2015

A secure sharing design for multi-tag RFID authentication protocol

Ayad Al-Adhami
Plymouth University, Plymouth, UK, ayad.al-adhami@plymouth.ac.uk

Marcel Ambroze
Plymouth University, Plymouth, UK, m.ambroze@plymouth.ac.uk

Colin Cristopher
Plymouth University, Plymouth, UK, c.cristopher@plymouth.ac.uk

Ingo Stengel
Plymouth University, Plymouth, UK; University of Applied Sciences Karlsruhe, Germany, Ingo.Stengel@plymouth.ac.uk

Martin Tomlinson
Plymouth University, Plymouth, UK, m.tomlinson@plymouth.ac.uk

DOI: 10.4225/75/57a9467dd3353
This paper was originally presented at The Proceedings of [the] 8th Australian Security and Intelligence Conference, held from the 30 November – 2 December, 2015 (pp. 87-93), Edith Cowan University Joondalup Campus, Perth, Western Australia.

A SECURE SHARING DESIGN FOR MULTI-TAG RFID AUTHENTICATION PROTOCOL

Ayad.Al-Adhami[1], Marcel Ambroze[1], Colin Cristopher[2], Ingo Stengel[1, 3] & Martin Tomlinson[1]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2]School of Computing, Electronics and Mathematics, Plymouth University, Plymouth, UK
[3]University of Applied Sciences Karlsruhe, Germany
{Ayad.Al-Adhami, M.Ambroze, C.Cristopher, Ingo.Stengel, M.Tomlinson}@plymouth.ac.uk

Abstract
RFID technology, in recent years, has gained significant momentum with increased use in supply chain management. In view of its great potential, RFID technology can provide accurate information, ease of control and labor cost reduction (Masum and Bhuiyam, 2013). Despite the fact that RFIDs can enhance the efficiency of supply chain management, there exist some issues that require due consideration; these issues include scalability and security challenge. RFID based solutions are actually developed, yet they do not tend to address number of risks related to security and privacy of the information that is stored in each tag, e.g. unauthorised reader can read the information inside the tag, illegitimate tags or cloned tags can be accessed by reader that generate privacy and security problem. Most of these developed authentication protocols; however, they still focus only on single reader and single tag authentication. This paper seeks proposal of an authentication protocol that allows shares of the encryption message with multi-tag during the authentication process. The proposed design complements the idea of combining the lite version of Cramer-Shoup cryptosystem with the Shamir's secret key scheme. This combination allows the sharing of the encrypted message within multi-tag and managing up keys distribution during the authentication scheme. The security and privacy of the proposed protocol insures by the property of the lite version of Cramer-Shoup which is secured against non-adaptive chosen cipher-text.

Keywords
RFID security, Authentication protocol, Secret sharing, The lite version of Cramer-Shoup cryptosystem, Multi-tag authentication protocol.

INTRODUCTION

RFID technology takes a place to become one of the most promised technologies which can be used in many applications that need automatic identification (Vaidya et al., 2012). RFID technology contains three parts: RFID tag, RFID reader and a back-end server as shown in figure 1. Depending on power supply, there are three types of RFID tags; passive, semi-passive and active tag. Because of the low cost, passive RFID tag is most popular which have been deployed in many applications such as supply chain management, animal tracking, passports, hospital, building access, transporters and libraries. RFID system identifies tagged objects automatically without human intervention. RFID system allows the identification of tagged objects by using RF signals to collect information from using a reader and by communicating with back-end server (Hunt et al., 2007).

Figure (1) RFID system

Nevertheless, the transformation of data through RF has to be secure due to importance information that mostly contains secret information in the RFID tag. Usually, RFID tag communicates with RFID reader via wireless communication while RFID reader communicates with a back-end server via wire of wireless communication. Because of the wireless communication between RFID tags and RFID reader, many threats eavesdropping or interception the message exchange between RFID tag and RFID reader which increasing the demand of security and privacy. Also, illegitimate reader can get information about the tag and the tag's owner. In order to manipulate the security demand, cryptographic algorithms have been introduces within authentication process to decrease the security and privacy issues of RFID system. Authentication is used to trust and validate an identity to a verifier and this process is considered as the first line of defence against wireless attack (Malek and Miri, 2012). Cryptographic mechanisms are used during the authentication process; the requirements of cryptographic

protocols often depend on a share key mechanism, speed and the size of secret keys. However, computation feasibility in RFID tag is an issue with using cryptographic algorithms due to the memory resources and data storage of the RFID tag. Cryptographic authentication is based on using symmetric key encryption or asymmetric key encryption. In this paper we review existing protocols on RFID authentication that are based on using asymmetric key encryption. Furthermore, explores two designs for multi-tag authentication protocol that can be used in supply chain management.

LITERATURE REVIEW

RFID Authentication Requirements

Despite of that passive RFID tags have a limited resources, an authentication protocol has to satisfy some authentication requirements. For instance, consider RFID system have been applied to supply chain managements. The requirement can be divided into two important parts: A) System requirement part and B) security requirement part.

A. System requirements

RFID system has to be identified objects without a physical contact within a various locations. Detecting objects is a primary requirement for an authentication protocol. RFID readers have to emit signal to RFID tags and power them on, wherever they are even that they are hidden then getting information about them. The level of public information must be limited otherwise any close reader can leak the information of RFID tags and raise the privacy concerns. Identification is required; each RFID tag has a unique identification number. An authentication protocol must assure the uniqueness of the RFID tag identity to avoid multi response and a rise the privacy problem when RFID tag automatically identifies itself to any reader. Scalability of the protocol is also required to avoid imposing of workload.

B. Security Requirements

The most important requirement for authentication protocol is to provide security against threats. In other words, an authentication protocol has to provided confidentiality, integrity and availability to the system. Confidentiality for RFID system means that all secret information must be transmitted in a secure channel. To ensure confidentiality, RFID reader or RFID tag must encrypt the transmit message and the other party have to decrypt the transmit message. Integrity means that data must be protected from tampering by other unauthorised parties. Also ensuring availability of the system is required to providing, storing and processing information. Availability means that ensuring the system available at any time of authentication process.
The nature of the communication of RFID system that works via insecure wireless channel is vulnerable to a various type of attacks. The attacks of RFID system can be classified as follows:

- Denial of Service attack (DoS): In this type of attack, the attacker can cause a lose synchronization between a server and tags by blocking the transmitted message (Weis, et al., 2003; Lee and Yi, 2011). The attacker sends a large number of tag's identifier to the reader then to the back-end server (Sandhya and Rangaswamy, 2011). This attack also can make a smashing to a server when receiving fakes request.
- Reply Attack(RA): In this type of attack, the attacker can lesson to the message exchanged between a server and tags then replay the query to the tag, reader and then the back-end server as a valid tag with a successful authentication process (Dimitriou, 2005; Wei et al., 2011).
- MitM (Man in The Middle) attack: In this type of attack. The attacker interferes and listens to the communication between a server and a tag, then manipulate information by insert, modify, delete and redirect it (Jules, 2004).
- Tag impersonation (TI): In this type of attack, an attacker can communicate with a server instead of specific tag and be authenticated as a tag (Weis, 2003).
- Location tracking attack (TA): In this type of attack, the listing and analysing of the communication between RFID systems can be tracked the location of a specific tag (Wei et al, 2011).
- Backward Traceability (BT): In this type of attack, an attacker might be able to trace previous transactions between a service and a tag. this trace can be done by using the knowledge of the internal state of the tag and given all the internal state of the target tag at time T. The attacker can identifies the tag's past transaction at time T'<T (Ohkubo, Suzki, and Kinoshita 2003)

- Forward Traceability (FT): In this type of attack, an attacker might be able to trace future transaction between a service and tags by using the knowledge of the internal state of the tag and given all the internal state of the target tag at tine T. In addition, the attacker can also identify the tag's past transaction at time $T^{/} > T$ (Lim and Kwon, 2006).

Authentication protocol based on using asymmetric key encryption

In 2005, Wolkerstorfer (2005) introduced and discussed the concept of using elliptic curve cryptography within RFID system and the feasibility of ECC. However, the author did not propose any specific authentication scheme. Tuyls and Batina (2006) proposed an identification scheme based on using Schnorr identification protocol, which is a zero knowledge proof on elliptic curve discrete logarithm problem ECDL. They proved that their protocol can resist against passive attack such as counterfeiting and replay attack (Lee et al, 2008).
Lee et al (2008) proved that the Tuyls and Batina protocol suffered from tracking attack and cannot provide anonymity. Also, this protocol cannot provide forward security and suffered from scalability problem. In 2007, Batina et al (2007) proposed Okamoto's identification RFID protocol based which is also based on using on ECDLP. They proved that their protocol can resist against active attack. Lee et al (2008) presented that Batina et al protocol has issues with location tracking and forward attack. In 2007, Mcloone and Robshaw (2007) implemented an authentication protocol based on using GPS identification protocol (Girault, Poupard and Sterm protocol) which is a version of zero knowledge proof of elliptic curve. In their protocol they proved that the GPS scheme can resist against passive attack. However, the authentication protocol does not provide privacy. In order to provide privacy to the GPS protocol, Bringer et al (2009) also proposed the randomized GPS to ensure privacy. Bringer et al (2009), proposed randomized hashed GPS protocol which is a zero knowledge proof protocol. Bringer et al (2009), proposed the randomized Schnorr protocol to solve the privacy issued of the original Schnorr protocol. In 2009, Martinez et al proposed an authentication protocol that is based on using zero knowledge prove and ECC. They proved that Schnorr protocol is secure against relay attack and man in the middle attack. According to Lv et al (2011), Martinez et al scheme is vulnerable to tracking attack. In 2011, Zhang et al proposed two modifications to improve EC-RAC and Schnorr protocol. Their scheme is aimed to resist to tracing attack. However, Babaheidarian et al (2011) proved that the impersonation attack can affect Zhang et al schemes. Table 1 shows a summery on asymmetric key authentication protocols in terms of violation resistant.

Table 1: Summery for asymmetric key encryption authentication protocols

Attack / Protocol	TL	IA	TA	RA	MitM	DoS	FT	BT
Tuyles and batina	☑	☒	☒	☑	☒		☒	
Batina et al	☑	☒	☒	☒	☒		☒	
GPS	☒	☑	☒	☑	☒	☑	☒	☒
Randomized GPS	☑	☑	☑	☑	☒	☑		
Randomised Hash GPS	☑	☑	☑	☑				
Randomised Schnorr	☑	☑	☑	☑	☑		☑	
Martinies et al	☑	☒	☒	☑	☒	☑		
Zhang et al	☒	☒	☑	☑				

CRYPTOGRAPHY PRIMITIVE

Shamir secret key

In 1979, Shamir (1979) came up with idea to share a key within a based polynomial interpolation. The threshold scheme is divide a secret key within parties. A secret key is defined by a polynomial where the polynomial coefficients are from finite field.
Given k points in 2-dimension plane (x_1, y_1) …. (x_k, y_k) there is only one polynomial of degree $k-1$ such that $q(x_i) = y_i$ for all i. A (k, n) threshold schmes is represented by a polynomial of degree $k-1$. The secret key is split it out to the points $\big(x, f(x)\big)$, where $(x_0, f(x_0))$ is the secret key. For example a $(3, n)$ threshold scheme is defined by a quadratic equation where $(x_0, f(x_0)$ is the secret key and can be constructed by using Lagrange interpolation such as $f(x) = y_i \prod_{i \neq j}^{k-1} \frac{x-j}{i-j}$.

The lite version of Cramer-Shoup Cryptosystem

The lite version of Cramer-Shoup was developed in 1998 and its security based on the hardness of the Dffie-Helman decision problem. This scheme is secure against a non-daptive chosen cipher text attack (Cramer and Shoup, 1998). The lite version of Cramer-Shoup cryptosystem requires a group G of prime order q. and work as follows: the sender selects a prime number $q \in G$ such that $p - 1 = 2q$ where p is also prime. Then choose $g1, g2 \in G$ and $x, y, a, b \in \{0,\ldots$.q-1. Compute $h = g_1^x . g_2^y$ and $C = g_1^a$ and send to the receiver. Now the public key is (g_1, g_2, h, C) and the private key is (x, y, a, b). The encryption process starts after choosing $m \in Z$, then randomly selects $r \in \{0, \ldots . q-1\}, then\ computes\ u = {g_1}^r, \quad v = {g_2}^r\ W = mh^r$, and $e = C^r = ({g_1}^x . {g_2}^y)^r$. The cipher text is (u, v, w, e) and sends it back. The sender check if $e = u^a . v^b\ then\ m = \frac{W}{u^x v^y}\ otherwise\ m = \perp$.

A PROPOSED DESIGN FOR MULTI-TAG AUTHENTICATION PROTOCOL

The proposed design seeks to design an authentication protocol that can be used in supply chain management. Usually, in supply chain management goods are packed into boxes at manufacturers, shipped to warehouses, and then sent to retailers and distributors. As an RFID-tagged box leaves the manufacturer, it scans the information of the tag and records the tag's ID to create lists of items for the inventory purpose. The manufacturer then updates their database that lists the tags associated with the shipped items. This database tracks the tags and the tagged items. So, for example, the manufacturer may mark the state of shipped items as possibly with the location of the warehouse. When the warehouse receives the parcels, it scans the case and the tags which are attached to items, and then a scanner compares the results of the scan with the listing of goods. The warehouse system can detect any of goods that are lost or stolen even that tags that did not respond or failed to deliver to an appropriate place. The warehouse can determine these faults by checking the existing parcel with the listing of goods

For this scenario of distributing and shipping goods, a suggest design model will be introduced to help with the procedure of this scenario. The idea of the design is based on a problem of scanning one parcel which contains boxes and these boxes contain items and each item has a passive RFID tag with one reader to scan the whole parcel.

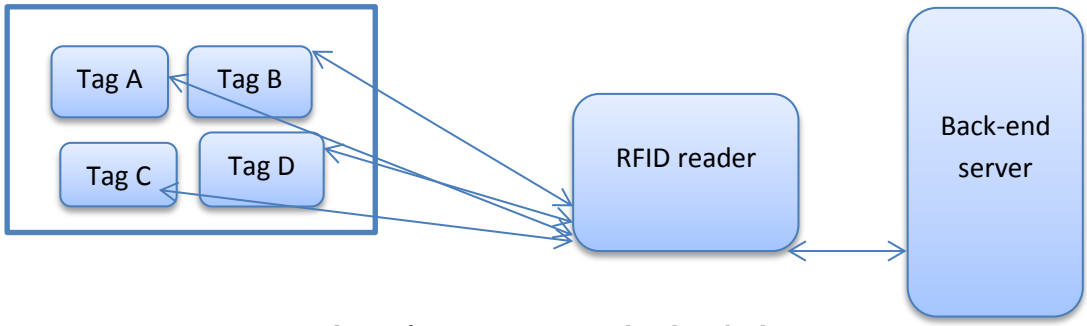

Figure 2: First design for scanning a parcel with multiple RFID tags

Figure 2 describes the basic idea of the protocol. The parcel contains multi-tags and need to be authenticated one by one within a reader and share tags information to a back-end server without revealing secret information

about tags. The main advantage of this design is to avoid a problem of missing item by checking tag information and realise items by checking its information with the back-end server.
The second design can be done by adding a primary tag (Tag G). This tag is reasonable for the authentication between the RFID reader and the parcel while the tag G will be authenticated with the other tags: tag A, tag B, tag C, and tag D in the parcel as shown in figure 3.

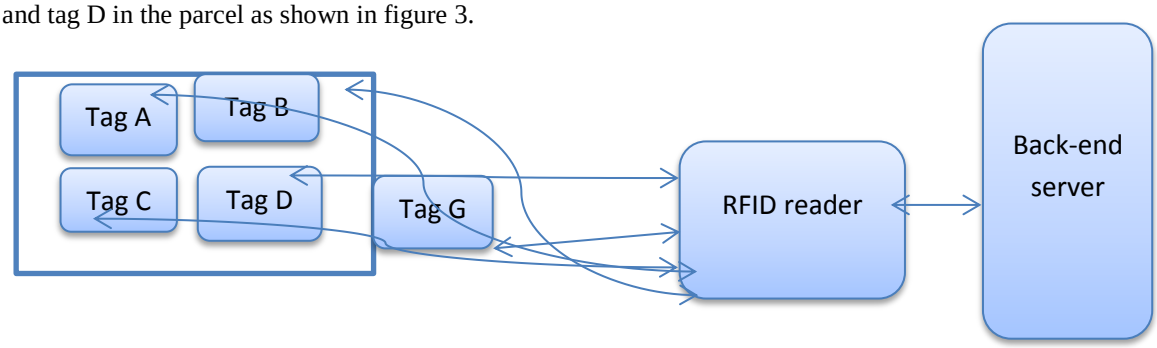

Figure 3: Second design for scanning a parcel with multiple RFID tags

The tag G is considered as a primary tag for the authentication process. It is the authentication link between a reader and the other tags. The primary tag G is responsible for the connection between the reader and the parcel. The tag G can be authenticated with a reader and other tags should be prevented to be communicated with a reader to avoid collision problem. This can be done by providing a protocol that prevents tags ID to be communicated with a reader. The main benefit of this idea is to track and record the movement of the parcel in each procedure. Also the parcel can be updated if an item is stolen or missing during the movement of the parcel. However, the ability of passive tags is limited, although, passive tag cannot communicate with other tags but it can be used for recording the tags information. The handle reader can get the last shipping update of the parcel by checking the tag G. The information can be updated during the shipping procedure by using a handle reader or a fixed reader. However, the tag G can be damaged during the shipping procedure and that can affect the parcel information. In that case, the authentication can be done without the primary tag. The reader should scan objects in the parcel individually by checking the tag's information.

Security consideration for the proposed authentication protocol

The process of designing an authentication protocol for multi-tag should be conducted in a secure manner. The main objective of the proposed solution is to design an authentication protocol that has to satisfy the security needs. Security and privacy should be provided to the protocol design to avoid the lack of security and privacy. Identification is required by defining the tag identifying number to a reader. Furthermore, scalability is another matter for the RFID system; the proposed protocol should have the ability to still scalable and efficient even that a huge number of tags will be provided.
The objective of the proposed protocol is to motivate the lack of security in RFID system. The proposed protocol is based on the following assumption: The channel between a back-end server and an RFID reader is secure. Therefore the back-end server is responsible for generating and updating encryption's keys for tags and reader. In the case of using a handle reader, the communication between RFID system components is through a wireless channel which increases the demand for providing security and privacy to the system. Although, the communication between the back-end server and an RFID reader is assumed to be secure, information exchange on air is easy capture by an adversary that can affect the authentication process. That can be concluded as any information should be prevented from exchange or loss.

The authentication protocol can has three phases, the first phase will be between the parcel tags (tag A, tag B, tag C, tag D) and the primary tag G. This authentication phase can prevent an adversary to eavesdrop the communication be by using Cramer-Shoup lite cryptosystem. Cramer-Shoup cryptosystem has the property that is secure against non-adoptive chosin cipher text attack which is considered as a high security definition

Usually, the back-end server is responsible for generating keys. Taking in consideration, the lite version Cramer-Shoup protocol is based on the intractable computation in the finite field, so the second phase will be based on generalised Cramer-Shoup lite to be able to send multi-tag's ID instead of send one by one ID. In this authentication phase the primary tag should send the tag's ID to the reader and the reader will authenticate the primary tags.

The third phase of authentication will be between the reader, the primary tags and the back-end server. The authentication will be done by sending the tag's ID and making a protocol to prevent other tag to be communicated with the reader. In multi tag's ID instead of sending one by one tag's ID.

The generalisation of the lite version of Cramer-Shoup can be done for $i = 1, \dots, n$ as follows: the sender selects a prime number $q \in G$ such that $p - 1 = 2q$ where p is also prime. Then choose $g1, g2 \in G$ and $x_i, y_i, a_i, b_i \in \{0 \dots .\text{q-1}\}$. Compute $h_i = g_1^{x_i}.g_2^{y_i}$ and $C_i = g_1^{a_i}$ and send to the receiver. The encryption process starts after choosing $m_i \in M \in Z_q$,where M is shared by using Shamir's secret sharing scheme, then randomly selects $r_i \in \{0, \dots . . q-1\}, then\ computes\ u_i = {g_1}^{r_i},\ v = {g_2}^{r_i}\ W = m_i h^{r_i}$, and $e_i = C_i^{r_i} = ({g_1}^{x_i}.{g_2}^{y_i})^{r_i}$. The cipher text is (u, v, w, e) and sends it back. The sender check if $e_i = u_i^{a_i}.v_i^{b_i}\ then\ m = \frac{W_i}{u^{x_i}v_i^{y_i}}\ otherwise\ m_i = \perp$.

CONCLUSION

The main purpose of this framework is to design an authentication protocol for multi-tag RFID system that can be used in supply chain management. As well as, ensuring the security and privacy for the RFID system. Firstly, the proposed scheme distributes the secret message by using Shamir's secret key during the authentication process. After that completes the encryption and decryption process by using the lite version of Cramer-Shoup cryptosystem. The lite version of Cramer-Shoup cryptosystem provides security of tags because of the property of achieving non-adaptive chosen cipher-text attack.

REFERENCES

Babaheidarian, P., Delavar, M., & Mohajeri, J. (2012, September). On the security of an ECC based RFID authentication protocol. In Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on (pp. 111-114). IEEE

Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007, March). Public-key cryptography for RFID-tags. In Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on (pp. 217-222). IEEE

Bringer, J., Chabanne, H., & Icart, T. (2008). Cryptanalysis of EC-RAC, a RFID identification protocol. In Cryptology and Network Security (pp. 149-161). Springer Berlin Heidelberg.

Bringer, J., Chabanne, H., & Icart, T. (2009, March). Efficient zero-knowledge identification schemes which respect privacy. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security* (pp. 195-205). ACM.

Cramer, R., & Shoup, V. (1998, January). A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Advances in Cryptology—CRYPTO'98 (pp. 13-25). Springer Berlin Heidelberg

Dimitriou, T. (2005, September). A lightweight RFID protocol to protect against traceability and cloning attacks. In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on (pp. 59-66). IEEE.

Hunt, V. D., Puglia, A., & Puglia, M. (2007). RFID: a guide to radio frequency identification. John Wiley & Sons.

Juels, A. (2004, March). "Yoking-proofs" for RFID tags. In Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on (pp. 138-143). IEEE.

Lee, Y. K., Batina, L., & Verbauwhede, I. (2008, April). EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In RFID, 2008 IEEE International Conference on (pp. 97-104). IEEE.

Lee, Y. K., Sakiyama, K., Batina, L., & Verbauwhede, I. (2008). Elliptic-curve-based security processor for RFID. Computers, IEEE Transactions on, 57(11), 1514-1527.

Lim, C. H., & Kwon, T. (2006). Strong and robust RFID authentication enabling perfect ownership transfer. In Information and Communications Security (pp. 1-20). Springer Berlin Heidelberg.

Malek, B., & Miri, A. (2012, June). Lightweight mutual RFID authentication. In Communications (ICC), 2012 IEEE International Conference on (pp. 868-872). IEEE.

Martínez, S., Valls, M., Roig, C., Miret, J. M., & Giné, F. (2009). A secure elliptic curve-based RFID protocol. Journal of Computer Science and Technology, 24(2), 309-318.

Masum, K. M., & Bhuiyan, F. (2013). Impact of Radio Frequency Identification (RFID) Technology on Supply Chain Efficiency: An Extensive Study. Global Journal of Researches In Engineering, 13(4).

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003, November). Cryptographic approach to "privacy-friendly" tags. In RFID privacy workshop (Vol. 82).

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The evolution of RFID security. IEEE Pervasive Computing, (1), 62-69.

Sandhya, M. and Rangaswamy, T. R. "A Forward Secured Authentication Protocol For Mobile", International Journal of Information Technology and Knowledge Management vol. 4, no. 2, pp. 549–553. 2011

Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

Tuyls, P., & Batina, L. (2006). RFID-tags for Anti-Counterfeiting. In Topics in cryptology–CT-RSA 2006 (pp. 115-131). Springer Berlin Heidelberg

Vaidya, B., Makrakis, D., & Mouftah, H. T. (2012, September). Robust RFID Authentication for Supply Chain Management. In Vehicular Technology Conference (VTC Fall), 2012 IEEE (pp. 1-5). IEEE.

Van Deursen, T., & Radomirovic, S. (2009). Untraceable RFID protocols are not trivially composable: Attacks on the revision of EC-RAC. IACR Cryptology ePrint Archive, 2009, 332.

Wei, C. H., Hwang, M. S., & Chin, A. Y. H. (2011). A mutual authentication protocol for RFID. IT Professional, (2), 20-24.

Weis, S. A. (2003). Security and privacy in radio-frequency identification devices (Doctoral dissertation, Massachusetts Institute of Technology).

Wolkerstorfer, J. (2005, July). Is elliptic-curve cryptography suitable to secure RFID tags. In Workshop on RFID and Lightweight Cryptography, Graz-August.

Zhang, X., Li, L., Wu, Y., & Zhang, Q. (2011, May). An ECDLP-Based Randomized Key RFID Authentication Protocol. In Network Computing and Information Security (NCIS), 2011 International Conference on (Vol. 2, pp. 146-149). IEEE.