Aalto University
School of Science

Four$\mathbb{Q}$ on FPGA:
New Hardware Speed Records for Elliptic Curve Cryptography over Large Prime Characteristic Fields

K. Järvinen[1], A. Miele[2], R. Azarderakhsh[3], and P. Longa[4]

[1] Aalto University
[2] Intel Corporation
[3] Rochester Institute of Technology
[4] Microsoft Research

Contact: kimmo.jarvinen@aalto.fi, plonga@microsoft.com

CHES 2016, Santa Barbara, CA, USA, August 17–19, 2016

Introduction

Four$\mathbb{Q}$:

- Four$\mathbb{Q}$ is a high-performance elliptic curve with very good SW performance (2–3$\times$ faster than Curve25519)
- Four$\mathbb{Q}$ has been shown to offer the fastest scalar multiplications on a wide range of software platforms:
  - On several 32-bit ARM microarchitectures (SAC 2016)
  - On several 64-bit Intel/AMD processors, low and high-end (ASIACRYPT 2015)
- Four$\mathbb{Q}$ employs four-dimensional scalar decompositions, requires extensive precomputation, complex control, etc.
  $\Rightarrow$ Not clear how well it suits for HW implementation

Introduction

Contributions:

- The first FPGA-based implementations of Four$\mathbb{Q}$
- Four$\mathbb{Q}$ offers 2–2.5$\times$ faster performance than Curve25519
- Speed-area tradeoff is the primary optimization goal
- Protected against timing and SPA attacks
- We present three implementations:
  single-core, multi-core, and Montgomery ladder variant

Four$\mathbb{Q}$

Costello, Longa, ASIACRYPT'15

$$\mathcal{E}/\mathbb{F}_{p^2} : -x^2 + y^2 = 1 + dx^2y^2$$

- Twisted Edwards curve with $\#\mathcal{E}(\mathbb{F}_{p^2}) = 392 \cdot \xi$ where ξ is a 246-bit prime
- Defined over $\mathbb{F}_{p^2}$ with the Mersenne prime $p = 2^{127} - 1$
- Complete addition formulas over extended twisted Edwards coordinates (Hisil et al. ASIACRYPT'08)

Four$\mathbb{Q}$
Costello, Longa, ASIACRYPT'15

$$\mathcal{E}/\mathbb{F}_{p^2} : -x^2 + y^2 = 1 + dx^2y^2$$

- Twisted Edwards curve with $\#\mathcal{E}(\mathbb{F}_{p^2}) = 392 \cdot \xi$ where ξ is a 246-bit prime
- Defined over $\mathbb{F}_{p^2}$ with the Mersenne prime $p = 2^{127} - 1$
- Complete addition formulas over extended twisted Edwards coordinates (Hisil et al. ASIACRYPT'08)
- Two efficiently-computable endomorphisms ψ and ϕ
- Four-dimensional decomposition for the 256-bit scalar m with (a_1, a_2, a_3, a_4) such that $a_i \in [0, 2^{64})$:

$$[m]P = [a_1]P + [a_2]\psi(P) + [a_3]\phi(P) + [a_4]\psi(\phi(P))$$

Scalar Multiplication

Input: Point P,
integer $m \in [0, 2^{256})$

Output: $[m]P$

Decompose and recode m

Precompute lookup table T

$Q \leftarrow T[v_{64}]$

for $i = 63$ **to** 0 **do**

  $Q \leftarrow [2]Q$

  $Q \leftarrow Q + m_i T[v_i]$

Scalar Multiplication

Input: Point P,
integer $m \in [0, 2^{256})$
Output: $[m]P$

Decompose and recode m
Precompute lookup table T
$Q \leftarrow T[v_{64}]$
for $i = 63$ **to** 0 **do**
    $Q \leftarrow [2]Q$
    $Q \leftarrow Q + m_i T[v_i]$

Scalar decompose and recode

- Decompose to a multi-scalar (a_1, a_2, a_3, a_4)
- Sign-aligned so that $a_1[j] \in \{\pm 1\}$ and $a_i[j] \in \{0, a_1[j]\}$ for $2 \leq j \leq 4$
- Recode to signs $m_i \in \{-1, 1\}$ and values $v_i \in [0, 7]$ (point index)

Scalar Multiplication

Input: Point P,
integer $m \in [0, 2^{256})$
Output: $[m]P$

Decompose and recode m
Precompute lookup table T
$Q \leftarrow T[v_{64}]$
for $i = 63$ **to** 0 **do**
    $Q \leftarrow [2]Q$
    $Q \leftarrow Q + m_i T[v_i]$

Precomputation

- Precompute 8 points: $T[u] = P + [u_0]\phi(P) + [u_1]\psi(P) + [u_2]\psi(\phi(P))$ for $u = (u_2, u_1, u_0) \in [0, 7]$
- Store them with 5 coordinates $(X + Y, Y - X, 2Z, 2dT, -2dT) \Rightarrow$
  $+T[u] : (X + Y, Y - X, 2Z, 2dT)$
  $-T[u] : (Y - X, X + Y, 2Z, -2dT)$
- $68\mathbf{M} + 27\mathbf{S}$ and several additions

Scalar Multiplication

Input: Point P,
integer $m \in [0, 2^{256})$
Output: $[m]P$

Decompose and recode m
Precompute lookup table T
$Q \leftarrow T[v_{64}]$
for $i = 63$ **to** 0 **do**
  $Q \leftarrow [2]Q$
  $Q \leftarrow Q + m_i T[v_i]$

Main for-loop

- Fully regular and constant-time
- Only 64 double-and-adds
- Doubling:
  $(X, Y, Z, T_a, T_b) \leftarrow (X, Y, Z)$
- Addition:
  $(X, Y, Z, T_a, T_b) \leftarrow$
  $(X, Y, Z, T_a, T_b) \times$
  $(X + Y, Y - X, 2Z, 2dT)$

Aalto University
School of Science
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
R·I·T
Microsoft Research

General Architecture

Scalar Decomposition and Recoding Unit

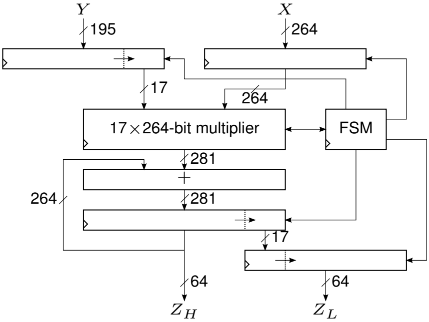
- Decomposes and recodes the scalar
- Mainly multiplications with constants

Field Arithmetic Unit ("the core")

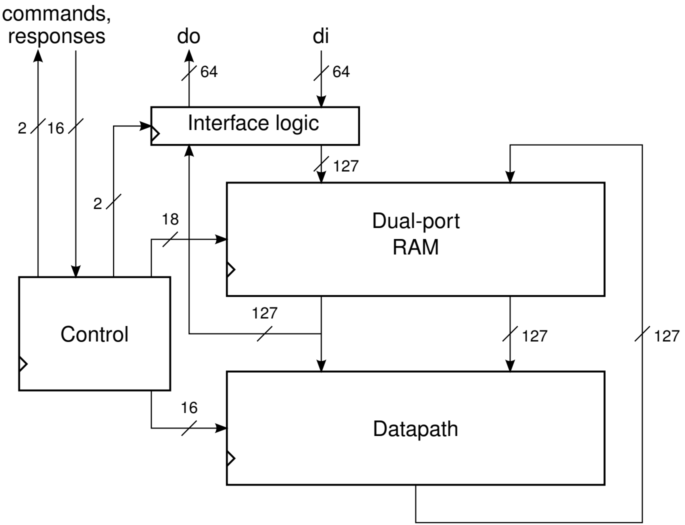
- Precomputation and the main for-loop
- Highly optimized for $\mathbb{F}_p$ with the Mersenne prime

Scalar Unit

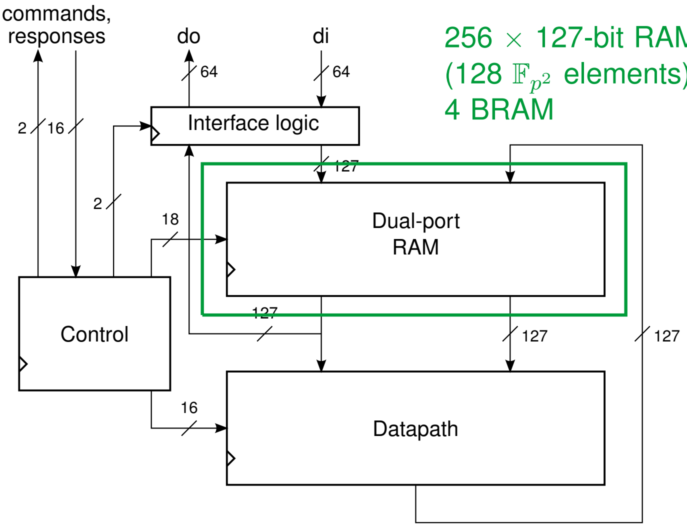
- Decomposition is computed with a truncated multiplier (mainly multiplications with constants)
- The main component is a 17×264-bit row multiplier built by using 11 DSPs
- Recoding is bit manipulations and 64-bit additions
- Outputs (m_0, v_0) first, scalar multiplication begins with (m_{64}, v_{64})
  $\Rightarrow$ Store in a LIFO buffer



Field Arithmetic Unit

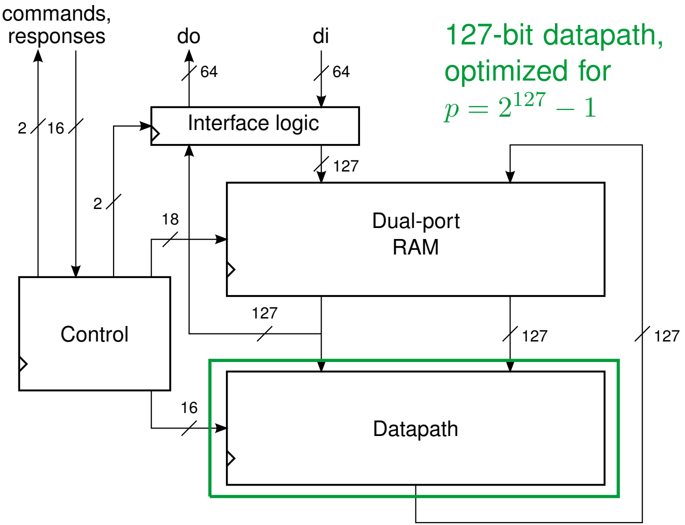


Field Arithmetic Unit



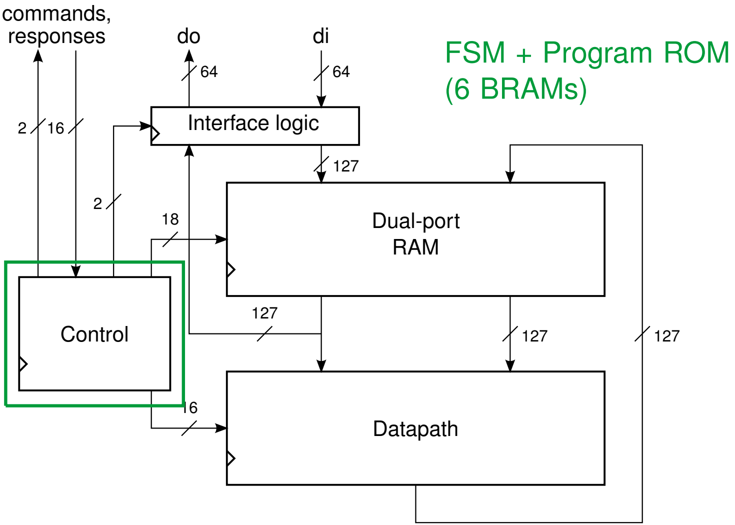
256 $\times$ 127-bit RAM
(128 $\mathbb{F}_{p^2}$ elements)
4 BRAM

Field Arithmetic Unit

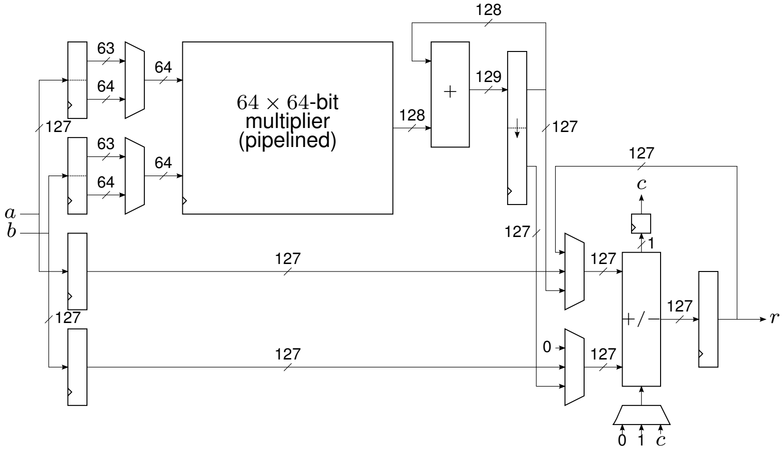


127-bit datapath, optimized for $p = 2^{127} - 1$

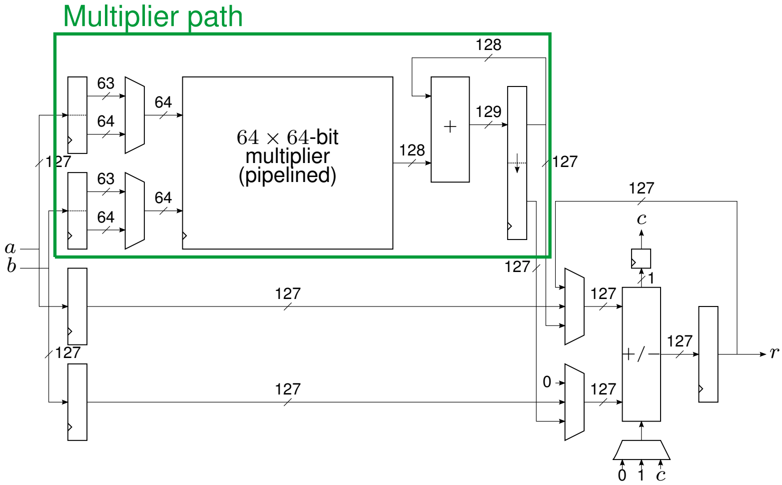
Field Arithmetic Unit



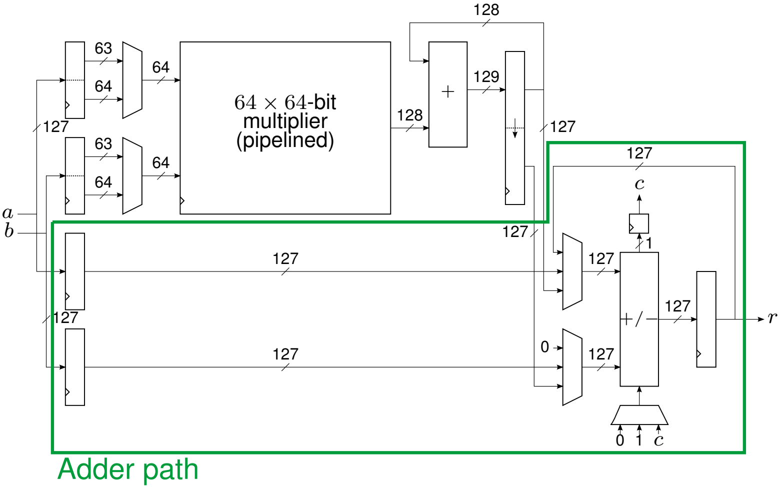
Field Arithmetic Unit: Datapath



Field Arithmetic Unit: Datapath



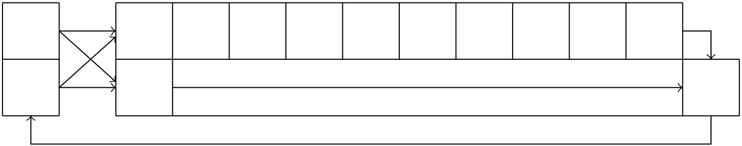
Field Arithmetic Unit: Datapath



Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

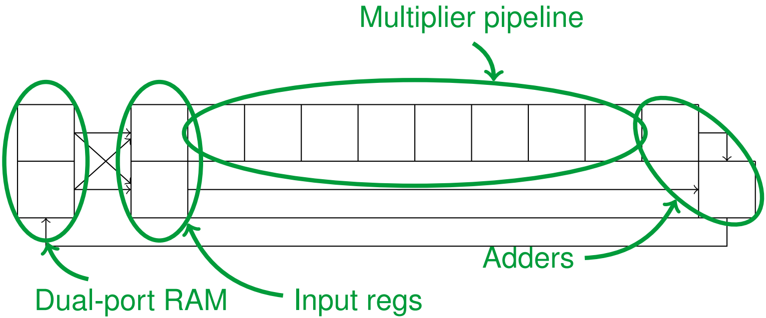
$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$



Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

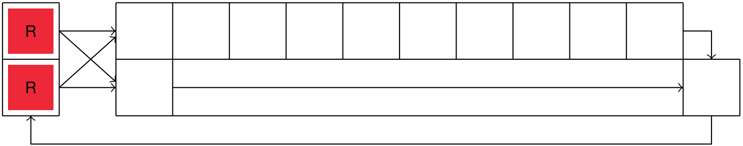
$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$



Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

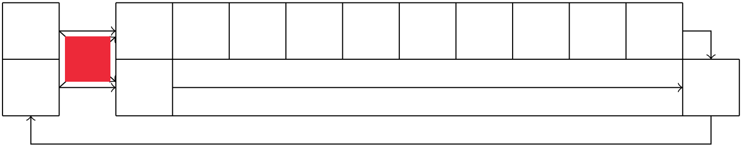


1

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

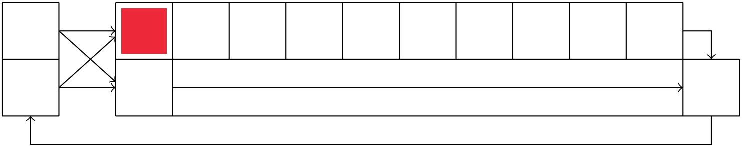


2

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

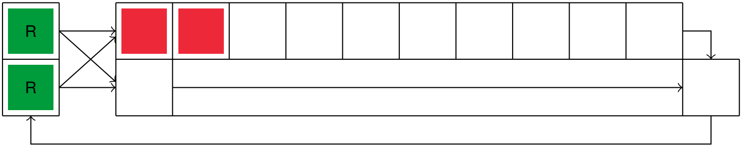


3

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

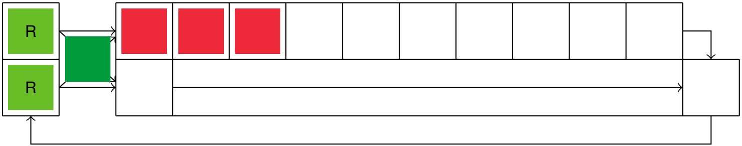


4

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

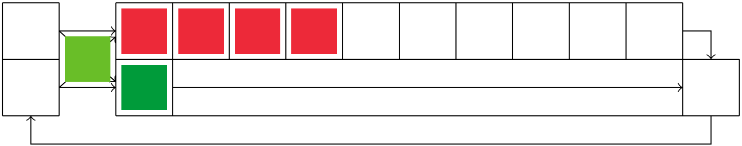


5

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$
\begin{aligned}
a \times b &= (a_0, a_1) \times (b_0, b_1) \\
&= (a_0 \cdot b_0 - a_1 \cdot b_1 \; , \; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)
\end{aligned}
$$

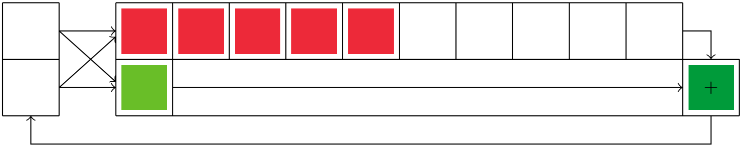


6

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

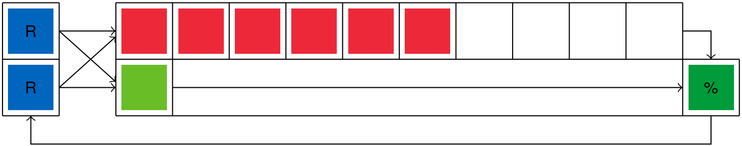


7

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

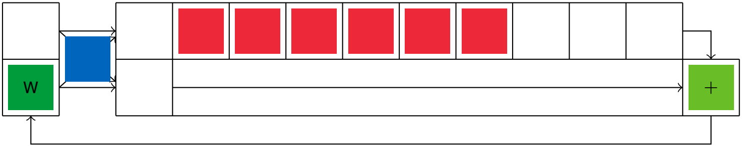


8

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

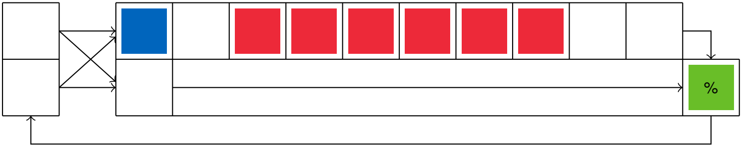


9

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \;,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

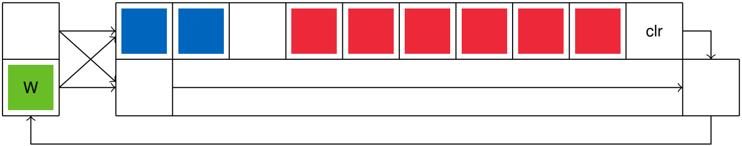


10

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

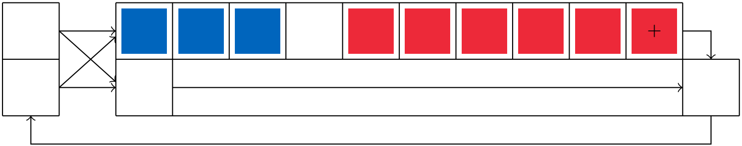


11

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

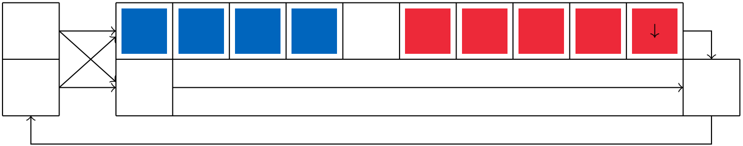


12

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$
\begin{aligned}
a \times b &= (a_0, a_1) \times (b_0, b_1) \\
&= ({\color{red}a_0 \cdot b_0} - {\color{blue}a_1 \cdot b_1}\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)
\end{aligned}
$$



13

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

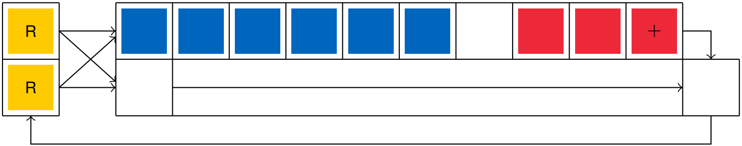
$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \, , \; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

14

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$
\begin{aligned}
a \times b &= (a_0, a_1) \times (b_0, b_1) \\
&= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)
\end{aligned}
$$

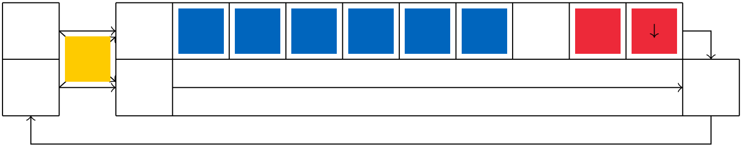


15

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

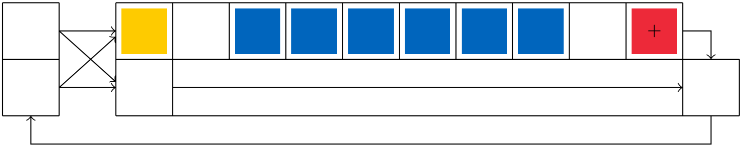


16

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

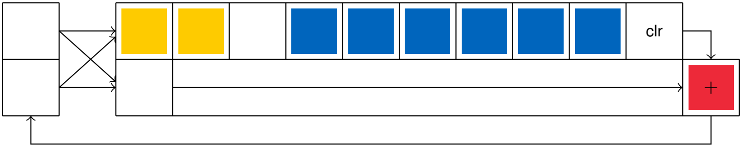


17

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$



18

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

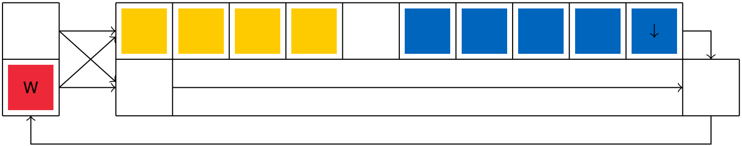
$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \;,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

19

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$



20

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

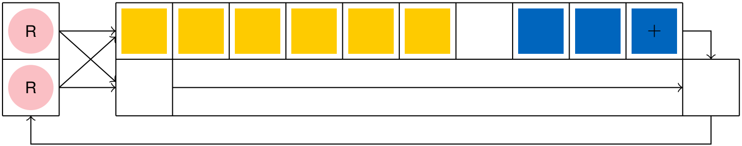
$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

21

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \, , \, (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$



(1) 22

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

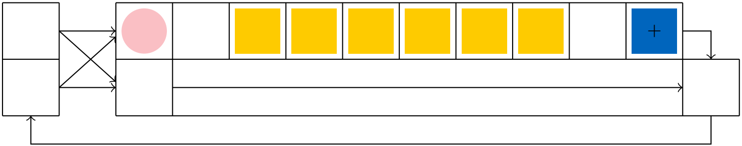
$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \, , \, (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

(2) 23

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

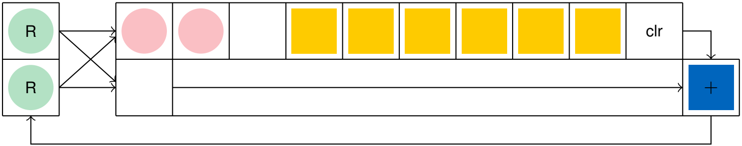


(3) 24

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

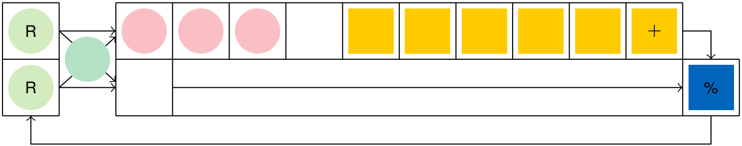


(4) 25

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

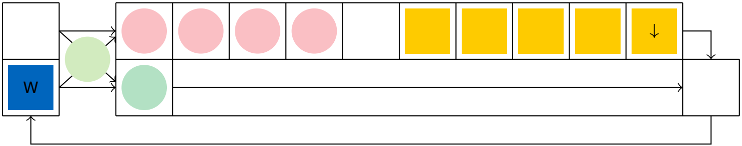


(5) 26

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$\begin{aligned} a \times b &= (a_0, a_1) \times (b_0, b_1) \\ &= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1) \end{aligned}$$

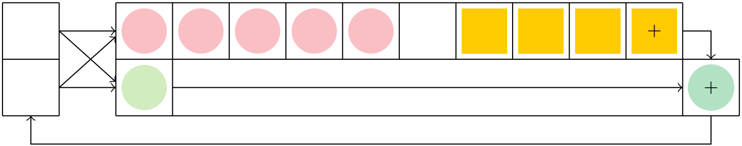


(6) 27

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

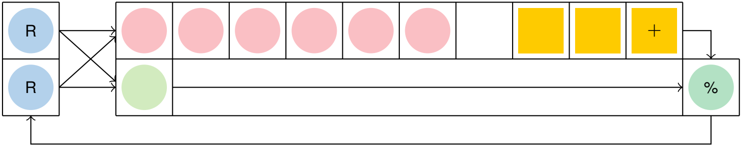


(7) 28

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\, (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

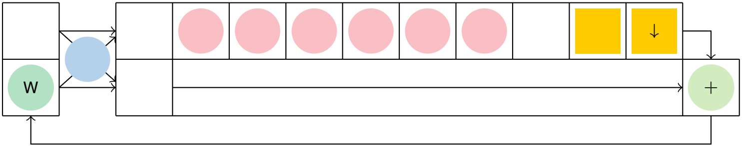


(8) 29

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

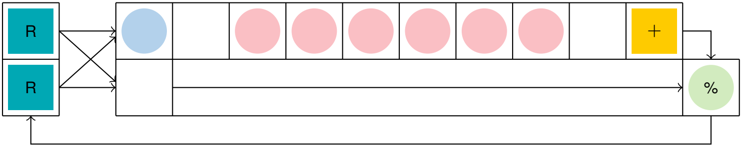


(9) 30

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$\begin{aligned} a \times b &= (a_0, a_1) \times (b_0, b_1) \\ &= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1) \end{aligned}$$

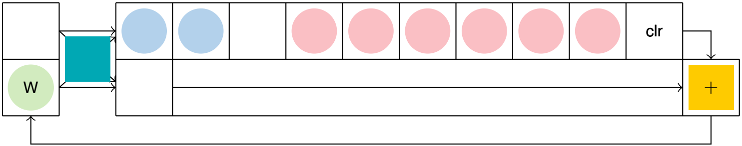


(10) 31

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

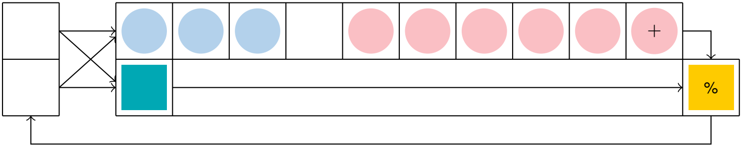


(11) 32

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \,,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

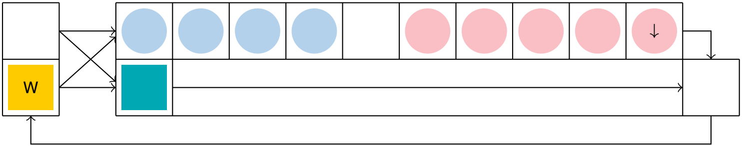


(12) 33

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

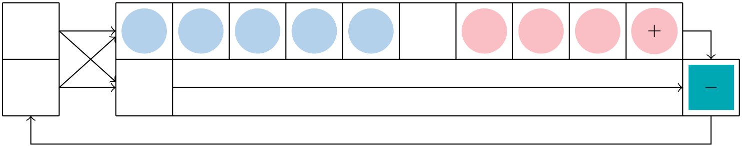


(13) 34

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \;,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

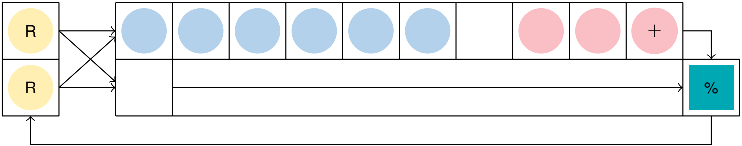


(14) 35

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \;,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

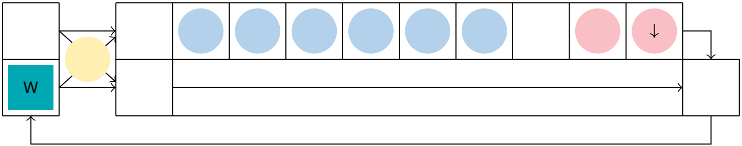


(15) 36

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

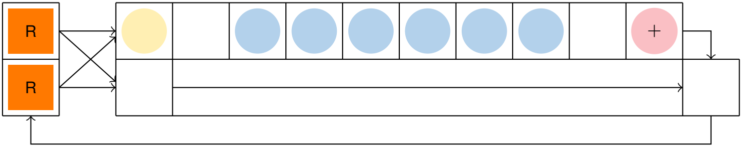


(16) 37

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

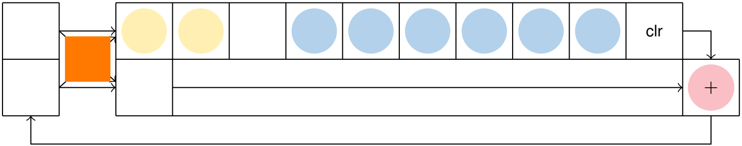


(17) 38

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

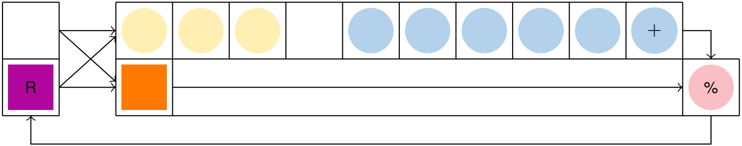


(18) 39

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

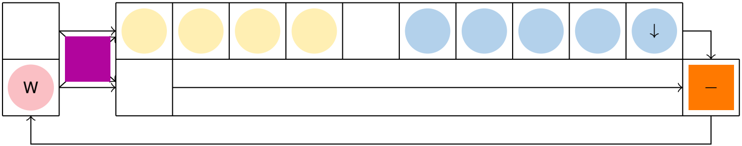


(19) 40

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \, , \, (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

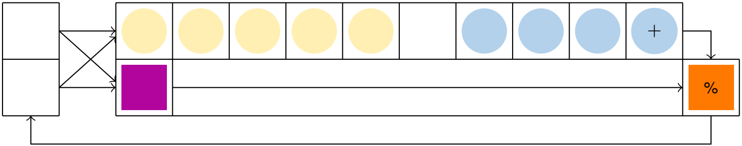


(20) 41

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

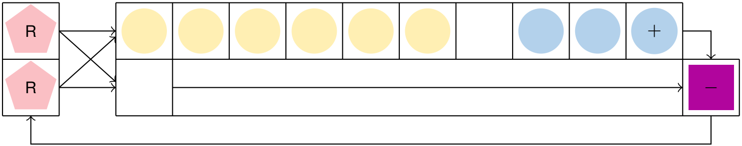


(21) 42

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \;,\; (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

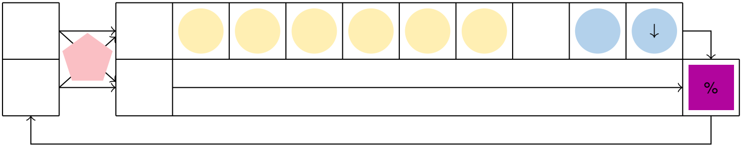


(1,22) 43

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1 \ , \ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$

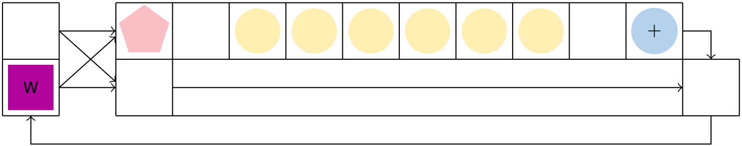


(2,23) 44

Example: Multiplication in $\mathbb{F}_{p^2}$

3 multiplications, 2 additions and 3 subtractions in $\mathbb{F}_p$:

$$a \times b = (a_0, a_1) \times (b_0, b_1)$$
$$= (a_0 \cdot b_0 - a_1 \cdot b_1\ ,\ (a_0 + a_1) \cdot (b_0 + b_1) - a_0 \cdot b_0 - a_1 \cdot b_1)$$



(3,24) 45

Latencies

Field operations

	in $\mathbb{F}_p$	in $\mathbb{F}_{p^2}$
Addition	6 (2) clocks	8 (4) clocks
Multiplication	20 (7) clocks	38/45 (31/21) clocks
Squaring	20 (7) clocks	28 (16) clocks
Inversion	2760 clocks	2817 clocks

In practice, almost all additions in parallel with multiplications

Latencies

Field operations

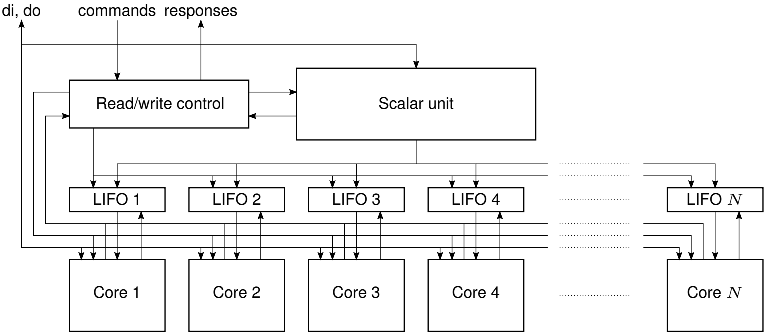
	in $\mathbb{F}_p$	in $\mathbb{F}_{p^2}$
Addition	6 (2) clocks	8 (4) clocks
Multiplication	20 (7) clocks	38/45 (31/21) clocks
Squaring	20 (7) clocks	28 (16) clocks
Inversion	2760 clocks	2817 clocks

In practice, almost all additions in parallel with multiplications

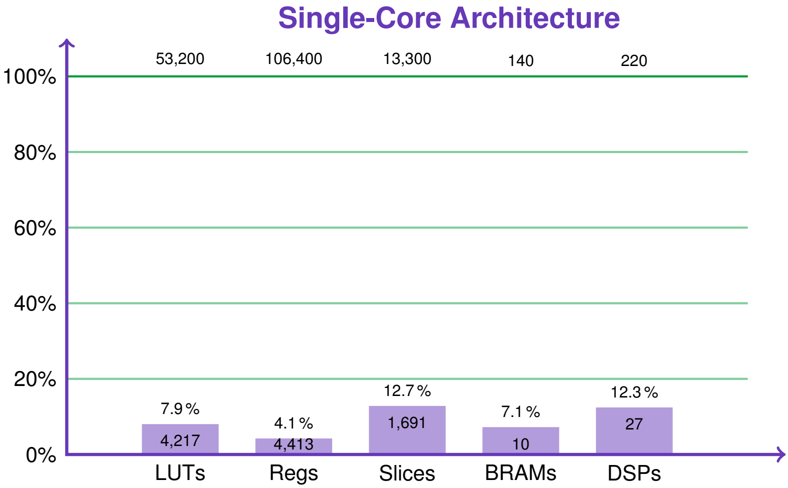
Operations for scalar multiplication

Precomputation	4185 clocks
Scalar decomposition and recoding	1984 (0) clocks
Double-and-add (64 times)	354 clocks
Affine conversion	2869 clocks
Scalar multiplication	29739 clocks

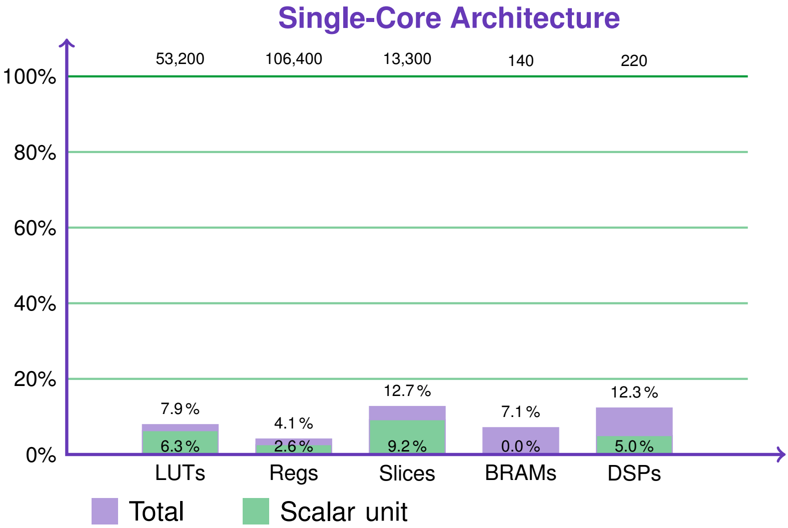
Multi-Core Architecture



Area Results on Zynq-7020

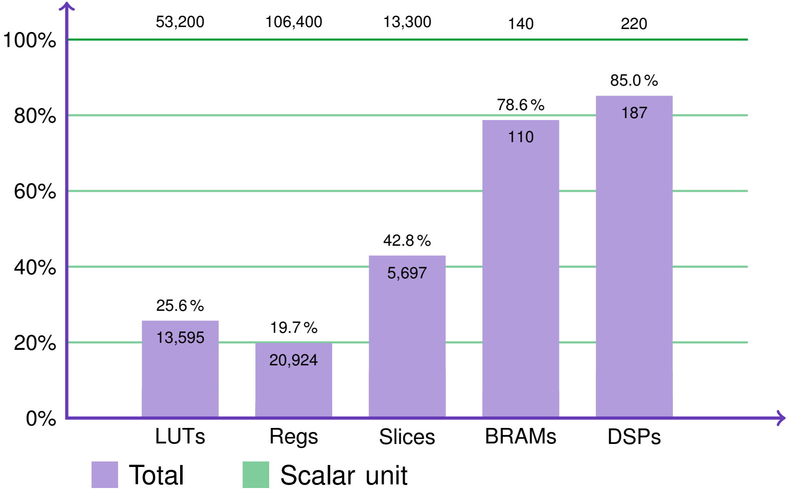


Area Results on Zynq-7020



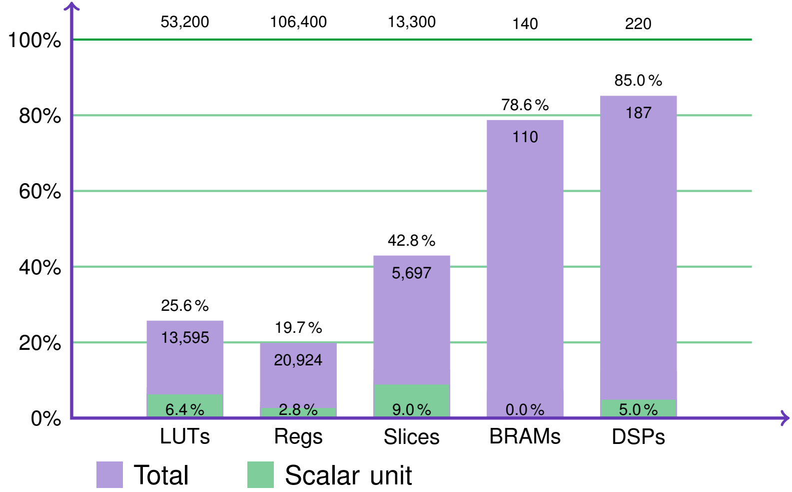
Area Results on Zynq-7020

Multi-Core Architecture $(N = 11)$



Area Results on Zynq-7020

Multi-Core Architecture $(N = 11)$



Performance Results on Zynq-7020

VHDL for Xilinx Zynq-7020 with Vivado 2015.4

- One scalar multiplication takes 29,739 clock cycles
- Single-core: 190 MHz $\Rightarrow$ 157 μs or 6,389 ops
- Multi-core: 175 MHz $(\times 11)$ $\Rightarrow$ 170 μs or 64,730 ops
- Point validation (124 clocks), cofactor killing (1760 clocks)

Performance Results on Zynq-7020

VHDL for Xilinx Zynq-7020 with Vivado 2015.4

- One scalar multiplication takes 29,739 clock cycles
- Single-core: 190 MHz $\Rightarrow$ 157 μs or 6,389 ops
- Multi-core: 175 MHz $(\times 11)$ $\Rightarrow$ 170 μs or 64,730 ops
- Point validation (124 clocks), cofactor killing (1760 clocks)

Variant using Montgomery ladder

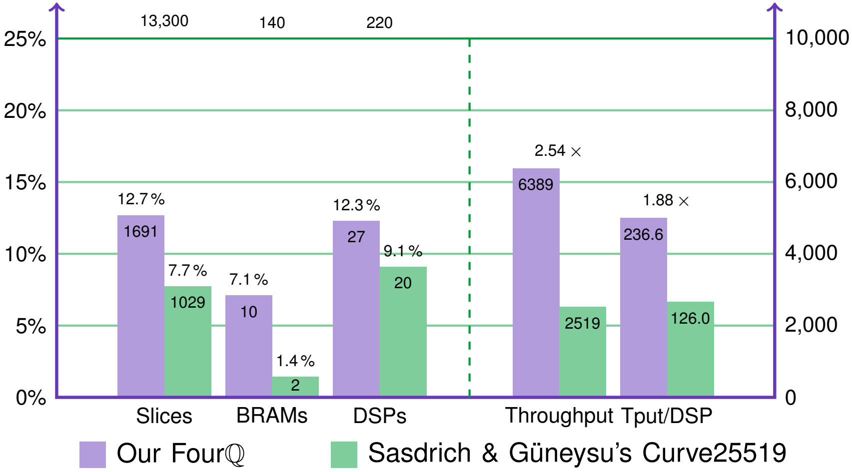
- No scalar unit (saves 11 DSPs), no precomputations, simpler control, etc.
- 522 slices, 7 BRAMs, 16 DSP
- 58967 clocks at 190 MHz $\Rightarrow$ 310 μs or 3,222 ops

Comparison

- Many implementations for ECC over prime fields
- Comparison is extremely difficult because of different FPGAs, different optimization goals, etc.
- Best match with Sasdrich & Güneysu's Curve25519 design, both on Xilinx Zynq-7020
- See the paper for further comparisons

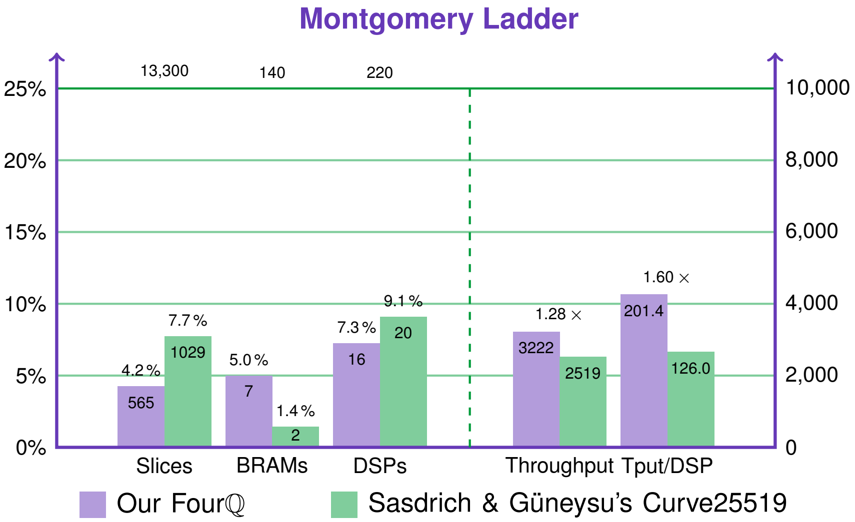
Four$\mathbb{Q}$ vs. Curve25519

Single-Core Architectures

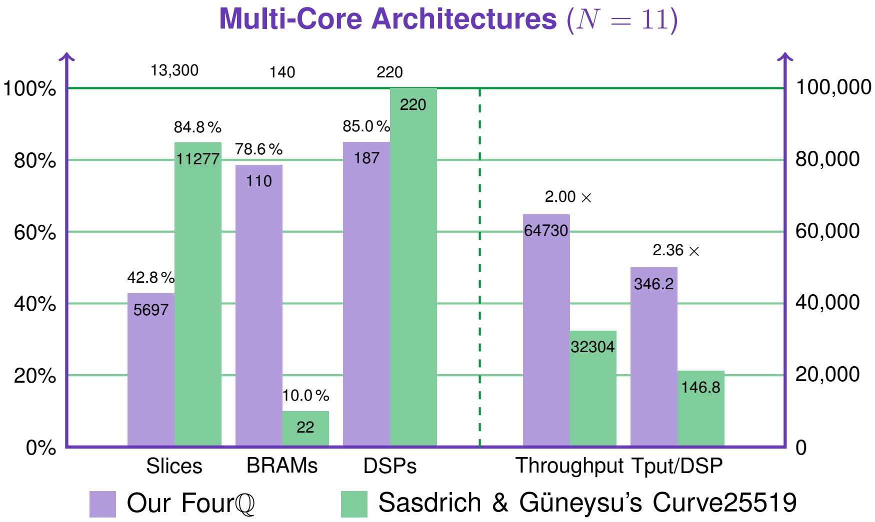


Aalto University School of Science
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
R·I·T
Microsoft Research

FourQ vs. Curve25519



FourQ vs. Curve25519



Conclusions

- We showed that Four$\mathbb{Q}$ is very efficient also on FPGAs
- Four$\mathbb{Q}$ is significantly more efficient in terms of speed-area ratio than the closest counterpart

Conclusions

- We showed that Four$\mathbb{Q}$ is very efficient also on FPGAs
- Four$\mathbb{Q}$ is significantly more efficient in terms of speed-area ratio than the closest counterpart

Future Work

- Low-latency implementation
- Better side-channel protection: e.g., against DPA and advanced horizontal attacks

Conclusions

- We showed that Four$\mathbb{Q}$ is very efficient also on FPGAs
- Four$\mathbb{Q}$ is significantly more efficient in terms of speed-area ratio than the closest counterpart

Future Work

- Low-latency implementation
- Better side-channel protection:
  e.g., against DPA and advanced horizontal attacks

Thank you! Questions?