ADVANCED REACTOR SAFEGUARDS & SECURITY

Integrity Enhancing Protocols

Advanced Reactor Safety and Security (ARSS) Spring Program Review

SAND2024-06096PE

PRESENTED BY

Romuald Valme, Christopher Lamb

May 15, 2024

Motivation and Background

- As technology advances security implementations are becoming inadequate
- OT environments are lacking in integrity verifying procedures
- Specific resource constraints in OT: storage, memory, CPU
- Prioritizing lower costs, and resource utilization
- Currently spending to our expense plan
  - Intend to be spent out by the end of the fiscal year

What is Cryptographic Integrity?

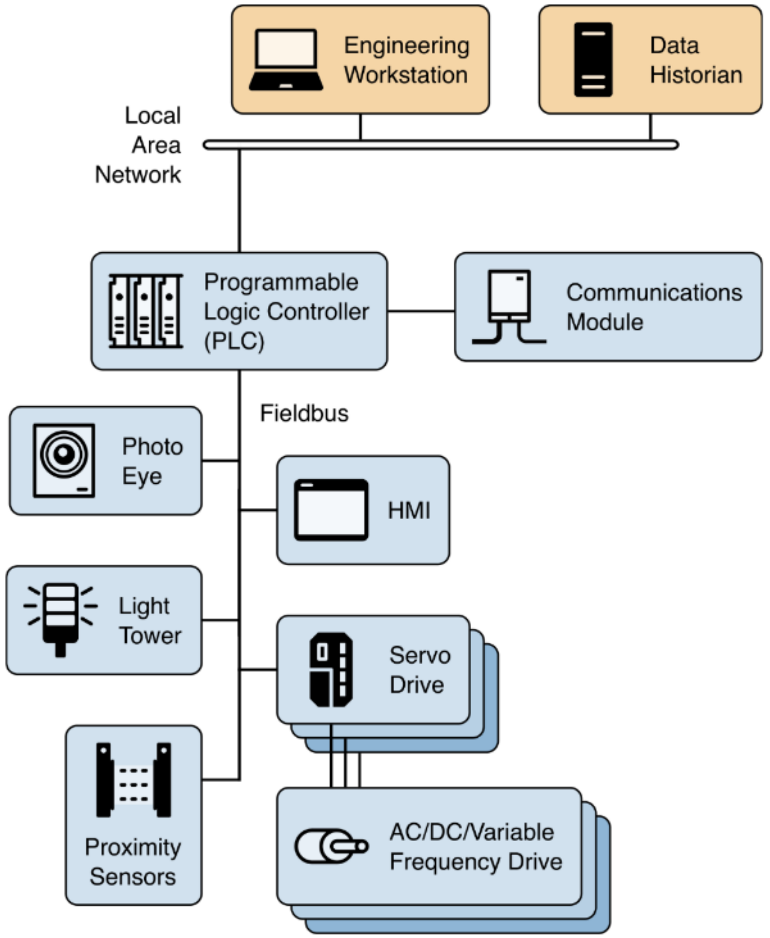
- Verifying that your received data has not been tampered with or altered from its specified source
- Guarantees data has not been altered by a hostile actor or system error
- Can provide authentication that you are communicating with the intended source
- Can provide non-repudiation in the case of public-key architecture

Need – Understanding of OT Integrity Protocols

- OT Systems have specific performance, security, and configurational requirements
- What protocols excel at meeting OT integrity requirements?

OT and Integrity Use Cases

- Control commands to actuators
- Sensor data to a PLC
- Information from and to the historian
- Data and identity verification
- Performant integrity verification is important in such cases



Project History and Overview

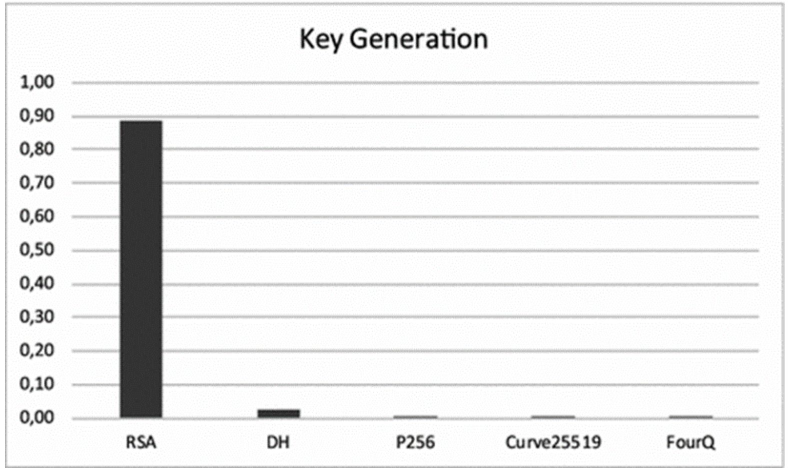
- Research began in FY24 on various Integrity Protocols
- Six categories considered for evaluation
  - Multi-signature, Lightweight, Quantum, Machine Learning, Verifiable Computing, Blockchain
  - We analyze these protocols through an evaluative framework designed to quantify and qualify OT system needs
- Current FY24 Status
  - Running scenarios and assessments in our testbed
  - Collecting attribute measures and metrics

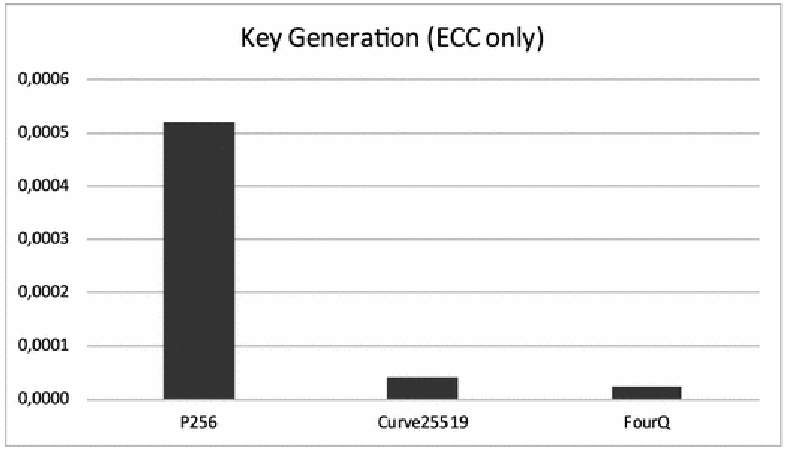
Literature Review – Promising Protocols

Category	Protocol
Multi signature	Modified El Gamal, Sequential Signing, Parallel Signing
Quantum	SPHINCS+, PQCRainbow, Falcon
Lightweight	ECDSA, SEMECS
Neural Cryptography	Autoencoders, I-EBP

Lightweight Cryptography

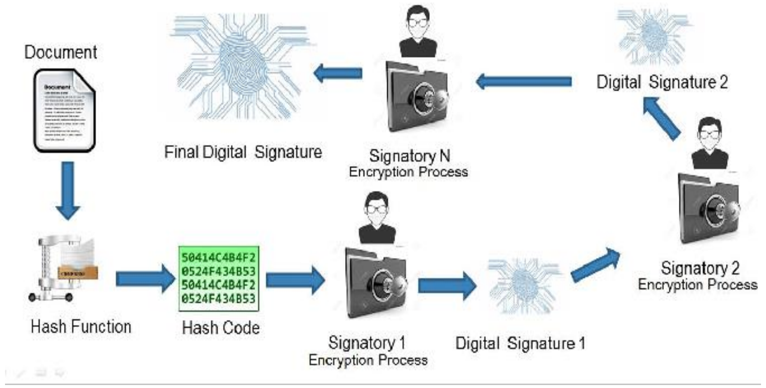
- Elliptic Curve Digital Signature Alg.
  - Various curve fields available
  - Smaller keys
  - faster encryption
- Signer Efficient Multiple-time Elliptic
- Curve Signature (SEMECS)
  - 32 byte private key
  - Modular vs. scalar multiplication
  - 118x Lower energy consumption
  - FourQ curve
-

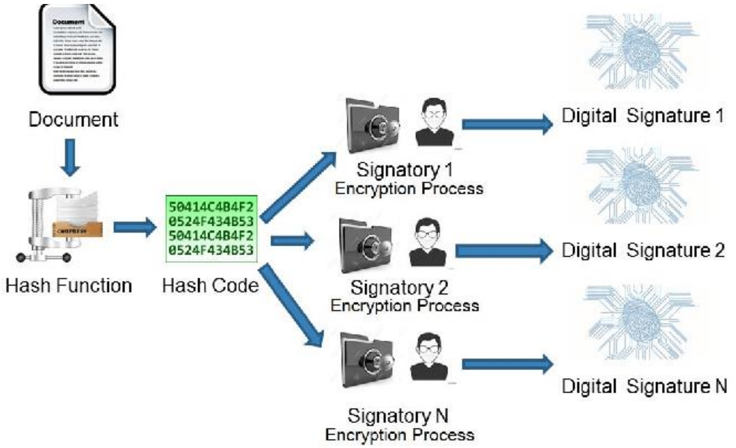




Multi Signature

- Sequential Signing
  - One output signature
  - Complex signing order
- Parallel Signing
  - The same input message is signed for all
  - Multiple output signatures
- Modified El Gamal
  - The pros of both
  - Combines keys of signatories



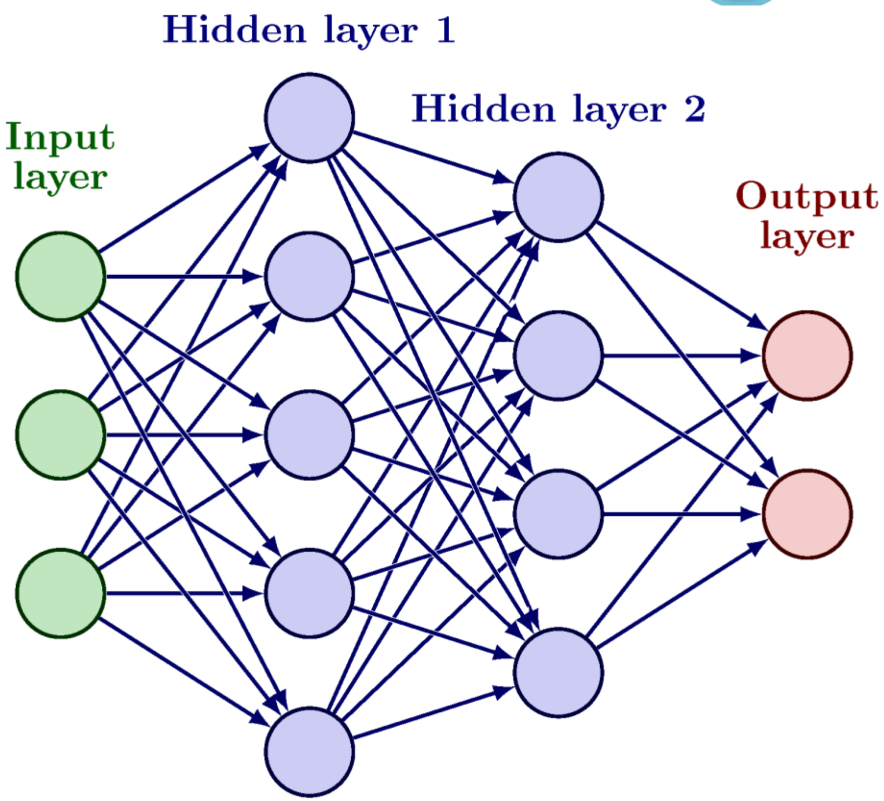


Post-Quantum Cryptography

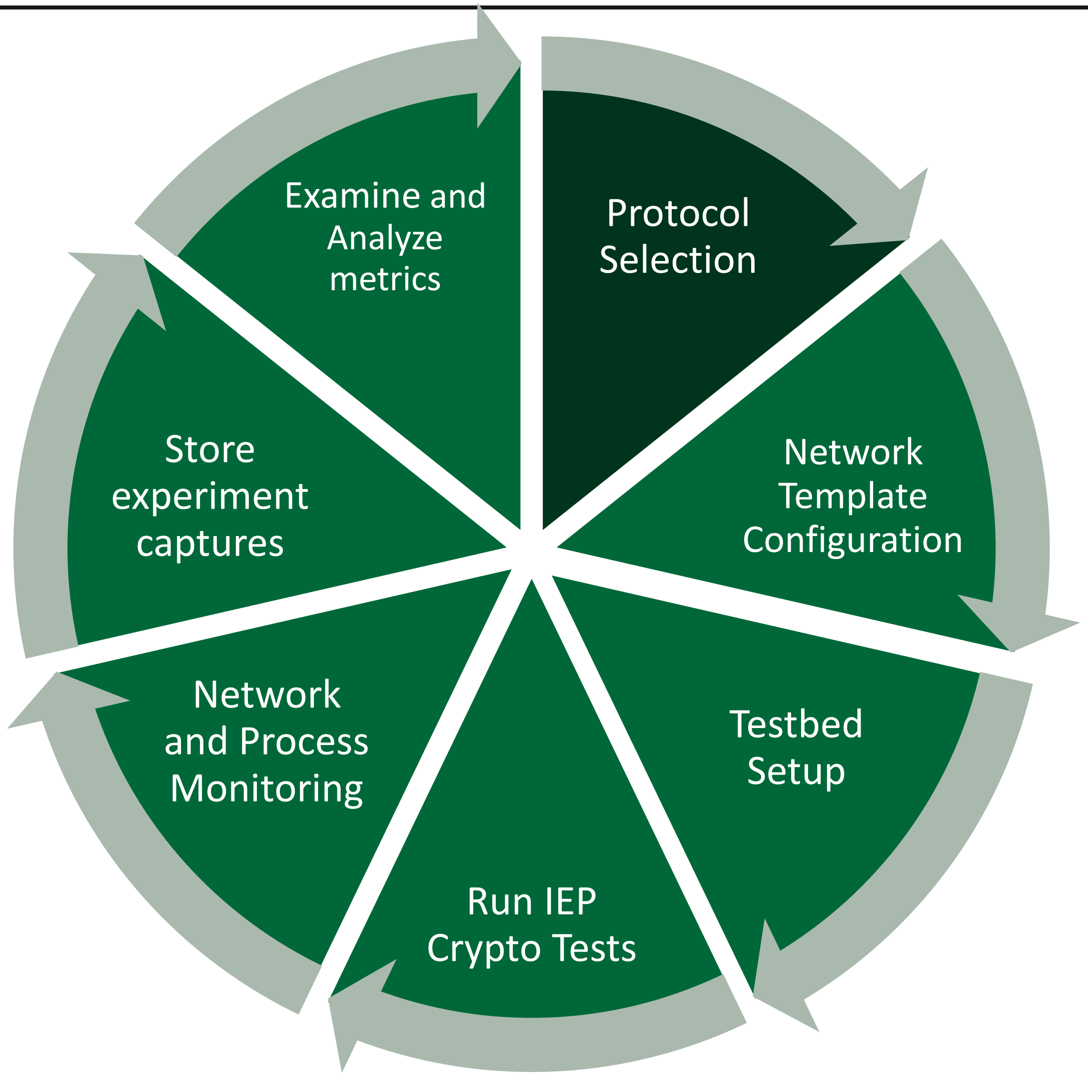
- Term denoting a wide range of protocols intended to resolve Quantum threats to traditional cryptographic schemes
- Lattice-Based Cryptography (Falcon, Dilithium, NTRU)
  - Based on hardness of high-dimensional lattice problems
- Multivariate Cryptography (LUOV, PICNIC, MQDSS)
  - Based on hardness of multivariate polynomial equations
- Limited evaluation of novel post-quantum protocols on OT hardware

Neural Cryptography

- Hebbian Rule
  - Updating weights in network based on paired output
  - Used to generate private and public key
- Models used for encryption function
  - Convolutional layers
  - Autoencoders
- Feature rich data
  - Biometrics
  - Improved key management and storage as weights
  - Train network to recognize identity



Evaluation Process and Framework



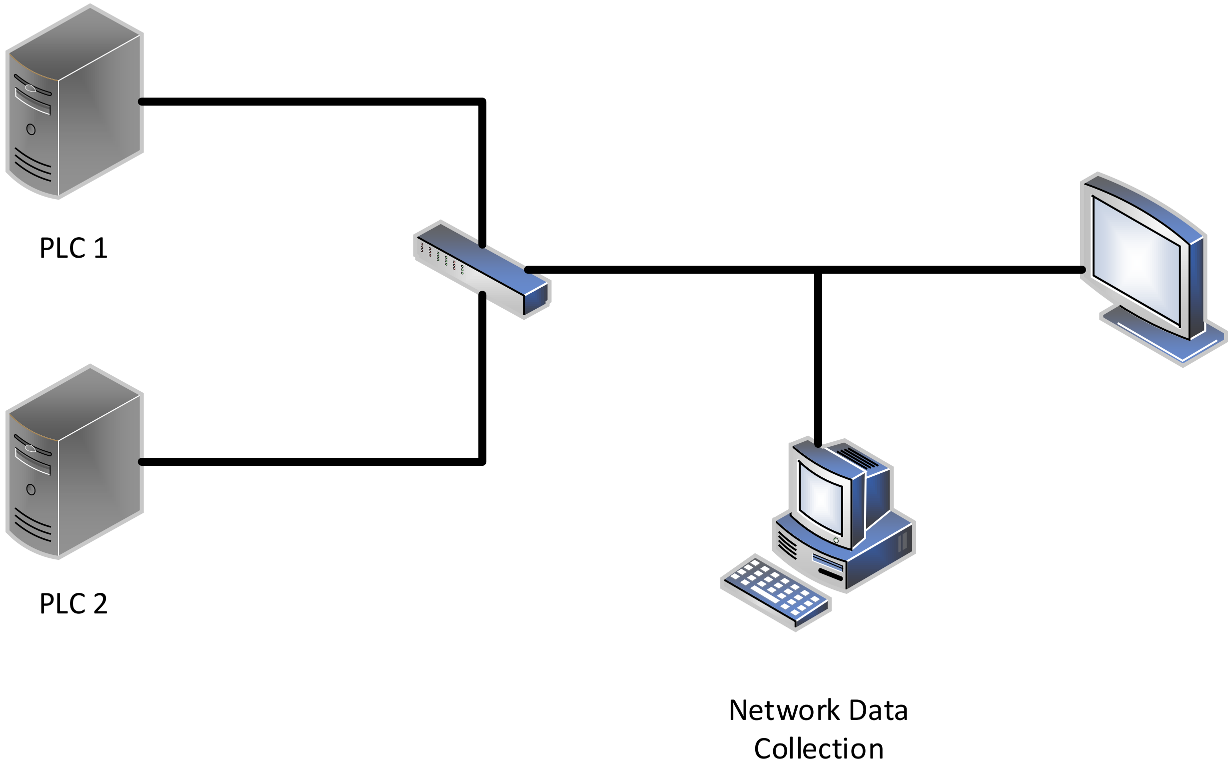
Framework Metrics and Groups

Attribute Group	Attribute	Metric	Notes
Protocol Running time	Key Generation Running Time	Microseconds (µs)	Measured in function call
	Key Generation Asymptotic Worst Case	Big O Notation (O(n))	Derived theoretically
	Key Encapsulation Running Time	Microseconds (µs)	Measured in function call
	Key Decapsulation Running Time	Microseconds (µs)	Measured in function call
Endpoint Storage Requirements	Key Storage Requirements	Bytes	Single key storage
	Cryptosystem Storage Requirements	Bytes	Algorithm component storage requirements
Protocol Hardware Performance	Cryptosystem Average CPU Utilization	Percentage	Average usage over a single transaction
	Cryptosystem Average Memory Usage	Bytes	Average usage over a single transaction
	Network Transmission Time	Milliseconds (ms)	Measured in function call
Existing Security Evaluation Level	NIST Security Classification of Modules (FIPS 140-2 [16])	Integer Scale (1-4)	Physical module security
	NIST PQC Security Project Levels [17]	Integer Scale (1-5)	Protocol security in relation to classical protocols

Scenarios and Testing

- Based on our PROMISE Capstone Environment
- PLC 1
  - Communicates sensitive sensor and actuator data across the network
- PLC 2
  - Communicates sensitive sensor and actuator data across the network
- Router
  - Facilitate data flow throughout network
- Network Data Collection
  - Capture packets, testing data security and integrity

Emulation Environment



Environments and Tools

- Minimega/PHENIX
    - A virtual machine and network emulator environment
- Wireshark/tcpdump
    - Observing network traffic
- Python
    - Cryptographic libraries and profiling tools
- Standard Linux commands
    - ps, top, etc. for machine metrics

Q&A