

# LMAP: A Lightweight Mutual Authentication Protocol for Low-cost RFID tags

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

Computer Science Department – Carlos III University

RFIDSec, 2006  
Graz

# Outline of Topics

## 1 Introduction

- Motivation
- Related Work

## 2 Lightweight Protocol

- Model Assumptions
- The Protocol
  - Tag Identification
  - Mutual Authentication
  - Index-Pseudonym and Key Updating

## 3 Evaluation

- Security Analysis
- Performance Analysis

## 4 Implementation

## 5 Conclusions

- A huge number of security problems need to be addressed before the mass deployment of RFID systems.
- Low-cost RFID tags can only:
  - Store hundreds of bits.
  - Have 5K-10K gates: only 250-3K for security.
- Low-cost RFID tags are incapable of implementing traditional cryptographic primitives.

- A huge number of security problems need to be addressed before the mass deployment of RFID systems.
- Low-cost RFID tags can only:
  - Store hundreds of bits.
  - Have 5K-10K gates: only 250-3K for security.
- Low-cost RFID tags are incapable of implementing traditional cryptographic primitives.

- Since the work of Sarma et. al [8] in 2002, most of the proposals are based on the use of hash functions:
  - Implementing cryptographic hash functions with only 250-3K gates is hard.
  - No explicit algorithms are suggested.
  - New proposals not sufficiently explored to be considered secure.

Solutions	Implementation	Gate Count
<b>Hash</b>	Universal Hash Yksel [12]	1.7K gates
	SHA-1 Yaps [13]	4.3K gates
	MD5 Helion [7]	16K gates
	Fast SHA-1 Helion [7]	20K gates
	Fast SHA-256 Helion [7]	23K gates

- There are solutions that exclusively use non-cryptographic primitives:
  - Vajda [9] propose a set of extremely lightweight challenge-response authentication algorithms.
  - Juels [5] proposed a solution based on using a list of pseudonyms.

### Conclusions

We believe that the security of Low-Cost RFID tags can be significantly improved with *minimalist cryptographic* solutions.

A Lightweight Mutual Authentication Protocol (LMAP) is proposed.

- There are solutions that exclusively use non-cryptographic primitives:
  - Vajda [9] propose a set of extremely lightweight challenge-response authentication algorithms.
  - Juels [5] proposed a solution based on using a list of pseudonyms.

### Conclusions

We believe that the security of Low-Cost RFID tags can be significantly improved with *minimalist cryptographic* solutions.

A Lightweight Mutual Authentication Protocol (LMAP) is proposed.

# Model Assumptions

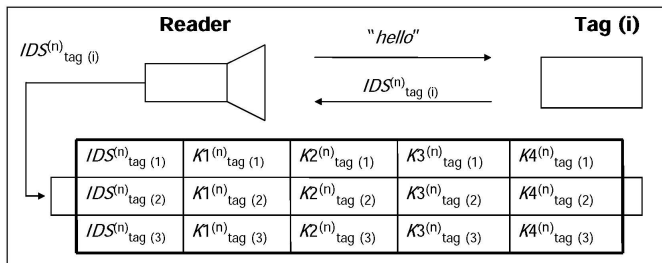
- Our protocol is based on index-pseudonyms.
- Information about a tag:
  - A key, which is divided in four 96-bit subkeys. ( $K = K1 \parallel K2 \parallel K3 \parallel K4$ )
  - The static identification number (ID).
- Operations:
  - Costly operations such as random number generation will be done by the reader.
  - Tags are limited to simple operations: bitwise XOR ( $\oplus$ ), bitwise OR ( $\vee$ ), bitwise AND ( $\wedge$ ), and addition mod  $2^m$  ( $+$ ).
- Communication:
  - Communication must be initiated by readers.
  - Backward & forward channels can be listened by an attacker.
  - Communication channel between reader and database is secure.

The protocol can be split in four main stages:

- 1 Tag Identification
- 2 Mutual Authentication
- 3 Index-Pseudonym Updating
- 4 Key-Updating

# Tag Identification

- Before starting the protocol, the reader has to identify the tag.
- By means of the IDS, an authorized reader can access the associated information related with the tag.



# Mutual Authentication

Tag Identification:

Reader → Tag: *hello*

Tag → Reader: *IDS*

Mutual Authentication:

Reader → Tag:  $A \parallel B \parallel C$

Tag → Reader:  $D$

$$A = IDS_{tag(i)}^{(n)} \oplus K1_{tag(i)}^{(n)} \oplus n1 \quad (1)$$

$$B = (IDS_{tag(i)}^{(n)} \vee K2_{tag(i)}^{(n)}) + n1 \quad (2)$$

$$C = IDS_{tag(i)}^{(n)} + K3_{tag(i)}^{(n)} + n2 \quad (3)$$

$$D = (IDS_{tag(i)}^{(n)} + ID_{tag(i)}) \oplus n1 \oplus n2 \quad (4)$$

- We have analyzed the statistical properties of these four messages with three well-known suites of randomness tests, namely ENT, DIEHARD and NIST: all test were passed (including B and C submessages), so submessages are not easily distinguishable from a random source, not even for the eavesdropper cryptanalyst. The whole report is available in <http://163.117.149.208/lmap>.

# Index-Pseudonym and Key Updating

- After the mutual authentication the updating stage must be carried out:
  - Only use efficient operations: bitwise XOR ( $\oplus$ ), bitwise OR ( $\vee$ ), bitwise AND ( $\wedge$ ), and addition mod  $2^m$  ( $+$ ).
  - The number of operations is limited by temporary requirements.

$$IDS_{tag(i)}^{(n+1)} = (IDS_{tag(i)}^{(n)} + (n2 \oplus K4_{tag(i)}^{(n)})) \oplus ID_{tag(i)} \quad (5)$$

$$K1_{tag(i)}^{(n+1)} = K1_{tag(i)}^{(n)} \oplus n2 \oplus (K3_{tag(i)}^{(n)} + ID_{tag(i)}) \quad (6)$$

$$K2_{tag(i)}^{(n+1)} = K2_{tag(i)}^{(n)} \oplus n2 \oplus (K4_{tag(i)}^{(n)} + ID_{tag(i)}) \quad (7)$$

$$K3_{tag(i)}^{(n+1)} = (K3_{tag(i)}^{(n)} \oplus n1) + (K1_{tag(i)}^{(n)} \oplus ID_{tag(i)}) \quad (8)$$

$$K4_{tag(i)}^{(n+1)} = (K4_{tag(i)}^{(n)} \oplus n1) + (K2_{tag(i)}^{(n)} \oplus ID_{tag(i)}) \quad (9)$$

- The statistical properties of the five values are good, including the 1<sup>st</sup>, the 4<sup>th</sup>, and the 5<sup>th</sup>, (again verified with ENT, DIEHARD and NIST randomness batteries), so there is no evidence to ensure that there are different from a random variable.

- *User Data Confidentiality*

Tag sends message  $D = (IDS_{tag(i)}^{(n)} + ID_{tag(i)}) \oplus n1 \oplus n2$  hiding the tag  $ID$  to a nearby eavesdropper equipped with an RFID reader.

- *Tag Anonymity*

Reader generates message  $A||B||C$ , which serves to authenticate him, as well as to transmit, in a secure form the nonces  $n1$  and  $n2$  to the tag. This two random numbers will be used in the answer messages of the tag:  $(IDS_{tag(i)}^{(n)} + ID_{tag(i)}) \oplus n1 \oplus n2$ .

- *Data Integrity*

Part of the memory of the tag is rewritable, so modifications are possible.

- *Mutual Authentication*

We have designed the protocol with both reader-to-tag authentication (message  $A || B || C$ ) and tag-to-reader authentication (message  $D$ ).

- *Forward Security*

Since key updating is fulfilled after mutual authentication, a future security compromise on an RFID tag will not reveal data previously transmitted.

- *Man-in-the-middle Attack*

Our proposal is based on a mutual authentication, in which two fresh random numbers ( $n1$ ,  $n2$ ) are used in each iteration.

- *Replay Attack prevention*

After mutual authentication, *IDS* and key  $K$  will be updated.

- *Forgery Resistance*

Information stored in tag is sent operated (bitwise XOR ( $\oplus$ ), bitwise OR ( $\vee$ ), bitwise AND ( $\wedge$ ), and addition mod  $2^m$  ( $+$ )) with nonces ( $n1$ ,  $n2$ ).

# Security Analysis: Comparison between protocols

- *Data Recovery*

Intercepting or blocking messages is a DoS attack preventing tag identification.

Protocol	HLS [10]	EHLS [10]	HBVI [4]	MAP [11]	<b>LMAP</b>
User Data Confidentiality	×	△	△	○	○
Tag Anonymity	×	△	△	○	○
Data Integrity	△	△	○	○	△
Mutual Authentication	△	△	△	○	○
Forward Security	△	△	○	○	○
Man-in-the-middle Attack	△	△	×	○	○
Replay Attack Prevention	△	△	○	○	○
Forgery Resistance	×	×	×	○	○
Data Recovery	×	×	○	○	○

††Notation: ○ Satisfied △ Partially satisfied × No Satisfied

# Performance Analysis

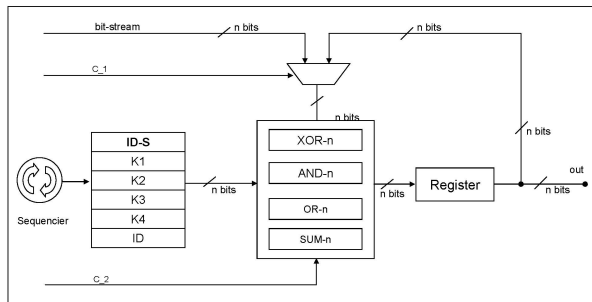
Protocol	Entity	HLS [10]	EHLS [10]	HBVI [4]	MAP [11]	<b>LMAP</b>
No. of Hash Operation	T	1	2	3	2	↯
	B	↯	n	3	2Nt	↯
No. of Keyed Hash Operation	R	↯	↯	↯	1	↯
	B	↯	↯	↯	1	↯
No. of RNG Operation	T	↯	1	↯	↯	↯
	R	↯	↯	↯	1	↯
	B	↯	↯	1	↯	↯
No. of Basic Operation <sup>1</sup>	T	↯	↯	↯	4	19
	R+B	↯	↯	↯	2(Nt+1)	21
No. of Encryption	B	↯	↯	↯	1	↯
No. of Decryption	R	↯	↯	↯	1	↯
Number of Authentication Steps		6	5	5	5	4
Required Memory Size <sup>2</sup>	T	$1\frac{1}{2}L$	1L	3L	$2\frac{1}{2}L$	6L
	R+B	$2\frac{1}{2}L$	$1\frac{1}{2}L$	9L	$9\frac{9}{2}L$	6L

††Notation: ↯: Not required Nt: Number of tags L: Required memory size

<sup>1</sup>Basic Operations: ⊕: Bitwise XOR ∨: Bitwise OR

∧: Bitwise AND +: Addition mod  $2^m$

# Implementation: Logic Scheme and Architectural Features



Word length		8-bit	16-bit	32-bit	64-bit	96-bit
Number of	ALU	72	144	288	576	864
Gates	Control	14	29	58	115	173
	<b>Total</b>	<b>86</b>	<b>173</b>	<b>346</b>	<b>691</b>	<b>1037</b>
Number of clock cycles		864	432	216	108	72
Answers/second		<b>115</b>	<b>231</b>	<b>462</b>	<b>925</b>	<b>1388</b>

- Low-cost RFID tags are very constrained systems, incapable of performing true cryptographic operations.
- **Minimalist cryptography is possible!!**  
A Lightweight Mutual Authentication Protocol is proposed.
  - It can be implemented in low-cost RFID tags (100-1K gates).
  - Tag should be fitted with a small portion of rewritable memory and other read-only memory.
  - The main security aspects have been considered.
  - Efficiency:
    - Does not require an exhaustive search in the back-end database.
    - Only four messages need to be exchanged.

- A deeper security analysis is needed, including some kind of formal analysis.
- We seek the implementation in a FPGA architecture, to verify our assumptions about complexity and another hardware features.

Thank you

`pperis@inf.uc3m.es`

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



M. Feldhofer, S. Dominikus, and J. Wolkerstorfer.

Strong authentication for RFID systems using the AES algorithm.  
In *Proc. of CHES'04*, volume 3156 of *LNCS*, pages 357–370, 2004.



M. Feldhofer, K. Lemke, E. Oswald, F. Standaert, T. Wollinger, and J. Wolkerstorfer.

State of the art in hardware architectures.  
In *Technical report, ECRYPT Network of Excellence in Cryptology*, 2005.



M. Feldhofer, J. Wolkerstorfer, and V. Rijmen.

AES implementation on a grain of sand.  
In *IEEE Proc. on Information Security*, volume 152, pages 13–20, 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,



## A. Juels.

Minimalist cryptography for low-cost RFID tags.

In *Proc. of SCN'04*, volume 3352 of *LNCS*, pages 149–164.  
Springer-Verlag, 2004.



## M. Jung, H. Fiedler, and R. Lerch.

8-bit microcontroller system with area efficient AES coprocessor for transponder applications.

*Ecrypt Workshop on RFID and Lightweight Crypto*, 2005.



## Datasheet Helion Technology.

MD5, SHA-1, SHA-256 hash core for Asic.

<http://www.heliontech.com>, 2005.



## Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels.

RFID Systems and Security and Privacy Implications.

In *Proc. of CHES'02*, volume 2523, pages 454–470. *LNCS*, 2002.



## I. Vajda and L. Buttyán.

Lightweight authentication protocols for low-cost RFID tags.

In *Proc. of UBICOMP'03*, 2003.



S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels.

Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.

In *Proc. of Security in Pervasive Comp.*, volume 2802 of *LNCS*, pages 454–469, 2003.



J. Yang, J. Park, H. Lee, K. Ren, and K. Kim.

Mutual authentication protocol for low-cost RFID.

*Ecrypt Workshop on RFID and Lightweight Crypto*, 2005.



K. Yksel, J.P. Kaps, and B. Sunar.

Universal hash functions for emerging ultra-low-power networks.

In *Proc. of CNDS'04*, 2004.



J.P. Yaps, J.P. Kaps, B. Sunar.

Energy Comparison of AES and SHA-1 for ubiquitous computing.

In *Proc. of EUC'06*, 2006.