Secure Anonymous RFID Authentication Protocols

Christy Chatmon
Computer & Information Sciences
Florida A & M University
Tallahassee, Florida 32307-5100
cchatmon@cis.famu.edu

Tri van Le and Mike Burmester
Department of Computer Science
Florida State University
Tallahassee, Florida 323206-4530
{levan,burmester}@cs.fsu.edu

Abstract

The growing use of Radio Frequency Identification (RFID) technology to enhance ubiquitous computing environments has only begun to be realized. It allows for the identification of objects and/or subjects remotely using attached RFID tags via a radio frequency channel, hence identification is achieved in a contactless manner. The advantages of using RFID technology is growing tremendously and is gaining much attention as is seen by an increase in its deployment, such as object tracking and monitoring, supply-chain management, and personalized information services. Numerous authentication protocols for RFID systems were proposed in an attempt to prevent unauthorized tracking and monitoring, impersonation or cloning, and information leakage. Many of these attempts fail to enforce anonymity and offer only weak authentication and some fail under denial of service.

In this paper we propose three anonymous RFID authentication protocols and prove that they are secure in the traditional cryptographic framework. Our model allows most of the threats that apply to RFIDs systems including, denial of service, impersonation, malicious traceability, information leakage through power analysis and active man-in-the middle attacks. Our protocols are efficient and scalable.

Keywords: RFID, Authentication, Anonymity, Privacy, Availability, Scalability.

1 Introduction

Radio Frequency Identification (RFID) technology as an enabler of ubiquitous computing environments has only begun to be realized. The technology has made inroads in a variety of industries as an instrument for object identification, such as in automobile manufacturing, microchip fabrication, consumer products, and even cattle herding. The increased attention and attraction by researchers to RFID solutions can be contributed to its deployment in several large organizations in the retail industry, such as Procter and Gamble, Wal-Mart[9], Target, Albertsons, and also the United States Department of Defense. Its presence in everyday life will certainly be a reality in the near future.

The primary goal of RFID technology is to automatically identify objects that are contained in electromagnetic fields. RFID tags do not require physical contact for identification. This allows objects to be read in large numbers without physically handling the objects. Most RFID systems contain small and inexpensive passive tags in which it derives its power from the signal

of an interrogating reader. The small size of the tags is also an attractive feature allowing tags to be embedded and associated with objects in a more ubiquitous manner. A further advantage is the ability of tags to be uniquely coded and capable of holding a limited amount of data. Objects can be tracked and monitored as a means to thwart product theft, manage access control, oversee product inventory, lessen queuing time in retail stores, personalized information services, and much more. The increased deployment of RFID's is apparent as seen in the following examples:

- Hitachi has developed a 0.4mm-square RFID tag to embed into photocopier paper to allow for automatic document tracking [6].
- The November 2000 Transportation Recall Enhancement Accountability and Documentation (TREAD) Act mandated that RFID tags be embedded in automobile tires to allow precise tire tracking in the event of a recall. This was passed due to the Firestone/Ford scandal [8].
- Suppliers of consumer goods sent to Wal-Mart and the U.S. Military have begun embedding RFID tags in cases and pallets to make goods scannable by automatic inventory-control systems [9].

The widespread adoption and deployment of RFID technology by corporate and government interests, poses several privacy-related concerns for consumers and organizations alike. The first concern addresses the need to maintain secure user/location privacy (anonymity and untraceability). Passive eavesdroppers and active intruders should not successfully identify or track tags (users). The privacy issue has been recognized by many - politicians, media, organizations, and researchers. Researchers have proposed many solutions [2] such as tag "killing", frequent renaming of tags over time using an encrypted identifier, audit systems for RFID privacy (Watchdog Tag monitors and RFID Enhancer Proxy), blocker tags preventing unwanted scanning [13], etc.

The second issue is related to those attacks that attempt to disrupt the functionality of RFID tags. Effectively this type of attack can be defended against by cleverly incorporating authentication techniques as RFID tags and readers exchange messages. Such attacks as denial of service and counterfeiting can be combated if authentication is successful.

1.1 Related work

Several researchers have attempted to resolve the security concerns related to the use of RFID tags and have proposed protocols that claim either to achieve secure authentication or to prevent unauthorized traceability. Most of these solutions only apply for weak adversary model (see e.g., [4, 5, 7, 11, 12, 17, 16, 14]). In particular, those protocols for which a back-end server is a trusted third party and the channel between the reader and the server is insecure, are susceptible to man-in-the-middle attacks.

Weis-Sarma-Rivest-Engels [18] propose an RFID system in which random numbers are used in the tag's response messages to hide the identification of the tag and to avoid its reuse. This system addresses traceability, but at the cost of an increase in the work load of the back-end server to identify and verify the tag, by applying an exhaustive search. Impersonation is also possible using this scheme by performing an off-line attack, in which the tag is queried for a valid pair and then forwarding this pair to a reader for validation.

Henrici-Muller [20] propose a 3-round protocol for low-cost RFID systems based on a one-way hash function and a random number generator. The protocol begins as the reader queries the tag, and the tag responds with its hashed identification and the current transaction number. The response is forwarded by the reader to the back-end server for validation. To identify the tag the server checks the validity of the identifying information of the tag. The server then concludes by sending a random number to the tag so that the tag's identification is refreshed and

synchronized. This scheme was found to be insecure by Dimitriou in [10]. Like most previous schemes where the protocol relies on the back-end server to refresh the tag's identification, the approach is susceptible to a man-in-the-middle attack [19]. It also falls prey to an attack based on desynchronization of the counters shared by the tag and back-end server. Furthermore, the tag remains traceable based on the transaction numbers even though they are refreshed.

Hopper-Blum [7] describe two protocols that provide symmetric authentication for low cost RFID tags: the HB protocol and the HB+ protocol. It is claimed that HB is secure against passive attacks, while HB+ is secure against both passive and active attacks. Recently, Gilbert-Robshaw-Sibert [5] have shown that HB+ is vulnerable to active attacks with linear computational and communication complexity, Juels-Weis [1] and Katz-Shin [14] have shown that HB+ is provably secure in a weak security model in which the adversary is not allowed to attack an ongoing authentication session in order to learn the key.

More recently, Tsudik [16] proposed a tag authentication system that resists tracking by using monotonically increasing timestamps and a keyed hash. This approach requires no on-demand computation for the back-end server as a result of it pre-computing the hash-table for later tag verification. In this system, the reader sends the tag a timestamp that is compared to the previous value of the timestamp—and bounded by a maximum allowable value. The tag, based on the the results of the comparison, sends either the hashed (MAC) timestamp or a pseudo-random number to the reader, allowing the responses to be indistinguishable. This is forwarded to the back-end server where the tag is identified in a hash look-up table. Tsudik points out that this scheme is subject to a DoS attack in which the locally stored values of the timestamps of the tag and server are desynchronized, when the adversary sends an inaccurate timestamp to the tag.

¿From the work cited above, and the drawbacks, it is clear that in order to avoid traceability, the adversary must not be able to distinguish a tag's response from a random value during exchanges and the tag's identification must be refreshed and never reused. In order to avoid impersonation attacks, a challenge-response exchange must be incorporated in the scheme.

1.2 Our contribution

We propose three anonymous RFID authentication protocols: a 2-pass protocol and two 1-pass protocols. Our last protocol is "optimistic": the cost is minimal when the adversary is passive. These protocols are designed for low complexity systems and low power devices, and are scalable. We prove that they are secure using the traditionalcryptographic framework for authentication and anonymity. Our threat model allows for most of the threats that apply to RFID devices, including power analysis (side-channel) attacks [15] and active man-in-the middle attacks [4].

2 Model and Definitions

A Model for an RFID authentication system An RFID authentication system has three components: tags T, readers R, and a trusted server S. Tags are wireless transponders: they typical have no power of their own and respond only when they are in an electromagnetic field. Readers are transceivers and generate such fields: they challenge by broacast any responding tag. There are two types of broadcast challenges: multicast and unicast. Multicast challenges are addressed to all tags in the range of the reader, whereas unicast challenges are addressed to specific tags. In our protocols below we have both types of challenges. However, our multicast challenges are just random strings, and *all* tags in the range of a reader R are challenged with *the same* random string. This kind of action is *not* usually counted as a communication pass.

We shall assume that all ("honest") tags T adhere to the system specifications and the requirements of the authentication protocol. The same applies for the readers R and of course the trusted server S—they are all "honest". Tags are issued with private keys K which they share (only) with the trusted server S. These keys are used by the tags for identification. We denote by $\mathcal{K}$ the set of all authorised keys (issued by S). Figure 1 illustrates the flow of exchanged

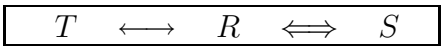

Figure 1: The authentication flow in an RFID system.

data, between a tag T and the trusted server S via the reader R, during the authentication of T. We shall refer to the interaction between T and R as *a conversation* and the data as an *authentication transcript*. In our RFID authentication protocols we shall assume that R and S are linked by a secure communication channel (reliable and authenticated). Therefore, our protocols are essentially two party protocols, one party being a tag T and the other a reader $R = R^S$, with secure access to a server S. These parties are abstracted as probabilistic Turing machines. T-machines with severly restrained resources, and R-machines with adequate resources. For "optimistic" authentication protocols, the resource must be minimized for both machines.

This model describes the setting for the "honest" parties: the tags that are authenticated with private keys $K \in \mathcal{K}$, that adhere to the protocol, the readers R that adhere to the protocol, and the trusted server.

The adversary The adversary $\mathcal{A}$ can control a certain number of tags and readers. The tags of the adversary, denoted by T', are unauthorised, in the sense they do not have a private key $K \in \mathcal{K}$. Similarly, the readers of the adversary, denoted by R', are unauthorized, in the sense that they do not have authenticated access to the trusted server S.

An *active* adversary $\mathcal{A}$ can modify the conversations between any pair T, R arbitrarily (e.g. adaptively and concurrently), and indeed initiate and terminate a session, at its choice. As an extension of a passive (eavesdropping) adversary, $\mathcal{A}$ is also allowed to learn the output of the session, *i.e.* the reader's decision to accept or not, at the end of every sessions. Since the channel between a reader R and the server S is assumed secure (authenticated), we do not need allow $\mathcal{A}$ to interact with the server S directly, but only through ("honest") readers.

When designing secure RFID authentication protocols one should also take into account attacks that are excluded from the security model used (the "system"). Sometimes these attacks may be prevented by using "out-of-system" protection mechanisms. Of course, it is preferable to deal with such attacks within the model. Below we list two such attacks:

1. *Power analysis attacks (side channel attacks).* These are attacks in which the private key of a device is extracted by exploiting either its power consumption when inaccure/accurate received bits are processed or the variations in the timing of its energy output.
2. *Online man-in-the-middle relay attacks.* These are attacks in which an unauthorised reader R' and tag T' interpose between an authentic tag T and reader R so that, the authentication flow in (T, R, S) is diverted to a flow (T, R', T', R, TS) that authenticates the imposter T' using the authentication data of T.
3. *Offline man-in-the-middle active attacks.* These are attacks in which an unauthorized reader R' and tag T' interpose between an authentic tag T and reader R so that, when R' challenges T appropriately in (T, R'), the data obtained will leak private information of T when input to $(T'R, S)$.

The security framework RFID transponders are typically low complexity and low power devices that are only activivated when in the range of an reader. Due to their low complexity, we do not allow *concurrent* executions of the tags: that is, an authorized tag T cannot initiate an authentication with reader R_1 while it is being authenticated by reader $R_2 \neq R_1$. Indeed this should be prevented by the authentication protocol (for example, by marking the tag's internal state that it is in an active session) even when $R_1 = R_2$ (we don't want the same tag to be counted twice in a single period). This means that all concurrent executions of an authentication protocol in the range of a reader R are for different tags T (with *independent* private keys K). Unauthorised tags of course may execute the protocol concurrently.

Secure protocols are *universal composable* if they remain secure even when they are composed with arbitrary protocols, or more generally when used as a component of an arbitrary system. It is important therefore that when dealing with security one uses a security framework that supports universal composability. In general designing secure protocols that are universally c omposable is a challenging task. This task is significantly alleviated in our case because we discount concurrency for the tags and our protocols are essentially one-pass protocols (the server only uses secret keys in the last pass).

Security definitions The security of an RFID protocol can be described in terms of three games, an *authentication game* $\mathcal{G}_{auth}$, an *anonymity game* $\mathcal{G}_{anon}$, a *tracing game* $\mathcal{G}_{trace}$ and an *availability game* $\mathcal{G}_{avail}$, with players: the adversary $\mathcal{A}$ against the honest tags T and the honest readers R. In these games there are two steps. The first step is a preparing step for the adversary $\mathcal{A}$: $\mathcal{A}$ is allowed to interact arbitrarily with the tags and the readers. In the second step, $\mathcal{A}$'s knowledge is tested. The score of $\mathcal{A}$ in game $\mathcal{G}$ is his advantage $adv_{\mathcal{G}}^{\mathcal{A}}$. $\mathcal{A}$ wins if his advantage is non-negligible. We now describe in more detail the second steps of the four games: $\mathcal{G}_{auth}$, $\mathcal{G}_{trace}$, $\mathcal{G}_{anon}$ and $\mathcal{G}_{avail}$.

Authentication In the second step of $\mathcal{G}_{auth}$, $\mathcal{A}$ must impersonate some tag T to some reader R. During this impersonation step, $\mathcal{A}$ is allowed to interact arbitrarily with all other tags and readers, *except the one tag* T that $\mathcal{A}$ is trying to impersonate.

The advantage of the adversary $adv_{\mathcal{G}_{auth}}^{\mathcal{A}}$ is the probability that $\mathcal{A}$ succeeds in authenticating itself to R. An RFID protocol is a secure *authentication protocol* if $adv_{\mathcal{G}_{aut}}^{\mathcal{A}}$ is negligible.

We have excluded $\mathcal{A}$ from interacting with the tag T from the second step because this seems to correspond to reality: if $\mathcal{A}$ were allowed to interact with T as a reader R' during this step, and then simply relay faithfully the conversation between T and R' to an authorised reader R in order to get authenticated as T (without mounting any attack). This is the online man-in-the middle attack described above in 3.

Untraceability is a weak notion of anonymity. In the second step of the tracing game $\mathcal{G}_{trace}$, $\mathcal{A}$ must trace some tag T: $\mathcal{A}$ is given access to (i.e. ability to interact with) a challenge tag T^* and must tell whether T^*, is T or not, better than guessing. In this tracing step, A is also allowed to interact with all tags and readers, in particular, interacting with T. The advantage $adv_{\mathcal{G}_{trace}}^{\mathcal{A}}$ of the adversary in this game is

$$|\text{Prob}[\mathcal{A} \text{ correct}] - \frac{1}{2}|, \text{ where Prob}[\mathcal{A} \text{ correct}] = \text{Prob}[\mathcal{A} = yes \mid T = T'] + \text{Prob}[\mathcal{A} = no \mid T \neq T']$$

and we require that $\text{Prob}[T = T'] = \frac{1}{2}$. We have untraceability if $adv_{\mathcal{G}_{trace}}^{\mathcal{A}}$ is negligible.

Unlinkability is a strong notion of anonymity, which is the one we use in this paper. For anonymity we require that the advantage $adv^{\mathcal{A}}_{\mathcal{G}_{anon}}$ of the adversary in the second step of $\mathcal{G}_{anon}$ in linking two different interactions to the same tag is negligible. The setting for $\mathcal{G}_{anon}$ is the same as in $\mathcal{G}_{trace}$, except that in $\mathcal{G}_{trace}$ the adversary already knows T through other interactions in the first step. In $\mathcal{G}_{anon}$ both T and T^* are challenge tags. Through interacting with T and T^*, as well as all other normal tags and readers, $\mathcal{A}$ must tell whether it is interacting with identical tags or not, *i.e.* whether T and T^* have the same key $K \in \mathcal{K}$ or not..

Availability In $\mathcal{G}_{avail}$ the adversary $\mathcal{A}$ must prevent a tag T from being authenticated by a reader R in a challenge session *ses*, without interacting with this session *ses*. In this attack, $\mathcal{A}$ is allowed to interact with all tags and all readers, except of course for the session *ses*. The advantage $adv^{\mathcal{A}}_{\mathcal{G}_{avail}}$ of $\mathcal{A}$ in this game is the probability that R rejects T in the challenge session *ses*.

For *completeness* of an authentication protocol π, we explicitly require that: for all authorized tags T and readers R, π accepts with overwhelming probability. We note that this is implied implicitly in the availability game $\mathcal{G}_{avail}$.

Our RFID authentication protocols in the next section are designed to deal with power analysis attacks and offline man-in-the middle active attacks. For the online man-in-the middle attacks an "out-of-system" solution should be sought.

3 Anonymous RFID authetication protocols

In this section we propose three RFID authentication protocols, a 2-pass authentication protocol and two 1-pass authentication protocols. The last protocol is optimistic, in the sense that its cost is low when the adversary is passive. We shall prove that these are secure using our security model, and that the tags are untraceable.

These protocols address most of the drawbacks of the authentication protocols in [10, 11, 16, 12, 17], and will also thwart power analysis attacks. Our first protocol is an extension of YA-TRAP proposed by G. Tsudik [16] which we briely describe below.

3.1 YA-TRAP – Yet Another Trivial Authentication Protocol

For this protocol, the timeline is divided into small periods, during which each tag is allowed to be authenticated at most once. The readers and the server maintain a (loosely) synchronized timestamp t_{sys}. The tags do not have clocks. Each tag T is equipped with a pseudo-random number generator (which may be resolved as an iterated keyed hash function), and is initialized with a private key K and timestamps t_0 and t_{max}. $\mathcal{K}$ is the set of all keys that have been issued to tags.

When a reader R activates tag T, it broadcasts the current timestamp t_{sys}. If $t_{sys} \leq t_{tag}$, where t_{tag} was the last timestamp that T received, or if $t_{sys} > t_{max}$, then T broadcasts a pseudo-random string; otherwise T broadcastes $h = H_K(t_{sys})$, and sets $t_{tag} = t_{sys}$. Here $H_K(t_{sys})$ is the hash of t_{sys} with key K, and t_{tag} is initialized with the value t_0.

The server S finds the value of the key that T has used in h from a hash look-up table –see Figure 2. In this table, whenever a timestamp t_s is updated, the server computes the keyd hash values $H_K(t_s)$ for all keys $K \in \mathcal{K}$, and get the next row of the table. This table, $\{h_{i,j} = H_{K_i}(j)\}$, makes it possible for the server S to find out whether the tag T that issued the hash h is authentic, $h = h_{t_{sys},j}$ for some $j \in [1, n]$, without having to search exhaustively for the key each time a new tag is challenged during time period t_s (typically one or a few minutes).

	K_1	K_2	$\cdots$	K_n
$t_s = 1$	$h_{1,1}$	$h_{1,2}$	$\cdots$	$h_{1,n}$
$t_s = 2$	$h_{2,1}$	$h_{2,2}$	$\cdots$	$h_{2,n}$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
$t_s = i$	$h_{i,1}$	$h_{i,2}$	$\cdots$	$h_{i,n}$

Figure 2: The hash look-up table.

Tsudik points out [16] that there is a drawback in YA-TRAP: the adversary can send a wildly inaccrate timestamp t'_{sys} (say the maximum timestamp allowed) and incapacitate the tag. This is a DoS attack which will kill the tag. It quite is difficult to address this attack since the tag T needs to update its time t_{tag} regardless of the value of the time t'_{sys} sent by adversary, otherwise its identity will be traced by sending the same t'_{sys} every time. To avoid tracing, it is not sufficient to randomize the tag's response since that would eliminate the savings that the server gets from using the look-up table.

There is also a "future-time" attack in which the adversary queries the tag offline with several valid time periods $t_{sys,i}$, $i = 1, 2, , \ldots$. The adversary then captures the tag's responses and can use that for online authentication when these time periods. Therefore, by using a predictable time value as a challenge for the tag will not work.. In the following section we show who to deal with these attacks while keeping the server scalable by adapting the protocol YA-TRAP.

3.2 A 2-Pass optimistic anonymous RFID authentication protocol

YA-TRAP is (essentially) a 1-pass protocol, in the sense that the timestamp is broadcast (not unicast) by R to all tags in range. We now show that how to extend YA-TRAP to deal with the DoS attack in which the adversary disables the tag T by sending an inaccurate timestamp.

The protocol we propose is essentially a 1-pass authentication protocol with an optional pass. In the first step the tag is authenticated, whereas in the second step the server authenticates the timestamp. The protocol is given in Figure 3.

R broadcasts (t_{sys}, r_{sys}).

1. $T \rightarrow R \rightarrow S$: $r_{tag},\ h_1 = H_K(0, t_{sys}, r_{sys})$ if $t_{sys} > t_{tag}$
   $r_{tag},\ h_1 = H_K(1, r_{tag}, r_{sys})$ if $t_{sys} \leq t_{tag}$
2. $S \rightarrow R \rightarrow T$: $r_{tag},\ h_2 = H_K(2, r_{tag}, t_{sys})$ (optional)

– S accepts T as authentic only if:
$\exists K \in \mathcal{K} : (h_1 = H_K(0, t_{sys}, r_{sys})) \vee (h_1 = H_K(1, r_{tag}, r_{sys}))$.

– T verifies that $h_2 = H_K(2, r_{tag}, t_{sys})$. (optional)

– T sets $t_{tag} = t_{sys}$ if $t_{sys} > t_{tag}$.

Figure 3: A 2-Pass optimistic anonymous RFID authentication protocol

In our protocol the tag T, instead of sending a pseudo-random string when the timestamp it gets is out of its bounds, it sends a keyd hash of the string $(1, r_{tag}, t_{sys})$. This will save the

tag T, but now the server S must work harder. More specifically, if the hash value h is not in the look-up table (see Figure 2), then the server must search exhaustively for the key K. Of course, this only happens with tags that the adversary has tried to kill (or incapacitate).

Our approach is to shift the adversary's attack from the low complexity tags to the server. This approach is optimistic, in the sense that when the adversary is passive than the server need only use the look-up table. Note that pass 2 is optional. This pass is only used by the server during time periods when the number of attacks occur beyond a certain threshold and the server would like to resynchronize the time t_{sys} to all the tags so that their stored time t_{tag} is valid.

This is applied to all tags during such time periods so that no identity information are revealed. When this period passes, the server could return to normal operation and will bypass pass 2. This makes the scheme resistant to DoS while being almost as efficient as [16].

3.3 A 1-Pass optimistic anonymous RFID authentication protocol

keys	K_1	K_2	$\cdots$	K_n
strings	r_{K_1}	r_{K_2}	$\cdots$	r_{K_n}

Figure 4: A look-up string table.

This protocol uses a key lookup table in which the keys K are linked to session number r_K, see Figure 4. The optimistic protocol is described in Figure 5 and is only one pass.

R broadcasts r_{sys}.

1. $T \rightarrow R \rightarrow S : r_{tag},\ \ h = H_K(r_{sys}, r_{tag})$

– T updates $r_{tag} \leftarrow H_K(r_{tag})$.

– S accepts T only if:

$\exists K$: (r_{tag}, K) are in the key look-up table s.t.: $h = H_K(r_{sys}, r_{tag})$ (optimistic)

OR $\exists K \in \mathcal{K}$ such that $h = H_K(r_{sys}, r_{tag})$ (exhaustive search)

– S updates $r_{tag} \leftarrow H_K(r_{tag})$.

Figure 5: A 1-Pass anonymous RFID authentication protocol

The protocol described in Figure 5 always uses only one pass. When a tag has been attacked, its pseudorandom value r_{tag} will be out-of-sync with its counter part s_K stored in the server. At this time, the server will have to search for all keys to find the correct one and then resynchronize s_K. Even when this happens, the scheme has the advantage that the server only needs to do extra computation for tags that are authenticated, not for all the tags. When no fault occurs, the server simply has to do one lookup and hashing for each authenticating tag. So computation is saved on tags that do not communicate.

In the non-optimistic version of this protocol, the tag and server uses true random r_{tag} and therefore the server needs to search and udpate its value for any tag that requires authentication. This scheme is suitable for cases where the number of active tags is smaller than the number of tags. We leave the detail of the protocol for the full version of the paper.

3.4 Proof of security

The security properties of the schemes can be shown to follow from modeling the hash function by pseudorandom function. The approach is similar to the one used by Bellare and Rogaway in [3] adapted to take into account availability and unlinkability.

References

[1] Ari Juels and Stephen Weis, Authenticating Pervasive Devices with Human Protocols. Advances in Cryptology – CRYPTO 2005, LNCS, volume 3621, pages 293-308, 2005.

[2] M. Bellare, R. Canetti and H. Krawczyk, Pseudorandom functions revisited: The cascade construction and its concrete security, *Proceedings of the 37th Symposium on Foundations of Computer Science,* IEEE, 1996.

[3] Mihir Bellare and Phillip Rogaway. Entity Authentication and Key Distribution. *Advances in Cryptology - CRYPTO 93*, Lecture Notes in Computer Science, vol. 773, pp. 232-249, Springer, 1994.

[4] Henri Gilbert and Matthew Robshaw and Herve Sibert. An Active Attack Against HB+ - A Provably Secure Lightweight Authentication Protocol. eprint.iacr.org/2005/237.pdf

[5] Henri Gilbert and Matthew Robshaw and Herve Sibert. An Active Attack Against HB+ - A Provably Secure Lightweight Authentication Protocol. *PerSec '04*, March 2004.

[6] Hitachi unveils smallest rfid chip. RFID Journal, March 2003.

[7] N.J. Hopper and M. Blum. Secure Human Identification Protocols. *Advances in Cryptology - Asiacrypt '01*, 2001.

[8] Michelin embeds rfid tags in tires. RFID Journal, January 2003.

[9] Wal-mart details rfid requirement. RFID Journal, November 2003.

[10] Gildas Avoine. Adversarial model for radio frequency identification, 2005.

[11] Tassos Dimitriou. A lightweight rfid protocol to protect against traceability and cloning attacks. *IEEE SECURECOMM*, 2005.

[12] Tassos Dimitriou. A secure and efficient rfid protocol that can make big brother obsolete. *International Conference on Pervasive Computing and Communications, PerCom*, 2006.

[13] Ari Juels, Ronald Rivest, and Michael Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. *Conference on Computer and Communications Security - ACM CCS*, October 2003.

[14] Jonathan Katz and Ji Sun Shin. Parallel and Concurrent Security of the HB and HB+ Protocols Cryptology ePrint Archive: Report 2005/461 (to appear in the proceedings of Eurocrypt 2006).

[15] Adi Shamir. EPC tags subject to phone attack, *RFID Journal.* http://www.rfidjournal.com/article/articleview/2167/1/1/

[16] Gene Tsudik. Ya-trap: Yet another trivial rfid authentication protocol. *International Conference on Pervasive Computing and Communications, PerCom*, 2006.

[17] Istv Vajda and Levente Butty. Lightweight authentication protocols for low-cost rfid tags. *Workshop on Security in Ubiquitous Computing*, October 2003.

[18] S. Weis and S. Sarma and Ronald Rivest and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Indentification Systems. *Proc. of the 1st Security in Pervasive Computing, LNCS*, October 2004.

[19] Jeongkyu Yang and Kui Ren and Kwangio Kim. Security and Privacy on Authentication Protocol for Low-cost RFID. *Symposium on Cryptography and Information Security*, January 2005.

[20] D. Henrici and P. Muller. Hashed-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. . *PerSec '04*, March 2004.