DOI: doi.org/10.47363/JBRR/FinTech2025/2025(2)3

How RDH Uses Entanglement Emulation to Protect Smart Cards, POS Terminals and Digital Banking from AI and Quantum Threats

Chad Wanless

Software Programmer and Engineering Technologist, Canada

Abstract:

The global financial sector faces a perfect storm of emerging threats. Artificial intelligence is accelerating malware development and code decompilation, allowing attackers to reverse-engineer wallet apps and clone digital payment systems. At the same time, quantum computing is rapidly approaching the capability to break conventional encryption algorithms. Together, these forces threaten the very foundation of trust in online banking and e-commerce.

The Randomized Data Handshake (RDH) introduces a new defense model for FinTech: a quantum-resilient, zero-trust encryption protocol designed specifically for mobile banking, e-commerce, and POS transactions. RDH wraps around lightweight ciphers such as ASCON and AES, enabling two parties to authenticate and create identical session keys without ever transmitting those keys or any sensitive account data. In practical terms, RDH can process a credit card purchase without ever transmitting the credit card numbers or data—eliminating the most common point of theft in financial systems.

Unlike traditional software-based methods, RDH executes entirely within tamper-resistant hardware—smart cards, NFC tokens, or secure biometric dongles—ensuring that every cryptographic operation occurs only under explicit user control. A physical tap, button press, or fingerprint scan is required to activate a transaction. This architecture renders malware, spoofed apps, and relay-based fraud attempts useless because the handshake cannot be initiated or cloned without verified user presence.

For banks and payment providers, RDH offers a deployable path to quantum-safe, AI-resistant authentication that integrates directly with existing EMV, PCI-DSS, and ISO 7816 infrastructures. Benefits include:

- No transmission of sensitive card data or session keys
- Resistance to AI-based decompilation and code imitation
- Post-quantum resilience using existing symmetric algorithms
- Hardware-anchored two-factor authentication for wallets, POS, and banking apps

RDH achieves these protections with minimal computational overhead—using 160 to 256 bytes of bandwidth per handshake—making it ideal for real-time financial transactions and IoT payment systems.

As the industry prepares for the quantum era, RDH provides an immediately deployable bridge between today's infrastructure and tomorrow's threats. By removing data transmission from the encryption process itself, RDH restores what digital finance urgently needs most: trust without exposure