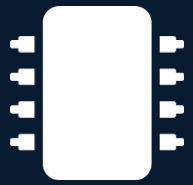


Open-Source Silicon

Building sustainable, secure, transparent chip ecosystems

Dom Rizzo (domrizzo@zerorisc.com)
Founder & CEO, zeroRISC
Chair of the Trusted Open Source Silicon Task Force, GlobalPlatform

The Open Source Precedent in Software

97%

of codebases contain open-source components

2-5×

RoI for active contributors vs. passive consumers

$8.8T

estimated value of OSS to the global economy

Open source transformed software by accelerating innovation, fostering collaboration, and increasing transparency. Now, the same paradigm is reshaping hardware.

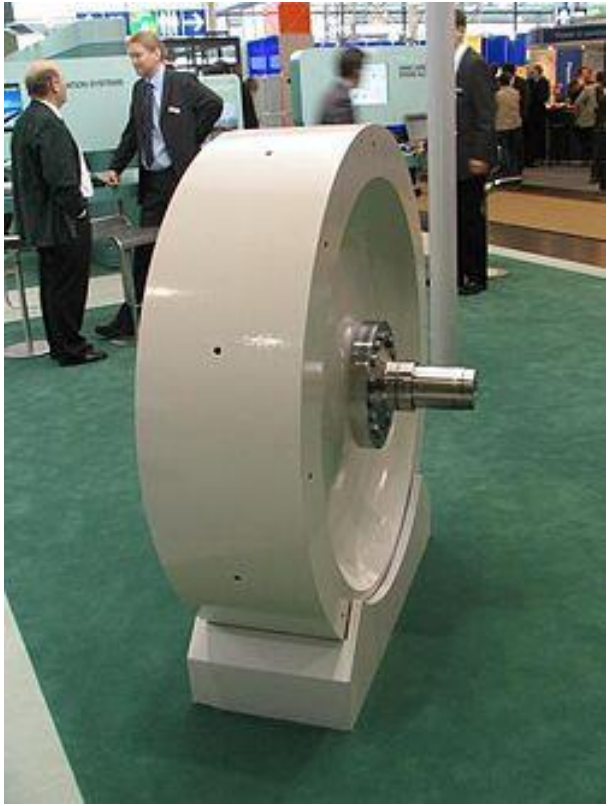
Why can’t silicon have nice things too?

RISC-V and Open Silicon

RISC-V provides an open, royalty-free ISA—but an ISA alone isn't an open implementation

1999	OpenCores founded—early open-source hardware community
2010	RISC-V ISA defined at UC Berkeley
~2013	First PULP designs at ETH Zürich—open-source processor platform
2015	RISC-V Foundation formed; industry adoption begins
2018	OpenTitan launched—first open-source silicon root of trust
2023	RISC-V International exceeds 4,000 members
2026	Open silicon enters production in consumer devices

The open-source “flywheel”



Momentum and critical thresholds

Enough technical collateral (RTL, DV, code) and structure (docs, style guides, established governance) has to exist for positive feedback

Those barriers are higher in silicon

Creating a chip is much more costly than the digital design, production-quality bar is higher, **lack of open source EDA (**e.g. compilers) possibly the highest bar

Lack of meta-circular commercialization

Without the ability to test and iterate (no free compilers), hard to iterate to commercial products, lack of broad commercial pull makes sustaining an open source ecosystem challenging

Sustainable Open-Source Silicon

Common misperceptions, open issues, and ongoing work

#1 Picking the right problem

Why Open Source Secure Silicon — A Personal Journey

A persistently unsolved problem, addressed iteratively

~1999

OpenCores.org

- First open-source silicon effort; inconsistent implementations
- Green shoots of standardization; wishbone open-source bus
- Remember the flywheel; establishing norms and ecosystems is costly

~2014

Honest Machines

- RISC-V existed, was building momentum
- Program pitch to DARPA for verifiable hardware; remove the leap of faith
- Goal: production-quality open silicon ecosystem
- Grab-bag: formally verified crypto all the way through tagged architectures

~2018

OpenTitan

- Essentially Honest Machines, but motivated by a business concern
- “How do we continue to buy OTS equipment and maintain a consistent security bar?”
- Proposal: lift all boats with a solid, open-source implementation

Kerchoff’s Principle (stumbling on the right answer)

In proprietary silicon, you trust a vendor's claims. In open silicon, you can verify them.

“a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge”

This is important for inspection, development, trustworthiness, innovation and development; cryptography is subtle

Collaborate on the core, compete on the edges

VS

THE CORE

Collaborate

Non-differentiated, must-work infrastructure.

Open source thrives here:
New technology, lower in the stack, not yet winner-take-all, evolving regulations, security

THE EDGES

Compete

Differentiated features where companies add proprietary value.

Proprietary value here:
Winner-take-all, well-established tech, higher in the stack, differentiation exists

Secure silicon fits squarely into Core

Trusted Open Source Silicon Task Force (TOSSTF)

A GlobalPlatform Initiative

A cross-industry initiative to establish a permissively licensed open-source silicon distribution that is secure-by-design and compatible with certification schemes by default — balancing commercial viability with community-driven development to support the broadest possible ecosystem.

Governance Model

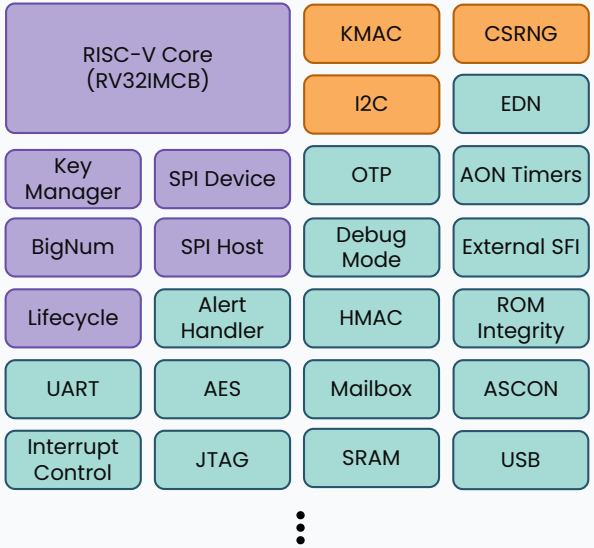
- Working relationships with GP Technical Committees to ensure ongoing standards alignment
- Distribution working model applying Open Source Software norms to silicon
- Synergies with existing and forthcoming GP efforts
- Secure-by-design principles as default configuration

Legal Framework

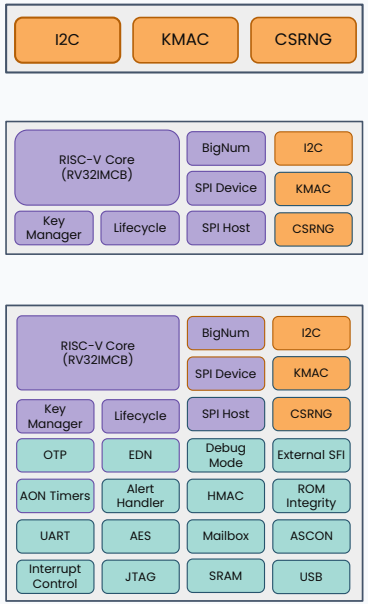
- Clear license and legal frameworks for any contributed or consumed collateral
- Particular attention to balancing commercial & community needs
- Certification-compatible contribution agreements
- Standards body engagement beyond GP (NIST, CC)

Ecosystem of Standards-Compatible Cores

Low cost, high quality, silicon-proven configurable IP ecosystem…



…that spans a full range of commercially valuable use cases



Identity: Integrity rests on identity; minimal configuration to secure the supply chain

Attestation: Extends Identity to include firmware and software attestation for the SoC and platform

Execution: Attestation plus a complete secure execution platform certifiable to support multiple applications like payments, MNO credentials, digital IDs and content protection (EMVCo, Common Criteria PP-0117, FIPS 140-3, TEE)

#2 Open-source is “free” (myth)

Open-source is not just “free” stuff

Contributions take effort

Upstream process can be long; (small) commit, (big) RFC => reviews => feedback => approval

Maintenance takes effort

Maintainers are typically hard-working volunteers, not shared employees

Integration takes effort

Not winner-take-all, new technology, lower in the tech stack, evolving regulations

Resource cost for upkeep

Continuous integration platform, emulation platforms, web hosting, events

But it is capital efficient*

49%

of consumers contribute upstream; 45% maintain private forks

2-5×

Benefit-to-cost ratio across upstream contribution types

5,160

labor hours per release cycle to maintain private forks

Actively participating in projects upstream is far more cost effective than passive consumption

*"ROI for Open Source Software Contribution", Sam Boysel and Adrienn Laws

#3 Open-source silicon projects are fundamentally different from open-source software (myth)

Common Misperceptions About Open Silicon

MYTH

“It takes a ton of money”

REALITY:

- Tapeouts are expensive…for a company producing a product
- Project is responsible for enforcing contribution quality
- Project is ideally commercially convincing
- But typically not responsible for making chips

MYTH

“Can’t fix mistakes after tapeout”

REALITY:

- Analogously, open source software projects are not responsible for bugs in commercial software
- Best practice: responsible disclosure and comms policy (good commercial argument to be involved)
- Reality is also more complex; chicken bits, embedded firmware, ROM patching, etc.

MYTH

“It’s legally risky from an IP perspective”

REALITY:

- An open-source project is responsible for both upstream contribution and downstream consumption frameworks
- Downstream is the license; OSI-approved typically
- Upstream is DCO, CLA or both; statements contributors agree to regarding right to contribute

Why Hardware Is (Not) Different

Commercial hardware **PRODUCT** is different, open-source hardware **PROJECT** is identical

	Software	Hardware
Open-Source Project	• Patch & deploy in hours • Marginal distribution cost ≈ $0 • CI/CD validates continuously • Rollback is cheap and routine	• Patch & deploy (RTL, DV, SW) in hours • Marginal distribution cost ≈ $0 • CI/CD validates continuously • Rollback is cheap and routine
Commercial Product	• Support or extensions of the Project • Bugs are fixed through regular patches • Regular releases / updates • Easy to file bug reports • Rollback is trivial • Vendor maintains paid product	• Tapeout adds analog, foundry, backend • Bugs are permanent in silicon • $10Ms per tapeout • Verification takes months pre-fab • No rollback after fabrication • Vendor owns errata and advisories

Open-source projects are not themselves products and should not be confused with each other

Example: Open Silicon PQC

Open implementations enable broad collaborations

Quick Intro — Post-Quantum Cryptography

THE PROBLEM

Q-Day

The day a cryptographically relevant quantum computer can break RSA, ECC, and Diffie-Hellman—the algorithms that protect virtually all digital communication today.

Harvest Now, Decrypt Later

Adversaries are already recording encrypted traffic today, banking on future quantum capability to decrypt it. For long-lived secrets—firmware keys, device identities, state secrets—the threat is present tense.

THE SHIFT

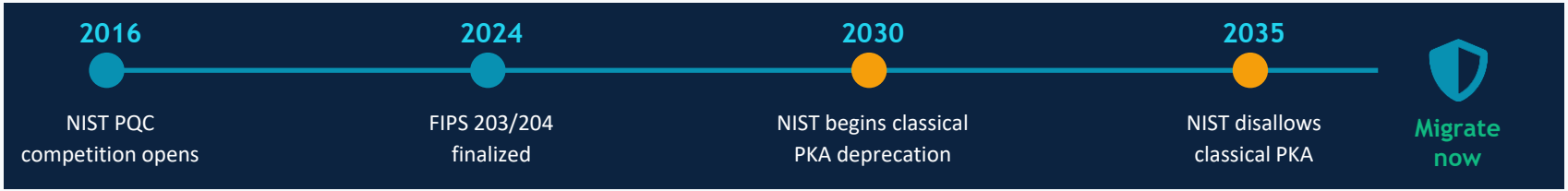
RSA / ECC
integer factoring
elliptic curves

ML-KEM / ML-DSA
lattice-based
problems

Why Lattices?

NIST standardized ML-KEM (key encapsulation) and ML-DSA (digital signatures) in FIPS 203/204. Both rely on structured lattice problems—believed hard even for quantum computers.

Larger keys & signatures → hardware acceleration matters.



Multi-Year, Multi-Organization Collaboration

Open Silicon was a key unlock to enabling a hyper-productive industry and research collaboration

Multiple Organizations

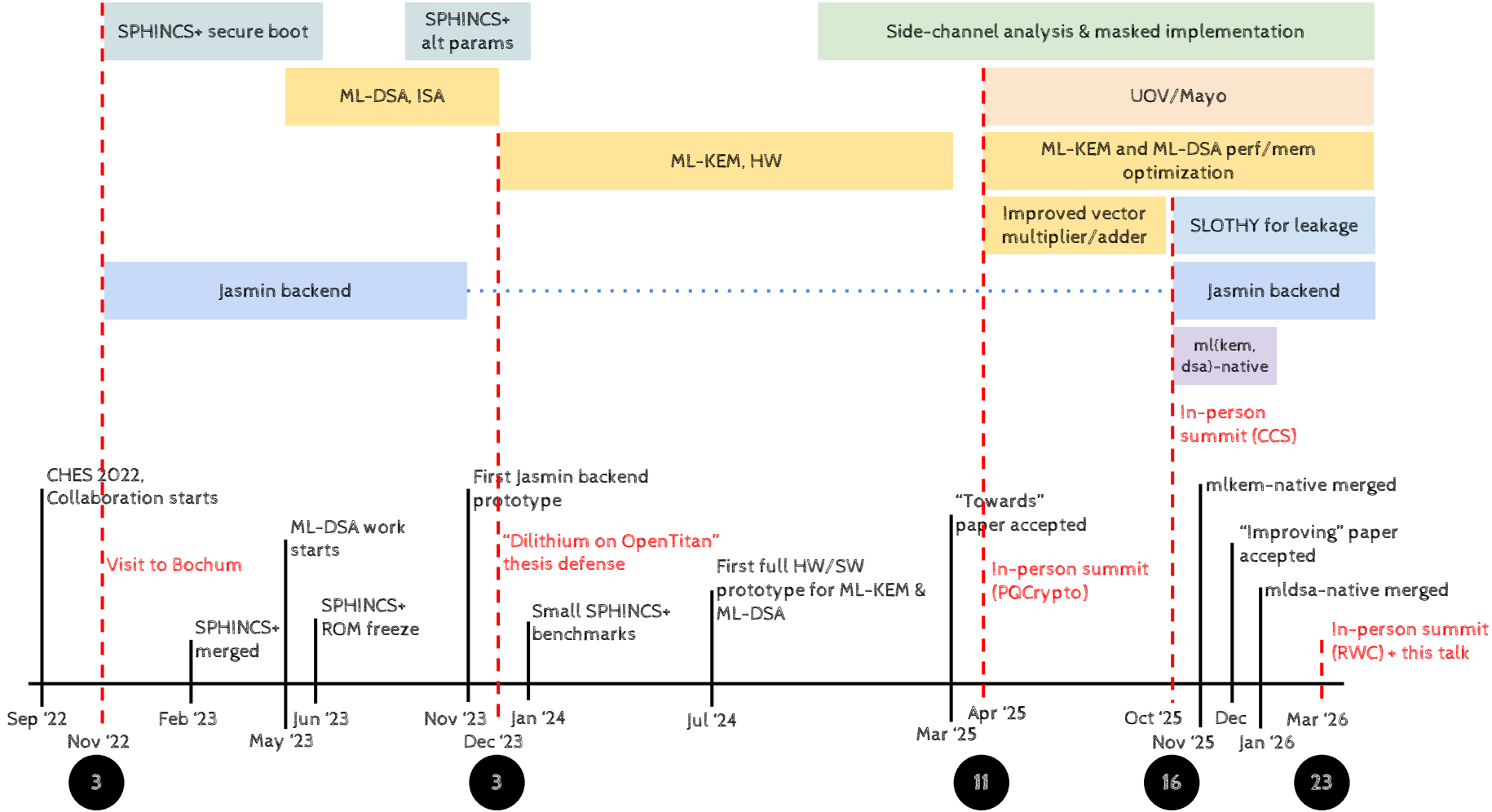
Open Silicon enabled all the participating organizations to collaborate in the open; Max Planck Institute for Security and Privacy in Bochum, Fraunhofer AISEC, Academia Sinica and ZeroRISC

Mutually Beneficial

The academic collaborators were able to publish cutting edge cryptography research, my team was able to step in and perform non-research engineering refinement to bring it up to production quality (testing, design verification, optimization)

Academic Rigor, Peer Reviewed Credibility

IEEE S&P 2005, CHES 2026, RWC 2026, numerous blog posts


SPHINCS+ secure boot
SPHINCS+ alt params
Side-channel analysis & masked implementation
ML-DSA, ISA
UOV/Mayo
ML-KEM, HW
ML-KEM and ML-DSA perf/mem optimization
Improved vector multiplier/adder
SLOTHY for leakage
Jasmin backend
Jasmin backend
ml(kem, dsa)-native
In-person summit (CCS)
CHES 2022, Collaboration starts
Visit to Bochum
SPHINCS+ merged
ML-DSA work starts
SPHINCS+ ROM freeze
First Jasmin backend prototype
"Dilithium on OpenTitan" thesis defense
Small SPHINCS+ benchmarks
First full HW/SW prototype for ML-KEM & ML-DSA
"Towards" paper accepted
In-person summit (PQCrypto)
mlkem-native merged
"Improving" paper accepted
mldsa-native merged
In-person summit (RWC) + this talk
Sep '22
Nov '22
Feb '23
May '23
Jun '23
Nov '23
Dec '23
Jan '24
Jul '24
Mar '25
Apr '25
Oct '25
Nov '25
Dec
Jan '26
Mar '26
3
3
11
16
23

Worked Example: PQC Transition; Open Silicon Shines

Illustrates the full quartet of benefits in one project

Commercial Value	Significantly less costly than proprietary implementations
Standards Alignment	SPX+, ML-KEM and ML-DSA are NIST standards and entering broad use
Trustworthiness	Implementation is open and heavily peer reviewed by broader cryptography community
Innovation Accelerant	If in-house, would have required 5x people + time; if purely academic, no refinement to practice; both parties benefited mightily from the collaboration

Result: fully open-source, production-ready PQC + Classical asymmetric accelerator

OTBN + ML-DSA + ML-KEM = ACC

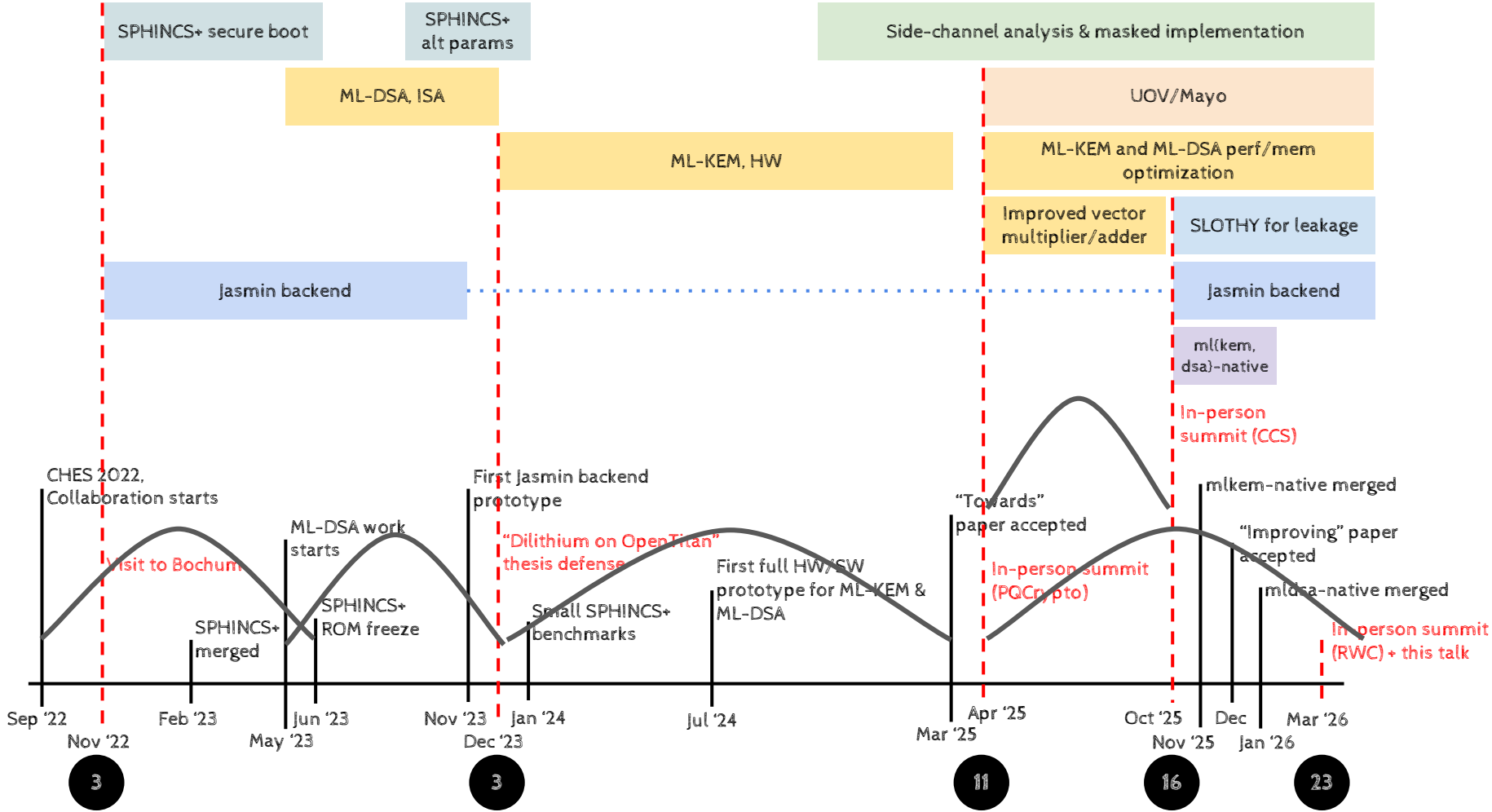
Asymmetric Cryptography Coprocessor

ML-KEM-768 decapsulation: 0.7ms at 100MHz
ML-DSA-65 signing (median): 6.5ms at 100MHz
Memory: 32KB IMEM, 32KB DMEM

Improvements relative to baseline

- 8–10x latency improvement from baseline for ML-KEM and ML-DSA operations
- Memory-optimized ML-DSA signing in 32KiB — with slowdowns of just 82–138% vs. the 200–400% originally anticipated
- 52% speedup for ML-DSA operations through novel vectorized rejection sampling
- 20% reduction in ML-KEM decapsulation cycles via a fully branchless sampling loop
- 36–75% improvement in maximum frequency

Open Silicon PQC


SPHINCS+ secure boot
SPHINCS+ alt params
Side-channel analysis & masked implementation
ML-DSA, ISA
UOV/Mayo
ML-KEM, HW
ML-KEM and ML-DSA perf/mem optimization
Improved vector multiplier/adder
SLOTHY for leakage
Jasmin backend
Jasmin backend
ml(kem, dsa)-native
In-person summit (CCS)
CHES 2022, Collaboration starts
Visit to Bochum
SPHINCS+ merged
ML-DSA work starts
SPHINCS+ ROM freeze
First Jasmin backend prototype
"Dilithium on OpenTitan" thesis defense
Small SPHINCS+ benchmarks
First full HW/SW prototype for ML-KEM & ML-DSA
"Towards" paper accepted
In-person summit (PQCrypto)
mlkem-native merged
"Improving" paper accepted
mldsa-native merged
In-person summit (RWC) + this talk
Sep '22
Nov '22
Feb '23
May '23
Jun '23
Nov '23
Dec '23
Jan '24
Jul '24
Mar '25
Apr '25
Oct '25
Nov '25
Dec
Jan '26
Mar '26
3
3
11
16
23

Open-Source Silicon took longer

But is poised to have industry-wide impact

Dominic Rizzo; CEO

domrizzo@zerorisc.com,
dom.rizzo@globalplatform.org

Open Silicon PQC