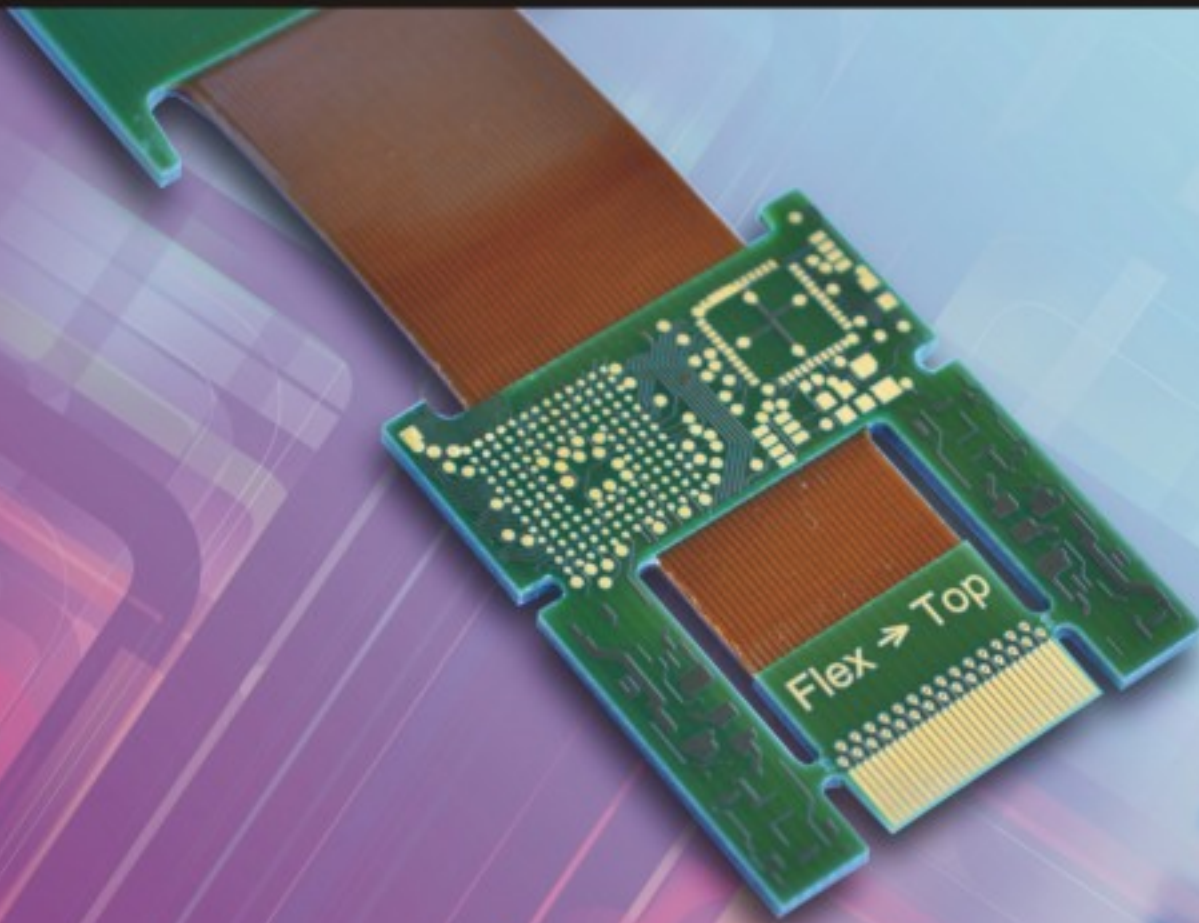


SENSORS & TRANSDUCERS

ISSN 1726-5479

vol. 152
5/13



Sensor Buses and Interfaces

International Frequency Sensor Association Publishing



Sensors & Transducers

**International Official Journal of the International
Frequency Sensor Association (IFSA) Devoted to
Research and Development of Sensors and Transducers**

Volume 152, Issue 5, May 2013

Editor-in-Chief
Sergey Y. YURISH



IFSA Publishing: Barcelona • Toronto

Copyright © 2013 IFSA Publishing. All rights reserved.

This journal and the individual contributions in it are protected under copyright by IFSA Publishing, and the following terms and conditions apply to their use:

Photocopying: Single photocopies of single articles may be made for personal use as allowed by national copyright laws. Permission of the Publisher and payment of a fee is required for all other photocopying, including multiple or systematic copyright, copyright for advertising or promotional purposes, resale, and all forms of document delivery.

Derivative Works: Subscribers may reproduce tables of contents or prepare list of articles including abstract for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution.

Permission of the Publisher is required for all other derivative works, including compilations and translations.

Authors' copies of Sensors & Transducers journal and articles published in it are for personal use only.

Address permissions requests to: IFSA Publisher by e-mail: editor@sensorsportal.com

Notice: No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

Printed in the USA.



Sensors & Transducers

Volume 152, Issue 5,
May 2013

www.sensorsportal.com

ISSN 2306-8515
e-ISSN 1726-5479

Editors-in-Chief: professor Sergey Y. Yurish,
Tel.: +34 696067716, e-mail: editor@sensorsportal.com

Editors for Western Europe

Meijer, Gerard C.M., Delft Univ. of Technology, The Netherlands
Ferrari, Vittorio, Università di Brescia, Italy

Editor for Eastern Europe

Sachenko, Anatoly, Ternopil National Economic University, Ukraine

Editors for North America

Katz, Evgeny, Clarkson University, USA
Datskos, Panos G., Oak Ridge National Laboratory, USA
Fabien, J. Josse, Marquette University, USA

Editor South America

Costa-Felix, Rodrigo, Inmetro, Brazil

Editors for Asia

Ohyama, Shinji, Tokyo Institute of Technology, Japan
Zhengbing, Hu, Huazhong Univ. of Science and Technol., China

Editor for Asia-Pacific

Mukhopadhyay, Subhas, Massey University, New Zealand

Editor for Africa

Maki K.Habib, American University in Cairo, Egypt

Editorial Board

Abdul Rahim, Ruzairi, Universiti Teknologi, Malaysia
Abramchuk, George, Measur. Tech. & Advanced Applications, Canada
Ascoli, Giorgio, George Mason University, USA
Atalay, Selcuk, Inonu University, Turkey
Atghiaee, Ahmad, University of Tehran, Iran
Augutis, Vygtantas, Kaunas University of Technology, Lithuania
Ayesh, Aladdin, De Montfort University, UK
Baliga, Shankar, B., General Monitors, USA
Basu, Sukumar, Jadavpur University, India
Bousbia-Salah, Mounir, University of Annaba, Algeria
Bouvet, Marcel, University of Burgundy, France
Campanella, Luigi, University La Sapienza, Italy
Carvalho, Vitor, Minho University, Portugal
Changhai, Ru, Harbin Engineering University, China
Chen, Wei, Hefei University of Technology, China
Cheng-Ta, Chiang, National Chia-Yi University, Taiwan
Chung, Wen-Yaw, Chung Yuan Christian University, Taiwan
Cortes, Camilo A., Universidad Nacional de Colombia, Colombia
D'Amico, Arnaldo, Università di Tor Vergata, Italy
De Stefano, Luca, Institute for Microelectronics and Microsystem, Italy
Ding, Jianning, Changzhou University, China
Djordjevich, Alexander, City University of Hong Kong, Hong Kong
Donato, Nicola, University of Messina, Italy
Dong, Feng, Tianjin University, China
Erkmen, Aydan M., Middle East Technical University, Turkey
Gaura, Elena, Coventry University, UK
Gole, James, Georgia Institute of Technology, USA
Gong, Hao, National Institute of Singapore, Singapore
Gonzalez de la Rosa, Juan Jose, University of Cadiz, Spain
Guillet, Bruno, University of Caen, France
Hadjiloucas, Sillas, The University of Reading, UK
Hao, Shiyong, Michigan State University, USA
Hui, David, University of New Orleans, USA
Jaffrezic-Renault, Nicole, Claude Bernard University Lyon 1, France
Jamil, Mohammad, Qatar University, Qatar
Kaniusas, Eugenijus, Vienna University of Technology, Austria
Kim, Min Young, Kyungpook National University, Korea
Kumar, Arun, University of Delaware, USA
Lay-Ekuakille, Aime, University of Lecce, Italy
Li, Si, GE Global Research Center, USA
Lin, Paul, Cleveland State University, USA
Liu, Aihua, Chinese Academy of Sciences, China

Mahadi, Muhammad, University Tun Hussein Onn Malaysia, Malaysia
Mansor, Muhammad Naufal, University Malaysia Perlis, Malaysia
Marquez, Alfredo, Centro de Investigacion en Materiales Avanzados, Mexico
Mishra, Vivekanand, National Institute of Technology, India
Moghavvemi, Mahmoud, University of Malaya, Malaysia
Morello, Rosario, University "Mediterranea" of Reggio Calabria, Italy
Mulla, Intiaz Sirajuddin, National Chemical Laboratory, Pune, India
Nabok, Aleksey, Sheffield Hallam University, UK
Neshkova, Milka, Bulgarian Academy of Sciences, Bulgaria
Passaro, Vittorio M. N., Politecnico di Bari, Italy
Penza, Michele, ENEA, Italy
Pereira, Jose Miguel, Instituto Politecnico de Setebal, Portugal
Pogacnik, Lea, University of Ljubljana, Slovenia
Pullini, Daniele, Centro Ricerche FIAT, Italy
Reig, Candid, University of Valencia, Spain
Restivo, Maria Teresa, University of Porto, Portugal
Rodríguez Martínez, Angel, Universidad Politécnica de Cataluña, Spain
Singhal, Subodh Kumar, National Physical Laboratory, India
Sadeghian Marnani, Hamed, TU Delft, The Netherlands
Sapozhnikova, Ksenia, D. I. Mendeleev Institute for Metrology, Russia
Singhal, Subodh Kumar, National Physical Laboratory, India
Shah, Kriyang, La Trobe University, Australia
Shi, Wendian, California Institute of Technology, USA
Shmaliy, Yuriy, Guanajuato University, Mexico
Song, Xu, An Yang Normal University, China
Srivastava, Arvind K., LightField, Corp, USA
Stefanescu, Dan Mihai, Romanian Measurement Society, Romania
Sumriddetchkajorn, Sarun, Nat. Electr. & Comp. Tech. Center, Thailand
Sun, Zhiqiang, Central South University, China
Sysoev, Victor, Saratov State Technical University, Russia
Thirunavukkarasu, I., Manipal University Karnataka, India
Thomas, Sadiq, Heriot Watt University, Edinburgh, UK
Tianxing, Chu, Research Center for Surveying & Mapping, Beijing, China
Vazquez, Carmen, Universidad Carlos III Madrid, Spain
Wang, Jiangping, Xian Shiyou University, China
Xue, Ning, Agiltron, Inc., USA
Yang, Dongfang, National Research Council, Canada
Yang, Shuang-Hua, Loughborough University, UK
Yaping Dan, Harvard University, USA
Zakaria, Zulkarnay, University Malaysia Perlis, Malaysia
Zhang, Weiping, Shanghai Jiao Tong University, China
Zhang, Wenming, Shanghai Jiao Tong University, China

Contents

Volume 152
Issue 5
May 2013

www.sensorsportal.com

ISSN: 2306-8515
e-ISSN 1726-5479

Research Articles

- Research on the Structure and Signal Transmission of Rotary Piezoelectric Dynamometer**
Zhenyuan Jia, Yongyan Shang, Zongjin Ren, Yifei Gao and Shengnan Gao 1
- Piezoelectric Sensor of Control Surface Hinge Moment**
Zongjin Ren, Shengnan Gao, Zhenyuan Jia, Yongyan Shang and Yifei Gao 11
- Research Algorithm on Building Intelligent Transportation System based on RFID Technology**
Chuanqi Chen 18
- Using Displacement Sensor to Determinate the Fracture Toughness of PMMA Bone Cement**
Yongzhi Xu, Youzhi Wang 27
- Study on the Applications of Fiber Bragg Grating and Wireless Network Technologies in Telemetry System of Atmospheric Precipitation**
Han Bing, Tan Dongjie, Li Liangliang, Liu Jianping 33
- An Energy-Efficient Adaptive Clustering Protocol for Wireless Sensor Network**
Lü Tao, Zhu Qing-Xin, Zhu Yu-Yu 41
- A Case Study of Event Detection Performance Measure in WSNs Using Gini Index**
Luhutyit Peter Damuut, Dongbing Gu 51
- Fault Diagnosis of Tool Wear Based on Weak Feature Extraction and GA-B-spline Network**
Weiqing Cao, Pan Fu, Genhou Xu 60
- The Research Abort Concept Restructuring of the Sensor Semantic Networks**
Guanwei 68
- Coordinating Reasoning Method for Semantic Sensor Networks**
Shi Yun Ping 76
- A Novel Intelligent Transportation Control Supported by Wireless Sensor Network**
Zhe Qian, Jianqi Liu 84
- Research on the Special Railway Intelligence Transportation Hierarchy and System Integration Methodology**
Meng-Jie Wang, Xi-Fu Wang, Wen-Ying Zhang, Xue Feng 89
- Application of a Heterogeneous Wireless Framework for Radiation Monitoring in Nuclear Power Plant**
Gu Danying 98

| | |
|--|-----|
| Acoustic Emission Signal Analysis of Aluminum Alloy Fatigue Crack <i>Wenxue Qian, Xiaowei Yin, Liyang Xie</i> | 105 |
| A New Ultra-lightweight Authentication Protocol for Low Cost RFID Tags <i>Xin Wang, Qingxuan Jia, Xin Gao, Peng Chen, Bing Zhao</i> | 110 |
| AGC Design in Frequency Modulation System for Voice Communication via Underwater Acoustic Channel <i>Cheng En, Chen Sheng-Li, Li Ye, Ke Fu-Yuan, Yuan Fei</i> | 116 |
| Joint Source-Channel Coding for Underwater Image Transmission <i>Chen Hua-Bin, Chen Wei-Ling, Li Ye, Cheng En, Yuan Fei</i> | 122 |
| Study on the Applications of Cross-Layer Information Fusion in Target Recognition <i>Xing Liu, Shoushan Jiang</i> | 129 |
| A Simple Tree Detector Using Laser and Camera Fusion <i>D. Wang, J. H. Liu, J. L. Wang, T. Li</i> | 137 |
| Simulation and Analysis of T-Junction Microchannel <i>Kainat Nabi, Rida Rafi, Muhammad Waseem Ashraf, Shahzadi Tayyaba, Zahoor Ahmad, Muhammad Imran, Faran Baig and Nitin Afzulpurkar</i> | 146 |
| Mass Flow Measurement of Fluids by a Helically Coiled Tube <i>Tian Zhou, Zhiqiang Sun, Zhenying Dong, Saiwei Li, Jiemin Zhou</i> | 152 |
| Comparative Creep Evaluation between the Use of ISO 376 and OIML R60 for Silicon Load Cell Characterization <i>Ebtisam H. Hasan, Rolf Kumme, Günther Haucke and Sascha Mäuselein</i> | 158 |
| Development of Noise Measurements. Part 3. Passive Method of Electronic Elements Quality Characterization <i>Yuriy Bobalo, Zenoviy Kolodiy, Bohdan Stadnyk, Svyatoslav Yatsyshyn</i> | 164 |
| Application of Mixed Programming in the Simulation of Lorenz Chaotic System's Dynamics Characteristics Based on Labview and Matlab <i>Peng Zhou, Gang Xu, Liang Chen</i> | 169 |
| A Nanostructure with Dual-Band Plasmonic Resonance and Its Sensing Application <i>Zongheng Yuan, Jing Huan , Xiaonan Li and Dasen Ren</i> | 174 |
| A Glucose Sensor Based on Glucose Oxidase Immobilized by Electrospinning Nanofibrous Polymer Membranes Modified with Carbon Nanotubes <i>You Wang, Hui Xu, Zhengang Wang, Ruifen Hu, Zhiyuan Luo, Zhikang Xu, Guang Li</i> | 180 |
| The Platform Architecture and Key Technology of Cloud Service that Support Wisdom City Management <i>Liang Xiao</i> | 186 |

Authors are encouraged to submit article in MS Word (doc) and Acrobat (pdf) formats by e-mail: editor@sensorsportal.com
Please visit journal's webpage with preparation instructions: <http://www.sensorsportal.com/HTML/DIGEST/Submission.htm>

Digital Sensors and Sensor Systems: Practical Design

Sergey Y. Yurish



Formats: printable pdf (Acrobat) and print (hardcover), 419 pages

ISBN: 978-84-616-0652-8,
e-ISBN: 978-84-615-6957-1

The goal of this book is to help the practitioners achieve the best metrological and technical performances of digital sensors and sensor systems at low cost, and significantly to reduce time-to-market. It should be also useful for students, lectures and professors to provide a solid background of the novel concepts and design approach.

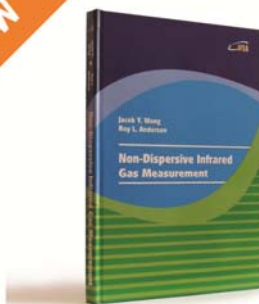
Book features include:

- Each of chapter can be used independently and contains its own detailed list of references
- Easy-to-repeat experiments
- Practical orientation
- Dozens examples of various complete sensors and sensor systems for physical and chemical, electrical and non-electrical values
- Detailed description of technology driven and coming alternative to the ADC a frequency (time)-to-digital conversion

Digital Sensors and Sensor Systems: Practical Design will greatly benefit undergraduate and at PhD students, engineers, scientists and researchers in both industry and academia. It is especially suited as a reference guide for practitioners, working for Original Equipment Manufacturers (OEM) electronics market (electronics/hardware), sensor industry, and using commercial-off-the-shelf components

http://sensorsportal.com/HTML/BOOKSTORE/Digital_Sensors.htm

NEW BOOK



Formats: printable pdf (Acrobat) and print (hardcover), 120 pages

ISBN: 978-84-615-9732-1,
e-ISBN: 978-84-615-9512-9

Jacob Y. Wong, Roy L. Anderson

Non-Dispersive Infrared Gas Measurement

Written by experts in the field, the *Non-Dispersive Infrared Gas Measurement* begins with a brief survey of various gas measurement techniques and continues with fundamental aspects and cutting-edge progress in NDIR gas sensors in their historical development.

- It addresses various fields, including:
 - Interactive and non-interactive gas sensors
 - Non-dispersive infrared gas sensors' components
 - Single- and Double beam designs
 - Historical background and today's of NDIR gas measurements

Providing sufficient background information and details, the book *Non-Dispersive Infrared Gas Measurement* is an excellent resource for advanced level undergraduate and graduate students as well as researchers, instrumentation engineers, applied physicists, chemists, material scientists in gas, chemical, biological, and medical sensors to have a comprehensive understanding of the development of non-dispersive infrared gas sensors and the trends for the future investigation.

http://sensorsportal.com/HTML/BOOKSTORE/NDIR_Gas_Measurement.htm

A New Ultra-Lightweight Authentication Protocol for Low Cost RFID Tags

¹ Xin Wang, ¹ Qingxuan Jia, ¹ Xin Gao, ¹ Peng Chen, ² Bing Zhao

¹ School of Automation, Beijing University of Posts and Telecommunications, Beijing 100876, China

² China Electric Power Research Institute, Beijing 100192, China

E-mail: buptwxin@gmail.com, zhaob@epri.sgcc.com.cn

Received: 15 April 2013 /Accepted: 15 May 2013 /Published: 27 May 2013

Abstract: The Radio Frequency Identification (RFID) system has been widely used in almost every aspects of the society. At present, the problem of security and privacy become a key factor of severely blocking the widespread of its usage. However, due to restraints on RFID tag's manufacturing cost, the traditional methods of encryption are not good candidate to defend the security of wireless communication channel between reader and tag. Designing lightweight or ultra-lightweight RFID authentication protocol has become a hot research topic recently. This paper proposes a new ultra-lightweight RFID authentication protocol with high robustness and execution efficiency. The proposed protocol requires only simple bit-wise operations, it has the characteristics of low storage requirement and communication cost. At the same time, through elaborate mechanism design, avoid the vulnerability of the existing ultra-lightweight authentication protocols. *Copyright* © 2013 IFSA.

Keywords: RFID, Security, Privacy, Ultra-lightweight, Authentication.

1. Introduction

Compare with bar-code, Radio Frequency Identification (RFID) has mesh points of non-contact recognition, batch read and remote access, identification of high speed moving object. It was widely used in supply chain management, access control, payment, retail inventory control or product tracking. With popularization and application of large-scale RFID system, the cost of RFID tag is one of the key factors that limit its development. However, the cost is too low is bound to bring about lower the tag's computational capabilities, storage capacity. Consequently, the traditional encryption schemes are no longer suitable for low-cost RFID tag, conduct correlation researches of lightweight or ultra-lightweight security mechanisms have become a hot research topic recently.

Recently, many ultra-lightweight protocols for RFID system have been proposed. However, they

have varies of flaws and weaknesses more or less. In 2006, Peris-Lopez et al. proposed a family of ultra-lightweight mutual authentication protocol, namely, UMAP protocol family [1-3], creates an interesting research direction. In UMAP, only simple bit-wise operations were adopted. Hence, the computational cost were very little suitable for low-cost tags. However, these protocols were demonstrated very vulnerable to de-synchronization attack, disclosed attack [4]. Chien et al. [5] proposed a new ultra-lightweight authentication protocol (SASI protocol) [5], this protocol introduced *ROT* operation and new and old dynamic identification provide greater security than UMAP. However, it is still vulnerable to trace attack, de-synchronization attack and full-disclosed attack [6, 7]. Gildas Avoine proposed a passive full-disclosure attack on SASI that works with any definition of the rotation [8]. P. D'Arco proposed de-synchronization attack and disclosed attack to SASI [9], only need 48.5 times to form

success de-synchronization attack on average. In addition, design the full-disclosed attack can disclose all the secret data. Pedro Peris-Lopez et al. (2009) put forward another ultra-lightweight authentication protocol, namely, Gossamer protocol [10]. The protocol introduced Double-Rot and *mixbits* algorithm which can better resistance to all sorts of common attacks. Thus, attackers can hardly get any useful information from tags. However, Tagra et al. proved that the protocol was insecure to de-synchronization attack [11]. Yun Tian (2012) proposed a new ultra-lightweight mutual protocol with permutation(RAPP protocol) [12], where the protocol adopted *Per* operation to break the orders of bits, compare with SASI protocol reached better encrypted and authentication effect. Unfortunately, Due to the design flaws, Wang Shao-Hui and Zahra Ahmadian, respectively, proposed effective de-synchronization attack and full-disclosed attack to RAPP protocol [13, 14].

In this paper, we propose a new ultra-lightweight RFID authentication protocol for low-cost RFID system. The proposed protocol can provide a security, stable and efficient channel for the legal tags and readers. The rest of this paper is organized as follows: Section 2, a new security protocol is proposed and description in details. Section 3, informal security analysis of the proposed protocol's ability against the attack modes, these attacks form great threats to existing RFID security protocols. Section 4, provide corresponding performance evaluation for the designed protocol. Finally, concludes are given in Section 5.

2. An Ultra-Lightweight RFID Protocol for Low Cost RFID Tags

2.1. Preliminaries and Notations

The RFID system mainly includes backend server, reader and tag. Due to working in Wireless network environment, the channel between reader and tag is vulnerable to a variety of severe attack modes. At the same time, due to backend server and reader have adequate computer power, storage space. The channel between them can adopt traditional encryption technology, the interactive operation between backend server and reader can be considered to be secure. To simplify the analysis, we only need design and analysis security certificate mechanism between reader and tag.

The notations used in the paper are denoted as follows:

- \oplus : Bit-wise XOR n_1 : Random number
- $+$: Addition mod 2 m, m=96
- ID : Static identification of the tag
- IDS_{old} / IDS_{new} : Tag's old/potential next dynamic identification

K_{old} / K_{next} : Tag's old/ potential next dynamic key
 $Rot(x, y)$: An $w(y)$ -bit left rotation on x , defined as follows:

```

z ← x
{z=z << w(y);}
return z;

```

(1)

where $w(y)$ denotes the Hamming weight of y .

mixbits(x, y) : Defined as follows:

```

z ← x
for (i=1; i<32; i++)
{z=(z >> 1)+z+z+y;}
return z;

```

(2)

Per(A, B): Let A and B are two L-bit word, where a_i and b_i is the i^{th} bit of A and B, such as: $A = a_1a_2...a_i...a_L$ $B = b_1b_2...b_j...b_L$,

where $w(A) = w(B) = m$, and $b_{k_1} = b_{k_2} = ... = b_{k_m} = 1$, $b_{k_{m+1}} = b_{k_{m+2}} = ...b_{k_L} = 0$,

Per(A, B) denoted as:

$$Per(A, B) = a_{k_1} a_{k_2} ... a_{k_m} a_{k_L} a_{k_{L-1}} ... a_{k_{m+2}} a_{k_{m+1}} \quad (3)$$

The shared secret values include $ID, K_{old} / K_{next}$ between reader and tag. To solve the problem of traceability, the dynamic identity IDS and secret key K are updated after each authentication session to resist traceability. Meanwhile, to resist de-synchronization attack, after each session ends, old and potential next dynamic identification and key were shared by reader and tag.

2.2. Protocol Description

The Protocol's thumbnail as shown in Fig. 1, it can be divided into two stages include: identification and authentication stage, update stage. The protocol detail is described in the following:

Phase 1: Identification and authentication

Step 1. Reader → Tag: *Hello*

The reader transmits handshake information "Hello" to tag

Step 2. Tag → Reader: *IDS*

After receiving the reader's handshake information, the tag transmits its dynamic identity *IDS* to the reader.

Step 3. Reader → Tag: *A* and *B*

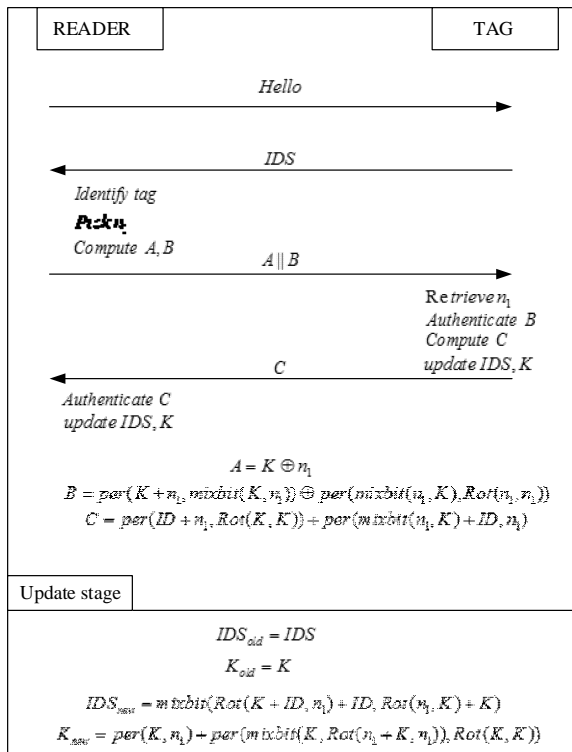


Fig. 1. An ultra-lightweight RFID protocol for low cost RFID Tags.

After receiving the tag's IDS , If the corresponding IDS_{new} cannot be found in the backend database, the reader will regenerate handshake information "Hello" to the tag. By this time, the tag will set $IDS = IDS_{old}$ and retransmits it to the reader. Or else, the reader adopts Pseudo-random number generator (PRNG) generates a random number n_1 , computer A and B as following:

$$A = K \oplus n_1$$

$$B = per(K + n_1, mixbit(K, n_1)) \oplus per(mixbit(n_1, K), Rot(n_1, n_1)) \quad (4)$$

Step 4. Tag → Reader: C

Upon receiving the reader's message $A || B$, the tag derives n_1 from the equation :

$$n_1 = A \oplus K \quad (5)$$

Then the tag computer B' with n_1 and K by the following equation:

$$B' = per(K + n_1, mixbit(K, n_1)) \oplus per(mixbit(n_1, K), Rot(n_1, n_1)) \quad (6)$$

If $B' = B$, the authentication gets through, the reader can be seen as legal. Then the tag computer C as following equation:

$$C = per(ID + n_1, Rot(K, K)) + per(mixbit(n_1, K) + ID, n_1) \quad (7)$$

The tag sends C to the reader. When the C is received, then the reader computer corresponding C' with local value in the backend server, if $C' = C$, the mutual authentication gets through, the protocol step into next phase, or else, the authentication protocol is failed.

Phase 2: Key updating

When the identification and authentication Phase between the reader and the tag is gets though, they update their Key and IDS each other in themselves as following equations:

$$IDS_{old} = IDS \quad (8)$$

$$K_{old} = K \quad (9)$$

$$IDS_{new} = mixbit(Rot(K + ID, n_1) + ID, Rot(n_1, K) + K) \quad (10)$$

$$K_{new} = per(K, n_1) + per(mixbit(K, Rot(n_1 + K, n_1)), Rot(K, K)) \quad (11)$$

Then both of them will update and save their $K_{old}, K_{new}, IDS_{old}, IDS_{new}$ in themselves, and update stage is finished.

3. Protocol Security Analysis

Currently, these attacks to break existing RFID authentication protocol mostly include as following: For one thing, attackers try to destroy the mutual message's confidentiality, integrity, availability; For another thing, an attacker could mount attacks by protocol's weaknesses, such as: de-synchronization attack, replay attack, disclosure attack and so on. We discuss our protocol's security as following:

Mutual authentication and Data confidentiality: Because of only genuine reader and genuine tag share secret values K, IDT , the mutual authentication between the tag and the reader can be go through by the messages A, B, C which are generated by the mixed operation of K, IDT, n_1 . At the same time, without knowledge of K , it is difficult to an attacker deduce the random number n_1 from $A || B || C$.

Thus, under the random number's protection, ensure the confidentiality and integrity of the static identification IDT and secret value K .

Tag anonymity and un-traceability: After every time success mutual authentication, the update of shared secret K and tag's dynamic identification IDS involve random number n_1 . Meanwhile, the introduced of $mixbits(x, y)$ operation overcome the weakness of hamming weight-invariant of RAPP protocol. Thus, the adversary cannot trace the same tag by the invariance of IDS .

Resistance to replay attack: Due to the generation of message $A || B || C$ involved new random number n_1 in each session, the attacker try to replay the message will not be approved. Moreover, the attacker could intercept the transmission of message C lead to the reader didn't update inter secret values. Meanwhile, send last time $A || B$ to the tag. However, the attacker cannot get any secret information and tag's internal states keep the same as the last session. It makes absolutely no sense to attacker.

Resistance to de-synchronization attack: Due to the use of radio link between the reader and the tag, the messages transmission can be interrupt easily by the malicious attacker or various natural factors. Hence, accidental transmission can result in de-synchronization between genuine reader and genuine tag. However, the protocol keeps the old and new key and dynamic identification, namely, $(K_{old}, K_{new}, IDS_{old}, IDS_{new})$. Hence, even if the message C transmission failed, the reader and the tag can make authenticate each other by the old key and dynamic identification. Thus, the protocol can return to the synchronization state.

In addition, the attacker make de-synchronization attack by change one or small bits in A , then obtain coordinated correctness pair (A', B', C') by change some bits on B or C . However, it is impossible to this way of attack, because of any slight changes can make the B and C almost change into a totally different number in our protocol.

Resistance to disclosure attack: The attacker may though change one or some bits in A and modified some bits on B and transmission them to the tag to verified the correctness of forged (A', B') , then infer some useful information from the response of the tag. However, constructed such (A', B') is almost impossible in our protocol, due to any slight modification in A will result to B varies greatly. Hence, the attacker cannot get any useful information for deduce secret information.

In addition, the introduce of $mixbits$ operation overcome the vulnerability of RAPP protocol proposed in [13].

In RAPP protocol, due to the improper use $ROT(x, x)$, lead to the problem as following:

When $[x]_i \neq [x]_{i+1}$, at the same time, denote $[x]_i$ stand for the bit at i position in x , $\bar{x}_{i,i+1}$ stand for the string with the same bit as x other than the bit of i and $i+1$:

$$\left\{ \begin{array}{l} per(y, ROT(\bar{x}_{i,i+1}, \bar{x}_{i,i+1})) \\ = per(y, ROT(x, x)) \\ per(y, ROT(\bar{x}_{i,i+1}, \bar{x}_{i,i+1})) \\ \oplus per(y, ROT(x, x)) = \bar{0}_{s,t} \end{array} \right. \quad (12)$$

The attack may adopt this vulnerability obtain the bit adjacent relation in x bit by bit.

In our protocol, the mechanism of $per(mixbit(n_1, K), Rot(n_1, n_1))$ effectively inhibited this way of attack, when $[n]_i \neq [n]_{i+1}$, $per(misbits(\bar{n}_{i,i+1}, K), ROT(\bar{n}_{i,i+1}, \bar{n}_{i,i+1}))$ and $per(misbits(n, K), ROT(n, n))$ have nothing relationship.

4. Protocol Performance Evaluation

Under the premise in security, computational cost, communication cost, storage requirement are metrics for evaluating whether a protocol's performance is fine. Table 1 compares the performance of our protocol with some common ultra-lightweight authentication protocols proposed recently. The protocol proposed in this paper has good performances base on ensure security.

Computational cost: The protocol only adopts simple bit-wise operation, such as XOR operation, modulo addition operation. In addition, we adopt non-triangular operations, such as ROT operation, $mixbits$ and per operation. The $mixbits$ operation only requires some right shift operation and modulo addition operation, the per operation only requires some simple permutation operation. Hence, even if to low-cost tag, these operations are easy to implement. At the same time, compare with SASI and RAPP protocol, our protocol only use one time pseudo random number generator in an interaction session, so save the computational cost and time.

Communication cost: The interaction messages transmitted between the tag and the reader mainly include $IDS || A || B || C$. The whole transmitted message demand 384 bits. Due to the fewer bytes in the transmission channel, the data transport time effective is cut.

Table 1. Comparison of Ultra-lightweight Authentication Protocols.

| Protocols | U-MAP family | SASI | GOSSA MER | RAPP | Ours |
|---|---------------------------|--------------------------------|-----------------------------|--------------------|--------------------------------|
| Protect user privacy | NO | YES | YES | YES | YES |
| Resistance to Desynchronization attacks | NO | NO | NO | NO | YES |
| Resistance to Disclosure attacks | NO | NO | YES | NO | YES |
| Mutual Authentication | YES | YES | YES | YES | YES |
| Total messages for mutual authentications | 4-5 L | 5L | 5L | 6L | 4L |
| Mesmory size on tag | 6L | 7L | 7L | 5L | 5L |
| Mesmory size for each tag server | 6L | 4L | 4L | 9L | 5L |
| Operations in the tag | $\oplus, \wedge, \vee, +$ | $\oplus, \wedge, \vee, +, ROT$ | $\oplus, +, ROT^2, MLXBITS$ | \oplus, ROT, Per | $\oplus, +, ROT, mixbits, Per$ |

L designates the bit length of variables used

Storage requirement: Each tag require 96 bytes read-only memory to preserve the static identification of tag, at the same time, needs 384 bytes erasable memory for the update of $(IDS_{old}, IDS_{new}, K_{old}, K_{new})$ in each session. Hence, the protocol needs little storage requirement and meet the requirement of low-cost RFID tag.

5. Conclusion

Privacy and security issues have become enormous challenges to the current RFID domain. It is one of the key problems to be solved that design high performance, strong security ultra-lightweight RFID authentication protocol for ensure the security of the channel between the reader and the tag. In this paper, we proposed a novel new ultra-lightweight RFID authentication protocol, the protocol require only simple bit-wise operation, meanwhile, ingenious adopt two non-triangular proposed recently: *mixbits* and *per* operation. Through the elaborate design, the protocol achieves better encryption and authentication effects. In addition, overcome the problem of pure to adopt *per* per operation which result in de-synchronization attack and full-disclose attack. The informal analysis indicated that the protocol resistance to common attacks in wireless transmission network. At the same time, compare with many existing ultra-lightweight authentication protocols, the protocol have characteristics of low computational cost, communication cost and storage requirement. Hence, the protocol proposed in this paper is highly efficient for low-cost RFID tags.

Acknowledgements

This work is supported by the National Basic Research Program of China (973 Program) (2012CB724400) and Special Program for International S&T Cooperation Projects of China (2013DFG72850).

References

- [1]. Peris-Lopez P., J. Cesar Hernandez-Castro, J. M. Estevez-Tapiador, et al. EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags, in *Proceedings of the OTM Federated Conf. and Workshop: IS Workshop*. November 2006, pp. 352-361.
- [2]. Peris-Lopez P., J. Cesar Hernandez-Castro, J. M. Estevez-Tapiador, et al. M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags, in *Proceedings of the Int'l Conf. Ubiquitous Intelligence and Computing (UIC '06)*, 2006, pp. 912-923.
- [3]. Peris-Lopez P., J. Cesar Hernandez-Castro. LMAP: A Lightweight Mutual Authentication Protocol for Low-cost RFID tags, *Hand. of Workshop on RFID and Lightweight Crypto*, 2006.
- [4]. Li Ticyan, Wang Guilin, Security analysis of two ultra-lightweight RFID authentication protocols, *Proceedings of the International Federation for Information*, 232, 2007, pp. 109-120.
- [5]. Chien, H. -Y. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, *IEEE Trans Dependable and Secure Computing*, Vol. 4, No. 4, 2007, pp. 337-340.
- [6]. Hung-Min Sun, Wei-Chih Ting. On the Security of Chien's Ultralightweight RFID Authentication

- Protocol, *IEEE Transactions on Dependable and Secure Computing*, Vol. 8, No. 2, 2011, pp. 315-317.
- [7]. Raphael C W, Phan, Cryptanalysis of a New Ultralightweight RFID Authentication Protocol—SASI, *IEEE Transactions on Dependable and Secure Computing*, Vol. 6, No. 4, 2009, pp. 316-320.
- [8]. Avoine G, Carpent X, Martin B., Privacy-friendly synchronized Ultralightweight authentication protocols in the storm, *Journal of Network and Computer Applications*, Vol. 35, No. 2, 2012, pp. 826–843.
- [9]. Paolo D’Arco, Alfredo De Santis, On Ultralightweight RFID Authentication Protocols, *IEEE Transactions on Dependable and Secure Computing*, Vol. 8, No. 4, 2011, pp. 548-563.
- [10]. Peris-Lopez P, J. Cesar Hernandez-Castro, et al. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol, *Information Security Applications*, Vol. 53, No. 79, 2009, pp. 56-68.
- [11]. Tagra D, Rahman M, Sampalli S., Technique for preventing DoS attacks on RFID systems, in *Proceedings of the 18th IEEE International Conference on Software Telecommunications and Computer Networks (SoftCOM’10)*, Bol, Island of Brac, Croatia, 2010, pp. 6-10.
- [12]. Yun Tian, Gongliang Chen, and Jianhua Li, A new ultralightweight RFID authentication protocol with permutation, *IEEE Communications Letters*, Vol. 16, No. 5, 2012, pp. 702-705.
- [13]. W. Shao-Hui, H. Zhijie, L. Sujuan, C. Dan-Wei, Security analysis of RAPP an RFID authentication protocol based on permutation, *Cryptology ePrint Archive*, Report 2012/327, 2012.
- [14]. Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref, Desynchronization attack on RAPP ultralightweight authentication protocol, *Information Processing Letters*, Vol 113, No. 7, 2013, pp. 205-209.
- [15]. Avoine G, Carpent X., Yet Another Ultralightweight Authentication Protocol that is Broken, in *Workshop on RFID Security - RFIDSec’12*, Lecture Notes in Computer Science, 2012.

2013 Copyright ©, International Frequency Sensor Association (IFSA). All rights reserved.
(<http://www.sensorsportal.com>)

SENSORS WEB PORTAL 

- MEMS
- NEMS
- NANOSENSORS
- SMART SENSORS

All about SENSORS
<http://www.sensorsportal.com>

The graphic features a dark blue background with a grid pattern. On the right, a computer monitor displays the Sensors Web Portal website. The text is primarily in yellow and white, with the IFSA logo in white and yellow.



The Fourth International Conference on Sensor Device Technologies and Applications

SENSORDEVICES 2013

25 - 31 August 2013 - Barcelona, Spain

Tracks: Sensor devices - Ultrasonic and Piezosensors - Photonics - Infrared - Gas Sensors - Geosensors - Sensor device technologies - Sensors signal conditioning and interfacing circuits - Medical devices and sensors applications - Sensors domain-oriented devices, technologies, and applications - Sensor-based localization and tracking technologies - Sensors and Transducers for Non-Destructive Testing

Deadline for papers: 30 March 2013

<http://www.iaia.org/conferences2013/SENSORDEVICES13.html>



The Seventh International Conference on Sensor Technologies and Applications

**Deadline for papers:
30 March 2013**

SENSORCOMM 2013

25 - 31 August 2013 - Barcelona, Spain

Tracks: Architectures, protocols and algorithms of sensor networks - Energy, management and control of sensor networks - Resource allocation, services, QoS and fault tolerance in sensor networks - Performance, simulation and modelling of sensor networks - Security and monitoring of sensor networks - Sensor circuits and sensor devices - Radio issues in wireless sensor networks - Software, applications and programming of sensor networks - Data allocation and information in sensor networks - Deployments and implementations of sensor networks - Under water sensors and systems - Energy optimization in wireless sensor networks

<http://www.iaia.org/conferences2013/SENSORCOMM13.html>



The Sixth International Conference on Advances in Circuits, Electronics and Micro-electronics

CENICS 2013

25 - 31 August 2013 - Barcelona, Spain

Deadline for papers: 30 March 2013

Tracks: Semiconductors and applications - Design, models and languages - Signal processing circuits - Arithmetic computational circuits - Microelectronics - Electronics technologies - Special circuits - Consumer electronics - Application-oriented electronics

<http://www.iaia.org/conferences2013/CENICS13.html>

Aims and Scope

Sensors & Transducers is a peer reviewed international, interdisciplinary journal that provides an advanced forum for the science and technology of physical, chemical sensors and biosensors. It publishes original research articles, timely state-of-the-art reviews and application specific articles with the following devices areas:

- Physical, chemical and biosensors;
- Digital, frequency, period, duty-cycle, time interval, PWM, pulse number output sensors and transducers;
- Theory, principles, effects, design, standardization and modeling;
- Smart sensors and systems;
- Sensor instrumentation;
- Virtual instruments;
- Sensors interfaces, buses and networks;
- Signal processing and interfacing;
- Frequency (period, duty-cycle)-to-code converters, ADC;
- Technologies and materials;
- Nanosensors;
- Microsystems;
- Applications.

Further information on this journal is available from the Publisher's web site:
<http://www.sensorsportal.com/HTML/DIGEST/Submission.htm>

Subscriptions

An annual subscription includes 12 regular issues and some special issues. Annual subscription rates for 2013 are the following:

Electronic version (in printable pdf format): 400.00 EUR

Printed with b/w illustrations: 640.00 EUR

Printed full color version: 760.00 EUR

40 % discount is available for IFSA Members.

Prices include shipping costs by mail. Further information about subscription is available through IFSA Publishing's web site: http://www.sensorsportal.com/HTML/DIGEST/Journal_Subscription.htm

Advertising Information

If you are interested in advertising or other commercial opportunities please e-mail sales@sensorsportal.com and your enquiry will be passed to the correct person who will respond to you within 24 hours. Please download also our Media Planner 2013: http://www.sensorsportal.com/DOWNLOADS/Media_Planner_2013.pdf

Books for Review

Publications should be sent to the IFSA Publishing Office: Ronda de Ramon Otero Pedrayo, 42C, 1-5, 08860, Castelldefels, Barcelona, Spain.

Abstracting Services

This journal is cited, indexed and abstracted by Chemical Abstracts, EBSCO Publishing, IndexCopernicus Journals Master List, ProQuest Science Journals, CAS Source Index (CASSI), Ulrich's Periodicals Directory, Scirus, Google Scholar, etc. Since 2011 *Sensors & Transducers* journal is covered and indexed by EI Compendex index (including a Scopus, Embase, Engineering Village and Reaxys) in *Elsevier* products.

Instructions for Authors

Please visit the journal web page <http://www.sensorsportal.com/HTML/DIGEST/Submission.htm> Authors must follow the instructions very carefully when submitting their manuscripts. Manuscript must be send electronically in both: MS Word 2003 for Windows (doc) and Acrobat (pdf) formats by e-mail: editor@sensorsportal.com

ADVANCES IN SENSORS: REVIEWS

2

Sergey Y. Yurish

Editor

Sensors and Biosensors, MEMS Technologies and its Applications



The second volume titled '*Sensors and Biosensors, MEMS Technologies and its Applications*' from the '*Advances in Sensors: Review*' Book Series contains eighteen chapters with sensor related state-of-the-art reviews and descriptions of the latest achievements written by experts from academia and industry from 12 countries: China, India, Iran, Malaysia, Poland, Singapore, Spain, Taiwan, Thailand, UK, Ukraine and USA.

This book ensures that our readers will stay at the cutting edge of the field and get the right and effective start point and road map for the further researches and developments. By this way, they will be able to save more time for productive research activity and eliminate routine work.

Built upon the series *Advances in Sensors: Reviews* - a premier sensor review source, it presents an overview of highlights in the field and becomes. This volume is divided into three main parts: physical sensors, biosensors, nanoparticles, MEMS technologies and applications. With this unique combination of information in each volume, the *Advances in Sensors: Reviews* Book Series will be of value for scientists and engineers in industry and at universities, to sensors developers, distributors, and users.

Like the first volume of this Book Series, the second volume also has been organized by topics of high interest. In order to offer a fast and easy reading of the state of the art of each topic, every chapter in this book is independent and self-contained. The eighteen chapters have the similar structure: first an introduction to specific topic under study; second particular field description including sensing applications.

Order online:

http://sensorsportal.com/HTML/BOOKSTORE/Advance_in_Sensors_Vol_2.htm



www.sensorsportal.com

ISSN 1726- 5479



9 771726 547001