Method Decoder for Low-Cost RFID Tags

Ari Juels
RSA Laboratories, USA

Abstract

A radio-frequency identification (RFID) tag is a small, inexpensive microchip that emits an identifier in response to a query from a nearby reader. The price of these tags promises to drop to the range of $0.05 per unit in the next several years, offering a viable and powerful replacement for barcodes. The challenge in providing security for low-cost RFID tags is that they are computationally weak devices, unable to perform even basic symmetric-key cryptographic operations. Security researchers often therefore assume that good privacy protection in RFID tags is unattainable. In this paper, we explore a notion of minimalist cryptography suitable for RFID tags. We consider the type of security obtainable in RFID devices with a small amount of rewritable memory, but very limited computing capability. Our aim is to show that standard cryptography is not necessary as a starting point for improving security of very weak RFID devices. Our contribution is threefold:

1. We propose a new formal security model for authentication and privacy in RFID tags. This model takes into account the natural computational limitations and the likely attack scenarios for RFID tags in real-world settings. It represents a useful divergence from standard cryptographic security modeling, and thus a new view of practical formalization of minimal security requirements for low-cost RFID-tag security.

2. We describe protocol that provably achieves the properties of authentication and privacy in RFID tags in our proposed model, and in a good practical sense. Our proposed protocol involves no computationally intensive cryptographic operations, and relatively little storage.

3. Of particular practical interest, we describe some reduced-functionality variants of our protocol. We show, for instance, how static pseudonyms may considerably enhance security against eavesdropping in low-cost RFID tags. Our most basic static-pseudonym proposals require virtually no increase in existing RFID tag resources.

1. Introduction

A passive radio-frequency identification (RFID) tag is a microchip that is capable of transmitting a static identifier or serial number for a short distance. It is typically activated by a query from a nearby reader, which also transmits power for the operation of the tag. Several varieties of RFID tag are already familiar in daily life. Examples include the small plaques mounted on car windshields for the purpose of automated toll payment, the theft-detection tags attached in shops to consumer goods such as clothing, and the proximity cards used to control physical access to buildings. More expensive RFID tags can execute advanced cryptographic and other functions, but we concern ourselves in this paper with the inexpensive variety geared to serve as a next-generation successor to barcodes.

The cost of rudimentary RFID tags promises to drop to roughly $0.05/unit in the next several years, while tags as small as 0.4mm × 0.4mm, and thin enough to be embedded in paper are already commercially available. Such improvements in cost and size augur a rapid proliferation of RFID tags into many areas of use. Indeed, Wal-Mart has issued a directive to its top one hundred suppliers requiring deployment of RFID at the pallet level [10], while The Gillette Company has recently placed an order for half a billion tags for use in supply-chain and retail environments [12]. A goal of researchers in RFID tag development is to see them serve ubiquitously as a replacement for barcodes. This change promises more flexible and intelligent handling of consumer goods and devices. Here are just a few enticing possibilities: Microwave ovens that can read the tags on packages and cook food without explicit instructions, refrigerators that can recognize expired and depleted foodstuffs, and closets that can inventory their contents (and perform a Web search for custom

fashion advice).

The impending ubiquity of RFID tags, however, also poses a potentially widespread threat to consumer privacy [27]. If RFID tags are easily readable, then tagged items will be subject to indiscriminate physical tracking, as will their owners and bearers. Researchers have recognized this problem for some time [21], and have yet to propose a truly satisfactory remedy.

The issue has also seen recent attention in the popular press, whose negative news coverage forced the clothing retailer Benetton to withdraw plans for embedding RFID tags in its items of apparel [6]. Corporate privacy is similarly problematic, as RFID tags can facilitate corporate espionage by revealing information about the operation of supply chains.

Auto-ID Labs and EPC Global (together formerly known as the Auto-ID Center) have been leading institutions in the development and standardization of RFID tags. Their initial RFID-chip designs are geared toward general corporate and consumer use. So as to permit inexpensive manufacture, they carry only the most basic functionality, emitting a static, 96-to- 256-bit identifier on receiving a reader query. Auto-ID Center chip designs give recognition to importance of privacy by permitting an RFID tag to be "killed," i.e., rendered permanently inoperable on receiving a short, specially designated key. Other design proposals propose a pair of complementary "sleep" and "wake" commands that allow a chip to be rendered inoperable on a temporary basis. Thus, for example, a supermarket might deploy RFID tags to facilitate tracking of shipments and monitoring of shelf stocks. To protect the privacy of customers, checkout clerks might "kill" the tags of purchased goods. Alternatively, to permit tag use in the home, a consumer might furnish a secret "sleep" key at the time of checkout. This key could be used to put tags to sleep when the consumer leaves the supermarket, and to reawaken them for later use.

There are many environments, however, in which simple measures like use of "kill" or "sleep" commands are unworkable or undesirable for privacy enforcement. Consumers may wish RFID tags in their possession to remain active, or may simply find it inconvenient to manage their wake/sleep patterns. Businesses may have concerns about unauthorized monitoring of tags before they are "killed."We enumerate a few examples here of important uses and privacy concerns for which "kill" or "sleep" commands are unsatisfactory:

– **Access delegation**: A consumer may wish certain tags in her possession to be permanently active so as to enable reading by other parties. For example, a consumer might wish to use RFID tags for effortless physical access control,1 for theft-protection of belongings, for wireless cash and fidelity cards, and so forth. New and clever consumer applications are already beginning to emerge. For example, a Prada store in New York City tracks the RFID tags of items held by customers in order to display related accessories on nearby screens [2]. Function creep promises to result in many more uses unimagined or unimaginable today.

– **Consumer use**: As mentioned above, RFID readers may eventually be inexpensive enough and RFID tags prevalent enough to make a range of smart appliances practical in the home. In the shorter term, there are other consumer benefits, like the ability of consumers to return RFID-tags items to shops without the need for a receipt.

– **Industrial espionage**: Industrial espionage is a likely concern prior to the "killing" of tags. This is true, for example, in a retail environment, where a competitor capable of reading tags in shops or warehouses may gather business intelligence regarding the turnover rate of stocks, the shopping patterns of customers, and so forth.

– **Banknote tracking**: If tags are embedded in banknotes, then they must be permanently accessible to law enforcement agencies. One straightforward approach to enforcing privacy would be to distribute banknotes in a "sleep" state, and to assign a "waking" key to law enforcement. This is problematic in that to awaken banknote tags, a law enforcement reader must transmit the key, rendering it easily vulnerable to capture. Keys cannot be assigned on a fixed per-banknote basis, because in that case a banknote would have to emit a unique identifier in order to enable law enforcement to determine the correct key for that banknote. Thus a given awakening key would potentially have to be associated with a wide batch of banknotes, in which case one would expect privacy to be swiftly and broadly compromised.

RFID tags that promiscuously emit static serial numbers pose another serious problem, namely that of authentication. Such tags may be easily cloned by an attacker that has read access: The attacker need merely read the RFID tags of passersby to harvest their identifiers for later re-use. This is highly problematic for a number of the current and projected uses of RFID tags, most notably physical access to buildings via passive RFID tokens, and inventory tracking (especially with an eye to protection against counterfeiting). Privacy protection and the problem of authentication are thus intimately related, a fact highlighted by our investigations in this paper.

One of the most advanced of the current generation of

small, inexpensive RFID tags is the Atmel TK5552 [11]. This tag has 992 bits of storage and a data transmission rate of about 100kB / sec. It permits both reading and writing to the contents of its memory. The Atmel TK5552, however, costs as much as $1.00 per unit. Projections on the likely resources in several years of RFID tags with cost in the vicinity of $0.05 include several hundred bits of memory and somewhere between 5,000 and 10,000 logical gates, of which a considerable fraction will be required for basic tag functions. Such RFID tags may be expected to perform some basic computational operations, but not conventional cryptographic ones. At best, they may include security functions involving static keys, such as keyed reads and keyed writes, i.e., essentially just PIN-controlled data accesses.

Remark: One might take the view that Moore's law will ensure greater processing power on tags in the coming years, and thus that cryptographic functionality will eventually be available in five-cent tags. There is a competing phenomenon in this case, though: Users of low-end RFID tags are more concerned to see prices drop and RFID tags become more widespread than to see functionality increase. This means that cryptographic functionality in basic tags may be some time in coming.

2 . A Security Model for RFID Tags

Given the very basic functionality of RFID tags, it is natural to consider an adversary in an RFID-tag system whose capabilities are quite limited. In most cryptographic security definitions, as for IND-CCA security on public-key encryption schemes [4], an adversary is presumed to be able to experiment extensively with elements of the system in the course of mounting an attack. In particular, the adversary is regarded as capable of submitting a large number of "oracle" queries, that is, exploratory inputs to the cryptographic operations composing the system. (In asymptotic analyses, the number of such oracle queries is polynomially bounded in the security parameters for the system; in concrete analyses, the bound on queries aims to reflect the limits of current computing ability, and may be on the order of, say, 280 for local computation. Smaller bounds, e.g., 230 may be imposed for practical modeling where interaction with, e.g., an actual signing or decrypting party is involved.)
In modeling an RFID system, it is natural to treat both tags and tag-verifiers as oracles. Given the limited computing ability of tags, however, a practical system cannot feasibly withstand an adversary that can submit a large number of arbitrarily ordered queries to all oracles in the system. Moreover, a high degree of adversarial power would not accurately reflect the physical characteristics of an RFID-tag system. Both readers and tags operate only at short range, and tags may in many cases be highly mobile. Thus, the collection of "oracles" available to an adversary at a given time is likely to be small in practice.

We seek to model the limitations on adversarial power in an RFID-tag system by the following key assumption: An adversary may only interact with a given tag on a limited basis before that tag is able in turn to interact in a protected manner with a valid verifier. We refer to this protected interaction as a refresh. In particular, a refresh is a privacy and integrityprotected session between a verifier and tag in which the verifier may update keying data in the tag. A refresh models the use of a tag with a legitimate reader outside the range of the adversary. In our security model, we impose two restrictions on adversarial interaction with tags between refreshes:

Limited successive tag queries: We assume that an adversary may interact with targeted RFID tags only a relatively small number of times in rapid succession prior to a refresh. This restriction would follow naturally from use of the throttling mechanism that we propose. Suppose, for example, that an RFID tag only permits reading once every several seconds. Given that an RFID-tag typically has a read range of at most a few meters, a rogue reader would have difficulty in harvesting more than, say, one or two pseudonyms from most passersby; tags might easily store half-a-dozen or so pseudonyms, however.2 An attacker bringing a reader into a monitored environment like a shop or warehouse might similarly face difficulties in attempting prolonged intelligence gathering. We rely on this assumption to help enforce privacy protection in our proposed protocol.

3. Our Proposed Scheme

As explained above, our proposed protocol relies upon rotation by a tag through multiple pseudonyms, which we denote by _1, _2, . . ., _k. These pseudonyms, however, do not themselves serve as the sole means of authentication for tags. If a tag authenticated itself to a verifier merely by releasing a key ai, then an adversary could clone a tag very simply as follows. The adversary would query the target tag, obtaining ai; the adversary would then separately interact with the verifier, using the key ai to simulate a valid tag. Indeed, this is precisely the type of cloning attack to which standard RFID tags with static identifiers are vulnerable, e.g., current EPC designs. Any single-flow protocol is

necessarily vulnerable to such an attack.

To prevent this type of attack in our protocol, a tag only authenticates to a verifier after the verifier has itself authenticated to the tag. The verifier authenticates to a tag by releasing a key βi; this key βi is unique to a given pseudonym αi. Once the verifier has authenticated to the tag, the tag authenticates itself to the verifier by releasing an authentication key βi Like βi, this authentication key γi is unique to an identifier αi.. Briefly stated, we propose a kind of challenge-response protocol, but one that is carefully interwoven with pseudonym rotation.

In order to maintain the integrity of a tag over an extended period of time and in the face of multiple probing attacks by an adversary, we take the approach in our protocol of having the verifier update the {αi.}, {βi}, and {γi} values in an RFID tag after successful mutual authentication between tag and verifier. This introduces a new problem, however: An adversary can eavesdrop on or tamper with the secrets used in this update process. Our strategy for addressing this problem is to update values using one-time pads that have been transmitted across multiple authentication protocols. Thus an adversary that only eavesdrops periodically is unlikely to learn the updated {αi.}, {βi}, and {γi} values.

Updating tag values in this way provides integrity protection as an important side-benefit. An adversary without knowledge of the one-time pads used during a update cannot, for instance, mount a swapping attack involving the substitution of keys from one compromised tag into another tag.

3.1 The protocol

As above, let k be a parameter denoting the number of pseudonyms stored in a given tag and let m denote the number of authentication sessions over which one-time pads are constructed; in other words, the higher the value of m, the stronger the eavesdropping-resistance of the system. For visual clarity in our protocol figure, we omit variable ranges and tag subscripts on variables for keys. The variables i and j, however, always span the ranges {1, 2, . . ., k} and {1, 2, . . .,m} respectively. We use $\in_R$ here and elsewhere to denote uniform random selection. In case of a message-delivery failure, we assume the input of a special symbol $\perp$ (leading to protocol termination).We assume initialization of all entities by a trusted party, who generates a key set ABC for every tag and distributes this to both the tag and the verifier. All counters are initialized at 0. Details of our protocol are provided in Figure 1.

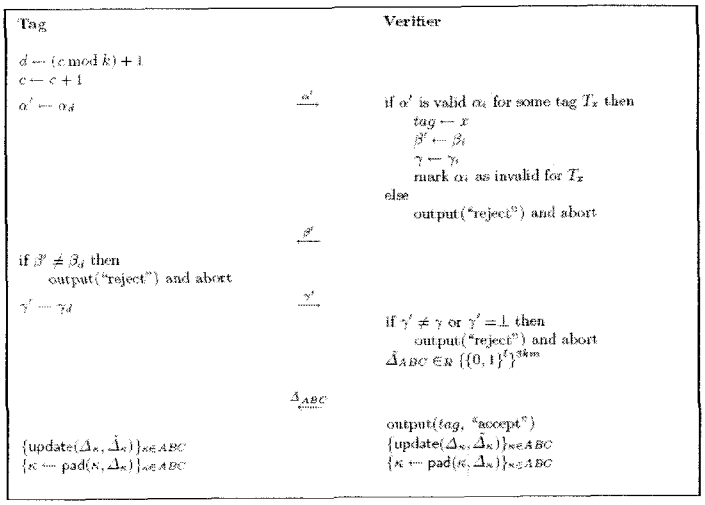

Figure. 1. Full RFID-tag authentication protocol

Remarks: We assume no collisions among tag identifiers here – a property that can be enforced during tag initialization and updates with only a very slight skew from a uniform random distribution over identifiers. Due to space limitations, we are forced to relegate formal security definitions and proofs for our proposed protocol to the paper appendices.

4 . Practical Deployment

4.1 Pruning our scheme

The full-blown scheme we have proposed is practical for very low-cost tags only with the use of small security parameters. There are a number of strategies, however, for reducing the functionality of scheme while still retaining important properties.

To begin with, in real-world deployments, the moderate security afforded by relatively short keys {βi} and perhaps also short {γi} keys would be acceptable in many cases. For example, if βi and γi keys are a mere twenty bits each, then an adversary would have roughly a onein- a-million chance of defeating the authentication protocol in a single try. Tag pseudonyms, i.e., the {αi} keys, must be considerably longer to permit unique identification of tags and to avoid pseudonym collisions. We believe that 100-bit _ values would suffice for this purpose in most environments. (It should be noted, however, that if a pseudonym collision occurs in the naming of a new tag, then different pseudonyms may be selected by the verifier. Such a naming strategy would probably permit a reduction in the lengths of αi tags to around 80 bits.) In

any event, large values of m or k are unlikely to be practical. Indeed, m = 0 (no updates via refresh) or 1 and k = 4 or 5 might be a reasonable choice for a real-world system.

A range of truncated versions of the protocol itself is also interesting. One example is a scheme that excludes the fourth flow from our protocol. In other words, the ABC values in the tag may remain the same throughout its lifetime. A much reduced variant might involve only the first flow in our protocol. This would mean that a tag merely cycles through a static set of pseudonyms, preferably with the benefit of throttling. This approach offers better privacy assurances than a system using static identifiers, but does not protect against cloning. (Such a degenerate case of our protocol also does not meet our security definitions unless the process of tag refresh in our model is replaced with elimination of a tag from the system.) Simple approaches like this might be especially attractive as a low-cost way of realizing privacy protection for RFID-enabled banknotes, weaker in some respects but involving much less overhead than the scheme proposed in [21]. Another, similarly useful truncation is one in which multiple identifiers $\{\alpha i\}$ are stored in a tag, but only a single key β and single key for common use with all identifiers.

These and kindred approaches have the advantage of backward compatibility with existing RFID systems employing just a static identifier or challenge-response. In other words, a reader does not have to have awareness of the fact than an identifier is in fact a pseudonym: Only the verifying application on the back-end needs to. Such systems would merely have to include some application-level support for linkage of pseudonyms, but would not necessarily require any software or firmware adjustments at the level of the reader.

Another interesting, restricted case is that involving just one identifier, but with the challenge-response and pseudonym replacement protocols intact. This limited variant would be useful for cases in which consumers are borrowing RFID-tagged books from libraries or renting RFID-tagged videos. Use of a single pseudonym like this would not prevent physical tracking. But authenticated rotation of the pseudonym would help prevent the bigger problem of passersby being scanned to determine what books or videos they are carrying. Given plans by the San Francisco public library to implant RFID tags in books, and the resistance of civil libertarians in reaction to the USA Patriot Act , this seems like a potentially attractivesolution.

5. Conclusion: Further Research

Our investigation here has proceeded under the assumption that even standard symmetric-key cryptographic algorithms lie beyond the computational reach of RFID tags. Such algorithms still deserve investigation along the lines of . We may, after all, anticipate greater future capabilities in RFID tags, as well as a broadening of the varieties and pervasiveness of computational devices in everyday surroundings.

One hardware-related problem is that of distributing pseudonyms efficiently to both tags and software applications. Pseudonyms might be determined at the time of manufacture, but it might also be convenient to make a master key for the pseudonyms of a particular tag readable via an optically or physically enabled channel, by analogy with [21]. This would make registration and transfer of ownership more fluid. A comprehensive perspective on key management is thus important in RFID-tag system development.

Finally, security modeling is another line of research that deserves further attention. We feel that the model proposed here captures a range of the special characteristics of RFID-tag environments in an effective way. This model can no doubt benefit from refinement, however, particularly as real-world experience with RFID-tag systems evolves, and as it becomes possible to draw on analogous experience and results from the field of ad-hoc networking. The centralized verifier model that we work with in this paper, for instance, is valuable as a first step toward RFID-system characterization. Further development and understanding of RFID systems will certainly yield other useful models involving varying degrees and forms of decentralization.

6. References

[1] Security technology: Where's the smart money? The Economist, pages 69–70. 9 February 2002.

[2] Prada's smart tags too clever? Wired News, 27 October 2002.

[3] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication
and key exchange protocols (extended abstract). In STOC '98, pages 419–428, 1998.

[4] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key
encryption schemes. In H. Krawczyk, editor, CRYPTO '98, pages 26–45. Springer-Verlag, 1998. LNCS no.

1462.
[5] M. Bellare and P. Rogaway. Entity authentication and key distribution. In D.R. Stinson, editor, CRYPTO '93, pages 232–249. Springer-Verlag, 1993. LNCS no. 773.
[6] Benetton undecided on use of 'smart tags'. Associated Press, 8 April 2003.
[7] D. Boneh, N. Modadugu, and M. Kim. Generating RSA keys on a handheld using an untrusted server. In B.K. Roy and E. Okamoto, editors, Indocrypt '00, pages 271–282. Springer-Verlag, 2000. LNCS no. 1977.
[8] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the
ACM, 24(2):84–88, 1981.
[9] D. Chaum. Security without identifications: transaction systems to make Big Brother obsolete. Communications
of the ACM, 28(10), 1985.
[10] J. Collins. The cost of Wal-Mart's RFID edict. RFID Journal, 10 Sept. 2003.
11. Atmel Corporation. Atmel TK5552 data sheet, 2001. Referenced at
http://www.atmel.com/atmel/products/prod227.htm.
[12] D.M. Ewatt and M. Hayes. Gillette razors get new edge: RFID tags. Information Week, 13 January 2003. Referenced at
http://www.informationweek.com/story/IWK20030110S0028.
[13] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31:469–472, 1985.
[14] S. Garfinkel. An RFID Bill of Rights. Technology Review, page 35, October 2002.
[15] G. Goebel. Codes, Ciphers, and Codebreaking. 1 March 2002. Online publication. Referenced at
http://www.vectorsite.net/ttcode.html.
[16] I. Goldberg and A. Shostack. Freedom network 1.0 architecture, November 1999.
[17] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. Springer-Verlag, 2004. To appear.
[18] L. Guillou and J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing
both transmission and memory. In C. G. G¨unther, editor, EUROCRYPT '88, pages 123–128.
Springer-Verlag, 1988. LNCS no. 330.
[19] J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: A ring based public key cryptosystem. In ANTS III, pages 267–288, 1998. LNCS no. 1423.
[20] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In D. Naccache, editor, RSA-CT '01, pages
176–191. Springer-Verlag, 2001. LNCS no. 2020.
[21] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, Financial Cryptography '03, pages 103–121. Springer-Verlag, 2003. LNCS no. 2742.
[22] A. Juels, R.L. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy.
In V. Atluri, editor, 8th ACM Conference on Computer and Communications Security, pages 103–111. ACM Press, 2003.
[23] RSA Laboratories. What is SecurID?, 2003. Referenced at
http://www.rsasecurity.com/rsalabs/faq/5-2-5.html.
[24] Auto-ID Labs. 13.56 MHz ISM band class 1 radio frequency identification tag interference specification: Candidate recommendation, version 1.0.0. Technical Report MIT-AUTOID-WH-002, Auto-ID Labs, 2003. Referenced at http://www.autoidlabs.org.
[25] Auto-ID Labs. 860 MHz-960 MHz class 1 radio frequency identification tag radio frequency and logical communication interface standard: Recommended standard, version 1.0.0. Technical Report MIT-AUTOIDTR-
007, Auto-ID Labs, 2003. Referenced at http://www.autoidlabs.org.
[26] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In H.M. Heys and C.M. Adams,
editors, Selected Areas in Cryptography, pages 184–199. Springer-Verlag, 1999. LNCS no. 1758.
[27] D. McCullagh. RFID tags: Big Brother in small packages. CNet, 13 January 2003. Referenced at
http://news.com.com/2010-1069-980325.html.
[28] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.
[29] S. Micali, S. Even, and O. Goldreich. On-line/off-line digital signatures. Journal of Cryptology, 9(1):35–67, 1996.
[30] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA broadcast authentication protocol. Crypto-Bytes, 5 (Summer), 2002.