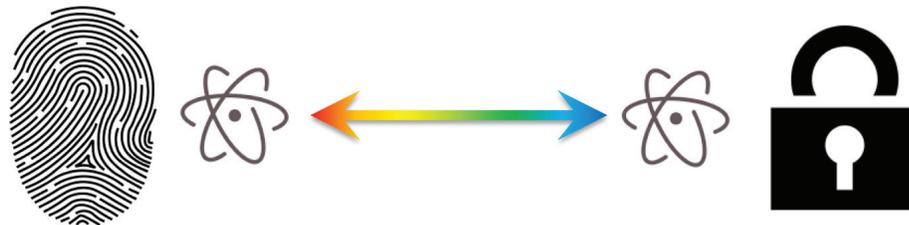


Patent Pending

SD# 14490

Technology Readiness Level: 2

Concept and/or application formulated



Secure Quantum Authentication is the ultimate protection for companies that provide and have a need for secure physical equipment assemblies, facilities such as banks using verification of keys for vaults, and any organization that relies on ID cards for secure access and use. This technology is different from others in that it is inherently protected from hacking and other forms of compromise.

Technology Summary

With the emergence of quantum computers and their exceptional computing powers, conventional authentication methods are vulnerable to cracking or bypassing the authentication process entirely. While the current cryptosystem technology of Elliptic curve cryptography (ECC) has made it harder to crack the private key needed for decryption, it requires a large number of complex calculations, leading to high energy consumption, but still leaves a chance for attacks. Secure Quantum Authentication is much more practical in preventing such attacks and successfully imposing a mandatory secure authentication process with bit-by-bit comparison, while realizing very low energy consumption and the opportunity to use less demanding processors.

Description

Secure Quantum Authentication relies on the uncertainty principle, which is fundamentally imposed by quantum mechanics. By initially pairing the authentic key generator and the user to generate a unique "fingerprint," the later identification involves quantum measurements that never allows information leakage due to the complete randomness of measurement. Only the key length amount of addition/subtractions in its calculations is needed.

TECHNICAL BENEFITS

- Immune to hacking and compromise - more secure
- Reduced computation demand - less demanding processors, smaller form factor
- Low energy consumption - reduced costs
- Reduction in code renewal frequency

INDUSTRIES & APPLICATIONS

- Weapons systems
- High value manufacturing environments
- Secure access facilities
- Information transfer through untrusted channels
- Financial transactions

 ip.sandia.gov
 ip@sandia.gov