Practical Escrow-free Identity-based Mutual Authentication and Key Management without Pairings

Project PN-II-PT-PCCA-2013-4-1651

Phase II: Solutions Development and Implementation

December 2, 2015

Contents

Part I
Summary of Phase II

The second phase of the project, *Solutions Development and Implementation*, is dedicated to the development of new solutions for IBE and ABE schemes, based on quadratic residuosity problem. Our results improves the existing ones and comes with totally new schemes whose efficiency is proven by direct comparisons with the existing schemes.

The studies and research in this phase of the project are included into the following research papers:

1. G.D. Năstase F.L. Ţiplea: *On a Lightweight Authentication Protocol for RFID Systems*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

2. F.L. Tiplea, E. Simion: *New Results on Identity-based Encryption from Quadratic Residuosity*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

3. N. Roşia, V. Cervicescu, M. Togan: *Efficient Montgomery Multiplication on GPUs*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

4. F.L. Ţiplea: *Sharing Secrets on Boolean Circuits: Application to Key-policy Attribute-based Encryption*, invited talk, Romanian Cryptology Days, Sept 21-23, 2015, Bucharest (Romania).

The first paper proposes a lightweight authentication protocol for RFID system, based on an operation which is the bases for Real Privacy Management (RPM) technology. The second paper reports new results obtained on IBE schemes based on quadratic residuosity. The third paper reports efficient implementations for Montgomery multiplication on GPUs. Our fourth paper shows how secret sharing can be used in conjunction with bilinear and multilinear maps to design ABE schemes.

We consider that the four research papers mentioned above cover very well the objectives of the Phase II of the project (see “Expected Results” in the project’s

realization plan), highlighting the most important aspects needed for the third phase. Moreover, we explicitly mention that our results are mostly published in the Lecture Notes in Computer Science Series (by Springer-Verlag).

Part II
Scientifical and Technical Description

Mutual Authentication and Key Management are crucial components of all the security techniques incorporated in the nowadays communication technologies, such as IPsec, SSL&TLS, Voice over IP (VoIP), and Self-organizing Networks (SONs). The existing techniques are mainly based on public key infrastructures (PKI) which have many practical shortcomings highlighted by many researchers and practitioners, that make them impractical for large systems or highly dynamic systems or systems with limited computational power (such as mobile ad-hoc or sensor networks). This is because:

1. Each node in a network (system) is assumed to have a public key signed by a Certifying Authority (CA). This requirement is considerable costly for the node;

2. Almost each PKI based protocol assumes that each node k nows the certificate of the destination before it sends the m essage. Caching certificates rises problems with trust and storage, and this adds large overhead on local storage in large systems or systems with limited computational power;

3. In highly dynamic systems, with nodes constantly joining and leaving the network, certificates can quickly become invalidated and therefore the management process become complex.

All these show that the PKI solution to key management is not very adequate, and better solutions are needed to:

1. Simplify public key distribution and management;

2. Simplify access control;

3. Secure messages and strength the (mutual) authentication in a more lightweight and clean way compared to certificate-based approaches.

The next sections will discuss in more details the contributions brought by the project to the authentication and key management mechanisms in these technologies.

1 Authentication

This section is based on

> G.D. Năstase F.L. Ţiplea: *On a Lightweight Authentication Protocol for RFID Systems*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

An RFID system is typically composed of three elements: an RFID reader (transceiver), a number of RFID tags (transponders), and a back-end database (or server). The reader and the back-end database may be viewed as a single entity as they communicate through a secure channel. However, the communication between reader and tag is insecure and, therefore, it is subject to eavesdropping. As a conclusion, the (mutual) authentication between reader and tag becomes one of the most important problems in this context.

Many authentication protocols for RFID systems have been proposed. They are usually classified according to the computational power of the tag. If the tag has strong computational capabilities, then it can implement protocols based on strong cryptographic primitives [15, 2, 3, 26, 31]. Of course, such tags can be too costly to be adopted in most retailer operations which are envisioned as major applications of the RFID technology. A large number of authentication protocols proposed so far are based on hash functions, hash function chains, pseudo-random functions, and random number generators [46, 19, 28, 1, 27, 41, 31]. A third class of authentication protocols is the class of lightweight and ultra-lightweight authentication protocols. They only require to perform primitive operations such as random number generation, arithmetic bit-wise operations, cyclic redundancy code checksum, or even light hash or pseudo-random functions [44, 23, 24, 33, 32, 9, 36, 8, 34, 31, 35, 10]. There is a widespread view that the lightweight and ultra-lightweight authentication protocols will be the best candidate technology for securing the future low-cost RFID systems.

In [12], a lightweight authentication protocol has been proposed. The main idea is to use non-linear feedback shift register (NLFSR) sequences generated by the position digit algebra function (PDAF) [42, 43, 37, 38]. Unfortunately, some of the main properties of the PDAF, as described in [43] are flawed and, as a consequence, the NLFSR sequences used in [12] might have short periods. We discuss this weaknesses in this paper and we propose better NLFSR sequences. Based on these NLFSR sequences we improve the protocol in [12] and, moreover, we provide formal arguments for its security and privacy.

The protocol includes three parties: a reader R, a tag T, and a back-end server S equipped with a database which maintains information about tags. We assume that the channel between the reader and the back-end server is secure, while the one between the reader and the tag is insecure.

The initialization phase, which is to be described below, sets the basic elements needed for the protocol to be run.

Protocol initialization

1. An integer $r \geq 2$ and a hash function h are chosen and made public;
2. A private key K_R of some symmetric cryptosystem (such as AES) is chosen uniformly at random and securely distributed to the reader R;
3. For each tag T, the following steps are performed:
   (a) sets $n = r$;
   (b) seven values $K_{ST}, c_0, c_1, c_2, c_3, c_4, LT \in \mathbb{Z}_r^n$ are chosen independent and uniformly at random;
   (c) the value $P(T) = h(\{ID(T)\}_{K_R} \parallel K_{ST})$ is computed ("$\parallel$" denotes concatenation);
   (d) $P(T), K_{ST}, c_0, c_1, c_2, c_3, c_4, LT$ are stored in the tag T;
   (e) $P(T), \{ID(T)\}_{K_R}, K_{ST}, c_0, c_1, c_3, c_4, LT, c_{4,prev}$ are stored in the server's data base, where $c_{4,prev} = c_4$.

A pictorial view on the distribution of these parameters is provided in Figure 1, and a short description of them is in order. The server cannot see the identities of the tags it manages because the they are encrypted by the key K_R known only to the reader. The random numbers c_0, c_1, c_2, c_3, c_4 act as seeds for four sequences α, β, γ, and γ^*, as in the previous section. The parameter LT (*last transaction*)

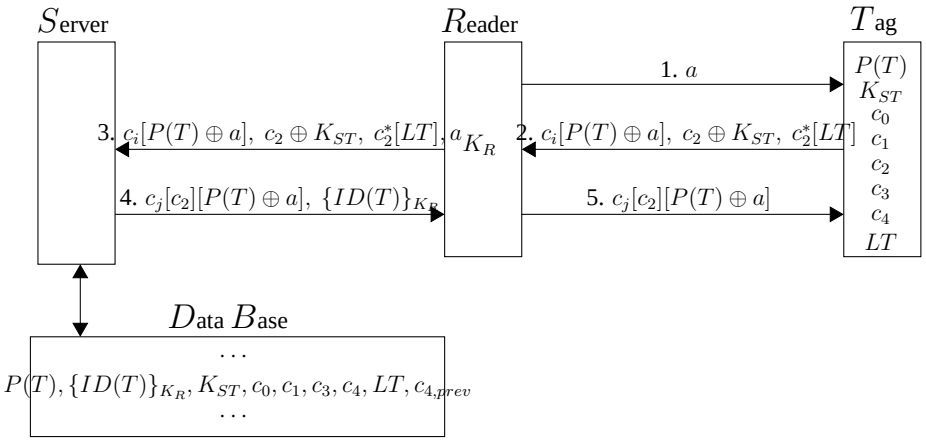

Figure 1: The protocol

is used to count the numbers of queries executed on the tag by readers, and to synchronize the database and the tag. The parameter $c_{4.prev}$ stores the previous value of c_4 and it is used by the server when the tag was not able to authenticate it at the previous query. More precisely, the search in the database uses first c_4. If the search fails for all database records, then it starts again with $c_{4,prev}$. If it succeeds now, the server learns that during the previous query the tag was not able to authenticate it.

Correctness Following [20], a RFID authentication protocol is correct if, executing it honestly, the identification of a legitimate tag only fails with negligible probability.

A simple inspection of the protocol, in the view of Remark **??**, shows that false negatives are not possible (in the absence of an adversary).

Security is the property that an illegitimate tag is not authenticated by the server, except for a negligible probability.

Assume that a tag T (legitimate or illegitimate) answers to some query a by

$$c_i[P(T) \oplus a'],\ c_2 \oplus K_{ST},\ c_2^*[LT]$$

and the reader sends

$$c_i[P(T) \oplus a'],\ c_2 \oplus K_{ST},\ c_2^*[LT],\ a$$

to the server.

According to the protocol description, the server looks in its database and, for each tag T' checks the equality

$$c'_b[P(T') \oplus a] = c_i[P(T) \oplus a']$$

for some bit b (see the step 4(c) in the protocol description). If this equality holds, the server identifies the tag T as being the tag T' (although T' might not be T, but the server does not know this).

As $c_i[P(T) \oplus a']$ and $P(T') \oplus a$ are fixed given values for the server, the problem is to estimate the probability of c'_b to fulfill the equality above. More generally, given two random numbers $y, v \in \mathbb{Z}_r^n$, we are interested in estimating the probability of finding x such that $x[y] = v$. Or, in other words, we are interested to estimate the maximum number of solutions in x to the equation $x[y] = v$. This equation is equivalent to the system

$$\begin{cases} x_1 \oplus_r x_{1 \oplus_r y_1} & = & v_1 \\ \cdots & & \\ x_n \oplus_r x_{n \oplus_r y_n} & = & v_n \end{cases} \tag{1}$$

The first remark is that if $i \oplus_r y_i = j$ and $j \oplus_r y_j = i$, for distinct indexes i and j, then:

1. if $v_i \not\equiv v_j \bmod r$, then the system (1) does not have solutions;
2. if $v_i \equiv v_j \bmod r$, then any solution to x_i leads to at most one solution to x_j (and vice versa).

(if i and j are as above, we will say that the ith and jth equations are *paired*).

Our second remark is that a variable x_i for one of the system's equations is substituted into another equation, the resulting equation still has at most two variables.

These two remarks leads to the conclusion that the worst case regarding the number of solutions to the system (1) is that when the variables are paired two by two as above. In such a case the maximum number of solutions to the system is upper bounded by $r^{n/2}$ (the variables are paired two by two and for each pair, a solution to one of the pair components leads to at most a solution to the other pair component).

Therefore, the probability of getting a solution to the equation $x[y] = v$ is at most

$$\frac{r^{n/2}}{r^n} = \frac{1}{r^{n/2}}$$

For large n, this is negligible.

Privacy The protocol we have proposed is lightweight and, therefore, it is improper to use a privacy model as the one in [30, 20] which is suitable for protocols based on pseudo-random functions or random oracles. However, we have identified a protocol in [30] which can be considered as a generalization of our protocol and allows us to reason about the privacy of our protocol.

In [30], the following protocol is considered, based on two random functions $F : \{0,1\}^{\alpha+k+1} \to \{0,1\}^k$ and $G : \{0,1\}^k \to \{0,1\}^k$

1. the initial state of the tag is set to a random k-bit string K_0;
2. the protocol rules are:
   (a) the reader picks a random α-bit string a and sends it to the tag;
   (b) the tag in state K sends the value $c = F(0, K, a)$, stores $d' = F(1, K, a)$ in its temporary memory, and refreshes its state K to $G(K)$;
   (c) the reader searches its database for a pair (T', K') with the property $c = F(0, G(K')^i, a)$ for some $i < t$. If it finds such a pair then it sends $d = F(1, G(K'), a)$ to the tag, and updates K' by $G(K')^i$;
   (d) the tag checks $d = d'$.

It is shown in [30] that this protocol is narrow-destructive private in the random oracle model, if k and t are polynomially bounded (in the security parameter) and 2^{-k} is negligible (the reader is referred to [45, 30] for privacy models for RFID protocols; the limited space does not allow us to recall them here).

Our protocol follows the same line as the protocol above. The internal state of the tag is the vector

$$P(T), K_{ST}, c_0, c_1, c_2, c_3, c_4, LT$$

The function F is the one which gives the answer to the reader's query (see step 2 in the protocol), while G is the function used by the tag and the server to update the internal state. The tag performs one more update of its state when it authenticates the reader but this does not make much difference between our protocol and the one described above. We have not included an upper bound on the number of incomplete sessions, but this can be added as mentioned in Remark **??**. Therefore, we may think that our protocol is an instance of the protocol described above and, as a conclusion, it may be thought of as a lightweight candidate to the narrow-destructive private class of mutual authentication RFID protocols.

The protocol does not achieve forward security. If a tag is corrupted and the adversary gets the internal state of the tag, then the adversary can impersonate the tag if it does not miss any complete session (a session is complete if the tag authenticates the server and, in such a case, it randomizes its state by the nonce received from the reader). However, if the adversary misses some complete session, then he can impersonate the tag with negligible probability. This property is common to many other authentication protocols such as [27, 25]. In fact, reaching forward security without public key cryptography is an open

2 Identity-based Encryption

This section is based on

> F.L. Tiplea, E. Simion: *New Results on Identity-based Encryption from Quadratic Residuosity*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

Identity-based encryption (IBE) was proposed in 1984 by Adi Shamir [40] who formulated its basic principles but he was unable to provide a solution to it, except for an identity-based signature scheme. Sakai, Ohgishi, and Kasahara [39] have proposed in 2000 an identity-based key agreement scheme and, one year later, Cocks [11] and Boneh and Franklin [5] have proposed the first IBE schemes. Cocks' solution is based on quadratic residues. It encrypts a message bit by bit and requires $2\log n$ bits of cipher-text per bit of plain-text. The scheme is quite fast but its main disadvantage is the ciphertext expansion. Boneh and Franklin's solution is based on bilinear maps. Moreover, Boneh and Franklin also proposed a formal security model for IBE, and proved that their scheme is secure under the Bilinear Diffie-Hellman (BDH) assumption.

The Cocks scheme [11] is very elegant and per se revolutionary. It is based on the standard QRA modulo an RSA composite. The scheme encrypts one bit at a time. The bits are considered to be exactly the two values (i.e., -1 and 1) of the Jacobi symbol modulo an RSA modulus n, when applied to an integer non-divisible by n. Thus, if Alice wants to send a bit $b \in \{-1, 1\}$ to Bob, she randomly generates an integer t with the Jacobi symbol b modulo n, hides t into a new message $s = t + at^{-1} \bmod n$ obtained by means of Bob's identity a, and sends s to Bob. The decryption depends on whether a is a quadratic residue or not modulo n. As neither Alice nor Bob knows whether a is a quadratic residue

or not, Alice repeats the procedure above with another integer t' whose Jacobi symbol modulo n is b, and sends $s' = t' - at'^{-1} \bmod n$ as well. Now, Bob can easily decrypt by using a private key obtained from the key generator, because either a or $-a$ is a quadratic residue modulo n. It can be shown that the Cocks IBE scheme is IND-ID-CPA secure in the random oracle model under the QRA.

The main disadvantage regarding the efficiency of the Cocks scheme consists of the fact that it encrypts one bit by $2 \log n$ bits. A very interesting idea proposed by Boneh, Gentry and Hamburg [6] is to encrypts a stream of bits by multiplying each of them by an Jacobi symbol randomly generated. The generation of these new Jacobi symbols are based on the equation $ax^2 + Sy^2 \equiv 1 \bmod n$. Any solution to this congruential equation leads to two polynomials f and g with the property that $g(s)$ and $f(r)$ have the same Jacobi symbol modulo n, for any square root s of S and any square root r of a. Therefore, g can be used to encrypt one bit, while f can be used to decrypt it. If the solutions of the above congruential equation can be obtained by a deterministic algorithm, then the decryptor knows how to decryt the ciphertext. Therefore, in order to send an ℓ-bit message to Bob, Alice has to solve 2ℓ equations as above (two equations for each bit, one for Bob's identity a and the other one for $-a$), while the decryptor needs to solve only ℓ equations. The ciphertext size is $2\ell + \log n$ bits. Some improvements at the sender side reduces the number of equations to be solved by the encryptor to $\ell + 1$.

An important improvement of the Boneh-Gentry-Hamburg (BGH) scheme was proposed later by Jhanwar and Barua [21]. The improvement works in two directions: improve the time complexity of the algorithm to solve equations $ax^2 + Sy^2 \equiv 1 \bmod n$, and reduce the number of equations to be solved. The first improvement is based on a careful analysis of the solutions of the equation $ax^2 + Sy^2 \equiv 1 \bmod n$. Thus, an efficient probabilist algorithm is developed to randomly generate solutions of such an equation. The second improvement is based on a composition formula according to which two solutions can be combined in some way to obtain a new solution. Therefore, to encrypt an ℓ-bit message, only $2\sqrt{\ell}$ equations need to be solved. Unfortunately, the probabilistic nature of the algorithm by which solutions are obtained leads to a ciphertext larger than in the case of the BGH scheme, namely $2\ell + 2\sqrt{\ell} \log n$ bits. The Jhanwar-Barua (JB) scheme was revisited in [14], where some errors were corrected; unfortunately, the security was not sufficiently argued as it was later remarked in [13]. Moreover, [13] also proposes an improvement by which the number of equations needed to be solved by Alice is reduced to $2 \log \ell$. The ciphertext size is also reduced to $2\ell + 2(\log \ell)(\log n)$ bits.

It is well-known that the Cocks scheme is not anonymous [6]. Several researchers tried to extend this scheme to offer identity anonymity; usually, such extensions are based on creating lists of ciphertext so that the identity becomes hidden in the lists. This approach gives rise to very large ciphertexts. It was also a believe that the Cocks scheme does not have homomorphic properties. A very recent result [22] rehabilitates the Cocks scheme with respect to these two weaknesses. Joye [22] identified the algebraic structure of the Cocks ciphertexts: he proved that these are squares in a torus like structure, and form a quasi-group. The underlying group law is the operation needed on ciphertexts to show that the Cocks scheme is homomorphic when the operation on clear messages is the multiplication. Therefore, the Cocks scheme offer homomorphic properties. Another important consequence obtained in [22] is about the anonymity of the Cocks scheme. It was shown that a different way of computing the ciphertext, without expansion, leads to identity anonymity.

A very interesting question is whether high order Jacobi symbols can be used in the Cocks scheme in order to encrypt more than one bit at a time. A first attempt to do that is the one in [7]. Unfortunately, the only secure scheme proposed in [7] suffers from massive ciphertext expansion.

3 Attribute-based Encryption

This section is based on

> F.L. Ţiplea: *Sharing Secrets on Boolean Circuits: Application to Key-policy Attribute-based Encryption*, invited talk, Romanian Cryptology Days, Sept 21-23, 2015, Bucharest (Romania).

Attribute-based encryption (ABE) is a new paradigm in cryptography, where messages are encrypted and decryption keys are computed in accordance with a given set of attributes and an access structure on the set of attributes. There are two forms of ABE: *key-policy ABE* (KP-ABE) [18] and *ciphertext-policy ABE* (CP-ABE) [4]. In a KP-ABE, each message is encrypted together with a set of attributes and the decryption key is computed for the entire access structure; in a CP-ABE, each message is encrypted together with an access structure while the decryption keys are given for specific sets of attributes.

In this paper we focus only on KP-ABE. The first KP-ABE scheme was proposed in [18], where the access structures were specified by monotone Boolean formulas (monotone Boolean circuits of fan-out one, with one output wire). An

extension to the non-monotonic case has later appeared in [29]. Both approaches [18] and [29] take into consideration only access structures defined by Boolean formulas. However, there are access structures of practical importance that cannot be represented by Boolean formulas, such as multi-level access structures [**?**, **?**]. In such a case, defining KP-ABE schemes to work with general Boolean circuits becomes a necessity. The first solution to this problem was proposed in [16] by using leveled multi-linear maps. A little later, a lattice-based construction was also proposed [17].

There are two main construction of KP-ABE schemes based on bilinear maps. The first one [18] works in two steps: in the first step, a secret is top-down shared on a Boolean tree, while in the second step some information is bottom-up reconstructed using just one bilinear map. The scheme is very appealing and practically efficient. However, it works only with Boolean trees (formulas); a direct extension of it to general Boolean circuits faces the backtracking attack [16]. The second construction [16] works in just one step which is a bottom-up reconstruction of some information, by means of a leveled multi-linear map (sequence of bilinear maps with special constraints). The scheme can be used with general Boolean circuits but is much less efficient than the one in [18]: the decryption key size depends on the number of gates of the Boolean circuit and the leveled multi-linear maps are more complex structures than bilinear maps. Moreover, leveled multi-linear maps of some depth k do not easily scale to fit Boolean circuits of depth larger than $k + 1$.

Whether KP-ABE schemes for general Boolean circuits can be constructed using only bilinear maps, is an open question. A starting point in answering this question would be to find a way of extending the scheme in [18] to general Boolean circuits. The simplest idea to do that is to look for methods of top-down secret sharing on Boolean circuits, capable to defeat the backtracking attack. In this paper we propose two such methods. The first one extends the scheme in [18] to work with general Boolean circuits. The scheme is practically efficient only for a subclass of Boolean circuits which strictly extends the class of Boolean formulas (and, therefore, it is a proper extension of the scheme in [18]). The second method, when used in conjunction with simplified forms of leveled multi-linear maps, gives rise to a scheme which works for general Boolean circuits and is much efficient than the scheme in [16]. Both schemes we propose are secure in the selective model.

Part III
Accomplishments

The results obtained during the second phase consist of four research papers:

1. G.D. Năstase F.L. Ţiplea: *On a Lightweight Authentication Protocol for RFID Systems*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

2. F.L. Tiplea, E. Simion: *New Results on Identity-based Encryption from Quadratic Residuosity*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

3. N. Roşia, V. Cervicescu, M. Togan: *Efficient Montgomery Multiplication on GPUs*, 8th International Conference on Security for Information Technology and Communications, SECITC 2015, June 11-12, 2015, Lecture Notes on Computer Science 9522.

4. F.L. Ţiplea: *Sharing Secrets on Boolean Circuits: Application to Key-policy Attribute-based Encryption*, invited talk, Romanian Cryptology Days, Sept 21-23, 2015, Bucharest (Romania).

These papers covers the authentication and key management in RFID systems, as well as identity-based cryptography together with its problems (such as key-escrow and construction of ABE schemes for general Boolean circuits). These completely cover the proposed outputs of Phase II. We thus consider that the objectives of the Phase II of the project have been completely reached, preparing the way for the third phase.

References

[1] G. Avoine and P. Oechslin. A scalable and provably secure hash-based RFID protocol. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 110–114, march 2005.

[2] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for RFID-tags, 2006.

[3] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-key cryptography for RFID-tags. In *Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 217–222, Washington, DC, USA, 2007. IEEE Computer Society.

[4] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, S&P 2007, pages 321–334. IEEE Computer Society, 2007.

[5] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 213–229, London, UK, UK, Aug. 2001. Springer-Verlag.

[6] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryptionwithout pairings. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 647–657, Washington, DC, USA, 2007. IEEE Computer Society.

[7] Dan Boneh, Rio LaVigne, and Manuel Sabin. Identity-based encryption with e^{th} residuosity and its incompressibility. In *Autumn 2013 TRUST Conference*, Washington DC, oct 2013. Poster presentation.

[8] M. Burmester and B. De Medeiros. The security of epc gen2 compliant RFID protocols. In *Proceedings of the 6th international conference on Applied cryptography and network security*, pages 490–506, Berlin, Heidelberg, 2008. Springer-Verlag.

[9] H.-Y. Chien and C.-W. Huang. Security of ultra-lightweight RFID authentication protocols and its improvements. *SIGOPS Oper. Syst. Rev.*, 41(4):83–86, July 2007.

[10] H.-Y. Chien and C.-W. Huang. A lightweight authentication protocol for low-cost RFID. *J. Signal Process. Syst.*, 59(1):95–102, April 2010.

[11] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pages 360–363, London, UK, UK, Dec. 2001. Springer-Verlag.

[12] Ferucio Laurenţiu Ţiplea. A lightweight authentication protocol for RFID. In Zbigniew Kotulski, Bogdan Ksiopolski, and Katarzyna Mazur, editors, *Cryptography and Security Systems*, volume 448 of *Communications in Computer and Information Science*, pages 110–121. Springer Berlin Heidelberg, 2014.

[13] Ferucio Laurenţiu Ţiplea, Emil Simion, and George Teşeleanu. An improvement of Jhanwar-Barua's identity-based encryption scheme. Technical report, 2015.

[14] Ibrahim Elashry, Yi Mu, and Willy Susilo. Jhanwar-Barua's identity-based encryption revisited. In ManHo Au, Barbara Carminati, and C.-C.Jay Kuo, editors, *Network and System Security*, volume 8792 of *Lecture Notes in Computer Science*, pages 271–284. Springer International Publishing, 2014.

[15] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the aes algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370. Springer Publishing Company, Incorporated, 2004.

[16] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In Ran Canetti and JuanA. Garay, editors, *Advances in Cryptology CRYPTO 2013*, volume 8043 of *Lecture Notes in Computer Science*, pages 479–499. Springer Berlin Heidelberg, 2013. Preprint on IACR ePrint 2013/128.

[17] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *STOC*, pages 545–554. ACM, 2013. Preprint on IACR ePrint 2013/337.

[18] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encypted data. In *ACM Conference on Computer and Communications Security*, pages 89–98. ACM, 2006. Preprint on IACR ePrint 2006/309.

[19] D. Henrici and P. Muller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pages 149–153, March 2004.

[20] J. Hermans, R. Peeters, and B. Preneel. Proper RFID privacy: Model and protocols. *Mobile Computing, IEEE Transactions on*, 13(12):2888–2902, Dec 2014.

[21] Mahabir Prasad Jhanwar and Rana Barua. A variant of boneh-gentry-hamburg's pairing-free identity based encryption scheme. In *Inscrypt*, pages 314–331, 2008.

[22] Marc Joye. On identity-based cryptosystems from quadratic residuosity. 2015.

[23] A. Juels. Minimalist cryptography for low-cost RFID tags (extended abstract). In Carlo Blundo and Stelvio Cimato, editors, *Security in Communication Networks*, volume 3352 of *Lecture Notes in Computer Science*, pages 149–164. Springer Berlin Heidelberg, 2005.

[24] A. Juels and S. A. Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, *Advances in Cryptology CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 293–308. Springer Berlin Heidelberg, 2005.

[25] Sleyman Karda, Serkan Çelik, Atakan Arslan, and Albert Levi. An efficient and private RFID authentication protocol supporting ownership transfer. In Gildas Avoine and Orhun Kara, editors, *Lightweight Cryptography for Security and Privacy*, volume 8162 of *Lecture Notes in Computer Science*, pages 130–141. Springer Berlin Heidelberg, 2013.

[26] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede. Elliptic-curve-based security processor for RFID. *IEEE Transactions on Computers*, 57(11):1514 –1527, nov. 2008.

[27] C. H. Lim and T. Kwon. Strong and robust RFID authentication enabling perfect ownership transfer. In P. Ning, S. Qing, and N. Li, editors, *Information and Communications Security*, volume 4307 of *Lecture Notes in Computer Science*, pages 1–20. Springer Berlin Heidelberg, 2006.

[28] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In *In RFID Privacy Workshop*, 2003.

[29] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In *ACM Conference on Computer and*

Communications Security, pages 195–203. ACM, 2007. Preprint on IACR ePrint 2007/323.

[30] Radu-Ioan Paise and Serge Vaudenay. Mutual authentication in RFID: Security and privacy. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '08, pages 292–299, New York, NY, USA, 2008. ACM.

[31] G. Pantelić, S. Bojanić, and Violeta Tomašević. Authentication protocols in RFID systems. In Y. Zhang and P. Kitsos, editors, *Security in RFID and Sensor Networks*, pages 99–120. Auerbach Publications, Apr 2009.

[32] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. Emap: An efficient mutual-authentication protocol for low-cost RFID tags. In Robert Meersman, Zahir Tari, and Pilar Herrero, editors, *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361. Springer Berlin Heidelberg, 2006.

[33] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. M2ap: A minimalist mutual-authentication protocol for low-cost RFID tags. In Jianhua Ma, Hai Jin, LaurenceT. Yang, and JeffreyJ.-P. Tsai, editors, *Ubiquitous Intelligence and Computing*, volume 4159 of *Lecture Notes in Computer Science*, pages 912–923. Springer Berlin Heidelberg, 2006.

[34] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *Information Security Applications*, pages 56–68. Springer-Verlag, Berlin, Heidelberg, 2009.

[35] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. Lightweight cryptography for low-cost RFID tags. In Y. Zhang and P. Kitsos, editors, *Security in RFID and Sensor Networks*, pages 121–150. Auerbach Publications, Apr 2009.

[36] S. Piramuthu. Protocols for RFID tag/reader authentication. *Decision Support Systems*, 43(3):897–914, Apr 2007.

[37] Relevant Security Corp., Denver, Colorado, USA. *Real Privacy Management^{TM} (RPM). Reference Guide Version 3.1*, 2009.

[38] Relevant Security Corp., Denver, Colorado, USA. *Real Privacy Management^{TM} (RPM). Cryptographic Description Version 3.2*, 2010.

[39] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security (SCIS2000)*, January 2000.

[40] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York.

[41] B. Song and C. J. Mitchell. RFID authentication protocol for low-cost tags. In *Proceedings of the first ACM conference on Wireless network security*, pages 140–147, New York, NY, USA, 2008. ACM.

[42] H. Tanaka. Security-function integrated simple cipher communication system. In *Proceedings of the 2006 Symposium on Cryptography and Information Security*, 2006.

[43] H. Tanaka. Generation of cryptographic random sequences and its applications to secure enchipering. In *Proceedings of the 2007 Symposium on Cryptography and Information Security*, 2007.

[44] I. Vajda and L. Buttyn. Lightweight authentication protocols for low-cost RFID tags. In *In Second Workshop on Security in Ubiquitous Computing Ubicomp 2003*, 2003.

[45] Serge Vaudenay. On privacy models for RFID. In *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'07, pages 68–87, Berlin, Heidelberg, 2007. Springer-Verlag.

[46] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Mller, W. Stephan, and M. Ullmann, editors, *Security in Pervasive Computing*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212. Springer Berlin Heidelberg, 2004.