講演番号	159

Strategic Aspect of Crypto Agility

Dennis Kengo Oka [1)] **Philipp Jungklass** [2)] **Claude-Pascal Stoeber-Schmidt** [2)]

1)IAV Co. Ltd., Uchikanda Chuo Bldg. 3F, 1-18-13 Uchikanda, Chiyoda-ku, Tokyo, 101-0047, Japan
(E-mail: dennis.kengo.oka@iav.jp)
2) IAV GmbH, Rockwellstr. 12, 38518 Gifhorn, Germany

KEY WORDS: **software and its underlying technologies, cybersecurity, quantum technology** PQC (E3)

The advancement of quantum computing poses a fundamental threat to the classical cryptographic algorithms relied upon across the automotive industry, including RSA and elliptic curve cryptography (ECC). These algorithms secure critical functions such as over-the-air (OTA) software updates, vehicle-to-everything (V2X) communication, digital key systems, TLS communications, charging communication via ISO 15118, and diagnostic access. Quantum computers capable of running Shor's algorithm at sufficient scale will render these mechanisms cryptographically insecure. Given that vehicles produced today must remain secure for fifteen or more years after the start of production (SOP), and that estimates for the arrival of a cryptographically relevant quantum computer (CRQC) converge around the mid-2030s, the industry faces a concrete planning imperative that cannot be deferred. The NIST Post-Quantum Cryptography (PQC) standardization process has already published its first three finalized standards covering ML-KEM, ML-DSA, and SLH-DSA, and the standardization landscape is maturing rapidly.

A common misconception is that the transition to PQC requires only algorithm replacement. In practice, as illustrated in Fig. 1, crypto agility encompasses a substantially broader set of organizational and technical dimensions. Algorithm replacement is the most visible but smallest part of the challenge. The more demanding dimensions include organizational readiness across engineering and management, a complete product-level cryptographic inventory covering all algorithms, protocols, and library dependencies, key management redesign to accommodate PQC key sizes and operational models, integration into resource-constrained ECUs operating under tight real-time and memory budgets, lifecycle and updateability planning to determine which assets can be migrated in the field versus requiring hardware replacement, and risk-based governance to structure prioritization decisions and track progress over time.

Not all vehicle components face equal quantum risk. Components relying on asymmetric key exchange or digital signatures face the most direct exposure. The OTA gateway, V2X PKI, telematics TLS sessions, digital key systems, and charging communication via ISO 15118 represent the highest PQC migration priority due to their reliance on asymmetric key exchange and digital signatures. ECU secure boot and UDS diagnostics carry medium priority, while internal CAN and Ethernet bus protection based on symmetric primitives carries low priority.

To address these challenges in a structured manner, this paper suggests a four-step framework for automotive PQC transition. The first step builds organizational awareness and alignment around the quantum threat, NIST PQC algorithm properties, and automotive-specific implications. The second step produces a complete cryptographic asset inventory across the product portfolio and ranks migration urgency by security function, lifecycle stage, and in-field updateability. The third step defines a multi-year, risk-based migration strategy covering phased roadmaps, hybrid versus pure PQC architectural decisions, hardware accelerator planning, key management redesign, and organization-level governance. The fourth step covers execution and validation for individual products, including PQC algorithm selection, library integration, performance benchmarking against ECU resource constraints, interoperability testing, and secure deployment via PQC-protected OTA mechanisms. Organizations that begin this process now, with the first three NIST PQC standards already finalized, will be well-positioned to achieve quantum resilience within the planning horizon that the vehicle lifecycle demands.

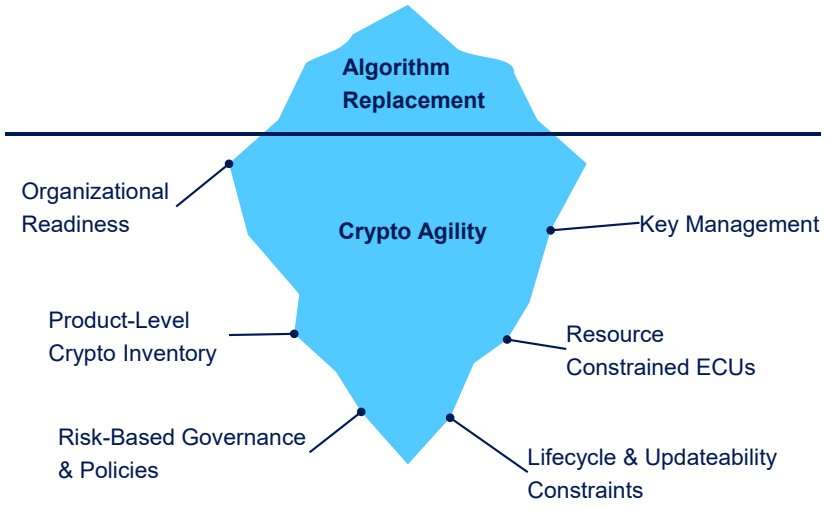

Fig 1. Crypto agility is more than algorithm replacement and requires strategic considerations.