QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things

Presenter: Venkata K. V. V. Bathalapalli

Venkata K. V. V. Bathalapalli[1], S. P. Mohanty[2], Chenyun Pan[3].
Elias Kougianos[4]

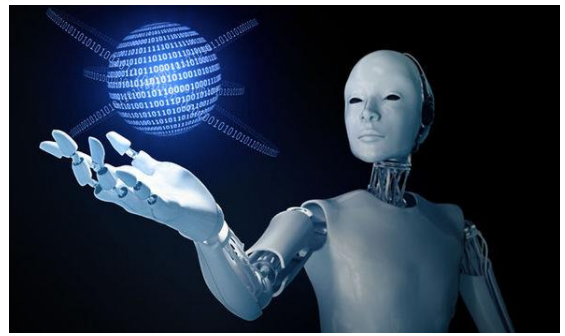
University of North Texas, Denton, TX, USA.[1,2,4] and
University of Texas at Arlington[3].

Email: vb0194@unt.edu[1] , saraju.mohanty@unt.edu[2] , chenyun.pan@uta.edu[3], elias.kougianos@unt.edu[4]

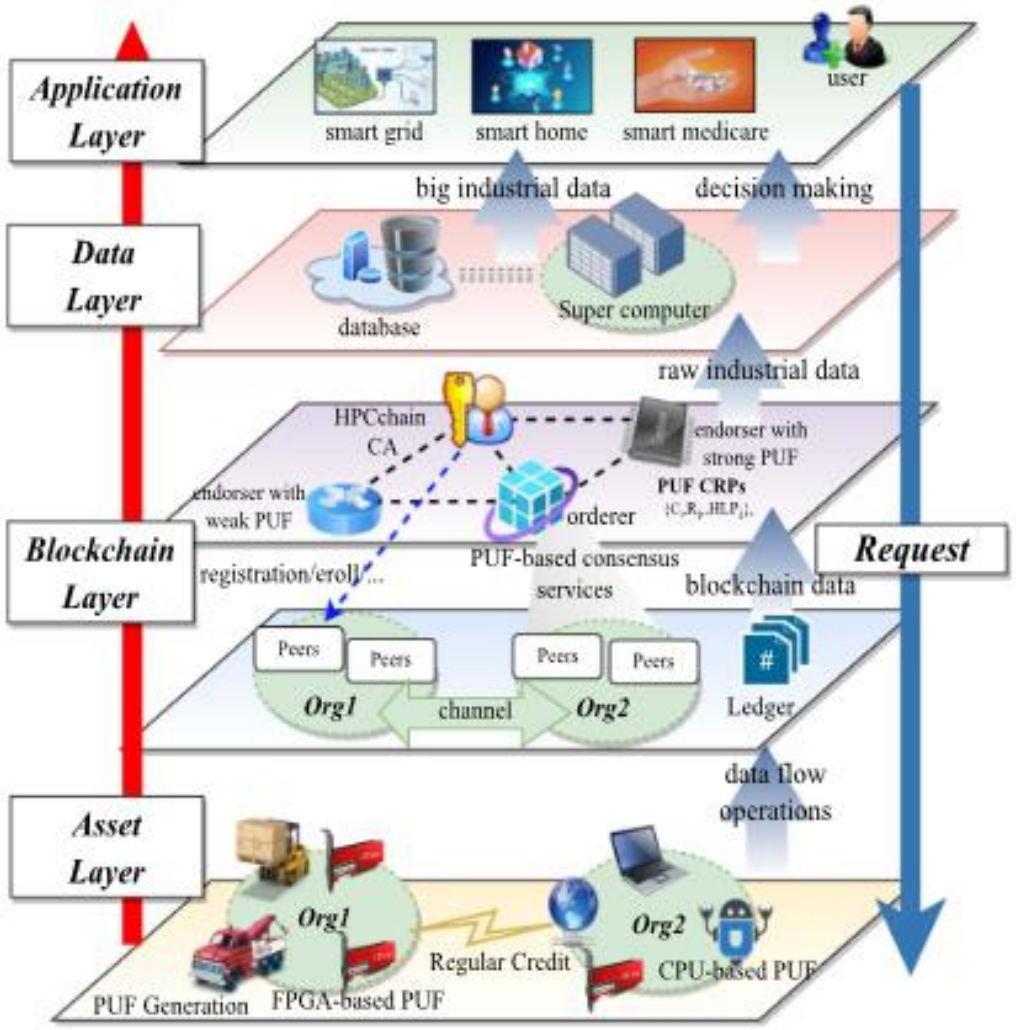
Outline

- Introduction to Quantum Computing
- Security-by-Design (SbD) in Quantum Computing
- Cybersecurity in Industrial Internet-of-Things (IIoT)
- Physical Unclonable Functions (PUF)
- Proposed Quantum Hardware-based PUF Design
- Experimental implementation Overview
- Conclusion & Future Research Directions

Security-by-Design (SbD) – Industrial Internet-of-Things (IIoT)



Architecture of I-CPS



Asset layer: This layer consists of smart manufacturing equipment, vehicles, drones, and sensors. These devices collect sensor data from IIoT network devices in real-time and communicate the data to the upper level.

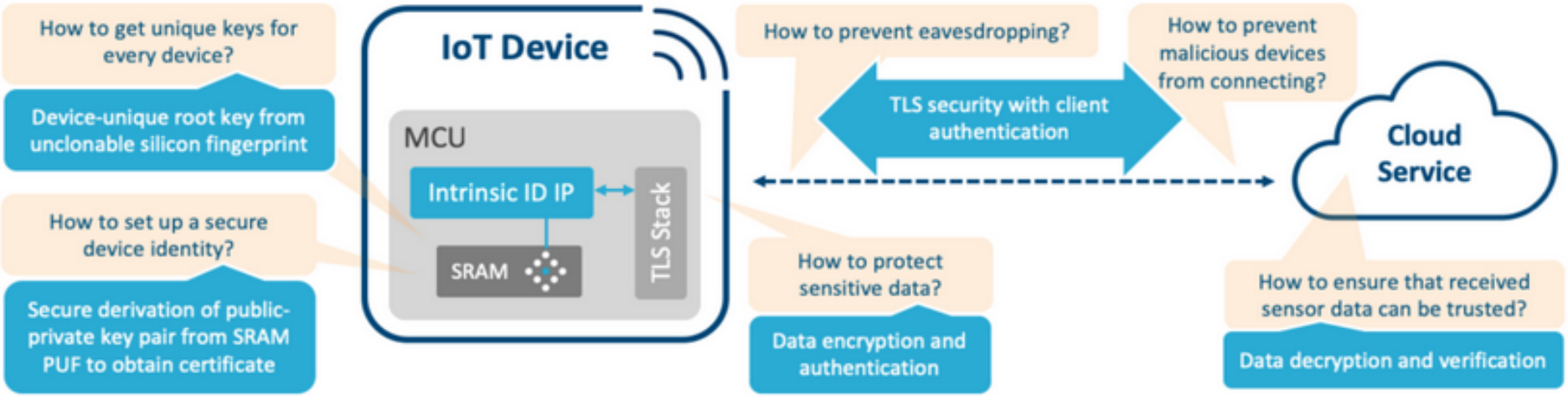
Blockchain Layer: Blockchain securely records the sensor data inside a digital ledger and broadcasts it to all the stakeholders or industrial entities in the IIoT system globally.

Data layer: This layer edge, cloud, and supercomputers for faster analysis, processing and decision-making of sensor data IIoT systems employ Powerful databases, supercomputers, and high-speed networks.

Application layer: This layer consists of policy and decision making which integrates numerous IIoT application scenarios and users. Especially in the future Industry 4.0 era, the application of IIoT will be further expanded.

Source: K. Qian, Y. Liu, X. He, M. Du, S. Zhang, and K. Wang, "HPCchain: A Consortium Blockchain System Based on CPU-FPGA Hybrid-PUF for Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 11, pp. 11205-11215, Nov. 2023, doi: 10.1109/TII.2023.3244339.

PUF as a SbD Primitive for IIoT



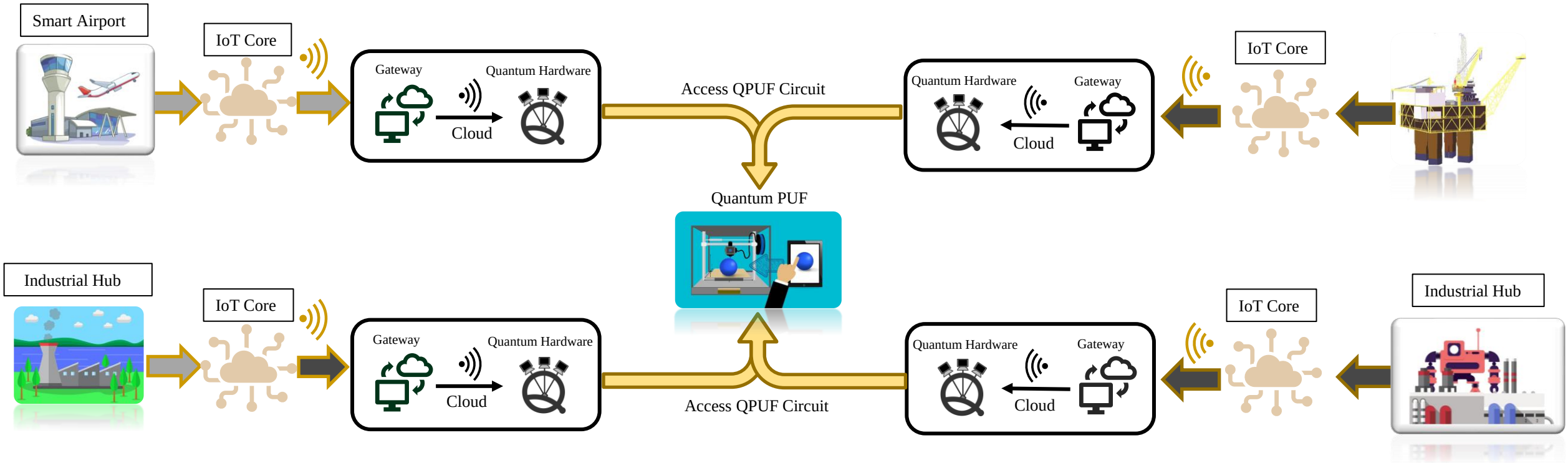
source: https://www.intrinsic-id.com/markets/industrial-iot/

Related Research Overview

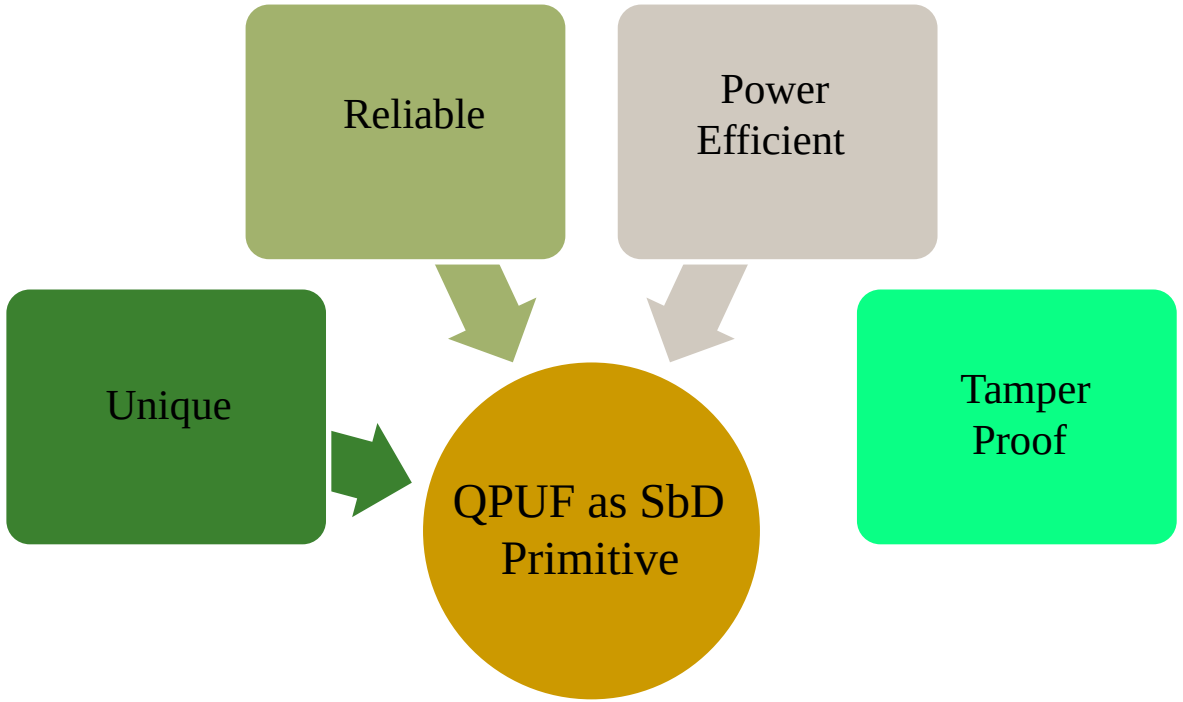
Research Works	Security Mechanism	Approach	Features	Platform
Barbareschi, et al. 2021	Pseudo-PUF for Industrial IoT	Weak PUF, Encryption Module	Low energy overhead	NA
Phalak, et al.2021	Decoherence and Hadamard PUF	Qubit Decoherence	Security in Quantum Computing	Cloud
Gong, et al. 2022	PUF-based Authentication in IIoT	PUF, Fuzzy extractor	Secure Machine to Machine Communication	Cloud Computing
Shan, et al. 2023	PUF-based sensor security	SRAM PUF, HMAC Algorithm	Industrial sensor data integrity	SCADA System
Qian, et al. 2023	PUF-based Blockchain for IIoT	Hybrid PUF, Consortium Blockchain	CPU & FPGA based PUF with enhanced uniqueness	NA
QPUF (This Work)	**Quantum Computing based PUF for IIoT**	**QPUF based on Quantum logic gates**	**Quantum hardware based Reliable QPUF responses**	**IBM's Quantum Cloud**

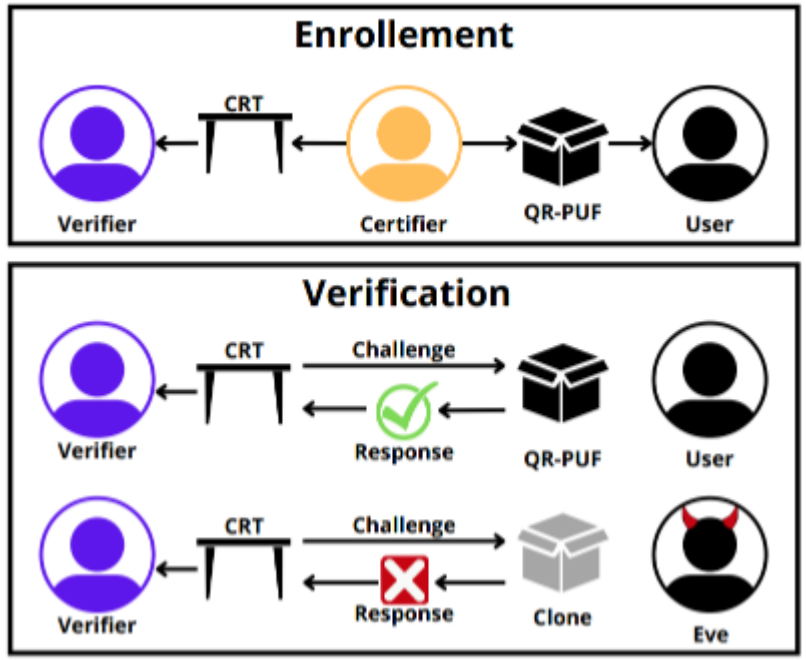
Quantum Physical Unclonable Function (QPUF) as a SbD Primitive

Architectural Overview of QPUF Enabled IIoT



QPUF as a SbD Primitive

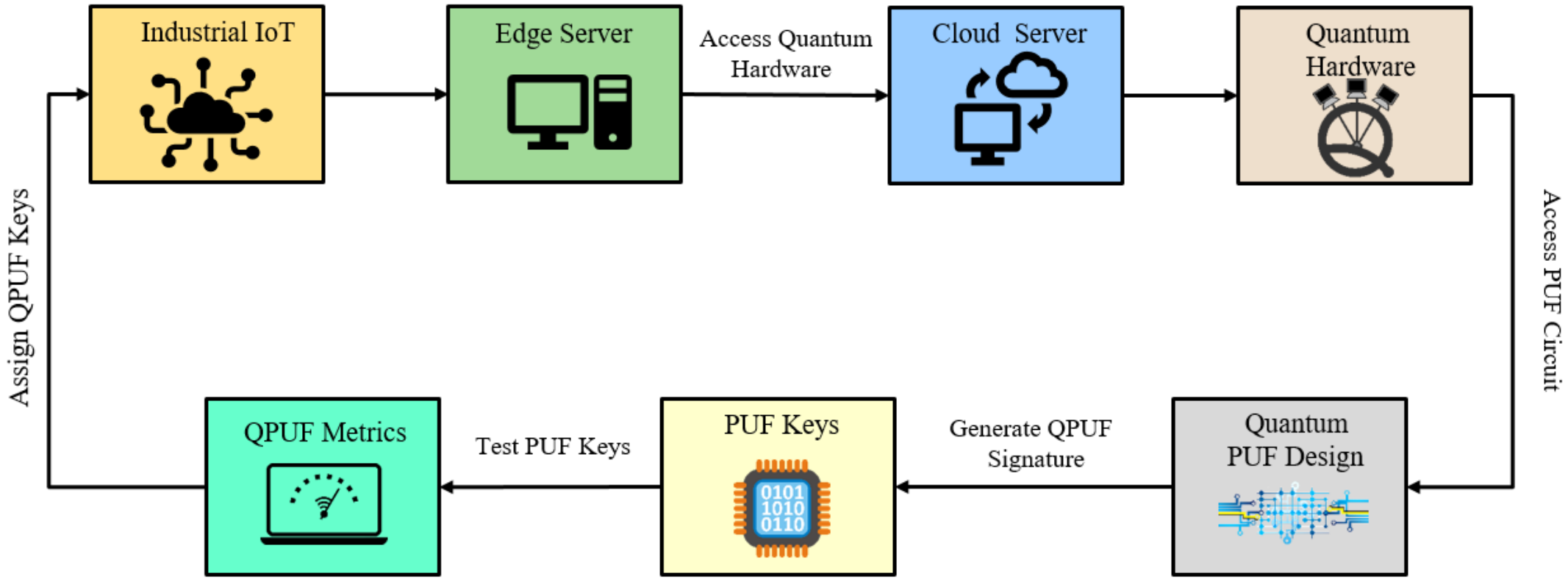




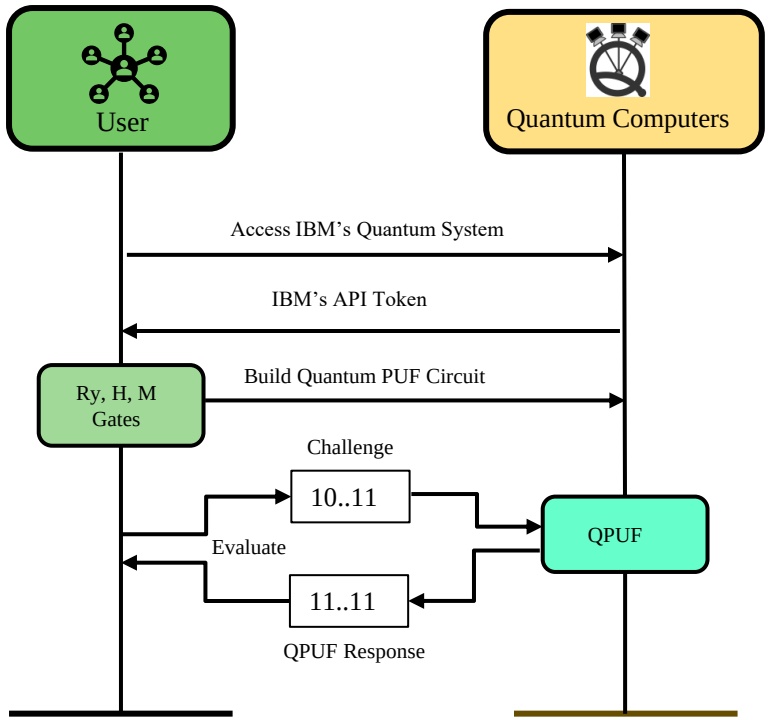
Enrollment: The Certifier generates the Challenge-Response Table (CRP) by querying the QR-PUF and submits it to the Verifier while the QR-PUF is given to the user.
Verification: The verifier extracts CRP from the user's QR-PUF through a Quantum channel.

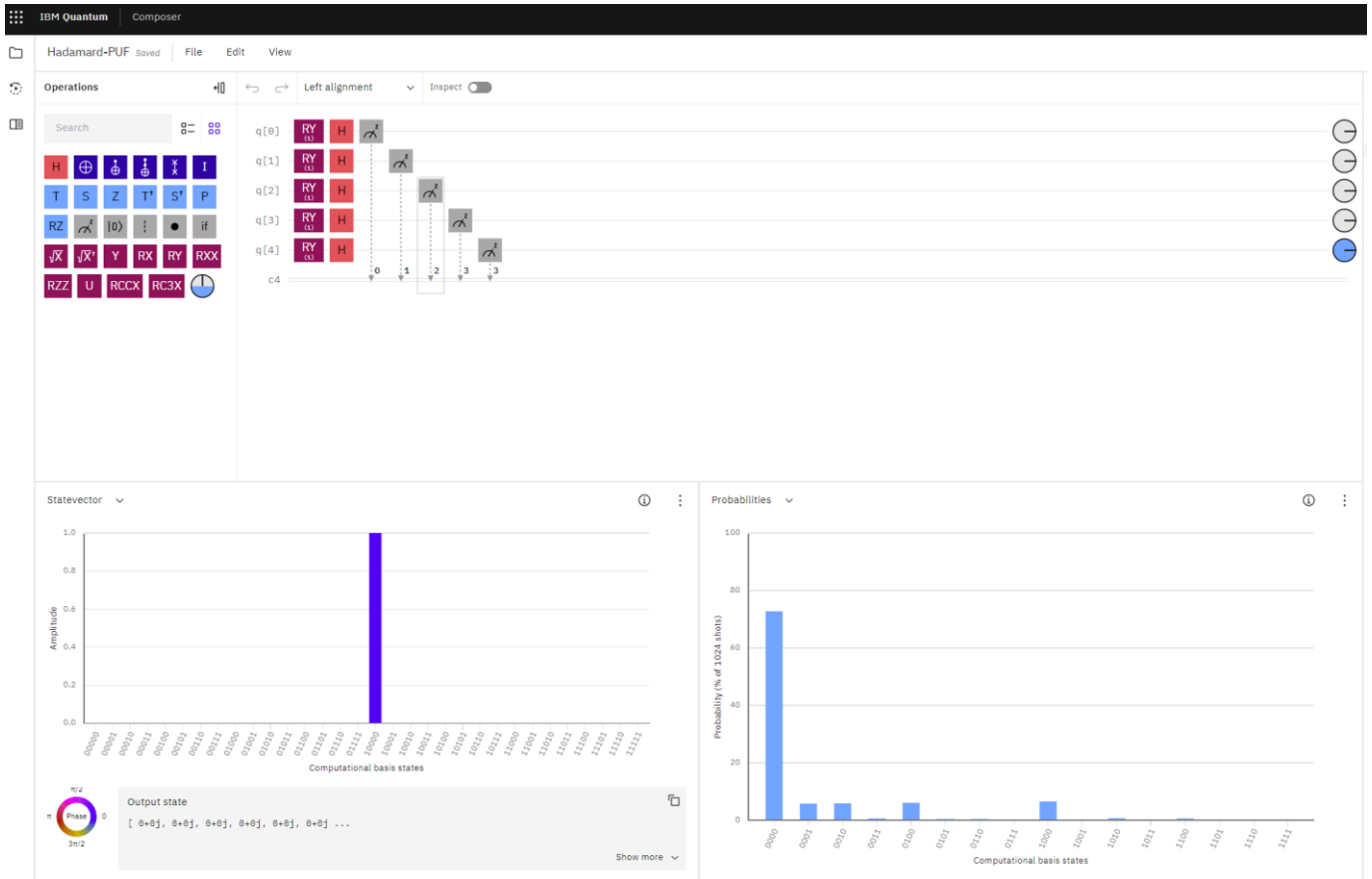
Source: V. Galetsky, S. Ghosh, C. Deppe and R. Ferrara, "Comparison of Quantum PUF models," *2022 IEEE Globecom Workshops (GC Wkshps)*, Rio de Janeiro, Brazil, 2022, pp. 820-825, doi: 10.1109/GCWkshps56602.2022.10008722.

Working Overview of QPUF for SbD of IIoT



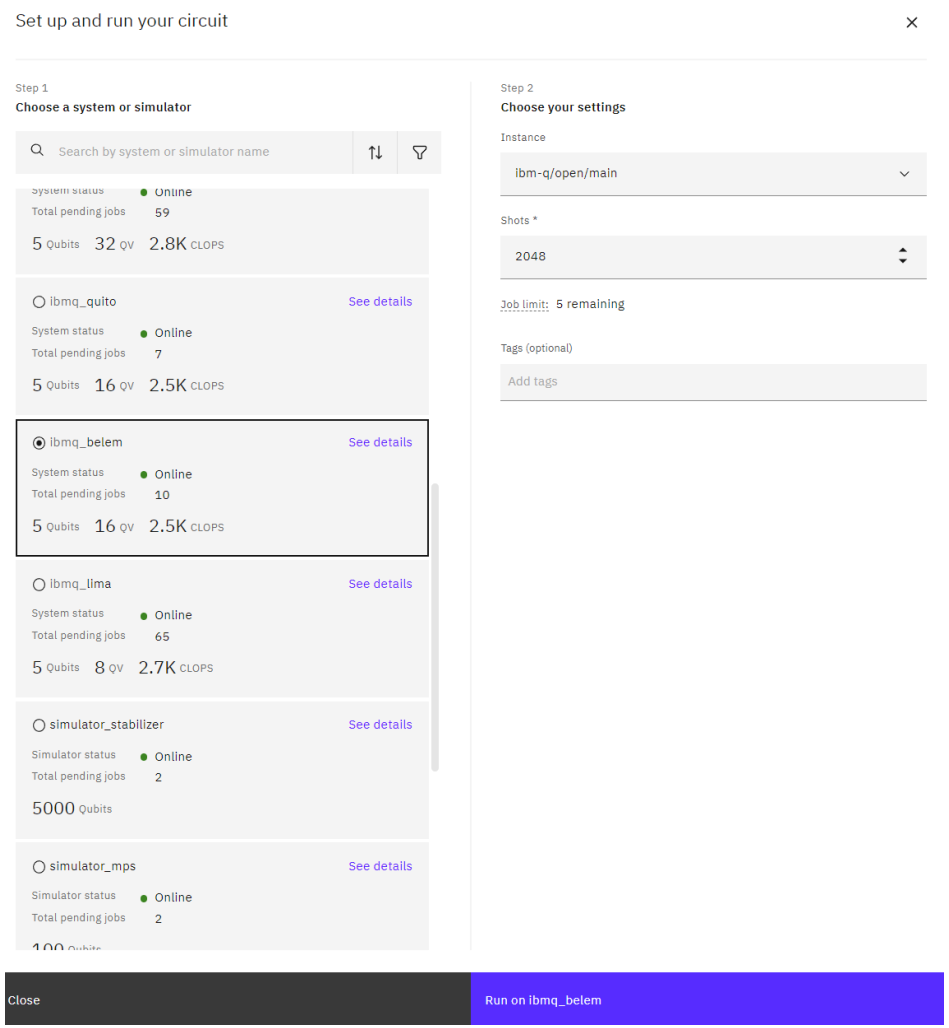
Accessing Quantum Hardware



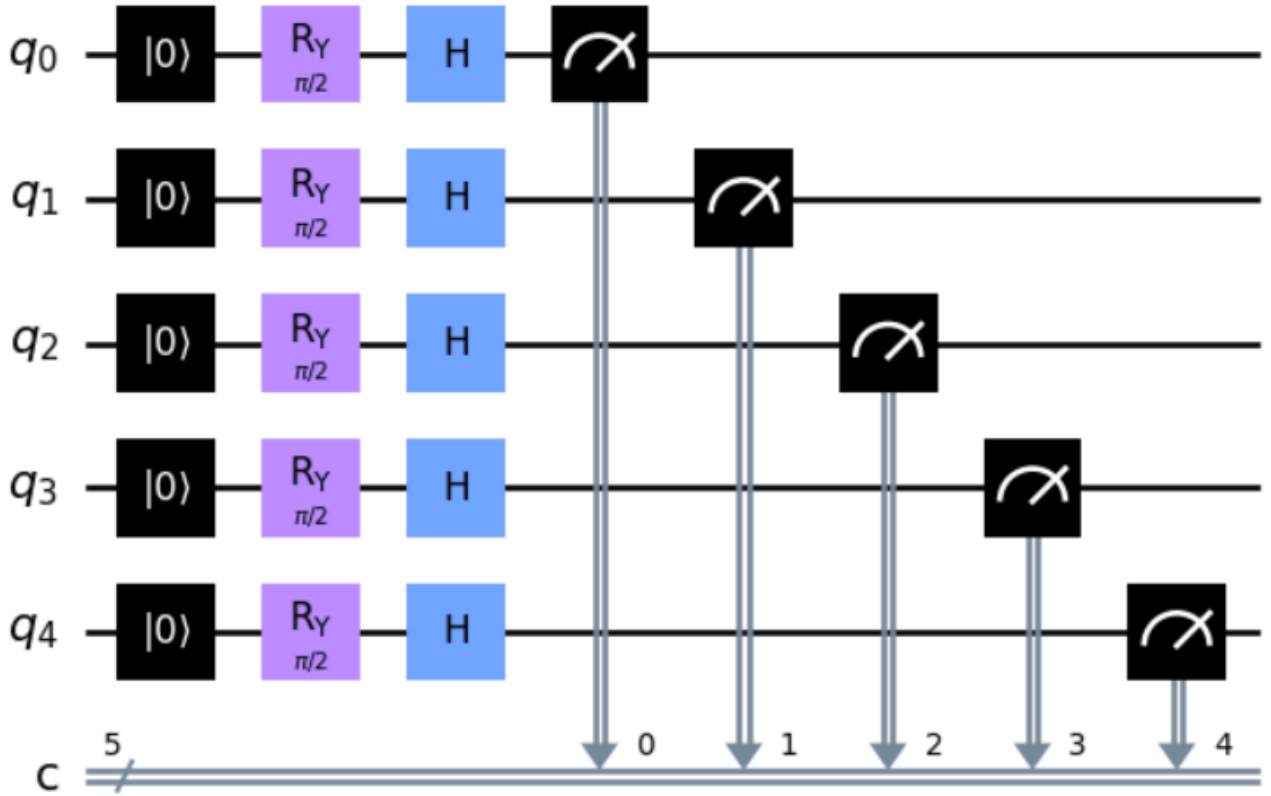


Choosing Quantum Systems from IBM Quantum

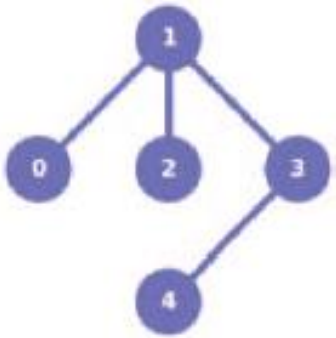
- 5 Qubit and 7-Qubit systems are the most widely chosen Quantum Hardware.
- Ibmq_lima, ibmq_quito, ibmq_belem are 5 Qubit systems.
- Ibmq_Jakarta, ibm_perth, ibmq_manila are 7 Qubit systems.
- At present 127 –Qubit Hardware is available for deployment of Quantum Circuits.

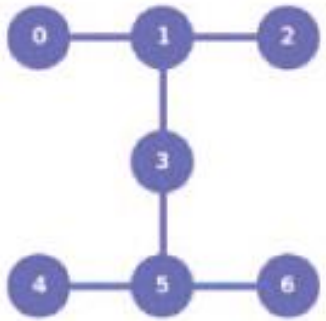


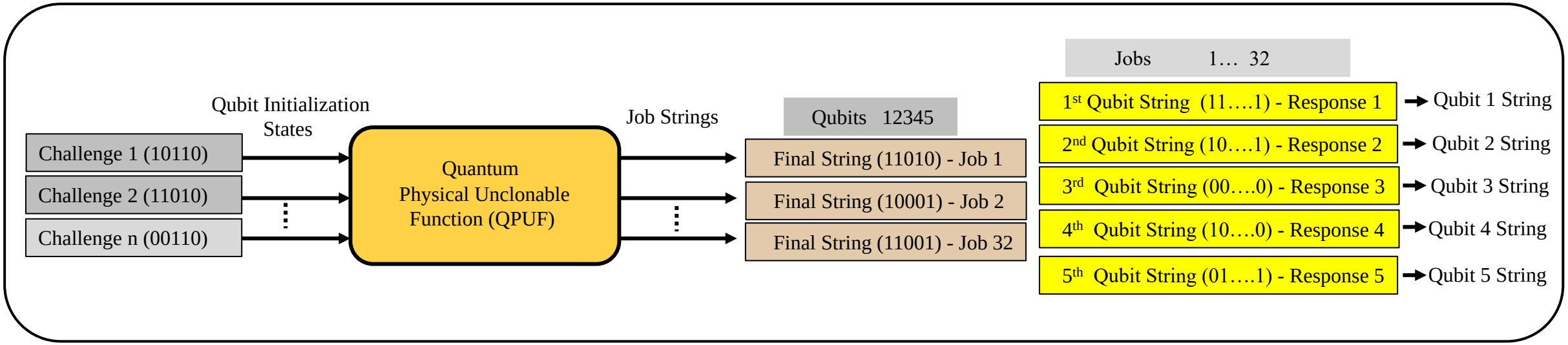
QPUF Design Using Quantum Logic Gates



QPUF Modelling Approach







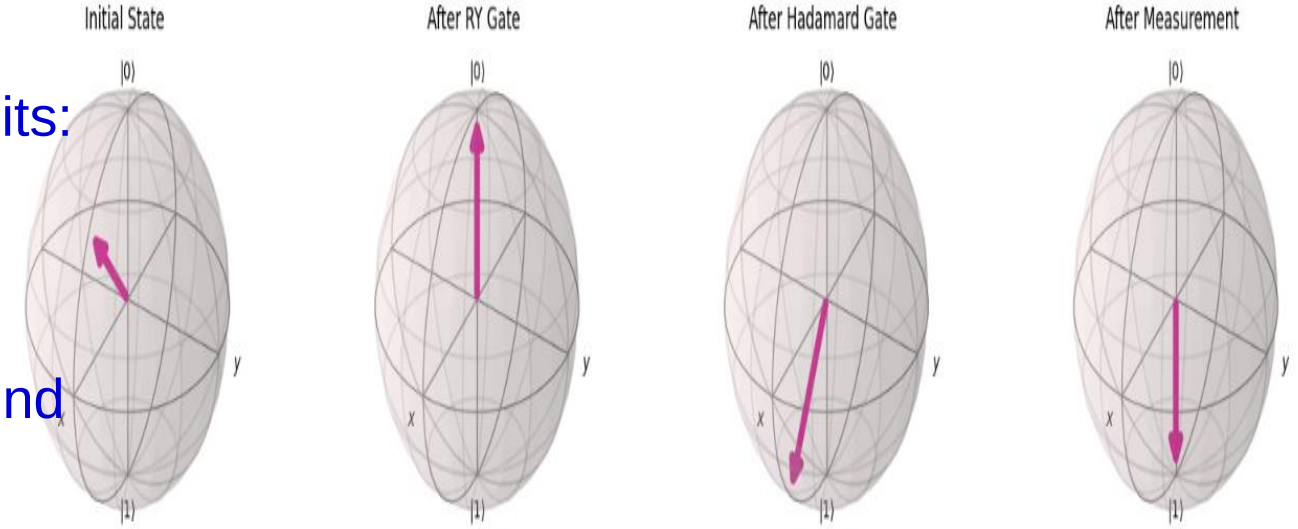
QPUF Quantum State Representation

- Initialize Qubits (Varying Initializations)
- Apply Ry gate to all Qubits: Ry Angle→pi/4, pi/2,...

  Circuit→ Ry[q]
- Apply Hadamard gate to all Qubits:

  Circuit→ H(Ry[q])
- Apply Measurement Gate(M)

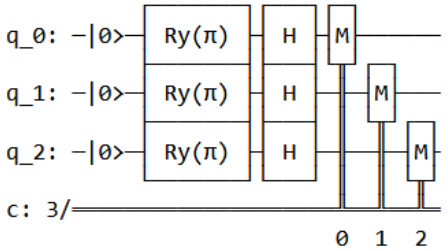
  Circuit→ M[H(Ry[q])]
- Execute the circuit on the Chosen backend
- Jobs sets-5 sets, Each job
- Inputs- Initialization, Ry Gate angle
- Extract results string from all jobs
- Extract Qubit strings from all job strings



QPUF Characterization

QPUF Parameters	Specific Details
Quantum System	IBM
Working Platform	IBM Quantum Experience
Environment	Qiskit
Quantum Logic Gates	Hadamard, Ry, and Measurement Gates
Quantum Systems	Hardware
Noise Reduction Scheme	Majority Vote
Quantum Hardware	Ibmq_belem, ibmq_lima, and ibmq_quito
Number of Jobs Submitted to Each Hardware	25
Number of Shots for Each Job	8192
Hardware	5-Qubit

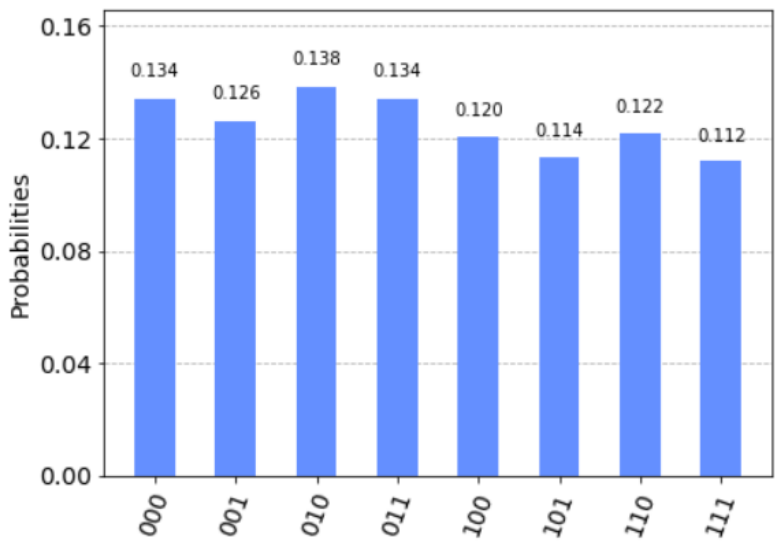
QPUF Validation




```
Total counts: {'000': 1, '010': 4, '101': 4, '001': 3, '100': 2, '110': 1, '111': 1}
Job Status: job has successfully run
```

In [2]:
```
result = job.result()
plot_histogram(result.get_counts(qc))
```

Out[2]:



Qubit Frequencies

Frequencies	ibmq_lima (GHz)	ibmq_quito (GHz)	ibmq_belem (GHz)
Qubit 0	5.03	5.30	5.09
Qubit 1	5.13	5.08	5.25
Qubit 2	5.25	5.32	5.36
Qubit 3	5.30	5.16	5.17
Qubit 4	5.09	5.05	5.26

QPUF Evaluation Results

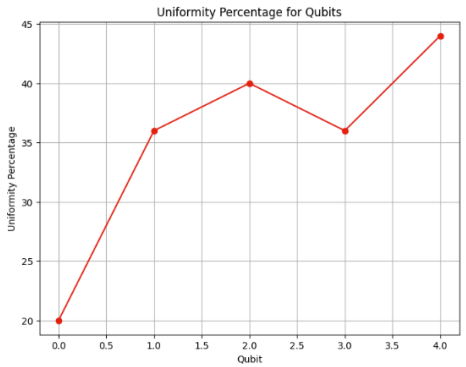
Figure-of-Merits	ibmq_lima	ibmq_quito	ibmq_belem
Overall Hamming Distance	40.0%	38.4%	34.4%
Uniformity of QPUF	35.2%	29.6%	27.6%
Uniqueness of QPUF	25.2%		
Reliability	60.0%	48.0%	-

QPUF Evaluation Results

Ibmq_lima

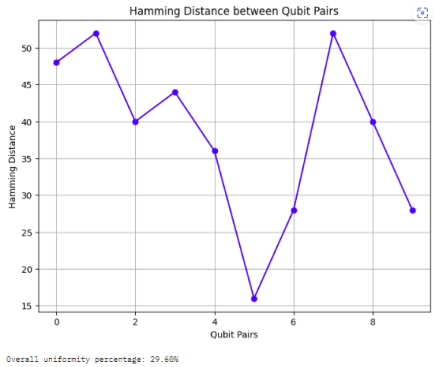
```
Qubit 0 string: 000100001000010000010000010
Qubit 1 string: 110001001011000001000011000
Qubit 2 string: 000101011011000001100l100
Qubit 3 string: 010001001010010010011l000
Qubit 4 string: 110000100110011001l011000
Calculating Hamming distance between qubit 0 and qubit 1.
Hamming distance between qubit 0 and qubit 1: 0.48
Calculating Hamming distance between qubit 0 and qubit 2.
Hamming distance between qubit 0 and qubit 2: 0.36
Calculating Hamming distance between qubit 0 and qubit 3.
Hamming distance between qubit 0 and qubit 3: 0.40
Calculating Hamming distance between qubit 0 and qubit 4.
Hamming distance between qubit 0 and qubit 4: 0.48
Uniformity percentage for qubit 0: 20.00%
Calculating Hamming distance between qubit 1 and qubit 2.
Hamming distance between qubit 1 and qubit 2: 0.36
Calculating Hamming distance between qubit 1 and qubit 3.
Hamming distance between qubit 1 and qubit 3: 0.16
Calculating Hamming distance between qubit 1 and qubit 4.
Hamming distance between qubit 1 and qubit 4: 0.40
Uniformity percentage for qubit 1: 36.00%
Calculating Hamming distance between qubit 2 and qubit 3.
Hamming distance between qubit 2 and qubit 3: 0.44
Calculating Hamming distance between qubit 2 and qubit 4.
Hamming distance between qubit 2 and qubit 4: 0.52
Uniformity percentage for qubit 2: 40.00%
Calculating Hamming distance between qubit 3 and qubit 4.
Hamming distance between qubit 3 and qubit 4: 0.40
Uniformity percentage for qubit 3: 36.00%
Uniformity percentage for qubit 4: 44.00%
Overall Hamming distance: 40.00%
Overall uniformity percentage: 35.20%
```

Overall uniformity percentage: 35.20%

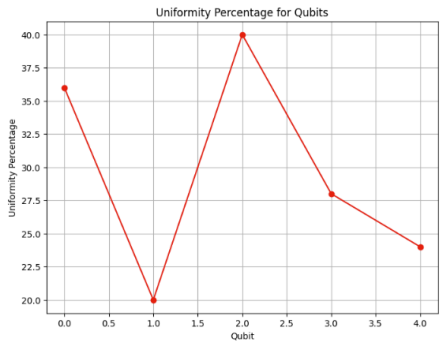


Ibmq_quito

```
Qubit 0 string: 100110011100010000l000010
Qubit 1 string: 010000001001000010000l000
Qubit 2 string: 001101001001001100l001001
Qubit 3 string: 010010001000110010000l000
Qubit 4 string: 010000100000010100l001000
Calculating Hamming distance between qubit 0 and qubit 1...
Hamming distance between qubit 0 and qubit 1: 0.48
Calculating Hamming distance between qubit 0 and qubit 2...
Hamming distance between qubit 0 and qubit 2: 0.52
Calculating Hamming distance between qubit 0 and qubit 3...
Hamming distance between qubit 0 and qubit 3: 0.40
Calculating Hamming distance between qubit 0 and qubit 4...
Hamming distance between qubit 0 and qubit 4: 0.44
Uniformity percentage for qubit 0: 36.00%
Calculating Hamming distance between qubit 1 and qubit 2...
Hamming distance between qubit 1 and qubit 2: 0.36
Calculating Hamming distance between qubit 1 and qubit 3...
Hamming distance between qubit 1 and qubit 3: 0.16
Calculating Hamming distance between qubit 1 and qubit 4...
Hamming distance between qubit 1 and qubit 4: 0.28
Uniformity percentage for qubit 1: 20.00%
Calculating Hamming distance between qubit 2 and qubit 3...
Hamming distance between qubit 2 and qubit 3: 0.52
Calculating Hamming distance between qubit 2 and qubit 4...
Hamming distance between qubit 2 and qubit 4: 0.40
Uniformity percentage for qubit 2: 40.00%
Calculating Hamming distance between qubit 3 and qubit 4...
Hamming distance between qubit 3 and qubit 4: 0.28
Uniformity percentage for qubit 3: 28.00%
Uniformity percentage for qubit 4: 24.00%
Overall Hamming distance: 38.40%
Overall uniformity percentage: 29.60%
```



Overall uniformity percentage: 29.60%

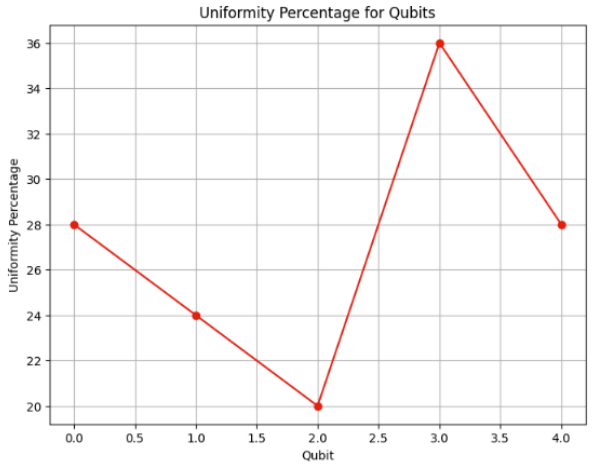


Continued…

Ibmq_belem

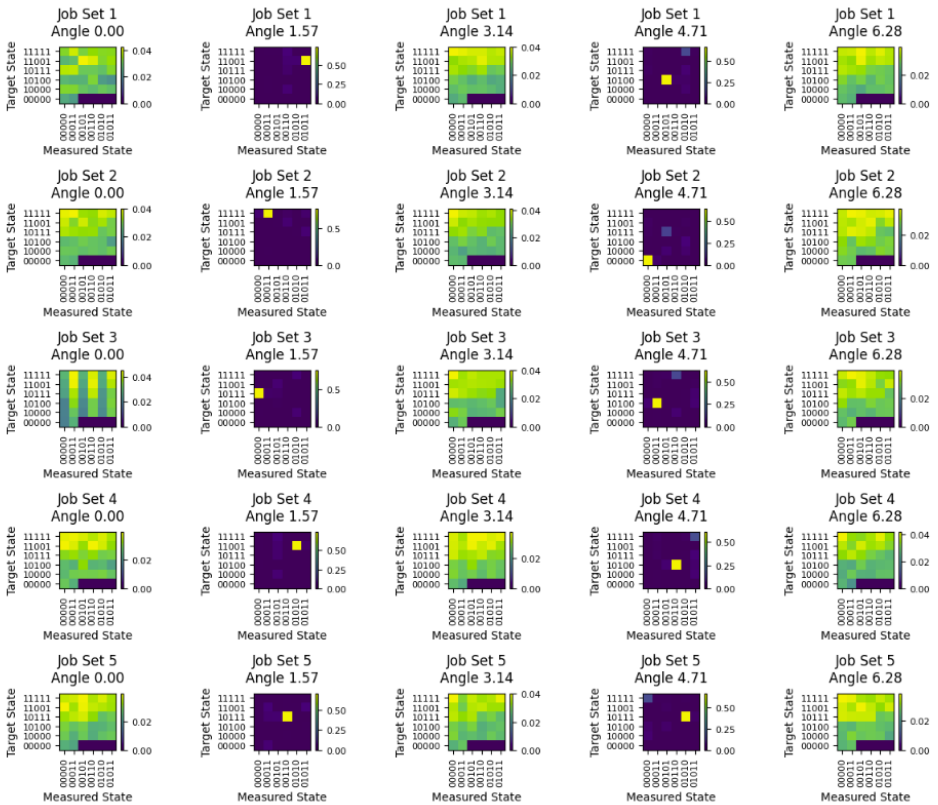
```
Qubit 0 string: 10010100100001000001000010
Qubit 1 string: 01001000100100001000001000
Qubit 2 string: 00010000100100000001001000
Qubit 3 string: 01000001110001001101010000
Qubit 4 string: 01000010000001000001101001
Calculating Hamming distance between qubit 0 and qubit 1...
Hamming distance between qubit 0 and qubit 1: 0.44
Calculating Hamming distance between qubit 0 and qubit 2...
Hamming distance between qubit 0 and qubit 2: 0.24
Calculating Hamming distance between qubit 0 and qubit 3...
Hamming distance between qubit 0 and qubit 3: 0.48
Calculating Hamming distance between qubit 0 and qubit 4...
Hamming distance between qubit 0 and qubit 4: 0.40
Uniformity percentage for qubit 0: 28.00%
Calculating Hamming distance between qubit 1 and qubit 2...
Hamming distance between qubit 1 and qubit 2: 0.20
Calculating Hamming distance between qubit 1 and qubit 3...
Hamming distance between qubit 1 and qubit 3: 0.28
Calculating Hamming distance between qubit 1 and qubit 4...
Hamming distance between qubit 1 and qubit 4: 0.36
Uniformity percentage for qubit 1: 24.00%
Calculating Hamming distance between qubit 2 and qubit 3...
Hamming distance between qubit 2 and qubit 3: 0.40
Calculating Hamming distance between qubit 2 and qubit 4...
Hamming distance between qubit 2 and qubit 4: 0.32
Uniformity percentage for qubit 2: 20.00%
Calculating Hamming distance between qubit 3 and qubit 4...
Hamming distance between qubit 3 and qubit 4: 0.32
Uniformity percentage for qubit 3: 36.00%
Uniformity percentage for qubit 4: 28.00%
Overall Hamming distance: 34.40%
Overall uniformity percentage: 27.20%
```

Overall uniformity percentage: 27.20%

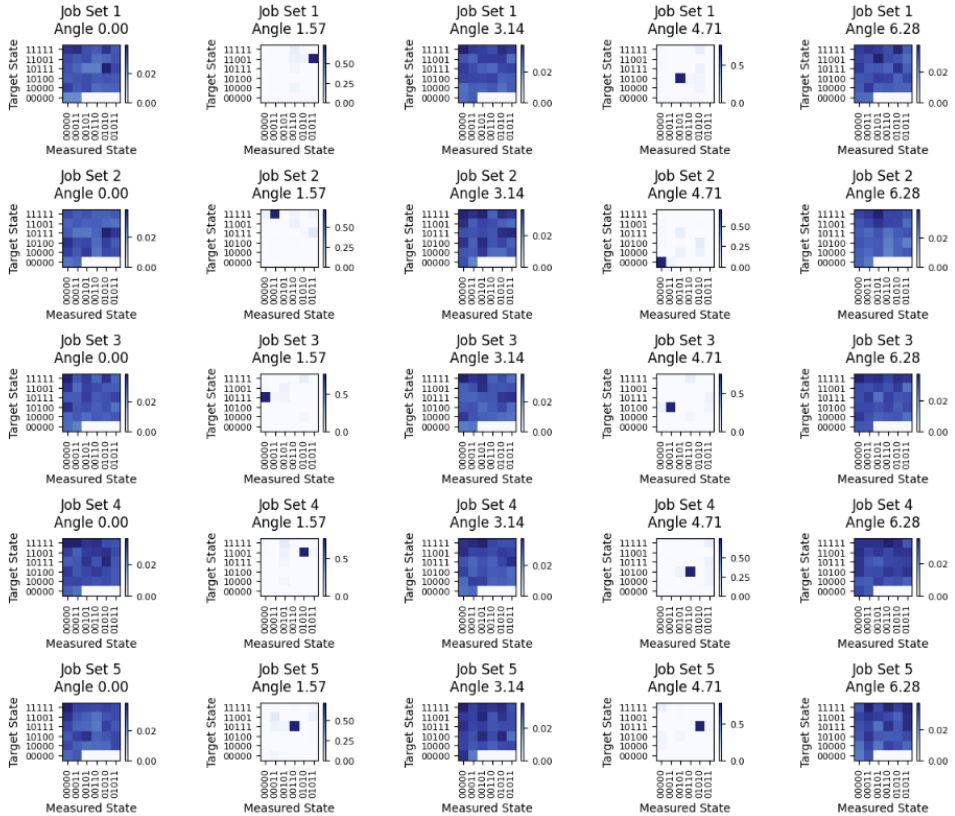


QPUF Outcome Probabilities

ibmq_belem

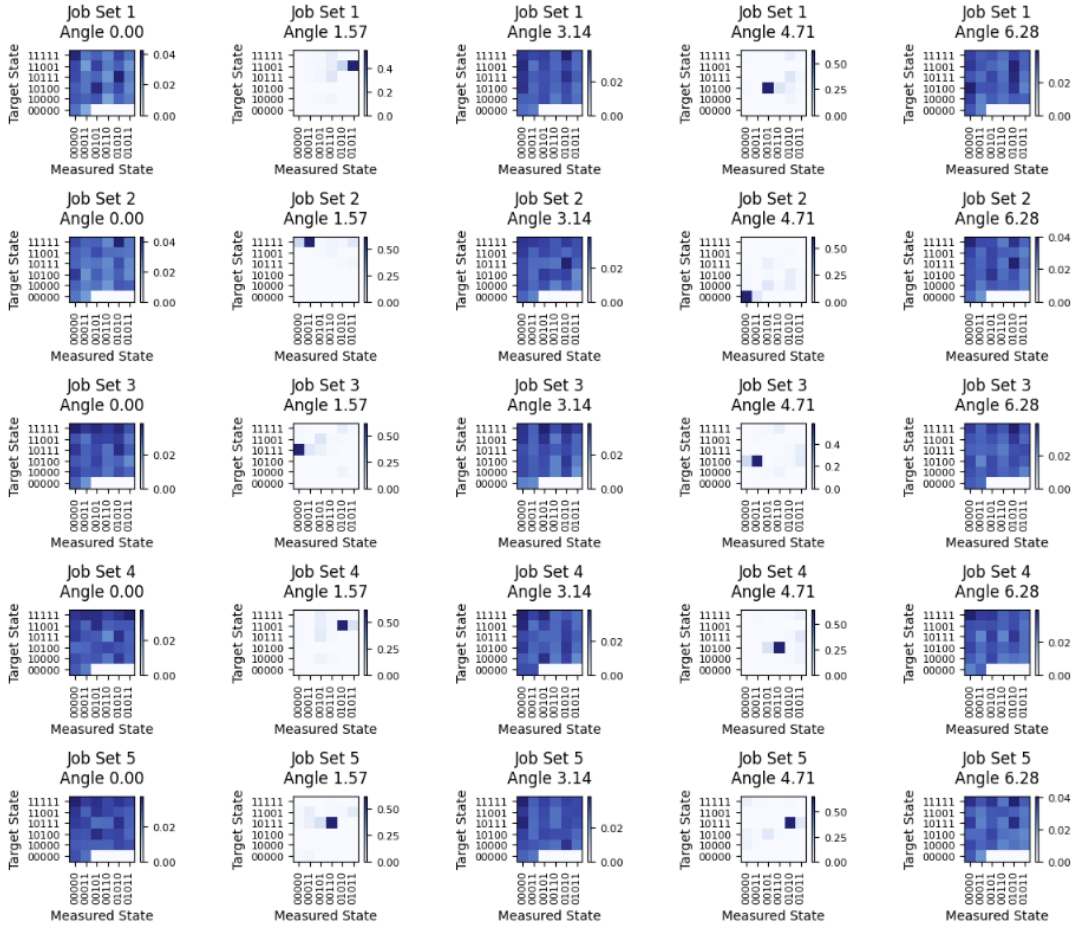


ibmq_lima



Continued..

ibmq_quito



Summary

- Implementing PUF technology in Quantum Computers which are noisy is a challenging task due to Qubit's nature of decoherence.
- The interaction of Qubit with the environment can result in its decoherence.
- This can be addressed by increasing the number of samples and executing a greater number of jobs.
- We found that the problem with the execution of jobs on IBM quantum backends is that some quantum systems tend to get faulty and require maintenance which can disrupt the execution of jobs.
- This work has successfully evaluated PUF metrics from QPUF and generated responses from the design.

Future Research

- Improving the accuracy of the proposed QPUF design through various noise reduction techniques can be a direction for future research.
- Furthermore, the proposed work could be integrated with the QKD protocol to enable secure exchange of PUF keys using Quantum mechanics principles.
- Exploring the QPUF application in IIoT to improve the performance of IIoT devices in I-CPS
- Extending QPUF design to various areas of IoT-based applications with minimal tradeoffs.
- Exploring the feasibility of further development of QPUF designs using teleportation, decoherence, and other properties of Quantum systems.

Thank You !!