

# Four Aspirations for RFID Security Research

Ari Juels

RSA Laboratories

1 April 2008

# Aspiration 1:

## Remember key management

- Number of papers on cryptographic protocols in RFID in 2007: 37
  - Privacy-preserving authentication protocols
  - Primitive designs
- Number of RFID Security papers in 2007 that treat key management: 0
  - Number in 2008?

# Aspiration 2: Start with problems, not tools

- Terms in *RFID Journal* articles on security:
  - Drug counterfeiting
  - Infant security
  - “Companies, Agencies Use Clandestine RFID Systems to Catch Thieves” (20 March 2008)
- Concepts in research papers:
  - Privacy-preserving tag authentication protocols
  - Cryptographic primitives in RFID tags
- E.g., privacy-preserving authentication
  - We have a linear bound on lookup cost for strong symmetric-key protocol [Damgård and Ostergaard (2006)]
  - How should we weaken privacy, not strengthen it? [Molnar and Wagner (2004)]

## Aspiration 3: Design systems for the RFID tags that people use

- < 40% of RFID tags sold in 2007 had strong crypto
  - Fraction will probably drop in 2008
- > 80% of research papers on RFID security assumed strong crypto
  - Fraction in 2008?

# Aspiration 4: Think practically about privacy

Here's  
Mr. Jones...



# Aspiration 4: Think practically about privacy



## ***TELL ME ABOUT YOURSELF - The Survey***

Name: **Amber**

Birthday: **March 28, 81 baby!**

Birthplace: **KU Med Center**

Current Location: **O-town (that's Olathe to those who aren't down) LOL**

Eye Color: **Green**

Hair Color: **Brown**

Height: **5'4"**

Right Handed or Left Handed: **Right**

Your Heritage: **Does anyone really care?**

The Shoes You Wore Today: **Shocks**

Your Weakness: **FIREMEN!!**

Your Fears: **Me...scared..ha...seriously**

Your Perfect Pizza: **Supreme**