Agri-Food Traceability Management using a RFID System with Privacy Protection

Agri-Food Traceability Management using a RFID System with Privacy Protection

P. Bernardi C. Demartini F. Gandino B. Montrucchio M. Rebaudengo E.R. Sanchez
Politecnico di Torino, Dipartimento di Automatica e Informatica, Torino, Italy
E-mail: {paolo.bernardi, claudio.demartini, filippo.gandino, bartolomeo.montrucchio, maurizio.rebaudengo, erwing.sanchezsanchez}@polito.it

Abstract

In this paper an agri-food traceability system based on public key cryptography and Radio Frequency Identification (RFID) technology is proposed. In order to guarantee safety in food, an efficient tracking and tracing system is required. RFID devices allow recording all useful information for traceability directly on the commodity. The security issues are discussed and two different methods based on public cryptography are proposed and evaluated. The first algorithm uses a nested RSA based structure to improve security, while the second also provides authenticity of data. An experimental analysis demonstrated that the proposed system is well suitable on PDAs too.

1. Introduction

Traceability can be considered a key factor in agri-food sector. Improving tracking and tracing without loosing data privacy is requested both by laws and consumer organizations. In several countries laws on traceability have been made during last years:

- in the USA, "Farm Security and Rural Investment Act" requires country of origin labeling for many kinds of food, including perishable agricultural commodities [1];
- in EU, Regulation (EC) No 178/2002 of The European Parliament And of The Council of 28 January 2002 [2] establishes that food business operators shall be able to identify, for the competent authorities, any person who supplied them with alimentary commodities, and any business which takes food from them; they shall, also, label adequately food, in order to facilitate the traceability.

Agri-food companies often apply simple systems, based on paper documents. Some systems exploit barcode to identify commodities: by using the identification number in the barcode, it is possible to find, in the company database, the information about the food. Today, new opportunities for the food traceability come from the Radio Frequency Identification (RFID) technology.

RFID is widely adopted as a contactless identification technology. A typical RFID system is made up of: a reader, which creates an electromagnetic field, and some passive tags without an own voltage supply. They can be read only if they are in the interrogation zone of a reader which supplies the power required through a coupling unit. Today, the size of the RFID tag memory allows recording directly on every commodity all useful information for the competent authorities to trace it.

The use of RFID tags hazards the privacy. In the USA, many organizations, such as Consumer Privacy and Civil Liberties Organizations, are requesting attention to privacy threats [3]. In Canada, the Annual Report to Parliament 2005 of the Privacy Commissioner underlines the importance to ensure that RFIDs do not erode informational privacy rights [4]. In EU, in compliance with the Working Document adopted on 2005 by the European Data Protection Working Party [5], the national authorities, set up to protect personal information, established guidelines needed for a safe use of RFID technology [6].

The privacy threads, arose from RFID, involve dangers such as man tracking, personal belongings monitoring and industrial espionage.

Many solutions to the privacy problem have been analyzed, some of them are:

- *killing the tag* [7], a command can stop the tag at the point-of-sale.
- using *passwords* or *encryption* [8], which try to avoid unauthorized readings of the tag;

21st International Conference on Advanced Networking and Applications(AINA'07)
0-7695-2846-5/07 $20.00 © 2007 IEEE

- *changing tag ID* [9], the use of different IDs makes difficult to recognize a tag;
- *blocking the anti-collision system of the reader* [10], a special tag stops the correct functioning of the reader.

This paper proposes a system which allows competent authorities to manage alimentary traceability, preventing new privacy problems. In this system, food business operators shall record on the RFID tag information on their treatments, in compliance with one precise outline. The present size of the tag memory allows using the whole memory for traceability, or leaving a part for other independent aims, such as anti-counterfeit [11] or marketing. Stored data will be protected using the public key cryptography: every operator will record its treatments and only the competent authorities, using private-keys, will be able to decrypt the information. In this way, by means of the resulting ubiquitous data system, authorities could immediately access information on alimentary commodities under examination. The use of encryption allows protecting the memory area of the traceability system, without blocking the memory; it is, moreover, possible to use additional privacy protection systems, in order to ensure the privacy of the whole tag. To improve the security level we propose two different algorithms suitable for different situations:

- Nested Cryptography Algorithm (NCA), that uses encapsulated ciphertexts in order to enhance the security optimizing memory occupation;
- Authenticating Cryptography Algorithm (ACA), that proves the authenticity of information.

The remaining of the paper is organized as follows: in Section 2 background about traceability management, privacy threats, RFID characteristics and cryptography theory are introduced, while in Section 3 the traceability management system and the privacy protection system are detailed. Finally, in Section 4, system abilities and costs are evaluated. In Section 5 some conclusions are drawn.

2. Background

Within this section the description of privacy and traceability management goes into more depth. Tags properties are depicted, spotlighting different nomenclature and current organization. In addition, information theory for cryptosystems is introduced.

2.2. Traceability management

Rules about traceability and food label information change according to the country. According to [2], food business operators shall register the origin and the destination of the alimentary commodities they manage, and they shall label food to facilitate its traceability. In general, alimentary operators shall track the food to allow its tracing. A typical case of food tracking management is shown in Fig. 1:

- a *producer*, yields a commodity;
- a *second operator* buys the commodity, registers the producer data, transforms the commodity or joins it to other commodities and registers its treatments;
- a *distributor* buys the commodity and registers the previous operator data;
- a *retailer* buys the commodity and registers the distributor data.

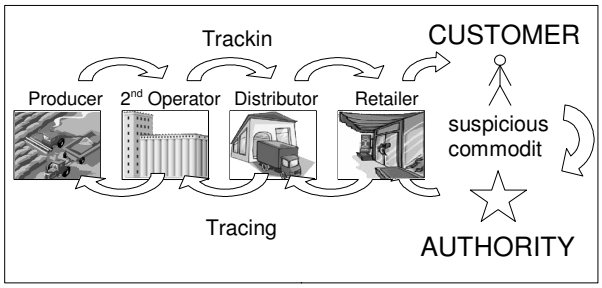

Figure 1. Agri-Food Tracking and Tracing

Whenever there are alimentary sophistications, contamination or infection caused by damaged food, the competent authorities control the retailer which sold them; the operator must search in its own centralized database to make available the information about its treatments and to identify any person who supplied it with food or any other substance included into the commodity. Then, authorities repeat the procedure with the next operator, and so forth. By using RFID tags to label alimentary commodities, every operator could write a copy of its data and of any other useful information directly on the tag, transforming the previous divided databases in only one ubiquitous database, and making the authorities' work easier and faster

2.3. Privacy Threats

Rules about privacy change according to the country, as well. However in many countries there is a great attention on privacy risks. There are many privacy threats connected to RFID [12][13]:

- The serial number of a tag can be associated with the customer's identity, so it is possible to monitor the customer or, knowing the object identified by the serial number, to get information for profiling. Besides knowing which object a person buys, it is possible to know how often a person uses it as well.
- Even without associating a tag number with a person identity, a set of tags can track an unidentified person, violating the "location privacy" [14].
- The transfer of a tag from a set to another set means that an object passes from a person to another one, so it is possible to know that there is a relation between those persons.
- By reading the tag's memory, it could be possible to know which commodities a person possesses.
- Companies would like to keep private their information, in order to avoid industrial espionage and unauthorized monitoring of their sales.

Privacy threats, due to recording of the tracking information on an RFID tag, are mainly the risk of unauthorized readings of information about the belongings of a person, and the industrial espionage. In this paper a solution to these problems is proposed.

2.4. RFID Tag Properties and Organization

A tag is composed by a radio frequency interface block, a memory component and a logic element. Tags have usually no battery (*passive* ones), so they acquire the power from the external radio frequency communication. Otherwise, a*ctive* tags have their own power supply. Commonly, computational capacities are extremely limited in a tag. The major concern of an RFID reader consists in accessing the tag's memory. Memory, which plays an important role in the tag architecture, may be a ROM or an EEPROM memory. It contains the unique identification number and may have up to several kilobits of storage capacity. Operational frequency used in an RFID system may vary from low frequencies (several kilohertz) to ultra high frequencies (a couple of gigahertz).

Despite the fact that some RFID tags are able to perform cryptographic operations [15][16][17] because of their internal logic circuitry, the majority of RFID devices have not real capabilities for cryptanalysis functions in part due to their power constraints. Most of RFID tags are passive ones, with limited processor performance and, hence, restricted computational resources.

While first generation tags did not even have memory for an identification number, current versions may have several kilobits for user memory. Our proposed traceability system is aimed for simple-passive tags with user memory.

2.5. Cryptographic Theory

Cryptographic algorithms have been used for decades in order to guarantee communication privacy. The proposed privacy system uses RSA [18] algorithm, that is based on public key cryptography, firstly presented in [19]. Many other applicable algorithms based on public-key cryptography have been proposed in the literature: El Gamal scheme [20], Knapsack scheme [21], Rabin scheme [22].

In a public key cryptosystem, given a pair of families $\{E_K\}_{K\in\{K\}}$ and $\{D_K\}_{K\in\{K\}}$ of algorithms representing inverting transformations, E_K:$\{M\} \rightarrow \{M\}$ and D_K:$\{M\} \rightarrow \{M\}$, on a finite message space {M}, the following must be true:

- for every $K \in \{K\}$, E_K is the inverse of D_K,
- for every $K \in \{K\}$ and $M \in \{M\}$, algorithms E_K and D_K are easy to compute,
- for almost every $K \in \{K\}$, each algorithm equivalent to D_K is computationally infeasible to derive from E_K,
- for every $K \in \{K\}$, it is feasible to compute inverse pairs E_K and D_K from K.

Therefore, by making $K = Ko$, a pair of ciphering functions D_{Ko} and E_{Ko} are fixed. The third property allows making public the key E_{Ko} without compromising the security of the secret key D_{Ko}. In this way, a *plaintext* message $P \in \{M\}$, may be ciphered by means of the public key. The result is a *ciphertext* message $C \in \{M\}$ that can be deciphered using the secret key. Thus, the following relation is true, $C = E_{Ko}(P) = E_{Ko}(D_{Ko}(C))$.

Secret and public keys are generated by means of the RSA algorithm as follows. Two large prime numbers n and p are chosen. The number of elements q in $GF(q)$ is computed by multiplying n and p. A random value E, relatively prime to $(n-1)(p-1)$, is picked. Subsequently, the number D is calculated $D=[k(n-1)(p-1)+1]/E$, with k chosen in order to make D an integer number. Private algorithm is defined as

$$D_{Ko}(P) = P^D \bmod q = C, \qquad (1)$$

and the public algorithm as

$$E_{Ko}(C) = C^E \bmod q = P. \qquad (2)$$

To avoid risks from chosen plaintext attacks and chosen ciphertext attacks, RSA is normally combined

with a padding scheme, such as OAEP [23]. The OAEP processes the plaintext prior to encryption in order to convert the RSA deterministic encryption scheme in a probabilistic scheme, and to prevent partial decryption of the plaintext.

The properties of the public key cryptosystem can be obtained exploiting the apparent difficulty of computing logarithms over a finite *Galois Field* with a number q of elements. Security is measured accordingly with the computational complexity of calculating the logarithmic operation. While it is widely believed that breaking the RSA encryption scheme is as difficult as factoring the modulus q, no such equivalence has proven [24].

While enlarging q improves system security, it also places constraints within computational time. The time required to calculate ciphering and deciphering functions is augmented mainly because of the size of the numeric values involved in the computation. Normally, a reasonable value for q should be on the order of 2^{1024}. Considering that regular bit length for numerical values is, at most, 64 bits in a computing system, appropriate algorithms should be used to manage 1024 bit or bigger values.

3. Traceability Management System

RFID tags could be defined as an unsecured channel, since they are a means of conveying information that intruders have the ability to read. In our system every operator in the agri-food chain has to write information about its treatments in a specific area of the commodity tag. Unfortunately, unauthorized persons can read tag information to know which kind of commodities an individual owns or to spy a competitor. As to address the privacy needs of a system, unauthorized readings of the tag memory should be forbidden. The traceability management and privacy protection system are described in the following.

3.2. General Architecture

At the present time, in order to find the operators that treated a commodity, the authorities have to follow a trail of breadcrumbs. They find the first operator and then they have to trace back, step by step, in order to detect any other.

In order to make easier authorities' work, we propose to create a ubiquitous tracking database, by labeling the alimentary commodities with an RFID tag. Every operator of the chain controls a part of the tag memory (*memory slot*) and it has to record its own data and its treatments information on it. In this way all the traceability information are immediately available to the competent authorities.

The tag memory is divided, at logic level, in a sufficient number of areas, to allow a sufficient number of operators to write. On the other hand, the size of a memory slot, that corresponds to the *Maximum Allowed Information Size* (MAIS) of each operator, must be large enough to store all its data. An accurate template is needed to streamline the use of the memory space. In way of employing a smaller memory area than using strings of characters, information must be translated in numerical codes. The use of codes to implement the traceability is under study also by EAN [25]. Codes have to identify operators, their geographic zone, their sector, the kind of commodity and the executed treatment types. The competent authority will fill in a reference table for any kind of code:

- *identification codes (IDC)* reference tables; a group of three tables that identifies the operator:
  - *geographic code (GC)* reference table; the first part of the code identifies the country, the second the region, and the last the municipality; the authorities, by using this code, can immediately identify the origin of a commodity;
  - *sector code (SC)* reference table; the sector code defines the kind of operator, e.g. “farmer” or “distributor”;
  - *operator identification (OID)* reference table; this code identifies the single operator;
- *commodity code (CC)* reference table; this code identifies the kind of commodity; it is useful when a food is made by different elements;
- *treatment code (TC)* reference tables; in every sector a table holds the list of the relevant operations, and their codes.

An operator must also write the IDC of its supplier, in order to enhance system reliability against frauds.

In the agri-food chain the commodity follows different steps. Initially the producer stores its data into the first memory slot. Step by step each operator adds its data. The following situation may modify the initial product:

- Simple treatment; the operator adds its data at the bottom of previous information.
- Merge of commodities; if the number of available memory slots is enough, the operator copies the information of all the old tags in the new one. If information regarding the commodities would overfill the memory, it writes only a summary, including a header (the summary special area identifier flag) and the identification

codes of suppliers that matched to commodity codes. Then the operator adds its data at the bottom of previous information.

- Partition of a commodity; the operator adds its data at the bottom of previous information, and it tags all the new commodities.

Operators must put in a database the data contained in all tags, in order to be able to prove, in case of an authorities' inspection, their propriety.

3.3. Privacy Protection System

We elaborated two cryptographic algorithms, adapted to different contexts. Both the algorithms are based on RSA algorithm. The two algorithms are presented in sections 3.4 and 3.5.

Periodically the competent authorities establish a set of Authority Public Keys (APuKs) and Authority Private Keys (APrKs) with different lengths, and distribute public key set to all operators.

For the common part of the algorithms, every operator encrypts a plaintext, by using one of the authority public keys, and it writes the resulting ciphertext in the appropriate memory area. The authorities can decrypt the ciphertext by using the private keys coupled to the public keys used by the operator. By changing private and public keys periodically, authorities can increase security; in fact, an unauthorized entity which finds some private keys could use them for a short period of time while authorities can decrypt old and new ciphertexts.

3.4. Nested Cryptographic Algorithm (NCA)

This system uses pairs of APuK and APrK of different length. To understand the benefit of using different key lengths, it is important to remember that enhancing the length of the keys increases security and ciphertext size. Each operator uses a particular APuK depending on its position in the chronological sequence of the production chain (increasing numbers, e.g., 1 for the farmer, and so on). The MAIS is the same for all operators. The tag memory is, at logical level, divided in slots with this size. The description of this algorithm is shown in the Fig. 2.

The first operator has the shortest key, the length of its key is equal to the MAIS. Its information is encrypted by the first APuK, and the relative ciphertext is written in the first memory slot.

The length of any operator APuK is equal to the MAIS multiplied by the number of the operator position in the chain. All operators, subsequent to the first one, compose their plaintext adding their information to the bottom of the previous ciphertext. After the encryption, operators write the new ciphertext in the first part of the memory tag, occupying a number of memory slots equal to the operator position. The last operator, theoretically the retailer, uses always the last and longest key. Its ciphertext occupies all the memory slots.

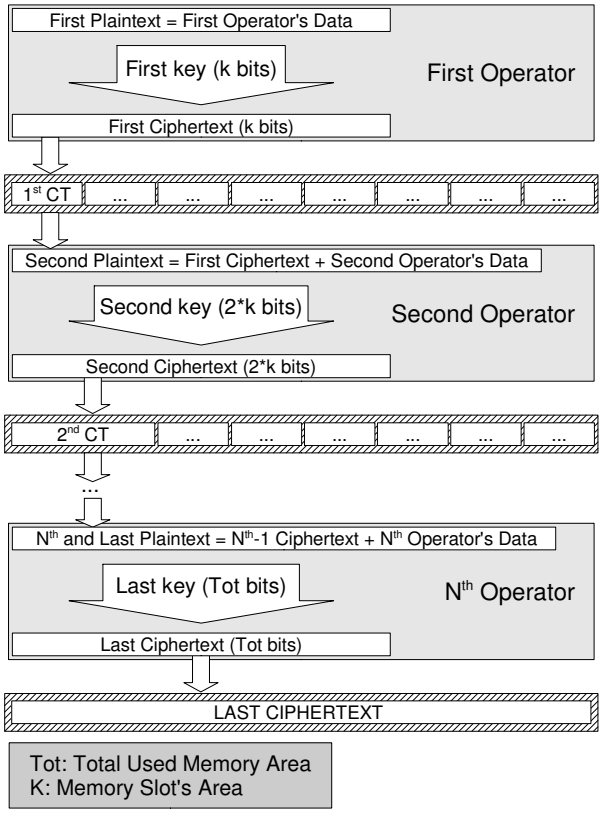

Figure 2. NCA Algorithm

At each chain ring the security grows. In the first part of the chain there is not a high security, the privacy of customers is not in danger, but the protection of information on the first businesses is low. Instead, out of the production chain, the security is to the maximum level.

Authorities decrypt, one by one, all the ciphertexts by using the correct private key.

3.5. Authenticating Cryptographic Algorithm (ACA)

In this system, there is only one APuK and one APrK. The memory slot size and, consequently the MAIS, is the same for all operators.

The scope of this system is to ensure also the authenticity of the message. Periodically every operator establishes its own Operator Private Key (OPrK) and

Operator Public Key (OPuK), and sends the OPuK to the authority. The pair of keys of the operator is used to prove the authenticity of the message. The description of this algorithm is shown in the Fig. 3.

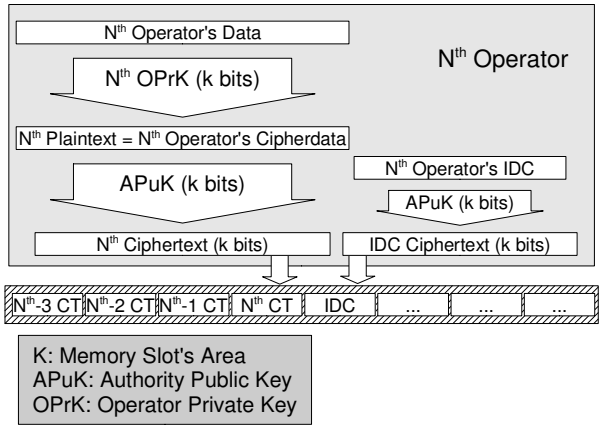

Figure 3. ACA Algorithm

The first step for operators is to translate their data by their OPrK. Since the OPrK is secret, only the authentic operator can write the cipherdata which can be decrypted by using its OPuK.

Every operator subsequent to the first erases the memory slot that contains the IDC of the previous operator.

Each operator encrypts its cipherdata and writes the resulting ciphertext in the first free memory slot, which contained the previous operator IDC.

The last step of every operator is to encrypt its IDC by using the APuK, and to write the resulting text in the first subsequent free memory slot.

Authorities decrypt the last used memory slot by using the APrK. In this slot there is the IDC of the last operator. The previous slot is decrypted by using the APrK and then by using the OPuK that is related to the IDC. Since all operators write the IDC of its supplier, authorities know what OPuK is correct to decrypt the previous memory slot.

This system protects from frauds by proving the message originality. The security level depends on the memory slot size.

4. Experimental Results

We experimentally evaluated the proposed technique implementing a prototype. Initially we filled out part of the code reference tables, sufficient to test the system. The simulation allowed knowing the performance time of the system and the differences among the cryptography algorithms.

To put into operation the system, the authorities need an RFID reader for mobile devices and a PDA with the reading software. The agri-food operators need an RFID reader to write on the tag. A small reader for mobile devices and a PDA with the writing software is enough as well. To increase the efficiency it is possible to use PCs with appropriate readers, instead. We used the following resources:

- RFID tag: SRIX4K from STMicroelectronics, passive tag, compliant with ISO14443, frequency 13.56 MHz, EEPROM with 4 kbits.
- RFID reader: ACG Dual ISO CF Card Reader Module from ACG, compliant with ISO14443, frequency 13.56 Mhz.
- Computing system: PDA with a 624 MHz Intel PXA270 processor.

In the simulation we use the whole memory, of 4096 bits, for the traceability system.

Table 1 shows the composition of the data in a memory slot. The first 10 bytes identify the commodity and the operator, the subsequent byte shows the number of treatments. Then each group of 7 bytes describes a treatment and its time.

Table 1. Memory Slot

Name	Code	Bytes
Geographic code - nation	GC1	1
Geographic code - region	GC2	1
Geographic code - city	GC3	2
Sector code	SC	2
Operator identification	OID	2
Commodity code	CC	2
Number of treatments	NoT	1
Treatment code – first one	1st TC	7
Treatment code – nth one	Nth TC	7
Supplier IDC	SIDC	8

In the NCA algorithm we set the MAIS to 512 bit, so a slot can hold at most 6 treatment codes. There are 8 keys, from 512 bit to 4096.

In the ACA algorithm we set the MAIS to 1024 bit. The security level depends on the length of the keys, so the MAIS is a compromise between the security and the number of memory slot.

We implemented the software by using a not optimized implementation of RSA algorithm, so the processing time cannot show the real performance of the system, but it can show the differences when using different key lengths. The authorities' check of a

memory slot, encrypted using a 512 bits key, in the NCA is completed in 3800 ms, in the ACA in 3930 ms, 3500 of which are spent by the decryption algorithm. Operators in the NCA employ 500 ms to entirely generate and write their ciphertext, in the ACA 3930 ms, the encryption needs on the order of 130 ms to be concluded. Anyway, by using a PC, with a Pentium 4 at 3.20 GHz processor, the decryption needs 62 ms and the encryption 1 ms; with a 4096 bit key the decryption needs 4125 ms, the encryption 31 ms. The difference between encryption and decryption comes from the use of a very optimized public key. Figures 4 and 5 show the encryption/decryption time. Although, this time table results from the simplicity of the used algorithm implementation; we did not attempt to improve it since its characteristics are not part of this paper objectives.

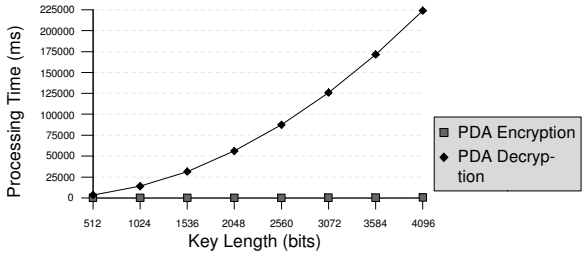

Figure 4. PDA Encryption/Decryption Time

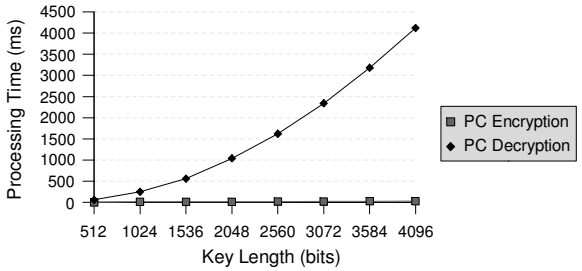

Figure 5. PC Encryption/Decryption Time

5. Conclusion

Today, an efficient management of the traceability is necessary; RFID technology offers the possibility to implement a rapid and effective ubiquitous system. Unfortunately, recording operators and commodity data on a RFID tag involves, in addition to standard RFIDs privacy problems, the risk of unauthorized readings of information about the belongings of a person, and industrial espionage. However, privacy can be protected by using an opportune cryptosystem: algorithms presented in this paper produce a satisfactory reply to these privacy problems.

Even considering the possible optimization of the cryptography algorithm implementation, the decryption time requires the use of a PC, while the encryption can be made simply by a PDA. The ACA implies one encryption and one decryption for any operation, so, unless using short keys, it requires a PC.

In the NCA it is not possible to lock an area until the subsequent operators have written on the tag, while the ACA requires larger tag memory to ensure a high level of security, but it allows locking a memory slot, after recording on it.

In order to increase the protection from fraud, also in the NCA it is possible to use the authenticating system, but it involves the management of a great number of keys and it extends the operation time.

Our traceability system, with a suitable RSA implementation, can satisfy efficiency and privacy demands. Future work involves the practical implementation of the proposed algorithms in a wine bottling chain. We think it could address the safety of alimentary commodities, improving actual standards.

This work was partially supported by “Progetto Regionale Ricerca Applicata 2004” and by “Laboratorio Wireless Sensor Networks – DIADI”.

References

[1] U.S. Federal Register, “Farm Security and Rural Investment Act of 2002 ”, Vol. 68, No. 210, October 30, 2003.

[2] Official Journal of the European Communities, “Regulation (EC) No 178/2002 Of The European Parliament And Of The Council of 28 January 2002“, Article 18.

[3] “RFID Position Statement of Consumer Privacy and Civil Liberties Organizations”, Privacy Rights Clearinghouse, November 30, 2003.

[4] Privacy Commissioner of Canada, “Annual Report to Parliament 2005 – Report on the Personal Information Protection and Electronic Documents Act”, pp. 39-42.

[5] Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data, “Working document on data protection issues related to RFID technology”, *ARTICLE 29 Data Protection Working Party*, January 19, 2005.

[6] Garante per la protezione dei dati personali, “"Smart (RFID) Tags": Safeguards Applying to Their Use”, Bollettino del n. 59/March 2005, March 9, 2005.

[7] EPCglobal, *13.56 MHz ISM band class 1 radio frequency (RF) identification tag interface specification*.

[8] Weis, S. A., Sarma, E. S., Rivest, R. L., and Engels, D. W., “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, *Security in Pervasive Computing*, 2003.

[9] A. Juels, “Minimalist Cryptography for RFID Tags,” *4th Conf. Security in Comm. Networks* (SCN), C. Blundo and S. Cimato, eds., Springer-Verlag, 2004, pp. 149-164.

[10] A. Juels, R. Rivest, and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID tags for Consumer

Privacy," *8th ACM Conf. Computer and Comm. Security*, V. Atluri, ed., ACM Press, 2003, pp. 103–111.

[11] P. Bernardi, et al., "An Anti-Counterfeit Mechanism for the Application Layer in Low-Cost RFID Devices", 3rd IEEE International Conference on Circuits and Systems for Communications, July 2006, pp.207-211.

[12] A. Juels, S. Garfinkel, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security and Privacy*, vol. 3, no. 3, pp. 34–43, May/Jun. 2005.

[13] A. Juels "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[14] Alastair Beresford and Frank Stajano. "Location Privacy in Pervasive Computing", *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[15] S. Weis. Security and privacy in radio-frequency identification devices (master thesis), May 2003.

[16] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Proc. Workshop on Cryptographic Hardware and Embedded Syst.*, M. Joye and J.-J. Quisquater, Eds. New York: Springer-Verlag, 2004, vol. 3156, Lecture Notes in Computer Science, pp. 357–370.

[17] A. Juels and S.Weis, "Authenticating pervasive devices with human protocols," in *Proc. Advances in Cryptology*. New York: Springer-Verlag, 2005, vol. 3621, Lecture Notes in Computer Science, pp. 293–308.

[18] R. L. Rivest. A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, pp. 120-126. Feb. 1978.

[19] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[20] T. El Gamal, "A public-key cryptosystem and a Signature scheme based on Discrete Logarithms," IEEE Trans. on Info. Theory, Vol. IT-31, pp. 469-472, 1985

[21] B. Chor, R. Rivest, "A Knapsack-type public-key cryptosystem based on Arithmetic in Finite Fields," IEEE Trans. on Info. Theory, Vol. IT-34 (5), pp. 901-909, 1988.

[22] M. O. Rabin. "Digitalized signatures and public key functions as intractable as factorization". Techbical Report, MIL/LCS/TR212, MIT Lab. Computer Science, Cambridge, Mass., January 1979.

[23] M. Bellare and P. Rogaway. "Optimal Asymmetric Encryption - How to Encrypt with RSA". In Eurocrypt '94, LNCS 950, pages 92-111. Springer-Verlag, Berlin, 1995.

[24] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[25] EAN-UCC *Traceability Implementation*, EAN International, 2003.