His Late Master's Voice:⋆ barking for location privacy⋆⋆

Mike Burmester

Florida State University, Tallahassee, Florida, U.S.A.
burmestercs.fsu.edu
http://www.cs.fsu.edu/∼burmeste

The only way to be safe is to never be secure.
Macbeth, III.5.2, W. Shakespeare

Abstract. Bob died suddenly leaving his treasure to sister Alice. Eve will do anything to get it, so Alice hides the treasure together with Nipper, and promptly departs. Nipper is a low-cost RFID device that responds *only* to Alice's calls—making it possible for Alice to locate the hidden treasure later (she is quite forgetful) when Eve is not around. We study the design of Nipper, the cryptographic mechanisms that support its functionality and the security of the application.

Keywords: RFID, localization privacy, location privacy, device discovery.

1 Introduction

Radio Frequency Identification (RFID) is a promising new technology widely deployed for supply-chain and inventory management, retail operations and more generally, automatic identification. The advantage of RFID over barcode technology is that it does not require line-of-sight reading. Furthermore RFID readers can interrogate RFID tags (devices) at greater distances, faster and concurrently. One of the most important advantages of RFID technology is that tags have read/write capability, allowing stored information to be altered dynamically.

In this paper we focus on *passive* RFID devices that are battery-less and harvest power from RFID readers. Some passive RFID devices such as WISP (Wireless Identification and Sensing Platform) [21] developed by Intel Labs, have additional features such as a real-time clock (that relies on harvested power) and a 3D-accelerometer, while others are more basic. EPCGlobal [8] recently ratified the EPC Class 1 Gen 2 (EPC-Gen2) standard for passive RFID deployments which defines a platform for RFID protocol interoperability. This supports basic reliability guarantees and is designed to strike a balance between cost and functionality. EPCGen2 operates in the 860-960 MHz band for which the effective broadcast range is rather restricted—typically less than $10m$.

⋆ The HMV trademark comes from a painting by Francis Barraud who inherited from his late brother a fox terrier, Nipper, a cylinder phonograph and a number of his (late brother's) recordings [11]. The painting portrays Nipper listening to the sound emanating from the trumpet of the phonograph.

⋆⋆ This material is based upon work supported by the National Science Foundation under Grant No. 1027217.

RFID systems that broadcast at GHz frequencies, such as those used with automatic toll collection systems, have a larger range, typically $100m$.

Several RFID protocols that address security issues for passive devices have been proposed in the literature. We refer the reader to a comprehensive repository available online at [1]. Most RFID protocols use hash functions [19, 16, 10, 2, 7, 15]. Some protocols use pseudo-random functions [5, 20, 3], or pseudo-random number generators. Recently a lightweight RFID protocol was proposed [4] that is based on loosely synchronized pseudo-random number generators.

Our contribution in this article is to study a novel application of RFID in which tags will only "backscatter" a signal if this is authentic. Authentication is the primary goal for RFID deployments, however it is important that the process used to support it does not have a negative impact on other security goals, such as privacy. If an RFID tag has to reveal its identity to get authenticated, then an eavesdropper can track its movement in the supply chain. For some applications *linkability* is a serious privacy threat. To deal with such threats one typically uses pseudonyms. However this still will not prevent the adversary from detecting the *presence* of responding tags. The location of a transmitting device can be determined by analyzing its radio signals. For outdoor applications the signal strength and/or direction are used (with triangulation protocols (see e.g., [17]); for indoor applications one may have two antennas on each tag and analyze the phase difference of their signals (to deal with multi-path effects, see e.g., [9]). *Localization privacy* requires that an RFID tag will only respond to a challenge from an RFID reader if it can first ascertain that the challenge is authentic and fresh (current).[1] In particular, that it is not replayed. Since the range of RFID readers is rather short, replay attacks are a major threat for RFID deployments—in the scenario discussed in the abstract, Eve may find the treasure by replaying Alice's call to Nipper, if Eve happens to be close to the treasure and Alice is out-of-range.

Localization privacy captures a novel aspect of privacy extending the traditional privacy notions of anonymity and unlinkability to devise discovery. Anonymity and unlinkability (see e.g., [6, 14]) are slightly weaker notions: even though the adversary may not be able to recognize a tag, or link its interrogation sessions, knowing its location will identify that tag to some degree, particularly if the tag is static and there are only a few tags in the range of an RFID reader—see Section 2.1, Application 1. Localization privacy is essentially a steganographic attribute. The goal of steganography is to hide data in such a way that the adversary cannot detect its existence, while the goal of localization privacy is to hide a device in such a way that its presence cannot be detected.

Our Contribution. RFID localization techniques enable applications that reveal the location of tags. In this paper we consider the problem of protecting the privacy of localization. We show that:

- If temporal and location mechanisms are available then location privacy can be achieved for one-time interrogation applications in the presence of a ubiquitous adversary. For applications requiring multiple tag interrogations we only get weak localization privacy.

[1] The title of this paper: "Nipper barks for location privacy", captures this functionality.

– If only location mechanisms are available then localization privacy can be achieved for one-time tag interrogations in the presence of a ubiquitous adversary. For applications requiring multiple tag interrogations we only get weak localization privacy.
– If only temporal mechanisms are available then we cannot achieve localization privacy for ubiquitous adversaries (unless the reader and tags have highly synchronized clocks); however we do get weak localization privacy.
– If neither temporal nor location mechanisms are available then we cannot achieve any kind of localization privacy.

2 RFID tags know the current time and their location

To motivate our application we start with the case when RFID tags have clocks and know their location.

In our first protocol (and the following) the RFID reader shares with each tag a unique secret key k. Let $time_r$ be the time the reader sends its challenge and loc_r the location of the reader (as measured by the reader); and let $time_t$ be the time the challenge was received by the tag and loc_t its location (as measured by the tag).

Protocol 1

Step 1. The RFID reader sends to the tag the challenge:

$$time_r,\ loc_r,\ x = MAC_k(time_r, loc_r).$$

where MAC_k a keyed message authentication code (*e.g.*, OMAC [12]).

Step 2. The tag checks the challenge. If the authenticator x is valid, $|time_t - time_r| < \delta_{time}$ and $dist(loc_r, loc_t) < \delta_{range}$, where $\delta_{time} > 0$, $\delta_{range} > 0$ are appropriate bounds, then the tag responds with

$$y = MAC_k(x).$$

Step 3. The RFID reader checks the response y. If this is valid it accepts the tag (as authentic).

Step 1 of this protocol authenticates the RFID reader to the tag, and can be thought of as the response to a "time and location" query from the environment (a trusted entity that is not under the control of the adversary). The tag only responds if the time the challenge was sent and the location of the reader are within acceptable ranges related to its own time reading and location. This assures localization privacy. Replay attacks beyond the range of the reader are thwarted by having the location of the reader included in the challenge; replay attacks in the range of the reader (at a later time) are thwarted by having the time the challenge was sent included in the challenge.

The actual location of the tag is determined by analyzing its response in Step 2, *i.e.,* its radio signals using a localization algorithm. Such algorithms determine the source of a transmission by using signal strength and/or direction (triangulation algorithms [17]), or the phase difference [**?**]. More than one reader will be needed but only one reader needs to broadcast the challenge.

The tag's response authenticates the tag to the reader, so we have mutual authentication. In Section 6 we shall show that this protocol provides mutual authentication with localization privacy for device discovery against ubiquitous adversaries (as defined in Section 2.2).

2.1 Applications

There are several applications for localization privacy. In this paper we consider two such applications for static tags:

1. *Device discovery.* This involves one-time tag interrogations: when the device is discovered it is recovered and the task for that device terminates. An example of such an application involves the deployment of tagged plastic mines. More generally, applications in which objects are hidden so that they can only be recovered later by authorized agents. For such applications, for each object, localization privacy lasts for only one interrogation.
2. *Sensor deployments in hostile territory.* Tagged sensors can be deployed by casting them from aircraft over hostile territory. The sensors are used for monitoring the deployment area but are not networked for localization privacy. Instead an armored RFID reader traverses the deployment area interrogating those tags on its route that are in range (the route must go though every cell of the sensor range grid). For this application localization privacy should endure for several interrogations.

2.2 Threat model

Our threat model is based on a Byzantine adversary that can eavesdrop on, and schedule, all communication channels, adapted for the wireless medium to allow for: (i) *localization (or surveillance) technologies* that analyze radio signals (based on the strength and/or direction of the signal, phase differences, etc) and (ii) *radio jamming technologies* that override signals emitted by devices.

We distinguish two types of adversary: (i) *ubiquitous*, that can access all deployed tags,[2] and (ii) *local*, whose wireless range is approximately that of authorized RFID readers. Local adversaries are restricted by their broadcast range: protection against such adversaries assures only weak localization privacy. In our threat model for localization privacy we constrain the impact of localization and signal jamming technologies by assuming that:

1. The adversary must eavesdrop on *at least one* complete tag response to localize the tag.
2. The adversary *cannot* localize a tag during an authorized interrogation if the tag's response is too weak to be received by the RFID reader.[3] Similarly, the adversary *cannot* localize a tag during an interrogation by jamming its response (to prevent the reader from getting it).[4]

[2] This can be achieved in several ways, *e.g.*, by using a hidden network of listening devices—although setting up such a network may be perilous in a plastic mine deployment.

[3] The tag will only respond to the reader's signal if this is sufficiently strong.

[4] The reader will either identify, locate and destroy the intruder or refrain from interrogating the tag.

3. A local adversary *cannot* localize a tag from its response while it is interrogated by an authorized reader.[4]

Assumption 3 highlights the weakness of local adversaries. It is partly justified by noting that the tag's response (a modulated backscatter) is much weaker than the reader's challenge, and attenuates as the inverse fourth power of traveled distance. Without it we cannot have localization privacy with multiple tag interrogations since the location of the tag would be revealed the first time it responds to an authorized challenge.

From Assumption 2 we either have:

4. *Reliability.* If a tag is in the range of an authorized RFID reader that interrogates it, then the interrogation will be completed,

or we have a DoS-deadlock between the authorized reader and the adversary. We shall assume that in the second case, the authorized reader always wins—the intruder is located and destroyed.

Remark 1. A ubiquitous adversary can eavesdrop on all communication channels, and therefore can also localize any tag that is interrogated by an authorized RFID reader, *after* the reader has localized it (by Assumption 1; disruption attacks are restricted by Assumption 2). For such adversaries localization is restricted to one-time tag interrogations. After the tag is localized it is inactivated/killed. We have:

5. *One-time tag interrogation.* A ubiquitous adversary *cannot* localize (discover) a tag that has already been located by an authorized reader.

The scope of replay attacks against localization privacy with one-time tag interrogations applications (*e.g.*, device discovery), is restricted to replaying reader challenges beyond the range of the reader (by Assumptions 2,5, since a tag will only respond once, when the challenge is authentic.

Remark 2. In Protocol 1 the RFID reader must send a different challenge to each tag (using the shared key k). If the number of tags is large and the reader does not know the approximate location of each tag (as possibly in the sensor deployment discussed in Section 2.1) then tag interrogation can be time consuming—the protocol is not scalable. For such applications we may use Public Key Cryptography: the RFID reader authenticates the time and its location with an Elliptic Curve Cryptography (ECC) signature [13]: $sig_{\mathrm{SK}_r}(time_r, loc_r)$, instead of the message authentication code $MAC_k(time_r, loc_r)$. Here SK_r is the private key of the RFID reader. The tag can verify this using the public key PK_r of the RFID reader. However verifying ECC signatures can be computationally expensive.[5]

Remark 3. In both applications discussed in Section 2.1 only the RFID reader is mobile, while the location of the RFID tag is fixed for the lifetime of the system. Consequently

[5] If the tag responds with the message authentication code $MAC_k(time_r, loc_r)$, then we still have a scalability issue (but this time on the search time rather than the number of broadcast challenges): the reader must check the response for all keys k in its database. For one-time interrogation applications, the tag can include its tag ID, or a preassigned pseudonym.

if a Global Positioning System (GPS) is used, this is activated only once. It follows that the tag can be equipped with a small battery and a GPS used to establish its position on deployment. Several hybrid RFID solutions are currently available (see *e.g.*, [18]).

3 RFID tags know their location

In our second protocol the RFID reader shares with each tag a secret key k as well as a counter *ct* which is updated with each interrogation. The reader stores in a database for each tag a pair (k, ct) containing the key and the current value of the counter. The tag stores in non-volatile memory a list (k, ct^{old}, ct^{cur}) containing an old value and the current value of its counter. The stored values at the reader and tag are updated by: $ct \leftarrow next(ct)$ and $ct^{old} \leftarrow ct^{cur}$, $ct^{cur} \leftarrow next(ct^{cur})$, respectively, with the tag's update made only if the value of the received counter ct is the same as the stored value of ct^{cur}, where the operator $next(\cdot)$ gives the next value of the counter. At all times at least one of the two values of the counter of the tag is the same as that stored at the reader. Initially $ct = ct^{old} = ct^{cur}$.

Protocol 2

Step 1. The RFID reader sends to the tag the challenge:

$$ct, loc_r, x = MAC_k(ct, loc_r).$$

Step 2. The tag checks the challenge. If $dist(loc_r, loc_t) < \delta_{range}$, where $\delta_{range} > 0$ is an appropriate parameter, and if x is valid for either $ct = ct^{old}$ or $ct = ct^{cur}$ then it responds with:

$$y = MAC_k(x),$$

and if $ct = ct^{cur}$, sets: $ct^{old} \leftarrow ct^{cur}$ and $ct^{cur} \leftarrow next(ct^{cur})$.

Step 3. The reader checks y. If this is valid then it updates its counter $ct \leftarrow next(ct)$, accepts the tag (as authentic), and sends to the tag,

$$z = MAC_k(y).$$

Step 4. The tag checks z. If this is valid then its sets: $ct^{old} \leftarrow ct^{cur}$.

In this protocol the RFID reader updates its counter after receiving a response from the tag (Step 3). If a response is not received, then the same value of the counter is used the next time. This is why the tag must keep the old value of the counter ct^{old}. This value will only be updated when the interrogation is completed. It follows that at all times, at least one of the values of the counters of the tag is the same as that of the counter of the reader.

In Section 6 we shall show that Protocol 2 provides mutual authentication with localization privacy for one-time tinterrogation applications. For applications where a tag can be interrogated several times we only get weak localization privacy. This is because even though a local adversary cannot discover a tag while it is interrogated by an authorized reader (Assumption 3), it can eavesdrop on the interrogation and later replay the reader's challenge (in the same location) and use a localization algorithm to locate the tag.

Remark 4. In Protocol 2, loosely synchronized counters partly capture the functionality of loosely synchronized clocks in Protocol 1. However there is a subtle difference between these protocols. If the adversary in Protocol 2 is allowed to prevent the reader from receiving the tag's response in Step 2 (Byzantine adversaries schedule communication channels) then the reader will abort the session without updating its counter. The adversary may later replay the reader's challenge to localize the tag: since the counter was not updated the tag will respond. This attack is prevented by Assumptions 2,4. Protocol 1 is not subject to this weakness.

4 RFID tags know the current time

In our third protocol the RFID reader shares with each tag a secret key and the reader and tags have loosely synchronized clocks.

Protocol 3

Step 1. The RFID reader sends to the tag the challenge:

$$time_r\ ,\ x = MAC_k(time_r).$$

Step 2. The tag checks the challenge. If $|time_t - time_r| < \delta_{time}$, where $\delta_{time} > 0$ is an appropriate parameter, and if x is valid then it responds with:

$$y = MAC_k(x).$$

Step 3. The RFID reader checks y. If it is valid then it accepts the tag (as authentic).

This protocol does not provide (strong) localization privacy. A ubiquitous adversary can use an online man in the middle attack to relay the flows of the RFID reader to the tag, when the tag is not in range of an authorized reader—unless the tag and reader have highly synchronized clocks. In Section 6 we shall show that Protocol 3 provides mutual authentication with weak localization privacy.

Remark 5. Observe that temporal mechanisms in Protocol 3 cannot replace the location mechanisms of Protocol 2. The reason is that online man in the middle attacks on location mechanisms are constrained by the broadcast range of RFID readers (tags can determine their location in this range), while such attacks on temporal mechanisms are constrained by the speed of light (tags can only detect such attacks if they, and the reader, have highly synchronized clocks)—which for most applications is not lightweight.

5 RFID tags do not know the time or location

Theorem 1. *Localization privacy cannot be achieved when the tags are static if neither temporal nor location information is available to the tags.*

Proof. The proof is by contradiction. Suppose that neither temporal nor location information is available. First consider a ubiquitous adversary. If a tag is not in range of the RFID reader that challenges it, then the adversary can use an online man-in-the-middle relay attack to forward the reader's challenge to another area of the deployment zone were the tag may be. The tag has no way of checking that the challenge was sent from far away and/or much earlier. So it will respond. This violates localization privacy.

Next consider a local adversary. In this case suppose that the tag is not present during the interrogation. Then the adversary may record the challenge of the RFID reader and replay the challenge later (an offline man in the middle attack). Again the tag has no way of detecting that the challenge was sent from another location earlier, and will respond. □

6 Proofs for Protocols 2, 3 and 4

We now sketch the security proofs for the protocols presented in this paper. Proofs in a strong security framework will be given in the full version of the paper.

Theorem 2. *Protocol 1 provides mutual authentication with localization privacy for one-time tag interrogation applications against ubiquitous adversaries. For applications where tags may be interrogated several times we only get weak localization privacy.*

Proof. (Sketch) First consider a ubiquitous adversary with one-time tag interrogations. By Assumptions 5 the adversary cannot discover a tag that is already discovered (interrogated). Also, the adversary gains no advantage when the interrogation fails by Assumption 2. If the tag is not present while it is interrogated then the adversary can replay the reader's challenge to other areas where the tag may be. This is thwarted because the challenge contains location information. The only remaining attack is to forge the keyed message authentication code: if a cryptographic hash function is used this is not feasible.

Next consider applications where tags can be interrogated several times, with a local adversary. By Assumption 3 the adversary cannot localize a tag while it is interrogated. However it can replay the challenge of the reader in the same place at a later time: this attack is thwarted because the challenge contains temporal information. If the tag is not in the range of the RFID reader when it is challenged, then the adversary can replay the challenge to other places where the tag may be. This attack is thwarted because the challenge contains location information. Finally forging the message authentication code is not feasible as observed earlier.

We get mutual authentication because the RFID reader is authenticated to the tag in Step 1 and the tag is authenticated to the reader in Step 2. □

Theorem 3. *Protocol 2 provides mutual authentication with localization privacy for one-time tag interrogation applications against ubiquitous adversaries. For applications where tags may be interrogated several times we only get weak localization privacy.*

Proof. (Sketch) As in Theorem 2, a ubiquitous adversary will not succeed while the tag is interrogated, and will not succeed by replaying the reader's challenge to some other areas when the tag is not present during an interrogation, because the challenge contains location and information. Also forging the message authentication code is not feasible. The only remaining attack is to de-synchronize the counters of the reader and the tag. This is not possible because that tag always keeps an old value of the counter, and the counters are only updated when the interrogation is completed.

Next consider applications where tags are interrogated several times and the adversary is local. Again the adversary cannot localize a tag which is interrogated, but can replay the challenge either in the same location (later) or other locations. The first attack is thwarted because the reader and tag have updated their counters; the second because the challenge contains location information. Finally forgery and de-synchronization attacks fail as in the ubiquitous adversary case.

Mutual authentication is as in Theorem 2. □

Theorem 4. *Protocol 3 provides only mutual authentication with weak localization privacy, unless highly synchronized clocks are available.*

Proof. (Sketch) As observed in Section 4, a ubiquitous adversary can use an online man in the middle attack to relay the flows of the RFID reader to the tag, when the tag is not in range of an authorized reader—unless the tag and reader use highly synchronized clocks (which is not practical for lightweight applications). The tag will then accept the reader's challenge and respond. So we cannot have localization privacy.

Next consider applications where tags are interrogated several times with a local adversary. Again the adversary cannot localize a tag while it is interrogated by an authorized reader. However it can replay the challenge, later. Replaying it locally will not succeed because the tag will have updated its counter—it will complete its interrogation by Assumption 4. Replaying it to another location will not succeed because the challenge contains temporal information (this is an offline man in the middle attack, so the difference between the send and receive time will be greater than δ_{time}). Finally as in Theorem 3 forgery and de-synchronization attacks will fail and we have mutual authentication. □

Acknowledgement. The author would like to thank Xiuwen Liux and Zhenghao Zhang for helpful discussions on accurate localization technologies and security issues; Jorge Munilla for helpful comments on the protocols and localization; and all those present at the SPW 2011 presentation of this paper for helpful suggestions; finally Oakland.

References

1. AVOINE, G. RFID Security and Privacy Lounge. http://www.avoine.net/rfid/, 2010.
2. AVOINE, G., AND OECHSLIN, P. A scalable and provably secure hash-based rfid protocol. In *PERCOMW '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops* (Washington, DC, USA, 2005), IEEE Computer Society, pp. 110–114.
3. BURMESTER, M., AND DE MEDEIROS, B. The Security of EPC Gen2 Compliant RFID Protocols. In *ACNS* (2008), S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung, Eds., vol. 5037 of *Lecture Notes in Computer Science*, Springer, pp. 490–506.

4. BURMESTER, M., AND MUNILLA, J. Flyweight authentication with forward and backward security. *ACM Trans. Inf. Syst. Secur. 12* (2011), accepted 8/27/2010, available at http://www.cs.fsu.edu/ burmeste/103.pdf.
5. BURMESTER, M., VAN LE, T., AND DE MEDEIROS, B. Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In *Proceedings of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006)* (2006), IEEE Press.
6. DANEZIS, G., LEWIS, S., AND ANDERSON, R. How Much is Location Privacy Worth? Fourth Workshop on the Economics of Information Security (WEIS 2005). Harvard University, 2/3 June 2005.
7. DIMITRIOU, T. A secure and efficient RFID protocol that can make big brother obsolete. In *Proc. Intern. Conf. on Pervasive Computing and Communications, (PerCom 2006)* (2006), IEEE Press.
8. EPC GLOBAL EPC tag data standards, vs. 1.3. http://www.epcglobalinc.org/standards/EPCglobal_Tag_Data_Standard_TDS_Version_1.3.pdf.
9. HEKIMIAN-WILLIAMS, C., GRANT, B., LIU, X., ZHANG, Z., AND KUMAR, P. Accurate localization of rfid tags using phase difference. In *2010 IEEE International Conference on RFID* (2010), RFID 2010, IEEE, pp. 89–96.
10. HENRICI, D., AND MÜLLER, P. M. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *Proc. IEEE Intern. Conf. on Pervasive Computing and Communications* (2004), pp. 149–153.
11. HIS MASTER'S VOICE. http://en.wikipedia.org/wiki/His Master's Voice.
12. IWATA, T., AND KUROSAWA, K. Omac: One-key cbc mac. In *FSE* (2003), T. Johansson, Ed., vol. 2887 of *Lecture Notes in Computer Science*, Springer, pp. 129–153.
13. LEE, Y. K., BATINA, L., SINGELEE, D., PRENEEL, B., AND VERBAUWHEDE, I. Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. In *Towards Hardware-Intrinsic Security, Information Security and Cryptography – THIS 2010* (November 2010), A.-R. Sadeghi and D. Naccache, Eds., Springer, pp. 237–257.
14. LIU, L. From data privacy to location privacy: models and algorithms. In *Proceedings of the 33rd international conference on Very large data bases* (2007), VLDB '07, VLDB Endowment, pp. 1429–1430.
15. MOLNAR, D., SOPPERA, A., AND WAGNER, D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In *Proc. Workshop on Selected Areas in Cryptography (SAC 2005)* (2006), vol. 3897 of *LNCS*, Springer.
16. OHKUBO, M., SUZUKI, K., AND KINOSHITA, S. Cryptographic approach to "privacy-friendly" tags. In *Proc. RFID Privacy Workshop* (2003).
17. POIROT, J., AND MCWILLIAMS, G. Navigation by back triangulation. *IEEE Transactions on Aerospace and Electronic Systems AES-12(2)* (1976), 270–274.
18. RFIDNEWS. EarthSearch launches GPS-RFID hybrid solution. http://www.rfidnews.org/2009/03/16/earthsearch-launches-gps-rfid-hybrid-solution.
19. SHARMA, S. E., WEISS, S. A., AND ENGELS, D. W. RFID systems and security and privacy implications. In *Proc. of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 20002)* (2003), vol. 2523 of *LNCS*, Springer, pp. 454–469.
20. VAN LE, T., BURMESTER, M., AND DE MEDEIROS, B. Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange. In *Proc. of the ACM Symp. on Information, Computer, and Communications Security (ASIACCS 2007)* (2007), ACM Press, pp. 242–252.
21. WISP. Wireless Identification and Sensing Platform, Intel Labs, Seattle. http://seattle.intel-research.net/wisp/.