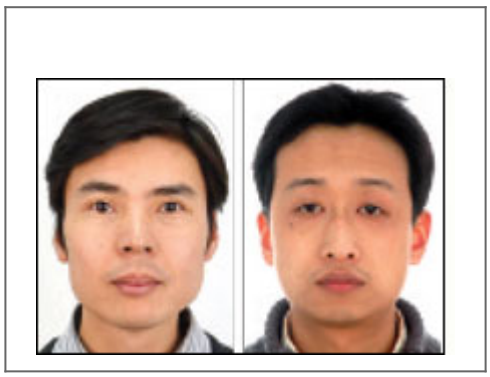
Encrypt Instead of ‘Kill’

Many companies are using RFID tags with Electronic Product Codes to track goods for supply-chain management. Some businesses are also employing EPC RFID tags to thwart counterfeiting and for product authentication. But these tags do not use on-chip cryptography algorithms to enhance security, because cryptography algorithms would draw too much power, impeding the long read ranges and high read rates

needed to track items in the supply chain.

EPC RFID tags can be disabled at the point of sale (POS) using a “kill” command, to protect consumers’ privacy. But that means the tag can no longer be used to access information about the product, or to manage warranties, returns and end-of-life applications.



At the Auto-ID Lab at Fudan University, we have developed a dual-mode EPC tag that addresses both issues. It has an on-chip cryptography algorithm and can work in either normal EPC mode or secure mode. When a dual-mode EPC tag is used for supply-chain management, the on-chip crypto engine is shut down to save power and the tag behaves just like any other EPC tag. Then, at the POS, using a “crypto-en” command, the tag can be changed to secure mode, in which the crypto engine is enabled. Just like the kill command, the crypto-en command is not reversible. But in the secure mode, consumers can access information on the tag.

We implemented different crypto engines for RFID tags, including Tiny Encryption Algorithm, International Data Encryption Algorithm, Hummingbird 1 and 2, and Advanced Encryption Standard. Mutual authentication protocols and channel encryption methods are applied for secure tags. The secure tags have a much higher power consumption than conventional EPC tags, reducing read ranges to less than 10 centimeters (4 inches). Consumers can use handheld or mobile devices to read the tags at a relatively short range, making

it unlikely that someone nearby could surreptitiously read the tag.

We also have developed a low-power, low-cost EPC reader system-on-chip that can be easily embedded in mobile phones, using a common serial communication interface. The highly integrated chip, manufactured using complementary metal-oxide semiconductor (CMOS) technology, includes a transceiver, protocol processor, microcontroller and power amplifier. EPC-enabled mobile phones can verify tags with the support of a trusted scalable service platform, which can be maintained by a third party.

Most mobile phones eventually will be equipped with Near-Field Communication (NFC) technology for payment and other short-range applications. The dual-mode EPC tag can coexist with NFC, so consumers will be able to use their mobile phones to access information about tagged products.

The prototype system is scheduled for demonstration in October, at the Internet of Things 2012 conference, in Wuxi, China.

Junyu Wang and Xi Tan are associate directors of the Auto-ID Lab at Fudan University, in Shanghai, China.

- Follow