Vulnerabilities in First-Generation RFID-Enabled Credit Cards

Kevin Fu

kevinfu@cs.umass.edu

Assistant Professor
Department of Computer Science
University of Massachusetts Amherst, USA
www.rfid-cusp.org

Berkeley
TRUST Seminar
March 22, 2007

Computer Science UMASS

Supported by NSF CNS-0627529

RFID Consortium for Security and Privacy

Outline of Today's Talk(s)

- **Real World: Security in RFID Credit Cards**

  ["Vulnerabilities in First-Generation RFID-Enabled Credit Cards" by Heydt-Benjamin, Bailey, Fu, Juels, O'Hare; Financial Crypto 2007]

- **Ivory Tower: Security of creative RFID crypto**

  ["Cryptanalysis of Two Lightweight Authentication Schemes" by Defend, Fu, Juels; IEEE PerSec 2007]

RFID Readers Everywhere

Japan Public Transportation

Current Balance

Entrance and exit date and station

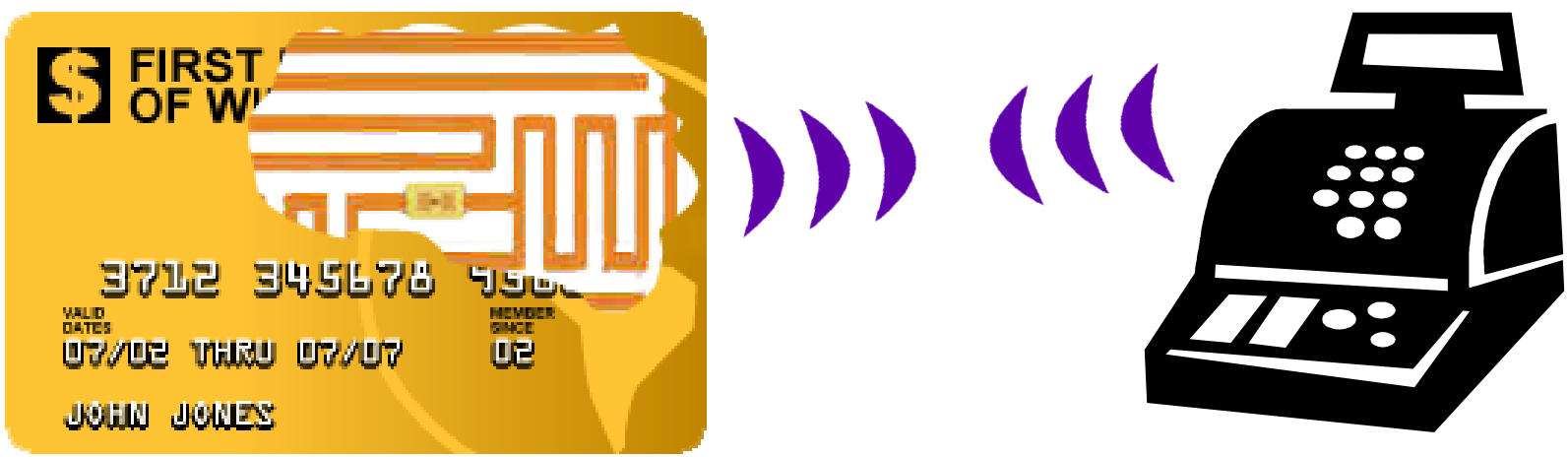
Details of merchandise purchase

Beginning Balance


SONY
FeliCa
Suica

What are RFID Credit Cards?

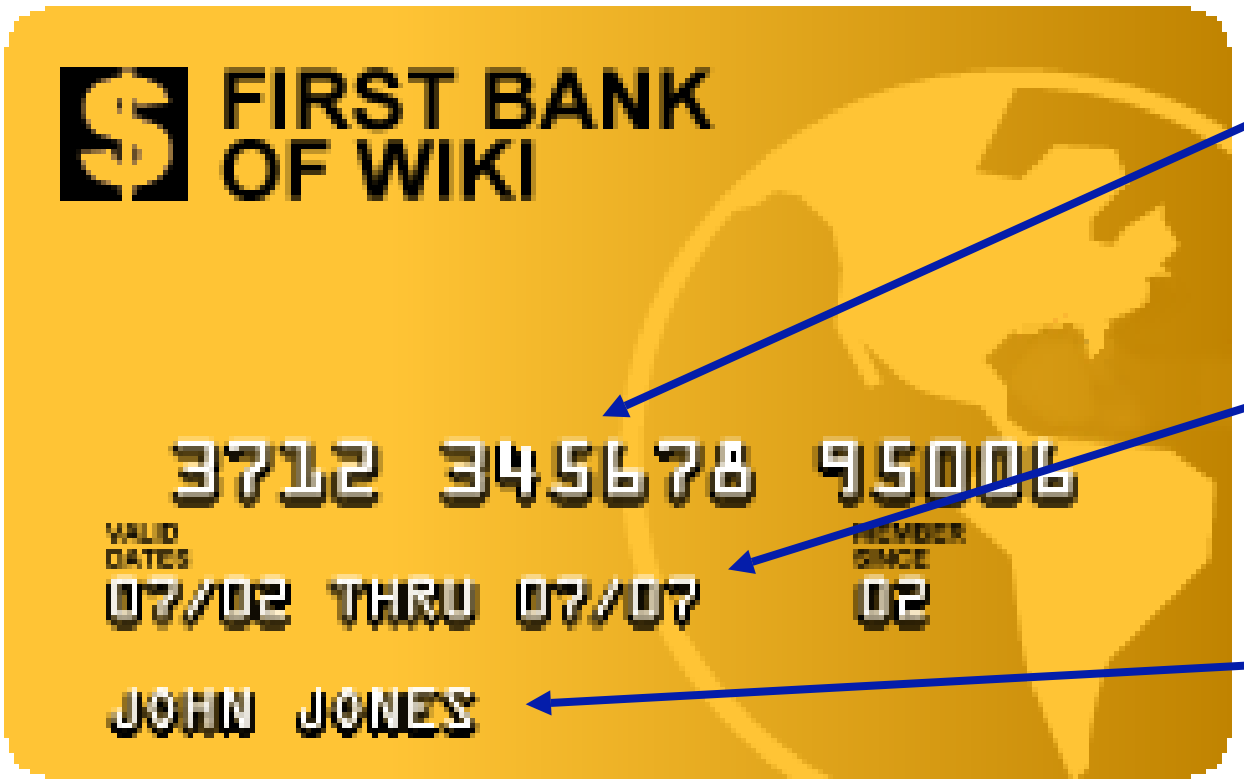
- Small mobile computing devices
- Transmit credit card information to reader over RF
- Passive 13.56MHz RFID transponder (ISO 14443-B)
  - Read range unknown, suspected to be around 10cm to 30cm
- "fastest acceptance of new payment technology in the history of the industry." [VISA; As reported in the Boston Globe, August 14th 2006]



Purchasing with an RFID CC

- Consumer authorizes purchase by bringing card near reader
- Some fraud can be detected or prevented by the network
- Charge processing networks are complex and heterogeneous
- This talk primarily considers the security of the RF transaction

What do RFID CCs Reveal?



Credit card number

Expiration date

Cardholder name

- One type of card uses an RF-only CC number
- Newer cards are beginning to withhold the cardholder name

Outline of Today's Talk(s)

- **Real World: Security in RFID Credit Cards**
  - Public perceptions
  - What vulnerabilities exist?
  - Experiments
  - Countermeasures
- Ivory Tower: Security of creative RFID crypto

What Vulnerabilities Exist?

- Disclosure of personal information on credit card
  - Financial fraud, but also
  - Distrust and lost consumer confidence
- Cross-Contamination
  - Data from RF transmission used in a different context
  - Example: A Web purchase

What Vulnerabilities Exist?

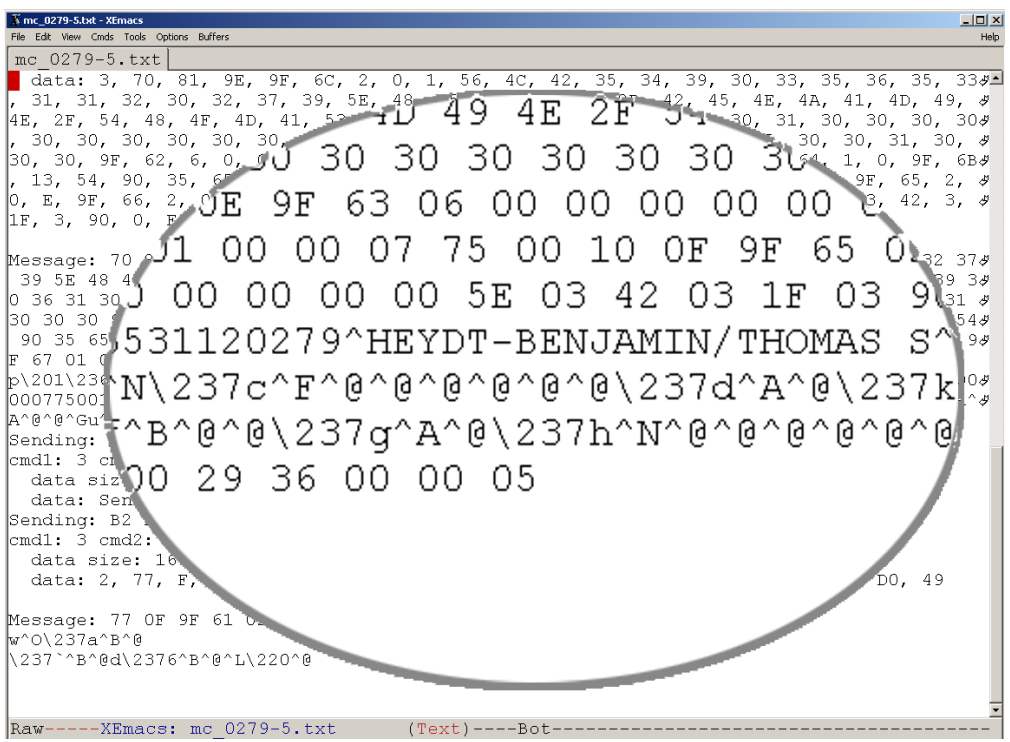
- Replay:

  Data obtained over RF are played back by adversary

- Relay:
  Queries from reader relayed by adversary to credit card without Alice's knowledge or consent
- Many other RFID privacy vulnerabilities [JMW05]

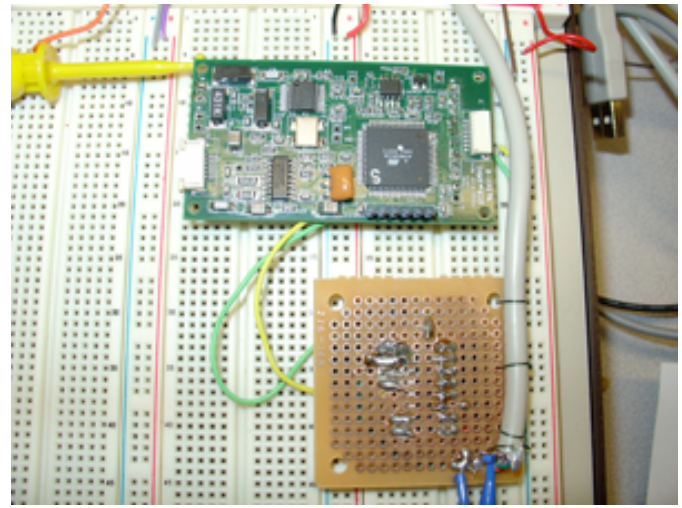
Eavesdropping

- Equipment: Antenna, oscilloscope, laptop, grad student
- Data disclosed before any challenge-response!
- No authentication of reader!



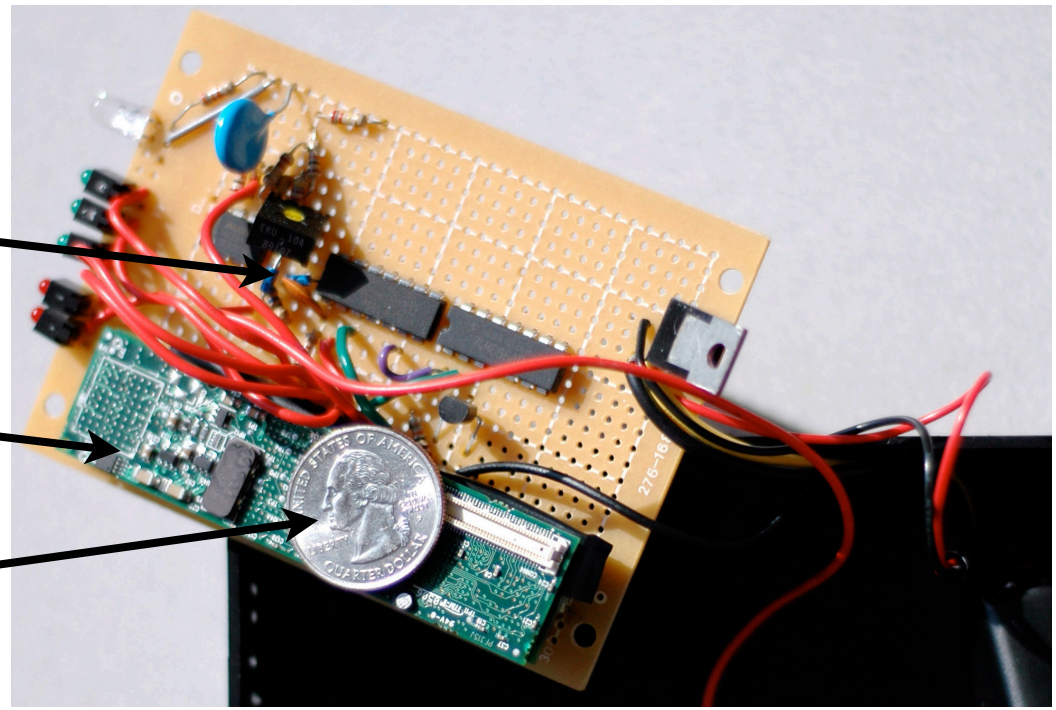
Cross-Contamination

- Disclosed PID sufficient for financial fraud?
  - Maybe…
  - CVC absent on RF, card face, mag-stripe
  - Collection of CVC varies
- But we bought toys with a skimmed card
  - New credit card in sealed envelope
  - Scanned with programmable reader
  - Address retrieved from phone book



Replay: Credit Card Cloning

- Some cards send static data w/ different transactions
- Our device below can replay these data
- Commercial readers accept the replay



Replay: Transaction Counters

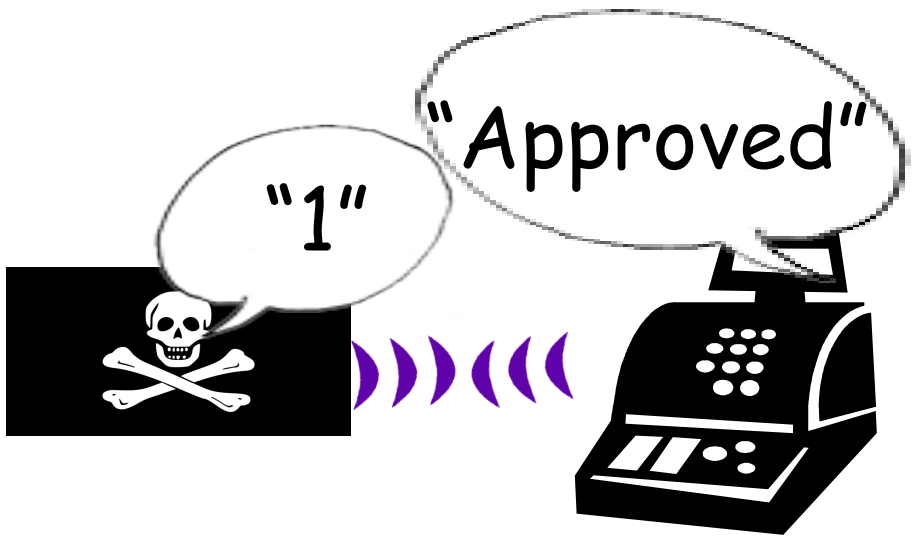
- Some cards use a transaction counter that increases with each RF transaction
- Transaction counter creates a race condition

Replay: Transaction Counters

- Under some circumstances counter prevents replay

Replay: Transaction Counters

- Some times the counter will not prevent replay



Replay: Challenge-Response

- Some cards use a challenge-response protocol
  - Details of algorithm unknown
  - Can protect against replay if back-end network is configured correctly
  - Challenge-response not used for protecting PID

Countermeasures

- The venerable Faraday cage
  - Does not protect during use

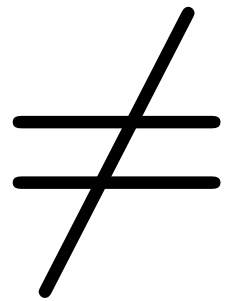
- Recent cards omit cardholder name
  - Caution: This lowers the bar on other attacks

Countermeasures

- Better use of cryptography
  - Some current cards may use cryptography
  - All we have seen transmit credit card data in the clear
- Smarter devices [Chaum 85]
  - Easier to assure user consent
  - More resources for cryptographic protocols

How to disable an RFID CC

Wireless threat model



Wired threat model

Summary of RFID CCs

- More convenient? (debatable)
- Good fraud control? (maybe)
- Consumer privacy? (not yet)

How to improve privacy

- Consumers need
  - ✓ Justified confidence
    - Not just "security theater" marketing
- Technology should be **open** to public scrutiny
  - RFID CCs use **proprietary** protocols
  - ✓ Ex: Secure Web sites use **public** protocols

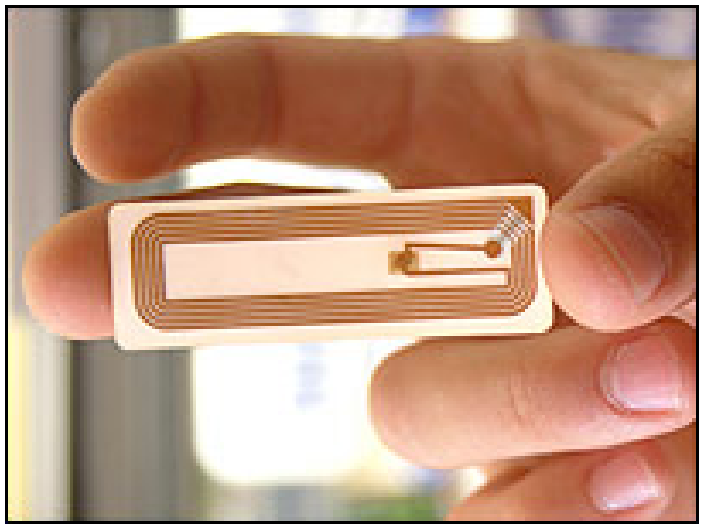
Outline of Today's Talk(s)

- Real World: Security in RFID Credit Cards

- **Ivory Tower: Security of creative RFID crypto**
  - **Protocol to authenticate a low-cost tag**
  - **Crypto being proposed without sufficient analysis**

Low Cost vs. Higher Cost

	Low Cost	Higher Cost
Storage	Few 100 bits	Few kB
Computational Capabilities	XOR, simple operations	RSA, AES, Triple DES
Cost	Few cents	Few dollars

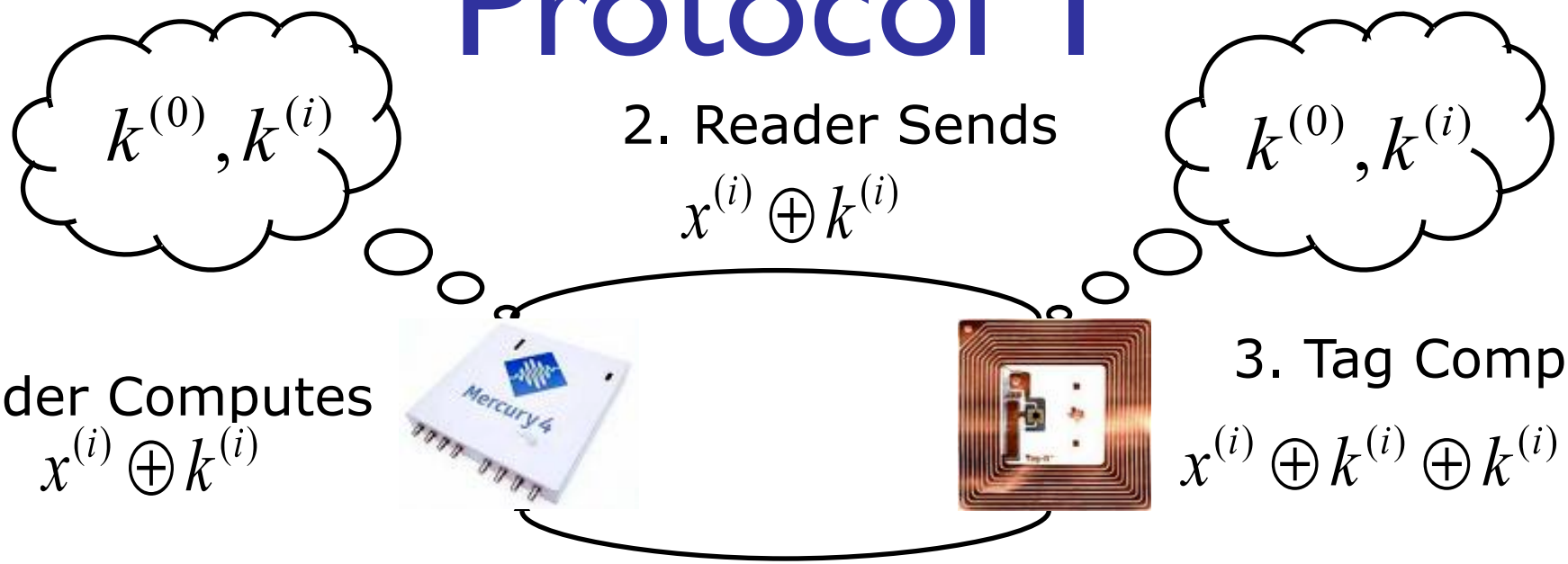


Vajda and Buttyán Protocol 1

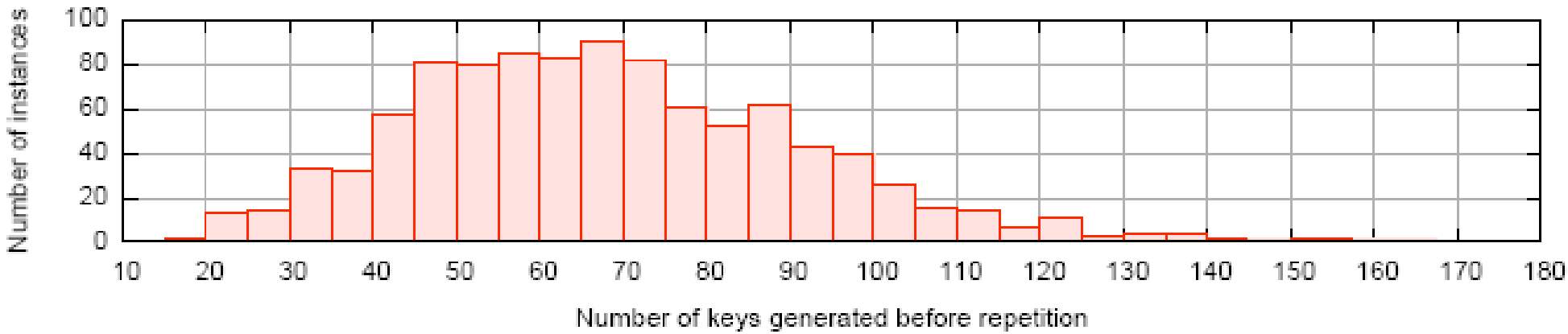
- Challenge/Response Protocol
  - Authenticates tag to reader
  - Evolves shared secret with XOR operations
  - Tag sends reader a function of evolving secret to authenticate
  - Think PRNG

["Lightweight Authentication Protocols for Low-Cost RFID Tags" by I. Vajda and L. Buttyan. In UBICOMP, 2003.]

Vajda and Buttyán Protocol I



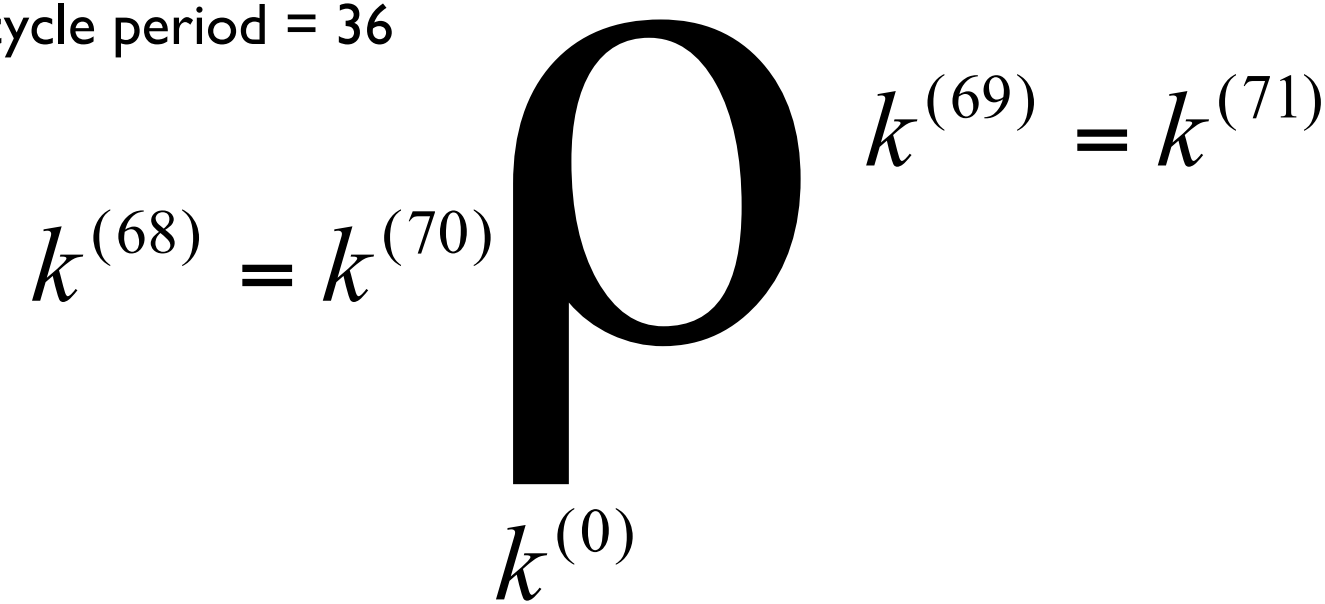
Key Repetition



- Average 68 transactions until 128-bit key repeats
- Average cycle length is 2 keys (the head of \rho)

Implementation Results

- With 128-bit key length and 1,000 trials with 10,000 sessions/trial
- After an average of **68 keys**, the session key **repeats**
  - Average: 68.7%, cycle period = 2, i.e. $k^{(i)}=k^{(i-2)}$
  - Minimum: 31.9%, cycle period = 1
  - Maximum: 0.1%, cycle period = 36



Implications of Repeated Keys Attack

- A passive eavesdropper can impersonate the tag after an average of:
  - 70 transactions if listening from start
  - 3 transactions if listening after 68th transaction
- Theoretical maximum before cycle:
  $16! \times 2 = 4.18455798 \times 10^{13}$ transactions
- But empirical measurement = 68

Conclusions on RFID S&P

- Real World: RFID credit cards
  - Disclose personal information
  - Vulnerable to replay and relay
  - Threat model not understood by industry
- Ivory Tower: RFID crypto protocols
  - There's a lot of squishy RFID crypto out there
  - Protocols failing statistical tests will never be cryptographically secure

RFID CC in Fiction