DOI: doi.org/10.47363/JAICC/ICAIC2025/2025(4)26

International Conference on
Artificial Intelligence and Cybersecurity (ICAIC 2025)

Conference Proceedings

November 27-28, 2025 (Virtual)

Trust Without Transmission: How RDH Uses Entanglement Emulation to Protect Digital Banking from AI and Quantum Threats

Chad Wanless

Software Programmer and Engineering Technologist with Experience in Developing Custom Tools for CAD Platforms Like AutoCAD, Canada

Abstract

As artificial intelligence accelerates, its capacity to reverse-engineer, decompile, and imitate software systems now poses a direct threat to the foundation of digital security. AI-assisted tools can already analyze compiled binaries, infer encryption logic, and reconstruct wallet or payment workflows that were once considered opaque. At the same time, quantum computing looms as the next existential risk to classical encryption. Together, these twin pressures demand a new paradigm—one that moves security out of software and into tamper-resistant hardware.

The Randomized Data Handshake (RDH) is a zero-trust encryption protocol engineered to counter both AI-based and quantum-based attacks. Acting as a lightweight wrapper around symmetric ciphers such as ASCON or AES, RDH allows two devices to derive identical session keys without ever transmitting them. Instead of sending secrets, RDH exchanges randomized challenge instructions that each side uses to construct keys locally, producing communication that contains no interpretable data in transit. This design not only removes the attack surface exploited by AI decompilation, but also emulates the information-exchange properties of quantum entanglement—where no usable key material ever leaves the device.

RDH is optimized for FinTech, IoT, and e-commerce environments where hardware constraints, latency, and trust boundaries intersect. It can be embedded in smart cards, NFC tokens, USB dongles, or dedicated processors, ensuring that all cryptographic operations occur within secure hardware under explicit user control. Biometric sensors or motion triggers confirm physical presence, preventing malware or spoofed applications from activating encryption without consent. Because it builds on existing symmetric standards, RDH offers quantum-resilient security with minimal computational overhead, avoiding the performance penalties of current lattice-based algorithms.

In an era where AI can read, clone, and manipulate code faster than humans can patch it, RDH redefines the trust model: software may be compromised, but hardware cannot be impersonated. The protocol transforms encryption from a passive defense into an active, user-anchored verification process—one that resists AI inference, survives quantum attack, and restores confidence in digital authentication.

By fusing AI awareness, zero-trust architecture, and post-quantum cryptography, RDH establishes a deployable framework for the next generation of secure communication—bridging the gap between hardware control and the AI-driven threat landscape.