SIMON and SPECK New Publication Update

In November of 2018, the International Organization for Standardization (ISO) published new standards (ISO/IEC 29167-21 and ISO/IEC 29167-22) for the use of the block ciphers SIMON and SPECK. The new standards were adopted for practical applications in the air-interface of radio frequency identification (RFID) technology.

Block ciphers such as SIMON and SPECK are designed specifically to operate in resource-constrained environments, like RFID. These standards are especially important to the RAIN (**RA**dio frequency **I**dentificatio**N**) global alliance that promotes the universal adoption of UHF RFID technology, in a similar manner to other adopted wireless technologies, like WiFi and Bluetooth. RAIN RFID is a wireless technology that connects billions of everyday items through the cloud (Internet of Things) for identification, location, authentication, and engagement.

RFID has important government and military applications in supply chain management and asset tracking. Vastly superior to barcodes, which require a direct line of site, RFID tags can be used to provide visibility into a supply chain or a collection of assets by logging items, together with relevant data about the items (maintenance history, environmental exposures, etc.) whenever they pass within the range of an RFID reader. RFID tags are severely constrained in both available circuitry and power, which makes securing them cryptographically difficult. But without cryptographic safeguards such as SIMON and SPECK and in particular, secure authentication protocols, tags can be impersonated, and the data which is shared by readers and tags is vulnerable to exposure or manipulation.

RFIDs have a variety of other use cases of interest to research, industry, and defense, where cryptography is an essential component. One example is access control (e.g., building entry). Another is wearable sensors (that communicate wirelessly) in military applications. There are many other current applications, and likely many new ones to come as industry further develops and matures the technology.

NSA is committed in its promotion of cybersecurity transparency and open source sharing of technological advancements. As such, it stands firmly behind the SIMON and SPECK algorithms and hopes that they will continue to contribute to improved security for constrained devices. NSA has funded prototyping efforts to explore U. S. National Security Systems use on such platforms.

For more information, please see https://nsacyber.github.io/simon-speck.