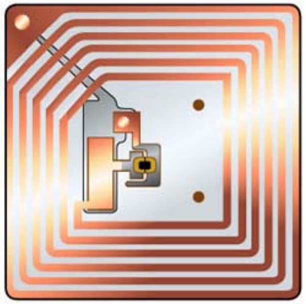
On the Security of RFID

Hung-Min Sun
Information Security Lab.
Department of Computer Science
National Tsing Hua University

What is RFID?

- Radio-Frequency Identification Tag



Reference

http://glossary.ippaper.com

Roles of RFID applications

Tags Reader Server(Database)

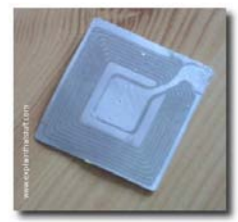
Barcode v.s. RFID

Barcode

1 30092 68125 9

- require a direct line of sight to the printed barcode
- have no read/write capability
- cheap

RFID



- can be read at much greater distances
- unique object id
- more expensive

Reference

www.cs.utexas.edu/~shmat/

Where Are RFID Used?

- Physical-access cards
- Inventory control
  - Gillette Mach3 razor blades, ear tags on cows, kid bracelets in waterparks, pet tracking
- Logistics and supply-chain management
  - Track a product from manufacturing through shipping to the retail shelf
- Gas station and highway toll payment
  - Mobile SpeedPass

Reference

www.cs.utexas.edu/~shmat/

Commercial Applications of RFID

- RFID cost is dropping dramatically, making it possible to tag even low-value objects
  - Around 5c per tag, $100 for a reader
- Logistics and supply-chain management is the killer application for RFID
  - Shipping, inventory tracking, shelf stocking, anti-counterfeiting, anti-shoplifting
- Massive deployment of RFID is in the works
  - Wal-Mart pushing suppliers to use RFID at pallet level, Gillette has ordered 500,000,000 RFID tags

Reference

www.cs.utexas.edu/~shmat/

Future Applications of RFID

- Location Awareness
- Health Care
- Apparel
- Smart Shelf

Reference

http://www.rfidjournal.com/

RFID Tag Power Sources

- Passive (this is what mostly used now)
  - Tags are inactive until the reader's interrogation signal "wakes" them up
  - Cheap, but short range only
- Semi-passive
  - On-board battery, but cannot initiate communication
    - Can serve as sensors, collect information from environment: for example, "smart dust" for military applications
  - More expensive, longer range
- Active
  - On-board battery, can initiate communication

Reference

www.cs.utexas.edu/~shmat/

RFID Frequency Ranges

- Low frequency (LF): (100~500KHz) 125 kHz, 135 kHz
  - Shortest read range < 50 cm, slowest read speed
  - Strong ability to read a tag on objects with liquid or metal components, Physical Access Control, Animal Identification
- High frequency (HF): (10~15 MHz), 13.56MHz
  - Read range < 1.5 meter, cheapest tag
  - Smart cards, smart shelves, health care
- Ultra-high frequency (UHF): (860 to 960) MHz
  - Read range 3~10m, faster read speed
  - EPC tags, supply chain systems
- Microwave: (> 1GHz), 2.45GHz, 5.8GHz
  - Read range 3~10m, fast read speed, most expensive
  - Supply chain systems, airline baggage tracking

Security Problems of RFID

- Eavesdropping
- Hot-listing
  - Attacker has special interests in certain items
- Replay attack
- Cloning
- Tracing
- Data forging
- Denial of Service

Fundamental problem:

Lack of mutual authentication

Challenges of RFID

- Low-cost tag costs US$0.05
- Limited computational ability and storage
  - Cannot implement common cryptographic functions on the tags
- Goal: Lightweight computation approaches for securing RFID
  - Lightweight mutual authentication protocols

However, RFID tag …

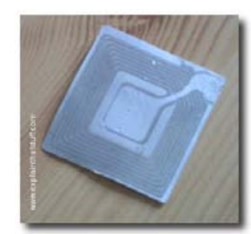
- No or very limited power
- Little memory
  - Static 64- or 128-bit identifier in current 5-cent tags
- Little computational power
  - A few thousand gates at most
  - Static keys for read/write access control
- Not enough resources to support public- or symmetric-key cryptography
  - Cannot support modular arithmetic (RSA, DSS), elliptic curves, DES, AES; hash functions are barely feasible
- Is resettable
  - Passive tag resets when power off

EPCglobal Class 1 Generation 2

- Most popular in long-range RFID applications
- Frequency: 860-960 MHz
- Reading range: 10-20 Feet
- ISO 18000-6C

Reader

RFID tag



Query →

← RN16 (16-bit random number)

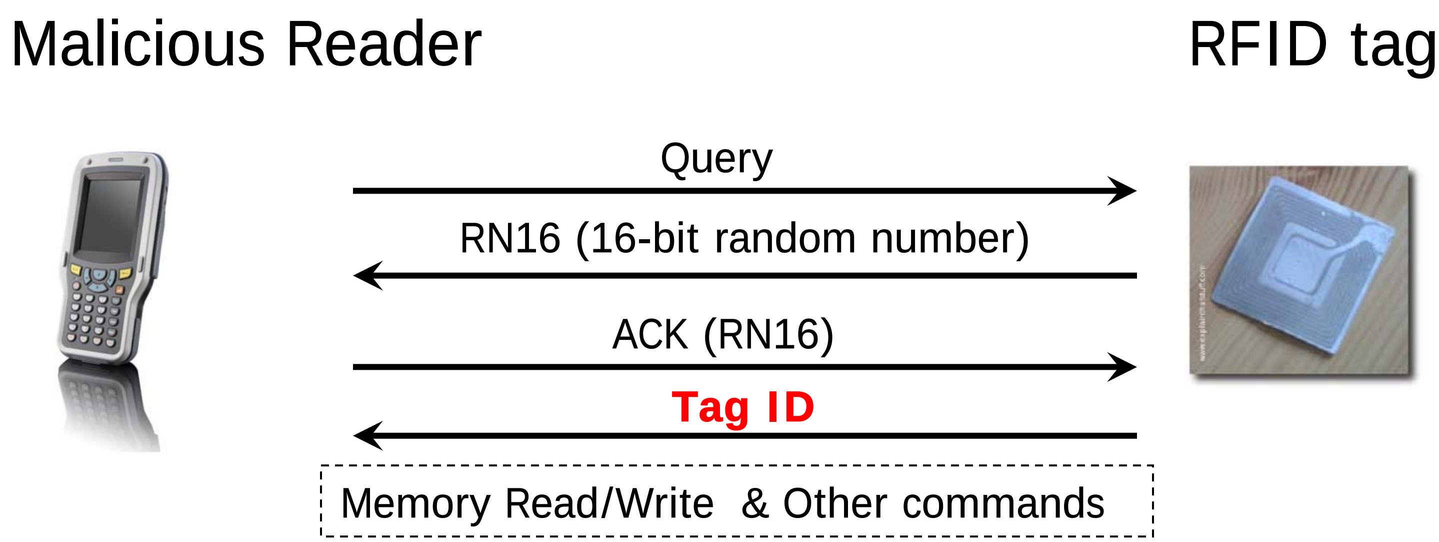
ACK (RN16) →

← Tag ID

Memory Read/Write & Other commands

Problems in EPCglobal C1G2

- Long reading range
- A naïve protection:
  - Use of 16-bit random number
- Tag ID is transmitted in plaintext
- Lack of "reader-to-tag" authentication



Secure Protocols for RFID

Secure RFID Protocols

Hash-based Approaches

- [1] S. Weis, “Security and Privacy in Radio-Frequency Identification Devices,” master’s thesis, Massachusetts Inst. of Technology (MIT), Massachusetts, USA, May 2003.
- [8] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic Approach to “Privacy-Friendly” Tags,” RFID Privacy Workshop, MIT, Massachusetts, USA, Nov. 2003.
- [9] T. Dimitriou, “A Lightweight RFID Protocol to protect against Traceability and Cloning Attacks,” Proc. 1st IEEE Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm ’05), Sep. 2005.
- [12] G. Tsudik, “YA-TRAP: Yet Another Trivial RFID Authentication Protocol,” Proc. 4th IEEE Int’l Conf. Pervasive Computing and Comm. (PerCom’06), Mar. 2006.
- [13] G. Avoine and P. Oechslin, “A Scalable and Provably Secure Hash Based RFID Protocol,” Proc. 3rd IEEE Int’l Workshop Pervasive Computing and Comm. Security (PERCOMW ’05), Mar. 2005.
- [14] D. Henrici and P. M¨ uller, “Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers,” Proc. First IEEE Int’l Workshop Pervasive Computing
- and Comm. Security (PerSec ’04), Mar. 2004.
- [36] Ohkubo, M., Suzuki, K., and Kinoshita, "RFID privacy issues and technical challenges," Commun. ACM 48, 9 (Sep. 2005).

Secure RFID Protocols

Lightweight Approaches

- [23] A. Juels, “Strengthening EPC Tags Against Cloning,” Manuscript, RSA Laboratories, Mar. 2005.
- [24] Y.C. Chen, W.L. Wang, and M.S. Hwang, “RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection,” Proc. 9th IEEE Int’l Conf. Advanced Comm. Technology (ICACT ’07), Feb. 2007.
- [25] A. Juels, “Minimalist Cryptography for Low-Cost RFID Tags,” Proc. 4th Int’l Conf. on Security in Comm. Networks (SCN ’04), Sep. 2004.
- [26] Y.Z. Li et al., “Security and Privacy on Authentication Protocol for Low-cost RFID,” Proc. Int’l Conf. Computational Intelligence and Security (CIS ’06), Nov. 2006.
- [27] P. Peris-Lopez et al., “M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags,” Proc. 3rd Int’l Conf. Ubiquitous Intelligence and Computing (UIC-06), Sep. 2006.
- [29] H.Y. Chien, “SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity,” IEEE T. Dependable Secure Comput., vol. 4, no. 4, pp. 337–340, 2007.
- [32] D.N. Duc et al., “Enhancing Security of EPCglobal Gen2 RFID Tag against Traceability and Cloning,”
- Proc. 3rd Conf. Symp. Cryptography and Inf. Security (SCIS’06), Jan. 2006.
- [35] A. Juels and S. Weis, “Authenticating Pervasive Devices with Human Protocols.” Crypto, Aug. 2005.

Security Analysis of RFID Protocols

	Hash-based Protocols							Lightweight Protocols							
	[1]	[8]	[9]	[12]	[13]	[14]	[36]	[23]	[24]	[25]	[26]	[27]	[29]	[32]	[35]
Tracing	‡	—	‡	‡	—	‡	—	‡	‡	—	$O(l^2)$	‡	‡	‡	‡
Skimming	‡	—	—	—	—	—	—	‡	‡	—	‡	‡	$O(2^{2l})$	$O(2^{16})$	‡
Spoofing	‡	—	‡	—	—	—	—	$O(q_J)$	$O(2^l)$	$O(2^{2L})$	‡	‡	‡	‡	‡
Cloning	‡	—	—	—	—	—	—	$O(q_J)$	$O(2^l)$	$O(2^{3kLm})$	‡	‡	$O(2^{2l})$	$O(2^{32})$	‡

q_J	size of PINSET	—	not possible	‡	constant time
l	bit length of pseudonym	m	security parameter		
L	bit length of one-time pad	k	number of pseudonyms		

So…
How to design a secure protocol for low-end RFID Tag?

Hung-Min Sun and Wei-Chih Ting,

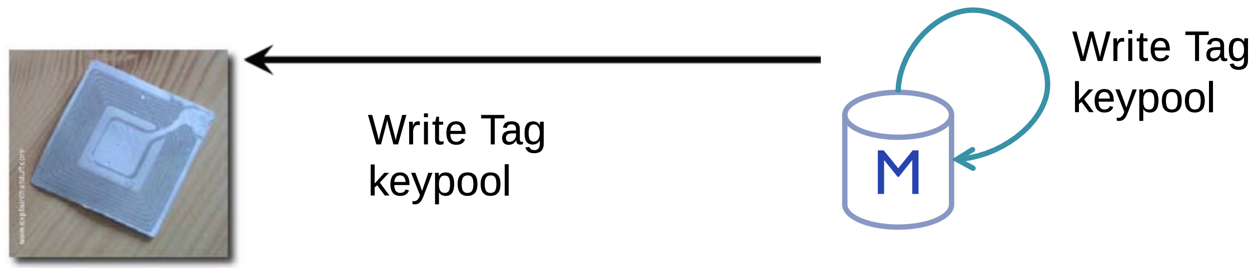
"A Gen2-based RFID Authentication Protocol

for Security and Privacy," *IEEE Transactions on Mobile Computing*, Vol. 8, No. 8, pp. 1052-1062,

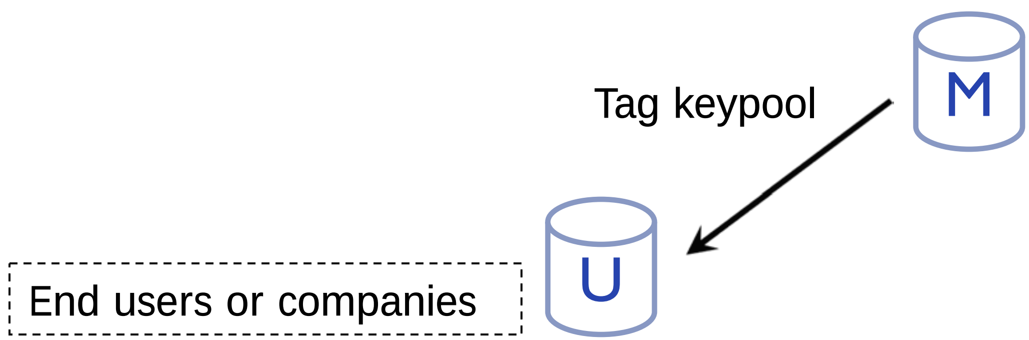
2009.

Gen2+

- Setup at manufacturer

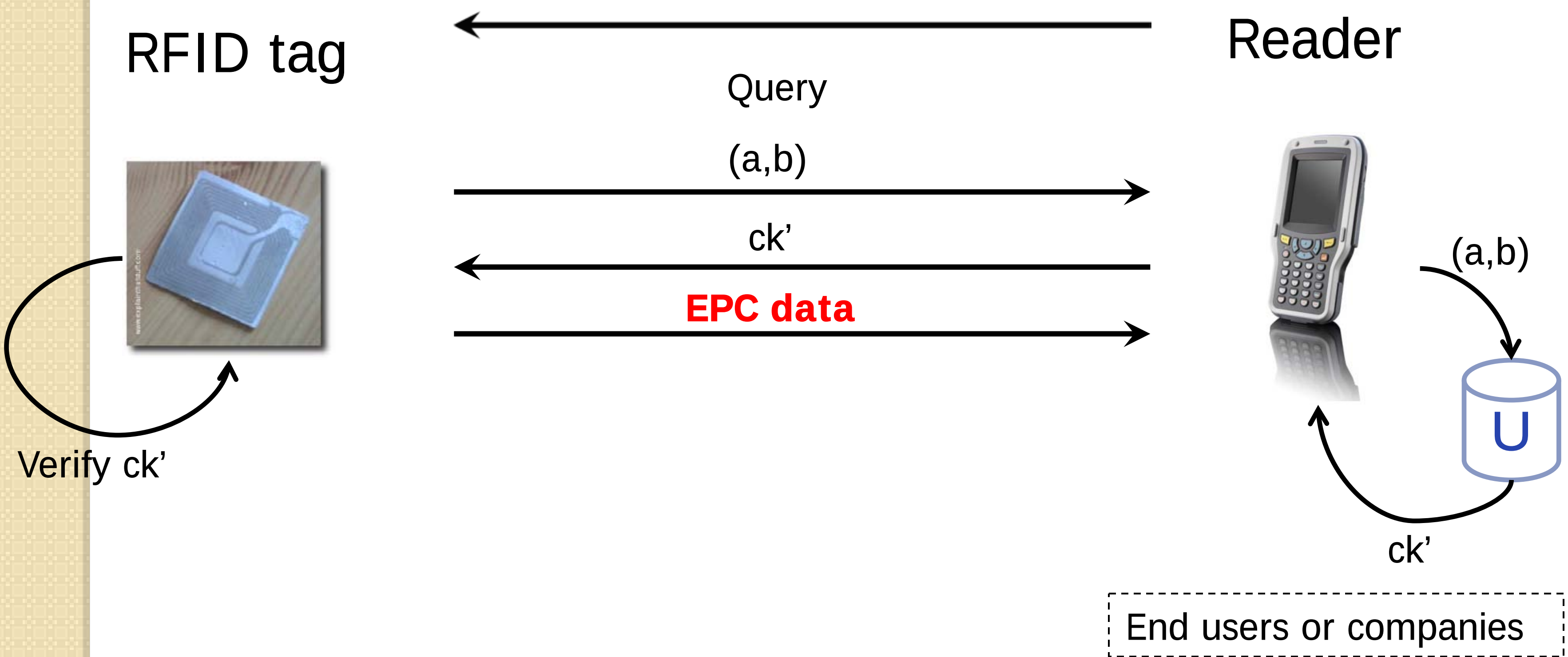


- After sold

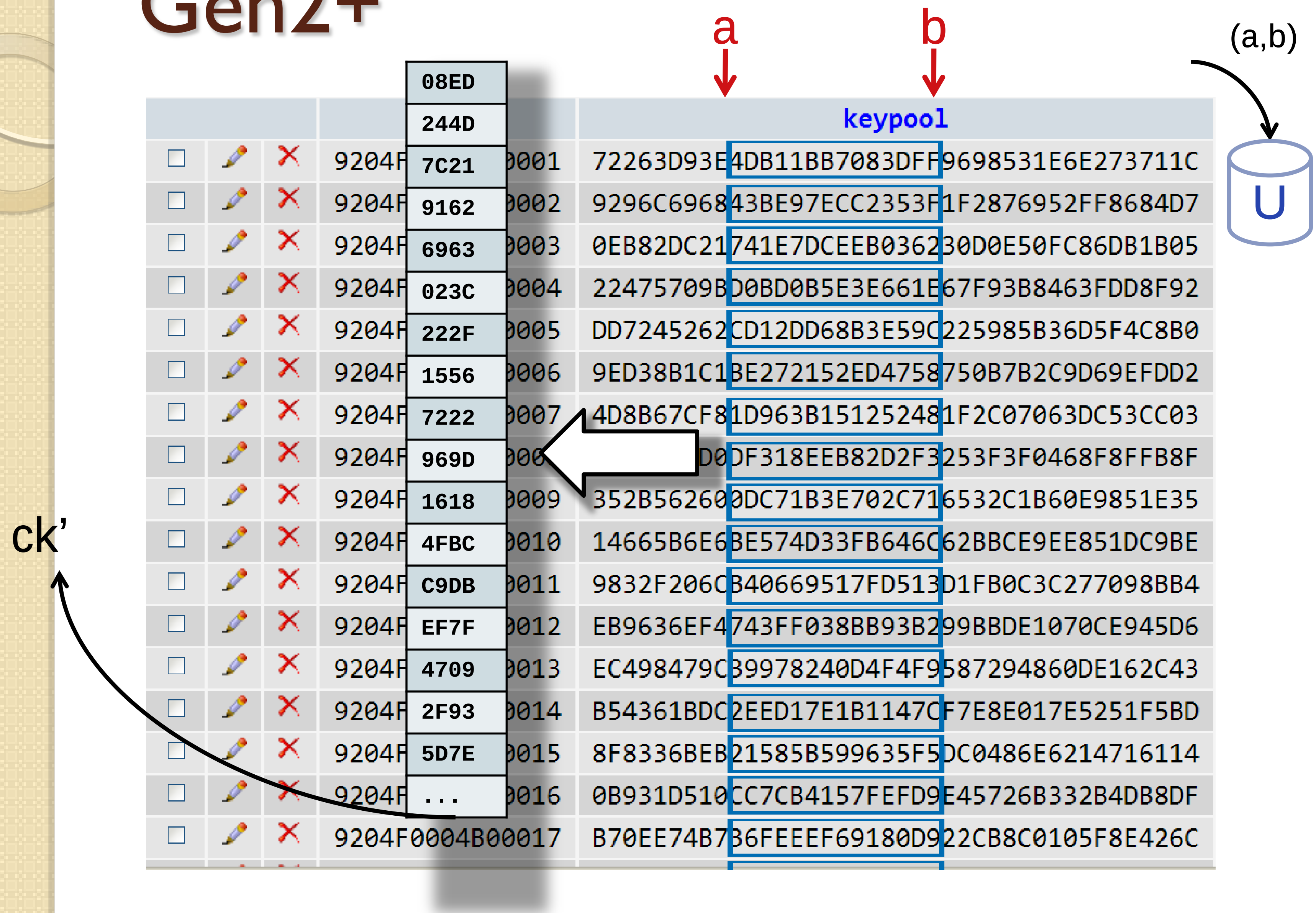


Gen2+

- In use

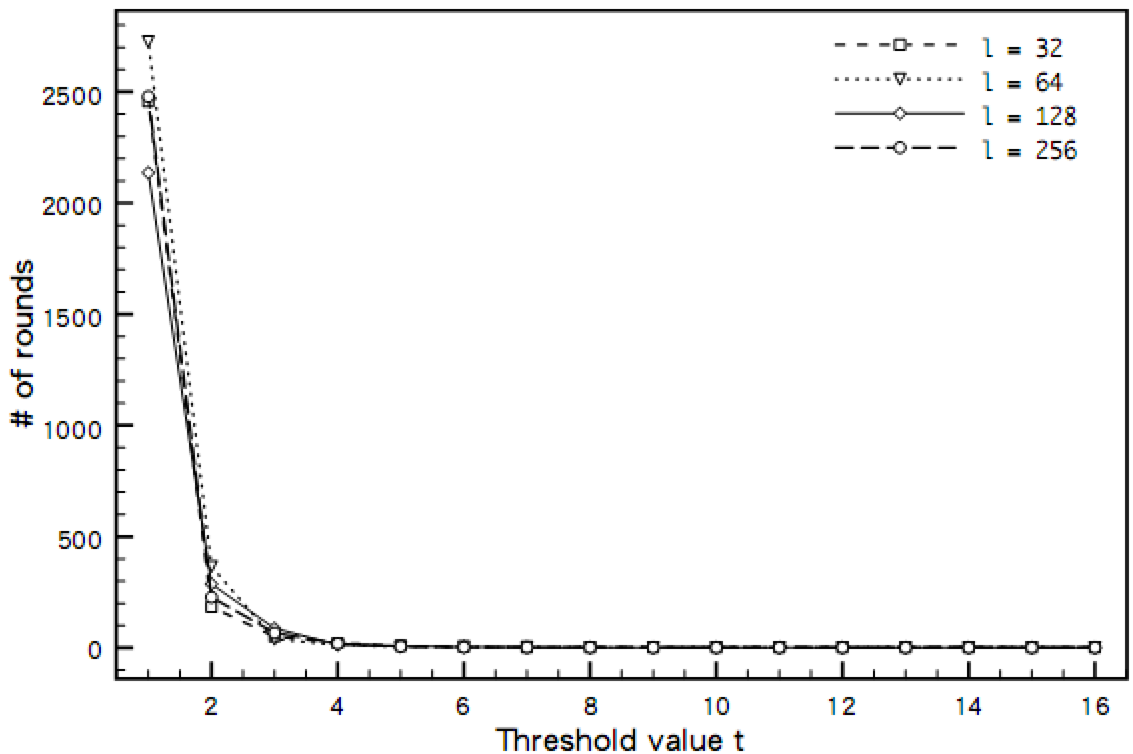

RFID tag
Reader
Query
(a,b)
ck'
EPC data
Verify ck'
(a,b)
U
ck'
End users or companies

Gen2+


a
b
(a,b)
U
ck'
keypool
08ED
244D
7C21
9162
6963
023C
222F
1556
7222
969D
1618
4FBC
C9DB
EF7F
4709
2F93
5D7E
...
9204F0004B00017
72263D93E4DB11BB7083DFF9698531E6E273711C
9296C69643BE97ECC2353F1F2876952FF8684D7
0EB82DC21741E7DCEEB036230D0E50FC86DB1B05
22475709BD0BD0B5E3E661E67F93B8463FDD8F92
DD7245262CD12DD68B3E59C225985B36D5F4C8B0
9ED38B1C1BE272152ED4758750B7B2C9D69EFDD2
4D8B67CF81D963B151252481F2C07063DC53CC03
D0DF318EEB82D2F3253F3F0468F8FFB8F
352B562600DC71B3E702C716532C1B60E9851E35
14665B6E6BE574D33FB646C62BBCE9EE851DC9BE
9832F206CB40669517FD513D1FB0C3C277098BB4
EB9636EF4743FF038BB93B299BBDE1070CE945D6
EC498479C39978240D4F4F9587294860DE162C43
B54361BDC2EED17E1B1147CF7E8E017E5251F5BD
8F8336BEB21585B599635F5DC0486E6214716114
0B931D510CC7CB4157FEFD9E45726B332B4DB8DF
B70EE74B736FEEEF69180D922CB8C0105F8E426C

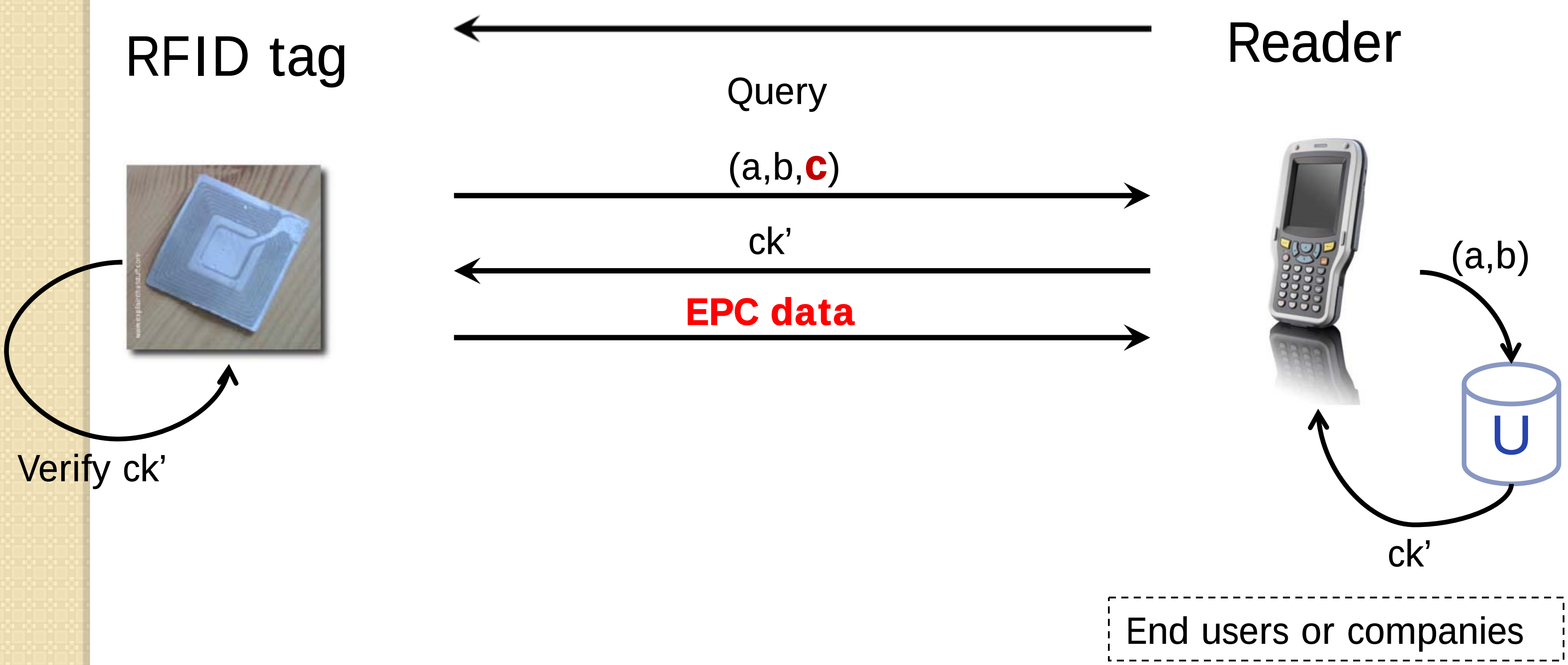
Gen2+

- Results before enhancement



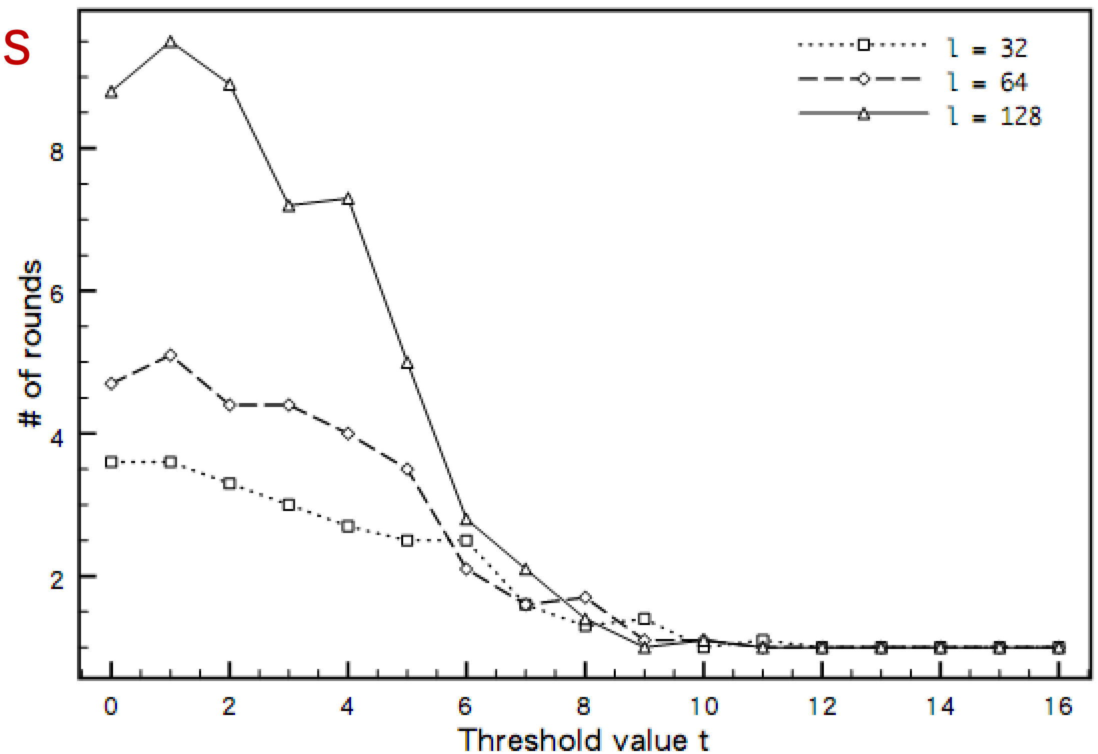
Gen2+

- In use


RFID tag
Reader
Query
(a,b,**c**)
ck'
EPC data
Verify ck'
(a,b)
U
ck'
End users or companies

- Results **after** enhancement

< 10 rounds



Thank You
Q & A