Annales Mathematicae et Informaticae
44 (2015) pp. 151–164
http://ami.ektf.hu

Survey of attacking and defending in the RFID system

Tibor Radványi, Csaba Biró, Sándor Király, Péter Szigetváry, Péter Takács

Eszterházy Károly College, Eger, Hungary
radvanyi.tibor@ektf.hu
birocs@aries.ektf.hu
ksanyi@aries.ektf.hu
takip@aries.ektf.hu
szigipet@aries.ektf.hu

Submitted October 5, 2014 — Accepted May 5, 2015

Abstract

In this article we are dealing with the connections between nowadays most dynamically improving automatic identification-related RFID technology and cryptographic algorithms. You are going to be introduced to the possibility of attacks against RFID systems and the ways to defeat them. We are also dwelling on the suitable and non-suitable cryptographic algorithms among the well known and frequently used ones. The type of the RFID tag highly influences the group of the suitable algorithms. The size of the tag's integrated memory matters a lot, as well as the fact that it uses its own intelligence or we are working with a cheap passive tag.

Keywords: RFID, data security, cryptography, Gen2, AES, DES, RSA

MSC: 68U35, 68M01, 90B18, 94A860, 68P25

1. Introduction

Nowadays widespread forms of identification systems are in use. It means such code- and communication systems which identify people and objects uniquely. The most dynamically improving state-of-the-art identification system is the RFID (radio-frequency identification), using more channels in the electromagnetic frequency interval between 125 KHz and 2.4 GHz to carry out its functions. We can expand the basic frequency to the 2.4–5.8 GHz range. This range is called SHF. The reading distance here is above 3 m.

Paired with different types of sensors or location systems it can be used in many fields. This technology is employed in motor vehicle production, logistics, pharmaceutical and army technology, and in a lot of other areas. Modern passports, digital identifiers, and the newest ways of payment all take advantage of its identification and security opportunities. [12, 13]

2. The RFID Systems and the direction of their development

In this section we will be presenting the part of RFID focused on the transponders and readers. Because they are exposed to attacks.

The RFID has a great advantage over the bar code systems, that it does not require a direct view of the reading. When we want to read the barcode, we need to catch all products, on witch there is label or vignette. It is a very slow task and it requires a lot of human resources. Therefore it is expensive. At the same time we can read a lot of transponders. If we have due RFID reader with a well positioned special antenna, we can realize long-distance reading too. Storage capacity depends on the integrated chip's capacity. It can range from a couple of dozen bytes to a few megabytes.

The RFID system can be partitioned to isolated sections of equipments. These are the transponders, named tags, readers with transmitting and receiver aerials, middle-ware, database and the user applications. The user application can be developed to smart-phones, to tablets and to PCs. The primary targets for attacks are the tags, which store the identification and descriptive data. The readers and aerials are the other side of electro-magnetic communication. The readers can be attacked with software tools. If the attack is successful, through the software of the middleware the database can be infected. In this case the danger escalates, because all information can be lost or worse, if it falls into the wrong hands.

2.1. Passive tags

The passive tags are low-cost and can store large quantities of data. They do not have an active transmitter, so they can not radiate data independently. They use the radiated energy from the reader. They collect the energy out of the reader wave and with own aerials send back the modulated wave to the reader. The aerials must be well set and tuned, because the energy will be spread and the aerial of reader will not detect it. The usability is increased by special or hard housing in industrial applications. This method can increase the costs too. So the industrial hard tags are used identification of valuable objects . Typically these tags are used in LF

(125 KHz), HF (13.5 MHz), UHF (900 MHz) and microwave (2.4 GHz). Standards direct for their distribution. But these might vary from country to country. [1]

2.2. Active tags

Active tags have a independent transmitter with energy source. They can radiate the stored data continuously. The energy source is usually a battery that could last for some years. Sometimes the active tags contain an energy harvesting chip, which collects the energy from the background radiation. These tags use the 433 MHz, 2.4 GHz and 5.2–5.8 GHz frequency. The reading distance can be around 100 m. One or two order of magnitude can be the difference compared to the passive tags. The UHF passive tag can be read from a distance of 1–3 m, but the active tag can be read from 100 m. Their price can be very high, but it can fluctuate depending on the size of the memory, the life of battery and the kind of their wrapping. The active tags are appropriated by high-value containers, rail cars. If the tags are collected and reused at the end of the logistics process, you can save a lot in termsof cost. [1]

2.3. The RFID operation principle

Those RFID technologies , which use the LF and HF/NFC frequency, are characterized with the small distance reading. Between the tag and the aerial an inductive coupling builds up. There is a coil-antenna in the antenna of the reader and the tag. They create together an electro-magnetic field. The tag collects energy from this common EM field and with the help of it the tag can radiate back the stored data. Therefore the tag and the aerial of the reader must be near to each other. That means a couple of inches. These systems are less sensitive to interference caused by liquid and metal. So the LF and HF/NFC tags can be used better and more efficiently in these environments.

The passive UHF tags apply the propagation coupling. This coupling uses the backscatter communication method. Backscattering has important applications in astronomy, photography and medical ultrasonography. In this way the reader and the tag don't constitute a combined EM field. The tag uses the energy emitted by the reader to radiate back an altered (modulated) wave.

2.4. Fields of application

Application, where we can use RFID technology.

- Access Control Systems
- Identification of people and animals
- Identification of things
- Products, tracking vehicles

We can use it in toll systems, because it is fast, reliable and we can write back to the memory of the tag a timestamp or validating data. This technology can be well used in the following important cases: for retail sale, for the library and timing sport events. It is in the e-passport too. It is frequently used and very necessary while travelling, but as such, it is at serious risk. It can become the main target of attacks, primarily cloning attacks. The e-passport to expand requires additional means of protection or identification capabilities. This can be biometric identification, for example fingerprint, or retinal scanner.

3. Researching and improving the RFID in order to increase its efficiency; security or efficiency

Today's RFID protocols are formed in such a way that optimizing efficiency has become more highlighted than consumers' data security. We insist on using so-called cryptographic protocols to be able to save all the pieces of information in a trustworthy manner. Our aim is to broaden the tasks and only affect efficiency in a minimized way.Through this procedure communication with identification could be made more efficient and safe.

The RFID based identify-and-follow systems used in the retail trade environment are the living examples of this hidden working principle. However, there are numerous danger factors regarding this method. We can picture it the way that the personal tools, used by the consumers, contain invisible microchips. Via them smooth, discreet checks can be taken through different procedures. As during these checks data streams and exchanges are going on in the system, outsiders and users might get others' personal information. These problems are really important and require an swift solution as nowadays the protection of personal information is the top priority during the operation of a computer system. Some experiments have been done, some of them are used in practice, but sometimes the technology is unsafe even with them.

Finally, the priority of safe and clear information handling has been accepted and the importance of efficiency has been overtopped. We also agree with the thesis that the data security is our top most priority, especially in the case of systems where privacy is paramount. For example, bank services should rather be slower but safer, than faster with the possibility of less security.

4. Main attack possibilities

Algorithmic attacks: performed through the transfer channel. We separate active and passive ways of attacking. The passive method means that the attacker gets hidden messages by bugging a public channel. Contrary to the passive, during an active attack the attacker distributes on the channel himself. We can see the attacks on the figure 1. In this figure we can see some attacks against the RFID system. You can see the attacks can come from many directions. The attack can be aimed at the transponder, the communication channel and at the software and hardware system. The destruction and detachment are danger factors too, but they cannot be taken advantage of. [6, 7]

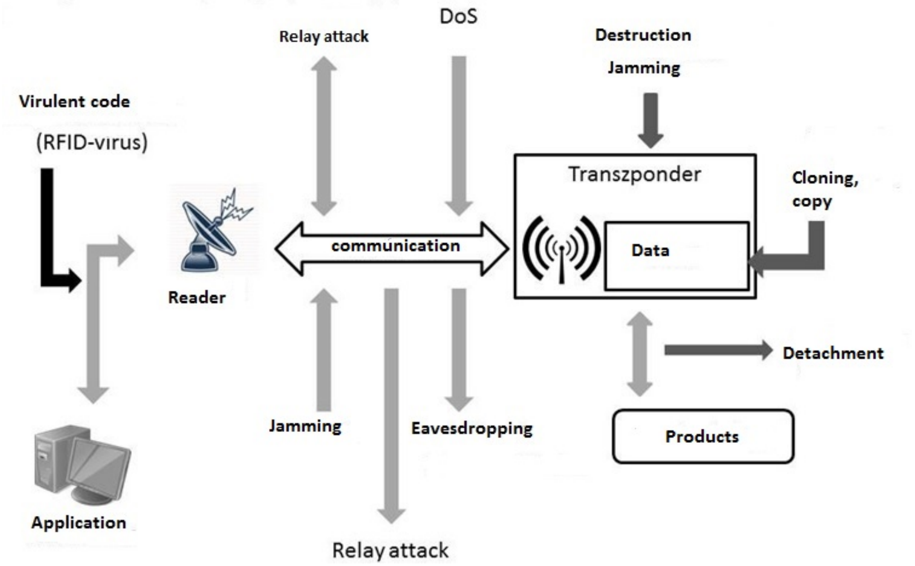


Figure 1: Attacks against the RFID system

4.1. Cloning a tag

If the RFID tag is not protected with encryption and we know its command set, function, and the memory partitioning, well, it is very easy to copy it or replace it with a copy. It causes problems if the system does not pay attention to the persistence of duplicated tags.

There are different complex solutions for storing data on tags. The simplest one is the read-only tag- it just contains an invariant unique identifier. If the read-only transponder gets close enough to the reader's field, it instantly wakes up and starts to radiate its identifier number. The attacker can easily create a clone which contains the exact same code. It is not necessary to get in physical touch with the transponder, we only need a reader which is able to read the identifier and write it to another. In more serious and complicated systems, where security is paramount we should avoid using read-only transponders and insecure data storage.

When working with more complex systems we should avoid using read-only transponders and unencrypted data storage. By default the transfer medium, in this case radio waves, transfer the data without encryption. Reading is not recorded on the transponder, so readings can be repeated without authorization.

Of course the transfer channel might be encrypted with the well-known encryption methods (DES, block encryption, RSA). Due to the small data quantity the transponder is able to store the key is usually small, so in case someone has the required amount of information the key can be decoded.

4.2. The Malware

Malware is malicious software, and its aim is to break and interfere with computer systems. RFID malware is a malware spreading through RFID tags.

A totally different type of threat comes to life when hackers and criminals make RFID tags work unexpectedly and maliciously. Through the queries of the computer-connected or the mobile readers hackers do it for the RFID tags' unique identifier, or for the data stored on the tag, which is usually the key for the database, or evokes a real action.

Until now everybody who works on RFID technology, silently claimed that reading the RFID tag cannot modify the background software, especially in a harmful way. Unfortunately they all were wrong. During a research it was proven that the RFID software has a weak point. A tag intentionally can be infected with a virus and the virus is able to infect the background database the RFID software uses. After that the virus can easily spread to other RFID tags.

For example: The perpetrator only needs to purchase a cheap item from the supermarket, which has a tag attached. After paying for the good he goes home and cuts off or destroys the tag. Then he puts an infectious tag on the product. Goes back to the supermarket, to the cash desk, and pays for the item again. But when the tag is scanned it infects the supermarket's product database, potentially inflicting any kind of damage, like changing the prices. But it means a far higher risk at airports. The virus might help drug smugglers or terrorists hide their packages. Furthermore, the infected database and luggage can infect other airports' databases as well. As a result of the virus packages might get to entirely different destinations than they ought to.

By this time the general structure of the problem has become clear. When an unsuspicious reader scans an infected tag, there is a risk that the tag takes advantage of a vulnerability in the middleware to evoke unwanted actions, like infecting the database. [10]

Classes of RFID malware:

1. The RFID exploit is a malicious tag data, using the parts of the RFID system it gets in touch with. RFID systems are as sensitive to hacker attacks as traditional computer systems. When a reader reads an RFID tag, it expects to get some information in a given format. However, someone can write a piece of data, the format and content of which are both so unexpected that it can influence the software, or potentially, the database of the RFID reader, too.

2. The RFID worm is an RFID-based exploit, taking advantage of the network connection to gain the ability of self-replication. RFID worms multiply by using the online RFID services, but they are able to spread themselves on tags as well. RFID worms make the unsuspicious RFID servers download

and out some files and carry out the instructions in them. This file aims to compromise the RFID middleware server the way most of the internet-based malwares do. The worm-infected RFID software is able to infect other RFID tags by overwriting their pieces of data with a replication of the RFID worm code.

3. The RFID virus is such an RFID-based exploit that replicates its code by itself to other tags without network access. RFID viruses might have contents that can interfere with or modify the RFID system's work in the background. As a freshly infected enters the world it infects other RFID systems (provided they use a common software system). Then these RFID systems infect other RFID tags, which infect other RFID software systems and so on.

4.3. Attack through the RF interface

Other types of attacks against RFID systems come through the RF interface. RFID systems communicate with the help of radio systems and electromagnetic waves both over short and long distance. This way the attacker has a chance to attack the RFID system through the radio frequency interface, as there is no need to get into physical connection with the reader or the transponder. One type of this attack is well known, so in the following paragraph We would like to explain it.

4.4. Eavesdropping

All kinds of wireless communications can be eavesdropped on a device which restrictive is made up of RFID technology. The attacker does not need energy and physical contact with the reader and the tag. Consequently, the attack can be performed from longer distances. The attacker has to catch the transmitted signals before the system stores it.

Eavesdropping occurs between the reader and the transponder. The effective range of the RFID systems vary between a few centimetres (e.g.: 13,56 MHz) to more meters (e.g.: 868 MHz). A radio's antenna requires a far smaller output voltage to get usable signals, so communication can be eavesdropped from a large distance.

Finke and Kelter have appointed that the 13.56 MHz inductively charged system can be eavesdropped from 3 meters. The receiver can sense the reader's motionless signals from hundreds of meters on a few kHz range. From a greater distance the signal might be disturbed by metal objects like fences, aluminium objects, or huge buildings. [14]

What does the success of eavesdropping our devices (reader and transponder) depend on? The number of influential factors is high.

- Depends on the characteristics of the RF space. This defines the geometry, structure and output power of the antenna.
- Interfering object between the reader and transponder and the size and location of metal objects are also an important factor.

- It is influenced by the quality, structure and geometry of the attacker's device, and also depends on the power emitted by the reader.

- It is also an important factor that passive or active transponders are used in the RF communication. If the tag is passive, it uses the power generated by the reader, this way the reflected useful information participates in the communication with lower energy usage. In the case of UHF tags (868 MHz – 915 MHz) 1–3 meter. If the tag is active or semi-passive so it has its own power source this range can be increased up to 10–30 meters. In case of active tags the emitted information is easier to catch due to its energy and easier to hide in larger attack areas. The at-tack area is a space where the attacker sets his eavesdropping device until he can perform a successful attack.

The following attacks may occur during eavesdropping:

- Secret or personal data may get into unauthorized hands. In this case the attack does not effect the communication, and it is almost impossible to detect the attack. Using cryptographic protocols may help defending the data.

- The attacker modifies the eavesdropped data and the false information is transmitted to the reader. This act requires a specific device and it is really hard to perform.

- Another possibility is that the attacker does not modify the data but replaces it. This could happen when the transponder sends a lot of information to the reader, so the communication requires much more time. In these cases of eavesdropping the attacker may get detected and his data blocked. Using control data, cryptographic algorithms and combinations of protocols may help detecting the attacker.

- The "relay attack" is a much more complicated type of eavesdropping and it also requires serious technical preparation. In this case the attacker does not only gather data but also transmits it on another channel. eg.: WIFI -– longer range. In the other place the data could get processed by an-other device eg.: during a purchase. This attack is really hard to block due to the properties of contactless payment methods. For the time being combined with other identifying methods it provides a good possibility. The simplest way is using a pin code but any personal or stationary biometric identification can be used. [15, 16]

It is clear that eavesdropping can be performed really easily sometimes. It holds a lot of possibilities for the attacker and it is really hard to detect and block. In order to protect data, if we can not secure the communication channel, we should make the information difficult to process in case of an attack. Cryptographic protocols provide data protection during in-formation exchange.

5. Cryptographic protocols - can be used?

Creating security in low-cost RFID systems is very difficult. Due to limited resources, strong ciphers are difficult or sometimes impossible to implement, so extremely simple algorithms and protocols need to be designed that take into account the limitations of passive systems. [8, 9, 11]

CrySys (Laboratory of Cryptography and Systems Security) recommends the XOR, and RSA.

The basic concept of development started out of the following:

$$R \to T : x \oplus k = a$$
$$T \to R : f(x) \oplus k = b$$

$$I(h, k) = H(x \oplus f(x))$$

where the

$$H(x \oplus f(x)) \text{ entropy of the } x \oplus f(x)$$

5.1. The XOR protocol

The structure of the XOR protocol is similar to the previous example, but it uses different keys in different directions. One option to achieve this the XOR key generation, where R randomly chooses a new k (i) , does XOR encryption, and performs k (i-1) key. We get the following protocol:

$$R \to T : x \oplus k_1 = a$$
$$T \to R : f(x) \oplus k_2 = b$$

We need a secure key-updating scheme.

$$R \to T : a^{(i)} = x^{(i)} \oplus k^{(i)}, k^{(i)} \oplus k^{(i+1)}$$
$$T \to R : b^{(i)} = x^{(i)} \oplus k^{(i)}$$

where $i = 2, 3, \ldots$ a counter, which is increased in every run, $x(i)$ the i-th random numeric and $k^{(0)}$ and $k^{(1)}$ shared keys are pre-set . $k^{(1)}$, $k^{(2)}$, $\ldots$ sequence does not change randomly, but the attacker cannot follow their value.

5.2. Other possibilities for defeating attacks

RFID systems are under different types of attacks.In several of these cases we need to protect the tag itself, but in other cases we have to inhibit the tag from being read and modified. In some countries where the e-passports are in use no copy-protection is provided for the users. We can prohibit cloning or attach-connected attacks with second level identification like a PIN code or biometric identification. Communication attacks are relatively easy to defeat with cryptographic methods as the messages can be encrypted with different algorithms.

6. Authentication

6.1. Legitimation based on derived keys

The main disadvantage of the legitimation mentioned above is that every transponder uses the same k encryption key. This feature means a potential danger factor for every similar application- which uses a very large number of transponders. Taking into consideration the fact that these transponders are available for everyone we have to consider the possibility of the key getting compromised. In this case the procedure becomes totally useless. To provide it, every transponder gets a unique key, increasing their security this way.

6.2. Encrypted data connection

We expand the previous situation with a potential attacker. Here the attackers can be divided into two groups. The first –Attacker1- tries to stay in the background and get useful information from the data store by eavesdropping and other passive methods. On the other hand Attacker2 actively takes part in the communication and modifies its content for his (or for someone else's) good. The cryptographic methods provide a solution against both attackers. The data which needs to be transferred (plain text) is encrypted so the attacker will not be able to reveal its original content. Random number generation is possible in such small sizes as the chip.Taking advantage of this, it is possible to expand cheap passive tags in order to implement the above mentioned encryption algorithms. [18]

6.3. Hash based access control

In case of the cheap smart labels it is necessary to provide a simple security scheme based on simple hash functions. The implementation of the algorithm is implemented in hardware. With this method the tags operating in closed and opened state are separating small slices from the memory in order to store so called metaIDs. The algorithms are relatively simple. The hash functions need to be implemented in the transponders. The scheme is flexible so it can be extended by multiple access or write authorizations. The meta-IDs are simple to query in this way the background database provides an easy building opportunity to third-party manufacturers. Furthermore the uniqueness of the meta-IDs may provide an easy identification.

6.4. Asymmetric key checking

Finally among the encryption methods the asymmetric key checking method needs to be emphasized. In this method when a reader wants to send data to a selected transponder (the message is v) it is enough for the tag generates a r random number during the transfer of listening-sensitive data and then sends it back to the reader. From this value the reader calculates the $v \oplus r$ then sends it to the tag. The listener who is out of the range of the backward channel just hears this $v \oplus r$ and he cannot conclude to value of the original v. [5]

Against eavesdropping we should detail and confirm the processes mentioned:

- The reader transmits a request to the tag.
- The tag identifies itself to the reader.

We try to force the defense to the communication between the tag and the reader, assuming that the inner data transmission between the reader and the background server is al-ready safe.

Of course the following protocol highly depends on the use of active or passive tags in the communication. The existing requirements are already different and the available computing capacity also shows a huge difference. Take a look at the communication scheme on figure 2.

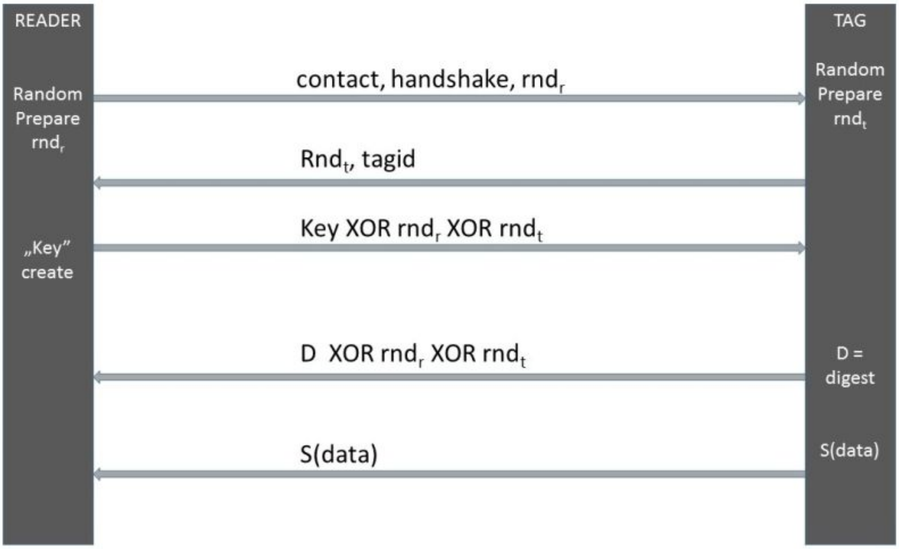


Figure 2: Reader and transponder communication

As shown we use a XOR function in the encryption which can be easily implemented on hardware level, so there is no difficulty in using it in passive tags. The XOR protocol uses different keys in different directions.

Also an S function appears which requires a little detail. First, consider the so-called P and S boxes. These are the basis of cryptographic algorithms. Their advantage is that they are easy to implement electro-technically. This way they can be integrated to the passive tag's limited set of tools. In case of active tags this is not a problem, because the tag contains intelligence, a programmable processor so the whole AES algorithm is feasible at a relatively low energy input and short time.

In case of passive tags we use the combination of P and S boxes. The P box is a function that creates an 8 bit output from and 8 bit input. A fast and simple electro-technical de-vice, and it's inverse function can be easily generated if we know the P box's assignment rule. It is responsible for mixing the 8 bit and a creating a bit permutation.

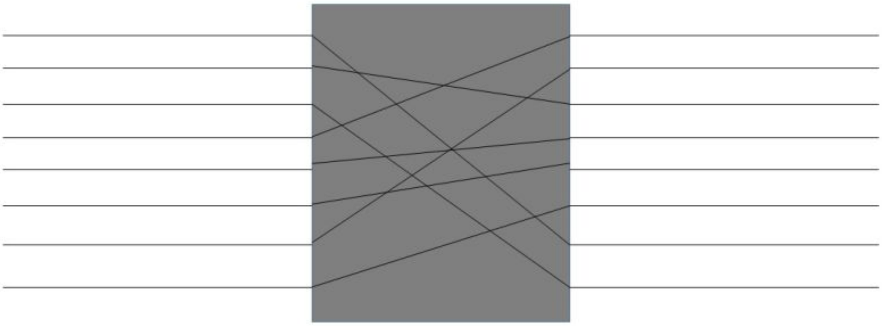
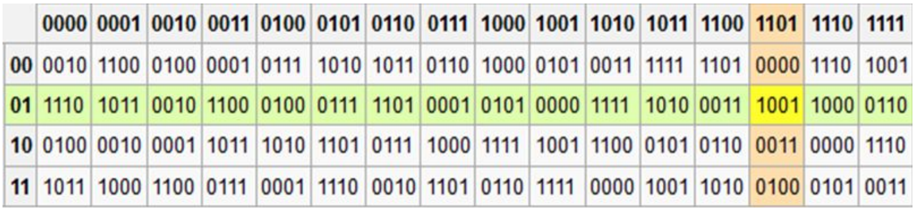


Figure 3: A possible P box

The S box is a device that implements a nonlinear function which creates 4 bit output from 6 bit input. [17] The operation of the S box is described by a table of 4 rows and 16 columns. Each S box has a different table. These tables allow us to encode the S box. Out of the incoming 6 bits the 1st and 6th gives the row indexes, while the other 4s decimal equivalent gives the column indexes. This way we get the 4 output bits based on the table cells.



	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Figure 4: A possible S box

Shows the S function, which generates the memory content of the user $S(data)$, and transmits it to the reader. This is a complex function that contains S and P boxes. As we know the used tables of S and P boxes.

$$S^{-1}(S(data)) = data$$

Based on this we get back the data stored in the tags. The use of S and P boxes is defined by the reader's key. The reader is a specific computer which has the computing and storage capacity that is required for generating keys and decrypting S(data). The tags are the electronic realizations of S and P boxes. For data control we create a digest from the stored data. The well-known HASH functions are suitable for solving this problem. We implement one of the HASH functions in the tags, eg.: SHA1 function. Using this method we are able to check the data after decrypting. This provides extra defense against data modifying, or data insertion attacks.

7. Conclusion

A product is exposed to many dangers during the way from the manufacturer to the costumer. From the factory it goes to a temporary storage, from there to a wholesale storage, from there to a retail distribution centre and finally the shelves of the supermarkets. This is a long process; during this the products can be lost, accidentally interchanged or stolen. EU regulations are pushing the responsibility of the manufacturer further and further so the traceability is becoming more and more important which can be implemented by RFID technology completely. During the production the way of the product is traceable, the technological orders, work phases and persons who took part in production or any other data. Use of RFID systems are changing nowadays. Many new technology are coming out, manufacturers and multinational companies are to carry these technologies to the users. Transponders come out from factories day by day cheaper and smaller; this helps their spread. Thanks to them being widespread, these systems can be found in more and more segments, so their vulnerability has to be considered scrutinously. Nowadays in Hungary reconciliation is in progress about mobile payment possibilities. Their spread might be a milestone for development. The users are not aware of the dangers of these. Most of them cannot or does not want to deal with this problem. So the manufacturers have to pay attention to the security, consider those possibilities that can cause any defect or data theft in systems surrounding users. Due to the decreasing production costs the data storage limit specific to cheap passive RFID systems is becoming irrelevant sooner or later. A move is in progress to active labels which can be used with more security and we don't have to create special algorithms in order to work on simple systems.

Acknowledgements. Tibor Radványi's research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP-4.2.4.A/ 2-11/1-2012-0001 "National Excellence Program".

The research of Csaba Biró, Sándor Király, Péter Szigetváry, Péter Takács was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of the TAMOP-4.2.2.C-11/1/KONV-2012-0014, title: The developing possibilities of RFID/NFC technology by the conception of "Internet of Things".

References

[1] Klaus Finkezeller, RFID Handbook, *Third Edition*(2010).

[2] Ziv Kfir and Avishai Wool, Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, `http://eprint.iacr.org/2005/052.pdf`.

[3] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim , KOMSCO, ICU, WPI Mutual Authentication Protocol for Low-cost RFID, 2005.

[4] Sebastien Canard, Iwen Coisel ,(Orange Labs RD, Caen, France) Data Synchronization in Privacy-Preserving RFID Authentication Schemes , 2008.

[5] Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu , (University of Massachusetts) Maximalist Cryptography and Computation on the WISP UHF RFID Tag, 2007.

[6] Sindhu Karthikeyan and Mikhail Nesterenko, RFID Security without Extensive Cryptography, 2005.

[7] M. McLoone and M.J.B. Robshaw, Public Key Cryptography and RFID Tags, 2008.

[8] Markku-Juhani O. Saarinen, Daniel Engels A Do-It-All-Cipher for RFID: Design Requirements IACR Cryptology ePrint Archive 2012, 317.

[9] SAARINEN, M.-J. O., Cryptanalysis of Hummingbird-1., In FSE 2011 (2011), A. Joux, Ed., vol. 6733 of LNCS, Springer, pp. 328—341.

[10] KROVETZ, T., AND ROGAWAY, P, The software performance of authenticated-encryption modes. In FSE 2011 (2011), A. Joyx, Ed., vol. 6733 of LNCS, Springer, pp. 306—327.

[11] ENGELS, D., SAARINEN, M.-J. O., SCHWEITZER, P., AND SMITH, E. M., The Hummingbird-2 lightweight authenticated encryption algorithm. In RFIDSec 2011 (2011), A. Juels and C. Paar, Eds., vol. 7055 of LNCS, Springer, pp. 19-–31.

[12] Biró Csaba, Radványi Tibor, Takács Péter, Szigetváry Péter, RFID rendszerek sebezhetőségének vizsgálata, MAFIOK 2013. ISBN: 978-963-358-035-6, 15–24 oldal.

[13] Radványi Tibor, Adatbiztonság az RFID alkalmazásakor, Acta Carolus Robertus 3(1) pp: 121–127, Gyöngyös, ISBN-978-963-269-201-2, 2012.

[14] Ernst Haselsteiner, Klemens Breitfuss, Security in Near Field Communication (NFC) Philips Semiconduc-torsMikronweg 1, 8101 Gratkorn, Austria.

[15] S. Yu, K. Ren, W. Lou, A privacy-preserving lightweight authentication protocol for low-cost RFID tags, in: IEEE MILCOM 2007, October 2007, pp. 1-–7.

[16] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, T.-C. Chen, An improvement on RFID authentication protocol with privacy protection, in: Third International Conference on Convergence and Hybrid Information Technology – ICCIT 2008, vol. 2, November 2008, pp. 569-–573.

[17] Lauren De Meyer, Beg Bilgin, and Bart ,Extended Analysis of DES S-boxes, Proceedings of the 34rd Symposium on Information Theory in the Benelux, 30-31 May 2013, Leuven, Belgium, pp. 140–146.

[18] Vikram Belur Suresh,On-Chip True Random Number Generation, Thesis, 2012, University of Massachusetts Amherst, Department of Electrical and Computer Engineering.