Vulnerability analysis of lightweight secure search protocols for low-cost RFID systems

Chao Lv*, Hui Li, Jianfeng Ma and Ben Niu

Key Laboratory of Computer Networks and Information Security,
Xidian University,
Xi'an, China
Email: lyvchao@gmail.com
Email: lihui@mail.xidian.edu.cn
Email: jfma@mail.xidian.edu.cn
Email: xd.niuben@gmail.com
*Corresponding author

Abstract: RFID systems have many security risks as an insecure wireless communication channel exists between tag and reader. Kulseng et al. have proposed several lightweight secure search protocols for low-cost systems: the basic protocol and the synchronisation-based protocol. To attack these two protocols successfully, the adversary needs to eavesdrop on the communication channel between reader and tag, and intercept and tamper with the exchanged messages. We show that the basic protocol cannot resist the *tracking attack*. The synchronisation-based protocol is vulnerable to the tracking attack and a kind of *desynchronisation attack*.

Keywords: RFID protocol; low cost; tracking attack; desynchronisation attack.

Reference to this paper should be made as follows: Lv, C., Li, H. Ma, J. and Niu, B. (2012) 'Vulnerability analysis of lightweight secure search protocols for low-cost RFID systems', *Int. J. Radio Frequency Identification Technology and Applications*, Vol. 4, No. 1, pp.3–12.

Biographical notes: Chao Lv received his BE degree from Fu Zhou University in 2002, ME degree from Yan Shan University in 2006. He is currently a PhD candidate at Xidian University, Xi'an, China. His research interests include cryptography, security protocol, RFID protocol and formal verification.

Hui Li received his BE degree from Fu Dan University in 1990, PhD degree in Communication and Electronic Engineering from Xidian University in 1998. Prof. Li has published around 30 academic papers in the areas of information security, coding theory, etc. His research interests include information security, coding theory and wireless network security.

Jianfeng Ma received his BE degree in Mathematics from Shaanxi Normal University in 1985 and his ME and PhD degrees in Computer Software and Communications Engineering from Xidian University, China, in 1988 and 1995, respectively. Since 1995 he has been with Xidian University as a Lecturer, Associate Professor and Professor. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. Currently, Prof. Ma is the Director of the Ministry of Education Key Laboratory of Computer Networks and Information Security. His research interests include information security, coding theory and cryptography.

Ben Niu received his BE and ME degrees from School of Telecommunications Engineering from Xidian University, China, in 2006 and 2010, respectively. He is currently a PhD candidate at Xidian University. His research interests include cryptography, security protocol and formal verification.

1 Introduction

Radio Frequency Identification (RFID) is a wireless Automatic Identification and Data Capture (AIDC) technology for identifying a product, animal or person by using radio signals (Juels, 2006). Due to the widespread distribution of RFID tags as well as the tag limitations in terms of the circuitry (computation power), storage and power consumption, it is a great challenge to design an efficient and secure RFID authentication protocol (López, 2008). One important functionality that an RFID system should provide is tag search, where a reader can detect if a particular tag is present or not. Tag search approaches pose challenge to security and privacy. Surprisingly, the problem of RFID search has not been widely addressed in the literature despite the availability of search capabilities in commercial RFID products (Tan et al., 2008).

Some RFID systems (Dimitriou, 2005; Lee et al., 2005; Tsudik, 2006) are based on a central database which is dependent on a reliable connection between an RFID reader and the central database. Tan et al. (2008) have proposed a more flexible authentication protocol that provides comparable protection without the need for a central database and provides a search protocol for RFID tags with security and privacy protection. The solutions in Tan et al. (2008) are based on hash function and are expensive for low-cost RFID systems (Kulseng et al., 2009).

Kulseng et al. (2009) have proposed several lightweight secure search protocols. Their schemes are built on Linear Feedback Shift Registers (LFSR) (Menezes et al., 2001) and Physically Unclonable Functions (PUF) (Suh and Devadas, 2007), which are very efficient for implementation in low-cost tags. They use LFSR to generate random numbers for the encryption of communication and rely on PUF to authenticate the identity of tags. The authors claim that the proposed protocols are able to prevent the leakage of tag information and the adversary from generating fake messages to impersonate the RFID reader or tag. However, in this paper, we show that the protocols in Kulseng et al. (2009) are vulnerable to *tracking attack* and *desynchronisation attack*. The adversary eavesdrops on the communication channel between reader and tag and intercepts or tampers the exchanged messages in order to trace the target tag or desynchronise the stored data on the reader (tag) side.

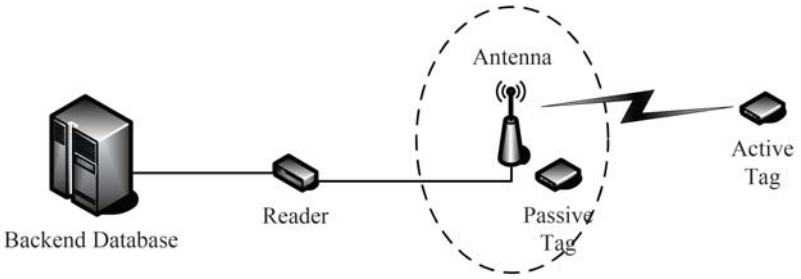
The rest of the paper is organised as follows. In Section 2, we introduce system model and threat model. In Section 3, we review the basic protocol. The security analysis of the basic protocol is presented in Section 4. We review the proposed synchronisation-based protocol in Section 5. The vulnerability analysis of this synchronisation-based protocol is discussed in Section 6. Finally, we conclude in Section 7.

2 System background

2.1 System model

A typical RFID system architecture (Thornton et al., 2006) consists of three key components: RFID tags, RFID readers and a backend server (see Figure 1). The reader sends a radio signal to the tag and listens to the tag's response. The tag detects this signal and replies with its identification. The reader and the tag communicate with each other through the wireless network, whereas the communication channel between reader and database can be wired or wireless. Usually, we assume that the communication between server and reader is secure due to the usage of advanced encryption scheme. The wireless communication channel between reader and tag is not secure, and an adversary can eavesdrop on it. The adversary can also intercept or even modify and inject the communication messages.

Figure 1 RFID system architecture



2.2 Threat model

RFID technology has been widely used in numerous applications, ranging from manufacturing, logistics, transportation, warehouse inventory control, supermarket checkout counters, to many emerging applications (Berbain et al., 2009). RFID systems may face many threats which are launched by all kinds of attackers. These attackers may be active or passive. The construction of formal RFID security and privacy frameworks is fundamental to the design and analysis of robust RFID systems.

Dolev–Yao intruder model (Dolev and Yao, 1983) is the classical model used to analyse security protocols. Under this model, the adversary may have full control over the network. The adversary can eavesdrop on all messages exchanged between reader and tag, modify or block any message sent from reader to tag or vice versa, and may inject its own modified messages making them look like they have been sent from tag or reader. Additionally, there is an assumption that the adversary can observe whether an agent has successfully completed its run (van Deursen and Radomirović, 2009) when we analyse RFID protocols. The representative adversary models for RFID protocol analysis can be found in Vaudenay (2007), Juels and Weis (2007), Paise and Vaudenay (2008) and Deng et al. (2010).

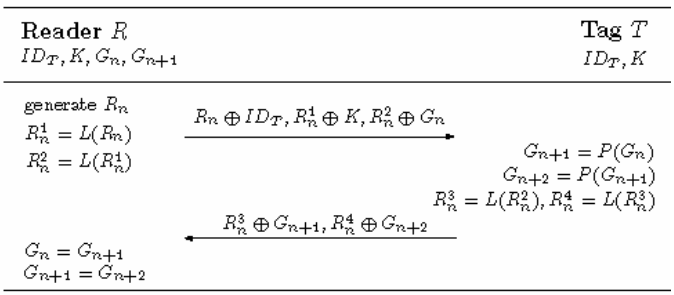
3 Review of lightweight secure search protocol: a basic protocol

In this section, we review the basic protocol proposed in Kulseng et al. (2009). The following notations are used throughout this paper:

- ID_T, the identity of target tag which is a q-bit length integer such that $1 \le ID_T \le 2^q$.
- K, the shared secret key between reader and target tag whose length is also q-bit. Each tag shares a different key with the reader.
- L: $[1, 2^q] \rightarrow [1, 2^q]$, a random permutation function whose input and output are both q-bit integers. L function is treated as a random generator and is constructed using LFSR. The construction of L function is public.
- P: $[1, 2^q] \rightarrow [1, 2^q]$, a random permutation function whose operation range is $[1, 2^q]$. P function is constructed by PUF.
- G_n, the *greeting* from reader to tag in the current round, where n is the round index with the initial value 1.
- G_{n+1}, the greeting used in the next round which is computed from $G_{n+1} = P(G_n)$.
- R_n, a random number generated by the reader to mask ID_T.

As illustrated in Figure 2, the basic protocol consists of two phases: set-up phase and search phase.

Figure 2 Review of the basic protocol



3.1 Set-up phase

In this phase, the reader and all the tags are preloaded with some secret information. The reader and the target tag share three items: ID_T, K and L. The tag, besides the three items, also stores function P. While the reader contains two greeting numbers: G_n and G_{n+1}.

3.2 Search phase

The details of steps for search phase are described as follows:

1 Reader R generates a random number R_n and computes $R_n^1 = L(R_n)$, $R_n^2 = L(R_n^1)$. Then reader broadcasts the query message $R_n \oplus ID_T, R_n^1 \oplus K, R_n^2 \oplus G_n$.

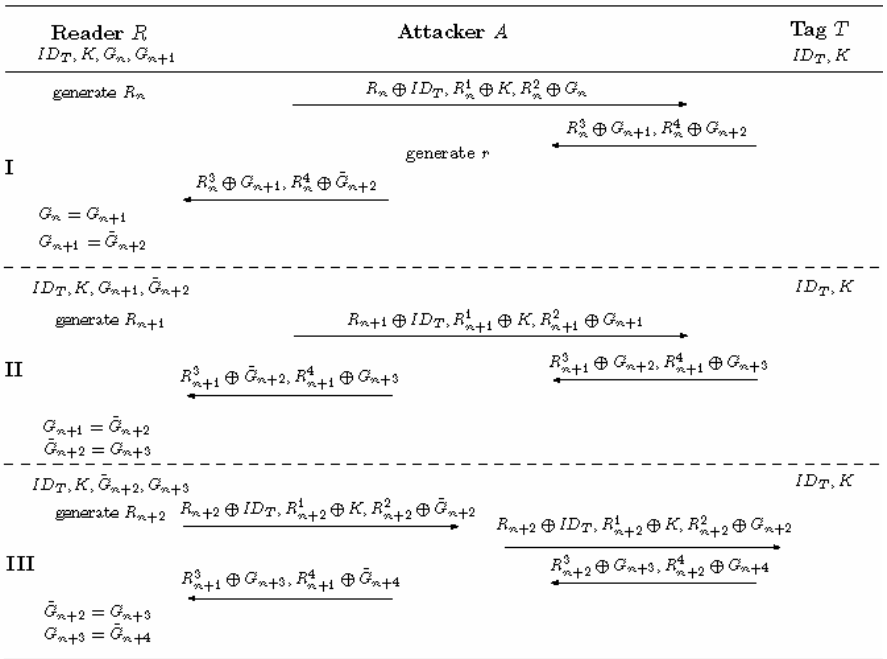
2 Upon receiving this query, each tag derives R_n from $R_n \oplus ID_T$ with its own ID_T. Then, it derives $K = R_n^1 \oplus K \oplus L(R_n)$. If the derived K equals the value stored by the tag, the tag can be certain that this query is looking for it. Only the target tag has the correct ID_T and only it can derive R_n and verify K successfully. The target tag computes $G_n = R_n^2 \oplus G_n \oplus L(L(R_n))$. Other tags will discard this query. Then it computes $G_{n+1} = P(G_n)$ and $G_{n+2} = P(G_{n+1})$ using the P function. It also calculates two sequential random numbers as $R_n^3 = L(R_n^2)$ and $R_n^4 = L(R_n^3)$. Finally, the target tag replies the reader with $R_n^3 \oplus G_{n+1}$, $R_n^4 \oplus G_{n+2}$.

3 After receiving this response, reader derives $G_{n+1} = R_n^3 \oplus G_{n+1} \oplus L(L(L(R_n)))$ and compares the derived G_{n+1} with the value it stores. If the two values are equal, it proves the existence of the target tag. Then reader computes G_{n+2} from $R_n^4 \oplus G_{n+2}$ and updates $G_n = G_{n+1}$ and $G_{n+1} = G_{n+2}$ for the next round.

4 Security analysis of the basic protocol

In this section, we perform the vulnerability analysis of the basic protocol under the Dolev–Yao intruder model. We present a kind of *tracking attack* which breaks the tag location privacy. The attack process consists of two phases which are shown in Figure 3 as I and II.

Figure 3 Attack on the basic protocol



4.1 First phase

1 A normal nth session takes place. The adversary eavesdrops on the message $R_n \oplus ID_T, R_n^1 \oplus K, R_n^2 \oplus G_n$.

2 The adversary is also able to sniff the message $R_n^3 \oplus G_{n+1}, R_n^4 \oplus G_{n+2}$, which is sent by the target tag and prevents the reader from receiving it. Then the adversary generates a random integer r with q-bit length and computes $R_n^4 \oplus G_{n+2} \oplus r = R_n^4 \oplus \tilde{G}_{n+2}$, where $\tilde{G}_{n+2} = G_{n+2} \oplus r$. Finally it sends $R_n^3 \oplus G_{n+1}, R_n^4 \oplus \tilde{G}_{n+2}$ to reader.

3 Upon receiving the tampered response replied by the adversary, reader first derives G_{n+1} and compares the derived G_{n+1} with the value it stores. This check is successful. Then the reader computes $\tilde{G}_{n+2} = R_n^4 \oplus \tilde{G}_{n+2} \oplus L(L(L(L(R_n))))$. Finally reader updates the stored G_n and G_{n+1} to G_{n+1} and $\tilde{G}_{n+2}$, respectively, for the next round.

4.2 Second phase

Now the (n+1)-th search session takes place, the adversary operates as a man in the middle.

1 Reader generates a new random number R_{n+1} and broadcasts the new query message $R_{n+1} \oplus ID_T, R_{n+1}^1 \oplus K, R_{n+1}^2 \oplus G_{n+1}$ for the (n+1)-th round of search.

2 Upon receiving this query, the target tag replies with new response $R_{n+1}^3 \oplus G_{n+2}, R_{n+1}^4 \oplus G_{n+3}$. The adversary intercepts this message and uses the same random number r which is generated in the first phase to calculate $R_{n+1}^3 \oplus G_{n+2} \oplus r = R_{n+1}^3 \oplus \tilde{G}_{n+2}$, where $\tilde{G}_{n+2} = G_{n+2} \oplus r$. In the end, the adversary sends the constructed message $R_{n+1}^3 \oplus \tilde{G}_{n+2}, R_{n+1}^4 \oplus G_{n+3}$ to the reader.

3 Once receiving $R_{n+1}^3 \oplus \tilde{G}_{n+2}, R_{n+1}^4 \oplus G_{n+3}$, reader derives $\tilde{G}_{n+2} = R_{n+1}^3 \oplus \tilde{G}_{n+2} \oplus L(L(L(R_{n+1})))$ and the derived $\tilde{G}_{n+2}$ is the same as it stores. The reader queries the target tag successfully and updates $G_{n+1} = \tilde{G}_{n+2}$ and $G_{n+2} = G_{n+3}$.

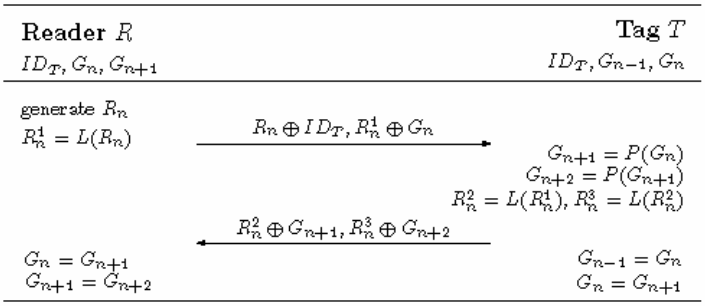
In this case, by checking the verification result of the reader that whether the derived $\tilde{G}_{n+2}$ is equal to the stored value, the attacker can easily identify the tag that it had monitored in the first phase from large number of tags and, thus, successfully perform a tracking attack.

After these two phases, if the attacker wants to continue tracking the target tag, then it needs to monitor the communication between the reader and the tag. Because the messages stored by the reader have been updated into $ID_T, K, \tilde{G}_{n+2}, G_{n+3}$, the attacker must intercept each exchanged message and modify them, which are shown in Figure 3 as III. In part III of the figure, $\tilde{G}_{n+4} = G_{n+4} \oplus r$.

5 Review of lightweight secure search protocol: a synchronisation-based protocol

The authors also propose a synchronisation-based lightweight secure search protocol (Kulseng et al., 2009), which is shown in Figure 4. In this protocol, the tag can record the queries that have been used, then it can recognise a replayed query and do not respond.

Figure 4 Review of the synchronisation-based protocol



In the *set-up phase*, tag stores G_{n-1} and G_n, where G_{n-1} is the greeting number in the previous round and G_n is the greeting number expected to be received in the current round. In the first round, only G_1 is needed, so G_0 is ignored and set to zero.

In the *search phase*, reader broadcasts its search query to all tags. The target tag checks if the greeting number in the query equals either G_{n-1} or G_n. If it can verify G_n, it replies with G_{n+1} and G_{n+2} which are masked with R_n^2 and R_n^3, separately. Meanwhile, it updates $G_{n-1} = G_n$ and $G_n = G_{n+1}$. If the query does not contain G_n, then the target tag keeps on verifying G_{n-1}. If G_{n-1} is found, the target tag replies with $R_n^2 \oplus G_n, R_n^3 \oplus G_{n+1}$, whereas it does not update the stored greeting numbers. If the query contains neither G_n nor G_{n-1}, the target tag concludes that it is a replayed query and discards this query.

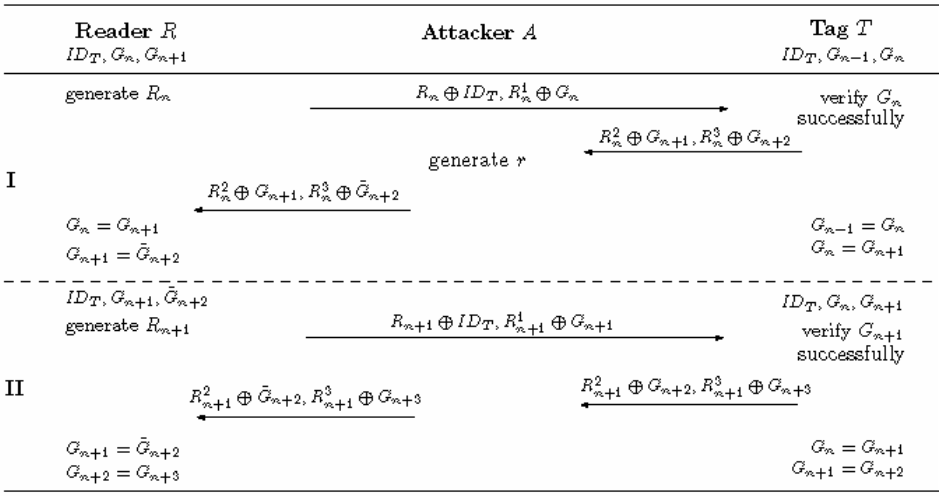
6 Security analysis of the synchronisation-based protocol

In this section, we show that the synchronisation-based protocol is vulnerable to *tracking attack* and *desynchronisation attack*. The attack steps are the same as attack on the basic protocol which are shown in Figure 5.

In the first phase, a normal *n*-th session takes place. The adversary intercepts the message $R_n^2 \oplus G_{n+1}, R_n^3 \oplus G_{n+2}$, which is sent from tag to reader. The adversary generates a random number r and calculates $R_n^3 \oplus G_{n+2} \oplus r = R_n^3 \oplus \tilde{G}_{n+2}$, where $\tilde{G}_{n+2} = G_{n+2} \oplus r$. Then the adversary sends the modified message to the reader. At last the reader updates $G_n = G_{n+1}$ and $G_{n+1} = \tilde{G}_{n+2}$, separately. The tag updates $G_{n-1} = G_n$ and $G_n = G_{n+1}$.

In the second phase, the (n+1)-th session takes place. In this session, the adversary also operates as a man in the middle. Firstly, the reader broadcasts the request message $R_{n+1} \oplus ID_T, R_{n+1}^1 \oplus G_{n+1}$. The target tag receives this message and verifies G_{n+1} successfully. Secondly, the target tag replies with the response $R_{n+1}^2 \oplus G_{n+2}, R_{n+1}^3 \oplus G_{n+3}$. The adversary blocks the reply message and calculates $R_{n+1}^2 \oplus G_{n+2} \oplus r = R_{n+1}^2 \oplus \tilde{G}_{n+2}$, where r is the same random number generated in last phase. Then the adversary sends this modified message to the reader. Lastly, the reader updates its stored data $G_{n+1} = \tilde{G}_{n+2}$ and $G_{n+2} = G_{n+3}$, separately. The target tag also updates its stored data as $G_n = G_{n+1}$ and $G_{n+1} = G_{n+2}$ as described above. The stored data G_{n+1} in each side are not the same. This is a kind of *desynchronisation attack*. As has been discussed for basic protocol in Section 4, this protocol also cannot resist the *tracking attack*.

Figure 5 Attack on the synchronisation-based protocol



7 Conclusion

In this paper, we have analysed two lightweight secure search protocols for low-cost RFID systems. These two protocols are the basic protocol and the synchronisation-based protocol. We have demonstrated that the basic protocol is vulnerable to tracking attack, and the synchronisation-based protocol is not secure against tracking attack and desynchronisation attack. Both these attacks are caused by the linearity operation $\oplus$. Our work shows that it may be quite unsafe using only simple bitwise operations to achieve RFID security under powerful adversary model. The security of RFID protocols must be proved with careful cryptanalysis. It is a challenge to design a secure protocol for low-cost RFID systems without using strong cryptographic algorithms such as hash function and symmetric encryption (Cao et al., 2009).

Acknowledgements

This work was supported by the following projects: the National Natural Science Foundation of China (Grant Nos. 60772136, 61003300), the 111 Development Program of China (B08038), the Doctoral Fund of Ministry of Education of China (20100203110002) and the Fundamental Research Funds for the Central Universities (JY10000901018, JY10000901021, JY10000901032 and JY10000901034).

References

Berbain, C., Billet, O., Etrog, J. and Gilbert, H. (2009) 'An efficient forward private RFID protocol', *CCS'09: Proceedings of the 16th ACM Conference on Computer and Communications Security*, Association for Computing Machinery, New York, NY, USA, pp.43–53.

Cao, T., Bertino, E. and Lei, H. (2009) 'Security analysis of the SASI protocol', *IEEE Transactions on Dependable and Secure Computing*, Vol. 6, pp.73–77.

Deng, R.H., Li, Y., Yao, A.C., Yung, M. and Zhao, Y. (2010) 'A new framework for RFID privacy', *Cryptology ePrint Archive*, Report 2010/059.

Dimitriou, T. (2005) 'A lightweight RFID protocol to protect against traceability and cloning attacks', *SECURECOMM'05: Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, IEEE Computer Society, Washington, DC, USA, pp.59–66.

Dolev, D. and Yao, A. (1983) 'On the security of public-key protocols', *IEEE Transactions on Information Theory*, Vol. 29, No. 2, pp.198–208.

Juels, A. (2006) 'RFID security and privacy: a research survey', *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp.381–394.

Juels, A. and Weis, S.A. (2007) 'Defining strong privacy for RFID', *PerCom Workshops'07: 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pp.342–347.

Kulseng, L., Yu, Z., Wei, Y. and Guan, Y. (2009) 'Lightweight secure search protocols for low-cost RFID systems', *ICDCS'09: Proceedings of the 29th IEEE International Conference on Distributed Computing Systems*, IEEE Computer Society, Washington, DC, USA, pp.40–48.

Lee, S-M., Hwang, Y.J., Lee, D.H. and Lim, J.I.L. (2005) 'Efficient authentication for low-cost RFID systems', ICCSA 2005: International Conference on Computational Science and its Applications, *Lecture Notes in Computer Science*, Vol. 3480, pp.619–627.

López, P.P. (2008) *Lightweight Cryptography in Radio Frequency Identification (RFID) Systems*, PhD thesis, Universidad Carlos III de Madrid.

Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. (2001) *Handbook of Applied Cryptography*, CRC Press, London.

Paise, R-I. and Vaudenay, S. (2008) 'Mutual authentication in RFID: security and privacy', *ASIACCS'08: ACM Symposium on Information, Computer and Communications Security*, ACM Press, Tokyo, Japan, pp.292–299.

Suh, G.E. and Devadas, S. (2007) 'Physical unclonable functions for device authentication and secret key generation', *DAC'07: Proceedings of the 44th Annual Design Automation Conference*, ACM, New York, NY, USA, pp.9–14.

Tan, C.C., Sheng, B. and Li, Q. (2008) 'Secure and serverless RFID authentication and search protocols', *IEEE Transactions on Wireless Communications*, Vol. 7, pp.1400–1407.

Thornton, F., Haines, B., Das, A.M., Bhargava, H. and Campbell, A. (2006) *RFID Security*, Syngress, Waltham, MA, USA.

Tsudik, G. (2006) 'YA-TRAP: yet another trivial RFID authentication protocol', *PerCom 2006: International Conference on Pervasive Computing and Communications*, IEEE Computer Society, Pisa, Italy, pp.640–643.

van Deursen, T. and Radomirović, S. (2009) *Attacks on RFID Protocols (Version 1.1)*, Technical Report, University of Luxembourg.

Vaudenay, S. (2007) 'On privacy models for RFID', Asiacrypt 2007: Advances in Cryptology, *Lecture Notes in Computer Science*, pp.68–87.