POST QUANTUM ENCRYPTION FOR BATTERY ENERGY STORAGE SYSTEMS (BESS)

PATERO
QUANTUM SECURE COMMUNICATIONS

TruGrid

Table of Contents

About TruGrid

TruGrid is a premier utility-scale engineering, procurement, and construction (EPC) contractor specializing in battery energy storage systems (BESS) and solar technology. Its mission is to connect customers and communities with reliable and valuable utility-scale clean energy projects. Based in Houston, Texas, TruGrid is at the forefront of North America's energy transition, offering integrated solutions that ensure the most profitable projects for customers. Proudly owned by Hull Street Energy, TruGrid is dedicated to advancing sustainability and leading the energy industry with a focus on excellence, safety, and reliability.

About Patero

Patero cloaks vulnerable network elements and makes data-in-motion indecipherable with quantum-resistant encryption. Patero delivers end-to-end protection for critical infrastructure, federal, and DoD networks. Its hybrid post-quantum security solution uses today's best encryption technology, which is hybridized with NIST's next-generation quantum resilient encryption algorithms.

Introduction

The Looming Cybersecurity Crisis in the Energy Sector

The United States electric grid is a vital national asset and mission-critical infrastructure, underpinning the nation's security, economic stability, and the daily lives of its citizens. Battery energy storage systems (BESS) are playing an increasingly important role in the grid, enhancing reliability, facilitating the integration of renewable energy resources, and optimizing grid operations. A BESS functions as a large-scale rechargeable battery that stores energy when it is abundant and releases it when demand peaks or renewable generation dips. This capability helps address the intermittency of renewable energy resources while supporting overall grid stability. Given their growing significance, it is imperative to secure BESS installations against potential cyberattacks, which could have severe consequences for grid reliability and the U.S. economy.

As battery technologies have advanced, so too have their applications and uses. Governments and regulatory bodies are increasingly emphasizing the importance of cybersecurity in critical infrastructure, including energy systems. Adopting advanced encryption standards aligns BESS with emerging regulatory requirements and future-proofs them against evolving standards. As

BESS growth becomes prevalent, they become part of the national energy critical infrastructure and therefore require robust cybersecurity measures to protect them from evolving threats. Traditional encryption methods will be insufficient to safeguard BESS operations and related data and operations from attacks and infiltration by quantum computing-powered threats, which are capable of breaking current security systems much faster than current computer capabilities. Post-quantum cryptography (PQC) is the solution. PQC incorporates cryptographic algorithms standardized by the National Institute of Standards and Technology that are resistant to quantum attacks.

This white paper explores the importance of securing BESS with PQC, the vulnerabilities of traditional encryption methods, and implementation strategies for integrating PQC into U.S. energy infrastructure.

What happens when cybercriminals exploit encryption flaws? Imagine a quantum-powered adversary intercepting internet traffic protected by outdated encryption, gaining unauthorized access to energy grid controls. Such an attack could compromise critical infrastructure, leading to widespread disruptions or even nationwide blackouts.

This risk is particularly concerning for BESS, which is now integral to the electric grid and, by extension, the U.S. economy. As energy storage deployment accelerates across North America, reliance on stored energy is expected to increase. BESSs will become “critical infrastructure” on which communities and governments depend in cases of regional emergencies, as well as on which grid operators rely for grid stability. Ensuring the security of these systems is paramount. If not secured to the degree critical energy infrastructure is secured, BESSs become an attack vector for domestic and foreign terrorists. Advanced security technologies, such as post-quantum cryptography, are becoming essential to safeguard distributed storage networks and protect the grid from emerging cyber threats.

TruGrid has partnered with Patero to advance the development of a post-quantum secure customer BESS solution, utilizing Patero’s post-quantum encryption software.

Global Battery Energy Storage System Market

Global installed energy storage is projected to rise from just under 0.5 terawatts in 2024 to over 4 terawatts by 2040, representing a ninefold increase driven by BESS technology.[1] In 2023, new BESS installations reached 74 gigawatt-hours, up from 27 gigawatt-hours the previous year.[2] The chart visualizes this growth pattern, showing how the industry has accelerated dramatically in recent years and is expected to continue this trajectory through 2040.

The growth is being driven by declining battery costs, increasing renewable energy deployment, and the need for grid flexibility and energy security.

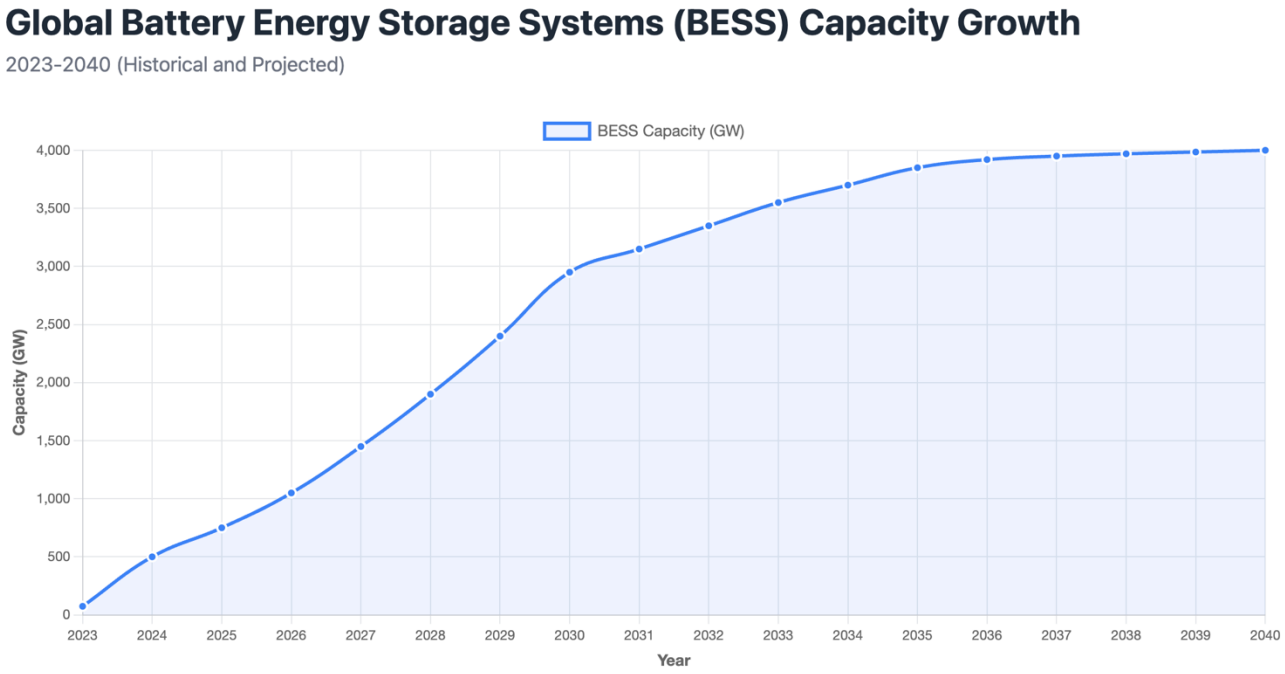

Figure 1 Global BESS Growth. Data Sources:
Primary Source: Rystad Energy (2024) - Energy Storage Outlook
https://www.rystadenergy.com/insights/whitepaper-energy-storage-outlook
Additional Reference: International Energy Agency (IEA) - Batteries and Secure Energy Transitions Report
https://www.iea.org/reports/batteries-and-secure-energy-transitions

[1] "Energy Storage Outlook". Www.Rystadenergy.Com, 2025, https://www.rystadenergy.com/insights/whitepaper-energy-storage-outlook. Accessed 2 Oct 2025.
[2] "Global new battery energy storage system additions 2020-2030". Www.Statista.Com, 2025, https://www.statista.com/statistics/1415439/battery-storage-system-installations-worldwide/. Accessed 2 Oct 2025.

Key Insights:

- • Rapid growth from 74 GW in 2023 to projected 4,000 GW (4 TW) by 2040
- • Steepest growth curve expected between 2024-2030 (averaging ~500 GW/year)
- • Growth rate moderates after 2030 as the market matures
- • Total capacity increases over 50-fold in this 17-year period

What is Post-Quantum Cryptography?

PQC is a set of software-based cryptographic algorithms specifically designed to withstand attacks from quantum computers. Unlike classic cryptography, PQC utilizes mathematical problems such as modular lattice-based "key encapsulation methods." These methods are believed to be extremely difficult for both classic and quantum computers to decode, ensuring long-term security.

Traditional asymmetric encryption methods have been proven to be easily decoded by powerful quantum computers and are, therefore, not quantum-resistant. Encrypted data that uses or will use asymmetrically generated encryption keys will be vulnerable to decryption by future quantum computers.

The Regulatory Push and Industry Awareness

U.S. National Security Memorandum (NSM-10) emphasizes the need for organizations to transition to quantum-safe cryptographic methods. The National Security Agency's (NSA) Commercial National Security Algorithm Suite 2.0 mandates compliance from critical infrastructure operators by 2030. While the North American Electric Reliability Corporation - Critical Infrastructure Program (NERC-CIP) has not yet commonly adopted PQC requirements, industry expectations suggest that such standards are under consideration as part of broader efforts to modernize grid cybersecurity.

Failing to implement PQC will leave power grids and BESS operators behind regulatory trends and, more importantly, expose critical assets to sophisticated cyber threats.

Understanding Post-Quantum Cryptography

The Rise of Quantum Computing and Its Threat to Security

Quantum computing could break the way we currently protect digital information. For example, Shor's algorithm, a quantum computing method, can quickly solve the math behind a Rivest–Shamir–Adleman (RSA) encryption. This normally keeps data safe because classical computers can't factor very large numbers. Likewise, quantum computers can crack Elliptic Curve Cryptography (ECC) encryption, which relies on the difficulty of solving certain math problems with curves.

Although large-scale, fault-tolerant quantum computers capable of breaking modern encryption are not yet available, progress is accelerating. In 2019, Google estimated that 20 million qubits would be required to efficiently break RSA. In 2025, Google revised that estimate downward by 95% to only 1,000,000 qubits.[3] IBM has solved the noisy qubit problem and will deliver Quantum Computing as a service from a full 200-functional qubit computer by 2030.[4] The Massachusetts Institute of Technology (MIT) extended the Oded Regev algorithm such that far fewer qubits with a higher tolerance to quantum noise would be required to factor integers.[5]

How PQC Works

PQC utilizes advanced cryptographic techniques, including lattice-based cryptography, multivariate polynomial equations, and code-based cryptography. These methods generate encryption keys that are resistant to the computational methods of quantum computers.

Traditional Encryption vs. PQC

Traditional network communications rely on encryption techniques that can be decrypted by quantum computers. Consider a cybersecurity breach in which an attacker intercepts encrypted internet traffic. That traffic can be decrypted later, likely within a few years, by using a future

---

[3] Matt Swayne. Google Researcher Lowers Quantum Bar To Crack RSA Encryption. (2025). Retrieved 5 August 2025, from https://thequantuminsider.com/2025/05/24/google-researcher-lowers-quantum-bar-to-crack-rsa-encryption/

[4] How IBM will build the world's first large-scale, fault-tolerant quantum computer. (2025). Retrieved 5 August 2025, from https://www.ibm.com/quantum/blog/large-scale-ftqc

[5] Adam Zewe | MIT News. "Toward a code-breaking quantum computer". 2025. News.Mit.Edu. https://news.mit.edu/2024/toward-code-breaking-quantum-computer-0823.

quantum computer. This "harvest now, decrypt later" attack is a serious concern for industries handling sensitive information, including power grids and BESS infrastructure. PQC prevents such vulnerabilities by utilizing encryption techniques resistant to quantum attacks.

Security in Addition to Firewalls

PQC is implemented in “hybrid” solutions, such as Patero’s CryptoQoR, which adds post-quantum cryptographic keys. These keys are combined with classic encryption keys to create “double-strength” cryptography. CryptoQoR secures communications through cryptographic tunneling, binding network access to device identity. CryptoQoR also adds a deeper layer of protection by enabling Zero Trust network architectures, which require continuous verification of every user, device, or connection.

In collaboration with partners such as TruGrid, Patero further implements cryptographic network segmentation by providing secure access across distributed environments. This cryptographic trust layer mitigates risk from “man-in-the-middle” attacks and unauthorized lateral movement, particularly in hybrid information technology/operational technology (IT/OT) or remote access scenarios.

Why PQC is Critical for Renewables & BESS

Growing Complexity and Increasing Vulnerabilities

Renewable energy plants operate at high levels of efficiency, are monitored remotely using machine learning for process optimization and predictive maintenance, and can be operated remotely for optimum efficiency. These capabilities require supervisory control and data acquisition (SCADA) systems and site-level sensors to connect with cloud-based and on-premises monitoring systems over the internet. These advanced systems inherently increase the plant attack surface, thus creating greater opportunities for data loss and man-in-the-middle attacks.

BESS: A Prime Target for Cyber Attacks

Utility-scale BESS are playing an increasingly important role by enhancing grid reliability and have become a component of our national critical energy infrastructure. Consequently, they are a target of cryptographic attacks. A successful cyberattack on these systems would compromise grid stability, leading to human suffering, financial losses, and grid instability.

PQC in Power Infrastructure: A Case Study

Partnership with Patero: Secure Grid Operations

Patero has pioneered a software PQC-based solution that enhances security without disrupting existing energy operations. The solution is targeted at industrial control operations and the management of critical assets.

Diagram: Secure Remote Access Architecture

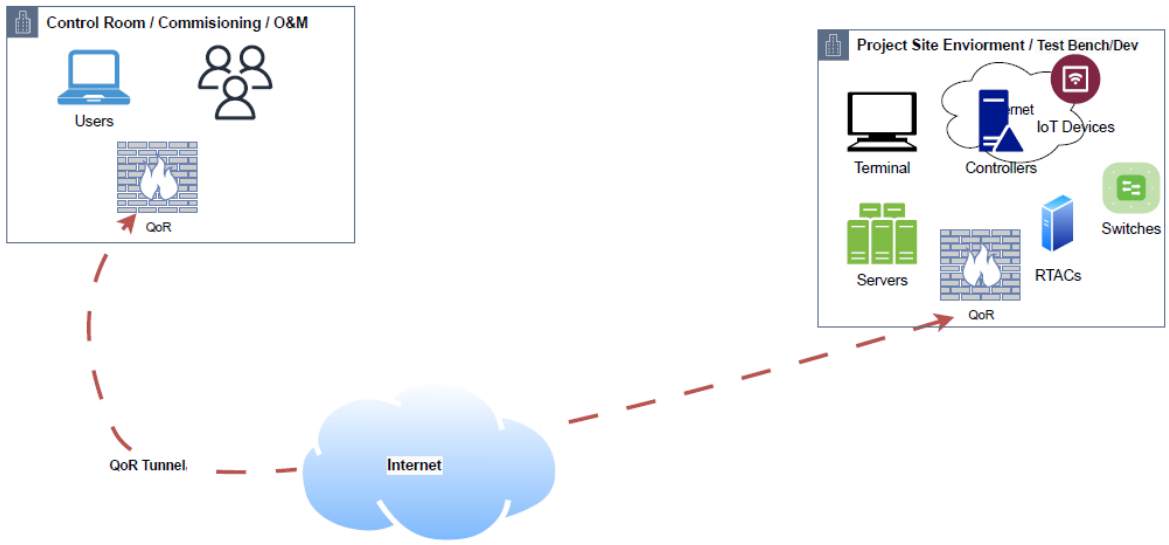

Figure 2: Post-Quantum Encrypted Tunnel, 'Patero QoR,' Protecting Remote Access Communications to a Project Site

Real-World Impact of PQC on BESS Operations

Making Remote Access Simple and Secure

PQC enables power plant operators and technicians to securely access BESS systems from anywhere. Patero's implementation of PQC creates "quantum private networks," which are tunnels, or secure pathways for data, protected by National Institute of Standards and Technology (NIST) standard post-quantum cryptography. Patero's implementation enables remote access and secure edge-to-anything data communication, eliminating the need for traditional virtual private networks (VPNs). By using a secure endpoint, such as Patero's CryptoQoR (QoR) software, a quantum-safe communication tunnel is established through the

internet. This ensures that all remote interactions remain encrypted and protected, even against future quantum-enabled attacks.

How It Works and What It Enables

Patero's solution creates an encrypted tunnel between external users and the BESS environment. Patero's solution enables Zero Trust networking such that the communicating devices are authenticated using "quantum certificates." Access to BESS environments can be managed using intermittent, session-based access to provide temporary access only active during approved intervals (e.g., support or maintenance). This Zero Trust and session-based access control ensures only trusted devices can request access and that the activity is further constrained by defined session intervals. This approach avoids the risks associated with "always-on" VPNs or static access credentials.

Key features include:

- Remote access via "quantum private network" tunnels, eliminating VPN complexity and improving trust
- Patero is protocol agnostic. It provides "protocol wrapping" to deliver a post-quantum cryptographic layer three "wrapping" of protocols such as MODBUS, MQTT, etc.

Rapid Deployment with Minimal Disruption

Patero's solution is software-based and hardware-agnostic, making it fast to deploy across different sites. Because the solution operates at Layer 3, wrapping existing SCADA or BESS protocols, no changes to existing control or data systems are required. An installation package is run at the edge gateway. Patero software running on the edge is used to configure connecting devices by generating a camera-readable quick response (QR) code or an importable configuration file. An outgoing firewall port configuration completes the installation and auto-connection of the configured remote devices.

Measuring Success

Operators know the implementation is successful when:

- Remote access works reliably with minimal change in latency or packet loss
- The attack surface of internet-exposed endpoints and internet protocol (IP) address ranges is reduced, and all network connection attempts by untrusted endpoints are ignored.

- Cryptographic inventories either report Patero-protected endpoints as Quantum Ready or do not detect them due to the cloaking effect of a reduced attack surface
- The solution integrates seamlessly without impacting operational workflows
- OT teams gain visibility and control over remote sessions
- Security posture improves, and the system is positioned to meet future regulatory demands

Optimized for industrial protocols and low-latency communication, Patero ensures efficient use of network bandwidth. Patero's CryptoQoR provides cryptographic enforcement of secure communications by encrypting data in transit and controlling access through identity-bound tunnels. CryptoQoR adds a layer of protection by ensuring that only authenticated and authorized devices can exchange data, which reduces exposure to attackers. This strengthens segmentation and supports micro-segmentation for tighter cyber control across IT/OT networks without altering existing firewall policies.

The following are performance expectations for a successful CryptoQoR implementation:

- **Enhanced Security**: Data integrity remains uncompromised. Patero's quantum-resistant encryption solution reduces the attack surface compared to traditional cryptographic solutions such as Transport Layer Security (TLS).
- **Minimal Latency**: Encryption overhead is negligible, maintaining real-time responsiveness required for grid operation, SCADA polling, and control signal delivery.
- **Ease of Deployment**: As a software-based solution, existing deployments can be easily upgraded with CryptoQoR to enhance the security of existing communication networks. Operators can go live within hours, minimizing downtime or technical friction.
- **Operational Compatibility**: Patero quantum private tunnels support communication protocols of operational technology tools such as Remote Terminal Automation Controllers (RTAC), Programmable Logic Controllers (PLC), and remote diagnostic platforms, without impacting the operation of these tools.
- **Network Performance Metrics**: Bandwidth usage remains within expected thresholds, and systems scale well with concurrent sessions, maintaining stable throughput and response times.
- **Regulatory Alignment**: PQC aligns with the NSA's Quantum-Safe Cryptography Roadmap. While current NERC-CIP frameworks do not yet mandate PQC, Patero's PQC solution positions infrastructure ahead of anticipated standards and strengthens TruGrid's short- and long-term compliance posture.

Conclusion: Why PQC is the Future of Energy Security

Post-quantum cryptography (PQC) offers energy operators a practical path to future-proof security. Here's how it strengthens networks, simplifies deployment, and enhances protection beyond traditional defenses:

1. Quantum-Resilient, Future-Proof Security

Patero's PQC fortifies energy networks against both today's advanced threats and tomorrow's quantum-enabled attacks. By adopting PQC now, operators stay ahead of regulatory mandates and demonstrate cybersecurity leadership in a high-risk, high-regulation sector.

2. Seamless Deployment with No Downtime

Designed for fast and frictionless integration, Patero's PQC solution overlays existing infrastructure—no forklift upgrades required. Its plug-and-play model enables secure remote access across IT/OT environments without disrupting operational continuity.

3. Defense Beyond the Firewall

Patero PQC adds a critical security layer beyond traditional firewalls. With built-in quantum-grade encryption, dynamic routing, and granular access control, it hardens internal communications and isolates critical systems from lateral movement—even if perimeter defenses are breached.