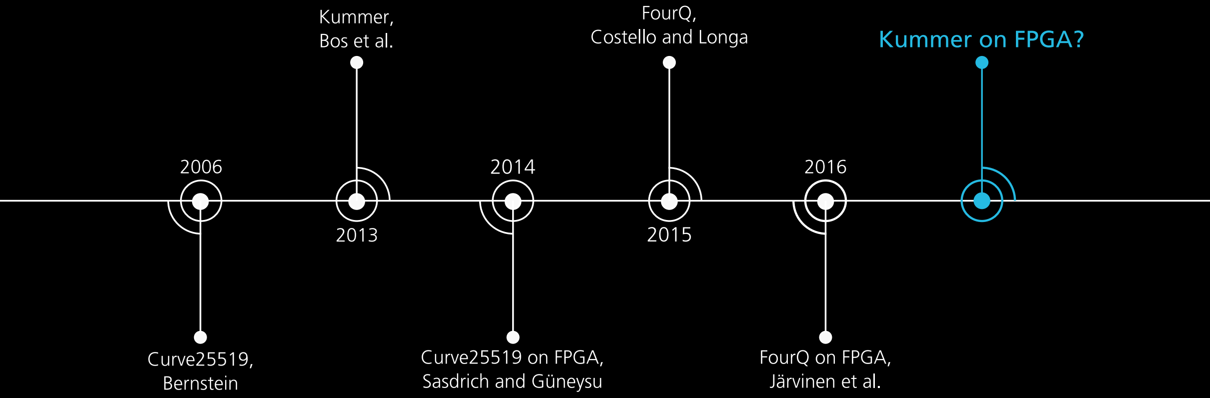
Fast FPGA Implementation of Diffie-Hellman on the Kummer Surface of a Genus-2 Curve

Philipp Koppermann, Fabrizio De Santis, Johann Heyszl and Georg Sigl

Fraunhofer
AISEC

History of High-Speed Curve Cryptography over Prime Fields



2006

Curve25519,
Bernstein

2013

Kummer,
Bos et al.

2014

Curve25519 on FPGA,
Sasdrich and Güneysu

2015

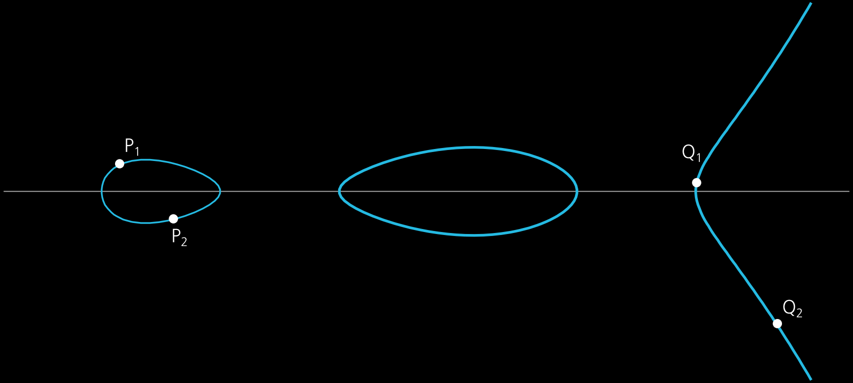
FourQ,
Costello and Longa

2016

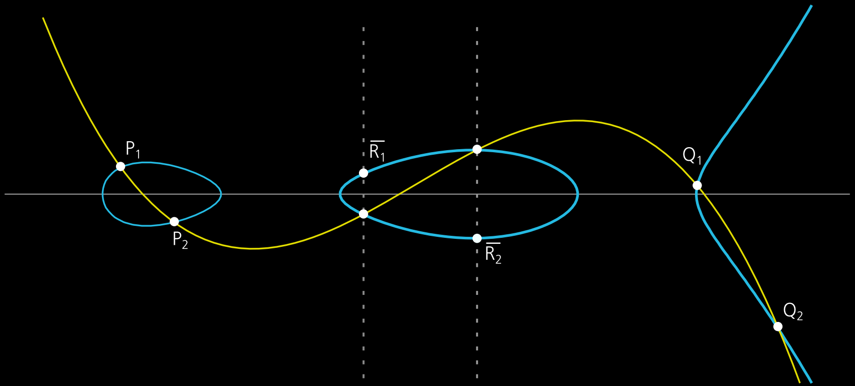
FourQ on FPGA,
Järvinen et al.

Kummer on FPGA?

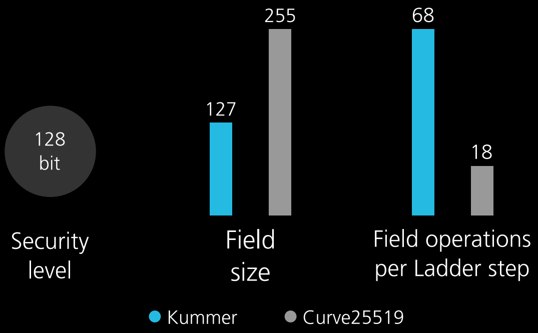
Point Addition on a Hyperelliptic Genus-2 Curve



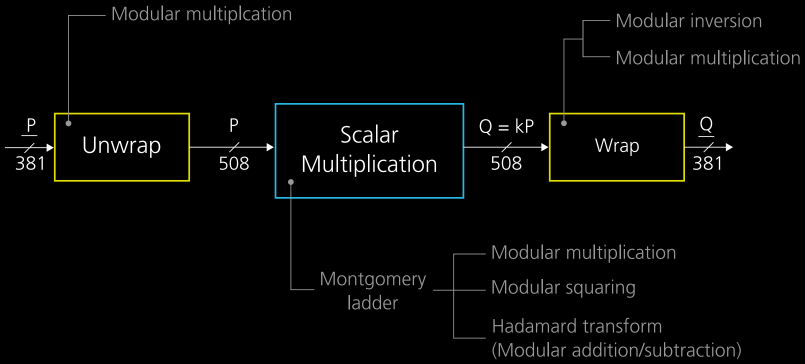
Point Addition on a Hyperelliptic Genus-2 Curve



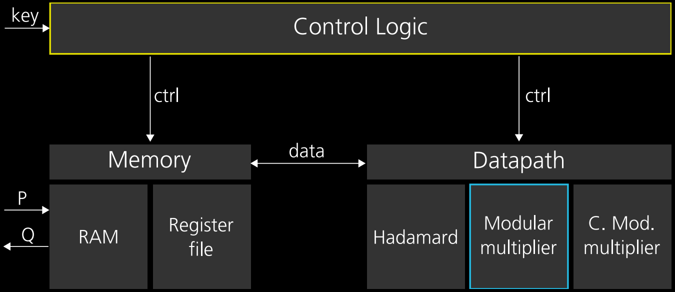
Kummer: Smaller Field But More Operations



Structure of the Kummer-Based Scalar Multiplication



Architecture of the Single-Core Implementation



Techniques for Designing the Modular Multiplier

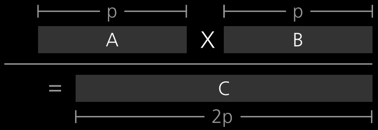
01 Multiplier computes and accumulates all digit-products in parallel

02 Use non-standard tiling to reduce DSP slices

03 Combine multiplication and reduction for better performance

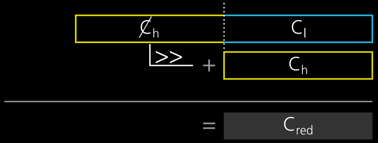
Modular Multiplication using Mersenne Primes $M_p = 2^p - 1$

Step 1:
multiplication

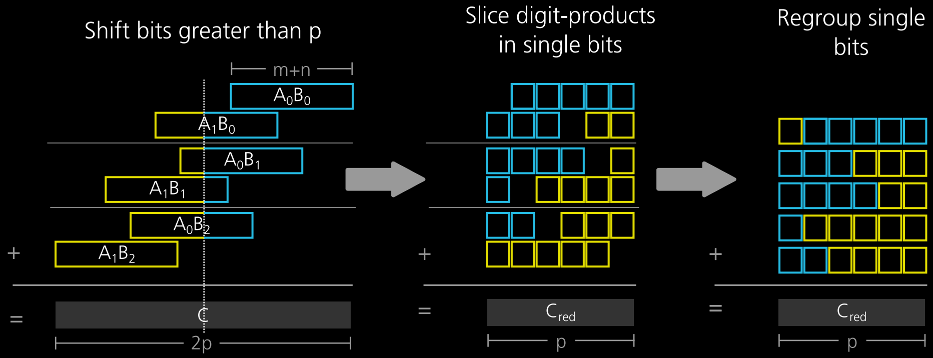


Step 2:
fast
reduction

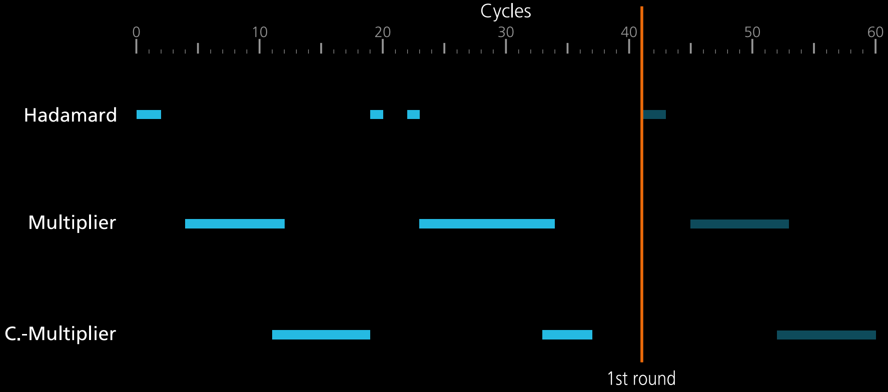
Crandall: $C \equiv \cancel{2^p}C_h + C_l \mod (2^p-1)$



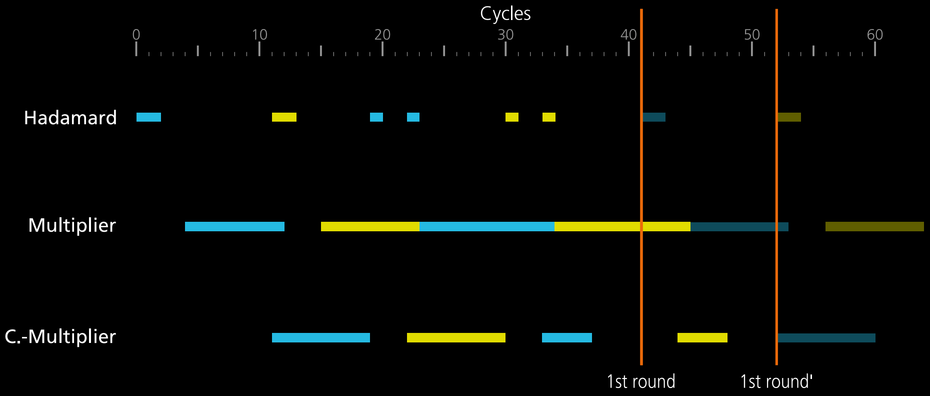
Regroup the Digit-Products on a Bit-Level



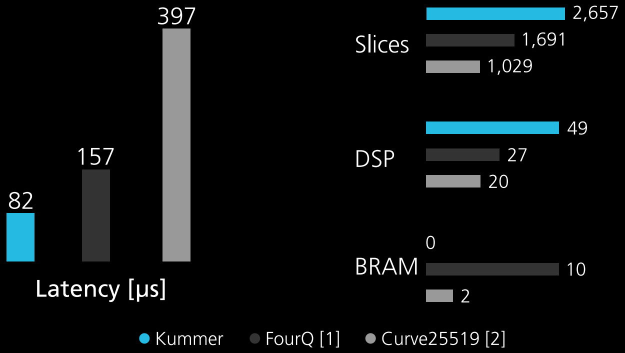
Scheduling the Field Operations for a Scalar Multiplication



Scheduling the Field Operations for a Scalar Multiplication



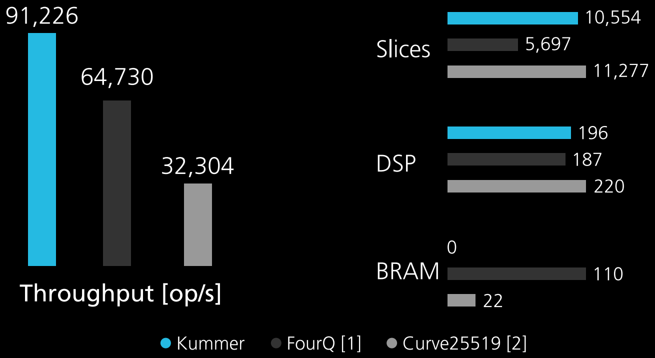
Single-Core: Performance and Area Results



[1] Järvinen et al. FourQ on FPGA: New hardware speed records for elliptic curve cryptography over large prime characteristic fields. CHES 2016

[2] Sasdrich and Güneysu. Efficient Elliptic-Curve Cryptography Using Curve25519 on Reconfigurable Devices, ARC 2014

Multi-Core: Performance and Area Results



[1] Järvinen et al. FourQ on FPGA: New hardware speed records for elliptic curve cryptography over large prime characteristic fields. CHES 2016

[2] Sasdrich and Güneysu. Efficient Elliptic-Curve Cryptography Using Curve25519 on Reconfigurable Devices, ARC 2014

Three Take Home Messages

01 Kummer based key exchange enables high-speed DH on FPGA

02 Difficult comparison due to very specific hardware optimization

03 HECC is an interesting alternative to ECC, but more research is required

Contact Information

Philipp Koppermann

Hardware Security

Fraunhofer Institute for Applied and Integrated Security (AISEC)

Phone: +49 89 3229986-138
E-Mail: philipp.koppermann@aisec.fraunhofer.de