Cryptanalysis of a Novel Authentication Protocol Conforming to EPC-C1G2 Standard

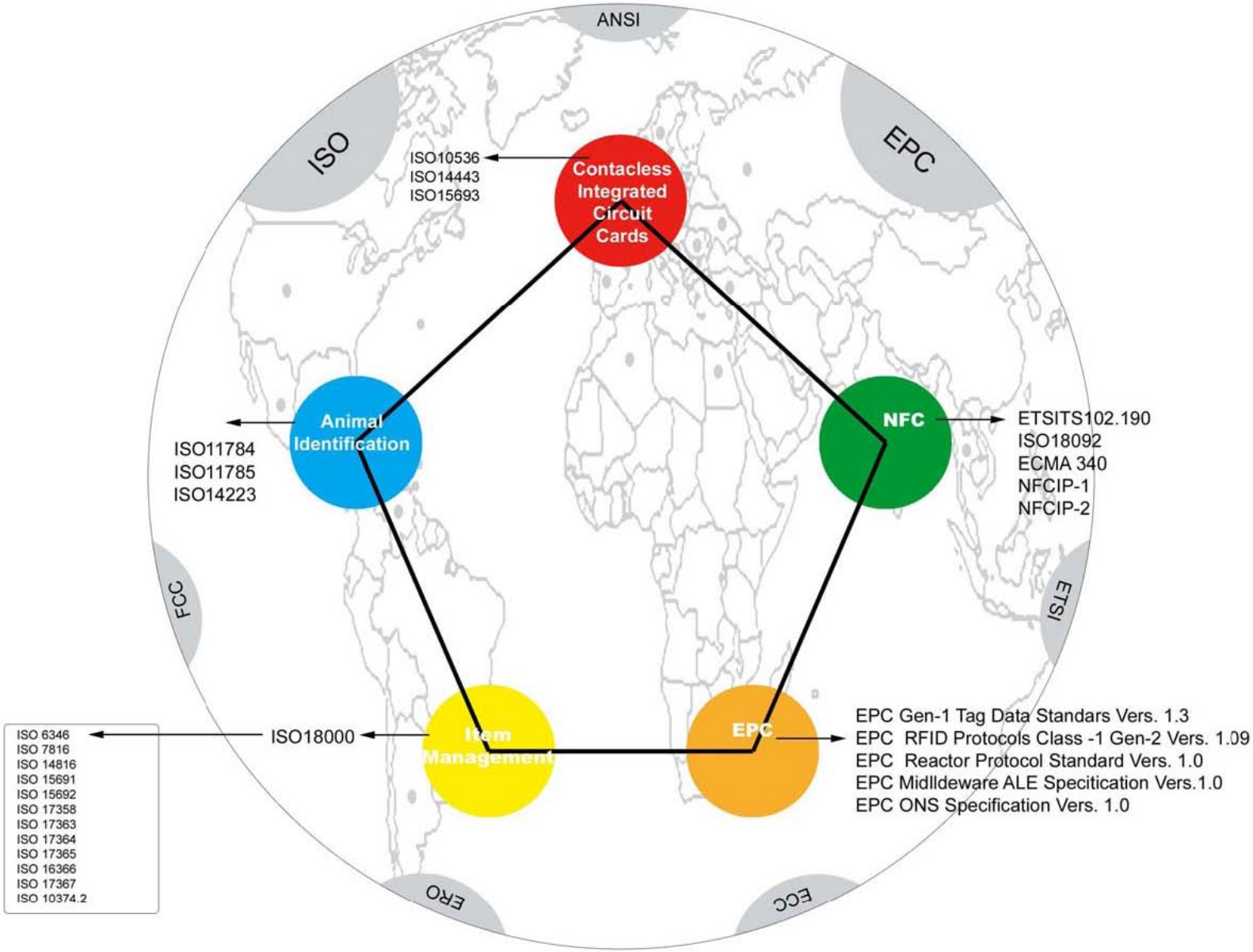
Pedro Peris-Lopez Julio C. Hernandez-Castro
Juan M. Estevez-Tapiador Arturo Ribagorda

Computer Science Department – Carlos III University

RFIDSec'07, 11-13 July, 2007
Málaga, Spain

Outline

RFID Standards



EPC-C1G2 and ISO 18000-6C

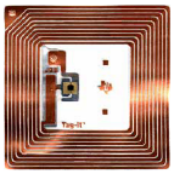
Tags specifications

- Tags are passive
- Tags have very constrained computing and storage capabilities
- Tags have on chip a 16-bit Pseudo-Random Number Generator and a **16-bit Cyclic Redundancy Code (CRC) checksum**
- Tags have two 32-bit PINs: Kill and Access

Tags Operations

- **Select:** select a subset of the tag population
- **Inventory:** identify a tag
- **Access:** interact with individual tags

Select Command



[1] Reader issues a Query

Query Request

[2] Generates RN16
while (RN16 <> 0)
RN16 - -
Tag backscatters RN16

RN16

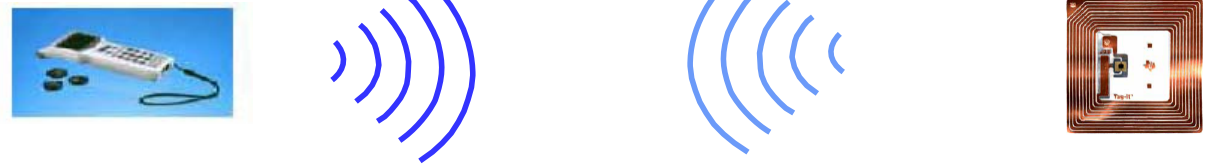
[3] Reader acknowledges Tag with an ACK including RN16

ACK(RN16)

PC, EPC, CRC16

[4] If valid RN16 :
Tag answers with PC, EPC, CRC16
If invalid RN16 : No reply

Select command: EPC is transmitted as plain text!



[1] Reader issues a Query

Query Request

[2] Generates RN16
while (RN16 <> 0)
RN16 - -
Tag backscatters RN16

RN16

[3] Reader acknowledges Tag with an ACK including RN16

ACK(RN16)

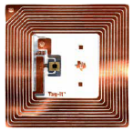
PC, EPC, CRC16

[4] If valid RN16 :
Tag answers with PC, EPC, CRC16
If invalid RN16 : No reply

Privacy **Tracking** **Spoofing**

Access Command



[5] Reader issues ReqRN using the same RN16

ReqRN(RN16) →

[6] If valid RN16 :
Tag responds with handle: RN16'
If invalid RN16 : No reply

← handle

[7.1] Reader issues ReqRN using the handle

ReqRN(handle) →

[7.2] Tag verifies the handle
Tag ignores command if the handle does not match.

← RN16'

PIN[31:16] ⊕ RN16'|| handle || CRC →

MSB

ReqRN(handle) →

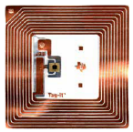
← RN16''

PIN[15:10 ⊕ RN16''|| handle || CRC →

LSB

Access Command: PIN can be disclosed!



[5] Reader issues ReqRN using the same RN16

ReqRN(RN16)

handle

[6] If valid RN16 :
Tag responds with handle: RN16'
If invalid RN16 : No reply

[7.1] Reader issues ReqRN using the handle

ReqRN(handle)

RN16'

[7.2] Tag verifies the handle
Tag ignores command if the handle does not match.

PIN[31:16] ⊕ RN16'|| handle || CRC

⊕ → **PIN[31:16]**

MSB

ReqRN(handle)

RN16''

PIN[15:10 ⊕ RN16''|| handle || CRC

LSB

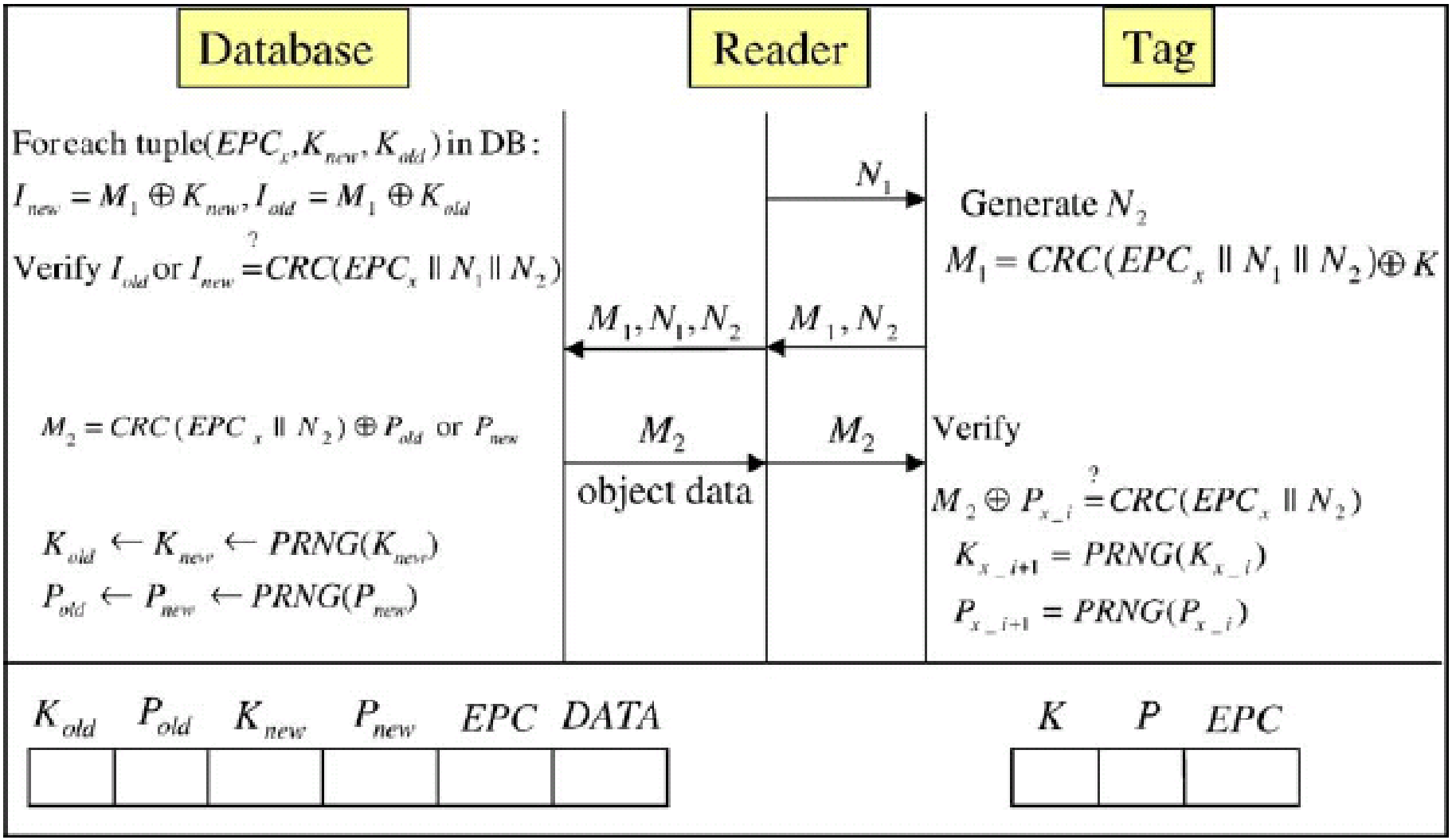
⊕ → **PIN[15:0]**

Chien's et al. Protocol

Motivation

- The security of EPC-C1G2 standard is too weak
- Standard cryptographic primitives can not be supported on EPC-C1G2 RFID tags (in spite of this, there are many hash-based proposals [4, 5, 6, 7, 8, 9])
- The security weaknesses of all previous proposals conforming to EPC-C1G2 [10, 11]

Chien's et al. Protocol



CRC - Cyclic Redundancy Codes (I)

- **CRCs are completely linear!**

Theorem

For any CRC (independently of its generator polynomial) and for any values a, b, c, and $d \in F_2[x]$, it holds:

$$CRC(a\|b) \oplus CRC(c\|d) = CRC(a \oplus c\|b \oplus d) \quad (1)$$

Corollary

In particular, if in Equation 1 we have $a = c$, then,

$$\begin{aligned} CRC(a\|b) \oplus CRC(a\|d) &= CRC(a \oplus a\|b \oplus d) \quad (2) \\ = CRC(0\|b \oplus d) &= CRC(b \oplus d) \end{aligned}$$

because $0 \cdot x^N \equiv 0 \cdot p(x)$

CRC - Cyclic Redundancy Codes (II)

Cyclic Redundancy Codes

- CRCs detect transmission errors
- CRCs should not be used for cryptography
- Chien et al.'s weakness are related with the abusive use of CRCs
- **Past examples**: SSH v1.5 [1, 2] and WEP [3] protocols

Cryptanalysis of Chien's Protocol

- **None of the protocol objectives are met!**

Vulnerabilities of Chien's Protocol

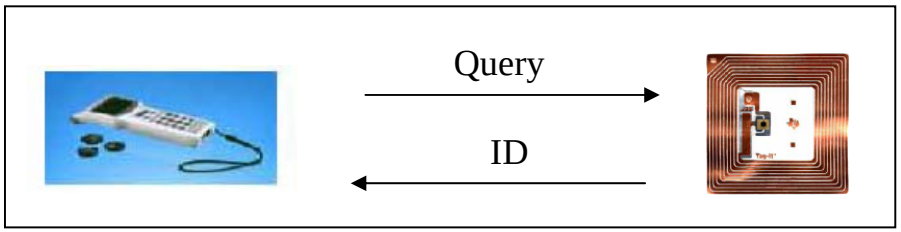
1. Unequivocal Identification
2. Tag Impersonation
3. Back-end Database/Reader Impersonation
4. Tracking
5. Back-end Database Auto-desynchronization

Unequivocal Identification

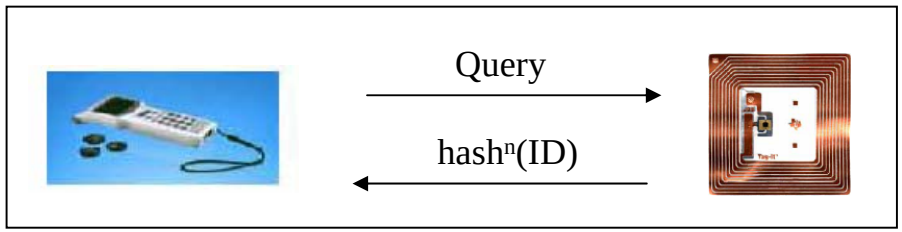
Barcodes - RFID tags:

- Automatic, without line of sight, through non-conducting materials, hundreds per second, several meters away
- **Unequivocal identification**

Non-secure Identification System



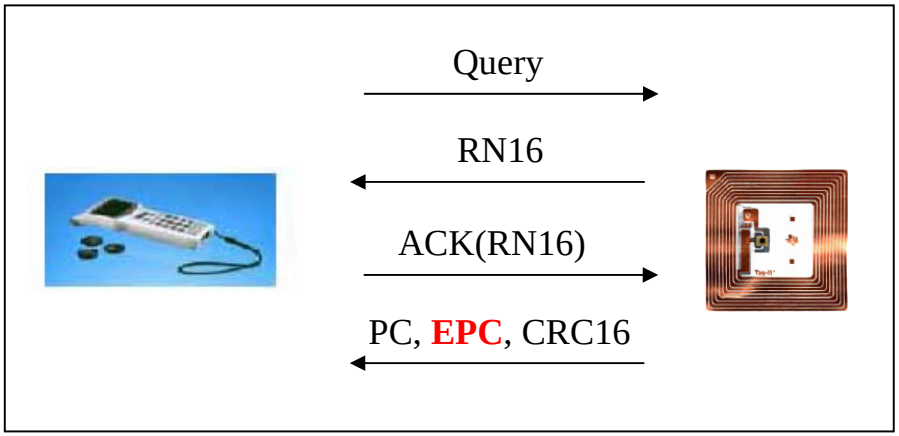
Hash-based solution



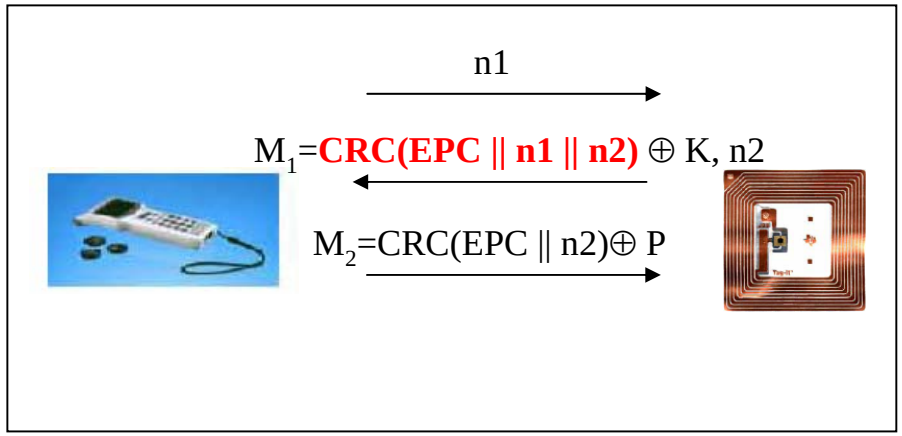
Trivial approximations that don't work

Unequivocal Identification

EPC Class-1 Gen-2 Standard



Chien et al.'s Protocol



Non-trivial approximations that don't work either!

General Identifier

	Header	General Manager Number	Object Class	Serial Number
GID-96	8	28	24	36
	0011 0101 **0x35** **Fixed Binary value**	268,435,455 (Max. decimal value)	16,777,215 (Max. decimal value)	68,719,476,735 (Max. decimal value)

- A GID-96 has 8 bits fixed to 0x35 and 88 free bits
- Tags support a 16-bit CRC
- 2^{88} values collapse through the CRC-16 into 2^{16} values in Chien's protocol:
  - $M_1 = CRC(EPC||n_1||n2) \oplus K$
  - $M_2 = CRC(EPC||n2) \oplus P$

Unequivocal Identification

Non-unequivocal identification Probability (P_{NUI})

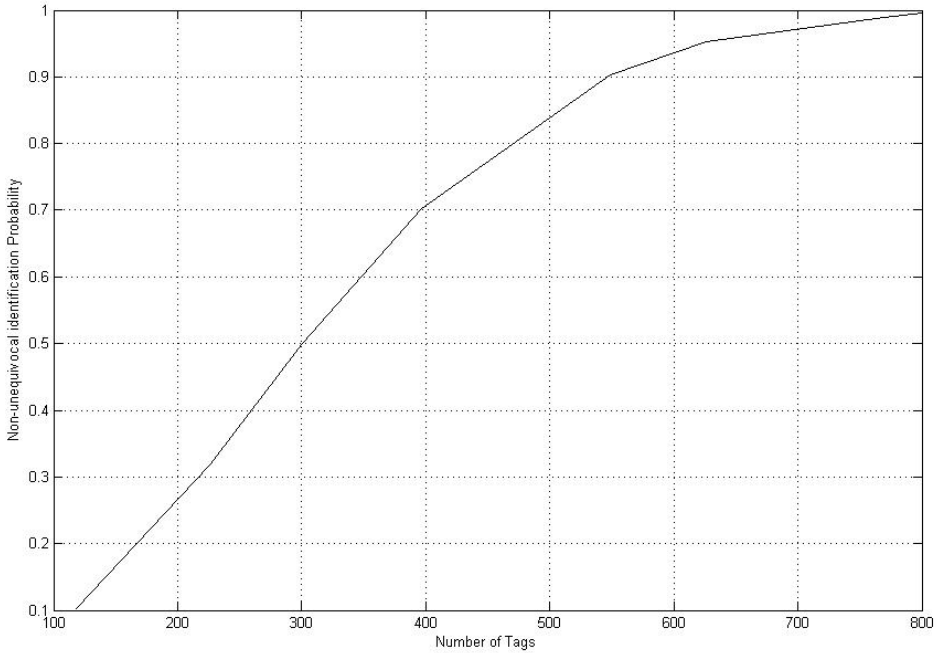
N tags simulation

(1) Reading of tag_x
(2) $M_1 = CRC(EPC_x||n_1||n_2) \oplus K_x$
(3) Send M_1, n_1, n_2 to the back-end database
(4) for($x' = 1$, $x' < N$, x'_{++})
$M_1' = CRC(EPC'_x||n_1||n_2) \oplus K'_x$
if ((x' != x) & (M_1' == M_1)) collision$_{++}$
(5) if collision$>$ 0 "Failed unequivocal identification"

- $N = 118, 226, \ldots 800$ and $T = 1000$
- EPC_x, K_x, n_1, n_2 randomly chosen

Unequivocal Identification

Non-unequivocal identification Probability (P_{NUI})



- For a low number of tags $N = 300 \Rightarrow P_{NUI} = 0.5$
- For relatively low number of tags $(N = 600) \Rightarrow P_{NUI} > 0.9$

Unequivocal Identification

Non-unequivocal identification Probability (P_{NUI})

Birthday paradox

- Birthday paradox: N tags and $d = 2^{16}$ boxes:

$$p(N;d) = \begin{cases} 1 - \prod_{k=1}^{N-1}(1 - \frac{k}{d}) & N \leq d \\ 1 & N > d \end{cases} \quad (3)$$

- Each time a tag is read:

$$\begin{aligned} M_1 &= M_1' \\ CRC(EPC_x||n_1||n_2) \oplus K_x &= CRC(EPC_{x'}||n_1||n_2) \oplus K_{x'} \end{aligned}$$

Unequivocal Identification

Failed identification Probability (P_{FI})

- Allowing the existence of collisions (unusual condition)

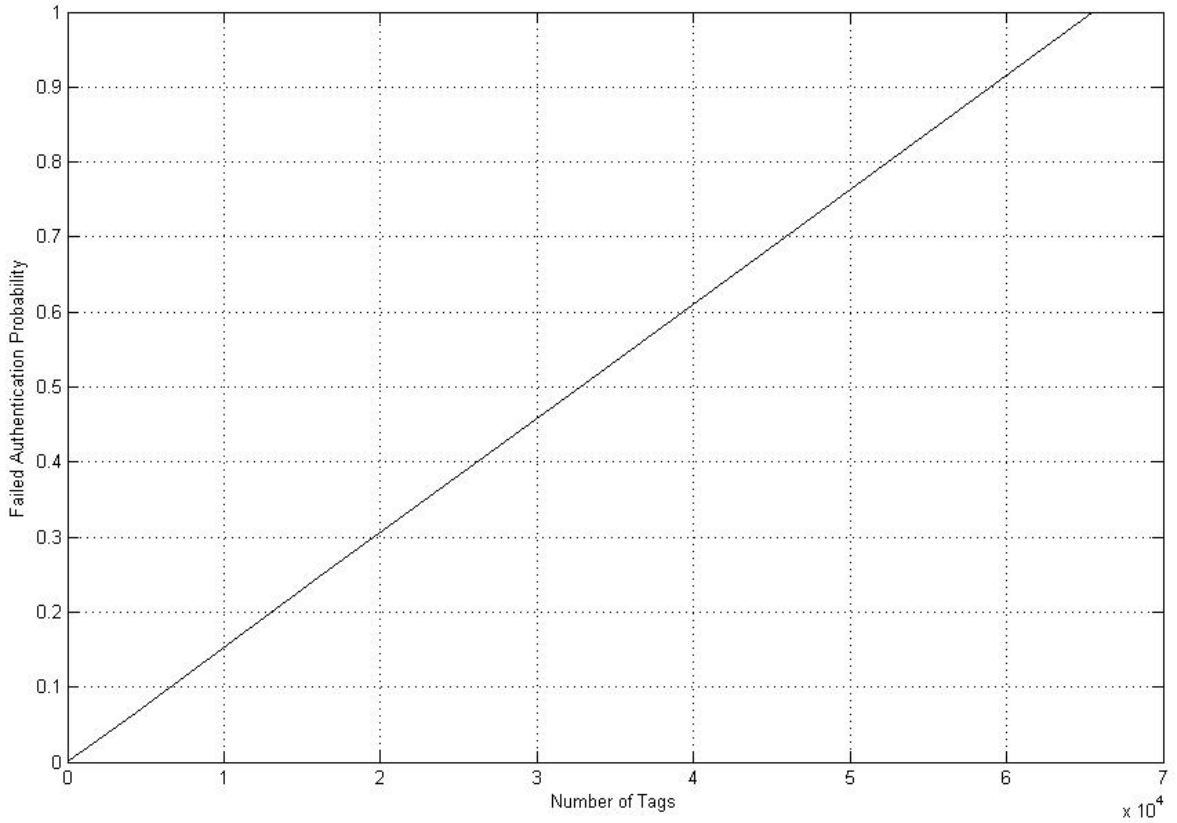
N tags simulation

(1) Reading of tag_x
(2) $M_1 = CRC(EPC_x||n_1||n_2) \oplus K_x$
(3) Send M_1, n_1, n_2 to the back-end database
(4) for($x' = 1$, $x' < N$, x'_{++})
$M_1' = CRC(EPC_x'||n_1||n_2) \oplus K_x'$
if ((x' != x) & (M_1' == M_1)) collision$_{++}$

- $N = 2^7, 2^{10}, \ldots 2^{16}$ and $T = 1000$
- EPC_x, K_x, n_1, n_2 randomly chosen

Unequivocal Identification

Failed identification Probability (P_{FI})



- Even, for a low number of tags $\Rightarrow$ P_{FI} is very high.

Tag Impersonation

An iteration reader - tag

(1) $R \rightarrow T$: n_1

(2) $T \rightarrow R$: $M_1 = CRC(EPC_x||n_1||n_2) \oplus K_x,\ n_2$

- The attacker isolates the tag
- The attacker knows $\begin{cases} M_1 \\ n_1 \text{ and } n_2 \end{cases}$

An iteration reader - fraudulent tag

(3) $R \rightarrow T$: n_1'

(4) T: The fraudulent tag generates n_2'

(5) $T \rightarrow R$: $M_1' = M_1 \oplus CRC(n_1 \oplus n_1'||n_2 \oplus n_2'),\ n_2'$

Chien et al's protocol does not guarantee the non-impersonation of legitimate tags!

Back-end Database/Reader Impersonation

An iteration reader - tag

(1) $R \rightarrow T$: n_1

(2) $T \rightarrow R$: $M_1 = CRC(EPC_x||n_1||n_2) \oplus K_x,\ n_2$

(3) $R \rightarrow Database$: $M_1\ ,\ n_1,\ n_2$

(4) $Database \rightarrow R$: $M_2 = CRC(EPC_x||n_2) \oplus P_x$

(5) $R \rightarrow T$: M_2

- Attacker: prevents the correct reception of message 5
- The attacker knows $\begin{cases} M_1, M_2 \\ n_1 \text{ and } n_2 \end{cases}$

An iteration fraudulent reader - tag

(6) $A \rightarrow T$: n_1'

(7) $T \rightarrow A$: $M_1' = CRC(EPC_x||n_1'||n_2') \oplus K_x,\ n_2'$

The atacker knows n_2'

(8) $A \rightarrow T$: $M_2' = M_2 \oplus CRC(n_2 \oplus n_2')$

Chien et al.'s protocol is vulnerable to back-end database/reader impersonation!

Non-updating key condition

(1) $R \rightarrow T$: n_1

(2) $T \rightarrow R$: $M_1 = CRC(EPC_x||n_1||n_2) \oplus K_x^n,\ n_2$

....

(1) $R \rightarrow T$: n_1'

(2) $T \rightarrow R$: $M_1' = CRC(EPC_x||n_1'||n_2') \oplus K_x^n,\ n_2'$

....

An attacker can verify if answers arise from the same tags by checking if the following equation holds:

$$M_1 \oplus M_1' = CRC(n_1 \oplus n_1'||n_2 \oplus n_2')$$

Chien et al.'s protocol does not guarantee the location privacy of tags!

Back-end database auto-desynchronization

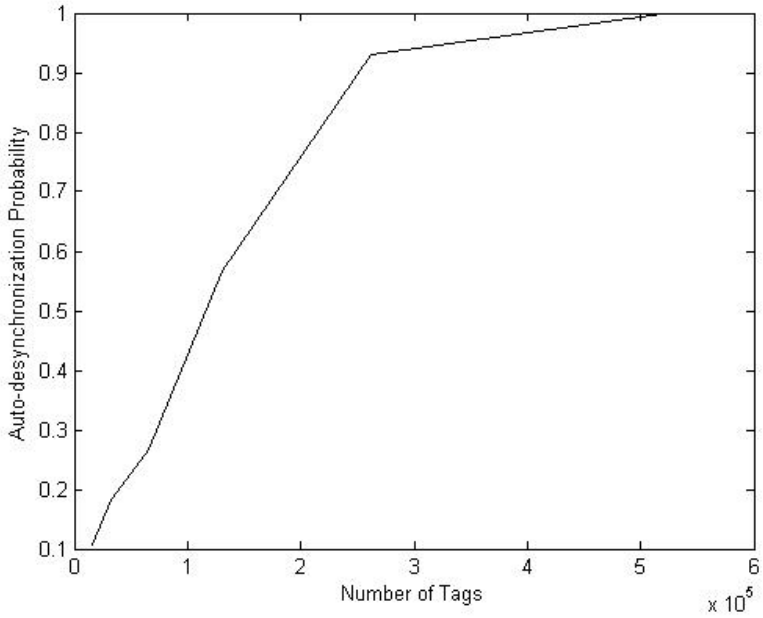
- Chien: A pair of keys (*new*,*old*) are maintained to avoid desynchronization
- The normal operation of the protocol $\Rightarrow$ synchronization loss

N tags simulation

(1) Reading of tag_x
(2) $M_1 = CRC(EPC_x||n_1||n_2) \oplus K_x$
(3) Send M_1, n_1, n_2 to the back-end database
(4) while(($x' < N$) & ($not(found)$))
M_1'$= CRC(EPC'_x||n_1||n_2) \oplus K'_x$
if ($M'_1 == M1$) autodesyn[x']$_{++}$; found=1
x"$_{++}$

- $N = 2^{14}$, 2^{15}, ... 2^{18} and $T = 1000$

Back-end database auto-desynchronization



Probability of auto-desynchronization:

$$P_{ADS} = \frac{1}{N} \sum_{x=1}^{N} (autodesyn[x] - 1)$$

- For a population of $N \geq 2^{17}$ tags, P_{ADS} is greater than 0.5
- This probability increases to 0.93 if the population is $N \geq 2^{18}$

Conclusions

- The security of EPC-C1G2 is weak
- Chien'protocol: abusive use of CRC
  - Non-unequivocal and auto-desynchronization: easy to solve by augmenting the CRC length
  - Tag impersonation, back-end database/reader impersonation tracking: CRC independent
  - CRC should be used to detect error transmissions and not to securize communications
- Increasing the security in the coming Generation-3
- Research direction:
  - New lightweight cryptographic primitives: Hash functions, PRNGs
  - New protocols not too compliant with the EPC-C1G2

Questions?

Thank you

pperis@inf.uc3m.es

http://www.lightcrypto.seg.inf.uc3m.es/chien


A. Futoransky and E. Kargieman.
An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes.
http://www.coresecurity.com/files/attachments/CRC32.pdf, 1999.


N. Provos and P. Honeyman.
Scanssh - scanning the internet for ssh servers.
In *In Proc. of USENIX'01*, 2001.


N. Borisov, I. Goldberg, and D. Wagner.
Intercepting mobile communications: the insecurity of 802.11.
In *Proc. of MobiCom'01*, ACM, pages 180–189, 2001.


S.E. Sarma, S.A. Weis, and D.W. Engels.
RFID systems and security and privacy implications.
In *Proc. of CHES'02*, volume 2523 of LNCS, pages 454–470, 2002.


E.Y. Choi, S.M. Lee, and D.H. Lee.
Efficient RFID authentication protocol for ubiquitous computing environment.
In *Proc. of SECUBIQ'05*, volume 3823 of LNCS, pages 945–954, 2005.


D. Henrici and P. Müller.
Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers.
In *Proc. of PERSEC'04*, pages 149–153. IEEE Computer Society, 2004.


S.M. Lee, Y.J. Hwang, D.H. Lee, and J.I.L. Lim.
Efficient authentication for low-cost RFID systems.
In *Proc. of ICCSA'05*, volume 3480 of *LNCS*, pages 619–627, 2005.


M. Ohkubo, K. Suzuki, and S. Kinoshita.
Cryptographic approach to "privacy-friendly" tags.
In *Proc. of RFID Privacy Workshop*, 2003.


J. Yang, J. Park, H. Lee, K. Ren, and K. Kim.
Mutual authentication protocol for low-cost RFID.
In *Proc RFIDSec'05*, 2005.


A. Juels.
Strengthening EPC tags against cloning.
Manuscript, March 2005.


D.N. Duc, J. Park, H. Lee, and K. Kim.
Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning.
In *Proc. of Symposium on Cryptography and Information Security*, 2006.