Feasible Privacy for Lightweight RFID Systems

David Evans
work with Karsten Nohl
University of Virginia

SPAR Seminar
Johns Hopkins University
17 October 2007

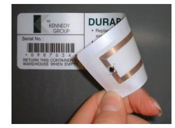
	UPC Bar Code	EPC Gen 2 RFID
		
Identities	8-12 digits (product identity)	64-128 bits (item identity)
Reading	Optical Scanner	Wireless Reader
Tag Cost	Ink, Paper ($0.00001?)	Circuit, Antenna ($0.05)

Photo by Bill Bryant

Protest at Texas Wal-Mart

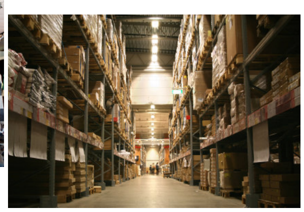
"More-Efficient Mugging"

"Just in case you want to know, she's got 700 Euro and 8 World Cup tickets..."

From Ari Juels USENIX Security 2004 talk
http://www.usenix.org/events/sec04/tech/slides/juels.htm

Realistic Threats

Profiling/Tracking



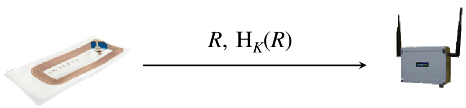
Corporate Espionage

Solutions for Paranoids

RFID Shield ($9.99)

Tin Foil

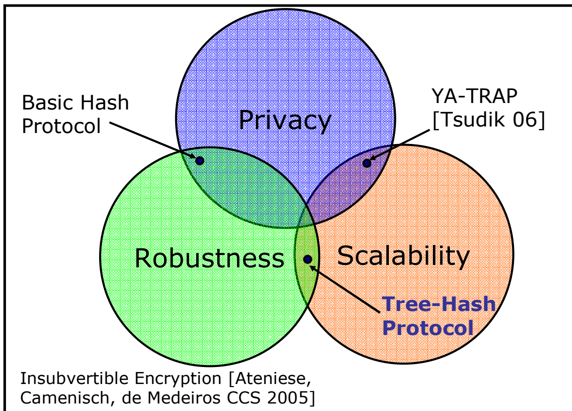
Basic Hash Protocol



key: K
nonce: R

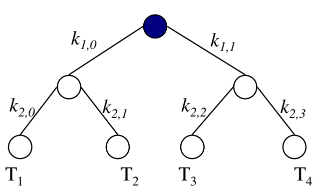
N tags
N hashes

Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. *Security in Pervasive Computing*, March 2003



Tree-Hash Protocol

David Molnar and David Wagner. CCS 2004.



Basic Hash Protocol at each level

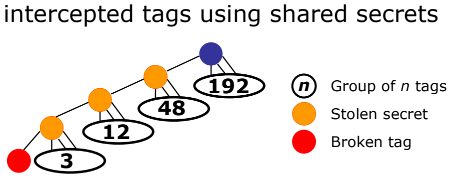
Reader computes up to $b \log_b N$ hashes

Analysis of Tree Protocol

- Attacker wants traces of individuals
- Attacker can easily acquire tags and break their secrets
- Assume no side channels: only protocol layer leaks
- Assume a good cryptographic hash function
  - Second part of the talk is about whether this is reasonable

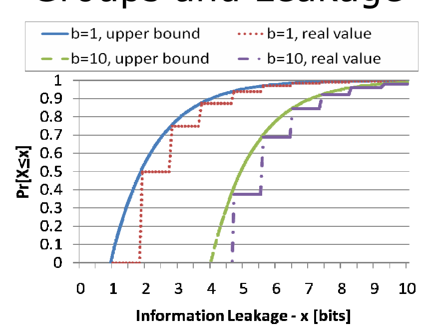
Shared Secrets

Each broken tag enables attacker to group intercepted tags using shared secrets

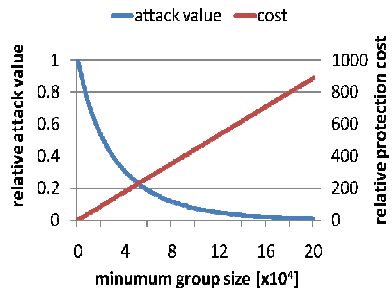


Information theoretic measure of privacy based on the group size

Groups and Leakage

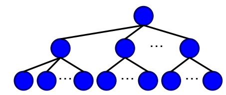


Cost Trade-Off



Low-Leakage Tree Protocol

- Avoid small groups
- Leads to two-level tree for systems with billions of tags
- Opposite of originally proposed binary tree



Reader computes up to $\sqrt{N}$ hashes

1B tags ~ 31K hashes

Tree-Hash Protocol Feasible?

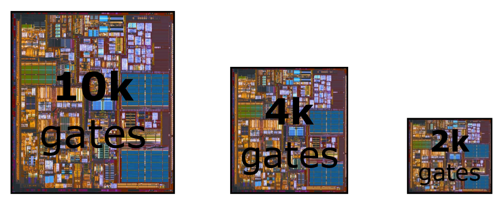
- Random Number

> An RN16 drawn from a Tag's RNG... shall not be predictable with a probability greater than 0.025% if the outcomes of prior draws from the RNG, performed under identical conditions, are known.
> *EPC Class 1 Gen 2 Standard*

~12 good bits out of 16

- **Hash function** (rest of this talk...)

Implementing Hash Functions



SHA-256 AES RFID tag

Power consumption scales with gates, not "Moore's Law".
Reading distance is inverse square-cube of power needed.

Cryptographic Hash Functions

Not sufficient for privacy!

- Pre-image resistance
  - Given $\mathbf{H}(x)$ it is hard to find x

Not necessary for privacy!

- Second pre-image resistance
  - Given y hard to find x such that $\mathbf{H}(x) = y$
- Collision resistance — Hardest
  - Hard to find x and y such that $\mathbf{H}(x) = \mathbf{H}(y)$

Non-Private Strong Hash

$$\mathbf{H}(x) = \mathbf{G}(x) \parallel x$$

where $\mathbf{G}$ is a strong, cryptographic hash function

Private Hash Function

$\mathbf{H}(R,K)$

R: (non-secret) nonce

K: key shared with reader

- **Correctness**: given $\mathbf{H}(R,K)$, R, and key set easy to find K
- **Privacy**: given a set of <$\mathbf{H}(R,K)$, R> tuples it is hard to identify two tuples generated by the same key (without knowing key set)

Abstract Design

$\mathbf{H}(R, K) = \mathbf{D}(R_1, K_1) \oplus \cdots \oplus \mathbf{D}(R_n, K_n)$

where

$R = R_1 \parallel \ldots \parallel R_n$

$K = K_1 \parallel \ldots \parallel K_n$

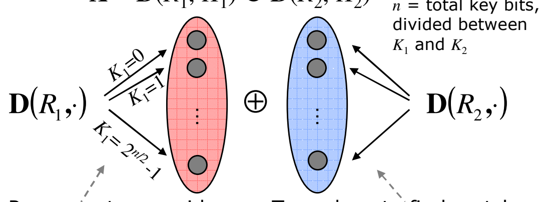
independent nonce/key shares

$\mathbf{D}(r, k)$ is a "Distortion Function" with:

- Even output distribution
- Black-box function with poly-time reversing oracle that outputs set of k's producing a given output

Security Argument: 2-split

$\mathbf{X} = \mathbf{D}(R_1, K_1) \oplus \mathbf{D}(R_2, K_2)$



Brute force attack: $\Theta(2^n)$

Meet-in-middle attack: $\Theta(2^{n/2})$ space, time

Concrete Abstract Design

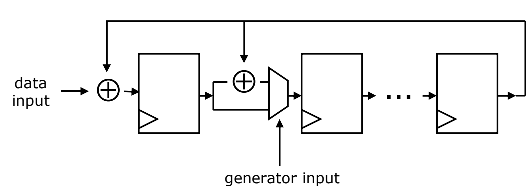
- 3-split: $\mathbf{D}(R_1, K_1) \oplus \mathbf{D}(R_2, K_2) \oplus \mathbf{D}(R_3, K_3)$
- Implementable Distortion Function
  - Even output distribution
  - o Black-box function with reverse oracle
  - ➔ Implementable function such that attacker cannot find correlations: no easier way to break than by finding the intermediate values

CRC

- Cyclic Redundancy Check
- Already required on EPC tags
- Designed [Peterson, 1961] to be easy to implement in hardware, error-checking code (no crypto goals)

$\mathrm{CRC}_g(X)$ = remainder of polynomial division X by g in GF(2)

Implementing CRC



Attempted CRC Privacy Protocol

Nguyen Duc, Park, Lee, and Kim. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. *Symposium on Cryptography and Information Security*, 2006.

$$\text{Tag} \rightarrow \text{Reader} : R, \text{CRC}(\text{ID} \parallel R) \oplus K$$

Fixed (standard) generator polynomial

K changes when updated by legitimate reader

CRC Properties

$$\exists x \in X_g = \text{set of values evenly divided by } g\text{:}$$

$$\mathbf{CRC}_g(X) = (X) \oplus x$$

$$A_1 = \mathbf{CRC}_g(K_1 \parallel R_1) = (K_1 \parallel R_1) \oplus x_1$$

$$A_2 = \mathbf{CRC}_g(K_2 \parallel R_2) = (K_2 \parallel R_2) \oplus x_2$$

$$x_1, x_2 \in X_g$$

CRC Does Not Provide Privacy

$x_1, x_2 \in X_g$ $\quad A_1 = \mathbf{CRC}_g(K_1 \parallel R_1) = (K_1 \parallel R_1) \oplus x_1$

$$A_1 \oplus A_2 = ((K_1 \oplus K_2) \parallel (R_1 \oplus R_2)) \oplus x_1 \oplus x_2$$

If two readings were from same tag:

$$A_1 \oplus A_2 \oplus (00 \ldots \parallel R_1 \oplus 00 \ldots \parallel R_2) = x_1 \oplus x_2$$

$$\text{CRC}_g(A_1 \oplus A_2 \oplus (00 \ldots \parallel R_1 \oplus 00 \ldots \parallel R_2)) = \underbrace{\text{CRC}_g(x_1 \oplus x_2)}_{0}$$

Otherwise, non-zero (with high probability)

Private Hash Function

$$\mathbf{D}(R_1, K_1) \oplus \overleftarrow{\mathbf{D}(R_2, K_2)} \oplus \mathbf{D}(R_3, K_3)$$

$$\mathbf{D}(r, k) = \mathbf{CRC}_{k_a \oplus r}(k_b)$$

Distortion Function Required Properties

- Confusion: changing one input bit flips each output bit with probability ½
- Diffusion: changing one generator bit flips each output bit with probability ½
- Even distribution: all outputs are equally likely
- Complexity: hard to correlate better than black box

Proof Sketches

- Confusion and Diffusion
  - Requires: Hamming weight of generator is ½ length
  - Proof: Follow bit probabilities through CRC
- Even Distribution
  - CRC provides even outputs over $[0, g\text{-}1]$
    - But not over all output bits
  - To get approximately even distribution: use only i low-order output bits, and combine outputs (second is reversed)

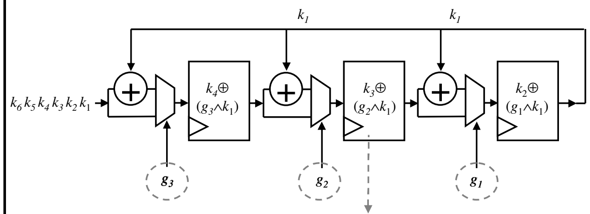
Attacks on Complexity

- Most known crypto attacks don't apply
- No chosen plaintext makes differential/linear cryptanalysis infeasible
  - Recall assumption: if attacker has physical access they can just extract key
- Statistical Attacks (e.g., distinguishing attacks) fail because output is evenly distributed and no state is kept

Algebraic Attacks

- Create and solve system of equations for bits
- Successfully break many stream ciphers (and some block ciphers)
- Even partial knowledge of single key bit can weaken privacy
- No general defense exists

3-bit CRC Complexity



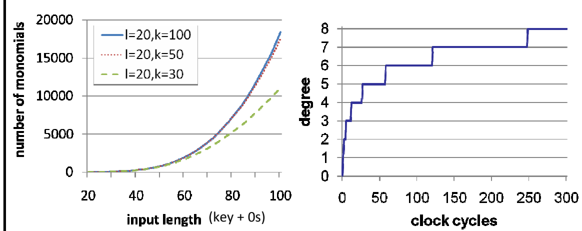
After 5 shifts:

$$H_{1,5} = k_1(g_1 + g_2) + k_2 g_1 + k_3$$
$$H_{2,5} = k_1(g_1 g_2 + g_3) + k_2 g_2 + k_4$$
$$H_{3,5} = k_1 g_1 g_3 + k_2 g_3 + k_5$$

Algebraic Attacks

- Difficulty depends on complexity:
  - Degree determines feasibility of linear system solving
  - Density determines possibility for simplifications
- Degree > 6 considered practically unsolvable [Courtois and Meier, EuroCrypt 2003]

Distortion Complexity



Shifting 250 times provides sufficient degree

Implementation

- CRC with fixed generator already included on tags (required by EPC Class 1 standard)
- Extend to support variable generator: 130 gates (355 total GE)
  - Smallest known AES: 3400 gates
- Reader: simple implementation can do 10x (AES) - 40x (SHA-256) as many hashes as alternatives

Summary

- Cheap RFIDs are expensive bar codes, not little computers
  - Can't do division, encryption, cryptographic hashing, etc.
- Privacy does not require strong crypto hashing
  - Very simple, inexpensive functions may be sufficient for privacy

"We cannot even answer the most basic questions because we don't know enough about you. That is the most important aspect of Google's expansion."

Eric Schmidt
(Google's CEO)
May 2007

For more information:
evans@cs.virginia.edu
http://www.cs.virginia.edu/evans

Karsten Nohl and David Evans. *Private Hash Functions: Lightweight Protection for RFID Systems.* (In submission, request by email)

Karsten Nohl and David Evans. *Optimizing Secret Trees for Privacy.* (In submission, request by email)

Karsten Nohl and David Evans. *Quantifying Information Leakage in Tree-Based Hash Protocols.* ICICS 2006.