barkhauseninstitut.org

barkhausen institut

Technische Universität Dresden

Secured and Adaptive Continuum:
Crypto Agility & Sustainable Security for Cyber-Physical Systems (or Physical AI)

‘Secure Digital Systems (SDS)‘ Research Group

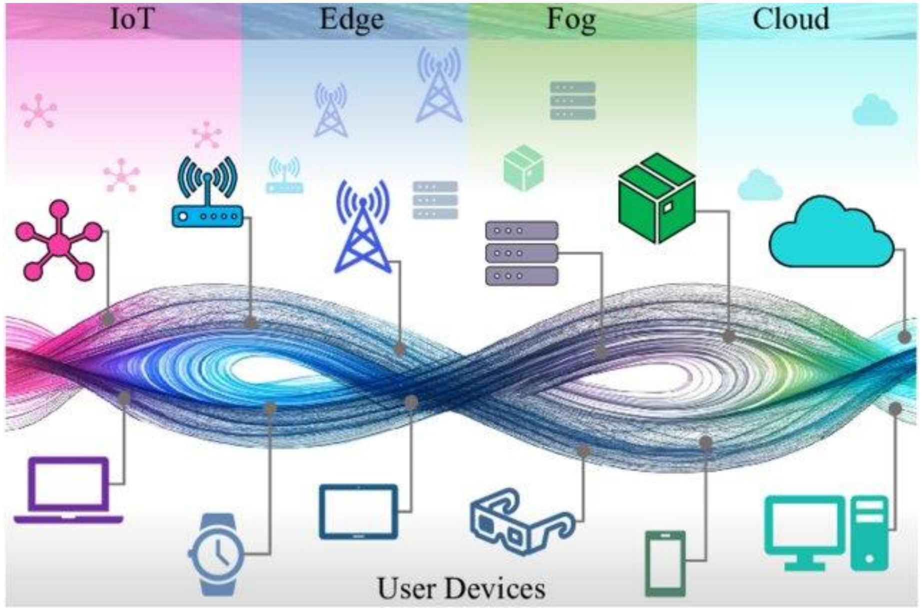
Elif Bilge Kavun

25.09.2025

What is “continuum“?

- In **computing & technology**

  - *Seamless integration* and *unified nature* of distributed computational resources, encompassing *devices from the cloud to the network edge**



[*] L. F. Bittencourt et al., The computing continuum: Past, Present, and Future, Computer Science Review, Volume 58, 2025, doi: 10.1016/j.cosrev.2025.100782
[Figure] V. Karagiannis, Data Sovereignty and Compliance in the Computing Continuum, 11th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 123-130, 2024, doi: 10.1109/FiCloud62933.2024.00027

“Security“ in Computing Continuum

- Security in the computing continuum is essential!*
  - Vast, interconnected nature of cloud, edge, and IoT devices creates an expansive attack surface and complex vulnerabilities
  - Requires **end-to-end**, **agile**, and **proactive** protection
  - Demand for **smart, automated mechanisms** to **secure all layers and components** against threats, ensuring the **confidentiality, integrity, and availability of data** and systems **throughout their entire lifecycle**

[*] https://www.horizon-europe.gouv.fr/secure-computing-continuum-iot-edge-cloud-dataspaces-32305

Why Security is Crucial?

- **Interconnected Ecosystem**
  - Countless interacting devices and platforms, from resource-constrained IoT devices to high-performance cloud systems, broadens the attack surface

- **Complex Vulnerabilities**
  - System complexity creates numerous opportunities for attacks, ranging from industrial control systems to smart city infrastructure applications

- **Sensitive Data**
  - Vast amounts of sensitive user and business data is handled, which must be protected from breaches, tampering, and unauthorized access across different layers

- **Evolving Threats**
  - Conventional security methods are often inadequate for addressing the unique challenges of the continuum, requiring adaptable protection mechanisms

What Needs To Be Secured?

- **All Levels**
  - Security measures at every level of the architecture, from the smallest edge devices to complex cloud environments
- **Components**
  - Individual components; including software, cloud infrastructure, and IoT devices
- **System Lifecycle**
  - Security and privacy measures should be available for all components and systems throughout their entire lifecycle, from deployment to disposal

Key Security Concepts and Technologies [1, 2]

- **End-to-End Security**
  - Security must be integrated across the entire continuum, from the origin of data to its destination
- **Privacy-Enhancing Technologies**
  - Enabling data analysis without compromising sensitive information
- **Dynamic Intrusion Detection**
  - Systems are needed to detect and respond to malicious activities in real-time
- **Attribute-Based Access Control**
  - Used for managing access rights and authorizations, ensuring that users only have access to necessary resources

[1] https://www.horizon-europe.gouv.fr/secure-computing-continuum-iot-edge-cloud-dataspaces-32305
[2] M. Barbareschi, V. Casola and D. Lombardi, "Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions," 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 273-278, 2023, doi: 10.1109/CloudCom59040.2023.00051

Key Security Concepts and Technologies [1, 2]

- **Physical Unclonable Functions (PUFs)**
  - Such unique hardware identifiers / hardware security anchors derived from physical/manufacturing variability can be used to enhance security, especially for resource-constrained devices, at low-cost

- **Data Encryption**
  - Encrypting sensitive data before it is uploaded to the cloud or transmitted over networks is fundamental

- **Identity and Access Management**
  - Regular review and updating of policies are critical to ensure proper user access

[1] https://www.horizon-europe.gouv.fr/secure-computing-continuum-iot-edge-cloud-dataspaces-32305
[2] M. Barbareschi, V. Casola and D. Lombardi, "Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions," 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 273-278, 2023, doi: 10.1109/CloudCom59040.2023.00051

Key Security Concepts and Technologies [1, 2]

- **Physical Unclonable Functions (PUFs)**
  - Such unique hardware identifiers / hardware security anchors derived from physical/manufacturing variability can be used to enhance security, especially for resource-constrained devices, at low-cost

- **Data Encryption**
  - Encrypting sensitive data before it is uploaded to the cloud or transmitted over networks is fundamental

- **Identity and Access Management**
  - Regular review and updating of policies are critical to ensure proper user access

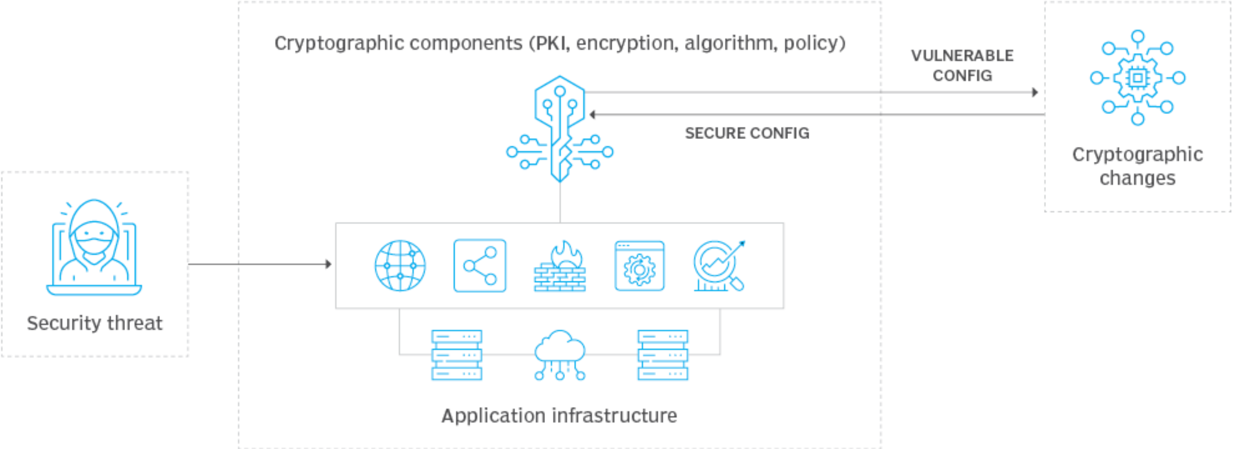
All calling for cryptographic solutions such as encryption algorithms and protocols!

[1] https://www.horizon-europe.gouv.fr/secure-computing-continuum-iot-edge-cloud-dataspaces-32305
[2] M. Barbareschi, V. Casola and D. Lombardi, "Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions," 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 273-278, 2023, doi: 10.1109/CloudCom59040.2023.00051

What is Crypto Agility?

- Ability of an organization to **swiftly and easily switch between different cryptographic algorithms, protocols, and keys** to **adapt to evolving threats and new standards** [1, 2]

- An inherent **flexibility minimizes risk by preventing significant infrastructure disruption** when **vulnerabilities are discovered or when new encryption technologies become necessary**



[1] https://www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018
[2] https://www.capgemini.com/ch-en/insights/expert-perspectives/crypto-agility-the-unsung-hero-in-the-quantum-security-race
[Figure] https://www.techtarget.com/searchenterpriseai/definition/crypto-agility

More exactly…

- **Adaptability**
  - Capability to replace or update cryptographic components without needing to change/replan the entire IT infrastructure
- **Response to threats**
  - Allows organizations to quickly respond to new cryptographic vulnerabilities or the emergence of more powerful computing capabilities
- **Proactive approach**
  - Instead of a one-time fix, a continuous, proactive process of building the flexibility to respond to threats and standards over time

Why important?

- **Long-term security**
  - Ensures that systems remain secure and trustworthy as technology and threats evolve
- **Minimizes risk and outages**
  - Enabling rapid adaptation helps preventing events like certificate outages and minimizes risk exposure for businesses and users
- **Future-proofing**
  - Prepares organizations for the challenges of new algorithms which may need to be adopted

How To Achieve?

- **Maintain a comprehensive inventory**
  - Track all cryptographic keys, certificates, and algorithms in use
- **Adopt flexible frameworks**
  - Use modern development frameworks and service software that allow cryptographic algorithms to be updated via configuration files or databases
- **Implement robust Public Key Infrastructure (PKI)**
  - For managing digital certificates, essential for authentication and encryption
- **Plan for transitions**
  - Develop detailed plans for migrating from older algorithms to new ones

An (Old) Example*

- **X.509 Public Key Certificate**
  - A public key certificate has cryptographic parameters including key type, key length, and a hash algorithm
  - X.509 version v.3, with key type RSA, a 1024-bit key length, and the SHA-1 hash algorithm were found by NIST to have a key length that made it vulnerable to attacks
  - Prompting the transition to SHA-2 (at least)

[*] https://www.csoonline.com/article/550478/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html

A New Reason…

- **Quantum Threat! [1, 2]**
  - Quantum computers, while beneficial for various fields, have the potential to break current cryptographic algorithms
  - Rendering existing secrets vulnerable within 5-10 years, or even sooner

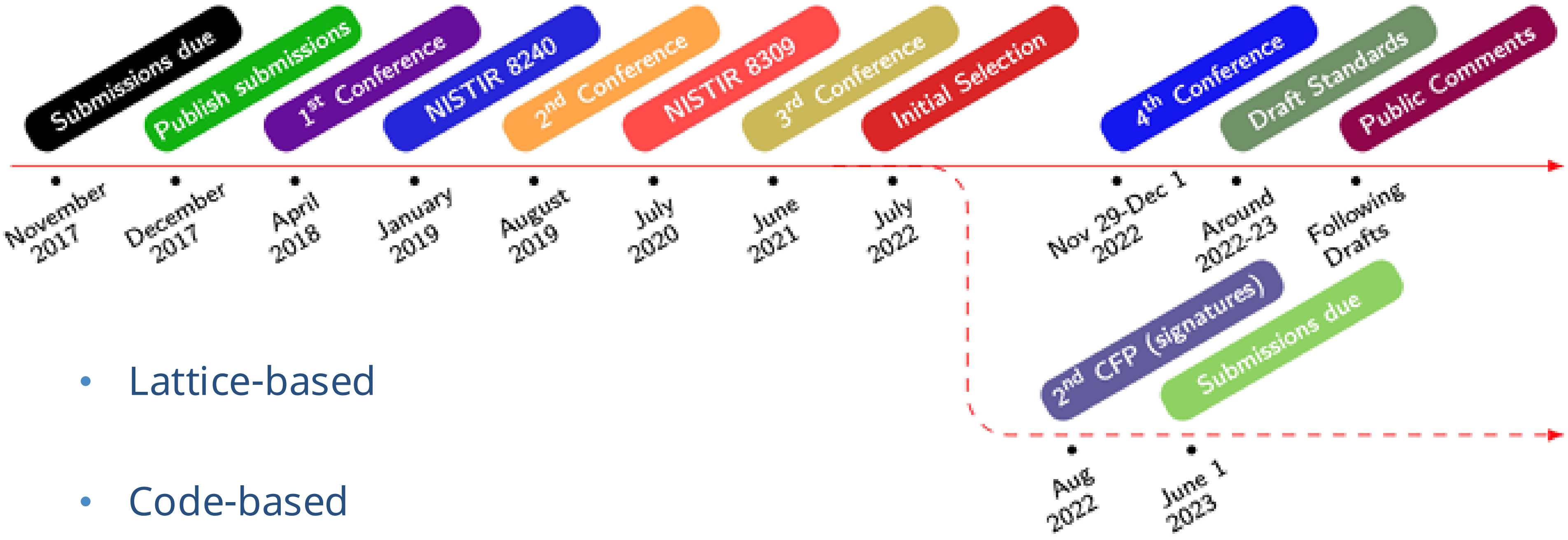
[1] https://csrc.nist.gov/projects/crypto-agility
[2] https://www.ibm.com/quantum/blog/crypto-agility
[Figure] https://quantumai.google/quantumcomputer

How?

- **"Harvest now, decrypt later!" [1]**
  - Encrypted data harvested today could be decrypted in the future by quantum computers
  - **Impact of Decryption:** If quantum computers break current encryption, sensitive information, digital signatures, electronic records, payment systems, and critical infrastructure could be compromised
  - Poses a significant threat to sensitive information like intellectual property and personal data

[1] https://www.ibm.com/quantum/blog/crypto-agility
[Figure] https://quantumai.google/quantumcomputer

NIST Competition: Post-Quantum Cryptography (PQC)



- Lattice-based
- Code-based
- Hash-based
- Isogenies …

[Figure] https://www.nccoe.nist.gov/sites/default/files/2023-08/pqc-light-at-the-end-of-the-tunnel-presentation.pdf

NIST Competition: Post-Quantum Cryptography

- NIST outlines the following timeline [*]
  - **From now until 2030**, existing encryption methods should be phased out
  - **By 2030**, algorithms relying on 112-bit security will be deprecated
  - **By 2035**, all systems will need to be transitioned, as traditional cryptographic algorithms will be disallowed

[*] https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/

NIST Competition: Post-Quantum Cryptography

- Digital Signature Algorithms [*]

Algorthims	Parameters	Deprecated	Disallowed
ECDSA, EdDSA, RSA	112 bits of security strength	2030	2035
ECDSA, EdDSA, RSA	≥ 128 bits of security strength	-	2035

[*] https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/

NIST Competition: Post-Quantum Cryptography

- Key Establishment Schemes [*]

Algorthims	Parameters	Deprecated	Disallowed
FInite Field DH and MVQ	112 bits of security strength	2030	2035
FInite Field DH and MVQ	≥ 128 bits of security strength	-	2035
Elliptic Curve DH and MQC	112 bits of security strength	2030	2035
Elliptic Curve DH and MQC	≥ 128 bits of security strength	-	2035
RSA	112 bits of security strength	2030	2035
RSA	≥ 128 bits of security strength	-	2035

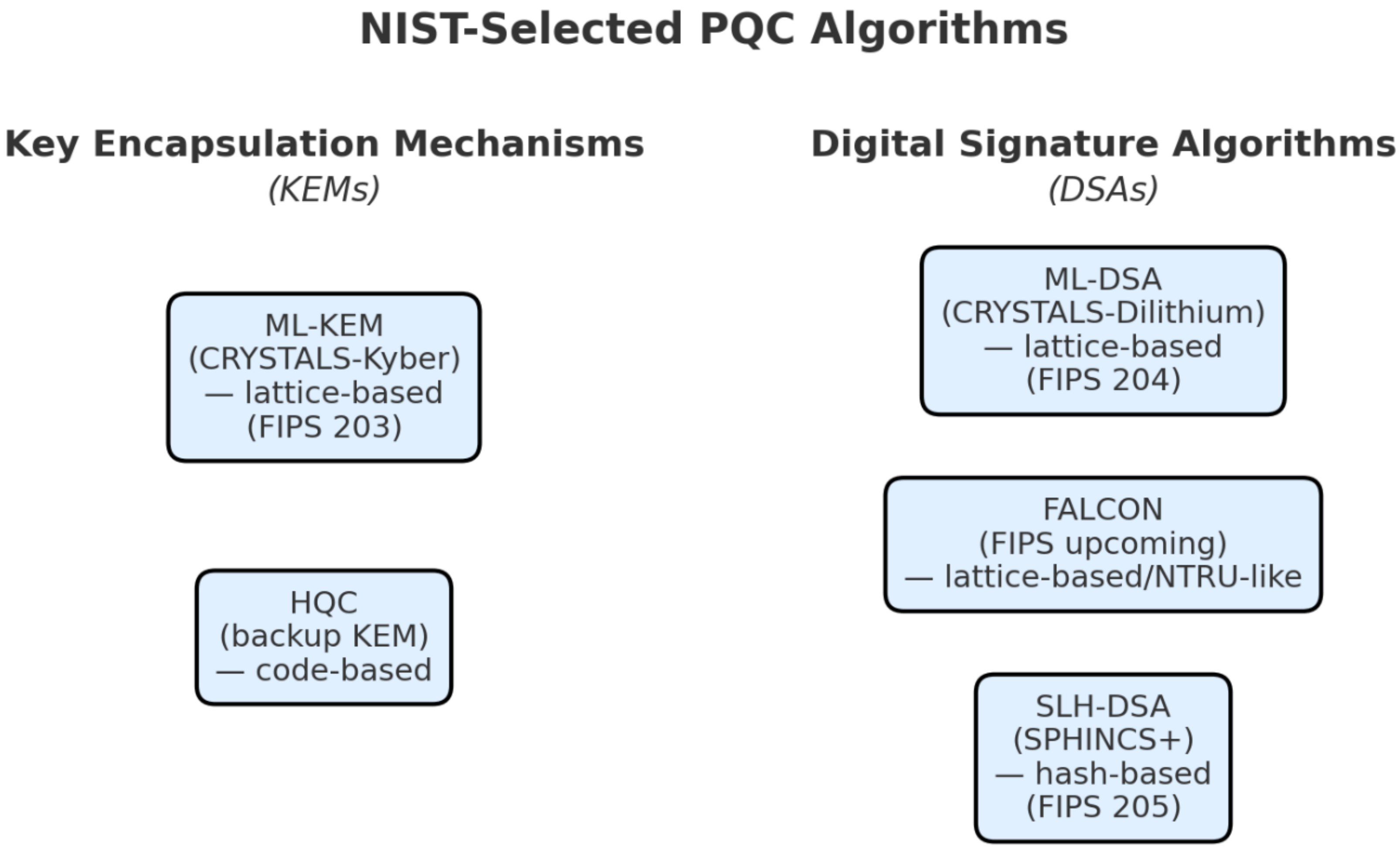
[*] https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/

NIST Competition: Post-Quantum Cryptography

- Symmetric Cryptography [*]
  - Symmetric cryptography standards are less vulnerable to quantum attack
  - Currently not included in PQC transition recommendations
  - **However**, standards at the 112-bit security level will be disallowed from 2030
  - Applications should move away from these when transitioning to PQC

[*] https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/

Post-Quantum Cryptography



Post-Quantum Cryptography

Federal Office
for Information Security

BSI – Technical Guideline

Designation: Cryptographic Mechanisms: Recommendations and Key Lengths

FrodoKEM-976 and FrodoKEM-1344, see [3, Section 2.5].

Table 2.5: Recommended parameters for FrodoKEM.

- mceliece460896, mceliece6688128 and mceliece8192128, see [2, Section 7],
- mceliece460896f, mceliece6688128f and mceliece8192128f (faster variants), see [2, Section 7].

Table 2.6: Recommended parameters for ClassicMcEliece-KEM.

- Quantum-safe signature algorithms
  - ML-DSA in the "hedged"-variant, see [104],
  - SLH-DSA in the "hedged"-variant, see [105], and
  - Stateful hash-based signatures[2](LMS/HSS and XMSS/XMSS^{MT}), see [98].

Table 5.3: Recommended signature algorithms.

Post-Quantum Cryptography

Asymmetric (All scenarios)	*Public-Key Encryption/KEMs*	CRYSTALS-KYBER	Classic McEliece, FrodoKEM	Any classical PKC
Asymmetric (Scenario 1 with Stateful Hash-based Signatures)	*Digital Signatures*	XMSS, $XMSS^{MT}$ LMS, HSS	Any NIST (Draft) Standards	Any classical PKC
Asymmetric (Scenario 1 without Stateful Hash-based Signatures)	*Digital Signatures*	Any NIST (Draft) Standards	-	Any classical PKC
Asymmetric (Scenario 2)	*Digital Signatures*	Any NIST (Draft) Standards	XMSS, $XMSS^{MT}$ LMS, HSS	Any classical PKC

Post-Quantum Cryptography

NIST-Selected PQC Algorithms

Key Encapsulation Mechanisms
(KEMs)

ML-KEM
(CRYSTALS-Kyber)
— lattice-based
(FIPS 203)

HQC
(backup KEM)
— code-based

Digital Signature Algorithms
(DSAs)

ML-DSA
(CRYSTALS-Dilithium)
— lattice-based
(FIPS 204)

FALCON
(FIPS upcoming)
— lattice-based/NTRU-like

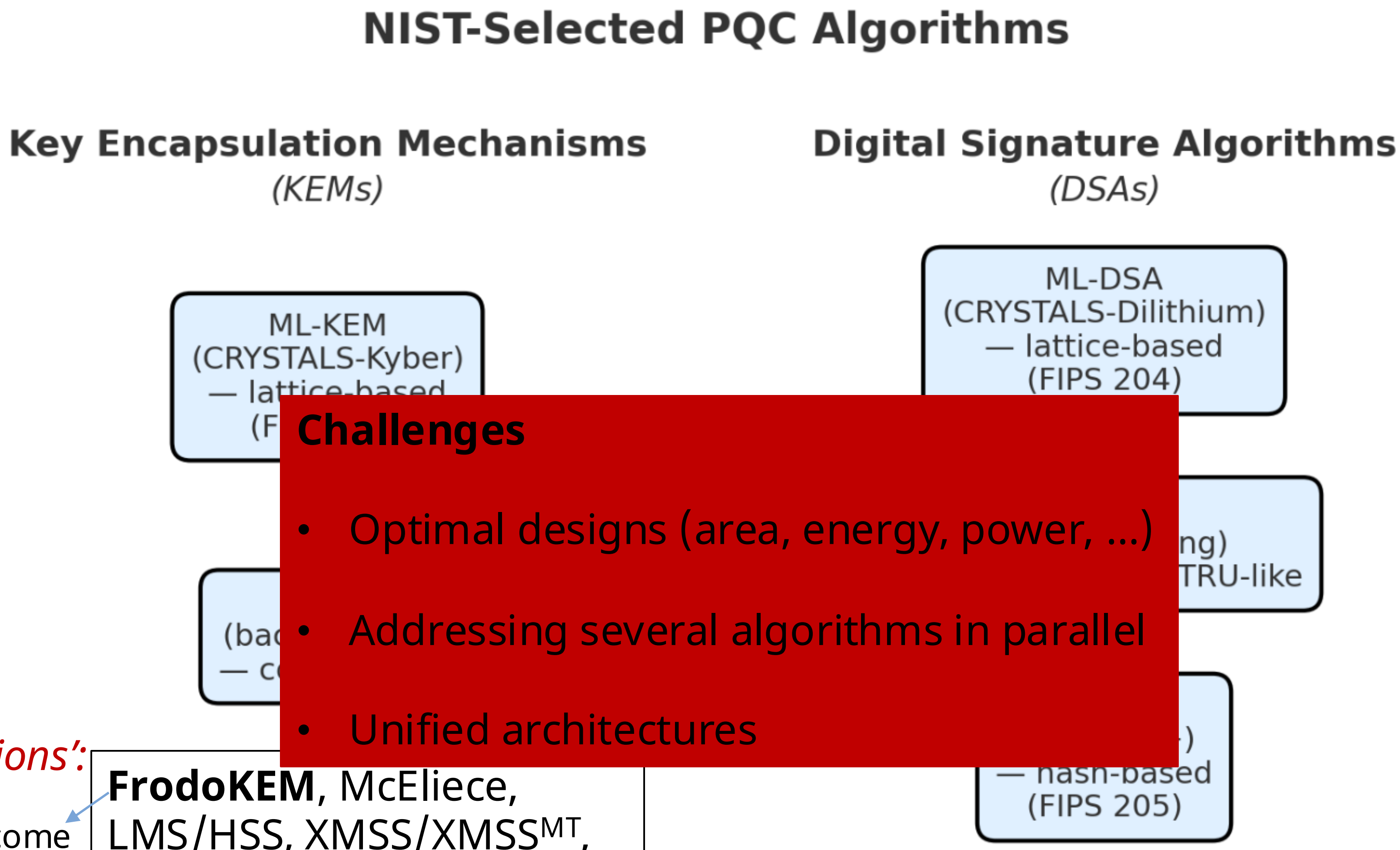
SLH-DSA
(SPHINCS+)
— hash-based
(FIPS 205)

Other ‘Recommendations’:

FrodoKEM, McEliece, LMS/HSS, XMSS/XMSS^{MT}, etc.

On track to become an ISO standard

Post-Quantum Cryptography



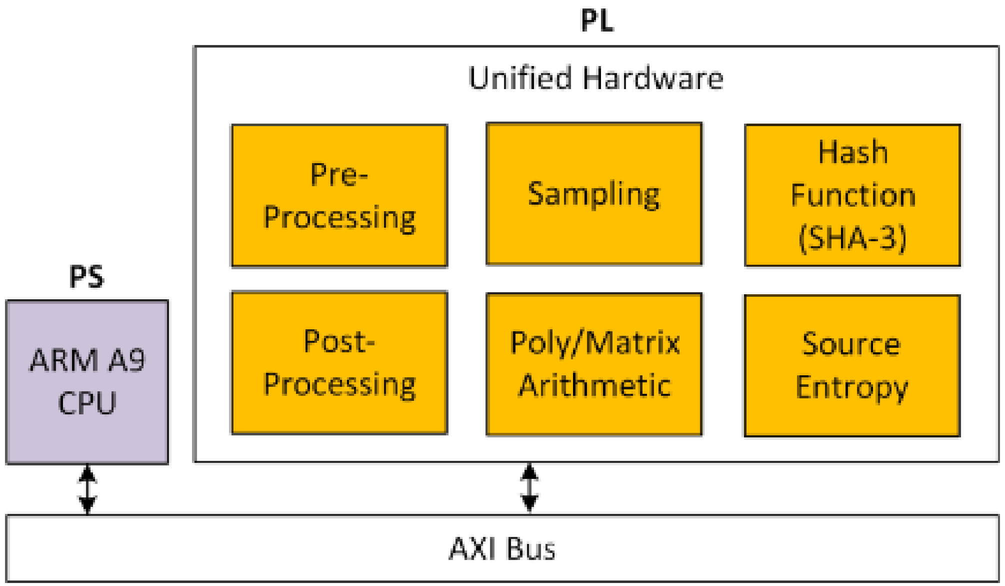
Challenges

- Optimal designs (area, energy, power, …)
- Addressing several algorithms in parallel
- Unified architectures

Other 'Recommendations': **FrodoKEM**, McEliece, LMS/HSS, XMSS/XMSS^{MT}, etc.

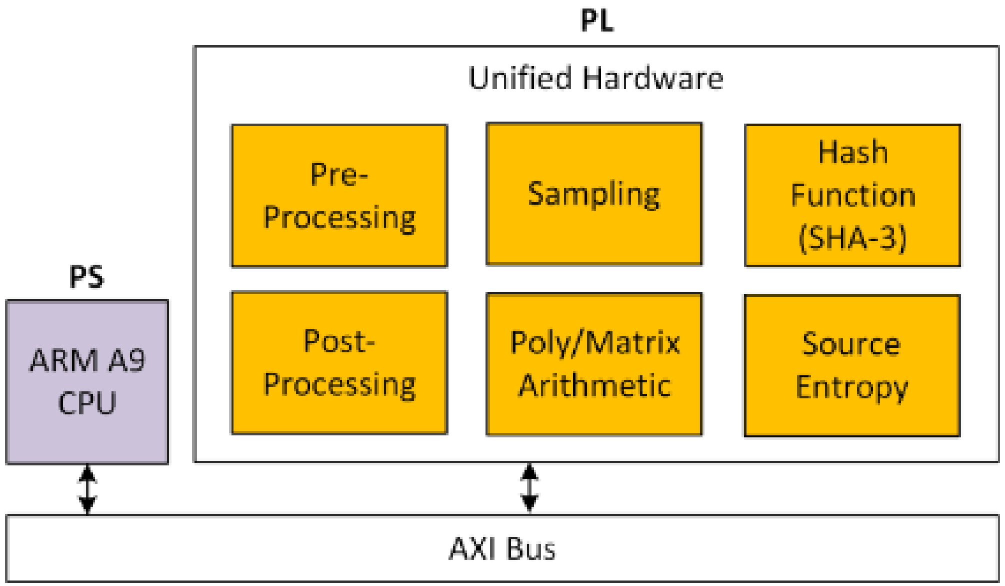
On track to become an ISO standard

Post-Quantum Cryptography
Bottlenecks



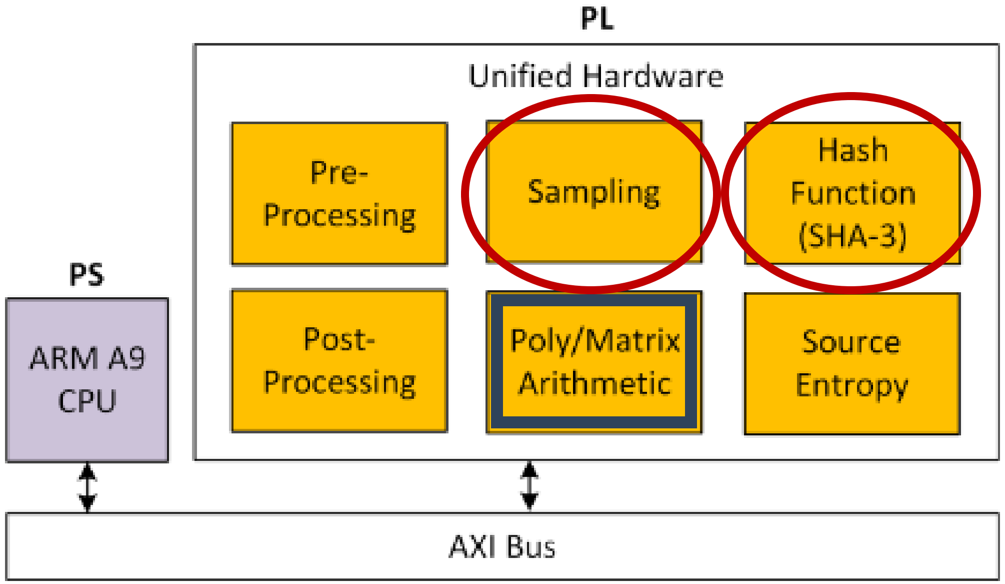
[*] Figure credit (next ten slides): Joint Project NSF (Award No. 2350142) - DFG (Project No. 543352068) with Dr. A. Aysu (NCSU, US)

Post-Quantum Cryptography
Bottlenecks



	Kyber KEM		FrodoKEM	
	Encaps	Decaps	Encaps	Decaps
Pre-processing	51.310	152.673	310.602	711
Post-processing	142.819	160.227	268.571	602.954
Matrix/Poly. Arith.	2.850.446	3.821.137	270.613.307	270.832.087
Sampling	497.525	496.469	436.428	458.370
Hashing	1.136.218	590.496	4.381.389	3.287.054
Misc.	112.409	18.397	90.791	197.224
Total	4.790.727	5.239.401	276.101.088	275.378.400

Post-Quantum Cryptography
Bottlenecks



	Kyber KEM		FrodoKEM	
	Encaps	Decaps	Encaps	Decaps
Pre-processing	51.310	152.673	310.602	711
Post-processing	142.819	160.227	268.571	602.954
Matrix/Poly. Arith.	2.850.446	3.821.137	270.613.307	270.832.087
Sampling	497.525	496.469	436.428	458.370
Hashing	1.136.218	590.496	4.381.389	3.287.054
Misc.	112.409	18.397	90.791	197.224
Total	4.790.727	5.239.401	276.101.088	275.378.400

AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation
  - To be presented at **2025 IFIP/IEEE 33rd International Conference on Very Large Scale Integration (VLSI-SoC)**

The Challenge: Post-Quantum Crypto Hardware

FALCON Signature Scheme

A lattice-based digital signature scheme designed to resist quantum computer attacks.

SamplerZ Bottleneck

This subroutine consumes over **65%** of signature generation cycles.

Complex Implementation

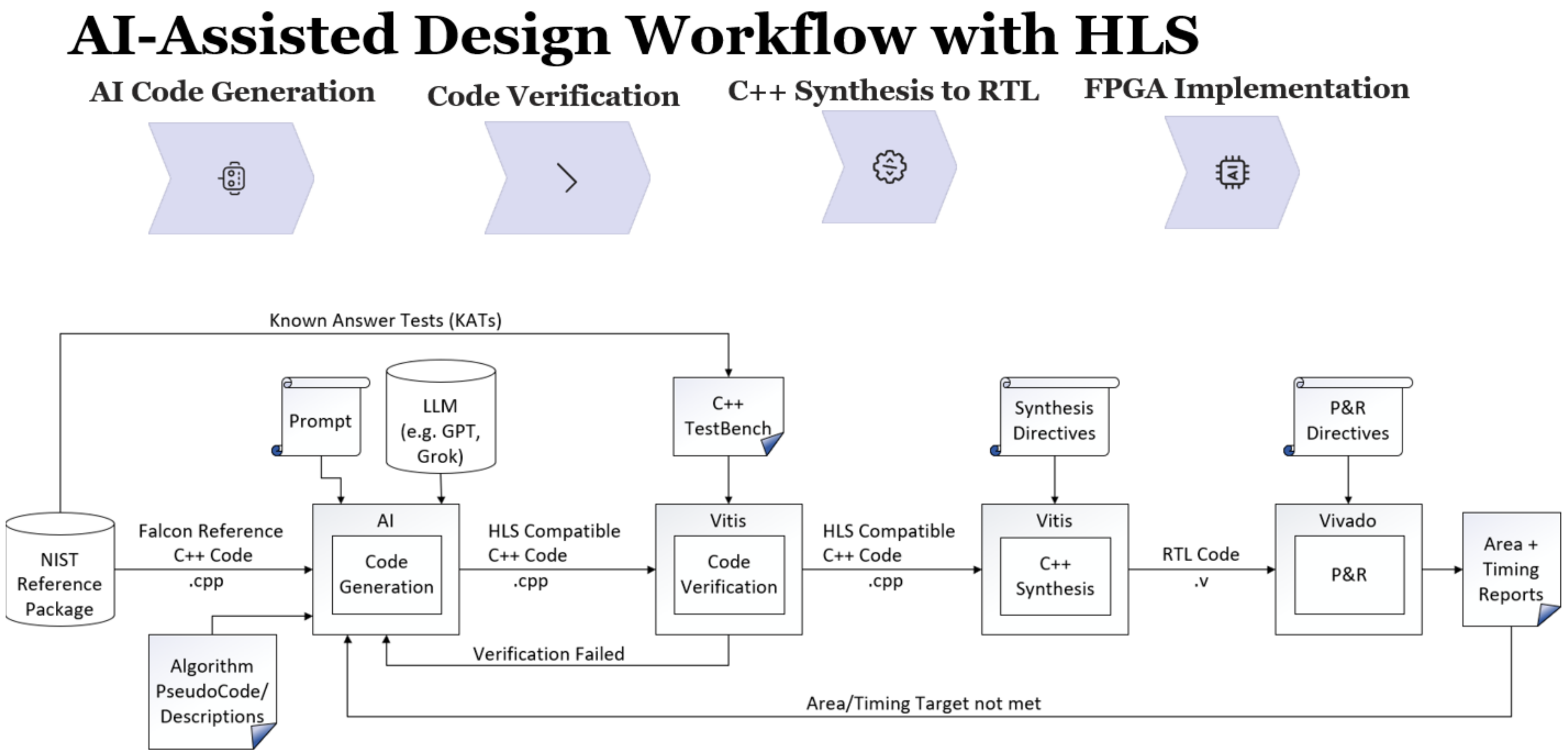
Involves discrete Gaussian sampling with intricate control flow and complex arithmetic.

No Available RTL Code

Allows testing the true creative capability of LLMs

AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation



AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation

The Prompt

```
Goal: Generate HLS-compatible C++ code for four
functions ApproxExp, BerExp, BaseSampler,
SamplerZ optimized equally for latency and
area-delay product.

Return: For each function, provide .cpp and .h
files using exact prototypes:
• uint64_t ApproxExp(double x, double ccs);
• int BerExp(uint8_t random_byte, double x,
  double ccs);
• int BaseSampler(ap_uint<72> random_bits);
• int SamplerZ(double mu, double sigma_prime,
  fpr sigma_min, ap_uint<72> BaseSampler_rand,
  uint8_t b_rand, uint8_t BerExp_rand);
```

```
Requirements:
• Distribute the random 88 bits in SamplerZ:
  First 9 bytes for BaseSampler, next byte for
  variable b in SamplerZ, and the last byte for
  BerExp using little-endian format.
• Make sure to use the exact function prototypes
  as listed above.
• Make sure to use MAXIMUM precision for all
  calculations to get the correct functionality
• Make sure that each function can be called
  correctly by the function in the level above
  it in the hierarchy.
• Make sure that all functions are HLS compatible
  with Vitis.

Context:
• I will attach the following  files for Context
 SamplerZ.c (source code) and images of all of
 the algorithms broken into steps for easier
 optimization of each step.
• I will also include a file that defines the
 function headers that should be implemented.
```

AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation

Key AI Optimization

Algorithm 13 ApproxExp(x, ccs)

Require: Floating-point values $x \in [0, \ln(2)]$ and $ccs \in [0, 1]$

Ensure: An integral approximation of $2^{63} \cdot ccs \cdot \exp(-x)$

Implementing e^x directly with Xilinx IPs is more efficient than computing approximation

1: C = `[0x00000004741183A3,0x00000036548CFC06,0x0000024FDCBF140A,0x0000171D939DE045, 0x0000D00CF58F6F84, 0x000680681CF796E3, 0x002D82D8305B0FEA, 0x011111110E066FD0, 0x0555555555070F00, 0x155555555581FF00, 0x400000000002B400, 0x7FFFFFFFFFFF4800, 0x8000000000000000]`

2: $y \leftarrow C[0]$ ▷ y and z remain in $\{0, ..., 2^{63} - 1\}$ the whole algorithm.

3: $z \leftarrow \lfloor 2^{63} \cdot x \rfloor$

4: for $1 = 1, \ldots, 12$ do

5: $\quad y \leftarrow C[u] - (z \cdot y) >> 63$ ▷ $(z \cdot y)$ fits in 126 bits, but we only need the top 63 bits

6: $z \leftarrow \lfloor 2^{63} \cdot ccs \rfloor$

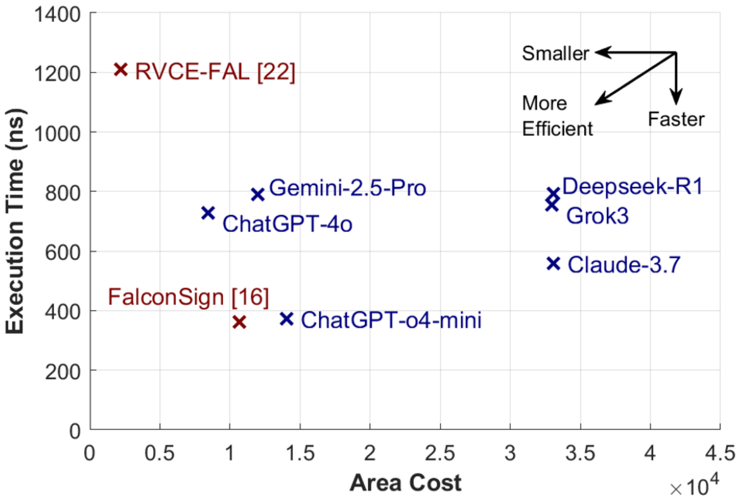
7: $y \leftarrow (z \cdot y) >> 63$

8: return y

AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation

BLUF: AI is Surprisingly Good



SAMPLERZ: HLS SYNTHESIS RESULTS ACROSS LLM MODELS

Metric/Model	ChatGPT-4o	ChatGPT-o4-mini	Claude3.7	Deepseek-R1	Gemini-2.5-Pro	Grok3	[16][1]	[22]
LUTs	7299	7683	11438	14995	7524	14646	9368	4761
FFs	10096	8266	12538	17529	7959	17411	4527	692
DSPs	52	108	273	265	82	265	76	9
BRAMs	0	0	6	0	6	0	0	0
Area Cost[2]	**8412**	14013	33079	33076	11970	32974	10690	**2198**
Target Freq (MHz)	200	200	200	200	200	200	-	-
Max Freq (MHz)	231	**297**	243	222	185	233	**185**	86
Latency (Cycles)	168	111	136	176	146	176	67	104
Execution Time (ns)	727	**374**	560	793	789	775	**362**	1209
ADP ($\times 10^6$)	6.12	**5.24**	18.51	26.22	9.45	24.91	4.63	**2.66**
Design Iterations[3]	20	5	3	2	13	6	-	-

[1]: The utilization of the ChaCha20 PRNG block from [16] has been subtracted to enable a direct comparison.[2]: The Area Cost calculation is defined as Area Cost $=$ (LUTs $\div$ 4) $+$ (FFs $\div$ 8) $+$ (DSPs $\times$ 102.4) $+$ (BRAMs $\times$ 116.2), which is based on [35], [36], which provides the conversion of 1 LUT/FF/DSP/BRAM to an equivalent number of slices. [3]: Each iteration is equivalent to approximately 4 hours of design time.

[16] Y. Ouyang, Y. Zhu, W. Zhu, B. Yang, Z. Zhang, H. Wang, Q. Tao, M. Zhu, S. Wei, and L. Liu, "FalconSign: An Efficient and High-Throughput Hardware Architecture for Falcon Signature Generation," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2025, no. 1, p. 203–226, Dec. 2024.
[22] X. Yu, Y. Sun, Y. Zhao, H. Kuang, and J. Han, "RVCE-FAL: A RISC-V Scalar-Vector Custom Extension for Faster FALCON Digital Signature," in 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE), Mar. 2024, pp. 1–6, iSSN: 1558-1101.

AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation

Novel AI-Discovered Optimizations

Floating-Point Replacement
ChatGPT-04-mini replaced complex integer-based exponentiation with standard exp() function.

Simplified Dataflow
Eliminated operations in the critical datapath while preserving functional correctness.

Leveraged Optimized IP
Used Xilinx's optimized floating-point IP to reduce area utilization.

Constant-Time Behavior
Maintained security guarantees with fixed-latency hardware implementation.

Challenges in AI-Assisted Design

Precision Issues
LLMs default to single-precision vs. required double-precision

Arithmetic Inconsistency
Mixing floating-point and fixed-point representations

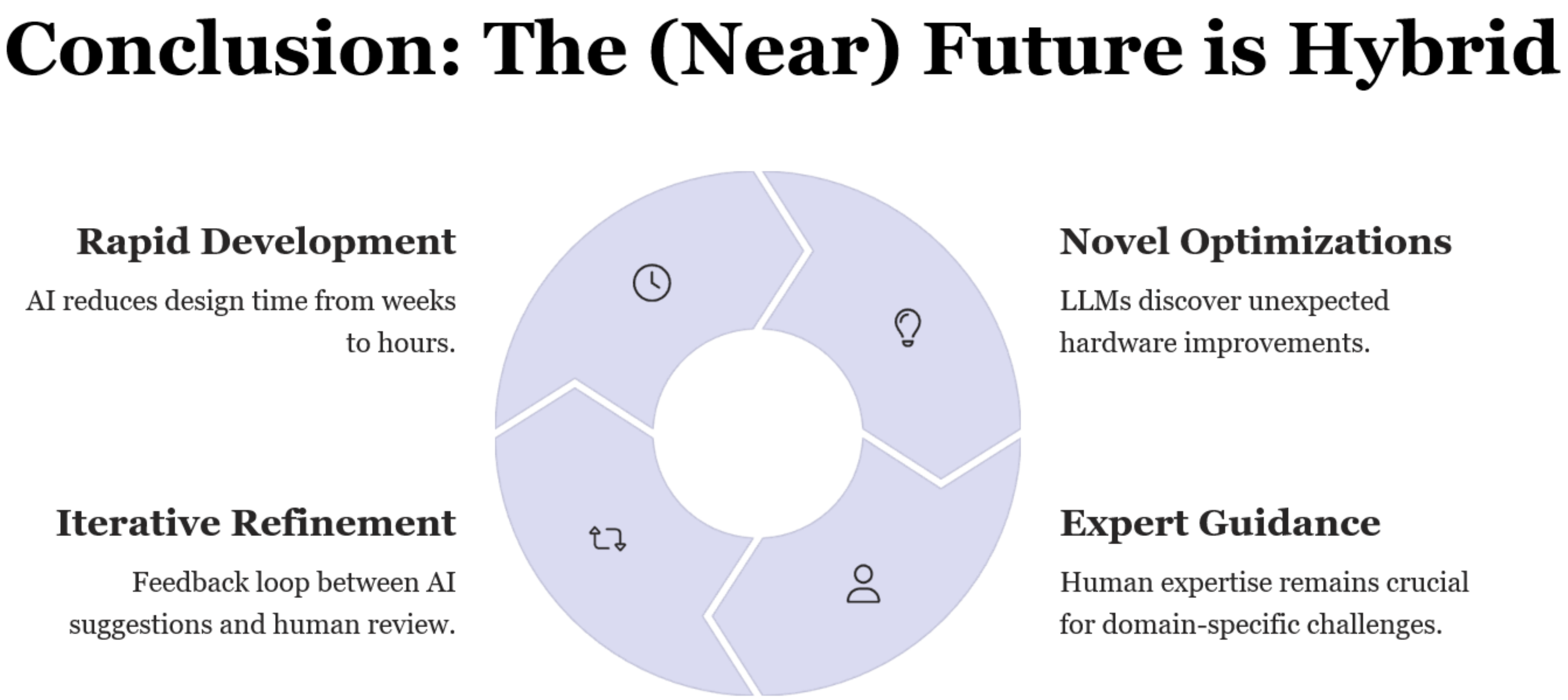
Interface Mismatches
Incorrect function signatures causing synthesis failures

Testbench Overfitting
Limited test vectors leading to over-optimized designs

Mathematical Errors
Misinterpreting complex expressions affecting algorithm correctness

AI for Optimizing PQC?

- Deus Ex LLMs: AI vs Humans in Post-Quantum Cryptographic Hardware Code Generation



Rolling Back To Crypto Agility: PQC View

- Future/Quantum-Proofing cryptographic implementations to allow for easy updates to new standards
  - NIST PQC Standards!

- Revisit **implementation steps** [*]
  - **Three main steps:** Discover, Manage, Remediate

[*] https://www.ibm.com/quantum/blog/crypto-agility

Rolling Back To Crypto Agility: PQC View

- Implementation Step 1: **Discover**
  - Create a cryptographic inventory to identify all cryptographic implementations within an organization
  - Requires automated scanning tools as manual methods are prone to errors
- Implementation Step 2: **Manage**
  - Define a crypto policy
  - Prioritize which systems to update first based on sensitivity
  - Track progress (likely multi-year project)
- Implementation Step 3: **Remediate**
  - Migrate from classical to quantum-safe cryptography
  - A crypto proxy can be used as a temporary solution to provide immediate protection during the migration phase
    - Converting PQC algorithms from the user's end to classical algorithms for legacy backend applications
  - Performance testing of these new algorithms is also crucial

Rolling Back To Crypto Agility: PQC View

- Hybrid Key Establishment Schemes

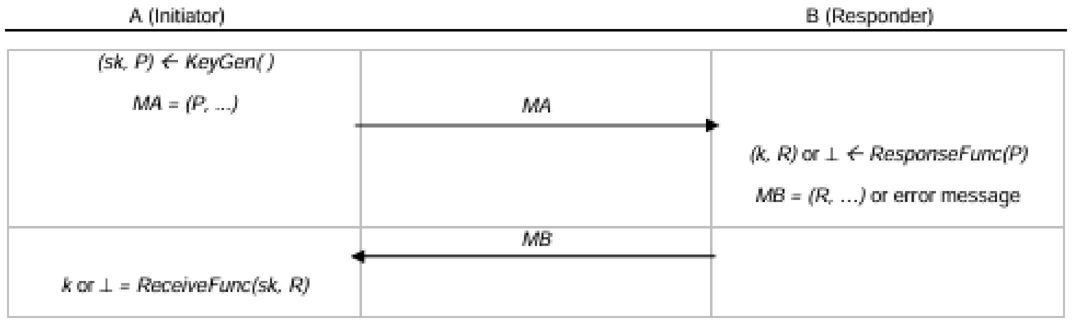


Figure 3: Key establishment abstraction

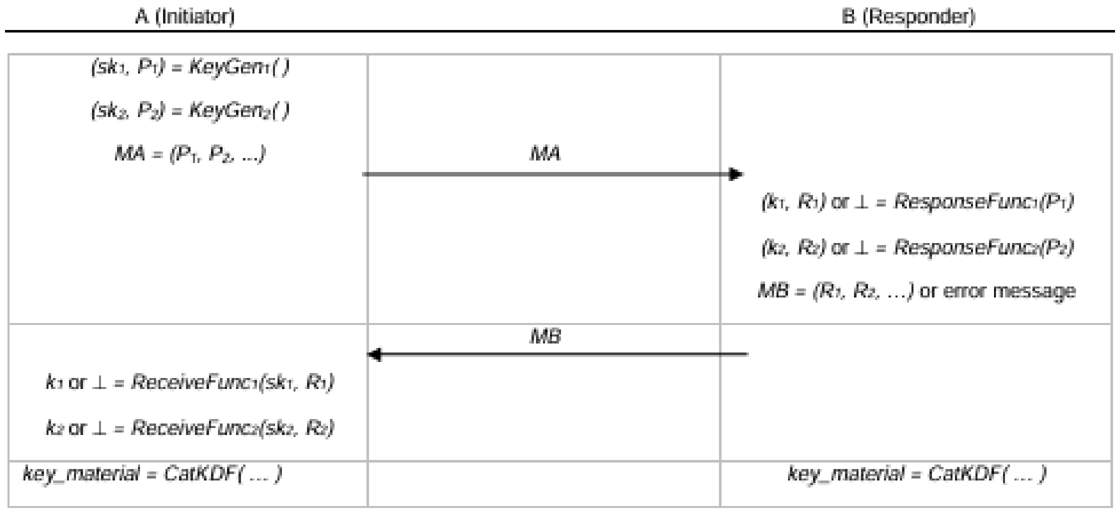


Figure 4: Concatenate hybrid key establishment - ephemeral

[Figures] https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf

Lessons Learned: Best Practices

- All business applications involving any sort of cryptographic technology should incorporate the latest algorithms and techniques
- Crypto agility requirements must be disseminated to all hardware, software, and service suppliers, who must comply on a timely basis
  - Suppliers who cannot address these requirements must be replaced
- Suppliers must provide timely updates and identify the crypto technology they employ
- Quantum-resistant solutions (PQC) should be kept in mind [*]

[*] Chen, Lily; Jordan, Stephen; Liu, Yi-Kai; Moody, Dustin; Peralta, Rene; Perlner, Ray; Smith-Tone, Daniel. "Report on Post-Quantum Cryptography (NISTIR 8105)". National Institute of Standards and Technology (NIST)

Lessons Learned: Best Practices

- Symmetric-key algorithms should be flexible in their key lengths
- Hash algorithms should support different lengths of outputs
- Digital certificate and private key rotations must be automated [*]
- Standards and regulations must be complied with [**]
- Used algorithms should be communicated; not assumed or defaulted

[*] “Digital certificate and private key rotations must be automated”. www.appviewx.com
[**] Macaulay, Tyson. “Cryptographic Agility in Practice”. InfoSec Global.

Thanks for listening!

Any questions?

(elif.kavun@barkhauseninstitut.org)