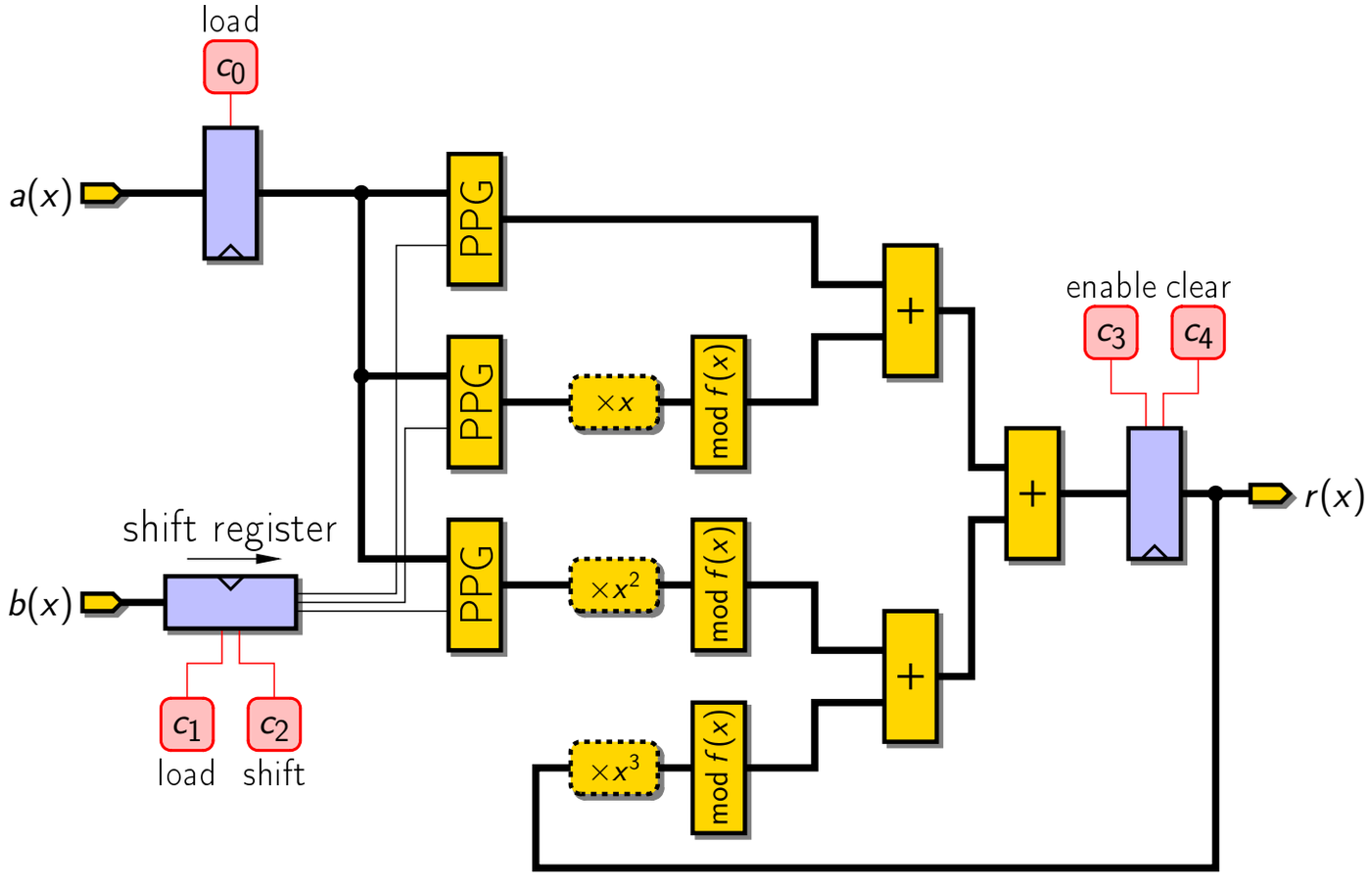
$$-a(x) \equiv 2a(x) \pmod 3$$

- feedback loop for accumulation

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

- Parallel-serial multiplication
  - multiplicand loaded in a parallel register
  - multiplier loaded in a shift register
- Most significant coefficients first
- D coefficients processed at each iteration: $\left\lceil \frac{m}{D} \right\rceil$ iterations per multiplication

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



- partial product generator (PPG): m multiplications over $\mathbb{F}_3$
- multiplication by x^i: only wiring
- simple modular reductions

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

- Cubing in characteristic 3 is the Frobenius map
- We compute the normal form of $a(x)^3 \bmod f(x)$

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

- Cubing in characteristic 3 is the Frobenius map
- We compute the normal form of $a(x)^3 \bmod f(x)$
- Example: $m = 97$ and $f(x) = x^{97} + x^{12} + 2$

$$
\begin{aligned}
a(x)^3 \bmod f(x) \quad = \quad & (a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0) \times 1 \\
+ \quad & (\ 0\ + a_{60}x^{95} + a_{88}x^{94} + \cdots + 0\ + a_{61}x + a_{89}) \times 1 \\
+ \quad & (\ 0\ + a_{60}x^{95} + a_{92}x^{94} + \cdots + 0\ + a_{61}x + a_{93}) \times 1
\end{aligned}
$$

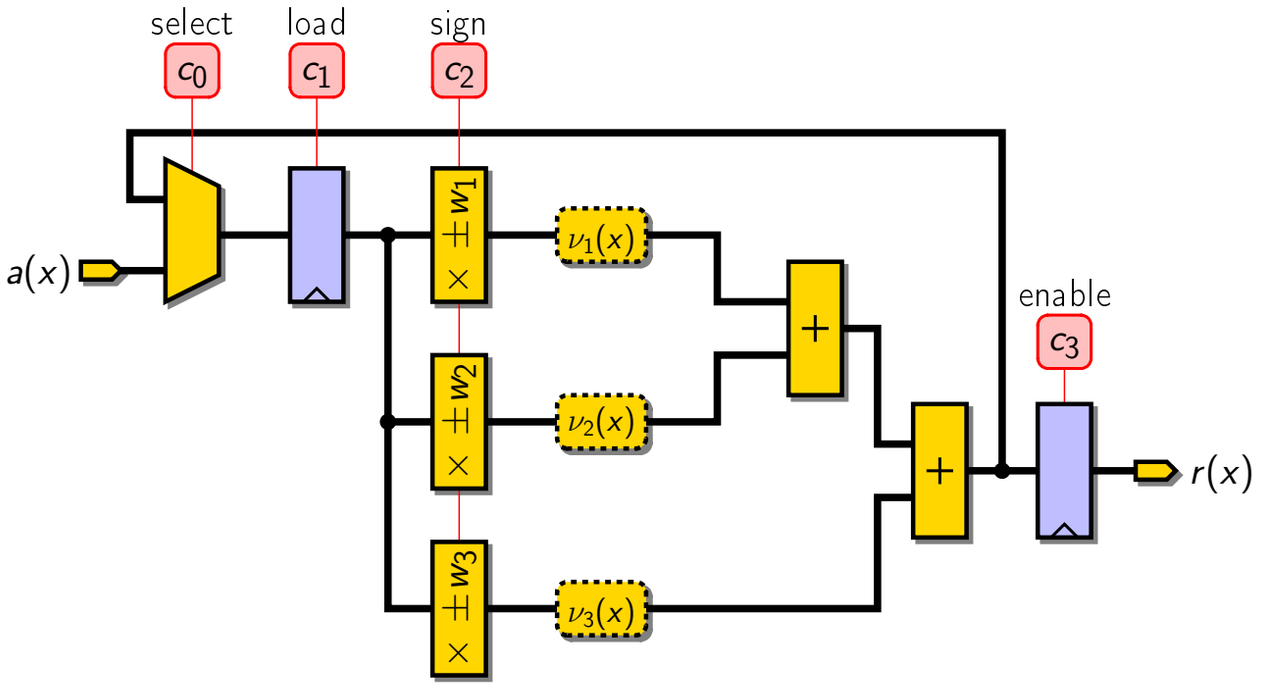
Cubing over $\mathbb{F}_{3^m}$

- Cubing in characteristic 3 is the Frobenius map
- We compute the normal form of $a(x)^3 \bmod f(x)$
- Example: $m = 97$ and $f(x) = x^{97} + x^{12} + 2$

$$
\begin{aligned}
a(x)^3 \bmod f(x) \quad = \quad & (a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0) \times 1 \\
+ \quad & (\ 0\ + a_{60}x^{95} + a_{88}x^{94} + \cdots + 0\ + a_{61}x + a_{89}) \times 1 \\
+ \quad & (\ 0\ + a_{60}x^{95} + a_{92}x^{94} + \cdots + 0\ + a_{61}x + a_{93}) \times 1 \\
\\
= \quad & w_1 \cdot \nu_1(x) + w_2 \cdot \nu_2(x) + w_3 \cdot \nu_3(x)
\end{aligned}
$$

- Required hardware:
  - only wires to compute the $\nu_i(x)$'s
  - possibly multiplications over $\mathbb{F}_3$
  - multi-operand addition over $\mathbb{F}_{3^m}$

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



- feedback loop for successive cubings
- sign selection for computing either $a(x)^3$ or $-a(x)^3$

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

- Extended Euclidean algorithm?

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

- Extended Euclidean algorithm?
  - fast computation
  - ... but need for additional hardware

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

- Extended Euclidean algorithm?
  - fast computation
  - ... but need for additional hardware
- Preferred solution: Fermat's little theorem

$$a(x)^{-1} = a(x)^{3^m-2} \text{ on } \mathbb{F}_{3^m}$$

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

- Extended Euclidean algorithm?
  - fast computation
  - ... but need for additional hardware
- Preferred solution: Fermat's little theorem

$$a(x)^{-1} = a(x)^{3^m-2} \text{ on } \mathbb{F}_{3^m}$$

  - algorithm by Itoh and Tsujii
  - requires only multiplications and cubings over $\mathbb{F}_{3^m}$

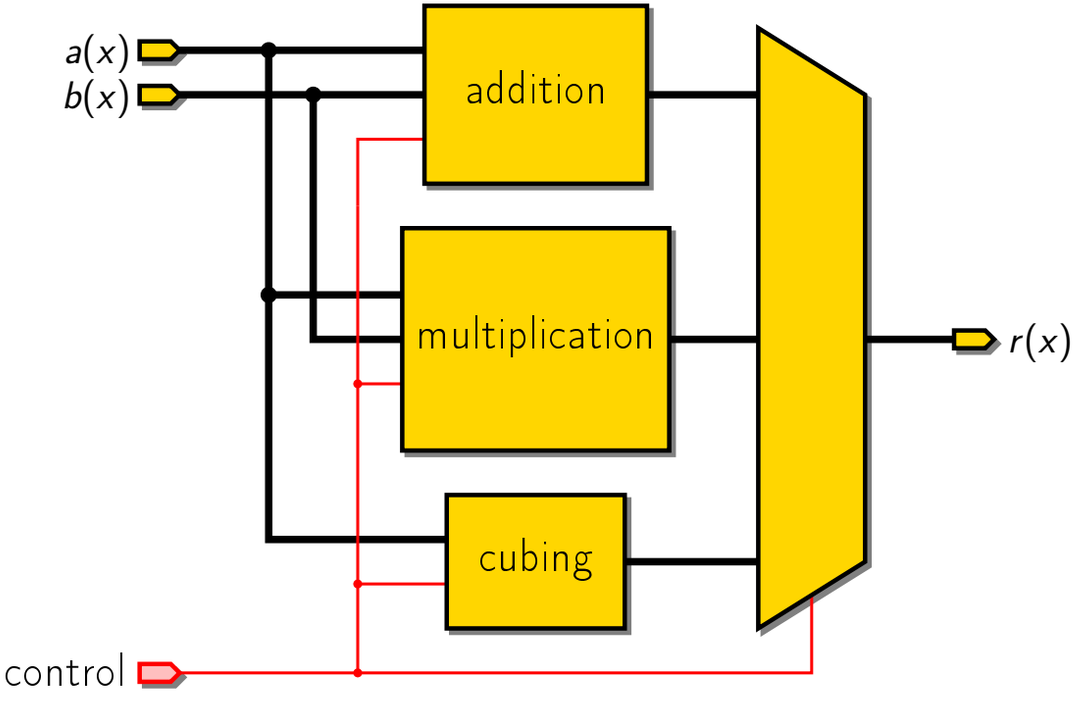
Inversion over $\mathbb{F}_{3^m}$

- Extended Euclidean algorithm?
  - fast computation
  - ... but need for additional hardware
- Preferred solution: Fermat's little theorem

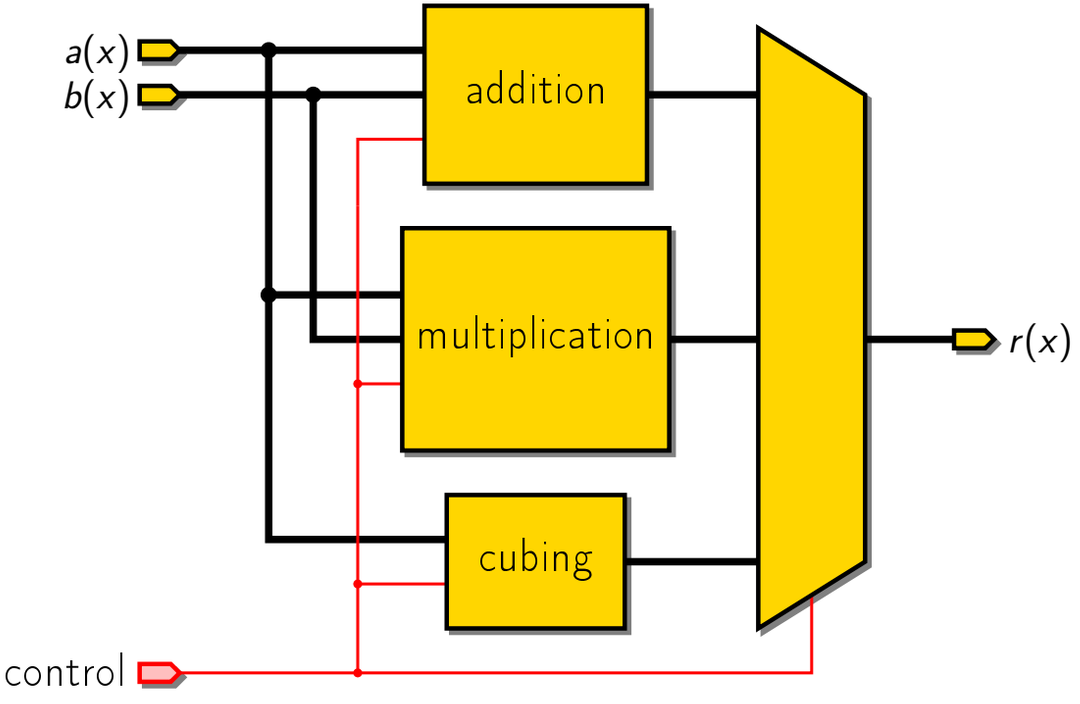
$$a(x)^{-1} = a(x)^{3^m-2} \text{ on } \mathbb{F}_{3^m}$$

  - algorithm by Itoh and Tsujii
  - requires only multiplications and cubings over $\mathbb{F}_{3^m}$
  - only one inversion for the full pairing: delay overhead is negligible ($< 1\%$)

The full processing element

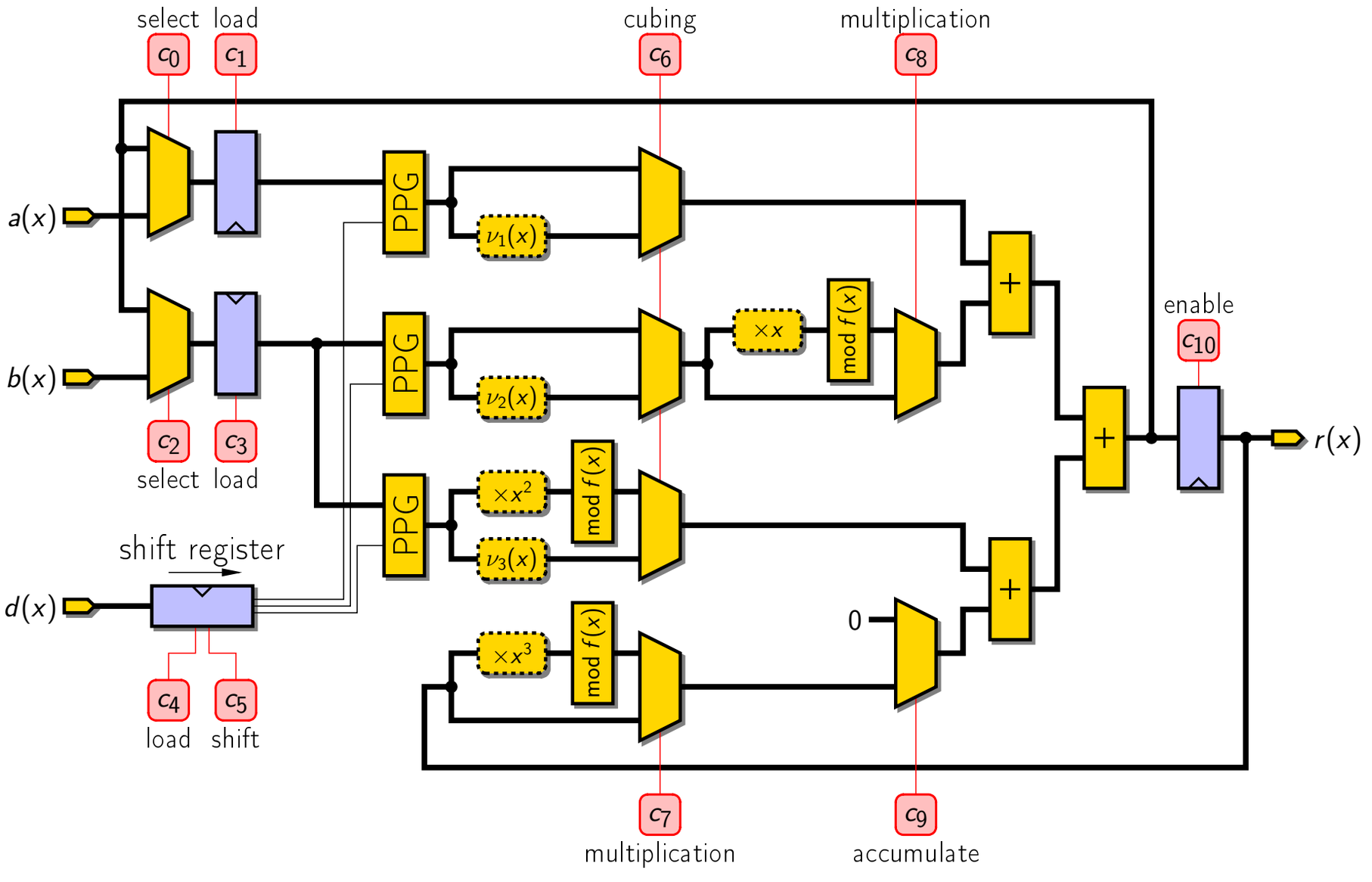


The full processing element

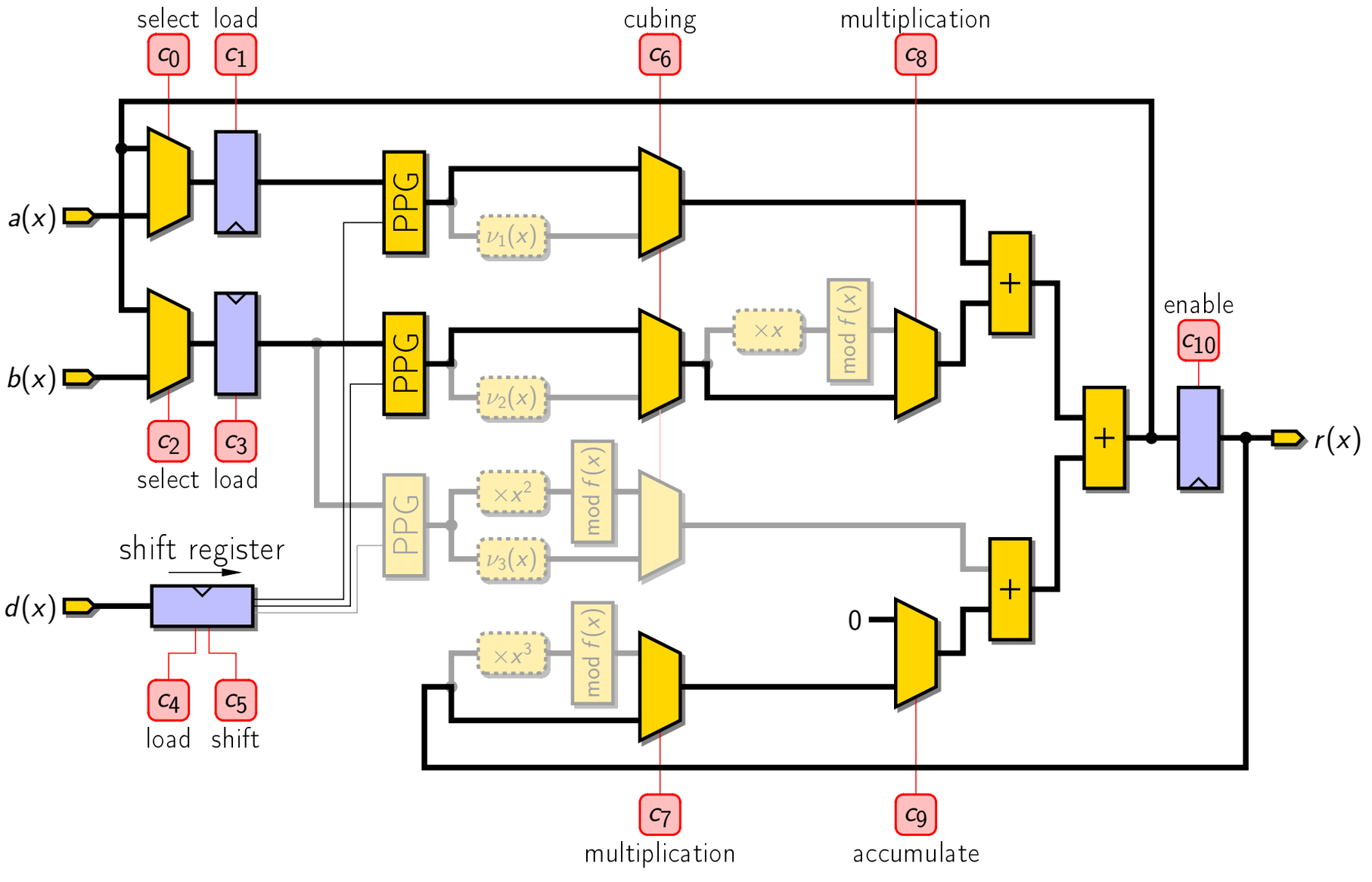


- For the η_T pairing:
  almost no parallelism between additions, multiplications and cubings
- Can we share hardware resources between the three operators?

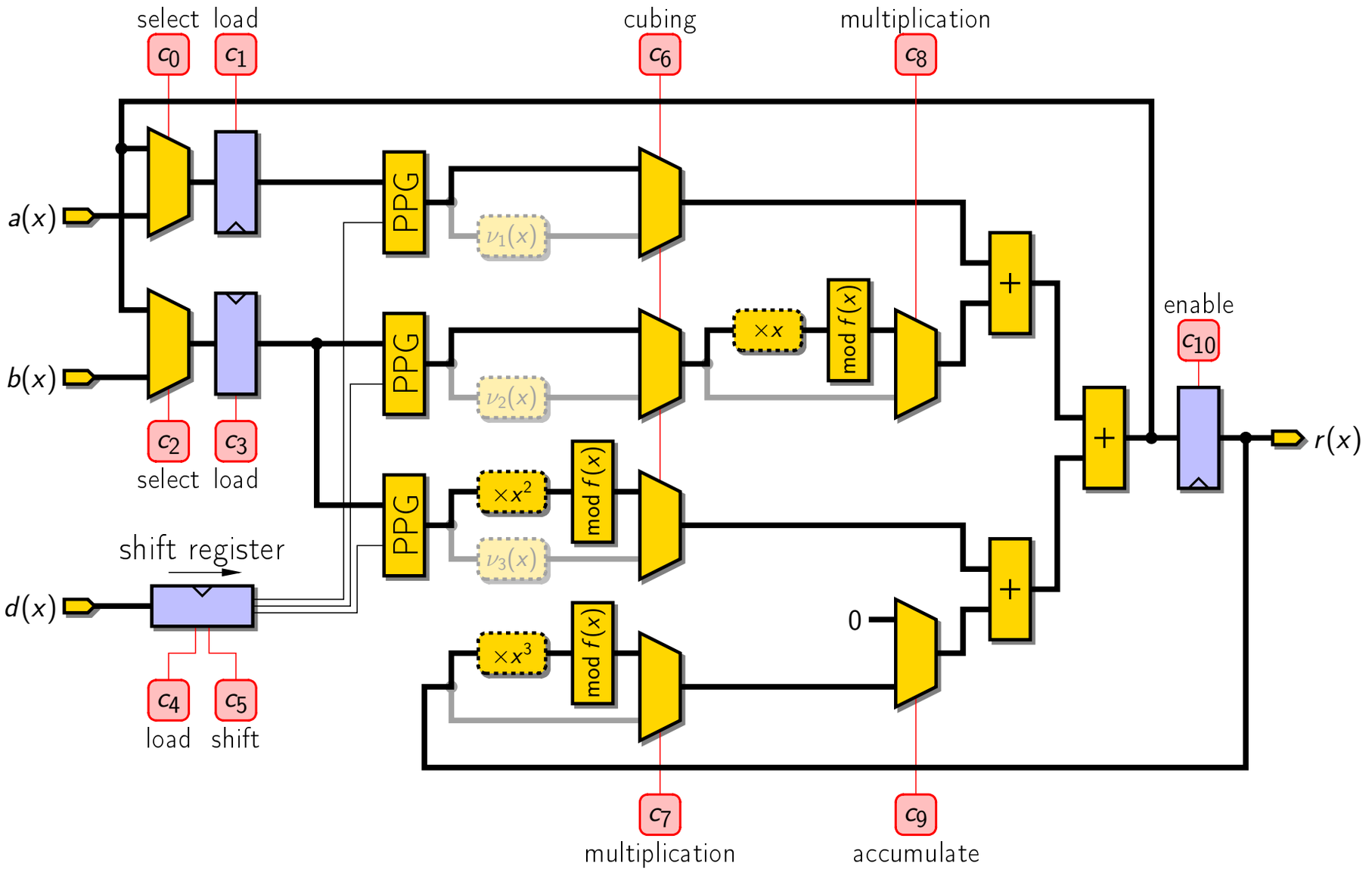
Unified operator



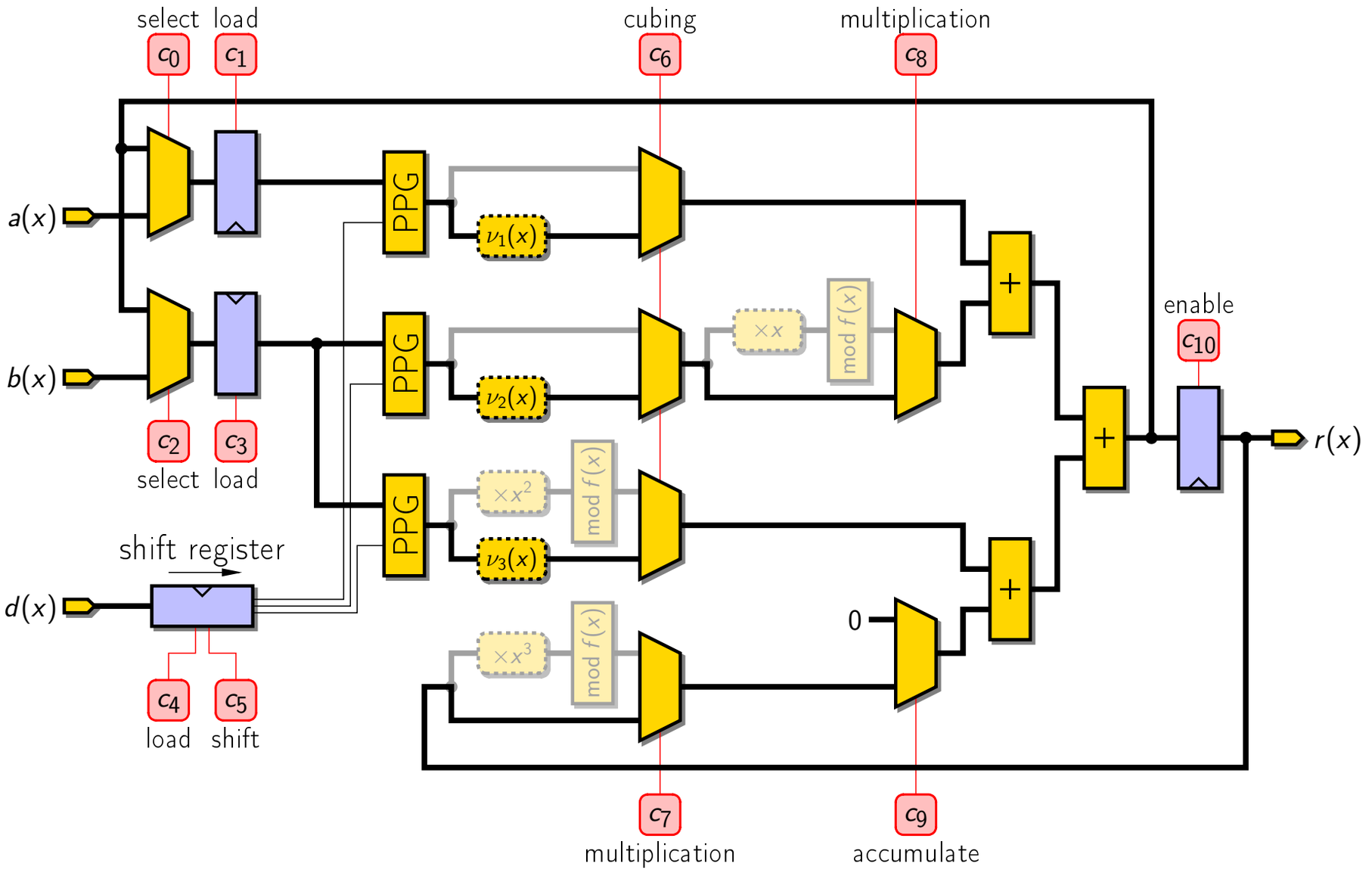
Unified operator



Unified operator



Unified operator



Results

- Full co-processor for computation of the η_T pairing
  - field: $\mathbb{F}_{3^{97}}$ with $f(x) = x^{97} + x^{12} + 2$
  - processing element: unified operator with $D = 3$
  - prototype on a Xilinx Virtex-II Pro 4 FPGA

Results

- Full co-processor for computation of the η_T pairing
  - field: $\mathbb{F}_{3^{97}}$ with $f(x) = x^{97} + x^{12} + 2$
  - processing element: unified operator with $D = 3$
  - prototype on a Xilinx Virtex-II Pro 4 FPGA
- Area: 1833 slices (63% of the FPGA) and 6 memory blocks (21%)
- Clock frequency: 145 MHz
- Full η_T pairing: 27800 clock cycles
- Computation time: 192 μs

Comparisons

Architecture	Area	Time	FPGA
Proposed solution (CHES'07)	1833 slices	192 μs	Virtex-II Pro
Grabher and Page (CHES'05)	4481 slices	432 μs	Virtex-II Pro
Kerins *et al.* (CHES'05)	55616 slices	850 μs	Virtex-II Pro
Ronan *et al.* (ITNG'07)	10000 slices	178 μs	Virtex-II Pro
Beuchat *et al.* (Arith'07 & WAIFI'07)	18000 LEs ($\approx$ 9000 slices)	33 μs	Cyclone II
Jiang (Univ. Honk Kong, 2007)	74105 slices	21 μs	Virtex-4 LX

Conclusion

- Unified operator generator
- Arithmetic over $\mathbb{F}_{p^m} \cong \mathbb{F}_p[x]/(f(x))$ for given p, m and $f(x)$
- Support for the following operations:
  - addition
  - multiplication
  - Frobenius map $(a(x)^p \bmod f(x))$
  - inverse Frobenius map $(\sqrt[p]{a(x)} \bmod f(x))$

Future work

- Characteristic 2
  - simpler arithmetic
  - better suited to FPGAs (fast multiplication)

Future work

- Characteristic 2
  - simpler arithmetic
  - better suited to FPGAs (fast multiplication)
- Pairing on hyperelliptic curves

Future work

- Characteristic 2
  - simpler arithmetic
  - better suited to FPGAs (fast multiplication)
- Pairing on hyperelliptic curves
- Ate pairing
- Side-channel

Thank you for your attention

Questions?