Validating a Private-public Key Pair

This technology is a cryptographic method providing a new level of security for key-pair validation, securing both traditional and quantum-resistant protocols for key establishment. Public key validation is a well-known security practice for modern key establishment protocols. While necessary in many proposed post-quantum systems, post-quantum cryptographic algorithms generally do not support direct public key validation. Migrations of modern Internet peer-to-peer communication protocols, such as Internet Key Exchange (IKE) and Transport Layer Security (TLS) to quantum-resistant technology will require a new key validation technique to be secure.

POTENTIAL APPLICATIONS:
- Secure communications ( possono, web browsing, voice-over IP)
- onion core/fi ghting website

Frequency Estimation for Geolocation

This technology is an improved method of estimating the location of an emitter from received signals. This estimation is based on a combination of cross-spectral methods and LaGrange interpolation. This technology allows accurate estimation of emitter and frequency of received signals. The output provides distance for light-free (Li-Fi) applications or can simultaneously integrate observations from multiple receivers to improve accuracy.

POTENTIAL APPLICATIONS:
- Aeromedical, aerospace, air traffic
- Position tracking
- Internet of Things applications

Multilevel Chain of Trust and Revision

This technology is a device and method of multilevel chain of trust and revision that certifies each user, device, action, and circumstance in the creation, modification, and transmission of computer information, and includes a revision history of any modification. With chain of authority certifications give some assurance that transmissions were not altered by an unauthorized entity, this technology makes detection of unauthorized alterations of electronic information at a glance through the encryption and transmission levels, notifying users of any revisions made to the electronic information.

POTENTIAL APPLICATIONS:
- Enhanced computer security applications
- Intrusion prevention systems
- Computer forensics

Newest Additions to the NSA Patent Portfolio

Click here for a full listing of our patented technologies that are available to license.