IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

CAS

Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography

Prasanna Ravi[1,2], Sundar Vijaya Kumar[2], Anupam Chattopadhyay[1,2], Shivam Bhasin[1], Arvind Easwaran[2]

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

[1] Temasek Labs, NTU Singpapore
[2] School of Computer Science and Engineering, NTU Singapore

Outline

- **Automotive Security**
- Description of LASAN
- Post-Quantum Cryptography
- Implementation Details
- Experimental Results
- Conclusion

Automotive Security

- Modern cars are connected to myriad external networks (V2X)
  - Increasing number of *attack surfaces*
  - *Snooping, Sensor Spoof, Wireless Attack*
- Complex intra-vehicular, heterogeneous system with multiple sub-systems from different vendors
  - Presence of Adversarial computation nodes
  - *Malicious Trojans, Information leakage, Hybrid attacks*
- With increasing autonomy, the importance of in-car data accumulation and processing will grow Automotive Security Market to touch **$5.77 Billion by 2025**
  - Multiple tech startups across the world
  - Regional/National efforts in standardization
- First step towards ensuring security in an in-vehicular network through deployment of robust security protocols to prevent adversarial/malicious nodes within the perimeter of the network.
- In other words, we need to have a reliable way to ensure that the automobile is operating with legitimate Electronic Control Units (ECU).

Dedicated Security Protocols for In-Vehicular Networks

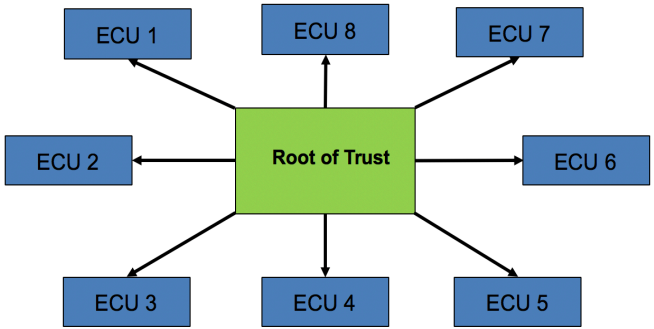
- Indeed, there are several dedicated in-vehicular authentication protocols such as **Libra-CAN**[1], **CANAuth**[2] and **TESLA**[3], but they assume use of **pre-shared keys** (**PSK**) which relies on presence of trusted parties in the network.
- PSK scenarios possess expoitable weaknesses especially in presence of static keys and when shared with multiple parties.
- There also exist sophisticated and malleable authentication protocols such as the **TLS** and **Kerberos** which utilize public-key cryptographic schemes, but are designed for complex and dynamic networks such as the **Internet**.
- But, nature of intra-vehicular network **fundamentally different** from networks such as the internet.
  - ***Hard Real-time*** *constraints*
  - ***Low power/bandwidth*** *constraints*
  - *Automotive networks are* ***static*** *– remain fixed over the lifetime of the vehicle*
  - ***Fixed Set*** *of* ***transmitter*** *and* ***receiver*** *nodes*
  - *Messages in automotive networks are typically* ***multicast/broadcast***

Outline

- Automotive Security
- **Description of LASAN**
- Post-Quantum Cryptography
- Implementation Details
- Experimental Results
- Conclusion

LASAN: An Initial Prototype

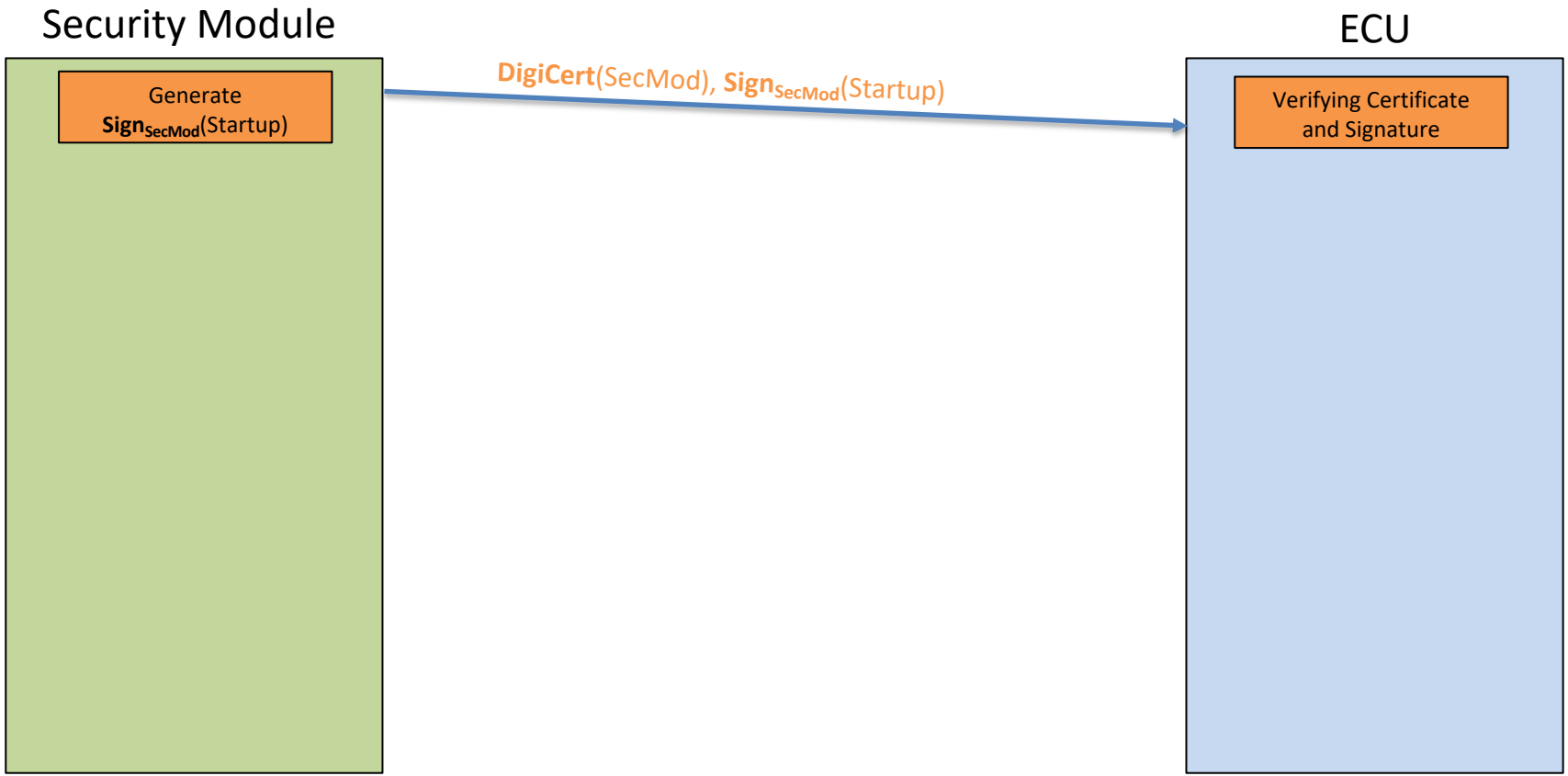
- Lightweight Authentication for Secure Automotive Networks (**LASAN**) proposed by Mundhenk et al.[4] is an **authentication** and **authorization** framework for secure transmission of real-time messages.
  - Formally proven to be secure
  - Compatible with the typical automotive processes performed in the automotive lifecycle
- Secure against **Dolev-Yao** adversary model
  - **Interception**, **Modification**, **Replay**, **Block**, **Injection** of new messages
- Operates with a **Root-of-Trust** node in the network which is responsible for authentication and authorization of ECUs
- Security handshakes for individual ECUs are done with the **root-of-trust.**
  - Key to Lightweight nature of LASAN
  - Removes costly many-to-many authentication routines



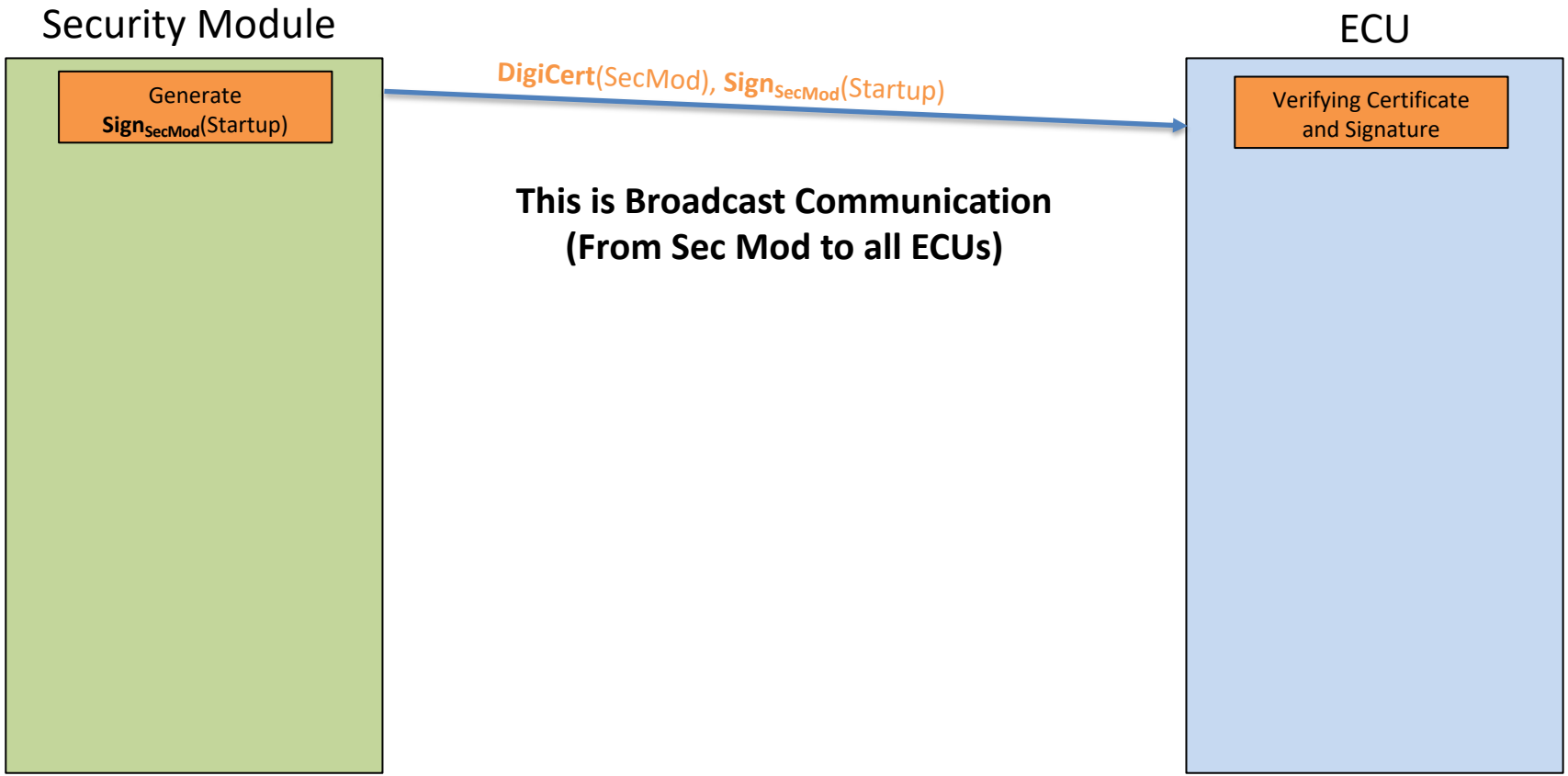
Cryptographic Primitives

- LASAN protocol consists of **two** phases:
  - **ECU Authentication:** Secure Authentication of all nodes on the network.
  - **ECU Authorization:** Authorization of ECUs for secure communication.
- **Public-key** cryptographic primitives include **digital signatures** (authentication) and **key-exchange schemes** (secure key sharing).
- **Private-key** cryptographic primitives include **Block-ciphers** (confidentiality) and **Message Authentication Codes** (integrity) or **Authenticated Encryption** (confidentiality with message integrity) schemes.
- The **ECU Authentication** phase remains the main focus of our work since it utilizes public-key cryptographic schemes.

Phase I: ECU Authentication



Phase I: ECU Authentication

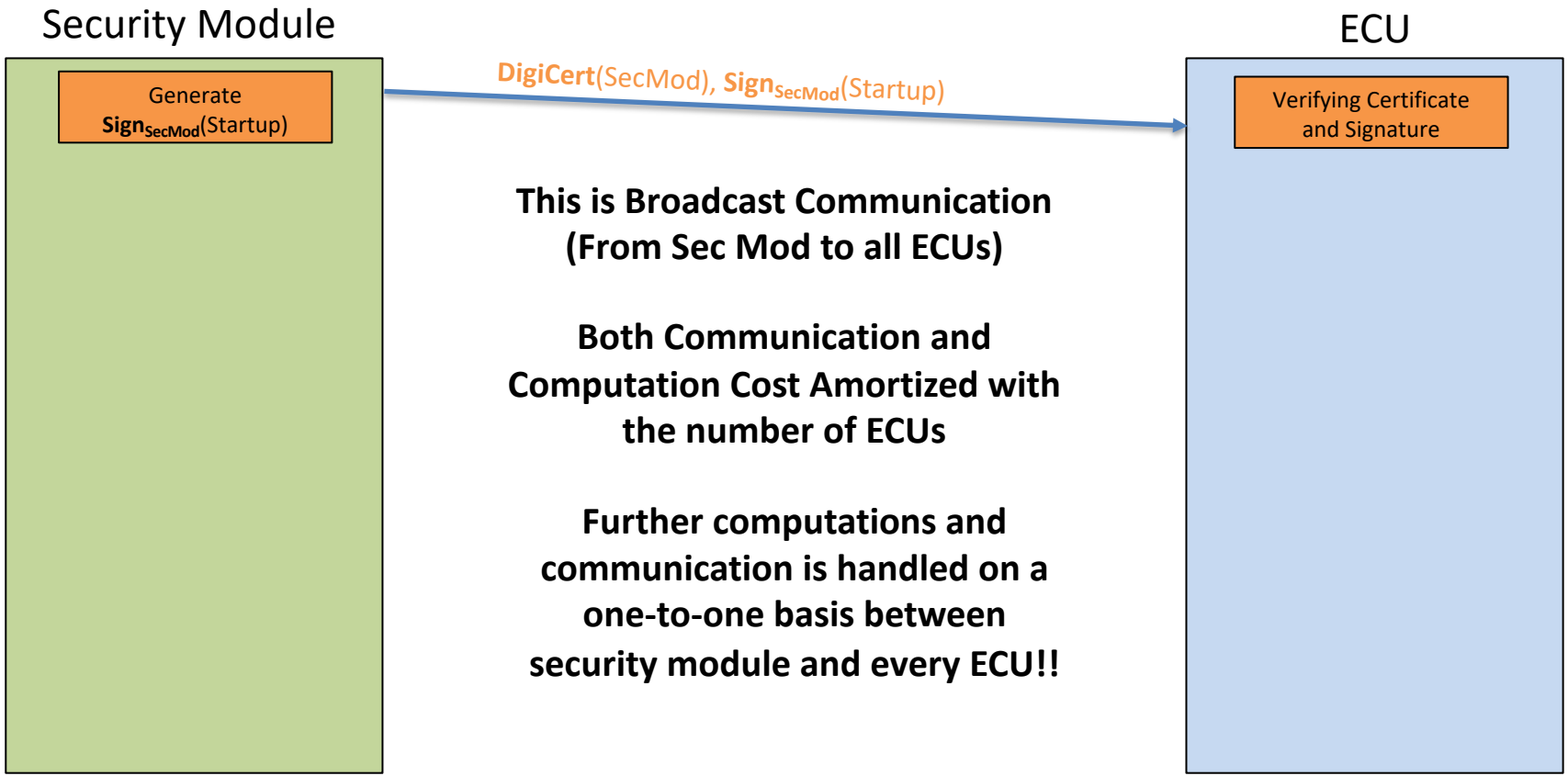


Phase I: ECU Authentication

This is Broadcast Communication (From Sec Mod to all ECUs)

Both Communication and Computation Cost Amortized with the number of ECUs

Phase I: ECU Authentication

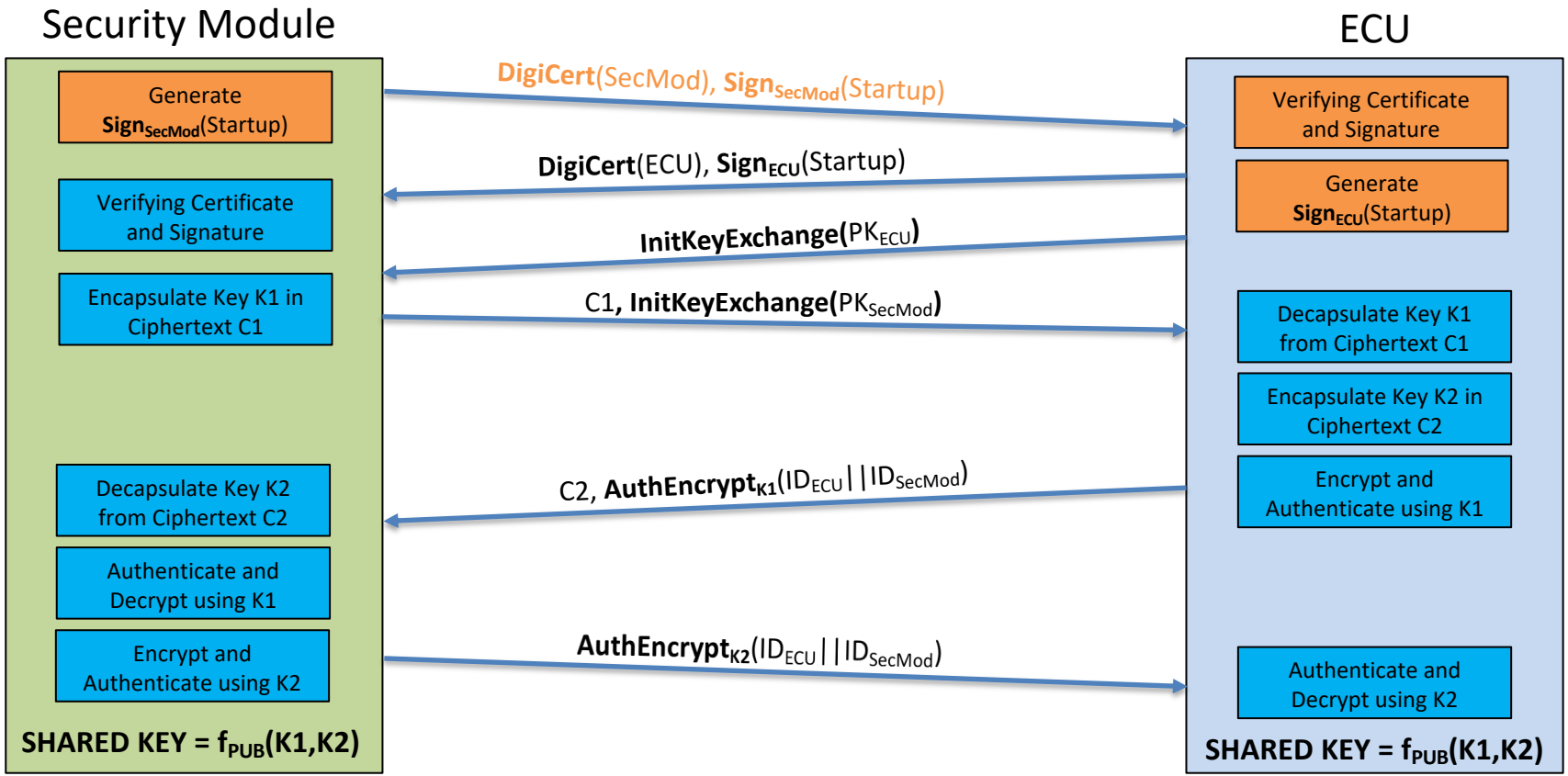


This is Broadcast Communication (From Sec Mod to all ECUs)

Both Communication and Computation Cost Amortized with the number of ECUs

Further computations and communication is handled on a one-to-one basis between security module and every ECU!!

Phase I: ECU Authentication

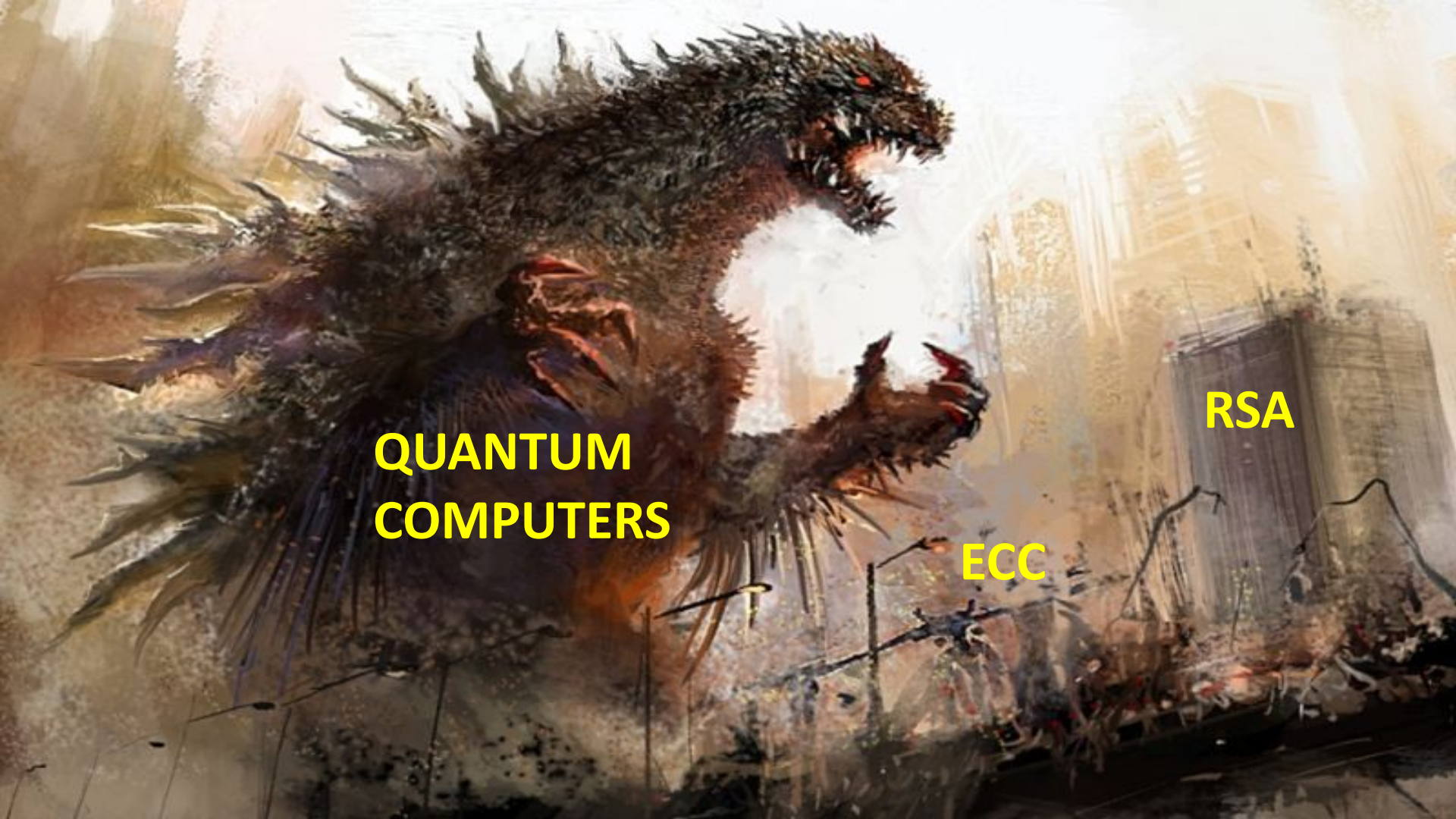


Cryptographic Primitives

- LASAN is a **protocol specification** and hence any type of public key and private key cryptographic schemes can be used within this framework.
- Typically, traditional public key cryptographic schemes based on RSA (Rivest-Shamir-Adi) and ECC (Elliptic Curve Cryptography) have been widely used for all types of implementations.
- However, in this work we implement LASAN on a practical automotive testbed using **post-quantum cryptographic schemes**.

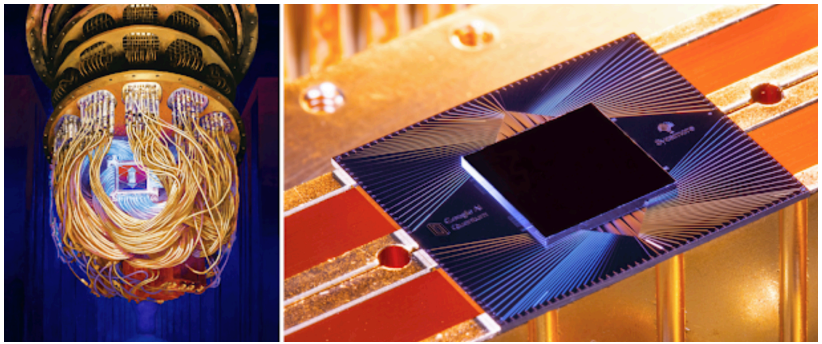
Outline

- Automotive Security
- Description of LASAN
- **Post-Quantum Cryptography**
- Implementation Details
- Experimental Results
- Conclusion


QUANTUM
COMPUTERS
RSA
ECC

Security in Quantum Era

- Huge money in quantum computing is being invested by computer industry giants like **Google**, **IBM**, **Intel** and other companies like **D-Wave**, **IonQ**.
- A large scale quantum computer has the potential to **break all of public key cryptography** (**RSA** and **ECC**) that we use today.
- This has prompted the cryptographic community to develop **quantum resistant** alternatives for public-key cryptography.



- **NIST** process for **standardization** of Post-Quantum cryptography is underway!!!
- Started in **November 2017** and could take about **4-5 years** to have the first draft standards.
- Symmetric cryptographic schemes are also affected by attack from quantum computers, but merely doubling the key-length would ensure protection in the post-quantum era (AES-128 to AES-256)

NIST Standardization Process

- NIST has previously conducted standardization competitions for **Advanced Encryption Standard** (AES) and **Secure Hashing Algorithm** (SHA).
- Want to break the **mono-culture** enforced by use of number theoretic based RSA and ECC-based cryptographic algorithms and not put all the eggs in the same basket!!
- First Round received **69 submissions** based on hard problems from varying fields of mathematics like algebraic geometry, coding theory, multivariate quadratic equations and elliptic-curve isogenies[5].

First Round:

Type	Signatures	KEM/Encryption	Overall
Lattice-based	5	23	28
Code-based	3	17	20
Multivariate	8	2	10
Hash-based	3	0	3
Isogeny-based	0	1	1
Others	2	5	7
Total	21	48	69

NIST Standardization Process

- NIST has previously conducted standardization competitions for **Advanced Encryption Standard** (AES) and **Secure Hashing Algorithm** (SHA).
- Want to break the **mono-culture** enforced by use of number theoretic based RSA and ECC-based cryptographic algorithms and not put all the eggs in the same basket!!
- First Round received **69 submissions** based on hard problems from varying fields of mathematics like algebraic geometry, coding theory, multivariate quadratic equations and elliptic-curve isogenies[5].

Second Round:

Type	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based	0	7	7
Multivariate	4	0	4
Hash-based	2	-	2
Isogeny-based	0	1	1
Others	0	0	0
Total	9	17	26

NIST Standardization Process

- NIST has previously conducted standardization competitions for **Advanced Encryption Standard** (AES) and **Secure Hashing Algorithm** (SHA).
- Want to break the **mono-culture** enforced by use of number theoretic based RSA and ECC-based cryptographic algorithms and not put all the eggs in the same basket!!
- First Round received **69 submissions** based on hard problems from varying fields of mathematics like algebraic geometry, coding theory, multivariate quadratic equations and elliptic-curve isogenies[5].

Third Round:

Type	Signatures	KEM/Encryption	Overall
Lattice-based	2	5	7
Code-based	0	3	3
Multivariate	2	0	2
Hash-based	2	0	2
Isogeny-based	0	1	1
Others	0	0	0
Total	6	9	15

NIST Standardization Process

- NIST has previously conducted standardization competitions for **Advanced Encryption Standard** (AES) and **Secure Hashing Algorithm** (SHA).
- Want to break the **mono-culture** enforced by use of number theoretic based RSA and ECC-based cryptographic algorithms and not put all the eggs in the same basket!!
- First Round received **69 submissions** based on hard problems from varying fields of mathematics like algebraic geometry, coding theory, multivariate quadratic equations and elliptic-curve isogenies[5].
- **Our main focus is to evaluate the performance of post-quantum cryptographic schemes compared to their pre-quantum counterparts.**

Third Round:

Type	Signatures	KEM/Encryption	Overall
Lattice-based	2	5	7
Code-based	0	3	3
Multivariate	2	0	2
Hash-based	2	0	2
Isogeny-based	0	1	1
Others	0	0	0
Total	6	9	15

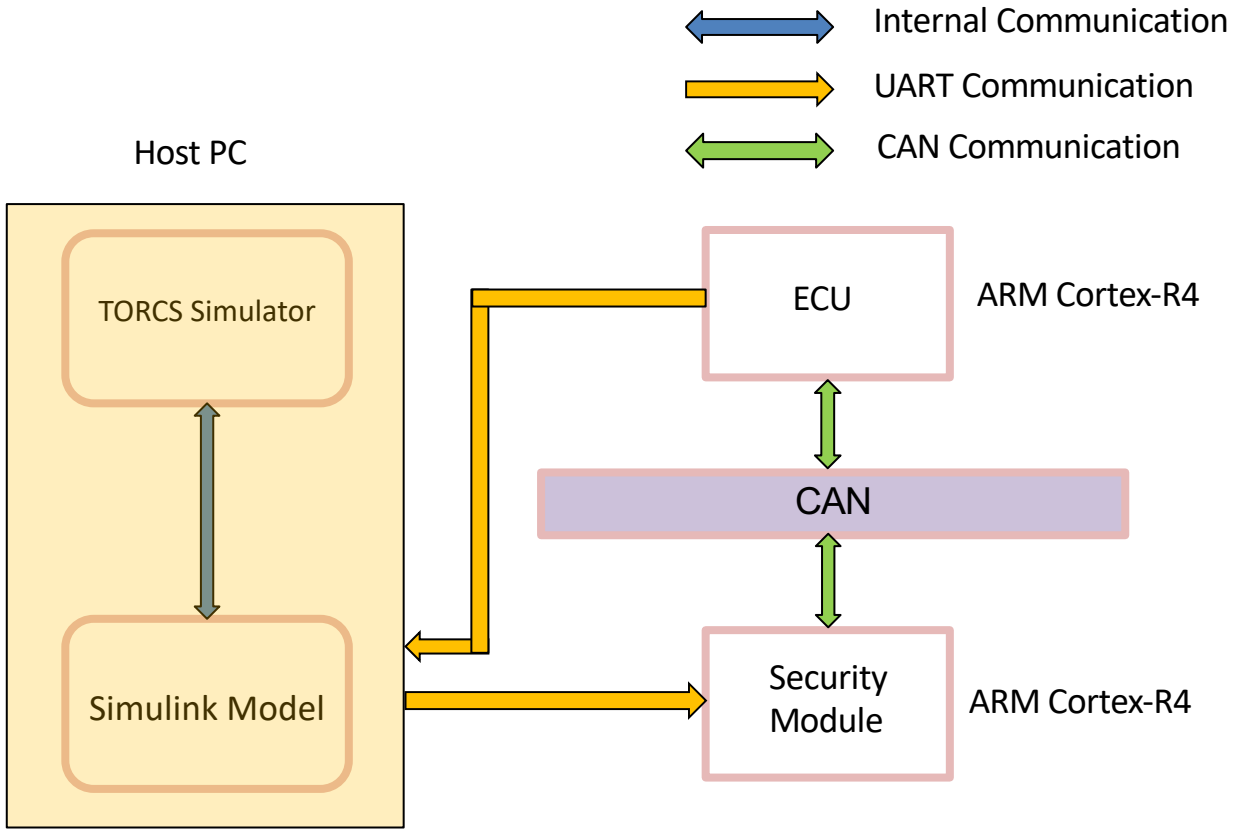
Lattice-Based Cryptography

- Schemes built upon hard problems over geometric structures called ”**lattices**” in n-dimensional space.
- **Average Case Hard Problems:** Learning With Errors (LWE), Short Integers Solution (SIS) problem
- **Good Efficiency Guarantees**: Computations over **polynomials in efficient polynomial rings**
- **Toolset**: Number Theoretic Transform (NTT), Toom-Cook and Karatsuba Multiplication
- Compared to other post-quantum schemes, lattice-based cryptographic schemes offer very good balance of security and efficiency guarantees (speed, efficiency and communication bandwidth).
- Thus, a combination of these attributes makes lattice-based cryptographic schemes very strong candidates in the ongoing NIST standardization process.
- In this work, we utilize two lattice-based schemes with the implementation of the LASAN protocol – (1) **Kyber KEM** [6] and (2) **Dilithium DS** [7], both of which are finalist candidates in the NIST post quantum standardization process.

Outline

- Background
- Post-Quantum Cryptography
- Description of LASAN
- **Implementation Details**
- Experimental Results
- Conclusion

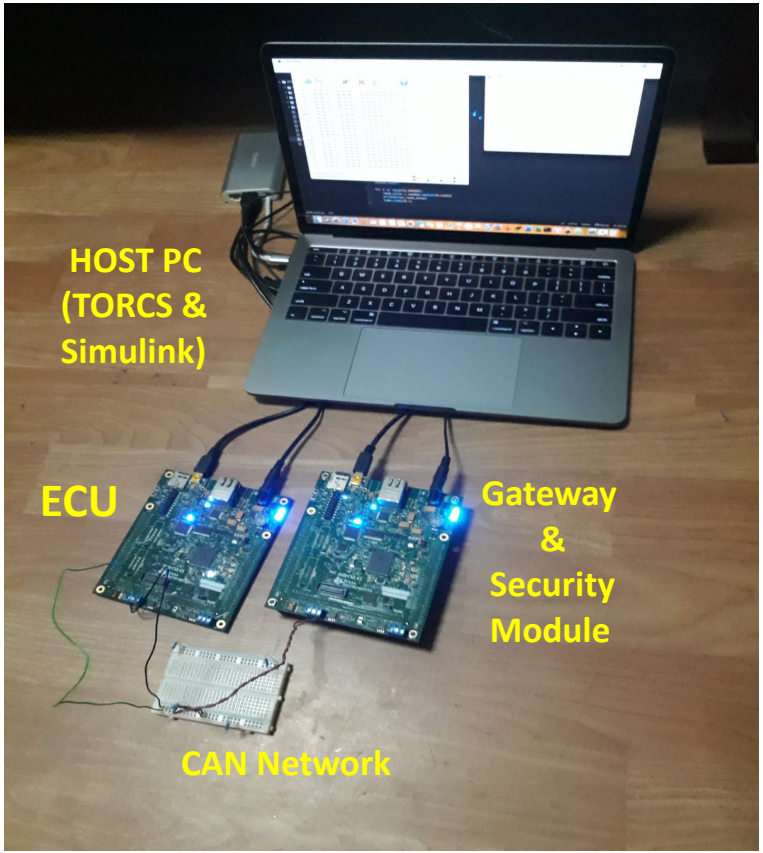
Hardware-in-the-Loop Testbed



Experimental Evaluation: ECU Authentication

- Automotive Setup based on the **TMS570LS3137**, 32-bit RISC Flash, Automotive Grade Safety-Critical micro-controllers based on the ARM Cortex-R4 CPU.
- Communication using Industry grade **CAN** bus operating at **500 Kbps**.
- Operating Frequency: **160 MHz**.
- Both devices run **FreeRTOS**, a real-time operating system and tasks scheduled using task fixed priority scheduler.
- Three real time tasks are executed during the authentication phase:
  - Send_CAN_Task – Sending CAN messages
  - Receive_CAN_Task – Receiving CAN messages
  - Crypto_Task – Compute cryptographic operations
- Synchronization between the communicating ECUs is achieved by ensuring that communication happens in a ping-pong manner.
- Both the devices are put in an active wait state to receive CAN data when there is nothing to compute or send, which we denote as the “rest” state.
- When reception of data is complete, subsequent computations are performed and computed data is immediately sent while the other ECU is already waiting for data over the CAN bus.

Automotive Testbed Architecture



Experimental Evaluation: ECU Authentication

- Instantiated LASAN with **two** crypto suites:
  - **Pre-Quantum Cipher Suite**: *LASAN_M_ECDHE_ECDSA_WITH_AES_256_GCM_8*
    - Ephemeral Elliptic Curve Diffie Hellman (**ECDHE**) for **key-exchange**
    - Elliptic Curve Digital Signature Algorithm (**ECDSA**) for **digital signatures**
    - AES-256 in GCM mode for **Authenticated Encryption cipher**
    - Implementations taken from the **CIFRA** library[8].
  - **Post-Quantum Cipher Suite**: *LASAN_M_KYBER_DILITHIUM_WITH_AES_256_GCM_8*
    - Lattice-based **Kyber** for **key-exchange**
    - Lattice-based **Dilithium** for **digital signatures**
    - Both lattice schemes are finalist candidates in the NIST standardization process
    - AES-256 in GCM mode for **Authenticated Encryption cipher**
    - Implementations taken from the **pqm4** library[9].

Experimental Evaluation: ECU Authentication

Comparison of Communication Bandwidth:

Scheme	Pre-Quantum schemes		
	Classical Security (bits)	Public key (bytes)	Ciphertext/Signature (bytes)
ECDH (secp256r1)	128	32	NA
ECDSA (secp256r1)	128	32	64
Scheme	**Post-Quantum schemes**		
	Post-Quantum Security (bits)	Public key (bytes)	Ciphertext/Signature (bytes)
Kyber	161	1088	1152
Dilithium	128	1472	2701

Outline

- Background
- Post-Quantum Cryptography
- Description of LASAN
- Implementation Details
- **Experimental Results**
- Conclusion

Initial Benchmarks: ECU Authentication

State	Pre-Quantum (secs)		Post-Quantum (secs)	
	Amortized	Non-Amortized	Amortized	Non-Amortized
Communication	**0.011**	**0.021**	**0.4315**	**0.7165**
Computation	0.052	0.275	0.066	0.231
Rest	0.052	0.295	0.066	0.165

- Time taken for single handshake:
  - Pre-Quantum: 0.706 secs
  - Post-Quantum: 1.676 secs (**x 2.37**)
- Overhead ignoring Amortized Cost (assuming large number of ECUs): **(x 1.85)**
- Pre-Quantum: **492 B** (amortized: 179 B)
- Post-Quantum: **20.528 KB** (amortized: 7.98 KB)
- Though computation times are comparable, **communication bandwidth** is main **bottleneck** with respect to implementation of po**st-quantum lattice-based** cryptographic schemes.

Outline

- Background
- Post-Quantum Cryptography
- Description of LASAN
- Implementation Details
- Experimental Results
- **Conclusion**

Conclusion

- Practical Implementation of authentication protocol LASAN on automotive testbed based on ARM Cortex-R4 safety grade MCUs.
- Instantiated LASAN with two cryptographic suites – Pre-Quantum (using ECC based schemes) and Post-Quantum (using lattice-based schemes – Kyber and Dilithium).
- Performed Comparative Evaluation of speed of authentication phase of LASAN with pre-quantum and post-quantum cipher suite.
- Identified Communication Bandwidth as the main bottleneck hampering performance of post-quantum cryptographic primitives.
- Future work will involve benchmarking multiple post-quantum cryptographic primitives on the same platform and development of efficient and optimized ciphersuites for LASAN.
- We place all the software described in this paper into the public domain available at https: //github.com/PRASANNA-RAVI/Automotive-Test-Bed-PQC.

Thank You. Questions?

References

[1] B. Groza, S. Murvay, A. Van Herrewege, and I. Verbauwhede, “Libra- can: a lightweight broadcast authentication protocol for controller area networks,” in *International Conference on Cryptology and Network Security*. Springer, 2012, pp. 185–200.

[2] A. Van Herrewege, D. Singelee, and I. Verbauwhede, “Canauth-a simple, backward compatible broadcast authentication protocol for can bus,” in *ECRYPT Workshop on Lightweight Cryptography*, vol. 2011, 2011.

[3] A. Perrig, D. Song, R. Canetti, J. Tygar, and B. Briscoe, “Timed efficient stream loss-tolerant authentication (tesla): Multicast source authentication transform introduction,” Tech. Rep., 2005.

[4] P. Mundhenk, A. Paverd, A. Mrowca, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, “Security in automotive networks: Lightweight authentication and authorization,” *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 2, p. 25, 2017.

[5] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta *et al.*, *Status report on the second round of the NIST post-quantum cryptography standardization process*. US Department of Commerce, National Institute of Standards and Technology, 2020.

References

[6] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle ́, "Crystals–dilithium: Algorithm specification and supporting documentation. round-1 submission to the nist pqc project," 2019.

[7] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyuba- shevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle ́, "Crystals-kyber: Algorithm specifications and supporting documentation (2017)," *https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.Citationsinthisdocument*, vol. 1, 2018.

[8] M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen, "PQM4: Post-quantum crypto library for the ARM Cortex-M4," https://github. com/mupq/pqm4/tree/Round1.

[9] J. Birr-Pixton, "Cifra, Collection of cryptographic primitives targeted at embedded use," https://github.com/ctz/cifra.