|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Paper (Year)** | **Domain / Scope** | **Algorithms / Techniques** | **Application to HRC / Industry 5.0** | **Strengths** | **Limitations** |
| Roadmap from classical cryptography to PQC in IoT (2023) | IoT migration security | Lattice-based (Kyber), Hash-based | Relevant for IoT devices in robot workspaces | Clear roadmap for PQC migration | Focused on IoT, not robot-specific |
| Securing IoT systems in a post-quantum environment (2022) | IoT authentication & encryption | Lattice-based schemes, hybrid PQC | Fits for cobot sensors/actuators in Industry 5.0 | Proposes hybrid auth protocols | Limited benchmarking on robotic hardware |
| Quantum-secure authentication & key agreement (2021) | IoT, communication protocols | PQ AKE protocols, Lattice-based, Code-based | Applies to robot–edge comms for safety | Comprehensive survey | Mostly theoretical, lacks implementation |
| Enhancing security of Internet of Robotic Things (2021) | IoRT, robotics networks | Blockchain, Encryption, IoT protocols | Direct to cobots & IoRT in factories | Integrates robotics + IoT security | PQC not deeply covered |
| Intelligent and secure Internet of Robotic Things (2022) | IoRT frameworks | AI-driven + encryption-based | Provides blueprint for secure HRC | Conceptual reference architecture | Doesn’t test PQC algorithms |
| Cyber security of robots: A comprehensive survey (2020) | Robotics cybersecurity | Threat models, comms channels (ROS, CAN, etc.) | Maps attack surfaces in HRC | Comprehensive robot threat taxonomy | Cryptographic solutions not detailed |
| Side-channel leakage assessment of CRYSTALS-Kyber (2022) | PQC implementation security | Kyber side-channel analysis | Useful for robot controllers using PQC | Practical embedded security insights | Focused only on Kyber, not system-level |
| Optimized Falcon Verify on Cortex-M4 (2022) | Embedded PQC performance | Falcon signature scheme | Directly applies to robot MCUs (controllers) | Shows PQC feasibility on resource-limited devices | Limited to Falcon, signature verification only |
| Securing IoT with Ascon-Sign (2023) | Lightweight PQC for IoT | Ascon-Sign (digital signature) | Fits into low-power robot sensors/updates | NIST-backed, lightweight | Still emerging, less tested in robotics |
| Quantum communication with RLP PQC in manufacturing (2023) | Industrial communication | RLP quantum-resistant crypto + QKD hybrid | Direct link to Industry 5.0 smart factories | Bridges PQC + industrial automation | Early-stage, little real-world deployment |

1. Roadmap from Classical Cryptography to Post-Quantum Resistant Schemes in IoT (2023)

This paper provides a comprehensive roadmap for transitioning IoT infrastructures from traditional public-key cryptography (RSA, ECC) to quantum-resistant alternatives. It focuses on lattice-based, hash-based, and code-based cryptographic families, analyzing their suitability for constrained IoT environments. The work emphasizes migration strategies and hybrid deployments that combine classical and PQC schemes during the transition. For Industry 5.0, it highlights how connected devices in robotic workspaces can maintain continuity and resilience against quantum threats.

2. Securing IoT Systems in a Post-Quantum Environment (2022)

This article investigates authentication and encryption protocols in IoT under the threat of quantum computing. It proposes a hybrid authentication protocol using lattice-based cryptography for key exchange, demonstrating how IoT nodes can balance performance and security. Its relevance to Industry 5.0 lies in adapting these PQC mechanisms to secure communication among collaborative robots, edge controllers, and cloud services.

3. Quantum-Secure Authentication and Key Agreement Protocols for IoT: A Survey (2021)

This survey reviews various quantum-secure authentication and key agreement (AKE) schemes designed for IoT. It compares lattice-based, code-based, and multivariate polynomial cryptography protocols, outlining their trade-offs in terms of security strength, computational efficiency, and scalability. Although theoretical, the survey provides a solid foundation for selecting suitable AKE schemes for human–robot collaboration, where low latency and robust security are critical.

4. Enhancing Security of the Internet of Robotic Things: A Review (2021)

This paper focuses on the Internet of Robotic Things (IoRT), where robots integrate with IoT and cloud systems. It reviews recent advances in securing robotic communication and coordination, emphasizing encryption, blockchain, and AI-driven approaches. The study is significant for Industry 5.0 as it directly addresses robot security in connected workspaces. However, it only mentions PQC tangentially, requiring further integration with quantum-resistant algorithms.

5. An Intelligent and Secure Internet of Robotic Things: A Research Agenda (2022)

This work proposes an end-to-end secure IoRT architecture integrating AI, cloud computing, and IoT security mechanisms. It emphasizes the need for dynamic threat detection, encrypted communication, and resilience in robotic networks. While PQC is not directly evaluated, the paper establishes a blueprint for secure robotic systems that can be extended with post-quantum layers, making it directly relevant for designing future Industry 5.0 collaborative work environments.

6. Cybersecurity of Robots: A Comprehensive Survey (2020)

This survey addresses cybersecurity threats unique to robots, such as vulnerabilities in Robot Operating System (ROS), industrial fieldbus protocols, and control architectures. It categorizes attack surfaces—sensors, actuators, communication networks—and provides countermeasures at the software and hardware levels. Though it does not cover PQC, its detailed threat models help identify the exact integration points where quantum-resistant cryptography should be applied in human–robot collaborative setups.

7. A Comprehensive Side-Channel Leakage Assessment of CRYSTALS-Kyber (2022)

This paper evaluates the side-channel resistance of Kyber, a NIST-selected lattice-based key encapsulation mechanism. It assesses information leakage in embedded implementations, focusing on power analysis and timing attacks. The results show possible vulnerabilities and countermeasures, making it highly relevant for secure deployment of PQC in robotic controllers and IoT devices that form the backbone of Industry 5.0 robotic workspaces.

8. Optimized Falcon Verify on Cortex-M4 for Post-Quantum Secure Embedded Systems (2022)

This research demonstrates optimized implementations of the Falcon signature scheme on ARM Cortex-M4 microcontrollers, commonly used in embedded robotic systems. It analyzes performance in terms of speed and memory consumption, proving that PQC algorithms can be practical even on resource-constrained devices. For Industry 5.0, this provides concrete evidence that lightweight robots and sensors can run PQC without significant performance trade-offs.

9. Securing IoT with Ascon-Sign (2023)

This paper explores the use of Ascon-Sign, a lightweight digital signature scheme recently standardized by NIST, for securing IoT communication. It highlights its suitability for low-power and constrained devices due to its small signature size and computational efficiency. In the context of human–robot collaboration, Ascon-Sign can be applied to secure firmware updates, robot authentication, and signed command messages in real-time operations.

10. Quantum Communication with RLP Quantum-Resistant Cryptography for Industrial Manufacturing (2023)

This article examines integrating quantum communication channels with quantum-resistant cryptographic protocols (RLP) in smart manufacturing systems. It bridges PQC and quantum key distribution (QKD), proposing a hybrid security layer for industrial automation. This is the closest match to Industry 5.0, as it directly addresses industrial manufacturing use cases with collaborative robotics, offering a practical roadmap for building quantum-resilient collaborative workspaces.