Intactness Verification in Anonymous RFID Systems

Kai Bu[⋆], Jia Liu[∗], Bin Xiao[•], Xuan Liu[•], Shigeng Zhang[◦,∗]
[⋆]*College of Computer Science and Technology, Zhejiang University*
[∗]*State Key Laboratory for Novel Software Technology, Nanjing University*
[•]*Department of Computing, The Hong Kong Polytechnic University*
[◦]*School of Information Science and Engineering, Central South University*
Email: [⋆]kaibu@zju.edu.cn, [∗]liujia@smail.nju.edu.cn, [•]{csbxiao, csxuanliu}@comp.polyu.edu.hk, [◦]sgzhang@csu.edu.cn

***Abstract*—Radio-Frequency Identification (RFID) technology has fostered many object monitoring systems. Along with this trend, tagged objects' value and privacy become a primary concern. A corresponding important problem is to verify the intactness of a set of tagged objects without leaking tag identifiers (IDs). However, existing solutions necessitate the knowledge of tag IDs. Without tag IDs as *a priori*, this paper studies intactness verification in anonymous RFID systems. We identify three critical solution requirements, that is, deterministic verification, anonymity preservation, and scalability. We propose Cardiff and Divar, two crypto-free, lightweight protocols that isolate tag IDs from intactness verification and satisfy solution requirements. Cardiff explores tag cardinality as intactness proof while Divar leverages Direct-Sequence Spread Spectrum (DSSS) enabled RFID. Both analytical and simulation results demonstrate that Cardiff and Divar can satisfy the requirements of accuracy, privacy, and scalability.**

***Keywords*-Anonymous RFID system, Intactness verification, Missing-tag detection, Privacy, Security**

I. Introduction

Verifying the intactness of a set of tagged objects becomes imperative as Radio-Frequency Identification (RFID) technology pervades every corner of our lives. Nowadays, RFID is in ever-increasing use for monitoring various objects [1], [2]—as predicted by IDTechEx, over 1.35 billion tags were sold in 2013 [3]. Tagged objects under monitoring range from daily goods in groceries [4] to precious ones such as luxuries [5], weapons [6], and even new born babies [7]. For many RFID monitoring systems, especially when the objects under monitoring are valuable, losing tagged objects may not be affordable. Lost objects may be attributed to thieves or misbehaved system administrators (e.g., salesmen in supermarkets) [8]. One significant problem is thus to accurately, timely verify whether a set of tagged objects is *intact* (i.e., all tagged objects are present).

Established efforts to verify RFID intactness concentrate primarily on identifiable RFID systems with tag identifiers (IDs) as *a priori*. Their common intuition is that to know whether any tag is absent, we need first know which tags are supposed to be present. Normally, all tags whose IDs are registered on the server should be present to guarantee the intactness [9]. An intactness verification protocol can either 1) re-identify present tags through collecting their IDs and compare the collected IDs against the registered ones, or 2) directly access the registered IDs on the server and design efficient polling schemes [8]. Existing work adopts the latter toward scalability in large systems, falling into two categories—*probabilistic detection* that detects the event of absence with certain probability [8], [10], and *deterministic identification* that accurately pinpoints the IDs of absent tags if any [9], [11], [12].

This paper aims to verify the intactness of anonymous RFID systems without tag IDs as *a priori* (Section II). Since tag IDs usually contain object-specific information, we should prevent such information from leakage when it is privacy sensitive for tagged objects [5], [13], [14]. In an anonymous RFID system, RFID readers are not expected to collect IDs from tags or to access them on the server [15]–[18]. This way, tag IDs achieve anonymity and protect their associated privacy. Privacy of concern might be commercial secrecy in luxury monitoring systems [5] and military strength in weapon tracking systems [6]. Existing work on RFID intactness verification, however, requires known tag IDs [8]–[12] and therefore can hardly apply to anonymous RFID systems.

We propose two protocols, Cardiff and Divar, toward intactness verification in anonymous RFID systems (Section III and Section IV). Both Cardiff and Divar satisfy three critical requirements we identify for anonymous intactness verification—deterministic verification, anonymity preservation, and scalability. Moreover, they adopt crypto-free, lightweight designs in favor of low-cost, resource-constrained RFID tags. To this end, we isolate tag IDs from Cardiff and Divar's designs; we explore other feasible intactness proofs that are ID unrelated, effective for intactness verification, and efficient to obtain. Specifically, Cardiff adopts tag cardinality—the number of tags—as intactness proof. Motivated by the vision that tag cardinality may also be privacy sensitive, we further propose Divar by leveraging recent advances in Direct-Sequence Spread Spectrum (DSSS) enabled RFID [19]. DSSS allows a group of tags (each assigned with a spreading code) to simultaneously transmit and extracts from the aggregated transmission the information of which tags transmit what data [19]. We

[⋆]Corresponding Author: kaibu@zju.edu.cn

propose two lightweight adaptations of DSSS, spreading code reuse and tag cardinality disguise, toward security and scalability. Armed with adapted DSSS, Divar is faster and more secure than Cardiff at the expense of limited memory cost on tags.

The paper makes the following three contributions.

- *Present intactness verification in anonymous RFID systems without tag IDs as a priori.* We identify three critical solution requirements (i.e., deterministic verification, anonymity preservation, and scalability).
- *Explore ID unrelated intactness proofs—tag cardinality and aggregated DSSS code.* We propose a cardinality determination method that counts the exact number of tags without collecting their IDs. Moreover, we propose two lightweight adaptations of DSSS—spreading code reuse and tag cardinality disguise—toward better security and higher efficiency.
- *Propose two anonymous intactness verifications protocols, Cardiff and Divar.* Cardiff adopts the cardinality determination method while Divar adopts the adapted DSSS. Both analytical and simulation results demonstrate their satisfaction of solution requirements (Section V). At the expense of limited memory cost in DSSS-enabled RFID systems, Divar is significantly faster than Cardiff. For example, in a system of 50,000 tags, with costing each tag 96-bit memory space for storing a DSSS code, Divar increases time efficiency by over 96%.

II. Problem Statement and Related Work

In this section, we first formulate the intactness verification problem in anonymous RFID systems. We then review related work in identifiable RFID systems.

A. Problem Statement in Anonymous RFID Systems

The problem of concern is verifying the intactness of a set of tags in an anonymous RFID system. The tag-set intactness indicates a "full attendance" of tagged objects. The presence of all tagged objects is of paramount importance for most RFID monitoring systems, especially when the objects under monitoring are highly valuable. Just think of RFID systems that track weapons (e.g., [6]) and new born babies (e.g., [7]). It is too high a cost to lose any of them. Therefore, RFID monitoring systems are soliciting solutions that can accurately, efficiently verify the tag-set intactness. We concentrate primarily on finding such solutions for anonymous RFID systems, suggesting system administrators take certain timely actions in response to any violated intactness.

RFID system. We adopt a typical RFID system model comprising a server, a reader, and a set of tags. Findings based on this model have significantly benefited RFID research ranging from fundamentals (e.g., tag identification [20], [21] and cardinality estimation [22]) to applications (e.g., information collection [23] and tag searching [24]). Under such model, each tag is attached to an object. The granularity of object could be an individual item in supermarkets or a container of some items in container terminals. The number of tags is equal to that of objets under monitoring. Each tag has a unique ID, part or whole of which may represent the corresponding object's information such as origin, category, and price [17]. Tags are initially loaded with object related data, for example, at the source of RFID-enabled supply chains [4]. When tagged objects enter an RFID system, the reader collects tag data and further reports them to the server. The communication is either between reader and tags or between server and reader; tags usually do not directly communicate with the server.

Anonymous scenario. An anonymous RFID system is defined in terms of the anonymity of tag IDs—the reader can neither collect IDs from tags nor retrieve them from the server [15]–[18]. As aforementioned, tag IDs may represent category, price, or other information of tagged objects. Such information is privacy sensitive and should be protected. Take, for example, RFID-based weapon tracking systems [6]. Weapon categories directly reveal military strength the system can supply whereas military strength is highly confidential. Consider also, for instance, precious tagged objects (e.g., jewelry) under secret monitoring. Jewelry prices captured by wireless eavesdroppers may elicit stealings. Against such privacy leakage, transmitting tag IDs in plaintext is prohibitive in anonymous RFID systems. Transmitting encrypted IDs is neither always a wise choice for at least three reasons. First, most off-the-shelf low-cost tags cannot afford complex cryptography techniques [13]. Second, encryption and decryption induce complexity and overhead. Third, granting the reader access to tag IDs on the server risks potential privacy leakage and manipulation attacks [15]. Therefore, to preserve the anonymity of tag IDs, a strict requirement is to avoid transmitting IDs both between reader and tags and between server and reader.

Problem formulation. The intactness verification problem in an anonymous RFID system is to verify whether *all* registered tags (with IDs recorded on the server) are present in the system without the knowledge of tag IDs. A feasible solution generates a binary report, yes or no, and should satisfy three requirements, *deterministic verification*, *anonymity preservation*, and *scalability*.

Requirement 1: Deterministic verification. For anonymous RFID systems monitoring precious objects [6], [7], administrators must receive a timely, assertive alert when the intactness is violated. A desirable solution thus should not be probabilistic design with tolerated uncertainty. Uncertainties of common concern are *false negative* (i.e., an intactness violation is not detected) and *false positive* (i.e., an intact system is deemed violated). Our proposed solutions do not generate false negatives or false positives.

Requirement 2: Anonymity preservation. As aforemen-

tioned, a critical criterion for this requirement is to not transmit (plain or encrypted) tag IDs either between reader and tags or between server and reader. We observe that a stricter criterion—to isolate the knowledge of tag IDs from solutions—would be more robust against anonymity violation. The isolation criterion prevents tag IDs from leakage by intactness verification protocols under manipulation attacks [15]. Our proposed solutions meet the isolation criterion through not basing their designs on specific tag IDs.

Requirement 3: Scalability. As with designing protocols for other systems, scalability becomes a primary concern when system scale becomes large. A desirable scalability promises linear time complexity with respect to the system scale (i.e., the number of tags in an RFID system). RFID systems are craving protocol scalability more than ever—over 1.35 billion tags were sold in 2013 [3]! In favor of such an explosive growth of RFID, our protocols guarantee a linear time complexity of $\mathcal{O}(n)$ for verifying the intactness of a set of n tags. With a little expense of memory space on tags, our solutions can even guarantee a much faster verification with average verification time for each tag approaching 1-bit's transmission time, the minimum for a tag to claim its presence [23].

B. Related Work in Identifiable RFID Systems

Previous efforts to verify tag-set intactness are dedicated to identifiable RFID systems using the knowledge of tag IDs as intactness proof [8]–[12]. In terms of verification accuracy, they fall into two categories, probabilistic detection [8], [10] and deterministic identification [9], [11], [12].

Probabilistic detection aims to verify intactness as fast as possible but with false negatives, trading accuracy for efficiency. Such protocols apply to large RFID systems where losing some tagged objects is tolerable [8]. Tan et al. pioneered the first leap in protocol efficiency through leveraging collision arbitration. Given the knowledge of tag IDs, the reader can predict which tags contend for medium access in which time slot. If a tag is supposed to respond in a time slot but the reader receives none, the reader regards the tag as absent. Luo et al. generalized Tan's proposal to gain higher efficiency [10]. These protocols have false negatives because they limit the number of time slots toward fast detection. Our work differs from Tan's and Luo's in that we assume no knowledge of tag IDs for anonymity preservation, achieve deterministic detection for protecting precious objects, yet strive for high efficiency for large systems as well.

Deterministic identification verifies the presence of each tag, ascertaining not only whether some tags are absent but also which ones are. Similar to probabilistic detection, deterministic identification uses the knowledge of tag IDs to predict the distribution of tag responses and verifies a tag's presence according to whether it responds as expected. Li et al. pioneered identifying all absent tags [9]. They explored a suite of useful cases to improve time efficiency. For example, when two tags are supposed to simultaneously respond, both are absent if the reader receives no response. In follow-up, Zhang et al. studied deterministic identification in multi-reader systems [11] while Zheng and Li adopted compressive sensing to further improve efficiency [12]. Different from these protocols, our work targets anonymous RFID systems, assuming no knowledge of tag IDs yet guaranteeing deterministic verification.

III. CARDIFF: EXPLORING CARDINALITY DIFFERENCE

In this section, we present a cardinality difference based protocol, *Cardiff*. It uses tag cardinality rather than specific tag IDs as intactness proof. We design an anonymous cardinality determination method, upon which we build Cardiff and analyze its performance.

A. Cardiff Design

Cardiff uses the number n_{exp} of recorded tag IDs, that is, *expected tag cardinality*, as intactness proof. The key component is anonymously, accurately counting the *current tag cardinality*, that is, the number n_{cur} of tags currently present in the system. Cardiff claims an intactness if n_{exp} is equal to n_{cur} and triggers an intactness-violation alarm otherwise (i.e., $n_{\text{cur}} < n_{\text{exp}}$).

We first design the following framed Aloha [25] based anonymous cardinality determination method. *The principle is that since a singleton slot contains only one tag response, the reader increments current tag cardinality n_{cur} whenever it detects a singleton.* A 10-bit response with CRC embedded suffices for the reader to distinguish singleton from collision [22]. This way, Cardiff acquires singletons for counting n_{cur} without revealing tag IDs. Because a frame achieves the highest ratio of singleton slots when frame size is set as the number of tags to respond in the frame [25] and n_{cur} is yet to obtain, Cardiff initially sets $f = n_{\text{exp}}$. After detecting a singleton, the reader increments n_{cur} and signals the tag in this slot to keep silent until Cardiff terminates. If not all tags choose singleton slots, Cardiff hardly counts all tags in the first frame. The reader then issues a new frame with adjusted frame size $f = n_{\text{exp}} - n_{\text{cur}}$ and updates n_{cur} therein. Cardiff iterates the preceding operation until no collision occurs in a frame, that is, each tag has been hashed to a singleton slot and counted.

Figure 1 illustrates how Cardiff detects a violated intactness using cardinality determination. The server records six tags, among which T3 and T5 are absent. Expected tag cardinality $n_{\text{exp}} = 6$ rather than specific IDs serves as intactness proof. Cardiff takes two rounds to determine current tag cardinality n_{cur}. In the first round, Cardiff sets frame size $f = n_{\text{exp}} = 6$ and initiates $n_{\text{cur}} = 0$. In response to the query frame, T1 and T6 respectively choose the second and the fifth time slot while T2 and T4 simultaneously choose the fourth time slot. The frame of six time slots therefore

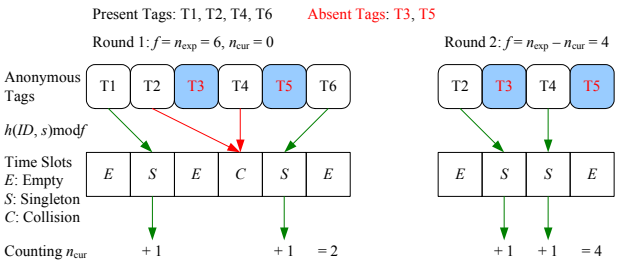

Figure 1. Anonymous cardinality determination based on framed Aloha. Tags transmit responses shorter than IDs yet long enough for the reader to distinguish singleton from collision. Cardiff detects the violated intactness by the evidence of $n_{\text{exp}} \neq n_{\text{cur}}$.

contains three empties, two singletons, and a collision. At the end of the first frame, Cardiff has updated n_{cur} to 2, the number of singletons in the frame. In the second round, Cardiff issues a frame of $n_{\text{exp}} - n_{\text{cur}} = 6 - 2 = 4$ time slots to count tags hashed into collision slots in the preceding frame. Both uncounted tags, T2 and T4, respond in singleton slots and are counted into n_{cur}, that is, $n_{\text{cur}} = 2+1+1 = 4$. Using the evidence of $n_{\text{exp}} \neq n_{\text{cur}}$, Cardiff successfully detects the intactness violation.

B. Performance Analysis

Cardiff satisfies the three solution requirements of deterministic verification, anonymity preservation, and scalability.

Accuracy. Cardiff delivers deterministic verification with neither false negatives nor false positives. Because the cardinality determination method accurately counts current tag cardinality n_{cur}, Cardiff can accurately verify whether or not n_{cur} conforms to expected tag cardinality n_{exp}. If $n_{\text{cur}} = n_{\text{exp}}$, Cardiff assures the intactness with no false positives. If $n_{\text{cur}} < n_{\text{exp}}$ (i.e., some tags are absent), Cardiff detects the intactness violation with no false negatives.

Anonymity preservation. Framed Aloha uses one-way hash functions; so even if an attacker could sniff the hash value of a tag ID (i.e., slot index in which a tag replies), it is hard for the attacker to infer the exact tag ID. A stubborn attacker may eavesdrop frame size f and random seed s for conducting exhaustive search over the entire ID space. For a 96-bit ID, there are 2^{96} possible IDs. Given frame size f, on average $\frac{2^{96}}{f}$ possible IDs fall into each time slot. When, for example, $f = 10{,}000$, we have $\frac{2^{96}}{f} = \frac{2^{96}}{10000} \approx 2^{82}$, which is too huge a number for the attacker to reverse hashing. The probability of correctly inferring an ID is nearly negligible.

Time efficiency. Cardiff achieves $\mathcal{O}(n)$ time complexity by inheriting linear time complexity from framed Aloha.

IV. Divar: Leveraging DSSS

In this section, we present a Direct-Sequence Spread Spectrum (DSSS) based intactness verification protocol for anon-ymous RFID systems, *Divar*. Allowing some participants (each assigned with a *spreading code*) to simultaneously transmit, DSSS can extract from the aggregated transmission the information of which participants transmit what data. DSSS thus promises a feature that verifies presence of participants by their transmissions. Divar writes spreading codes to tags by leveraging re-writable tag memory under Electronic Product Code Class-1 Generation-2 (C1G2) standard [26], [27]. Divar meets all solution requirements and is more efficient and secure than Cardiff at the expense of memory space on tags.

A. Motivation for Adopting DSSS

DSSS basics under RFID scenario. The reader and tags agree on a set of spreading codes each assigned to a tag. Tags use spreading codes to encode transmissions and the reader uses spreading codes to extract tag data from the aggregated transmission. We first introduce DSSS communication between the reader and a single tag. The tag encodes bit 1 by its spreading code and bit 0 by the complement of its spreading code. During transmission, DSSS modulates bit 1 with signal 1 and bit 0 with signal -1. The 1/-1 modulation sequence of a spreading code is its *bipolar notation*. Since the reader shares the same spreading code and thus its bipolar notation, the reader calculates normalized inner product of the bipolar notation and the received transmission—if the result is 1, the reader extracts bit 1 from the tag message; if the result is -1, the reader extracts bit 0 from the tag message.

When multiple tags communicate with the reader, DSSS requires their bipolar notations to be pairwise orthogonal[1]. This way, normalized inner products of different tags' bipolar notations are equal to zero. The multi-tag scenario thus boils down to a single tag scenario. Calculating the normalized inner product of each bipolar notation and an aggregated transmission, the reader can extract the information of which tag transmits what data (i.e., bit 1, bit 0, or neither). DSSS-friendly RFID systems have been engineered [19] and re-writable tag memory has been leveraged [27]. We would like to appreciate the established engineering efforts and concentrate more on how to build Divar upon them.

Limitations of adopting conventional DSSS. The *aggregated bipolar notation* by superimposing all tags' bipolar notations can be used as intactness proof. Suppose each tag transmits bit 1 with modulated signal equal to its bipolar notation. The reader can verify tag intactness through simply comparing the received transmission and the aggregated bipolar notation—intact if they match and not otherwise. We, however, observe that directly applying conventional DSSS has the following limitations in security and efficiency.

- *Tag cardinality inference.* A number l of 1's or -1's support up to l pairwise orthogonal bipolar notations [28]. For tag-memory efficiency, the system would write as short spreading codes to tags as sufficient for supporting their DSSS communications. That is, the

[1]We assume that the DSSS-enabled RFID system adopts algorithms like Hadamard matrix construction [28] for generating pairwise orthogonal bipolar notations.

number of tags is likely very close to or even equal to l. An attacker can thus infer tag cardinality and associated privacy through eavesdropping.

- *Lack of scalability and practicability in large systems.* As aforementioned, spreading codes of length l can support at most l tags to simultaneously transmit. For large systems accommodating tens of thousands of tags, it is impractical to load such long spreading codes to tags. We need adapt DSSS to large systems.

B. Adapting DSSS

We propose two lightweight adaptations of DSSS, *spreading code reuse* and *tag cardinality disguise*, toward more efficient and secure intactness verification in large systems.

Spreading code reuse prefixes each spreading code with a *group ID*. Scheduling tags in different groups to nonsimultaneously transmit, adapted DSSS reuses the same set of spreading codes for all groups. Consider l_{g}-bit group ID and l_{s}-bit spreading code. With such $(l_{\mathrm{g}}+l_{\mathrm{s}})$-bit code, adapted DSSS supports up to $2^{l_{\mathrm{g}}} \times l_{\mathrm{s}}$ tags whereas conventional DSSS only up to $l_{\mathrm{g}}+l_{\mathrm{s}}$. The increase of supporting tag cardinality by adapted DSSS is nearly base-2 exponential with respect to length l_{g} of group ID. Spreading code reuse thus empowers adapted DSSS to support large systems with affordable memory overhead.

Tag cardinality disguise intentionally lowers the utilization rate of group ID. When we set the utilization rate as 1 (i.e., using l_{g} bits to support $2^{l_{\mathrm{g}}}$ groups of tags), the reader will initiate $2^{l_{\mathrm{g}}}$ rounds of queries. An attacker may infer the number l_{g} of groups by eavesdropping $2^{l_{\mathrm{g}}}$ reader queries and the length $l_{\mathrm{g}}+l_{\mathrm{s}}$ of tag code by eavesdropping tag transmissions. The attacker then could infer tag cardinality as $2^{l_{\mathrm{g}}} \times l_{\mathrm{s}}$. To prevent such inference of tag cardinality, we use only $l_{\mathrm{g}}^{\mathrm{u}}$ out of l_{g} as utilized group ID, where $1 \le l_{\mathrm{g}}^{\mathrm{u}} < l_{\mathrm{g}}$. Let l denote the length of the entire tag code, that is, $l = l_{\mathrm{g}} + l_{\mathrm{s}}$. The expected tag cardinality n_{exp} is:

$$n_{\mathrm{exp}} = 2^{l_{\mathrm{g}}^{\mathrm{u}}} \times l_{\mathrm{s}} = 2^{l_{\mathrm{g}}^{\mathrm{u}}} \times (l - l_{\mathrm{g}}). \tag{1}$$

The inferred tag cardinality n_{infer} by an attacker is

$$n_{\mathrm{infer}} = 2^{l_{\mathrm{g}}^{\mathrm{u}}} \times (l - l_{\mathrm{g}}^{\mathrm{u}}). \tag{2}$$

Applying the condition of $l_{\mathrm{g}} > l_{\mathrm{g}}^{\mathrm{u}}$ to Equations 1 and 2, we have $n_{\mathrm{infer}} > n_{\mathrm{exp}}$. Therefore, lowering the utilization rate of group ID enlarges the attacker's inferred tag cardinality.

We now analyze optimal utilization rate r_{opt} for maximizing the difference n_{diff} between n_{infer} and n_{exp}. We develop the expression of n_{diff} as a function of utilization rate r:

$$n_{\mathrm{diff}} = n_{\mathrm{infer}} - n_{\mathrm{exp}} = 2^{r l_{\mathrm{g}}}(l_{\mathrm{g}} - r l_{\mathrm{g}}).$$

We obtain the value of r_{opt} by solving the following equation:

$$\frac{dn_{\mathrm{diff}}}{dr} = 2^{r l_{\mathrm{g}}}((\ln 2) l_{\mathrm{g}}(1-r) - 1) = 0.$$

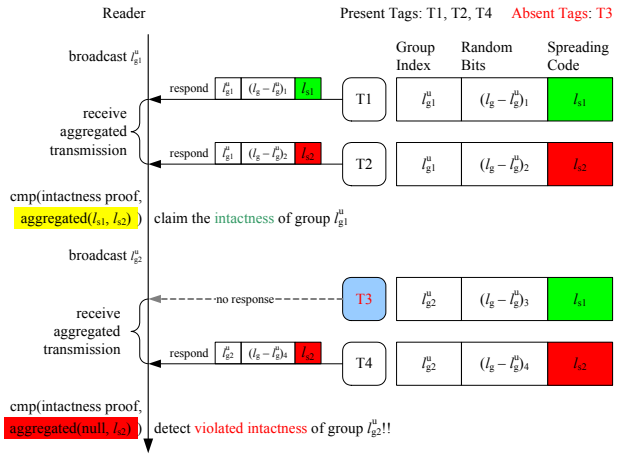

Figure 2. Divar execution instance for intactness verification in an DSSS-enabled anonymous RFID system. The intactness proof is the aggregated bipolar notation of spreading codes l_{s1} and l_{s2}. Divar detects the violated intactness by the absence of tag T3, because the received aggregated bipolar notation and the intactness proof mismatch.

Given the length l_{g} of group ID, we have

$$r_{\mathrm{opt}} = 1 - \frac{1}{l_{\mathrm{g}} \ln 2}. \tag{3}$$

C. Divar Design with Adapted DSSS

Divar design. Divar verifies the intactness of each DSSS group; only when all groups are intact can Divar claim the intactness of the entire system. A group uses the aggregated bipolar notation (of spreading codes) as intactness proof. Consider l-bit tag code, l_{g}-bit group ID, $l_{\mathrm{g}}^{\mathrm{u}}$-bit group index, and l_{s}-bit spreading code. Divar needs to verify the intactness of $2^{l_{\mathrm{g}}^{\mathrm{u}}}$ groups. To verify a group, the reader queries tags by broadcasting the group index. Upon receiving the query, a tag checks whether its group index matches the queried one. If yes, the tag responds to the reader with its l-bit tag code. Otherwise, the tag keeps silent. Tags do not reply with only l_{s}-bit spreading codes to avoid an attacker inferring tag cardinality by $2^{l_{\mathrm{g}}^{\mathrm{u}}} \times l_{\mathrm{s}}$. After receiving the aggregated transmission, the reader compares l_{s}-bit spreading code section with intactness proof. If they do not match, Divar detects violated intactness, triggers certain countermeasures, and terminates. Otherwise, Divar claims the intactness of the current group and continues to verify others.

Figure 2 illustrates how Divar detects a violated intactness (by tag T3) using adapted DSSS. The server records four tags divided into two groups with indices $l_{\mathrm{g1}}^{\mathrm{u}}$ and $l_{\mathrm{g2}}^{\mathrm{u}}$. Two reusable spreading codes, l_{s1} and l_{s2}, are used by both groups. The aggregated bipolar notation of l_{s1} and l_{s2} is used as intactness proof. The reader first queries the first group by broadcasting group index $l_{\mathrm{g1}}^{\mathrm{u}}$. Upon receiving the query, all tags compare their group indices with the queried one. T1, T2 pass the comparison and respond to the reader with their tag codes. The reader compares the bipolar notation section of the aggregated transmission with intactness proof

and verifies that group $l^{\mathrm{u}}_{\mathrm{g}1}$ is intact. The reader then applies the preceding verification process to group $l^{\mathrm{u}}_{\mathrm{g}2}$. Since T3 is absent, the reader receives the bipolar notation of only spreading code $l_{\mathrm{s}2}$. Divar thus fails the comparison with intactness proof and detects the violated intactness.

Discussions of Divar configuration. We next discuss how Divar divides, assigns, and loads tag codes.

Tag code division. We suggest dividing tag codes according to whether a system has a fixed tag cardinality. *First*, systems with fixed tag cardinality are, for example, tracking tagged weapons [6], which may not be used for quite a long time. In such systems, given tag cardinality n_{exp} and a long enough tag code of l bits, we can determine group ID length l_{g} and group index length $l^{\mathrm{u}}_{\mathrm{g}}$ by solving

$$n_{\mathrm{exp}} = 2^{l^{\mathrm{u}}_{\mathrm{g}}} \times l_{\mathrm{s}} = 2^{r_{\mathrm{opt}} l_{\mathrm{g}}} \times (l - l_{\mathrm{g}}) = 2^{l_{\mathrm{g}} - \frac{1}{\ln 2}} \times (l - l_{\mathrm{g}}).$$

Second, systems with dynamic cardinality are, for example, monitoring supply chain components (e.g., warehouse, super market, retailing store) [4]. We assume that such systems are aware of their capacity of accommodating at most $n_{\max}$ tagged products. Divar then could configure a big enough l for supporting up to $n_{\max}$ tags and a certain l_{g} for disguising tag cardinality. It is, however, hard to choose $l^{\mathrm{u}}_{\mathrm{g}}$ for achieving r_{opt} due to varying tag cardinality.

Tag code assignment. As shown in Figure 2, the segment of $l_{\mathrm{g}} - l^{\mathrm{u}}_{\mathrm{g}}$ bits is set as random bits. This preventing the aggregated $(l_{\mathrm{g}} - l^{\mathrm{u}}_{\mathrm{g}})$-bit segment from revealing certain patterns. An attacker may exploit patterns of the $(l_{\mathrm{g}} - l^{\mathrm{u}}_{\mathrm{g}})$-bit segment to infer the value of $l_{\mathrm{g}} - l^{\mathrm{u}}_{\mathrm{g}}$ and $l_{\mathrm{s}} = l - l^{\mathrm{u}}_{\mathrm{g}} - (l_{\mathrm{g}} - l^{\mathrm{u}}_{\mathrm{g}}) = l - l_{\mathrm{g}}$. If this is the case, the attacker could further infer tag cardinality of $2^{l^{\mathrm{u}}_{\mathrm{g}}} \times l_{\mathrm{s}}$. The assignment of random bits prevents such type of tag cardinality inference.

Tag code loading. Toward a better Divar applicability, we suggest writing DSSS codes to tags while a system registers tagged objects. When tagged objects enter a system for the first time, the system usually scans all tags to collect and store tag data. After collecting data from a tag, the reader can further write back a tag code and superimpose its corresponding bipolar notation on intactness proof. Recent work leveraging re-writable tag memory has excelled in, for example, cloning attack detection [27]. When a tag leaves the system, the reader subtracts the tag's associated bipolar notation from intactness proof. The tag's DSSS code can be reused for incoming tags.

D. Performance Analysis

Divar satisfies the three performance requirements described in Section II-A, that is, deterministic verification, anonymity preservation, and scalability. Furthermore, Divar is more secure and efficient than Cardiff.

Accuracy. Divar performs deterministic verification with neither false negatives nor false positives. Divar writes to each tag a tag code. Bipolar notations of tag codes' spreading codes are mutually orthogonal. Divar uses the aggregated bipolar notation as intactness proof. When all tags are present, the received aggregated bipolar notation should be identical with intactness proof. Divar then claims the intactness with no false positives. On the other hand, when at least one tag is absent, the received aggregated bipolar notation must differ from intactness proof. Take the xth signal value of the aggregated bipolar notation for example. No matter the xth bit of the absent tag's spreading code corresponds to 1 or -1, the xth value of the aggregated bipolar notation will be subtracted by 1 or -1. In both cases, the aggregated bipolar notation differs from intactness proof. Divar thus detects the violated intactness with no false negatives. Furthermore, Divar is resistant to tag replacement attack because an attacker can hardly counterfeit the tag code of the tag it stoles. The attacker thus cannot replace some tag(s) without making the received aggregated bipolar notation contradict intactness proof.

Anonymity preservation. Better than Cardiff that lets tags decide when to respond using their IDs, Divar completely isolates tag IDs from intactness verification and preserves anonymity. In essence, Divar anonymizes tags by assigning them DSSS codes. We carefully choose DSSS codes for intactness verification against tag cardinality inference. DSSS codes hold no specific information related to tags (or tagged products). Divar thus leaves an attacker no chance of inferring tag IDs or their associated privacy.

Time efficiency. Divar achieves $\mathcal{O}(n)$ time complexity and is much more efficient toward 1-bit presence confirmation than Cardiff. Divar takes $2^{l^{\mathrm{u}}_{\mathrm{g}}}$ rounds to verify intactness. In each round, the reader transmits $l^{\mathrm{u}}_{\mathrm{g}}$ bits to query tags and tags of the same group simultaneously transmit l bits to respond. Let t_{q} and t_{r} respectively denote the time for query and the time for response. The time T_{Divar} for Divar verifying intactness is as the following:

$$T_{\mathrm{Divar}} = 2^{l^{\mathrm{u}}_{\mathrm{g}}} \times (t_{\mathrm{q}} + t_{\mathrm{r}}) = \frac{t_{\mathrm{q}} + t_{\mathrm{r}}}{l_{\mathrm{s}}} \times n_{\mathrm{exp}}. \tag{4}$$

V. Performance Evaluation

We evaluate the performance of Cardiff and Divar through simulations. Since all established efforts are dedicated to identifiable RFID systems with known tag IDs [8]–[12], we conduct simulations without comparing Divar or Cardiff with existing work. As specified in Section II-A, we expect an anonymous intactness verification protocol to satisfy three requirements, deterministic verification, anonymity preservation, and scalability. Cardiff and Divar's satisfaction of accuracy and privacy has been assured by the analytical results in Section III-B and Section IV-D. We through simulation evaluate their time efficiency under various scenarios.

A. Time Efficiency of Cardiff

Following the analysis in Section III-B, we measure the execution time of Cardiff by the number T_{Cardiff} of time slots. Moreover, for ease of evaluating the time complexity,

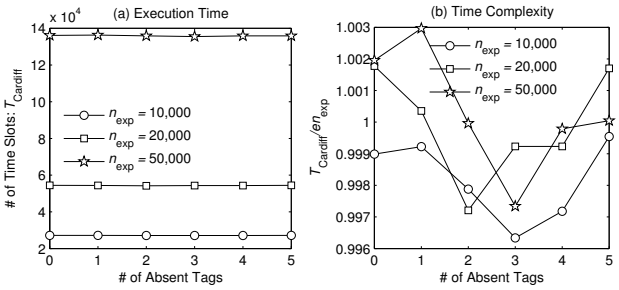

Figure 3. Cardiff's time efficiency with up to five absent tags.

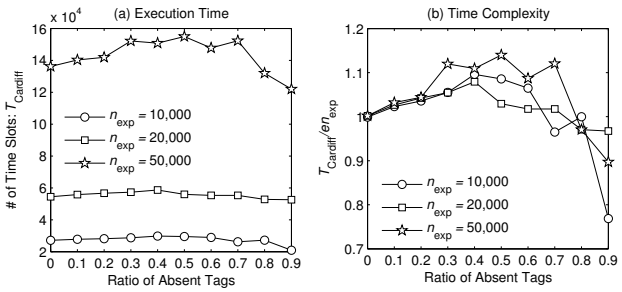

Figure 4. Cardiff's time efficiency with varying ratio of absent tags.

we report the ratio of T_{Cardiff} to en_{exp}. The expression en_{exp} represents the optimal number of time slots for framed Aloha to read n_{exp} tags. As the simulation results will show, T_{Cardiff} is under $1.2en_{\text{exp}}$ for $n_{\text{exp}} \leq 50{,}000$ with a various number of absent tags. Cardiff thus delivers a linear time complexity and is scalable for large RFID systems.

We first evaluate Cardiff's time efficiency when there are zero or only several absent tags. When no tag is absent, we expect T_{Cardiff} to approximate en_{exp}, which is the optimal number for framed Aloha to read n_{exp} tags. When only several tags are absent, we are interested in to what extent the execution time varies. Figure 3(a) reports Cardiff's execution time in terms of the number T_{Cardiff} of time slots when there are zero to five absent tags. Given a certain number of absent tags, T_{Cardiff} increases with system scale n_{exp}. The absence of several tags does not make the execution time fluctuate. As shown in Figure 3(b) with n_{exp} instances of 10,000, 20,000, and 50,000, when there is no absent tags, $T_{\text{Cardiff}}/en_{\text{exp}}$ ranges from 0.999 to 1.002; when the number of absent tags ranges from one to five, $T_{\text{Cardiff}}/en_{\text{exp}}$ ranges from 0.996 to 1.003.

We further evaluate how Cardiff's time efficiency varies with the ratio of absent tags. Figure 4(a) reports T_{Cardiff} under varying n_{exp} and absence ratio. Given a certain ratio of absent tags, T_{Cardiff} increases with system scale. The larger the system scale, the more fluctuations T_{Cardiff} experiences across different absence ratio. Figure 4(b) plots $T_{\text{Cardiff}}/en_{\text{exp}}$ to better demonstrate the variation amplitude and time complexity. When system scale is as high as 50,000, $T_{\text{Cardiff}}/en_{\text{exp}}$ is less than 1.2 under varying absence ratio.

In summary, Cardiff is scalable for large RFID systems. When a system accommodates up to 50,000 tags, the number of time slots for Cardiff to verify tag intactness is less than 1.2 times the optimal number of time slots for framed Aloha to read all tags.

B. Time-Efficiency Comparison of Divar and Cardiff

We further evaluate the time-efficiency improvement of Divar over Cardiff. The simulated large RFID system comprises 50,000 tags each with a 96-bit ID. Per Philips I-Code specification [29], a reader takes 0.8 ms to detect a singleton or collision and 2.4 ms to transmit a 96-bit tag ID [9]. For ease of measuring Divar's execution time, we assign a 96-bit DSSS code to each tag. Moreover, since a 10-bit string is sufficient for the reader to detect a collision [22], we assign the first 10 bits of each DSSS code as the group ID. Thus, we can approximate the transmission time of a group ID to 0.8 ms and that of a DSSS code to 2.4 ms. Under such configuration, we evaluate the time-efficiency gain by Divar costing each tag 96-bit memory space.

Figure 5 demonstrates the time-efficiency improvement of Divar over Cardiff. Figure 5(a) compares the execution time of Divar with that of Cardiff. We have two observations. First, Divar is more time-efficient than Cardiff. When, for example, there is no absent tag, Cardiff takes 108.9 seconds to verify the intactness of 50,000 tags whereas Divar takes only 3.3 seconds. Second, Divar has constant execution time regardless of the ratio of absent tags. This is because the execution time of Divar consists of the transmission time of group IDs and that of DSSS codes—given group IDs and DSSS with certain lengths, Divar yields constant execution time no matter how many tags are assigned the DSSS codes (Section IV-D). In fact, the simulated Divar instance can support up to $2^{10} \times (96 - 10) = 88{,}064$ tags. Divar thus holds the same execution time of 3.3 seconds as the system scale increases to 88,064 whereas the execution time of Cardiff linearly increases with the system scale. This further demonstrates Divar's sweet spot of protecting tag cardinality.

Figure 5(b) shows that Divar increases time efficiency by over 96% in comparison with Cardiff in the simulated system with 50,000 tags. We therefore believe that when a limited memory space overhead is affordable, Divar is more favorable than Cardiff in large RFID systems.

VI. Conclusion

We have studied intactness verification in anonymous RFID systems. Different from existing solutions that rely on the knowledge of tag IDs, we verify RFID intactness without tag IDs as *a priori*. Specifically, we propose Cardiff and Divar, two crypto-free and lightweight protocols by isolating tag IDs from intactness verification. To achieve Cardiff and Divar, we propose a series of methods such as anonymous cardinality determination, spreading code reuse, and tag cardinality disguise. Armed with these methods, both Cardiff and Divar satisfy solution requirements of accuracy,

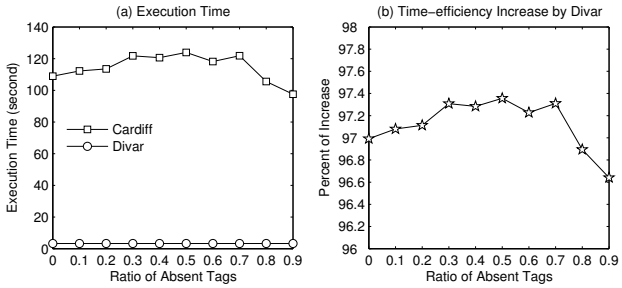

Figure 5. Time-efficiency comparison of Divar and Cardiff.

privacy, and scalability we identified for anonymous intactness verification. We demonstrate their performance through analytical and simulation results. We believe that Cardiff and Divar can benefit anonymous RFID systems with accurate, timely object-absence detection yet without compromising their privacy.

ACKNOWLEDGMENT

This work is supported in part by the Fundamental Research Funds for the Central Universities under Grant No. 2014QNA5012 and the National Science Foundation of China under Grant No. 61402404, 61103203, and 61373181. The authors would also like to sincerely thank IEEE ICPADS 2014 chairs and reviewers for their helpful feedback.

REFERENCES

[1] Z. Li, H. Shen, and B. Alsaify, "Integrating RFID with wireless sensor networks for inhabitant, environment and health monitoring," in *IEEE ICPADS*, 2008, pp. 639–646.

[2] T. A. Rahman, S. K. A. Rahim, *et al.*, "RFID vehicle plate number (e-plate) for tracking and management system," in *IEEE ICPADS*, 2013, pp. 611–616.

[3] RFID Market Reaches $7.67 Billion in 2012, http://bit.ly/QfTBNM.

[4] D. Delen, B. Hardgrave, and R. Sharda, "RFID for better supply-chain management through enhanced information visibility," *Production and Operations Management*, vol. 16, no. 5, pp. 613–624, 2007.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "RFID privacy issues and technical challenges," *Communications of the ACM*, vol. 48, no. 9, pp. 66–71, 2005.

[6] R. Harris, "Feasibility of radio frequency identification (RFID) and item unique identification (iuid) in the marine corps small arms weapons tracking system," DTIC Document, Tech. Rep., 2008.

[7] RFID Baby Tagging Systems, http://www.harlandsimon.com/RF_Baby_Tagging.php.

[8] C. Tan, B. Sheng, and Q. Li, "How to monitor for missing RFID tags," in *IEEE ICDCS*, 2008, pp. 295–302.

[9] T. Li, S. Chen, and Y. Ling, "Identifying the missing tags in a large RFID system," in *ACM MobiHoc*, 2010, pp. 1–10.

[10] W. Luo, S. Chen, T. Li, and Y. Qiao, "Probabilistic missing-tag detection and energy-time tradeoff in large-scale RFID systems," in *ACM MobiHoc*, 2012, pp. 95–104.

[11] R. Zhang, Y. Liu, Y. Zhang, and J. Sun, "Fast identification of the missing tags in a large RFID system," in *IEEE SECON*, 2011, pp. 278–286.

[12] Y. Zheng and M. Li, "P-mti: Physical-layer missing tag identification via compressive sensing," in *IEEE INFOCOM*, 2013, pp. 941–949.

[13] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006.

[14] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification-free batch authentication for RFID tags," in *IEEE ICNP*, 2010, pp. 154–163.

[15] M. Kodialam, T. Nandagopal, and W. Lau, "Anonymous tracking using RFID tags," in *IEEE INFOCOM*, 2007, pp. 1217–1225.

[16] H. Han, B. Sheng, C. Tan, Q. Li, W. Mao, and S. Lu, "Counting RFID tags efficiently and anonymously," in *IEEE INFOCOM*, 2010, pp. 1–9.

[17] K. Bu, X. Liu, J. Luo, B. Xiao, and G. Wei, "Unreconciled collisions uncover cloning attacks in anonymous RFID systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 429–439, 2013.

[18] K. Bu, M. Xu, X. Liu, J. Luo, and S. Zhang, "Toward fast and deterministic clone detection for large anonymous RFID systems," in *IEEE MASS*, 2014.

[19] C. Dabas, M. Balhara, and J. Gupta, "Cdma based anti-collision deterministic algorithm for RFID tags," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 603–606, 2009.

[20] M. Shahzad and A. X. Liu, "Probabilistic optimal tree hopping for RFID identification," in *ACM SIGMETRICS*, 2013, pp. 293–304.

[21] X. Liu, S. Zhang, K. Bu, and B. Xiao, "Complete and fast unknown tag identification in large RFID systems," in *IEEE MASS*, 2012, pp. 47–55.

[22] M. Kodialam and T. Nandagopal, "Fast and reliable estimation schemes in RFID systems," in *ACM MobiCom*, 2006, pp. 322–333.

[23] S. Chen, M. Zhang, and B. Xiao, "Efficient information collection protocols for sensor-augmented RFID networks," in *IEEE INFOCOM*, 2011, pp. 3101–3109.

[24] Y. Zheng and M. Li, "Fast tag searching protocol for large-scale RFID systems," in *IEEE ICNP*, 2011, pp. 363–372.

[25] L. Roberts, "ALOHA packet system with and without slots and capture," *ACM SIGCOMM Computer Communication Review*, vol. 5, no. 2, pp. 28–42, 1975.

[26] EPC class-1 generation-2 RFID protocol V.1.0.9, http://www.epcglobalinc.org/home.

[27] D. Zanetti, S. Capkun, and A. Juels, "Tailing RFID tags for clone detection," in *NDSS*, 2013.

[28] R. R. Yarlagadda and J. E. Hershey, *Hadamard matrix analysis and synthesis*. Kluwer Academic Publishers, 1997.

[29] I-CODE Smart Label RFID Tags, http://www.semiconductors.philips.com/acrobat_download/other/identification/SL092030.pdf.