Authentication in Ubiquitous Devices

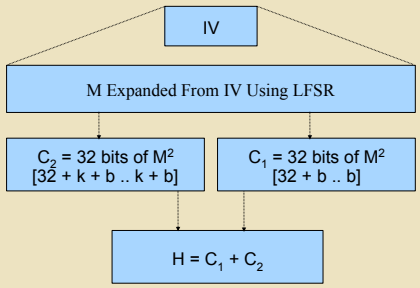
Serge Zhilyaev, Kevin Fu, Wayne Burleson
University of Massachusetts, Amherst

rfid-cusp.org

RFID Authentication Scheme on Intel's WISP

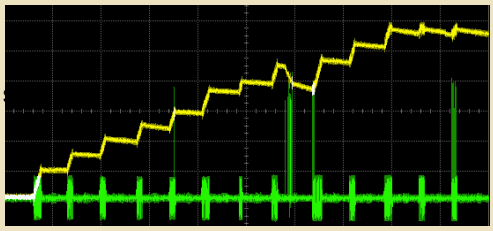
The Authentication Scheme

- An authentication scheme proposed by Adi Shamir that uses a novel hash function called SQUASH
- Reader and tag share a 64 bit secret S
- A 64 bit challenge R is issued by the reader
- Tag returns H(R xor S)
- Reader verifies tag's knowledge of S by computing H(R xor S)



The Hash Function

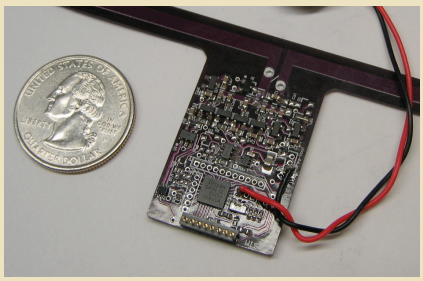
- Returns a subset of bits from c where $c = m^2 \bmod n$
- Words of m are generated from an IV = R xor S using a LFSR with a length of processor word
- A modulus of the form $2^k - 1$ allows the calculation of $m^2 \bmod n$ with no modular operations since $2^k = 1 \bmod n$
- Calculating a bit requires carry-in which is approximated by computing the carries of up to 11 previous bits. In addition to carry some shifts are required to align the bits in word chunks.



The yellow trace shows the charge on the WISP's capacitor as a function of time. The device can run on passive power by cycling through sleep and computing stages.

INTEL'S WISP

- MSP430 F1232 powered by UHF scavenging
- Emulates RFID gen 1 protocol
- 256/256/8k Bytes of RAM/FLASH/ROM
- No hardware multiplier



A WISP with the PCB antenna and "after market" buzzer not shown

- Due to the tiny memory available (256 Bytes total volatile memory including registers and peripherals) difficult to run some crypto algorithms at all on the WISP
- RC5 possible on WISP: comparing SQAUSH on the WISP to a CBC-MAC using RC5 as the CB and substituting H(R xor S) with CBC of R and S broken up into 32 bits yields comparable execution times but the SQUASH version has smaller RAM footprint, smaller code size, and no key setup
- Suitable for both sensor network node type devices and RFID tags as the design can be serialized

References
"Maximalist Cryptography and Computation on the WISP UHF RFID Tag" RFIDSec, 2007.
"Design of a passively-powered, programmable platform for UHF RFID systems." IEEE International Conference on RFID 2007.
"A wirelessly-powered platform for sensing and computation." Ubicomp, 2006.
"SQUASH: A New One-way Hash Function With Provable Security Properties for Highly Constrained Devices such as RFID Tags" Adi Shamir, presentation notes.

National Science Foundation WHERE DISCOVERIES BEGIN
This work made possible thanks to NSF