Institut für Steuerungs- und Regelungssysteme
Professur für Vernetzte Sichere Automatisierungstechnik
Univ.-Prof. Dr.-Ing. Mike Barth
Fritz-Haber-Weg 1 (Geb. 30.33), 76131 Karlsruhe

PQC for PKI in IACS
Or Why Nobody Will Implement It

Masterthesis

This thesis aims to evaluate current trends in Post-Quantum Cryptography (PQC) for Public Key Infrastructures (PKIs) in Industrial Automation and Control Systems (IACS).

Motivation

The Problem (a.k.a. "The Scary Part"):
While Industrial IoT devices are busy chatting across networks, current PKI security might soon become as useful as a chocolate teapot once quantum computers arrive. And here's the kicker, those devices have lifespans and innovation cycles longer than most celebrity marriages and in contrast are part of our critical infrastructure.
The Solution (a.k.a. "Your Thesis"):
You'll work on automating post-quantum certificate management for industrial systems. Previous research has shown that using Dilithium2 instead of classical ECDSA can make certificate request generation and response validation faster. Furthermore, Google and Cloudflare are going to start testing Merkle Tree Certificates for traffic using Chrome and talking to certain sites hosted on Cloudflare. But this won't include considerations for industrial plants.

Figure 1: PQC X.509 Certificate

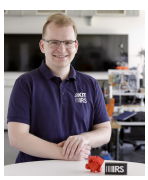
Goals

- Systematically analyze the gap between IT concepts and OT requirements
- Evaluate the impact on certificate management schemes
- Assessing composite certificate schemes that combine classical and post-quantum algorithms

Figure 2: Cloudflare Experiment

Interests and Helpful Prior Knowledge

- Basic understanding of PQC
- Interest in applied cryptography and industrial systems
- Motivation to get familiar with Industrial Automation



Supervisor
Marwin Madsen, M. Sc.
Build. 30.33, Room 118
Phone: 0721/608-42642
marwin.madsen@kit.edu

Thesis: Master
Date of Announcement: 03.03.2026
Tags: *Security, Industrial Control Systems, Post-Quantum Cryptograph, Publick Key Infrastructure*