



POLITECNICO
MILANO 1863

An Evaluation of the State-of-the-Art Software and Hardware Implementations of BIKE

A. Galimberti, G. Montanaro, W. Fornaciari, D. Zoni

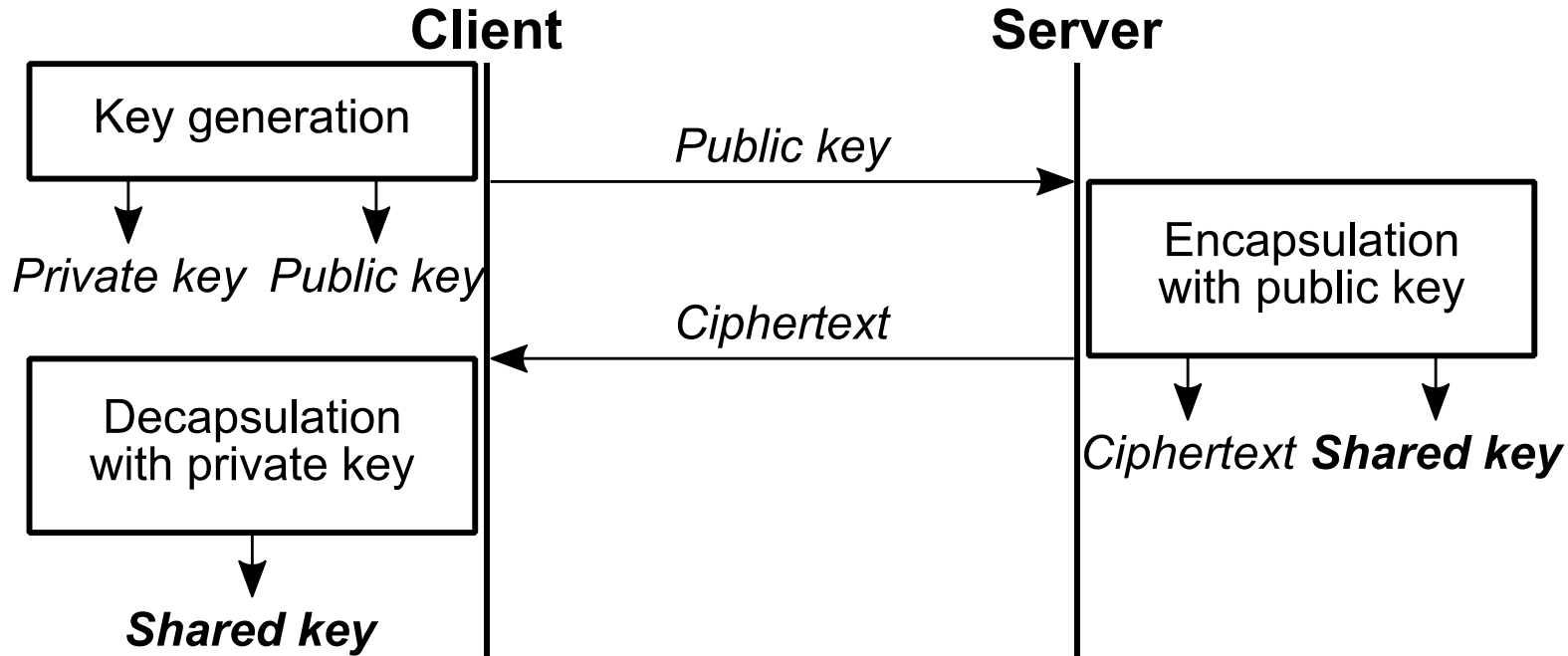
17/01/2023

NIST PQC Competition

- Secure cryptosystems
- Efficient HW/SW implementations
- Different categories of cryptoschemes

Status	KEMs	Digital Signatures
Selected for standardization	CRYSTALS-Kyber [L]	CRYSTALS-Dilithium [L] Falcon [L] SPHINCS+ [L]
Advancing to the fourth round	<u>BIKE</u> [C] Classic McEliece [C] HQC [C] SIKE [I]	


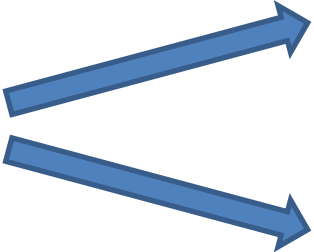
Legend: [C] = Code-Based, [L] = Lattice-Based, [I] = Isogeny-Based



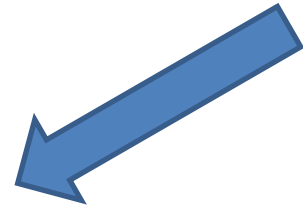
BIKE Cryptosystem

- QC-MDPC code-based
- Key-Encapsulation Mechanism (KEM)
- Three main primitives

Overview and Comparison of BIKE Implementations

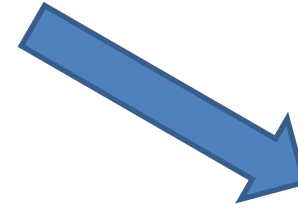
- Differences between available implementations  SW, HW and HW/SW implementations
- Testing BIKE performance on various platforms 
 - From low-end to desktop-class CPUs
 - Middle-range FPGA family

Chosen Implementations



Software

- Reference C99
- Portable C99
- Intel-AVX2 Optimized



Hardware and HW/SW

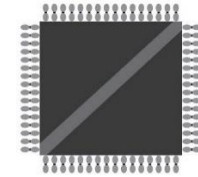
- Official
- Client/Server
- HLS-Based

- ARM Cortex-A9
- ARM Cortex-A53
- Intel Core i5 10310U



CPUs

(from low-end to desktop-class)

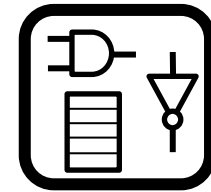


- Xilinx Artix-7



FPGAs

(entire family)

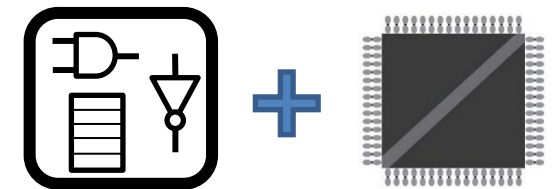


- Xilinx Zynq-7000



SoCs

(entire family)

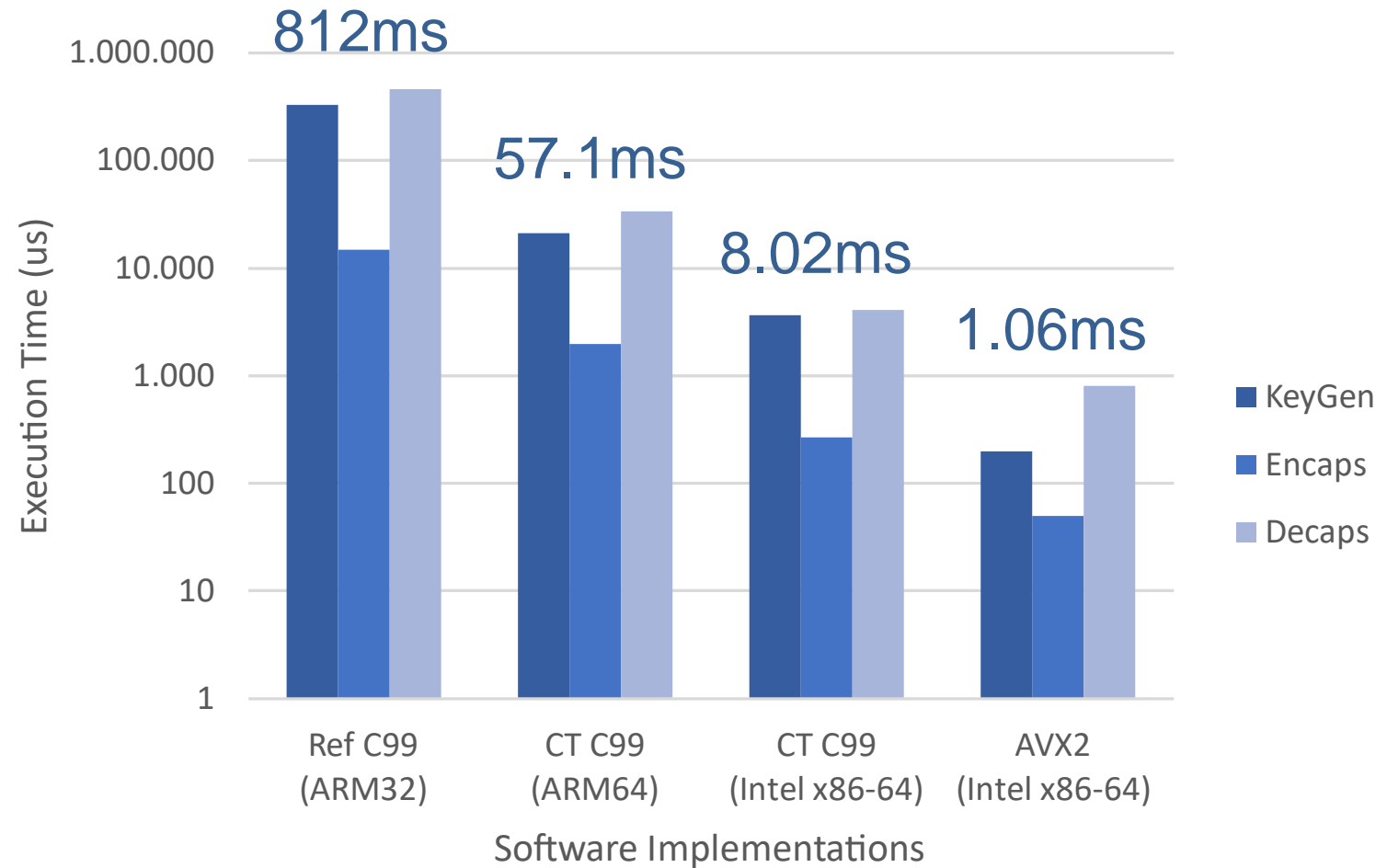


Software Performance

- Slowest: **Ref C99**
- **CT C99** is 7x faster on Intel x86-64 w.r.t. ARM64
- Fastest: **CT AVX2**

Clock Frequencies:

- 667MHz for ARM32
- 1GHz for ARM64
- 4GHz for Intel x86-64



Software Execution Breakdown

KeyGen:

PRNG + Inversion + Multiplication

Encaps:

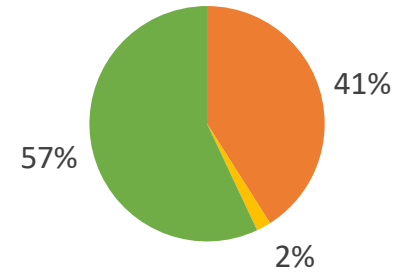
Multiplication + H, L, K Functions

Decaps:

Decode + H, L, K Functions

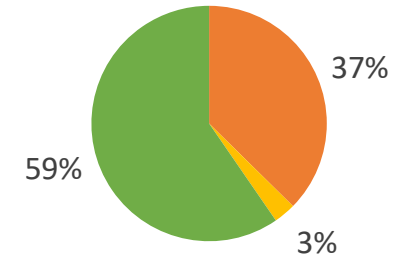
➔ AVX2 speeds up polynomial operations

Ref C99
(ARM32)



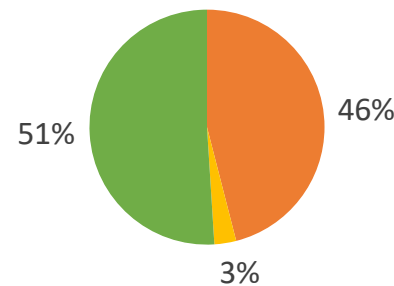
KeyGen Encaps Decaps

CT C99
(ARM64)



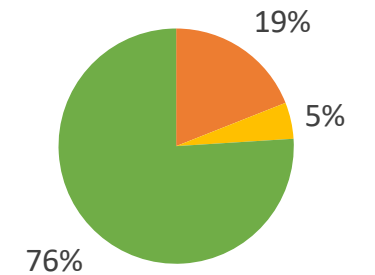
KeyGen Encaps Decaps

CT C99
(Intel x86-64)



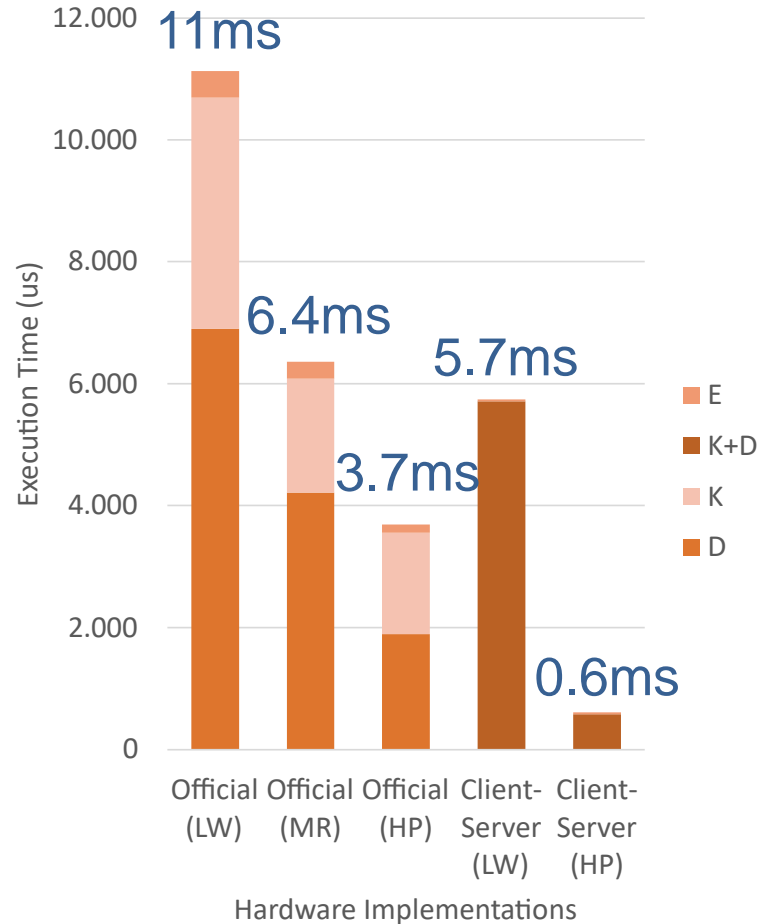
KeyGen Encaps Decaps

AVX2
(Intel x86-64)

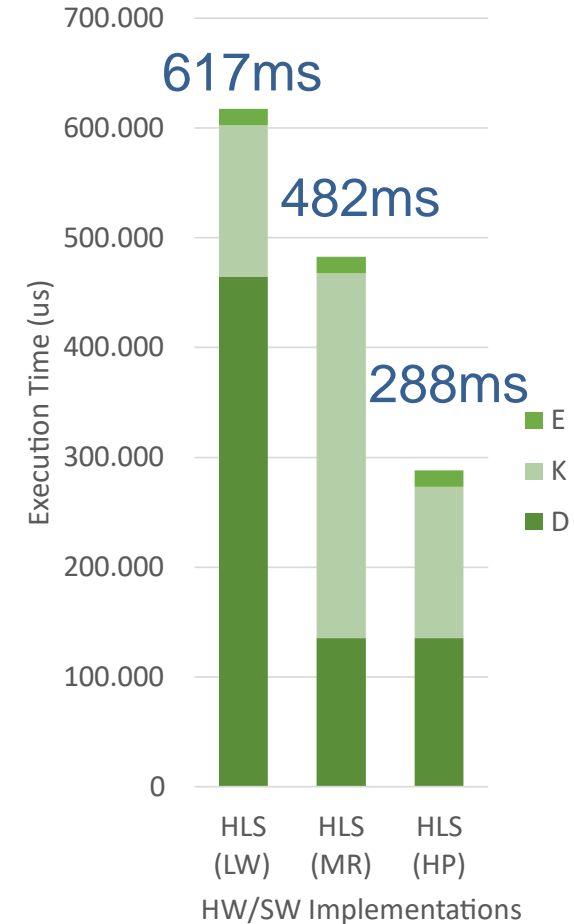


KeyGen Encaps Decaps

Hardware Performance



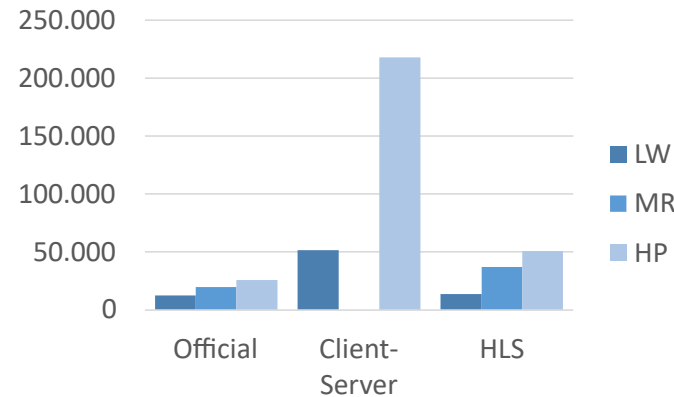
- **Official** is slower than Client-Server
- **Client-Server** is faster than AVX2
- **HLS** is orders of magnitude slower than handcrafted HW



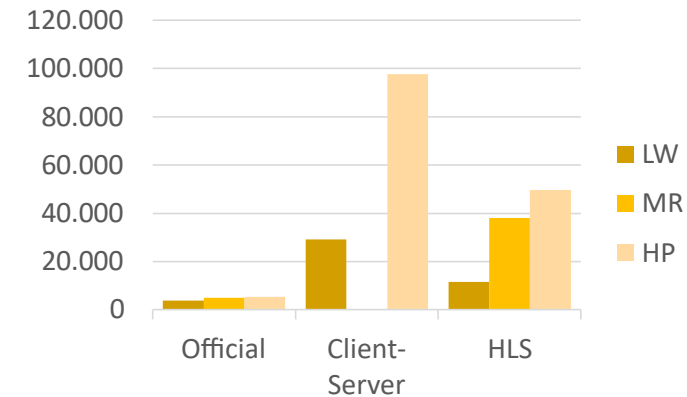
Hardware Resource Utilization

- **Official:** efficient utilization of available resources
- **Client-Server:** high performance at the cost of large resource consumption
- **HLS:** inefficient utilization of resources w.r.t. handcrafted HW

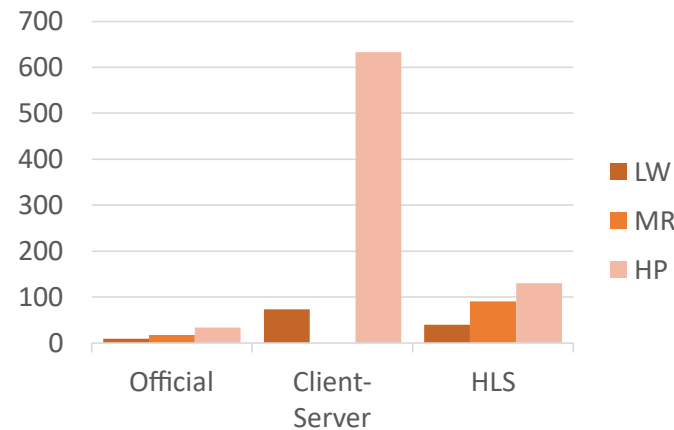
LUT Utilization



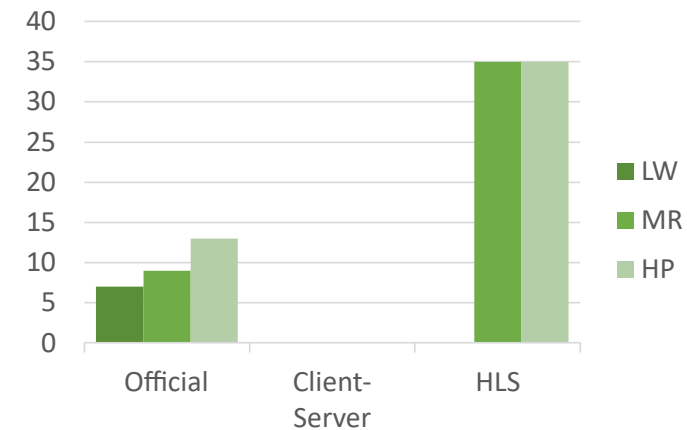
FF Utilization



BRAM Utilization



DSP Utilization



Evaluation of BIKE implementations

- Considerable differences between lower-end and desktop-class CPUs
- Best-performing HW outclasses the fastest SW implementation
- Superiority of handcrafted HW w.r.t. HLS solutions



Q&A

Gabriele Montanaro
gabriele.montanaro@polimi.it

Table 1 – SW Execution Time

KEM primitive	ARM32		ARM64		Intel x86-64			
	Ref C99		CT C99		CT C99		CT AVX2	
	SL1	SL3	SL1	SL3	SL1	SL3	SL1	SL3
KEYGEN	332.34	920.93	21.15	66.97	3.68	11.91	0.20	0.57
ENCAPS	14.83	40.94	1.99	5.60	0.27	0.77	0.05	0.09
DECAPS	464.82	1188.27	33.93	104.65	4.07	12.67	0.81	2.55
Overall KEM	811.98	2150.14	57.06	177.23	8.02	25.35	1.06	3.21

Table 2 – SW Execution Breakdown

KEM primitive	Operation	ARM32		ARM64		Intel x86-64			
		Ref C99		CT C99		CT C99		CT AVX2	
		SL1	SL3	SL1	SL3	SL1	SL3	SL1	SL3
KEYGEN	PRNG	0%	0%	1%	1%	0%	0%	1%	1%
	Inversion	39%	41%	34%	35%	43%	44%	17%	17%
	Multiplication	2%	2%	2%	2%	2%	2%	1%	1%
		41%	43%	37%	38%	46%	47%	19%	18%
ENCAPS	H function	0%	0%	1%	1%	1%	1%	2%	1%
	Multiplication	2%	2%	2%	2%	2%	2%	1%	1%
	L function	0%	0%	0%	0%	0%	0%	1%	1%
	K function	0%	0%	0%	0%	0%	0%	1%	0%
		2%	2%	3%	3%	3%	3%	5%	3%
DECAPS	Decoding	57%	55%	56%	56%	49%	48%	71%	75%
	L function	0%	0%	0%	0%	0%	0%	1%	1%
	H function	0%	0%	1%	1%	1%	1%	1%	1%
	K function	0%	0%	0%	0%	0%	0%	1%	0%
		57%	55%	59%	59%	51%	50%	76%	79%

Table 3 – HW Implementations

KEM primitive	Official			Client-server		HLS-based		
	LW	MR	HP	LW	HP	LW	MR	HP
KEYGEN	3.79	1.87	1.67	*5.71	*0.58	137.84	332.14	137.84
ENCAPS	0.44	0.28	0.13	0.03	0.03	14.86	14.86	14.86
DECAPS	6.90	4.21	1.89	*5.71	*0.58	464.61	135.48	135.48
Overall KEM	11.14	6.36	3.70	5.74	0.61	617.31	482.48	288.18

Resource	Official			Client-server		HLS-based		
	LW	MR	HP	LW	HP	LW	MR	HP
LUT	12319	19607	25549	51596	217932	13567	37160	50727
FF	3896	5008	5462	29206	97700	11621	38118	49739
BRAM	9	17	34	73.5	632.5	40	90	130
DSP	7	9	13	0	0	0	35	35
Target	A7-25	A7-35	A7-50	A7-100	2×A7-200	Z-7010	Z-7015	Z-7020

Received March 27, 2020, accepted April 17, 2020, date of publication April 21, 2020, date of current version May 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989423

Flexible and Scalable FPGA-Oriented Design of Multipliers for Large Binary Polynomials

DAVIDE ZONI¹, ANDREA GALIMBERTI, AND WILLIAM FORNACIARI¹, (Senior Member, IEEE)

Dipartimento di Elettronica Informazione e Bioingegneria (DEIB), Politecnico di Milano, 20133 Milano, Italy

Received August 10, 2020, accepted August 26, 2020, date of publication August 31, 2020, date of current version September 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3020262

Efficient and Scalable FPGA-Oriented Design of QC-LDPC Bit-Flipping Decoders for Post-Quantum Cryptography

DAVIDE ZONI¹, ANDREA GALIMBERTI, AND WILLIAM FORNACIARI¹, (Senior Member, IEEE)

Dipartimento di Elettronica Informazione e Bioingegneria (DEIB), Politecnico di Milano, 20133 Milan, Italy

Efficient and Scalable FPGA Design of $GF(2^m)$ Inversion for Post-Quantum Cryptosystems

Andrea Galimberti¹, Gabriele Montanaro, and Davide Zoni

FPGA implementation of BIKE for quantum-resistant TLS

Andrea Galimberti DEIB Politecnico di Milano Milano, Italy andrea.galimberti@polimi.it	Davide Galli DEIB Politecnico di Milano Milano, Italy davide11.galli@mail.polimi.it	Gabriele Montanaro DEIB Politecnico di Milano Milano, Italy gabriele.montanaro@polimi.it	William Fornaciari DEIB Politecnico di Milano Milano, Italy william.fornaciari@polimi.it
----------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

Davide Zoni
DEIB
Politecnico di Milano
Milano, Italy
davide.zoni@polimi.it

Presented at Euromicro DSD 2022

Hardware-Software Co-Design of BIKE with HLS-Generated Accelerators

Gabriele Montanaro DEIB Politecnico di Milano Milano, Italy gabriele.montanaro@polimi.it	Andrea Galimberti DEIB Politecnico di Milano Milano, Italy andrea.galimberti@polimi.it	Ernesto Colizzi SIAE MICROELETTRONICA Milano, Italy ernesto.colizzi@siaemic.com	Davide Zoni DEIB Politecnico di Milano Milano, Italy davide.zoni@polimi.it
------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

Presented at ICECS 2022