4-2009

Ensuring Dual Security Modes in RFID-Enabled Supply Chain Systems

Shaoying CAI
Singapore Management University, sycai@smu.edu.sg

Tieyan LI
Institute for Infocomm Research

Yingjiu LI
Singapore Management University, yjli@smu.edu.sg

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1007/978-3-642-00843-6_32

Ensuring Dual Security Modes in RFID-Enabled Supply Chain Systems

Shaoying Cai[1], Tieyan Li[2], Yingjiu Li[1], and Robert H. Deng[1]

[1] Singapore Management University, 80 Stamford Road, Singapore 178902
[2] Institute for Infocomm Research, 1 Fusionopolis Way, Singapore 138632
sycai@smu.edu.sg, litieyan@i2r.a-star.edu.sg,
yjli@smu.edu.sg, robertdeng@smu.eud.sg

Abstract. While RFID technology has greatly facilitated the supply chain management, designing a secure, visible, and efficient RFID-enabled supply chain system is still a challenge since the three equally important requirements (i.e., security, visibility, and efficiency) may conflict to each other. Few research works have been conducted to address these issues simultaneously. In this paper, we observe the different security requirements in RFID-enabled supply chain environments and differentiate the simplified model into two security levels. Accordingly, dual security modes are properly defined in our RFID setting. In the relatively secure environment, our system is set to the *weak security mode*, the tagged products can be processed in a highly efficient way. When in the *strong security mode*, our system guarantees a high level of security, while its efficiency is lower than that in the *weak security mode*. A set of RFID tag/reader protocols to facilitate the duel security modes are presented. Their security, visibility and efficiency are analyzed and compared with the relevant works.

1 Introduction

RFID systems consist of two main components: tags and readers. Tags are radio transponders attached to physical objects, while radio transceivers, or readers, query these tags for identifying information about the objects to which tags are attached. RFID technology, when combined with internet and networking technology, enables product information to be collected, integrated, shared, and queried at various levels (e.g., item, pallet, case, and container) in real time in a supply chain. RFID technology has been widely envisioned to have significant impact on the economy world-wide as an inevitable replacement of barcodes in the near future, which may facilitate the creation of secure, visible, and efficient supply chains. As a result, EPCglobal Network [2] is being formed to provide an open and standard interface to process RFID information in supply chain management.

The current EPCglobal Network standards depend entirely on honest supply chain partners to realize supply chain visibility. Few security mechanisms have been developed to ensure that the tracking services are confidential, verifiable,

and accountable in the presence of realistic and malicious attacks, especially those coming from corrupted supply chain partners. Most of RFID technologies have focused on protecting a single RFID channel [5, 6, 7, 8, 9, 10, 11] without considering the relationship among supply chain parties. Such techniques cannot be directly used to protect the sharing of information among supply chain parties.

We develop a new security solution for RFID-enabled supply chain systems. In our solution, even a valid supply chain party, if not authorized, cannot track RFID tags after the ownership handover of the tags to other supply chain parties. On the other hand, an authorized party can have full supply chain visibility to track a tagged item in a supply chain. A root secret, shared between a trusted authority and each tag, is used to guarantee the anti-track and track/visibility properties. To achieve better efficiency, we classify the supply chain environments into two security levels. In an environment where insiders or outsiders can actively interact with a tag for the purpose of tracking, we set the system to *strong security mode* so as to maintain high security. In an environment where active attacks are not possible (e.g., within the territory of a supply chain party), we can set the system to *weak security mode* to achieve high processing speed. We use a binary switch on the tag to control the security modes. A set of RFID tag/reader protocols like tag reading protocol, security mode switching protocol and secret updating protocol, to facilitate the duel security modes are presented. We analyze the schemes in terms of security, visibility and efficiency. At last, our solution is compared with the relevant works.

The rest of this paper is organized as follows. In Section 2, we introduce a simplified system model and architecture for RFID-enabled supply chains. In Section 3, we present our protocols to protect RFID-enabled supply chain systems. In Section 4, we analyze our protocols in terms of security, visibility, and efficiency. In Section 5, we discuss the related works. Finally, Section 6 concludes this paper.

2 Model

Assumptions. In this paper, we focus on the attacks conducted on the wireless communications between RFID readers and tags. The adversaries can be either supply chain outsiders or insiders (i.e., dishonest supply chain parties). The adversaries are assumed to have the power to listen in communication channels, counterfeit as a valid supply chain party, to initiate, delete, modify, or transfer messages between RFID tags and readers. We do not consider the physical attacks, denial of service attacks, and side-channel attacks. We further assume that the communications between a supply chain partner and its RFID readers, and the communications between supply chain parties are secure, which can be protected by standard security techniques without limitation of resources.

Requirements. As discussed in existing RFID literatures, common security requirements of RFID tags include unlinkability, confidentiality, etc, nonetheless, applying RFID tags in supply chain environments introduces some unique needs

such as supply chain visibility and extra efficiency. In the following, we list the details of the requirements for RFID system when deployed in the supply chain.

The security requirements of RFID-enabled supply chain are summarized in [12]. We increment the requirements to include forward and backward secrecy and de-synchronization resilience. The list of security requirements is given below: (i) Authoritative access: Only legitimate readers of an authorized party are allowed to identify and update a tag. (ii) Authenticity of tags: In a supply chain link, only legitimate RFID tags delivered by previous party will be accepted by the next party. (iii) Unlinkability: Weak unlinkability and strong unlinkability can be used to describe the security level of anti-tracking. Weak unlinkability requires that an unauthorized reader cannot link the responses of a tag interrogated before and after it is processed by an authorized party. Strong unlinkability requires that an unauthorized reader cannot link any two replies to the same tag. (iv) Forward and backward secrecy: If the communication between a tag and a party is compromised, it will not affect the security of the communication between the tag and any other party in the supply chain. (v) De-synchronization resilience: RFID communication protocol is resilient to the attacks that are targeted towards de-synchronizing a tag and a reader.

Besides security, supply chain visibility must be maintained in supply chain management. It means that the manager of the supply chain or any authorized party should be able to track the movement of RFID tags. The enhancement on supply chain visibility is the most attractive feature that RFID technology brings to the traditional supply chain management. It allows companies to track and monitor the progress of material flow without inefficient bar code scanning.

Due to mass product exchanging, the efficiency of RFID technology is crucial in supply chain management. Without incorporating security and visibility features, hundreds of read operations can be performed per second between a reader and tags. The processing speed should not be delayed by adding security and visibility features.

We stress that the three requirements (i.e., security, visibility, and efficiency) are equally important in supply chain environments. Our goal is to propose a practical solution for RFID-based supply chain systems under the three requirements with the lowest possible cost.

Architecture. Our solution involves four types of entities as shown in Figure 1: (i) a supply chain manager which is a trusted authority, denoted by TA; (ii) independent supply chain parties denoted by P_i; (iii) RFID readers inside a partner, which are collectively referred to as R_i controlled by its corresponding party P_i, and a back-end database referred to as D_i; (iv) RFID tags denoted by T_j.

The architecture we proposed is suitable for various types of supply chain structures [3] and compatible with contemporary EPCglobal network architecture [2]. In a third-party logistics (3PL) supply chain, TA can be the shipping company, which is specialized in handling the shipping issues in the supply chain. In the vendor managed inventory (VMI) supply chains, the vendor manages all the delivering of products; thus, it is straightforward for the vendor to take the role of TA. For the collaborative planning, forecasting, and replenishment

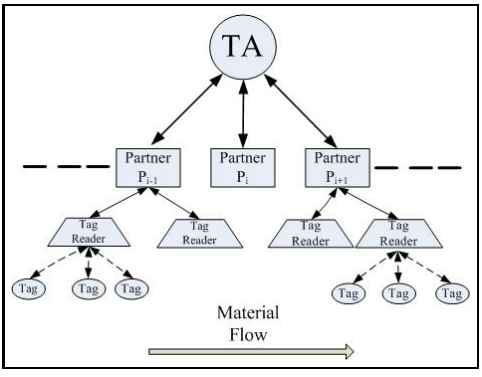

Fig. 1. A simplified RFID system architecture

(CPFR) supply chains, a supply chain hub is TA, which coordinates real-time sharing of supply chain information among supply chain parties. Finally, in supply network (SN), the situation is similar but more complex than in CPFR supply chains, where TA can be an existing supply chain hub or a dominant supply chain party.

3 Protocols

Since RFID tags will be used in vast numbers in supply chains, it is desired that the security design of the tags should be as cheap as possible. To achieve this goal, our protocols are designed to use passive tags that are equipped with pseudo-random number generators, standard XOR $\oplus$ and hash $H(\cdot)$ calculations.

A database is initialized by TA and sent to each supply chain party before the party can identify a batch of tags. With the help of the database, a supply chain party can switch security modes of RFID tags multiple times. Before a supply chain party sends a batch of tags to the next party in ownership handover, the current party needs to update the secret information in each tag. After ownership handover, the party can no longer identify the tags or track their movement.

3.1 Initialization

Tag initialization. Before the first supply chain party P_1 starts processing tagged products, TA will initiate three values (α_j, $\beta_{1\leftrightarrow j}$, *switch*) and embed them in each tag T_j in a secure manner.

- α_j is the tag root secret of length ℓ, which is fixed and shared between TA and the tag. The root secret is used to identify the tag uniquely.
- $\beta_{i\leftrightarrow j}$ is a temporary secret of length ℓ, which is shared between supply chain party P_i and tag T_j. The two parameters i and j of $\beta_{i\leftrightarrow j}$ denote the identity number of the supply chain party and the tag separately. This secret is initiated by TA to be $\beta_{1\leftrightarrow j}$. The temporal secret $\beta_{i\leftrightarrow j}$ will be updated by P_i to $\beta_{i+1\leftrightarrow j}$ before ownership handover to P_{i+1}.

– *switch* is a binary value used to indicate the security mode of a tag. This value is initiated to be 'on' for a strong security mode and it can be subsequently switched to 'off' for a weak security mode.

Database Initialization. Each party P_i maintains a database D_i in its local storage where each tuple in the database corresponds to a tag. D_i contains all RFID information with respect to a batch of tags except for tag root secrets α. D_i consists of five attributes $(\beta, x, p, s, switch)$, where $(\beta, switch)$ are defined the same as in tag initialization, (x, p, s) are defined below.

– Tag response x: Tag response to be received from the corresponding RFID tag (in weak security mode). When the tag is on strong security mode, the value of this attribute is set to NULL.
– Pointer p: An octet string containing an address where the business information relevant to the tag is stored. An alternative approach is to store information in this field directly. Obviously, it trades the storage cost for communication efficiency.
– Status s: Binary bit; $s = 1$ means that the corresponding RFID tag has been processed; otherwise not. We call an entry is unmarked if its value is zero.

Reader initialization. When the P_i is to handover a batch of tagged products to P_{i+1}, it updates the tag temporal secrets and informs TA that P_{i+1} is the next party. Then TA will distribute the database D_{i+1} to P_{i+1} through a secure channel (e.g., SSL).

3.2 Tag Reading

Upon receiving D_i from TA and the tagged products from P_{i-1}, supply chain partner P_i can read any tag T_j in either the *strong security mode* if *switch* is on or in the *weak security mode* if *switch* is off.

1. $R_i \rightarrow T_j$: r_1, where r_1 is a random number of length ℓ generated by the reader.
2. $T_j \rightarrow R_i$: On receiving r_1, the tag sends the reply (r_2, x) to the reader, where $x = H(r_1||r_2||\beta_{i \leftrightarrow j})$ and r_2 is a number of length ℓ. If the tag is in strong security mode, r_2 is a fresh random number generated by the tag; otherwise, $r_2 = 0$.

The tag reading protocol is illustrated in Figure 2. In the weak security mode, R_i can pre-compute the response of each tag x_j and store them in D_i. On receiving a response x , R_i identifies the tag if it can find a record $d_j = \langle \beta_{i \leftrightarrow j}, x_j, s_j, switch_j \rangle$ in D_i such that $x_j = x$ and $s_j = 0$. In the strong security mode, however, the response of each tag cannot be pre-computed due to the use of fresh tag random number; the value of x is set to NULL in each tuple of D_i in this case. Given a response (r_2, x), the reader identifies a tag by searching all of the unmarked($s = 0$) tuples in D_i until it finds a tuple d_j

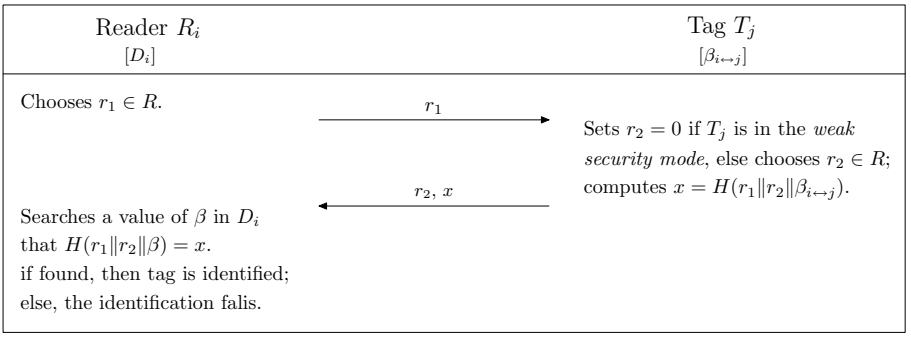

Fig. 2. Tag reading protocol

which satisfies $x = H(r_1||r_2||\beta_{i\leftrightarrow j})$. For each identified tag T_j, the reader sets its status $s_j = 1$. If p_j is not empty, the reader can also obtain relevant product information following the pointer p_j.

The above reading process can be performed multiple times by supply chain partner P_i if necessary.

3.3 Security Mode Switching

Once the party P_i receives D_i from TA, it can change the security mode of its tags in different environments. Although the strong security mode is secure against both active attacks and passive attacks, the RFID tags can be processed more efficiently in the weak security mode in an environment where the active attacks are impossible. We design a security mode switching protocol below.

1. $R_i \rightarrow T_j$: To update the security mode of tag T_j, the reader chooses a fresh random number r_3 and computes $a = \beta_{i\leftrightarrow j} \oplus r_3$, and $b = H(switch_0||a||r_3)$, where $switch_0$ is the new value of $switch$. The reader then sends the triple $(switch_0, a, b)$ to the tag.
2. $T_j \rightarrow R_i$: When tag T_j receives $(switch_0, a, b)$, it computes $r_3 = \beta_{i\leftrightarrow j} \oplus a$, and checks whether $b = H(switch_0||a||r_3)$ holds; if so, it updates $switch = switch_0$. After update of switch value, the tag T_j will send a confirmation (r_2, x) back to the reader, where r_2 is generated based on the switch value and $x = H(r_2||r_3||\beta_{i\leftrightarrow j})$.
3. R_i: Upon receiving (r_2, x), the reader R_i confirms the update of $switch$ by checking whether $x = H(r_2||r_3||\beta_{i\leftrightarrow j})$.

The protocol is also illustrated in Figure 3. Since a tag will send a confirmation to the reader after security mode update, any failure can be detected by the reader.

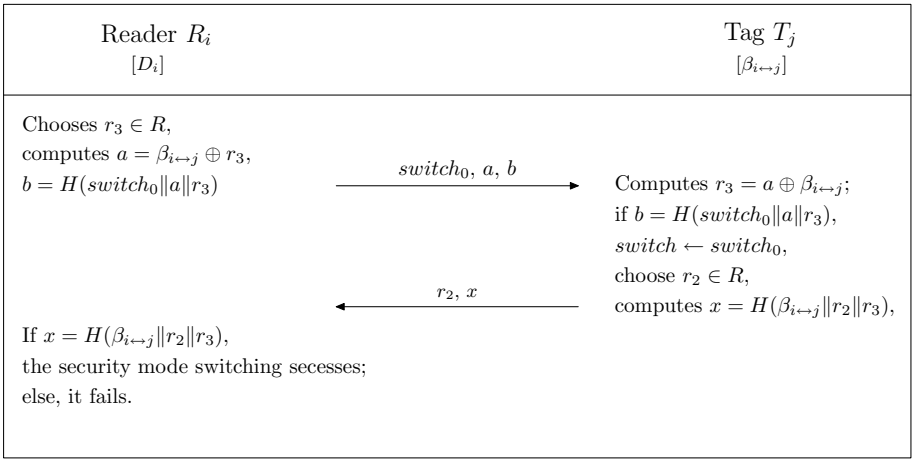

Fig. 3. Security mode switching protocol

3.4 Ownership Handover

Ownership handover is performed between two supply chain parties P_i and P_{i+1} with RFID tags in weak security mode without TA's active involvement. Before the handover, P_i will update the temporal secrets of its tags and informs TA, who will send D_{i+1} to P_{i+1} in a secure manner. Note that the database D_{i+1} is not needed during the handover process.

In order to prevent the tagged products from being tracked by party P_i after ownership handover, the tag's temporary secret must be updated from $\beta_{i\hookrightarrow j}$ to $\beta_{i+1\hookrightarrow j}$. This updating process is performed by P_i before handover. Without being appropriately updated, a tag will not be accepted by P_{i+1} in the handover process (see below). The update of tag temporal secrets guarantees that only P_{i+1} can access the tags although the update is conducted by P_i. This is under the assumption that P_i cannot get access to tag root secrets nor the new database D_{i+1}. The temporary secret updating protocol is shown in Figure 4. During ownership handover, both parties need to agree upon a list of the tagged products and report the agreed list to TA for supply chain visibility.

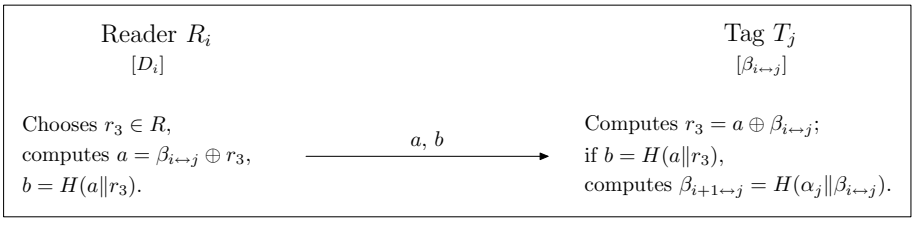

Fig. 4. Temporary secret updating protocol

During ownership handover, both parties need to agree upon a list of the tagged products and report the agreed list to TA for supply chain visibility.

1. For a batch of tagged products to be handed over to P_{i+1}, P_i performs tag reading protocol with the same random number r_1 of length ℓ and records a list L of responses x_j from all tags in the batch, where $x_j = H(r_1||r_2||\beta_{i+1 \leftrightarrow j})$, $r_2 = 0$. Then, P_i sends r_1 to P_{i+1}.
2. Upon receiving r_1, P_{i+1} performs the reading protocol with the same random number r_1 and records a list L' of all responses x'_j from all tags in the batch, where $x'_j = H(r_1||r_2||\beta_{i+1 \leftrightarrow j})$.
3. P_i and P_{i+1} compares the two list L and L'. If the lists match, then both sign on the matched list with the current time-stamp and keep a copy of the signed list. Party P_i sends the signed list to the TA for supply chain visibility. If the two lists do not match, the two parties will settle the disagreement till they reach an agreement. After the handover process, P_{i+1} should switch the tags into the strong security mode if P_i is still around.

The ownership handover process is illustrated in Figure 5. Note that P_i is responsible to report to TA since it is for P_i's interest to finalize the handover process as early as possible. TA is responsible to coordinate the handover process and manage the supply chain visibility accordingly. Our system remains secure even the tags are set to the weak security mode in the ownership handover process. The reason is that the tagged products remain static in this process; there is no point to track tags while they are not moving. After ownership handover, the tags are in P_{i+1}'s control, who will keep the tags secure by switching to appropriate security modes. If P_i has not updated some tags appropriately before ownership handover due to de-synchronization attacks or communication errors, both parties will detect the mismatch; P_i can re-update the tags to facilitate the handover. Therefore, our solution has the de-synchronization resilience property.

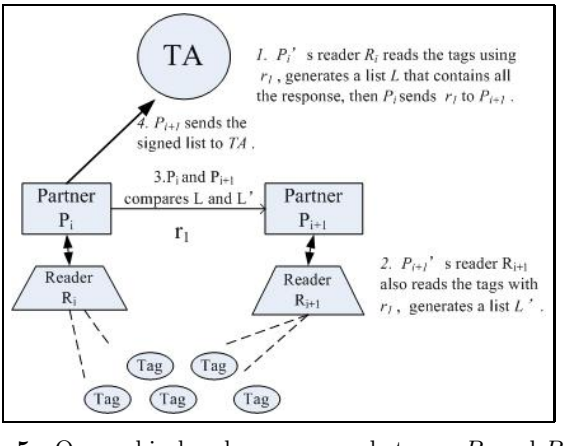

Fig. 5. Ownership handover process between P_i and P_{i+1}

4 Analysis

In this section, we analyze our protocols with respect to the requirements of security, visibility, and efficiency. We summarize our analysis results in the form of statements. Proofs and explanations of the statements will be given in the full version of this paper.

STATEMENT 4.1 (Authoritative access to RFID tags). *Only a valid reader with a tag's temporary secret authorized by TA is able to conduct reading and updating on the tag successfully.*

STATEMENT 4.2 (Authenticity of tags). *Given two numbers r_1 and r_2, the probability for an adversary without the knowledge of $\beta_{i \leftrightarrow j}$ to find a valid response x such that $x = H(r_1||r_2||\beta_{i \leftrightarrow j})$ holds is $\frac{1}{2^\ell}$, where ℓ is the length of $\beta_{i \leftrightarrow j}$.*

STATEMENT 4.3 (Weak unlinkability). *Given a response x_1 from a tag prior to being processed by party P_i and a response x_2 from a tag after being processed by P_i, it is computationally infeasible for a rogue reader to determine whether x_1 and x_2 is from the same tag.*

STATEMENT 4.4 (Strong unlinkability). *A tag is strong unlinkable in the strong security mode. It is also strong unlinkable in the weak security mode in an environment of no active attacks.*

STATEMENT 4.5 (Forward and backward secrecy). *If the protocol communication between a tag and a reader is compromised in certain party, it will not affect the security of the protocol communication between the tag and the reader in any other parties.*

STATEMENT 4.6 (De-synchronization resilience). *The temporary secret updating protocol and the security mode switching protocol in our security solution are resilient to de-synchronization attacks.*

STATEMENT 4.7 (Visibility). *While unauthorized entities are prevented from tracking the movement of material flow, authorized entities have access to the information about where and when a tag is processed.*

STATEMENT 4.8 (Efficiency). *In the weak security mode, the time complexity for an authorized reader to identify a batch of n tags is $O(n \log n)$. In the strong security mode, the time complexity is $O(n^2)$.*

The bottleneck of most RFID-enabled supply chain systems including ours is the process of identifying a large number of tags by each reader. According to [16,17], we roughly estimate that it takes about 210 CPU cycles of a Pentium CPU to perform a hash function (e.g., SHA-1) for digesting a 128-bit message and about 40 CPU cycles per sort operation for merge-sort or quick-sort algorithms. We assume that there are 2^{20} tags in each batch, and a 1-GHz Pentium machine is used in each reader's servant computer. In the weak security mode, it requires about 800ns in database search for identifying each tag. In the strong security mode, however, the batch size is better below 10^4 so that a reader can identify about 500 tags per second. Since an RFID reader usually can perform about 100 times reading, the speed of searching tags in database is sufficiently fast enough as it is higher than 100 tags per second.

5 Related Work

A bundle of research papers addressing RFID security and privacy problems have been published (refer to [4] for a detailed literature survey) in recent years. Among them, tens of (privacy enhanced) tag/reader mutual authentication protocols have been proposed in the literature such as the HB family of RFID protocols [5,6], symmetric cipher based protocols [7,8,9], and lightweight primitive based protocols [10, 11]. Unfortunately, all of these RFID protocols have focused on protecting tag to reader communication in a single domain, where no cross-domain relationship is considered among various supply chain parties. Therefore, their techniques cannot be directly used to ensure the information sharing protocols interacting multiple supply chain parties.

In this section, we compare our solution with the most related works [12,14,13] on RFID authentication protocols in supply chain environments. We realize that these works might have been attacked in some way [15], their original ideas are still meritable and worth being reviewed. A summary of our comparison is given in Table 1.

In [12], Li and Ding proposed a de-centralized solution for secure RFID communications in supply chains. In their solution, an access key is shared between each tag and each supply chain party. The access key of a tag can be updated by the current supply chain party before the tag is handed over to the next supply chain party. Since the updated access key is shared between the current supply chain party and the next supply chain party, their solution is vulnerable to insider attacks without backward or forward secrecy. Their solution is similar to our solution in the weak security mode in a sense that only weak unlinkability is provided. The time complexity of their solution is also similar to our solution in the weak security mode, which is $O(n \log n)$ for processing each batch of tags. Since there is no trusted authority involved in their solution, the supply chain visibility should be maintained by each party's database in a distributed manner.

Juels, Pappu, and Parno proposed an interesting solution for secure RFID-enabled supply chains [13]. In their work, a secret sharing method is used to break a secret key to multiple shares, with each share stored in a single tag along with the cipher of the tag id encrypted with the secret key. An authorized supply chain party, which is supposed to get access to a large number of tags can collect enough shares to recover the secret key, and thus decrypt the tags' IDs. An adversary is assumed to have limited access to the tags; thus, he or she cannot recover the secret key nor decrypt any tags' IDs. It is clear that this solution does not have any unlinkability feature. Anyone can track the movement of a tag even if it is encrypted. The advantage of this solution is that it can be directly used with the current EPC Gen2 tags [1] without any cryptographic extensions; therefore, the cost of tags is apparently lower than other solutions which have to incorporate hash and random number generation computations in tags.

Song proposed an RFID ownership transfer protocol recently [14]. In her solution, a supply chain party and a tag share a couple of secrets (t, s), where $t = h(s)$. The tag stores the value t, and the reader authorizes itself to the tag

Table 1. Comparison of our solution with three other solutions

	Unlinkability (anti-tracking)	Visibility (handover)	Efficiency (tag search)	Cost (tag)
[12]	Weak	Distributed	Batch process	Moderate
[13]	Null	Distributed	Decryption	Low
[14]	Strong	Distributed	Tag by tag	Moderate
Our solution	Strong	Centralized	Switch	Moderate

by proving its possession of s. In ownership handover, the current party must be online to help the next party to identify a tag; then, the current party will send the tag secret to the next party, which will use the secret information to update the tag secret to a new value. To provide strong unlinkability, each tag will generate its reply based on a fresh random number, which is similar to our solution in the strong security mode. The weakness of this solution is its low efficiency, especially in the handover process which takes $O(n^2)$ time for processing n tags one by one.

Comparing to the above works, our proposal solution is the only solution that involves a trusted authority. Therefore the supply chain visibility can be easily maintained in a centralized manner. On the one hand, our solution provides strong unlinkability under the assumption that the weak security mode is used in a relative secure environment of no active attacks. On the other hand, it can switch to the weak security mode for higher efficiency in tag reading. It thus provides higher efficiency in certain environment without downgrading the security features. In terms of tag cost, our solution is similar to [12, 14] as it involves random number generation and hash computations in tags. Note that our solution is suitable for the RFID tags of cost around US$0.5 and RFID reader of cost around US$1000. Such RFID readers and tags are currently available in the market and their costs are affordable in supply chain management at container, pallet, or case level (probably not at the item level).

6 Conclusion

In this paper, we investigate the security, visibility, and efficiency issues for RFID-enabled supply chain systems. High efficiency is particularly desirable in RFID-enabled supply chains since a large quantity of tagged products are routinely processed and exchanged among multiple supply chain parties such as suppliers, manufacturers, distributors, and retailers. In order to enhance the efficiency of a RFID-enabled supply chain system without sacrificing its security, we distinguish the environments into two secure levels. In a relatively secure environment with no active attacks, our RFID system can be set to the weak security mode so as to provide high processing speed. While in a relatively less secure environment that is exposed to active attacks, our RFID system can be switched to the strong security mode so as to maintain strong unlinkability. In the future, we are interested in investigating the scalability of our solution and verifying its practicality in real EPCglobal network or simulated environments.

Acknowledgment. This work is partly supported by A*Star SERC Grant No. 082 101 0022 in Singapore.

References

1. EPCglobal Inc., E.P.C. Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.1.0. EPCglobal Standards (October 2007)
2. EPCglobal Inc., Architecture Framework Standard v1.0
3. Liu, E., Kumar, A.: Leveraging information sharing to increase supply chain configurability. In: Twenty-Fourth International Conference on Information Systems, pp. 523–537 (2003)
4. Juels, A.: RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006)
5. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 293–308. Springer, Heidelberg (2005)
6. Bringer, J., Chabanne, H., Emmanuelle, D.: HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks. In: IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2006, Lyon, France. IEEE Computer Society Press, Los Alamitos (2006)
7. Sarma, S., Weis, S., Engels, D.: RFID systems and security and privacy implications. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 454–469. Springer, Heidelberg (2003)
8. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic approach to privacy-friendly tags. In: Proc. of RFID Privacy Workshop (2003)
9. Aigner, M., Feldhofer, M.: Secure Symmetric Authentication for RFID Tags. Telecommunication and Mobile Computing (March 2005)
10. Vajda, I., Buttyan, L.: Lightweight authentication protocols for low-cost RFID tags. In: Proc. of UBICOMP 2003 (2003)
11. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. In: Proc. of 2nd Workshop on RFID Security (July 2006)
12. Li, Y., Ding, X.: Protecting RFID Communications in Supply Chains. In: ASIACCS 2007: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, pp. 234–241. ACM, Singapore (2007)
13. Juels, A., Pappu, R., Parno, B.: Unidirectional key distribution across time and space with applications to rfid security. In: 17th USENIX Security Symposium, pp. 75–90 (2008)
14. Song, B.: RFID Tag Ownership Transfer. In: Conference on RFID Security (RFIDsec 2008), Budapest, Hungary (July 2008)
15. van Deursen, T., Radomirovic, S.: Attacks on RFID Protocols. Cryptology ePrint Archive: Report 2008/310 (2008)
16. Menascé, D.: Security performance. IEEE Internet Computing 7(03), 84–87 (2003)
17. Li, X., Zhang, X., Kubricht, S.: Improving memory performance of sorting algorithms. J. Exp. Algorithmics 5, 3 (2000)