Chair of Security in Information Technology
TUM School of Computation, Information and Technology
Technical University of Munich

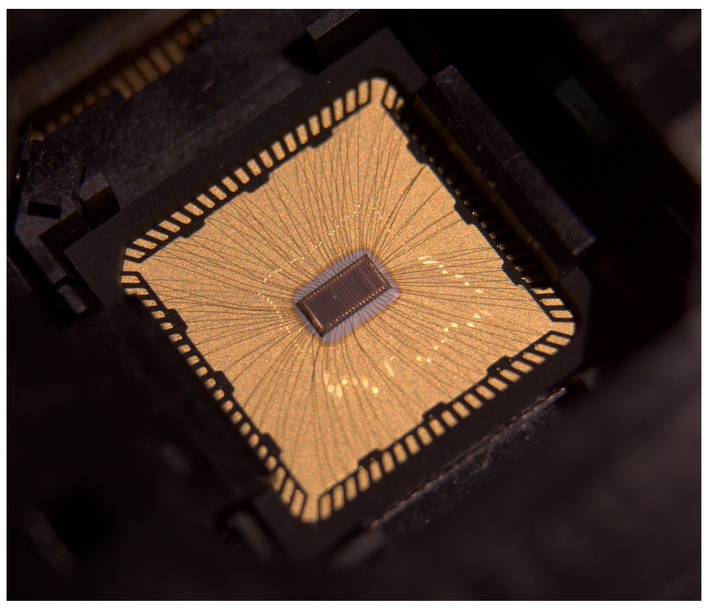
Silicon Proven Hardware Acceleration of Post-Quantum Cryptography on RISC-V

Jonas Schupp[1], Patrick Karl[1], and Georg Sigl[12]

Motivation

Hardware/Software co-designs offer a promising way to support different Post-quantum cryptographic algorithms on one platform. Especially, as these algorithms are not yet standardized, the flexibility of such an approach is important to support possible future algorithm changes in the standardization process. To explore the design space of such RISC-V based HW/SW co-designs, we present three different ASICs, designed since 2020, accelerating different subsets of the PQ-algorithms in the NIST competition, one in UMC 65nm and two in Globalfoundries' 22nm. All designs offer significant performance advantages over pure software implementations on the same platform, while largely maintaining the flexibility of a pure software approach.

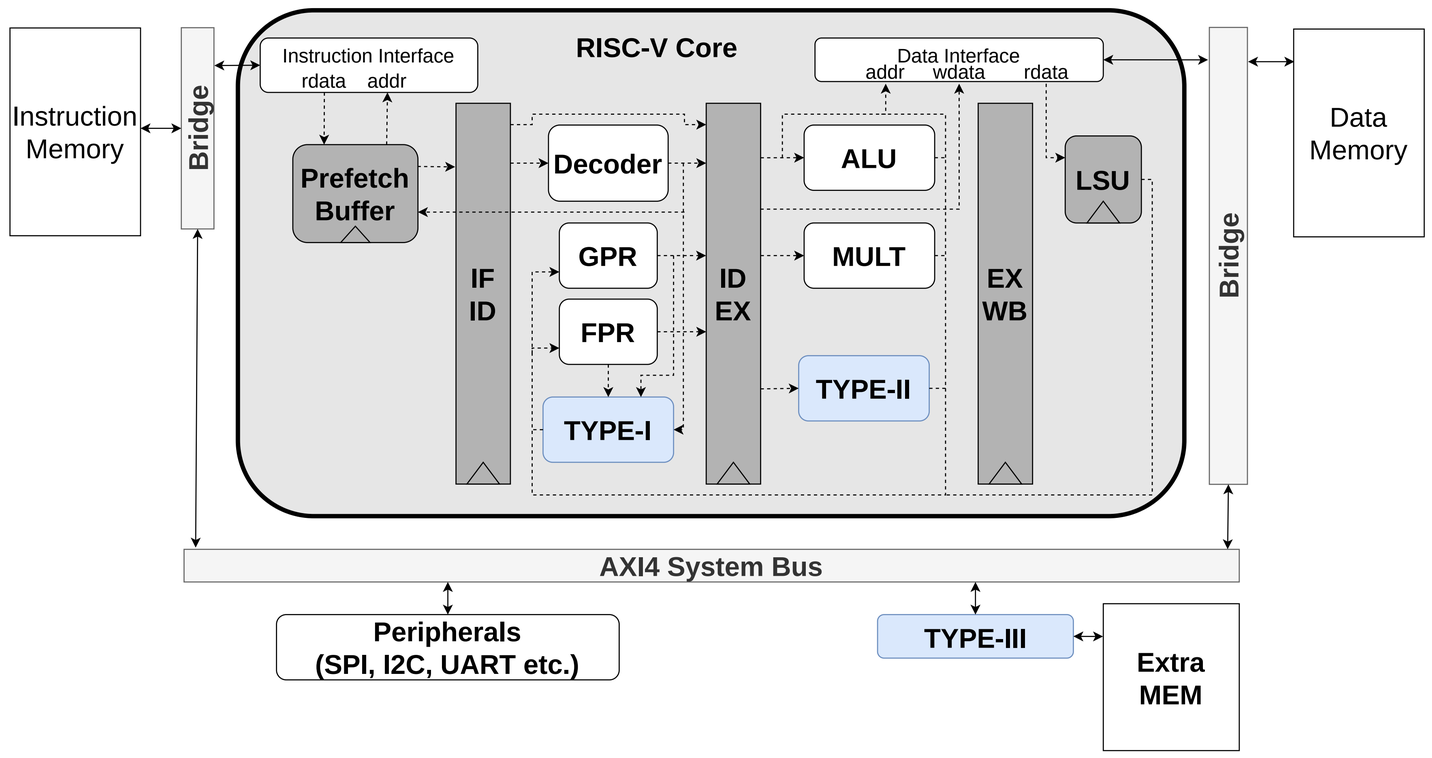
Bonded ASIC (Tapeout from 2021)



Hardware Acceleration[ab]

ISA extension (R-type instructions)
Example instructions from RISQ-V ISA extension

Opcode	Funct3	Funct7	Operation Name	Cycles
0x77	0x0	0x1	NTT Operation: *pq.ntt_multiple_bf*	83
0x77	0x1	0x1	NTT Operation: *pq.ntt_single_bf*	1
0x77	0x0	0x4	Keccak Operation: *keccak.f1600*	1



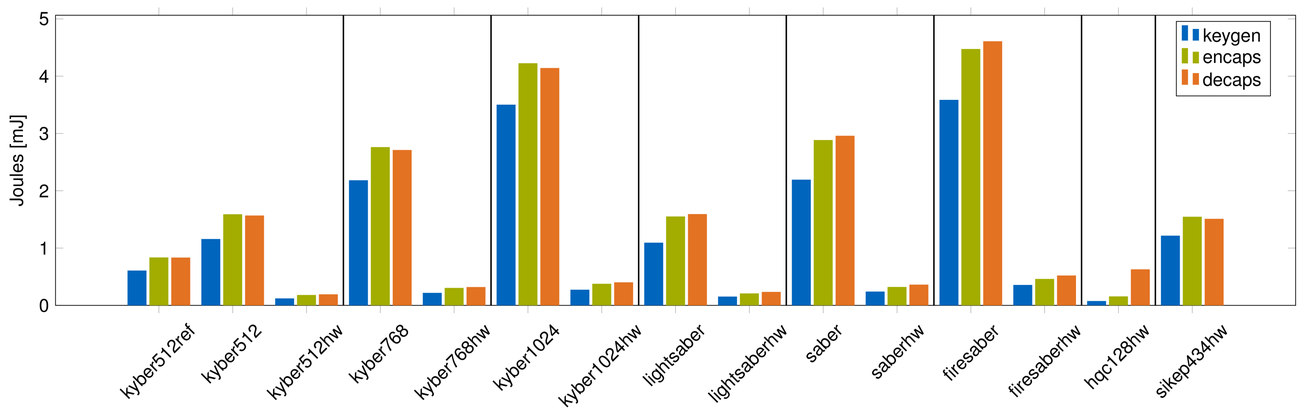
	Coupling	Performance	Cost	Possible Use-Case	Example
Type-I	tightly	high	moderate	cryptographic round function	Keccak
Type-II	tightly	moderate	lowest	customized multiplier	Binomial Sampling / Secure Adder
Type-III	loosely	highest	highest	complex subfunction / full algorithm	NTT

Performance Evaluation

RISQ-V (2020, 65nm)[b]: Power and energy consumption at $f = 10\,\text{MHz}$

Algorithm	Static Pwr. [mW]	Dyn. Pwr. [mW]	Tot. Pwr. [mW]	Cycles	Energy [µJ]
KYBER-512 CCA (baseline)	0.3	1.77	2.07	4,210,556	872
KYBER-512 CCA (w. accel.)	0.3	2.27	2.57	548,119	141

Accelerators for different PQ schemes (2021, 22nm)
Energy Consumption of different PQC algorithms with and without hardware acceleration at $f = 500\,\text{MHz}$



Accelerators for PQC Signatures (2022, 22nm)[c]
Latency comparison for Dilithium keygen/sign/verify in ms

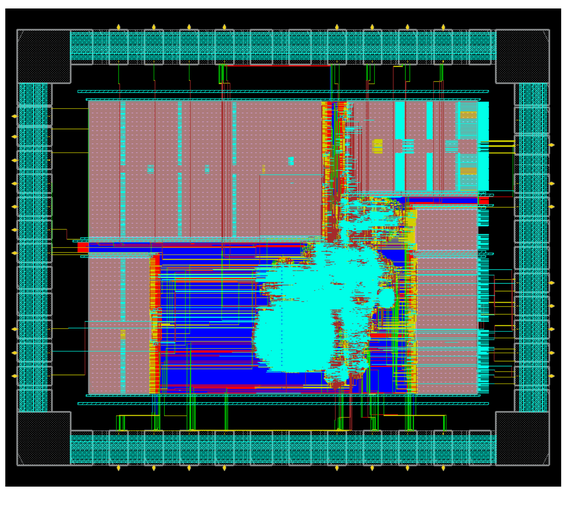
Platform	Dilithium-II	Dilithium-III	Dilithium-V
ASIC at 180 MHz	3.30 / 10.6 / 3.62	5.93 / 18.1 / 6.26	9.92 / 24.2 / 10.3
ASIC at 800 MHz	0.74 / 2.38 / 0.81	1.33 / 4.07 / 1.41	2.23 / 5.45 / 2.31
	2048 bit RSA	secp2561r1 ECDSA	
Cortex-M4 at 180 MHz[d]	450 / 448 / 12.5	8.43 / 12.3 / 25.2	

Area Cost

Change in footprint when adding the accelerators to the design for PQC Signatures

Design	Cell Count	Cell Area [µm²]
PULPino baseline	52,788	366,727
PULPino w. accel.	85,778 (+62%)	456,804 (+25%)

ASIC-Design of the RISC-V core with accelerators (Design from 2022)



⇒ The accelerators speed the considered algorithms significantly up while reducing the energy consumption of the designs at the same time

[1]Chair of Security in Information Technology, Technical University of Munich
[2]Fraunhofer Institute for Applied and Integrated Security, Germany

[a]Fritzmann et. al.: RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography (2020)
[b]Fritzmann et. al.: Masked Accelerators and Instruction Set Extensions for Post-Quantum Cryptography (2021)
[c]Karl et. al.: Post-Quantum Signatures on RISC-V with Hardware Acceleration (2023)
[d]Tasopoulos et. al.: Performance Evaluation of Post-Quantum TLS 1.3 on Resource-Constrained Embedded Systems (2021)