Public Key Cryptography on RFID tags
"A survey on the GPS identification scheme"

Spyridon Antakis

Eindhoven University of Technology
Department of Mathematics & Computer Science
Email: s.antakis@student.tue.nl

June 7, 2009

Abstract

In the last few years, a lot of research effort has been made in the area of *Radio Frequency Identification (RFID)* technology. The widespread deployment of RFID tags and their increased usage in open environments brought on surface a need for supporting more advanced security features. Applying *public-key cryptography* constitutes an attractive solution and until now there are several proposed models. However, the RFID hardware introduces a number of limitations with respect to computational power and production cost and thus the feasibility of such attempts is always questionable. This paper, presents a survey in the area of public-key cryptography on the RFID systems and focuses on the *GPS identification scheme*, which was one of the first innovated proposals for low-resources hardware. It describes a promising GPS scheme variant that can be applied to RFID devices and it discusses some of the experiments that have already been performed.

Keywords: *GPS identification scheme, RFID tag, Public-Key Cryptography.*

1 Introduction

Although, RFID technology has been available for several decades, the *21st century* constituted the beginning of a totally new period for the usage of RFID tags. The low production cost, the accuracy of the provided identification mechanisms and the many additional features that RFID systems were able to deliver, constituted an ideal combination for a broad commercial adoption. However, as it was expected, the revolutionary deployment revealed several concerns about the adequate security level that the RFID technology should support.

In the case of RFID tags, the decision about the usage of *public-key cryptography* for ensuring a higher level of security is a question that has a debatable answer. Usually, the security features are closely related to the environment in which a RFID system functions and of course they are also connected to the achievable non-negligible production cost for each tag. In fact, a common tag has a production cost of *5 cents* and respectively a tag which is able to perform public-key computations, costs even *five times more*. Therefore, it is understandable that in a RFID production line this difference causes a signicantly raise that exceeds the intended cost and makes the RFID hardware for supporting public-key cryptography, unacceptable expensive. Nevertheless, as technology evolves and new varieties of RFID applications are designed with the intention to be used in open environments (e.g. tolls, public transportations, passports, etc.), an increased demand for higher security even at low cost RFID tags appears.

During the past, several *identification schemes* that use public key cryptography have been proposed for low-cost devices. The proven ability of some of these schemes to function efficiently with limited computational resources by maintaining an adequate level of security, make them seem a quite promising and appealing solution for the RFID tags [8]. In this paper, we present the *GPS identification scheme*, which was proposed by M. Girault [1] in 1991 and proved secure by J. Stern and G. Poupard [2] in 1998. In section 2, a detailed description of the basic scheme is made and a brief security analysis is performed.

After that, an optimized GPS variant that followed and uses elliptic curves, is discussed. Finally, in section 3 some of the already performed experiments are presented and the paper concludes about the feasibility of GPS identification schemes on RFID tags.

2 GPS Identification Scheme

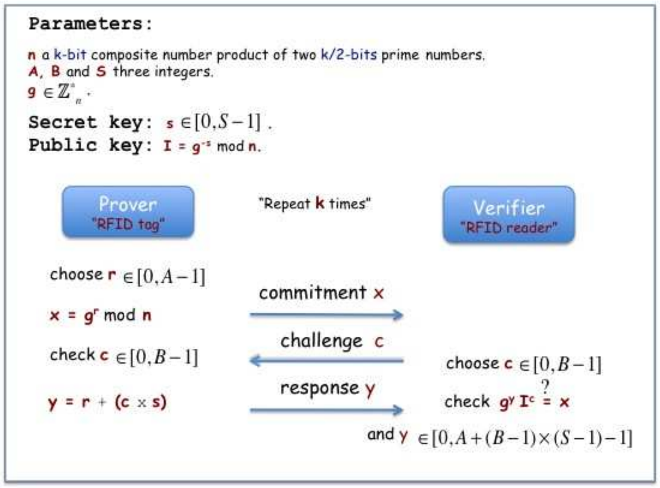
GPS, is basically a modified identification scheme that was developed as an efficient alternative of Schnorr's protocol. In 1989, C.P. Schnorr [3] presented a new asymmetric identification scheme which was based on the difficulty of the *"Discrete Logarithm Problem (DLP)*[1] *modulo a prime integer"*. However, this scheme had to perform modular reductions during the identification phase and thus the needed computational power was significantly higher than the one that a RFID tag, could support.

The GPS identification scheme improves the Schnorr's proposal and successfully minimizes the computational cost, as it decreases the modular reductions on the performed computations. In comparison to Schnorr's scheme, the GPS is based on the equivalent difficulty of the *"Discrete Logarithm Problem (DLP)*[1] *modulo a composite integer"*, where the composite integer is the product of two large prime integers. Moreover, as it is reported in [7], neither the order of the multiplicative group nor the order of the group element is needed to be known and thus the scheme can be used with most cryptographic group structures. In practice, GPS is a flexible *zero-knowledge* identification protocol that involves two parties, called *the prover* and *the verifier.* By the characterization zero-knowlegde, we simply express the fact that the prover is able to convince the verifier about the validity of a given statement without revealing any information beyond the truth of the statement [11]. In the case of RFIDs, the tag would prove that it contains a tag-specific secret to the reader and in that way the reader will be sure that the tag is indeed genuine.

There are several optimized GPS variants, but the initial proposal came from Girault's scheme which used the idea of *self-certified* public keys [1]. This section, presents the basic GPS identification scheme as it is standardized by ISO [4] and it makes a short security analysis for the basic scheme. Finally, it describes a GPS variant which is based on elliptic curve theory and uses pre-computed *coupons.* [5, 9, 10].

2.1 Basic GPS identification scheme

The basic GPS identification scheme uses a number of public parameters and the message exchange is performed into three steps. First, the prover sends a *commitment* x and then receives a *challenge* c from the verifier. After that, the prover depending on both the challenge and the secret private key sends a *response* y and the verifier checks the validity of the answer.



Parameters:

n a k-bit composite number product of two k/2-bits prime numbers.
A, B and S three integers.
$g \in \mathbb{Z}^*_n$.

Secret key: $s \in [0, S-1]$.
Public key: $I = g^{-s} \bmod n$.

Figure 1: *Basic GPS identification scheme.*

[1] DLP : Given a group $\mathbb{Z}_n$ and elements $g, h \in \mathbb{Z}_n$, find an integer x such that $g^x = h$. [12]

More precisely, before the identification round are defined, a secret key s such that $s \in_R [0, S-1]$ and a public key I such that $I = g^{-s} \ mod \ n$, where g is an element chosen from the group $\mathbb{Z}_n^*$. In a single identification round (fig. 1) the prover randomly chooses an integer r such that $r \in_R [0, A-1]$. Then, he computes the commitment $x = g^r \ mod \ n$ and he sends x to the verifier. After that, the verifier answers with a challenge c, which is chosen randomly such that $c \in_R [0, B-1]$. The prover checks that indeed $c \in [0, B-1]$ and computes the response $y = r + c \times s$. Finally, he sends y to the verifier who checks if $g^y I^c = x$ and if $y \in [0, A + (B-1) \times (S-1) - 1]$.

After a successfully message exchange at every involved stage, the last equality holds, since it will be: $g^y I^c = g^{r+cs}(g^{-s})^c \ mod \ n = g^r \ mod \ n = x$ and y indeed will belong to $[0, A + (B-1) \times (S-1) - 1]$ if all the parameters are chosen inside the defined sets. Based on the specification of the protocol, a complete identification procedure consists of repeating k times a single identification round. However, in many implementations k is taken for efficiency reasons such that $k = 1$, but without affecting the security of the scheme [2].

By implementing the GPS identification scheme on a RFID system, it is obvious that the pre-described roles of the prover and verifier, are now corresponding to the *RFID tag* and the *RFID reader*, respectively. During the design phase of such an implementation and especially for the side of the RFID tag, a decision must be made with respect to the provided features of the hardware. The increased need for computational power that appears and the fact that the hardware at the same time must remain inexpensive, induces a contradiction that must be balanced. Usually, the restricted environment of low-cost RFID tag is not able to perform complicated and expensive computations and a scheme optimization is necessary.

By examining closely the case of the basic GPS scheme, we realize that there are 2 expensive computations that the RFID tag should make in each identification round, an exponentiation and a modular reduction. On the other hand, the computations performed on the side of the RFID reader are not so expensive and if we consider also the fact that the reader is usually more powerful than the tag, then all the effort for optimization is focused on the side of the tag.

Looking at the basic GPS scheme, in order the tag to create the commitment x will have to perform the *exponentiation* g^r and then compute the result with respect to *modulo* n. These computations constitute a significant drawback and become really unaffordable for the RFID tag. Even if the basic GPS scheme tries to increase the computational efficiency by removing the modulo reduction that Schnorr's scheme introduced for the response y, the need for further optimization of the scheme seems unavoidable. In the following section, a brief security analysis for the basic GPS scheme is given and after that, a GPS elliptic curve variant which aims to exclude this kind of expensive computations is presented.

2.1.1 Security Analysis of the basic GPS identification scheme

The security of the basic GPS identification scheme is based on the assumption of the intractability of extracting discrete logarithms and since n will be a composite number, the problem is also related to factorization problem. By making this assumption, it is proved in [2] that:

- An *honest* user is always accepted.
- Given a public key I, if an attacker is accepted with non-negligible probability then he could be used to efficiently compute discrete logarithms modulo n in base g. So, by assuming that that the discrete logarithm problem is intractable, such attacks are not feasible.
- Even if prover is identified many times, essentially no information about his secret key can be retrieved by *passive eavesdroppers* or *cheating verifiers.*

In practice, each of the used parameters has a specific meaning for the security of the scheme. The parameters A, B and S are integers which constitute the upper bounds for the protocol and they are defined as follows: $A = 2^\rho$, $B = 2^\delta$ and $S = 2^\sigma$. The values ρ, δ and σ, constitute the security parameters of the scheme and they represent the binary size of the value that belongs respectively to each defined set. Therefore, in our case ρ will declare the binary size of the random exponent r, δ will declare the binary size of the challenge c and σ will declare the binary size of the private key s. In order the protocol to provide a sufficient level of security by maintaining also the proper efficiency for low-cost devices, a number of standard values should be chosen for the security parameters. The value of S is conditioned by the complexity of the existing algorithms for solving the discrete logarithm problem and thus σ should be greater or equal to 160 bits. The choice of B is related to the probability of impersonation of an adversary and therefore δ should be at least equal to 32 bits, since in that way it guarantees that an adversary cannot impersonate a user with probability larger that 2^{-32}. Finally, the parameter A must be large enough to guarantee the zero-knowledge property and therefore according to [4, 10], ρ is usually taken such that $\rho = \sigma + \delta + 80$.

Furthermore, the novelty of the scheme comes from the fact that all modulo computations can be performed with the use of a composite number n. The number n must be the product of two large prime numbers (usually 512-bits each), such that factoring n to be really difficult. In order to prevent n from being factored, a number n greater than 1024 bits should be chosen since from a practical point of view it is enough to ensure a high level of security based on the intractability of factorization. If n is chosen to be a prime number, then in this case we obtain an alternative *"on the fly"* version of Schnorr's scheme which is reported to be secure for n greater than 768 bits [5]. Finally, the element $g \in \mathbb{Z}_n^*$ must be chosen in such a way that computing discrete logarithm to be hard and as it is reported in [2], in many cases g is taken for efficiency reasons such that $g = 2$, but without reducing the security of the scheme.

For a full and detailed security analysis of the basic GPS identification system, the reader can refer to the proof which J. Stern and G. Poupard presented in [2] and also in the publication that M. Girault, G. Poupard and J. Stern made for groups of unknown order, in 2006 [7].

2.2 GPS Elliptic curve scheme variant

As it is presented in [9, 10], the GPS elliptic curve scheme variant combines several characteristics from different modes of use of GPS [5]. The security of the scheme is based on the equivalent *Elliptic Curve Discrete Logarithm Problem (ECDLP)*[2], which is considered to be really hard. The security parameters ρ, δ and σ are also present in this scheme and they follow exactly the same security restrictions that were discussed in section 2.1.1. In comparison to the basic scheme, this variant includes different operations which are combined in order to succeed the best possible performance for the tag. In fact, the main idea on the message exchange is preserved but the applied modifications create a totally new approach (fig. 2).

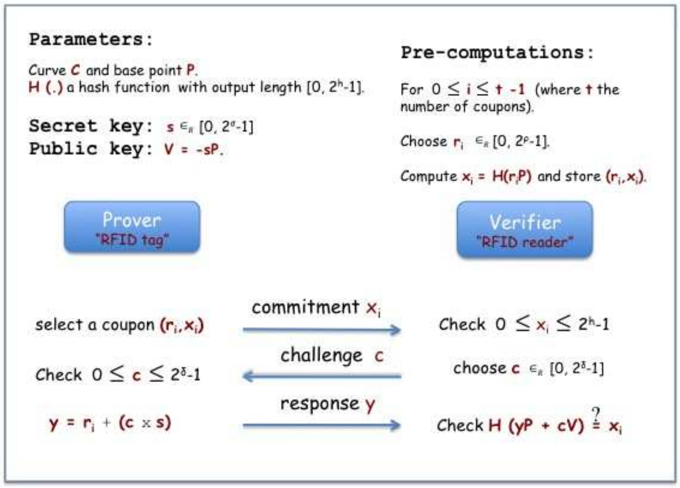


Figure 2: *GPS Elliptic curve scheme variant.*

A pre-computation phase is introduced and a method that is based on the storage of *coupons* is used. At initialization, t coupons are pre-computed and stored inside the RFID tag. A coupon consists of a randomly number r_i which is chosen such that $r_i \in_R [0, 2^\rho - 1]$ and a value x_i which is computed such that $x_i = H(r_i\mathcal{P})$, where $H()$ a hash function. After the end of the pre-computation phase, all the created coupons which have the form of pairs (r_i, x_i) for $0 \leq i \leq t-1$, are stored inside the RFID tag.

[2] ECDLP: Given an elliptic curve $\mathcal{E}$ defined over a finite field $\mathbb{F}_q$, and two points P, $Q \in \mathcal{E}(\mathbb{F}_q)$, find an integer l such that $lP = Q$ [12].

The initialization of the parameters in this variant are based on the elliptic curve theory and the computations are transformed in order to meet the needs of the new identification scheme. More precisely, an elliptic curve $\mathcal{C}$ is determined with a base point $\mathcal{P}$, a secret key s is chosen such that $s \in_R [0, 2^\sigma - 1]$ and a public key V is computed such that $V = -s\mathcal{P}$. When the identification phase starts, the RFID tag selects one of the pairs of the pre-computed coupons and sends as a commitment the value x_i. The RFID reader checks that indeed $0 \leq x_i \leq 2^h - 1$, where h the number of the communicated bits that are produced from the chosen hash function $H()$. Then, he replies with a randomly chosen challenge c, such that $c \in_R [0, 2^\delta - 1]$. The tag checks that $c \in [0, 2^\delta - 1]$ and computes the response $y = r_i + c \times s$. Finally, the tag sends y to the reader who checks if $H(y\mathcal{P} + cV) = x_i$. Indeed, if the message exchange is performed properly then the last equality holds, since it will be: $y\mathcal{P} + cV = (r_i + cs)\mathcal{P} + c(-s)\mathcal{P} = r_i\mathcal{P} \Rightarrow H(r_i\mathcal{P}) = x_i$.

Comparing the elliptic curve scheme with the basic GPS scheme, we observe that the expensive computations that were performed on the side of the RFID tag have been efficiently replaced. The scheme is using elliptic curves and thus it is able to generate smaller bit sizes for the exchanged messages but without decreasing the level of the provided security. The usage of 160 bits is enough to ensure an adequate level of security for the commitment x_i and thus that leads to a less demanding implementation with respect to the performed computations [8]. Furthermore, the usage of a pre-computation phase with coupons is really beneficial for the efficiency of the scheme, since the RFID tag avoids the complex operation of modular exponentiation. A set of coupons can be pre-computed by a trusted third party and stored to the RFID tag at manufacturing time. In this way, the only operations left to the RFID tag are one integer multiplication and one integer addition which are necessary to calculate the response $y = r_i + c \times s$. However, these computations are non-modular integer operations and thus are not so computational expensive for the RFID tag.

Finally, the usage of a hash function gives to the scheme another important advantage. According to [13] a hash function significantly decreases the storage requirements of coupons and minimizes the number of bits which must be transmitted between RFID tag and RFID reader during identification. In practice, a hash function is used to decrease the size of the commitment x_i. If a hash function is not used, then the x_i will maintain the number of bits that are produced from the computation of $r_i\mathcal{P}$. Thus, the usage of the hash function guarantees that the produced output would be 256 bits or even less, depending every time on the hash function (e.g. SHA-256) which is used. Since the commitments can be pre-computed on a computationally powerful device, the tags do not even need to know anything about the hash function and thus the hardware of the RFID tag is not involved.

3 Experiments & Performance

The existing optimized GPS variants offer a number of appealing features and capabilities. Variants like the elliptic curve scheme constitute a promising solution and they are able to minimize the computational cost. However, during the experimental phase a necessity for extra modifications appears and the pre-described GPS schemes is possible to take a new form. The limitations that the tag introduces with respect to computational power and storage space should be faced with the most efficient way, but without also missing any security properties. The trade-off between performance and security is unavoidable and applying public-key cryptography by using GPS identification schemes becomes a real challenge.

Until now, there are only a few published works that demonstrate results which could be considered applicable on RFID tags. This section gives an overview of some important performed experiments on GPS schemes variants and briefly discusses the alternatives that they use for obtaining better performance. Finally, it reports the security concerns which are introduced by some of the additional features used on the GPS scheme variants.

3.1 Low Hamming Weight challenge

In 2004, *M. Girault* and *D. Lefranc* [6] published an interesting proposal that can be applied on the basic GPS identification scheme. After a number of conducted experiments, they successfully transformed the multiplication that is performed at the side of RFID tag when computing the response $y = r + c \times s$, into a single addition. In this way, they succeeded to improve the computation cost for the reply that the tag must sent to the reader and thus they introduced a new solution that could be efficiently applied on RFID tags. In practice, they showed that even if usually the challenges are randomly chosen such that $c \in_R [0, 2^\delta - 1]$, any other subset of $\mathbb{Z}^+$ of the same cardinality is also suitable. They proposed to use challenges with *Low Hamming Weight (LWH)*, which means that the total number of bits that constitute c and which are equal to *one*, should be low. They demonstrated that in the generation of c, the bits equal to *one* should be separated by at least $\sigma - 1$ *zero* bits, where σ the binary size of the private key s. In this way, they created an alternative scheme that was able to effectively substitute the multiplication $c \times s$ with a serial addition of r with a modest numbers of repetitions of s.

In practice, this approach introduced some drawbacks with respect to the bit-size of the involved values. More precisely, the total number of bits of the challenge c was significantly increased and since c had a LHW, the only solution in order to decrease the size of c was to use a compression algorithm. Finally, if the size of c remained uncompressed then the product $c \times s$ was going also to be increased and thus in order not to lose the zero-knowledge property, the randomly chosen value r had to be very large. Despite of these obstacles, the proposal constituted an interesting reference for the researchers that followed and in combination with other additional features such as the pre-computed coupons, yielded promising results for resource-constrained environments.

3.2 Pseudo-Random Number Generator

In 2007, *M. Girault*, *L. Juniot* and *M.J.B. Robshaw* [8] performed an experiment which was based on the GPS elliptic curve scheme variant and the method of *Low Hamming Weight* challenge. More precisely, in order to design an even more efficient scheme they modified the functionality of pre-computed *coupons*, by introducing the usage of a *Pseudo-Random Number Generator (PRNG)*. In practice, they suggested the implementation of a sufficiently compact PRNG inside the RFID tag at the time of manufacture. The purpose of this random generator was to compute each r_i once at the time of manufacture and a second time on the RFID tag, when it was needed for computing the response y (fig. 3). The main advantage of this approach was that the RFID tag was saving a significant storage space, since instead of the storing the full coupon (r_i, x_i) had only to store the pre-calculated value of x_i.

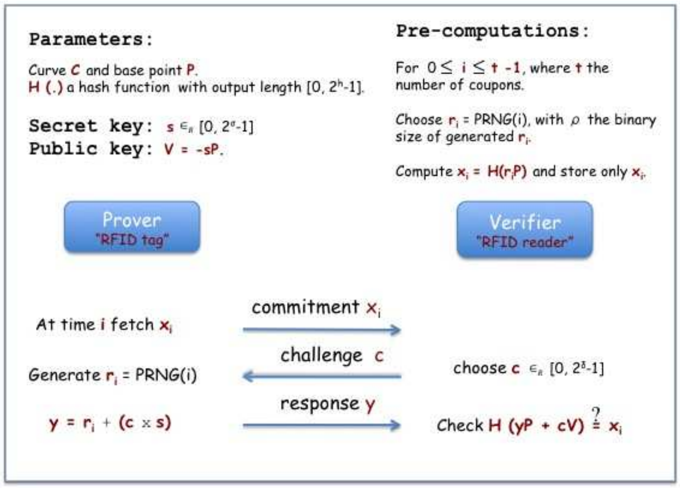

Parameters:
Curve C and base point P.
H (.) a hash function with output length $[0, 2^h\text{-}1]$.
Secret key: $s \in_R [0, 2^\sigma\text{-}1]$
Public key: $V = -sP$.
Pre-computations:
For $0 \leq i \leq t - 1$, where t the number of coupons.
Choose r_i = PRNG(i), with ρ the binary size of generated r_i.
Compute $x_i = H(r_iP)$ and store only x_i.
Prover
"RFID tag"
Verifier
"RFID reader"
At time i fetch x_i
commitment x_i
challenge c
Generate r_i = PRNG(i)
choose $c \in_R [0, 2^\delta\text{-}1]$
response y
$y = r_i + (c \times s)$
Check $H(yP + cV) \overset{?}{=} x_i$

Figure 3: *GPS scheme variant with PRNG.*

Moreover, the scheme applied the LHW technique in order to calculate the challenge c and reported as desired security parameters the following values : $\sigma = 160$ bits for the size of the secret key s, $\delta = 860$ bits for the size of the challenge c and $\rho = 1100$ bits for the size of each r_i. The 160 bits were enough to guarantee the security of the secret key s, since the scheme was based on elliptic curves. The 860 bits ensured that impersonation attacks are not feasible and the 1100 bits provided the scheme with the zero-knowledge property. At first sight, the scheme seemed inefficient due to the large values of challenge c and r_i. However, the authors succeeded to represent the 860 bits of *Low Hamming Weight* challenge

c with 25 bits by using a compression algorithm and they stated that the r_i values are generated from the PRNG, thus there are no storage implications for the RFID tag.

In conclusion, the careful combination of the several different features contributed to an efficient scheme. The conducted experiments, demonstrated a promising performance and showed that this scheme is able to function in a low-resources environment. The storage requirements for the tag were minimized and the authors presented a quite successful and feasible implementation of public key cryptography for RFID tags.

3.3 Concerns about the security

The fact that the basic GPS identification scheme was proved to be secure in [2], does not necessarily imply that all the followed variants are also secure. The usage of the same restrictions for the security parameters with the ones that the basic GPS scheme uses and the assumptions which are based on a proven difficult problem, are not always enough to guarantee the security of the scheme. The additional features that are introduced, in many cases hide vulnerabilities for the new designed schemes which are not obvious right from the start. Considering also that these schemes have not been tested yet to real life implementations, then the provided security becomes even more uncertain. Until now, there are two possible vulnerabilities that they have been revealed and could constitute a critical threat for the GPS-based RFID applications, *Denial of Service (DoS)*[3] attacks and *Side Channel*[4] attacks.

As it reported in [14, 15], DoS attacks are possible to be performed on a GPS scheme that use pre-computed coupons. Once all coupons are used, the tag cannot authenticate itself any more. Due to the authentication that is performed one-sided, a tag cannot determine whether an authentication request from a reader is genuine or not. If a tag contained k stored coupons, an attacker could disable the tag by requesting k authentications. Therefore this attack scenario imposes narrow constraints on the possible fields of application for coupon-based systems. A possible solution in order to prevent such attacks would be to give the tag the ability to re-calculate coupons. In practice, re-calculation means that tag hardware would be able to calculate an unlimited number of coupons instead of storing pre-computed coupons and thus such attacks will become infeasible. However, this solution is not always acceptable and depends every time on the production cost and the desired performance level that the RFID implementation should succeed.

Another important threat that must be considered when implementing an GPS identification scheme, is side channel attacks. At it was presented in [16], side channel attacks are also possible to be performed on a GSP identification scheme variant and if the proper countermeasures are not taken, the tag's secret key s can be easily revoked. In [16], it was demonstrated that if a GPS identification scheme uses the Low Hamming Weight technique in a certain way, it can leak the exponent's Hamming weight during the running time of the exponentiation. An effective countermeasure for defending against this kind of attacks is again the usage of re-calculated coupons. If coupons are randomly chosen during identification instead of the sequence in which they are usually computed, then an attacker will not be able to know the matching of retrieved side channel information with the observed commitment. Thus, finding the secret key s will be more difficult for an attacker.

In conclusion, even if *denial of service* and *side channel* attacks pose a serious threat, usually they are neglected during the design phase of a RFID implementation. The several existing GPS identification scheme variants are not always as secure as they seem and the need for better security features is most of the time against the performance of the RFID system. As long as the GPS-based identification schemes are not adopted by industry, the security that they can provide will be always questionable. In order a system to be properly evaluated must function under real circumstances, where the motivation for breaking the system is much higher and the number of the possible attackers is significantly larger. Only then, a system can be claimed to be or not, sufficiently secure.

[3] An attempt to make a resource unavailable to its intended users.

[4] Attacks based on the analysis of hardware characteristics, like timing behaviour or power consumption.

4 Conclusions

In conclusion, the first steps for applying public-key cryptography on RFID systems have already been made, through the usage of light-weight identification protocols. The GPS-based identification schemes are really promising and the elliptic curve variant combined with other additional features, demonstrated an acceptable performance for the low-cost RIFD tags. However, further research is needed with respect to security issues and even more optimized schemes should be designed. Moreover, the additional features must be every time carefully evaluated, since their improper implementation can introduce feasible attacks to a RFID system. The trade-off between security and performance is unavoidable for real life applications and a balance should be found. Until then, the GPS-based schemes will be considered inappropriate for the low-cost RFID tags and their commercial adoption will remain limited, if not absent.

This paper performed a survey on the feasibility of applying public-key cryptography on RFID tags. More precisely, it presented a detailed analysis of the popular basic GPS identification scheme and discussed its variants. It high-lighted the security that these schemes can provide and discussed some of the most promising experiments that have already been conducted on RFID tags, using GPS-based schemes. Finally, it brought on surface some of the feasible attacks that an adversary can perform on specific GPS schemes implementations and discussed possible countermeasures for these attacks.

References

[1] *Marc Girault,* "Self-certified public keys", Advances in Cryptology - Eurocrypt'91, LNCS volume 547, pp. 490-497, Springer Berlin / Heidelberg, (1991).

[2] *Guillaume Poupard and Jacques Stern,* "Security Analysis of a Practical "on the fly" Authentication and Signature Generation", Advances in Cryptology - Eurocrypt'98, LNCS volume 1403, pp. 422-436, Springer Berlin / Heidelberg (1998).

[3] *C.P Schnorr,* "Efficient Identification and Signatures for Smart Cards", Advances in Cryptology - CRYPTO' 89 Proceedings, LNCS volume 435, pp. 239-252, Springer Berlin / Heidelberg (1989).

[4] *ISO/IEC,* "International Standard ISO/IEC 9798-5:2004, Part 5: Mechanisms using zero-knowledge techniques", (2004).

[5] *Marc Girault, Guillaume Poupard and Jacques Stern,* "Some modes of use of the GPS identification scheme", In Proceedings of the 3rd NESSIE Conference,(2002).

[6] *Marc Girault and David Lefranc,* "Public Key Authentication with One (Online) Single Addition", Cryptographic Hardware and Embedded Systems - CHES 2004, LNCS volume 3156, pp. 967-984, Springer Berlin / Heidelberg (2004).

[7] *Marc Girault, Guillaume Poupard and Jacques Stern,* "On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order", Journal of Cryptology, volume 19, pp. 463-487, International Association for Cryptologic Research (2006).

[8] *M. Girault, L. Juniot and M.J.B. Robshaw,* "The Feasibility of On-the-Tag Public Key Cryptography", Workshop on RFID Security, RFIDSec '07 (2007).
Access on: `http://rfidsec07.etsit.uma.es/slides/papers/paper-32.pdf`

[9] *M. McLoone and M. J. B. Robshawn,* "Public Key Cryptography and RFID Tags", Topics in Cryptology CT-RSA 2007, LNCS volume 4377, pp. 372-384, Springer Berlin / Heidelberg (2007).

[10] *M. McLoone and M. J. B. Robshawn,* "New Architectures for Low-Cost Public Key Cryptography on RFID Tags", Circuits and Systems - ISCAS 2007, IEEE International Symposium, pp. 1827-1830, (2007).

[11] *B. Schoenmakers* "Cryptography II - Cryptographic Protocols", Eindhoven University of Technology, Department of Mathematics & Computer Science, v0.997, pp. 36-37, (March 2009).
Access on: `http://www.win.tue.nl/~berry/2WC13/LectureNotes.pdf`

[12] *Henk C.A. van Tilborg* “Fundamentals of Cryptology“, Eindhoven University of Technology, The Netherlands, Kluwer, pag. 111-114 & 213-236, (2000).

[13] *Amos Fiat and Adi Shamir,* ”How To Prove Yourself: Practical Solutions to Identification and Signature Problems”, Advances in Cryptology - CRYPTO’ 86, LNCS volume 263, pp. 186-194, Springer Berlin / Heidelberg (1987).

[14] *Benot Calmels, Sbastien Canard, Marc Girault and Herv Sibert,* ”Low-Cost Cryptography for Privacy in RFID Systems”, Smart Card Research and Advanced Applications, LNCS volume 3928, pp. 237-251, Springer Berlin / Heidelberg (2006).

[15] *Georg Hofferek and Johannes Wolkerstorfer,* ”Coupon Recalculation for the GPS Authentication Scheme”, Smart Card Research and Advanced Applications, LNCS volume 5189, pp. 162-175, Springer Berlin / Heidelberg (2008).

[16] *Julien Cathalo, Francois Koeune and Jean-Jacques Quisquater,* ”A New Type of Timing Attack: Application to GPS”, Cryptographic Hardware and Embedded Systems, LNCS volume 2779, pp. 291-303, Springer Berlin / Heidelberg (2003).