Haruhisa Ichikawa
We-Duke Cho
Ichiro Satoh
Hee Yong Youn (Eds.)

LNCS 4836

Ubiquitous Computing Systems

4th International Symposium, UCS 2007
Tokyo, Japan, November 2007
Proceedings

Springer

Haruhisa Ichikawa We-Duke Cho
Ichiro Satoh Hee Yong Youn (Eds.)

Ubiquitous Computing Systems

4th International Symposium, UCS 2007
Tokyo, Japan, November 25-28, 2007
Proceedings

Springer

Volume Editors

Haruhisa Ichikawa
The University of Electro-Communications
Tokyo 182-8585, Japan
E-mail: h.ichikw@hc.uec.ac.jp

We-Duke Cho
UCN/CUS Ajou University
Suwon, 443-749, South Korea
E-mail: chowd@ajou.ac.kr

Ichiro Satoh
National Institute of Informatics
Tokyo 101-8430, Japan
E-mail: ichiro@nii.ac.jp

Hee Yong Youn
Sungkyunkwan University
Suwon, 440-746 South Korea
E-mail: youn@ece.skku.ac.kr

Library of Congress Control Number: 2007938892

CR Subject Classification (1998): C.2, C.3, C.5.3, D.2, D.4, H.4, H.5, K.4, J.7

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743
ISBN-10 3-540-76771-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-76771-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12191024 06/3180 5 4 3 2 1 0

Preface

We cordially welcome you to the proceedings of the 2007 International Symposium on Ubiquitous Computing Systems (UCS) held at Akihabara, Tokyo, Japan. UCS has become a symposium for the dissemination of state-of-the-art research and engineering practices in ubiquitous computing with particular emphasis on systems and software. UCS 2007 was the fourth of this series of international symposia. This was the year for the Next Generation Network (NGN) to be commercially launched so that the Internet could become the infrastructure for communications and computing substituting the NGN in telephone networks. The maturity of the Internet encourages the research and development of the next computing systems, where ubiquitous computing is recognized as one of the most promising computing paradigms.

This symposium was organized by IPSJ SIGUBI, IEICE USN and UCN, Korea, in cooperation with the IEEE Tokyo Section, IPSJ SIGEMB, IEICE Smart Info-media Systems Technical Group, and Human Interface Society. It was also sponsored by Ubiquitous Networking Forum, Nokia, NTT, SCAT, IISF and TAF.

This year, we had 96 submissions from 18 countries. The Program Committee reviewed all the papers carefully and then selected 16 full papers and 8 short papers. The very low acceptance rate of about 22.6% clearly demonstrates the high quality of the conference, and this tradition will continue in the upcoming conferences. Two distinguished speakers were also invited for keynote speeches, who enlightened the audience on ubiquitous computing and applications.

The high-quality technical program of UCS 2007 depends very much on the precise and stringent review process. The Technical Program Committee consisted of 62 excellent members. Most reviews ware almost of journal paper review quality, and the paper selection was very serious and strict.

Along with the symposium, we also offered a workshop and a poster session. This was for providing the researchers and engineers with opportunities to share their ideas and solutions for a broad range of challenging problems in this area.

As General Co-chairs and Program Co-chairs, we would like to express our appreciation to all the volunteers working hard for the symposium: members of the Steering Committee, the Organizing Committee, the Program Committee, the authors and the reviewers. Special thanks go to Yoshito Tobe and Jin Nakazawa.

November 2007

Haruhisa Ichikawa
We-Duke Cho
Ichiro Satoh
Hee Yong Youn

Organization

Executive Committee

General Co-chairs	Haruhisa Ichikawa (NTT Corporation, Japan)
	We-Duke Cho (UCN, Ajou University, Korea)
Program Co-chairs	Ichiro Satoh (National Institute of Informatics, Japan)
	Hee Yong Youn (Sungkyunkwan University, Korea)
Local Arrangements Chair	Jin Nakazawa (Keio University, Japan)
Treasurer	Masashi Toda (Future University-Hakodate, Japan)
Publication Co-chairs	Kazunori Takashio (Keio University, Japan)
	Marc Langheinrich (ETH Zurich, Switzerland)
	Young Ik Eom (Sungkyunkwan University, Korea)
Publicity Co-chairs	Sozo Inoue (Kyushu University, Japan)
	Matthias Kranz (Technische Universität Braunschweig, Germany)
	Moon Hyun Kim (Sungkyunkwan University, Korea)
Industrial Liaison Chair	Yoshito Tobe (Tokyo Denki University, Japan)
Workshops Chair	Masayoshi Ohashi (KDDI Corporation, Japan)
Posters Chair	Masateru Minami (Shibaura Institute of Technology, Japan)
	Charles Perkins (Nokia, USA)
Demonstrations Chair	Kazushige Ouchi (Toshiba Corporation, Japan)
Secretariat	Kaori Fujinami (Tokyo University of Agriculture and Technology, Japan)
	Masayasu Yamaguchi (NTT Corporation, Japan)
Steering Committee	Tomonori Aoyama (Keio University, Japan)
	We-Duke Cho (UCN, Korea)
	Hyeon-Kon Kim (NCA, Korea)
	Tei-Wei Kuo (National Taiwan University, Taiwan)
	Hideyuki Nakashima (Future University-Hakodate, Japan)
	Joseph Kee-Yin Ng (Hong Kong Baptist University, Hong Kong)
	Ramakoti Sadananda (Rangsit University, Thailand)
	Sang-Chul Shin (NCA, Korea)
	Hideyuki Tokuda (Keio University, Japan)

Program Committee

Jörg Baus (Saarland University, Germany)
Christian Becker (Universität Mannheim, Germany)
Michael Beigl (Technische Universität Braunschweig, Germany)
Roy Campbell (University of Illinois at Urbana-Champaign, USA)
K. Selcuk Candan (Arizona State University, USA)
Diane Cook (The University of Texas at Arlington, USA)
Antonio Coronato (ICAR-CNR, Italy)
Christian Decker (University of Karlsruhe, Germany)
Alois Ferscha (University of Linz, Austria)
Kaori Fujinami (Tokyo University of Agriculture and Technology, Japan)
Hani Hagras (University of Essex, UK)
Mikio Hasegawa (Tokyo University of Science, Japan)
Lars Erik Holmquist (Viktoria Institute, Sweden)
Liviu Iftode (Rutgers University, USA)
Michita Imai (Keio University, Japan)
Sozo Inoue (Kyushu University, Japan)
Susumu Ishihara (Shizuoka University, Japan)
Jihong Jeung (Kookmin University, Korea)
Yoshihiro Kawahara (The University of Tokyo, Japan)
Takahiro Kawamura (TOSHIBA Corp., Japan)
Hideki Koike (University of Electro-Communications, Japan)
Mohan Kumar (The University of Texas at Arlington, USA)
Koichi Kurumatani (AIST, Japan)
Fusako Kusunoki (Tama Art University, Japan)
Marc Langheinrich (ETH Zurich, Switzerland)
Frederic Le Mouel (INRIA / INSA Lyon, France)
Dongman Lee (Information and Communications University, Korea)
Wonjun Lee (Korea University, Korea)
Claudia Linnhoff-Popien (University of Munich, Germany)
Cristina Videira Lopes (University of California Irvine, USA)
Javier Lopez-Munoz (University of Malaga, Spain)
Paul Lukowicz (University of Passau, Germany)
Fabio Martinelli (CNR-IIT, Italy)
Kazuhiro Minami (University of Illinois at Urbana-Champaign, USA)
Masateru Minami (Shibaura Institute of Technology, Japan)
Hiroyuki Morikawa (The University of Tokyo, Japan)
Jin Nakazawa (Keio University, Japan)
Sotiris Nikoletseas (University of Patras and Computer Technology Institute, Greece)
Kazushi Nishimoto (JAIST, Japan)
Paddy Nixon (University College Dublin, Ireland)
Melek Önen (Institut EURECOM, France)

Kazushige Ouchi (Toshiba Corporation, Japan)
Susanna Pirttikangas (University of Oulu, Finland)
Jukka Riekki (University of Oulu, Finland)
Yves Roudier (Institut EURECOM, France)
Umar Saif (MIT, USA)
Aruna Seneviratne (University of New South Wales, Australia)
Mukesh Singhal (University of Kentucky, USA)
Joshua Smith (Intel Research Seattle, USA)
Toshio Soumiya (FUJITSU LABS. LTD., Japan)
Yasuyuki Sumi (Kyoto University, Japan)
Yasuo Tan (JAIST, Japan)
Hiroyuki Tarumi (Kagawa University, Japan)
Tsutomu Terada (Osaka University, Japan)
Yoshito Tobe (Tokyo Denki University, Japan)
Tonouchi Toshio (NEC, Japan)
Anand Tripathi (University of Minnesota, USA)
Kristof Van Laerhoven (Darmstadt University of Technology, Germany)
Xin Wang (Stony Brook University, USA)
Steven Willmott (Universitat Politecnica de Catalunya, Spain)
Woontack Woo (GIST, Korea)
Keiichi Yasumoto (Nara Institute of Science and Technology, Japan)

Reviewers

Ioannis Aekaterinidis (University of Patras, Greece)
Martin Berchtold (University of Karlsruhe, Germany)
Shinsuke Hara (Osaka City University, Japan)
Mattias Jacobsson (Viktoria Institute, Sweden)
Antonis Kalis (AIT - Athens Information Technology, Greece)
Athanasios Kinalis (University of Patras and Computer Technology Institute, Greece)
Tomoya Kitani (Nara Institute of Science and Technology, Japan)
Mihai Marin-Perianu (University of Twente, The Netherlands)
Nishkam Ravi (Rutgers University, USA)
Till Riedel (TecO & University of Karlsruhe, Germany)
Mattias Rost (Viktoria Institute, Sweden)
Gregor Schiele (University of Mannheim, Germany)
Pravin Shankar (Rutgers University, USA)
Naoki Shibata (Shiga University, Japan)
Kenichi Takizawa (National Institute of Information and Communications Technology, Japan)
Morihiko Tamai (Nara Institute of Science and Technology, Japan)
Tadahiro Wada (Shizuoka University, Japan)

Sponsoring Institutions

Ubiquitous Networking Forum
Nokia
NTT
Support Center for Advanced Telecommunications Technology Research, Foundation
International Information Science Foundation
The Telecommunications Advancement Foundation

Supporting Societies

UCS2007 was organized by IPSJ SIGUBI, IEICE USN, and UCN (Korea) in cooperation with the IEEE Tokyo Section, IPSJ SIGEMB, IEICE Smart Infomedia Systems Technical Group, and Human Interface Society.

Table of Contents

UCS2007

Security and Privacy

Context Awareness

Sensing Systems and Sensor Network

Middleware

Modeling and Social Aspects

Smart Devices

Network

RFID Privacy Using Spatially Distributed Shared Secrets

Marc Langheinrich[1] and Remo Marti[2]

[1] Inst. for Pervasive Computing
ETH Zurich, 8092 Zurich, Switzerland
langheinrich@inf.ethz.ch
[2] Ergon Informatik AG
8008 Zurich, Switzerland
remo.marti@ergon.ch

Abstract. Many of today's proposed RFID privacy schemes rely on the encryption of tag IDs with user-chosen keys. However, password management quickly becomes a bottleneck in such proposals, rendering them infeasible in situations where tagged items are repeatedly exchanged in informal (i.e., personal) situations, in particular outside industrial supply-chains or supermarket checkout lanes. An alternative to explicit access control management are RFID privacy systems that provides access to tag IDs *over time*, i.e., only after prolonged and detailed reading of an item. Such themes can minimize the risk of unwanted exposure through accidental read-outs, or offer protection during brief encounters with strangers. This paper describes a spatially distributed ID-disclosure scheme that uses a (potentially large) set of miniature RFID tags to distribute the true ID of an item across the entire product surface. We introduce the underlying mechanism of our spatially distributed RFID privacy system and report on initial performance results.

1 Introduction

Today's best protection from unwanted RFID readouts is to completely disable the tag – either by executing a *kill-command* [1] at checkout that renders the tag silent to all reader requests, or by physically clipping the tag antenna [2]. In the future, however, additional services such as warranty returns and repairs, smart laundry machines, automated inventories, or electronically augmented everyday appliances [3] may offer tangible consumer benefits for RFID-tagged items beyond the supply chain, which would force consumers to choose between these novel services and their privacy.

Short of killing tags completely, so far only password-based methods have seemed feasible for protecting RFID tags from unwanted readouts [4,5,6].[1] While their general principle is easy enough for implementation on a tiny RFID tag,

[1] An excellent overview of RFID privacy methods can be found in [7].

H. Ichikawa et al. (Eds.): UCS 2007, LNCS 4836, pp. 1–16, 2007.

the practical use of such schemes is often challenging. In order to facilitate the exchange, sale, or return of tagged items, all involved parties must own and operate reasonably sophisticated information infrastructures that can pass and receive the individual passwords for each tagged item. In principle, NFC-enabled smartphones could easily receive such passwords as an integral part of a mobile phone based payment procedure, but in reality, it will still take many years before a majority of shoppers will own, carry, and use such phones. Equally unlikely is the fast spread of corresponding NFC-enabled point-of-sales systems, as retail-chains would need to add costly upgrades to their systems without clear benefits to their bottom line, while smaller outlets such as kiosks or newsstands would need to upgrade their entire procurement, inventory, and sales operations at costs that could easily dwarf their yearly profits.

A number of password-less alternatives for RFID privacy have since been proposed, such as Juels et al.'s *blocker tag* [8], where a specifically engineered RFID tag causes signal collisions with all regular RFID tags in its vicinity, effectively preventing their readout. While simple in use, the need for carrying a blocker tag puts the burden of privacy protection on the user, who looses this protection should she forget to carry it. Blocker tags are also subject to the same reliability concerns as ordinary tags, i.e., a suboptimal position in the reader's field might not sufficiently power the tag, thus allowing full access to all other RFID tags. In order to limit the types of deactivated tags, e.g., to only those belonging to the user, a password management scheme is again needed that allows configuring regular RFID tags to be protected by a particular blocker tag. Fishkin et al. [9] instead propose a simple but intuitive *distance-based* access control scheme, where tags reply with different levels of detail depending on their distance to the reader. Apart from the increased costs for the required on-tag circuitry to reliably detect signal strength, distance-based authentication might not always yield the desired functionality, e.g., when passing narrow passageways or small store entrances.

In an earlier paper [10], we have proposed a third alternative, called a *Shamir Tag*, which neither require costly password management nor error-prone distance measurements. Using the cryptographic principle of *secret shares* [11], Shamir Tags yield virtually no information to casual "hit-and-run" attackers, but only reveal their true ID after continuous and undisturbed reading from up-close – something that can hardly go unnoticed by an item's owner. At the same time, however, the system allows tag owners to use *caching* for speeding-up this process, effectively preserving instant item identification in home-automation or supply-chain applications.

In order to prevent secret long-range scanning with powerful antennas, Shamir Tags' antennas will need to be constructed with limited read-out ranges, potentially yielding only a few centimeters of distance for systems operating within the allowed power levels. This in turn might complicate the readout process also for tag owners, as tagged items need to be positioned more carefully with respect to the antenna. This paper presents a *multi-tag* extension to Shamir Tags, allowing the use of dozens, if not hundreds of miniature tags on the same product,

thus alleviating positioning problems without the need for increased read ranges. Our approach is based on the idea of *super-distributed RFID tag-infrastructures* (SDRI) [12], where tiny RFID chips are brought out in large numbers, e.g., mixed into wall paint, woven into carpets or clothing, or sprinkled into an item's plastic casing. Thus, instead of having a single RFID tag per item, we envision items that feature several hundreds of tags, with the item's ID being *spread out* across all tags. Given appropriate communication protocols and antenna sizes, reading that many tags at once will be infeasible, instead requiring readers to scan small areas sequentially. While clearly not yet a reality, we believe that current trends in RFID miniaturization, such as Hitachi's μ-chip,[2] offer ample potential for actually deploying such simple but reliable RFID privacy systems in the future.

The remainder of this paper is structured as follows. Section 2 will briefly describe our previously proposed Shamir Tags and their underlying principles, Shamir's *secret sharing* scheme and *bit-throttling*, as well as outline a distributed, multi-tag variant. Section 3 then presents two extensions that we developed for using distributed Shamir Tags concurrently, i.e., in a multi-item scenario. Section 4 will briefly outline the prototype system we built for evaluating our approach, before we report on the results of initial experiments in section 5.

2 Shamir Tags

Shamir Tags use two principles to protect the true ID of an item (e.g., its EPC-code) [10]. Firstly, data readout is performed in two stages using a *bit-by-bit* strategy. Initially, a Shamir Tag discloses a small subset (e.g., 5%) of bits to a reader, which allows owners to quickly identify the entire bit-string from a small list (cache) of personal items. This is then followed by a steady "trickle" of bits that reveals the entire ID to the reader only after prolonged reading, e.g., several minutes. This allows anybody to eventually identify an item, yet forces them to stay close enough to the tag during the entire time. This process is called *bit-throttling*, and it makes tag-tracking difficult.

However, since industrial code-schemes are often heavily structured, even releasing only a few bits might already disclose sensitive data. E.g., an EPC-header featuring the combination `10` at the third and fourth position uniquely identifies items tagged by the U.S. Department of Defense [13]. To prevent such data disclosure, Shamir Tags are additionally *encoded* using *shared secrets*. The process of creating a shared secret basically re-encodes the tag's true ID into n seemingly unrelated numbers. Only by combining all n numbers, the original ID can be (trivially) reconstructed. Section 2.1 will give some more background information on this process – for now it suffices to know that this encoding step basically protects our Shamir Tag from inadvertently disclosing meaningful bits.

[2] Hitachi's current generation μ-chip has a size of less than 0.2 mm^2, its next generation will have only about 0.02 mm^2. Also see `www.hitachi.co.jp/Prod/mu-chip`

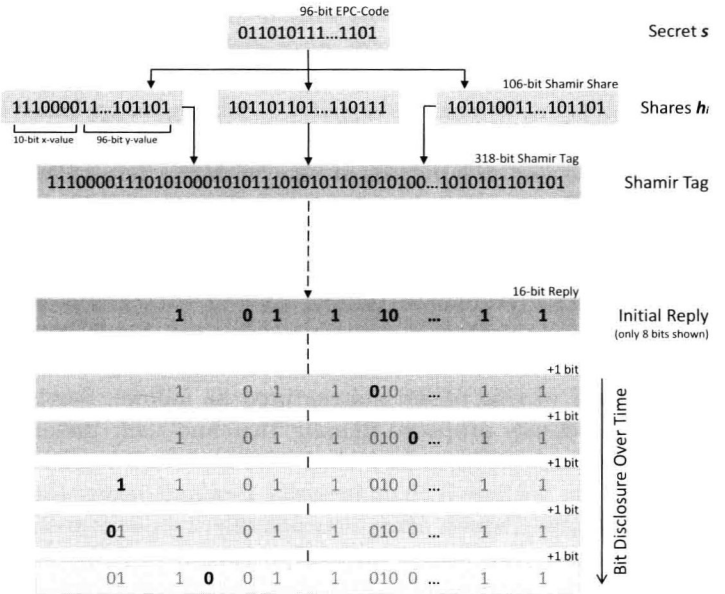

Fig. 1. *Principal Construction of a Shamir Tag* (from [10]). Based on the tag's "true" ID, e.g., its EPC-code, multiple Shamir shares are concatenated to form the tag's new ID, which is then stored on the tag. Upon reader inquiry, an initial set of random bits is released, with subsequent throttled single-bit releases.

Only after all bits have been read (which, due to bit-throttling, may take up to several minutes) they can be combined into the true ID.[3]

Figure 1 shows the principal construction of a Shamir Tag from a 96-bit EPC. In our previous work [10], we have shown that Shamir Tags provide an effective and cheap protection from unwanted and inadvertent tag readouts. Item owners can use simple caching strategies to ensure instantaneous identification of their own tags, while foreign readers will need to have continuous access to the tag for prolonged amounts of time, in order to read a sufficiently large percentage of bits from the tag that allows reconstructing the Shamir-encoded true ID. However, a critical factor of this protection is the effective read range of such tags – if the read range is too large, attackers can read out tags from several meters away whenever their owners are not moving fast enough, e.g., in public transport, or while waiting in line. Reducing the read range by limiting tag antenna sizes helps to prevent such attacks, yet at the same time complicates tag readout for legitimate owners, as they will also need to position their antennas very close to

[3] Note that if x bits are missing, rogue readers can of course try out all possible 2^x combinations to compute 2^x potential true IDs, and then use knowledge about valid EPC values (e.g., allowed manufacturer IDs, or known product IDs) to discard invalid IDs.

the tag. In industrial settings, or when the exact location of an embedded tag is not known, this might significantly hamper legitimate tag use.

Our solution to this is – as outlined in the introduction – straightforward: instead of using a single Shamir Tag with a reasonable antenna range that simplifies tag detection at the expense of long-range scanning protection, we use dozens, if not hundreds of miniature Shamir Tags, woven into the garment of clothing, or mixed into the plastic casing of products, that have a much shorter antenna range but which distribute the item's (protected) ID more or less evenly across the entire product surface. However, this approach offers new challenges for ID reconstruction, which are outlined in section 3 below. But first, we will briefly give some background on the construction of shared secrets using Shamir's scheme in the following section.

2.1 Shamir's Secret Sharing Scheme

In a secret sharing scheme, each participant receives a *share* that is a part of a secret. The secret can only be recovered if enough participants cooperate in recombining their shares. Schemes that allow a reconstruction of the secret with only t out of n participants involved are called *(t,n)-threshold schemes*. They fulfill the following two properties: Firstly, no subset of participants smaller than a threshold t can gain information on the secret s, even when cooperating with each other. Secondly, any subset equal to or larger than a threshold t can reconstruct the secret s at any time.

One of the most famous (t,n)-threshold schemes was introduced by Shamir in 1979 [11]. It is based on polynomials, and in particular on the observation that a polynomial of degree $t-1$ is defined by t coordinate-pairs (x_i, y_i). To encode a secret s for n participants with a threshold t, one chooses a random polynomial of degree $t-1$ that crosses the y-axis at s. The n participants are each given exactly one point on the polynomial's curve, thus allowing any t members to compute the exact polynomial and thus the y-intercept s.

The reconstruction of the secret is essentially a polynomial interpolation based on the *Lagrange* formula. Since only the y-intercept is of interest, it can be simplified to the following formula (with k being the number of tags read):[4]

$$s = q(0) = \sum_{i=1}^{k} y_i \prod_{1 \le j \le k, i \ne j} \frac{x_j}{x_j - x_i} \tag{1}$$

In practice, computing the secret s given large numbers of shares (e.g., thousands) quickly becomes infeasible. Calculations are therefore carried out in a finite field modulo p (written as $\mathbb{Z}_p$)[5], with p being a large prime number. Not only does this reduce the size of exponents, but it also removes the need for floating point operations (thus limiting numerical errors).

[4] Obviously, computing s with $k < t$ shares is not possible.

[5] $\mathbb{Z}_p$ designates the set $\{0, 1, ..., p-1\}$.

A comprehensive discussion of this topic is beyond the scope of this paper, but an excellent introduction, as well as efficient algorithms for solving (1) in $\mathbb{Z}_p$, can be found in [14]. Operating a secret sharing scheme within $\mathbb{Z}_p$ not only makes reconstruction of the secret s (e.g., its Electronic Product Code/EPC) feasible, but also helps with the practical problem of resolving multiple secrets concurrently. This will be described in section 3 below.

2.2 A Spatially Distributed Shamir Tag

A straightforward implementation of a distributed Shamir Tag would simply put the individual shares not just on a single tag, but distribute them among *multiple* tags on (or in) an item. As Shamir's scheme allows the reconstruction of the secret irrespective of the order of the shares, no special order would need to be observed when reading shares off the individual tags. Bit-throttling could also still be used, as each tag would choose a random temporary ID during readout, allowing a reader to group bits from the same share properly together. In order to make use of *caching* [10], however, bits would need to be continously numbered across all tags, in order to have a defined order. Note that this would *not* decrease the level of protection compared to a single Shamir Tag, as this simply orders the distributed bits just as in the non-distributed (i.e., single-tag) version – this would simply increase per-tag storage requirements, as each distributed share would need to also store its original position within the Shamir Tag.

By properly adjusting the threshold parameter t, defective or detuned tags could be tolerated. This also adds flexibility to the readout process, as only part of an item's surface would need to be scanned.[6] Just like in the single-tag case, a reader would gradually assemble the set of tags and their IDs in an item and repeatedly compute the secret s until a stable y-intercept had been found. Obviously, the overall disclosure-delay of a single tag could be significantly shortened, as the spatial distribution of the shares combined with the shortened read range of individual tags introduces an additional delay during readout.

3 Distributed Multi-item Identification

The approach described in section 2.2 above works well as long as only a single item/ID at a time needs to be reconstructed. However, once multiple items are within the reading range of the antenna, interpolation points from two or more polynomials would get mixed together that would never converge on a stable s value (nor yield multiple values for the different items). Since the Shamir scheme has no means of differentiating points from different polynomials, we will need to extend it if we want it to support decoding two or more secrets concurrently.

[6] The ratio between t and n could be adjusted individually for different products, depending on the envisioned privacy degree: a threshold t close to n requires many tags to be read, a small t allows the reconstruction of the secret s already with a small subset of tags.