Public-Key Cryptography for RFID-Tags*

L. Batina[1], J. Guajardo[2], T. Kerins[2], N. Mentens[1], P. Tuyls[2], and I. Verbauwhede[1]

[1] Katholieke Universiteit Leuven, ESAT/COSIC, Belgium
{Lejla.Batina,Nele.Mentens,Ingrid.Verbauwhede}@esat.kuleuven.be

[2] Philips Research Laboratories, Eindhoven, The Netherlands
{Jorge.Guajardo,Tim.Kerins,Pim.Tuyls}@philips.com

Abstract

RFID-tags are a new generation of bar-codes with added functionality. An emerging application is the use of RFID-tags for anti-counterfeiting by embedding them into a product. Public-key cryptography (PKC) offers an attractive solution to the counterfeiting problem but whether a public-key cryptosystem can be implemented on an RFID tag or not remains unclear. In this paper, we investigate which PKC-based identification protocols are useful for these anti-counterfeiting applications. We also discuss the feasibility of identification protocols based on Elliptic Curve Cryptography (ECC) and show that it is feasible on RFID tags. Finally, we compare different implementation options and explore the cost that side-channel attack countermeasures would have on such implementations.

1 Introduction

In recent years, the growth of counterfeit goods has experienced a rather steep increase. This increase translates into a large source of losses for manufacturers. For example, it has been estimated that the world market for counterfeit goods was worth between 350 and 385 billion USD in 2001 and it was expected to surpass the 500 billion USD per year mark by 2004 [13]. Notice that the above numbers only point to the economical consequences of counterfeit products. However, in the particular case of the pharmaceutical industry, counterfeit products have a direct (negative) impact on the health and life of thousands of people worldwide. It is clear that new technologies need to be put in place to thwart the counterfeiting threat. RFID has been identified as one of these technologies as shown for example by legislation introduced in the US mandating use of RFID technology as anti-counterfeiting technology for at-risk pharmaceuticals for all medicines in the supply chain by the end of 2010 [17]. However, the use of RFID as an anti-counterfeiting technology is at present rather primitive.

The whole security relies on the premise that an RFID tag is harder to copy than a bar code. However, it has already been demonstrated several times that simple RFID tags can be cloned. For example, Bono et al. [6] have shown how an RFID transponder device manufactured by Texas Instruments and used in many car keys can be successfully cloned with off-the-shelf equipment and minimal RF expertise (see also [30] for another example). Thus, sound technological solutions for the counterfeiting problem need to be developed. By sound, we mean solutions based on cryptography, fundamental physical properties of materials that make them unclonable or a combination of both. Notice that the anti-counterfeiting problem can also be rephrased as an authentication problem. In other words, how can a reader tell that a certain RFID tag is really the one that it intended to talk to? In this setting, RFID-tags contain some secret reference information that is used to check their authenticity. In order to avoid counterfeiting, RFID-tags have to be unclonable. First, this implies that it should be hard to make a physical clone. Secondly, this also means that retrieving the secret reference information by attacking the protocols that are carried out between the reader and a tag (proving its authenticity) should be infeasible. Protection against physical unclonability is provided by using physical countermeasures such as Physical Unclonable Functions [28] and protection against active or passive attacks on the protocols is provided by cryptographic techniques such as digital signatures and secure identification protocols. In short, RFID-based identification is an example of an emerging technology which requires authentication as a cryptographic service. This property can be achieved by symmetric as well as asymmetric primitives.

[*] A preliminary version of this paper appears in the Workshop for RFID Security 2006 which had no formal proceedings.

Previous work considered only symmetric-key algorithms e.g. AES [8]. It is still not clear whether Public-Key (PK) algorithms can be implemented in constrained devices, such as RFID tags, and still comply with the area, performance, and power requirements typical of these applications. Recently, a few papers [28, 31] discussed feasibility of ECC based PKC on RFID-tags. Here, we extend that line of work and discuss implementations aspects of even stronger PK-based protocols in more detail. In particular, the protocols investigated in [28] were only secure against passive attacks. Thus, in this paper, we investigate the efficiency of protocols (Okamoto-identification protocol) that are also secure against active and concurrent attacks. It is shown that only a small price for much additional security has to be paid. In addition, we present ECC-based implementation of the above mentioned protocols and compared different implementations methods available.

The remainder of the paper is organized as follows. Section 2 provides an overview of related work. In Sect. 3 we state our assumptions and review the protocol of [28] describing only the PUF-based protocol for the off-line authentication case. The Okamoto identification protocol and its hardware implementation for off-line verification are described in Sect. 4. Finally, our results are presented in Sect. 5.

2 Related Work

Protocols for cheap authentication have been presented [16, 15]. However, they focus on the on-line situation in which the reader shares a secret with the tag being authenticated. In addition, they do not take physical cloning into account. In [28], RFID-tags that withstand general cloning attacks (including physical ones) are introduced. Based on an Integrated PUF (I-PUF) [9, 29] a PUF-Certificate-Identity Based identification scheme was introduced. This scheme allows for off-line authentication. In [28] the implementation of the Schnorr Identification scheme was investigated for this purpose. This protocol is only secure against passive attacks but it is very efficient. There have not been many attempts at hardware implementations of PKC on RFID tags or other low-power application platforms *e.g.* sensor nodes. Gaubatz et al. [11] showed that RSA is not a feasible solution while NtruEncrypt can be implemented in about 3000 gates. More recent work of Wolkerstorfer [31] is the first to claim possible to have low-power and compact implementation of ECC that meets the constraints imposed by the EPC standard. However, our solution is smaller as the off-line authentication in our case does not require full ECDSA signature generation to be executed on the RFID tag. This allowed for further area optimizations.

3 Off-line Authentication

We distinguish between on-line and off-line authentication. Off-line authentication is the most attractive one from a practical point of view but also the most challenging one, as costs grow much more in this case. The particular case of on-line authentication was considered in [28] and it does not make use of PK cryptography, thus we do not discuss it any further.

3.1 Assumptions

We consider RFID-tags embedded in a product or its package for detection and prevention of product counterfeiting. The tag is manufactured and embedded into the product by a legitimate authority which is assumed to be trusted. We consider an active attacker that knows the position of the tag in the product or its package, so she can remove the tag from the package to investigate it. We also assume that the attacker can (passively) eavesdrop on the channel between a reader and the tag, or can install a fake reader that communicates with the tag (active attack). Finally, we assume that the attacker can physically attack the tag; *i.e.* she can try to read out its memory. The goal of the attacker is to produce a fake RFID-tag containing reference information such that it can only be distinguished from a real tag with small probability . Clearly, by embedding such a fake tag into a fake product, the fake product is identified as an authentic one.

3.2 Authentication Protocol

In [28] a PUF-Certificate-Identity based Identification scheme was proposed. For the sake of completeness we describe it briefly here but refer to [28] for the details. Given the following algorithms and definitions:

- a tag with identity I and a PUF,
- a standard identification scheme $\mathcal{SI} = (K_g, P, V)$, where K_g denotes the key generation algorithm, and P, V denote the interactive protocols run by the prover and verifier respectively, and
- a secure signature scheme $\mathcal{SS} = (\mathrm{SK}_g, \mathrm{Sign}, V_f)$, with SK_g denoting the key generation algorithm, Sign denoting the signing algorithm and V_f the verification algorithm run by a verifier

a PUF-Certificate-Identity based Identification scheme $(\mathrm{MK}_g, \mathrm{UK}_g, \hat{P}, \hat{V})$ can be constructed as follows.

During **enrollment** the issuer uses SK_g as the master-key generation algorithm MK_g for the secure signature scheme. The result is the issuer's master-key pair (mpk, msk). The algorithm UK_g creates for each tag a public-secret key pair

(pk, sk) using the algorithm K_g for the SI-scheme. The issuer runs a protocol with the tag to determine the PUF's challenge c and helper data w such that the PUF response $x(c)$ maps onto the secret key sk. The helper data w are written into the ROM (EEPROM) memory of the tag. Finally, the issuer, using his master secret-key msk to sign, creates the following certificate that is also stored in the ROM of the tag Cert $\leftarrow (pk, \text{Sign}(msk, pk||ID))$.

During **authentication** the algorithms $\hat{P}$ and $\hat{V}$ are run as follows. The tag (in the role of the prover) sends the certificate Cert to the reader. If Cert is valid, the tag and the reader run the SI-protocol. If the tag passes this protocol too, the reader decides that the tag is authentic and otherwise not. Note that in order to run this last step, the tag has to challenge its PUF and use the helper data to obtain the secret key sk from the measured response $y(c)$.

The security of the scheme depends on three factors: (i) the security of the PUF as a secure storage of the secret key, (ii) the security of the identification scheme used, and (iii) the security of the signature scheme used. It was shown in [28] that if the PUF is unclonable and a good Fuzzy Extractor is used for key extraction, the PUF provides a secure way of storing secret keys. The security of the scheme against impersonation attacks depends on the security of the identification scheme used against those attacks. Therefore, it is of crucial importance to understand which trade-off is being made between efficiency and security.

4 Okamoto's ID Protocol Based on ECDLP

In [28], Schnorr's identification protocol [26] is used as the SI in the Cert-IBI. Furthermore, it is shown that the elliptic curve version of Schnorr's identification protocol can be efficiently implemented. Schnorr's protocol is, however, only resistant against passive attacks under the discrete logarithm assumption. Another protocol that is also resistant against active and concurrent attack under the discrete logarithm assumption is Okamoto's identification protocol [25]. We investigate therefore the efficiency of the implementation of this protocol here in detail. Notice that we are considering Okamoto's identification protocol as it provides security against active adversaries and it is based on the hardness of the DL problem. Other protocols found in the literature include Beth's identification protocol [5] and the XDL-IBI scheme in [3]. Beth's protocol only requires one point multiplication but it remains an open problem to prove its security against active adversaries. The XDL-IBI scheme also requires only one point multiplication but is only secure against passive adversaries and concurrent attacks (under a modified assumption). Thus, it seems that by analyzing both Schnorr's and Okamoto's we cover the efficiency of all *available* ID protocols based on the hardness of the DL problem. Protocols based on the hardness of integer factorization also exist (see [3, 23] for a thorough classification of ID-based protocols) but their performance and scalability properties are worse, in general, than those based on ECDLP as the comparisons in [10] show.

1. **Common Input:** The set of system parameters in this case consists of: (q, *FR*, a, b, P_1, P_2, n, h). Here, q specifies the finite field, *FR* is a field representation, a, b, define an elliptic curve, P_i is a point on the curve of order n and h is the cofactor. In the case of tag authentication, these parameters are assumed to be fixed.

2. **Prover-Tag Input:** The prover's secret (s_1, s_2) such that $Z = -s_1 P_1 - s_2 P_2$.

3. **Protocol:** The protocol involves the exchange of the following messages:

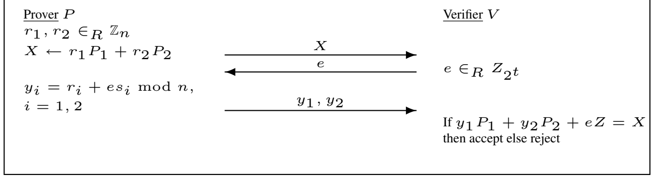
Prover P
$r_1, r_2 \in_R \mathbb{Z}_n$
$X \leftarrow r_1 P_1 + r_2 P_2$
$y_i = r_i + es_i \bmod n,$
$i = 1, 2$
X
e
y_1, y_2
Verifier V
$e \in_R Z_{2t}$
If $y_1 P_1 + y_2 P_2 + eZ = X$
then accept else reject

Figure 1. Okamoto's identification protocol.

4.1 Elliptic Curve Cryptography

The main operation in any ECC-based primitive is the scalar multiplication. The point scalar multiplication is achieved by repeated point addition and doubling. We can use the basic double-and-add algorithm in both cases. In the case of Schnorr's identification protocol, we can also use the Montgomery ladder method [22] and benefit from the Lopez-Dahab projective coordinates [19].

4.1.1 Point Addition and Doubling

The point addition/doubling depend on the type of projective coordinate used. Table 1 summarizes the number of operations required for known projective coordinates in terms of multiplications, squarings, and additions. The number of operations is assuming general values for Z. However, this value varies based on the values of the curve coefficients a, b are considered[1].

Table 1. Operation Counts for EC point addition and doubling

Coordinate System	Addition			Doubling		
	Mult.	Sqr.	Add.	Mult.	Sqr.	Add.
Jacobian projective $(X/Z^2, Y/Z^3)$ [7] $a \neq 0$	15	5	7	5	5	4
Jacobian projective $(X/Z^2, Y/Z^3)$ [7] $a = 0$	14	4	7	5	5	4
Lopez-Dahab $(X/Z, Y/Z)$ [19] $b \neq 1$	4	1	2	2	4	1
Lopez-Dahab $(X/Z, Y/Z)$ [19] $b = 1$	4	1	2	1	4	1
Modified Lopez-Dahab $(X/Z, Y/Z)$ [28] $b \neq 1$	6	1	2	3	5	1

4.1.2 Field Operations

Fields of characteristic two in polynomial basis were chosen as field arithmetic can be implemented efficiently and rela-

[1] The EC is defined as $y^2 + xy = x^3 + ax^2 + b$, with $a, b \in \mathbb{F}_{2^n}$.

tively cheaply in hardware. Notice that our emphasis is on minimizing area rather than performance. Addition of two elements $C = A + B \in \mathbb{F}_{2^n}$ is performed via an n–bitwise logical XOR operation. The simplest multiplier is based on Horner's scheme for multiplication. In particular, to compute the product $C = A \cdot B \in \mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/f(x)$, and $A = \sum_{i=0}^{n-1} a_i x^i$, $B = \sum_{j=0}^{n-1} b_j x^j$, $f = x^n + \sum_{i=0}^{s} f_i x^i$, $s < n$, we process one bit of B at the time as follows

$$C = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i b_j x^{i+j} \bmod f = A \sum_{j=0}^{n-1} b_j x^j \bmod f$$

The multiplication process then requires n iterations. Digit serial multiplication [27] is a generalization of this in which several coefficients of B are processed in parallel. Thus, we trade off area for performance. Algorithm 1 describes how to perform Most Significant Digit multiplication according to [12] which reduces the area of the multiplier with respect to [27] and [2] by not requiring either an additional reduction circuit as in [27] or additional $n + 2D - 1$ MUXes as in [2]. The cost is a longer critical path, which at the frequencies of operation that we are considering does not affect the overall performance. Squaring $c = a^2 \in \mathbb{F}_{2^n}$ is a special case of multiplication. It is well known that $a^2 = \sum_{i=0}^{n-1} a_i x^{2i}$ which can then be reduced modulo f to a field element in $\mathbb{F}_{2^n}$.

Algorithm 1 Most Significant Digit Multiplication in $\mathbb{F}_{2^n}$

```
Require: $A = \sum_{i=0}^{n-1} a_i x^i$, where $a_i \in \mathbb{F}_2$, $B = \sum_{j=0}^{-1} \widehat{b}_j x^{jD}$ where $\widehat{b}_j = \sum_{l=0}^{D-1} b_{Dj+l} x^l$, $b_i \in \mathbb{F}_2$, and $d = \lceil \frac{n}{D} \rceil$.
Ensure: $C = A \cdot B \bmod f(x)$
$C \leftarrow 0$
for $i = 0$ to $d - 1$ do
    $C \leftarrow \left(\widehat{b}_{d-1-i} A + C x^D\right) \bmod f$
end for
Return $C$
```

4.2 ECC processor

Our Elliptic Curve Processor (ECP) for RFID has the following operational blocks: a Control Unit(CU), an Arithmetic Unit (ALU), and Memory (RAM and ROM). The ECC parameters and the constants are stored in ROM. On the other hand, RAM contains all input/output and intermediate variables and it therefore communicates with both, the ROM and the ALU. The CU controls scalar multiplication and point operations. In addition, the controller commands the ALU which performs field multiplication, addition and squaring. The bits of the scalar multiplier $k = \sum_{i=0}^{n-1} k_i 2^i$, $k_i = \{0, 1\}$, $n = \lceil \log_2 k \rceil$, are evaluated from MSB to LSB. The CU consists of a number of simple state machines and a counter and its area cost is small.

5 Results and Discussion

In this section, we provide results for the latency and the area complexities of both Schnorr's and Okamoto's protocols. As we are interested in implementations of identification protocols (e.g. Schnorr, Okamoto) the operation required is one point multiplication in the case of Schnorr's protocol or multiple-point multiplication in the case of Okamoto's scheme.

5.1 Implementation of Okamoto's Scheme

In [28], the *feasibility* of the ECC version of Schnorr's identification protocol in an RFID system was investigated and area and latency estimates were provided. Here, we provide detailed numbers and we also investigate the feasibility of the Okamoto's scheme as it provides security against active adversaries which Schnorr's scheme does not. Table 2 summarizes the number of operations that the different addition formulae imply. Here we assume that for the Jacobian coordinates on average we perform n doublings and $n/2$ addition operations and that for the Lopez-Dahab coordinates we use the Montgomery ladder with n iterations[2]. Notice that the modified formulae presented in [28] provide simple side-channel attack resistance if implemented without the use of a dedicated squarer. In this case, the formula of [28] are almost 3 times as slow as the standard formulae from [19] which does *not* provide side-channel resistance.

Table 2. Cycle count for EC operations over $\mathbb{F}_{2^p}$. L: Load, C: Computation, S: Store, $d = \lceil \frac{p}{D} \rceil$, $n = \lceil \log_2 k \rceil$

Operation	L	C	S	Total Cycles
$\mathbb{F}_{2^p}$ addition	2	1	1	4
$\mathbb{F}_{2^p}$ squaring	1	1	1	3
$\mathbb{F}_{2^p}$ multiplication	2	d	1	$d + 3$
EC operations assuming a squarer				
Projective coordinate type		Addition	Doubling	Total $k \cdot P$
Jacobian projective $(X/Z^2, Y/Z^3)$ [7] $a \neq 0$		$15d + 88$	$5d + 46$	$12.5nd + 90n$
Jacobian projective $(X/Z^2, Y/Z^3)$ [7] $a = 0$		$14d + 82$	$5d + 46$	$12nd + 87n$
Lopez-Dahab $(X/Z, Y/Z)$ [19] $b \neq 1$		$4d + 23$	$2d + 22$	$6nd + 45n$
Lopez-Dahab $(X/Z, Y/Z)$ [19] $b = 1$		$4d + 23$	$d + 19$	$5nd + 42.5n$
Modified Lopez-Dahab $(X/Z, Y/Z)$ [28] $b \neq 1$		$6d + 29$	$3d + 28$	$9nd + 57n$
EC operations assuming no squarer				
Modified Lopez-Dahab $(X/Z, Y/Z)$ [28] $b \neq 1$		$7d + 29$	$8d + 28$	$15nd + 57n$

In Okamoto's scheme, the required computation on the tag is of the form $kP + lQ$. For the purpose of speeding-up this computation one uses Shamir's trick. The algorithm performs this so-called simultaneous point multiplication

[2] The actual number of doublings is $n - 1$ for the binary method, but we chose n in the interest of space.

computing at each of $\lceil \frac{n}{w} \rceil$ steps w doublings and 1 addition from a list of 2^w pre-calculated values of the form $iP + jQ$. As the width of the window w is variable, this allows to trade-off area for speed. We chose the smallest window *i.e.* $w = 1$. In this way, the memory requirements are minimized as only 3 points have to be stored: $P, Q, P + Q$. The expected running time of the algorithm for $w = 1$ is $\frac{3}{4}n$ point additions and $(n - 1)$ point doublings.

We have implemented the Schnorr scheme in VHDL and obtained area and timing values for a 0.25μm CMOS library. We have used these values to estimate the performance of Okamoto's identification protocol using Shamir's Trick and Jacobian coordinates. Table 3 summarizes the results. We notice that the amount of logic required to support Okamoto's protocol is not significantly larger than that corresponding to the implementation of Schnorr's. However, the required RAM to implement Okamoto's identification protocol is more than twice the required RAM required for Schnorr's. In practice this means an increase in area anywhere from 20% to 50% depending on the chosen RAM implementation (i.e. whether a RAM cell is implemented as a register requiring at least 6 equivalent gates worth of area or as dedicated embedded RAM requiring somewhere between 1.5 and 2 equivalent gates [14]). In terms of latency, Okamoto's identification protocol is almost twice as slow as Schnorr's over elliptic curves due to the fact that the coordinate representation introduced in [19] is only applicable to the Montgomery Ladder method of exponentiation. In addition, simultaneous double exponentiation is naturally about 25% slower than the regular binary method for exponentiation. With respect to the most compact solution, as required due to low gate-count and low-power requirements, implementing curve-based protocols with shorter bit-lengths appears to be an attractive option. For example, in the case of ECC one could use 130-bit long parameters. This solution would still maintain a suitable level of security [18], especially for low-cost RFIDs, and the gate complexity would scale-down accordingly resulting in more attractive solutions from the area and performance points of view. We conclude by noticing that the performance of the simultaneous point multiplication (as well as the binary method) can be easily improved by using Non-Adjacent Form representation for the multiplier. Such methods in the binary case would for example reduce the number of multiplications from a half on average to a third, providing significant performance improvements (see for example [21]).

Table 3. Implementation results @ 175 kHz and assuming a dedicated squarer circuit.

Implementation		ALU	RAM Mont.	RAM	Perf. Mont.	Perf.	Area wo RAM
Digit	Field	[gates]	Ladder	Okamoto	Ladder	Okamoto	[gates]
Size	Size		[bits]	[bits]	[s]	[s]	
D=1	$\mathbb{F}_{2^{131}}$	6306	917	2096	0.91	1.59	8582
	$\mathbb{F}_{2^{139}}$	6690	973	2224	1.02	1.79	9044
	$\mathbb{F}_{2^{163}}$	7846	1141	2608	1.38	2.44	10122
D=2	$\mathbb{F}_{2^{131}}$	6962	917	2096	0.48	0.83	8603
	$\mathbb{F}_{2^{139}}$	7379	973	2224	0.53	0.93	9734
	$\mathbb{F}_{2^{163}}$	8663	1141	2608	0.71	1.27	10933

5.2 A Word Regarding Power

At the present moment, we do not have an actual chip and we lack explicit power measurements for our simulations. Nevertheless, we believe that attaining the power values required for RFID applications using our design is possible. In fact, our processor architecture is very similar to the architecture presented in [31]. One particular characteristic of both designs is the usage of an Arithmetic Logic Unit (ALU) with a full-precision data path. The differences are on the details of our implementation: field size, choice of finite field arithmetic methodology (Montgomery vs. dedicated trinomial or pentanomial circuits), support for multiple fields versus support for a single field, hashing versus no hashing required in our implementation, etc. In general, our design is aimed at making our implementation as specific as possible to our particular application. This methodology leads to significant complexity reduction in the area requirements and thus also to power savings. Thus, since [31] was able to attain the power requirements of an RFID system, we are confident that our design, being smaller and simpler, will also attain the required power figures at the same or lower operating frequencies.

5.3 Generation of Randomness

Finally notice that a source of randomness is needed on the tag. In our case, this can be done by applying a random challenge to the PUF e.g. in a range out of its specification. The random challenge can be generated by the reader. For a construction of a random number generator based on a PUF, we refer to [24].

5.4 On Performance and Other Implementations

Recently, McLoone and Robshaw [20] explore the hardware cost of the GPS scheme modified for ultra-low cost devices, such as RFID tags. The authors achieve costs equivalent to those of symmetric-key encryption as described in the work of Feldhofer et al. [8], in other words in the order of 1700 equivalent gates for their largest implementation and requiring not more than 900 cycles, which at 100 KHz translates into 9 msec and under 3.4 μA of current. However, it is not possible to compare fairly the work of this paper with that of [20]. First, the implementation of [20] is based on the idea of coupons. In other words, the RFID tag stores a number of challenge-response pairs that have been precomputed and only performs the last part of the 3-pass authentication protocol which in general is much cheaper to implement and requires an addition and a single modular multiplication. This implies that the RFID tag can only authenticate itself a limited number of times. On the other hand, our solution can participate in an *unlimited* number of authentications. Second, the hardware requirements of [20] do not include the storage cost of the coupons in their estimates, whereas our implementation does include this cost[3]. Obviously, which solution is best will depend in the end on the requirements of the application. If the application only requires that the RFID tag be operational for just a few authentications, then the solution described in [20] will be adequate, otherwise our flexible elliptic curve solution would be the one of choice.

6 Concluding Remarks

In this paper we discussed the feasibility of public key based secure identification protocols for RFID-tags. As an example we investigated the implementation of Okamoto's identification protocol in detail. It was shown that it is just slightly more expensive than Schnorr's identification protocol. Finally, we notice that the performance of Okamoto's protocol can be further improved using the techniques presented in [1] and recently improved in [4]. Such improvements will be considered in future work.

Acknowledgments

We would like to thank the anonymous referees for their helpful comments. This work is also partially funded by FWO G.0450.04 and K.U.Leuven (OT).

References

[1] T. Akishita. Fast Simultaneous Scalar Multiplication on Elliptic Curve with Montgomery Form. In S. Vaudenay and A. M. Youssef, editors, *Selected Areas in Cryptography — SAC 2001*, volume 2259 of *LNCS*, pages 255–267. Springer, 2001.

[2] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public key cryptography for RFID-tags. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[3] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology — Eurocrypt 2004*, volume 3027 of *LNCS*, pages 268–286. Springer-Verlag, 2004.

[4] D. J. Bernstein. Differential addition chains. Technical Report Document ID: 9620b81ea01f66b2a782be234dade959, February 19th, 2006. Available at `http://cr.yp.to/papers.html`.

[5] T. Beth. Efficient Zero-Knowledge Identification Scheme for Smart Cards. In C. G. Günther, editor, *Advances in Cryptology — EUROCRYPT'88*, pages 77–84, 1988.

[6] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In P. McDaniel, editor, *USENIX Security Symposium — Security '05*, pages 1–16. Usenix, 2005.

[7] D.V. Chudnovsky and G.V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986.

[8] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems — CHES 2004*, volume LNCS 3156, pages 357–370. Springer, 2004.

[9] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas. Silicon physical random functions. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security — CCS 2002*, pages 148–160. ACM, November 18-22, 2002.

[10] G. Gaubatz, J.-P. Kaps, E. Öztürk, and B. Sunar. State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks. In *IEEE International Workshop on Pervasive Computing and Communication Security — PerSec 2005*, Kauai Island, Hawaii, March 2005.

[11] G. Gaubatz, J.-P. Kaps, and B. Sunar. Public Key Cryptography in Sensor Networks - Revisited. In *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, Heidelberg, Germany, August 2004.

[12] J. Guajardo, T. Kerins, and P. Tuyls. Finite Field Multipliers for Area Constrained Environments. Pre-print, 2006. .

[13] ICC Policy Statement: The fight against piracy and counterfeiting of intellectual property. Submitted to the 35th World Congress, Marrakech, Document no 450/986, ICC, June 1st, 2004.

[14] K. Itoh. Low-Voltage Embedded RAMs in the Nanometer Era. In *IEEE International Conference on Integrated Circuits and Technology — ICICT 2005*, pages 235–242. IEEE Computer Society, 2005.

[15] A. Juels. Strengthening EPC Tags Against Cloning. In M. Jakobsson and R. Poovendran, editors, *ACM Workshop on Wireless Security — WiSe 2005* , pages 67–76. ACM Press, 2005.

[16] A. Juels and S. A. Weis. Authenticating pervasive devices with human protocols. In V. Shoup, editor, *Advances in Cryptology: Proceedings of CRYPTO 2005*, volume 3621 of *LNCS*, pages 293–308. Springer-Verlag, 2005.

[17] R. Koh, E. W. Schuster, I. Chackrabarti, and A. Bellman. Securing the Pharmaceutical Supply Chain. White Paper MIT-AUTOID-WH-021, Auto-Id Center MIT, Cambridge, Ma 02139-4307, USA, September 1st, 2003. Available at `http://www.mitdatacenter.org/MIT-AUTOID-WH021.pdf`.

[18] A. Lenstra and E. Verheul. Selecting cryptographic key sizes. In H. Imai and Y. Zheng, editors, *Workshop on Practice and Theory in Public Key Cryptography — PKC 2000*, volume 1751 of *LNCS*, pages 446–465. Springer-Verlag, 2000.

[19] J. López and R. Dahab. Fast multiplication on elliptic curves over GF(2^m). In Ç. K. Koç and C. Paar, editors, *Proceedings of 1st International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 1717 of *LNCS*, pages 316–327. Springer-Verlag, 1999.

[20] M. McLoone and M.J.B. Robshaw. Public Key Cryptography and RFID Tags. In *Topics in Cryptology — CT-RSA 2007*, 2007. To appear.

[21] B. Möller. Algorithms for Multi-exponentiation. In S. Vaudenay and A. M. Youssef, editors, *Selected Areas in Cryptography — SAC 2001*, volume 2259 of *LNCS*, pages 165–180. Springer, 2001.

[22] P. Montgomery. Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of Computation*, Vol. 48:243–264, 1987.

[23] G. Neven. *Provably Secure Identity-Based Identification Schemes and Transitive Signatures*. PhD thesis, Faculteit Toegepaste Wetenschappen — Departement Computerwetenschappen, Afdeling Informatica. Katholieke Universiteit Leuven, Leuven, Belgium, 2004.

[24] C.W. O'Donnel, G.E. Suh, and S. Devadas. PUF-Based Random Number Generation. Technical Report 481, MIT CSAIL, November 2004. Available at `http://www.csg.csail.mit.edu/pubs/publications.html`.

[25] T. Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO'92*, volume 740 of *LNCS*, pages 31–53. Springer, 1992.

[26] C.-P. Schnorr. Efficient Identification and Signatures for Smart Cards. In Gilles Brassard, editor, *Advances in Cryptology — CRYPTO '89*, volume LNCS 435, pages 239–252. Springer, 1989.

[27] L. Song and K.K. Parhi. Low Energy Digit-Serial/Parallell Finite Field Multipliers. *Kluwer Journal of VLSI Signal Processing Systems*, 19(2):149–166, 1998.

[28] P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, *Topics in Cryptology - CT-RSA 2006*, volume 3860 of *LNCS*, pages 115–131. Springer Verlag, February 13-17 2006.

[29] P. Tuyls and B. Skoric. Secret Key Generation from Classical Physics: Physical Uncloneable Functions. In S. Mukherjee, E. Aarts, R. Roovers, F. Widdershoven, and M. Ouwerkerk, editors, *AmIware: Hardware Technology Drivers of Ambient Intelligence*, volume 5 of *Philips Research Book Series*. Springer-Verlag, September 2006.

[30] J. Westhues. Demo: Cloning a Verichip. `http://cq.cx/verichip.pl`, Last updated: July 2006.

[31] J. Wolkerstorfer. Scaling ECC Hardware to a Minimum. In ECRYPT workshop - Cryptographic Advances in Secure Hardware - CRASH 2005, September 6-7 2005. Invited talk.

[3] The storage costs in [20] will not be as high as in our implementation as they only require read-only memory which is cheaper than RAM.