Cryptography applications in protocols for RFID systems

Christiana Couto, Ronaldo Moreira Salles, Gabriela Moutinho de Souza Dias, Gustavo Claudio Karl Couto

Military Engineering Institute, Praça General Tibúrcio, 80, 22290-270, Praia Vermelha, Rio de Janeiro, RJ, Brasil. (christianacouto, salles, gabriela,gustavokcouto@ime.eb.br).

Abstract: Radio frequency identification systems are used in several applications for the unique recognition of objects. Due to the remote communication, malicious agents can read, alter and copy the transmitted information to damage the system. Therefore, researchers have created several protocols to protect these communications employing cryptographic techniques . Recently, Baashirah and Abuzneid proposed a serverless RFID authentication protocol (SLEC) based on elliptic curve cryptography to secure communication in RFID systems. Nevertheless, it has security vulnerabilities and its scalability is faulty. This work presents a comprehensive analysis that discusses the State of the Art of cryptographic applications in RFID systems and points out the SLEC protocol security and scalability issues.

Keywords: radio-frequency identification systems; cryptography; cryptographic protocols; RFID; information security;

1. INTRODUCTION

The radio frequency identification (RFID) systems are employed for uniquely object identification through radio frequency. They consist of tags, readers and a subsystem for data processing and storage. The tags are attached to objects and store the data, such as their IDs. Tags can be classified as active, in case an energy source is incorporated, or passive, if they are energized by the reader's magnetic field. Active tags are more expensive, but they can reach distances as far as a hundred meters. The readers require data from the tags and send it to the central subsystem (usually a back-end server) for processing (dos Santos, 2006).

The electronic product code (EPC) is an universal standard for product identification developed since 2003 by the EPCglobal Inc.. Tag identities can be discovered by a serial number, a bar code or a RFID system according to this standard as shown in Figure 1.

Currently, RFID systems are employed in many sectors such as financial, transports, logistics, healthcare, passports and access control (dos Santos, 2006; Zelbst, 2012; Ibrahim, 2017a). Nevertheless, the RFID systems have many security vulnerabilities, because an adversary can access the communication channel remotely to eavesdrop, read or tamper the messages being transmitted (Akgun, 2015; Akgün, 2015; Farzaneh, 2015a,b; Bilal, 2015). These attacks can be classified as active, when the adversaries can manipulate the transmitted data, or passive, when they can monitore it.

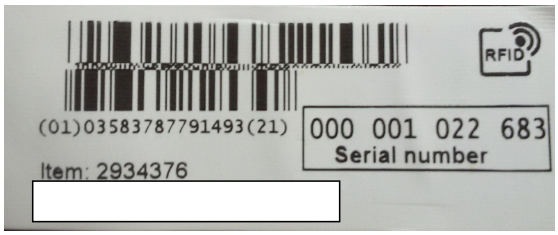

Figure 1. Tag containing a serial number, a bar code and an RFID tag

A solution for this problem is cryptography. The cryptographic objectives must be chosen according to the application context. For example, if financial data is transmitted, then many cryptographic schemes must be incorporated into the communication protocol to provide confidentiality and integrity.

On the other hand, employing cryptography is related to computational costs in a linear dependency. Therefore, as a system requires more security, the larger the costs for application management and hardware/software usage will became.

In order to protect RFID systems from more attacks, in 2019, Baashirah and Abuzneid proposed a serverless RFID authentication protocol (Baashirah, 2019). They claimed it could avoid replay attack, man- in-the-middle, eavesdropping, impersonate attack, trace- ability attack, desynchronization and denial of service but could adapt to large scale systems. Nevertheless, in this paper, we show

⋆ This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior- Brasil (CAPES) - Finance Code 001.

that their protocol is still vulnerable to attacks and has scalability issues.

Thus, the main contributions of this work are: comprehensively analyze the State of the Art of cryptographic applications in RFID systems and point out the SLEC protocol vulnerabilities and scalability issues.

This paper is divided as follows, then Section 2 describes the methodology and results of the bibliographic research about this topic. In section 3, the SLEC protocol is described and Section 4 its vulnerabilities and problems are pointed out. Finally, section 5 concludes this work.

2. RELATED WORK

This section details the bibliographic research made about the applications of cryptography in RFID systems.

2.1 Research methodology

Firstly, the bibliometric analysis was chosen as method to analyze and quantify the related bibliography (FREITAS, 2000). Then, the Dimensions database was selected, because it is commonly used for scientific productions, indexes many renown journals and is multidisciplinary.

The data collection was made in April 2021 employing as index terms "cryptography" and "radio frequency identification" in titles and abstracts. It was not defined any time range nor language filters, in order to recover all articles which descriptors are in English.

As result, 196 publications were recovered between 2007 and 2021. One can observe that the number of publications per year has grown as times goes by.

Then, these data was used as an input to the VOSViewer tool to find the most frequent terms in the recovered articles' titles and abstracts, considering at least thirty occurrences. After what, a map showing co-occurrence links between terms was produced, as shown in Figure 2 and a map describing from which countries the researches that have made more publications are (considering at least seven publications per country) was made as shown in Figure 3.

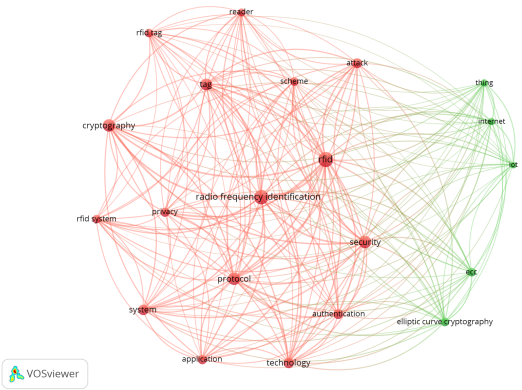

Figure 2. co-occurrence map of related terms generated by the VOSViewer

One can observe from Figure 2 that the more frequents terms are: security (122), protocol (117), tag (107), technology (89), system(84), attack (77), authentication (75) and privacy (70).

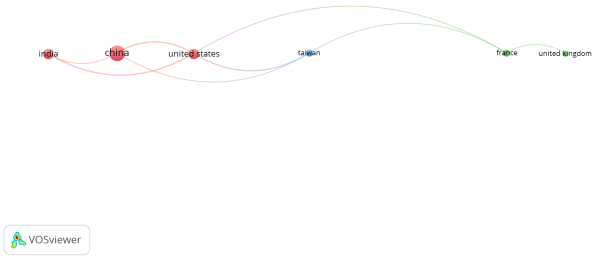

Figure 3. Countries from the researches that have made more publications elaborated by the VOSViewer

One can observe from Figure 3 that the most prominent countries are: China (46), United States (21), India (21), France (10), Taiwan (9) and the United Kingdom (7).

2.2 Premises

The following premises were selected for the bibliographic analyses:

- if the protocol provides confidentiality (1), integrity (2) and/or mutual (M)/ unidirectional (U) authentication (3);
- if hash functions are employed (4);
- if elliptic curve cryptography is employed (5); if so, if there is any optimization method for this algorithm (6);
- if the protocol scalability was considered (7);
- if timestamps were employed (8);
- if the transmission of more data than only the tag id was considered (9); and
- if the protocol is resistant against the following attacks: DoS (10), *Replay* (11), Impersonate (12), Man-in-the-Middle (13), tracking or tracing (14), desynchronization (15) and cloning (16).

2.3 Results

Table 1 shows the results of X related work. The symbols "T", "F", "?" e "-" mean that the respective premise is true, false, not informed or not applicable.

2.4 Discussion

All the researches considered have provided mutual authentication and confidentiality to the RFID systems, but only a part have shown attention towards integrity.

The scalability issue was considered in many works. It is a research trend. It was considered as future work by Al-Adhami, 2016. In some protocols, the back-end server must

Table 1. Bibliographic analysis about the State of the art of cryptographic applications in RFID systems

-	Ibrahim (2017a)	Mansoor (2019)	Baashirah (2018)	Al-Adhami (2016)	Baashirah (2019)
1	T	T	T	T	T
2	T	?	?	T	T
3	M	M	M	M	M
4	T	F	F	F	M
5	T	T	T	F	F
6	T	-	T	F	T
7	F	T	T	?	T
8	F	T	F	F	?
9	T	?	?	?	T
10	T	T	T	?	T
11	T	T	T	?	T
12	T	T	?	T	T
13	?	T	?	T	T
14	T	T	T	T	T
15	T	?	?	T	T
16	T	?	?	?	?

make a linear search for the tag ID in the database which causes scalability issues. One solution is to group the tags as made by Mansoor, 2019 and Baashirah, 2018).

Hash functions, elliptic curve cryptography and timestamps were employed in some works.

Only two protocols made considerations about the transmission of more data besides the tag ID.

The replay, tracking and Denial-of-Service were the most important attacks in the security evaluations.

It was also identified that many protocols have not been implemented, although their efficiency is evaluated by means of estimating the number of operations and the number of bits transmitted.

3. THE BASELINE PROTOCOL DESCRIPTION

This section reviews the baseline protocol of Baashirah and Abuzneid proposed in the work"SLEC: A Novel Serverless RFID Authentication Protocol Based on Elliptic Curve Cryptography" (Baashirah, 2019) and describes its vulnerabilities. Table 2 introduces the notations used in the SLEC protocol.

The baseline protocol aims to mutually authenticate RFID tags and readers in a scalable network. For that matter, tags groups must be created and each reader must receive a list containing data about all tags in the group for which it has access rights.

The tag and it group identities can be updated at each session between a tag and a server. Therefore, tags must store the current and last values of their group identities. A pseudo random number generator (PRNG) is employed to generate the random numbers for that and instead of the tag's EPC, a pseudo-identity is used.

SLEC consists of three phases: initialization, authentication and renewal. It is based on the elliptic curve cryptography, employing the Diffie-Hellman algorithm. It is considered a serverless protocol, because the participation of the server is unnecessary during the authentication step.

Table 2. SLEC protocol notation

Notation	Description
G	Additive group of prime order in an elliptic curve
Z_q	Finite field
P	Generator point
$y_{prv}, r_{prv}, t_{prv}$	Server, reader and tag private keys (r and $t \in Z_q$)
$Y_{pub}, R_{pub}, T_{pub}$	Server, reader and tag private keys
X_i	Tag identity
G_k	Group identity
T_s	Timestamp

3.1 The baseline protocol initialization phase

The SLEC protocol initialization phase scheme is shown in Figure 4.

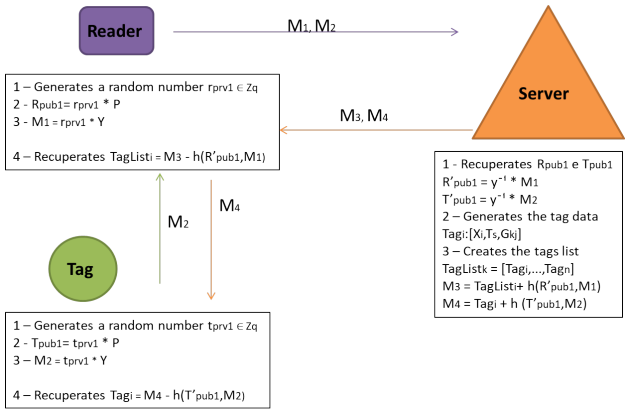

Figure 4. The SLEC protocol initialization phase

Firstly, reader and tag generate random numbers that shall be used to create their private keys r_{prv}, t_{prv}. After, their public keys R_{pub} and T_{pub} will be created by multiplying the private keys to the generator point. Then, the public keys will be multiplied by the server public key, Y, and sent to the server.

Then, the server will reply with the tag data: temporary identity, timestamps and group identity. For the reader, the server sends list of tags in its group.

3.2 The baseline protocol authentication phase

The authentication phase scheme is shown in Figure 5.

During this phase, the server is offline. Initially, the reader generates new private and public keys r_{prv2} and R_{pub2}. After, it sends its group identity, its public key and a timestamp encrypted to the tag.

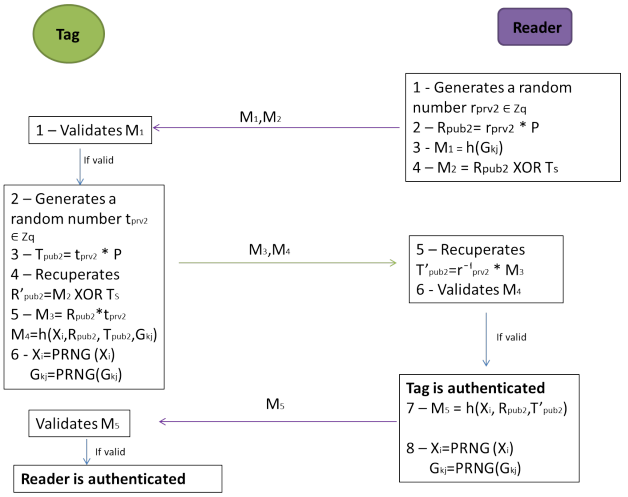

Figure 5. SLEC protocol authentication phase

After receiving these data, the tag verifies if the group identity is the same as its own. If they are equal, then the tag generates new private and public keys t_{prv2} and T_{pub}. After what, it recuperates the reader public key.

In the sequence, the tag sends its new private key, multiplied by the reader public key, its public key and its temporary identity. At the same time, the group and tag identities are updated.

After receiving these data, the reader recuperates the tag public key and validates its authenticity. Then, it updates the values of the tag and group identity and send a new message to the tag containing its new identity and public key.

The relationship $R_{pub1} = y^{-1}M_1$ can be obtained through the following steps:

$$\begin{cases} R_{pub1} = r_{prv1} * Pe \\ Y = y * P, then P = Y * y^{-1} \\ R_{pub1} = r_{prv1} * Y * y^{-1}, then \\ R_{pub1} * y = r_{prv1} * Y * y^{-1} * y = r_{prv1} * Y \\ M_1 = r_{rprv1} * Y = R_{pub1} * y, then \\ M_1 * y^{-1} = R_{pub1} * y * y^{-1} = R_{pub1} \end{cases} \quad (1)$$

In an analogue way, the relationship $T_{pub1} = y^{-1}M_2$ can be obtained.

The renewal phase happens in case some secret information is compromised. Then, tag and reader must communicate once more with the server to update their data.

4. EVALUATION OF THE BASELINE PROTOCOL

4.1 Security vulnerabilities

Some vulnerabilities that can be found in the SLEC protocol are the following:

(1) Messages M_1 and M_2 are not authenticated;
(2) As Baashirah et al have pointed out, the protocol security depends on the server public key protection, which is stored in all the tags and readers. If this information is captured by an attacker, which could be the case in a compromise attack, then all the protocol could be compromised;
(3) The protocol security depends on the security of its PRNG that generates the private keys and the tags/groups temporary identities. Nevertheless, the authors didn't evaluate the PRNG security. If an attacker is able to deduce the PRNG sequence, then the identities would be found and the system could become vulnerable to personification and tracking attacks; and
(4) SLEC needs to keep public keys as secrets, but according to the concept of public key cryptography they should be publicly available without risk to security.

Those vulnerabilities could be explored by an adversary in the following manners:

(1) The server public key can be found through the message M_2 by trying different timestamps, taking advantage of probable known time intervals;
(2) If the reader public key is found and compromised, then by intercepting M_3 messages, the tags' public keys will be disclosured;
(3) Fake messages, equivalent to M_1 and M_2, can be sent as a form of Denial-of-Service attack;
(4) An exhaustive search could be performed in order to find the finite field and the generator point by sending random numbers, until an authentication with the server is succeeded; and
(5) The security evaluation about tracking attacks is wrong because an adversary can still track the tags by traffic analysis considering they transmit more information after they answer the reader request.

4.2 Scalability evaluation

Besides the security vulnerabilities pointed out in the previous subsection, there is a scalability problem in the SLEC protocol: the identities of the tag groups are updated every session individually, then if one tag is updated more times then the others, its identity will become a value not recognized by the others. Then, the reader would only authenticate the value of the group identity corresponding to the tag that has been updated more times and this value predecessor. Therefore, the values prior to these two wouldn't be considered as valid anymore and the other tags wouldn't be validated.

This should be corrected by making the update only available for the entire group at once.

This process is shown in Figure 6. In this example, tag 1 is updated four times. Then, the reader won't authenticate tags 2 and 3, whose group identity value is still the initial one. As the group authentication is the first authentication performed by the tag, then this problem would stop the whole protocol run.

5. CONCLUSION

This work performed a study about the applications of cryptography in RFID systems. After a bibliographic research, their main cryptographic objectives identified were confidentiality and mutual authentication.

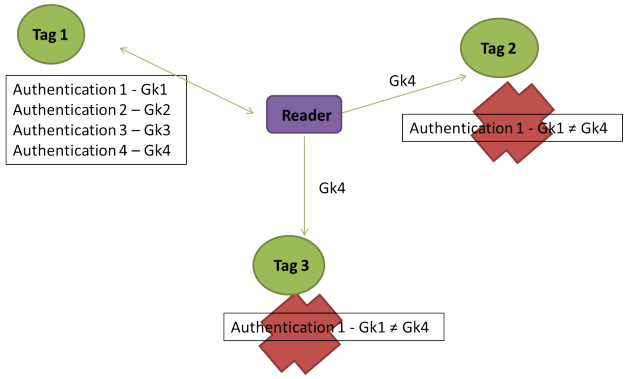

Figure 6. Scalability problem in the SLEC protocol

After the State of the Art analysis, the SLEC protocol was evaluated and many of its vulnerabilities were found such as the lack of authentication in some messages. Also, the SLEC protocol has scalability issues when tags in the same group are authenticated more times than others.

Future work will propose a new protocol based on the solutions for the problems find in the baseline protocol

REFERENCES

Agrahari, Abhay e Varma, S. (2019). Authentication in rfid scheme based on elliptic curve cryptography. In -, –.

Ahamed, Sheikh e Rahman, F.e.H.E. (2008). Erap: Ecc based rfid authentication protocol. *Future Trends of Distributed Computing Systems, IEEE International Workshop*, 0, 219–225. doi:10.1109/FTDCS.2008.20.

Akgün, Mete e Bayrak, A.O.e.c.M.U. (2015). Attacks and improvements to chaotic map-based RFID authentication protocol. *Security and Communication Networks*, -, –. URL -. -.

Akgun, Mete e Caglayan, M.U. (2015). Weaknesses of two RFID protocols regarding de-synchronization attacks. In *International Wireless Communications and Mobile Computing Conference IWCMC – 2015*, –. Dubrovnik, Croatia. URL -. -.

Al-adhami, Ayad e Ambroze, M.e.S.I.e.T.M. (2019). An effencient improvement of rfid authentication protocol using hash function zkp. In -, 87–92. doi:10.1109/SCCS.2019.8852614.

Al-Adhami, Ayad e Ambroze, M.e.S.I.e.T.M. (2016). A quorum system for distributing rfid tags. In *UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld*, 510–517. IEEE Computer Society. URL `http://dblp.uni-trier.de/db/conf/uic/uic2016.html`. -.

Alz, Mishall e Zhang, Z.e.Z.J. (2019a). Efficient and secure ecdsa algorithm and its applications: A survey. *International Journal of Communication Networks and Information Security*, 11, 7–35.

Alz, Mishall e Zhang, Z.e.Z.J. (2019b). Efficient and secure ecdsa algorithm and its applications: A survey. *International Journal of Communication Networks and Information Security*, 11, 7–35.

Andrew S. Tanenbaum, D.J.W. (2010). Computer networks. -, 13, 960. -.

Baashirah, Rania e Abuzneid, A. (2019). Slec: A novel serverless rfid authentication protocol based on elliptic curve cryptography. *Electronics*, 10, 1166. doi:10.3390/electronics8101166.

Baashirah, R.e. (2018). Improve healthcare safety using hash-based authentication protocol for rfid systems. –. doi:10.1109/UEMCON.2018.8796656.

Benssalah, Mustapha e Djeddou, M.e.D.K. (2018). A secure rfid authentication scheme for healthcare environments based on digital signature algorithm. In -, –. doi:10.1109/ISNCC.2018.8530914.

Bilal, Z. (2015). *Addressing Security and Privacy Issues in Low-Cost RFID Systems*. Ph.D. thesis, Royal Holloway, University of London, London, UK.

Brasil (2019). Glossário de segurança da informação. URL -. Seção 1, p. 3.

Chen, Chunling e Wang, Y.e.Y.H.e.Q.X.H. (2016). The rfid mutual authentication scheme based on ecc and otp authentication. In -, 1–4. doi:10.1109/ICUWB.2016.7790568.

Chien, H.Y. (2007). Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *IEEE Trans. Dependable Secur. Comput.*, 4(4), 337–340. URL `http://dblp.uni-trier.de/db/journals/tdsc/tdsc4.html`. -.

Colbach, G. (2018). *RFID Handbook: Technology, Applications, Security and Privacy*.

CUNHA, A. (2019). A planta mecatrime: uma plataforma para ensino, pesquisa, desenvolvimento e inovação em sistemas mecatrônicos e indústria 4.0.

Deebak, B D e Al-Turjman, F.e.M.L. (2019). A hash-based rfid authentication mechanism for context-aware management in iot-based multimedia systems. *Sensors*, 19(18), 3821. doi:10.3390/s19183821. URL `https://app.dimensions.ai/details/publication/pub.1120876583andhttps://www.mdpi.com/1424-8220/19/18/3821/pdf`. -.

Deursen, Ton e Radomirovic, S. (2008). Attacks on rfid protocols. *IACR Cryptology ePrint Archive*, -, 310.

dos Santos, L.M. (2006). *Contribuição do uso da RFID na cadeia de suprimentos: aplicação na distribuição de Pára-quedas*. Ph.D. thesis, Instituto Militar de Engenharia, Rio de Janeiro, Brasil. -.

e L. Fillatre e I. Nikiforov e P. Willett, V.L.D. (2017). Security of scada systems against cyber–physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, 32(5), 28–45.

Farzaneh, Yousof e Azizi, M.e.D.M.e.M.A. (2015a). Vulnerability analysis of two ultra lightweight RFID authentication protocols. *International Arab Journal of Information Technology*, 12(4), 340–345.

Farzaneh, Yousof e Azizi, M.e.D.M.e.M.A. (2015b). Vulnerability analysis of two ultra lightweight rfid authentication protocols. *International Arab Journal of Information Technology*, 12, 340–345.

FREITAS, H.M.R. (2000). *Revista de Administração-RAUSP*, 35(3).

González-Tablas Ferreres, A. (2013). A taxonomy and survey of attacks on digital signatures. *Computers Security*, 34, –.

Hankerson, D e Menezes, A.e.V.S. (2004). *Guide to Elliptic Curve Cryptography*.

He, Debiao e Wang, H.e.K.M.K.e.W.L. (2016). Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography.

IET Communications, 10(14), 1795–1802. URL http://dblp.uni-trier.de/db/journals/iet-com/iet-com10.html. -.

He, Debiao e Kumar, N.e.C.N.e.L.J.H. (2014). Lightweight ecc based rfid authentication integrated with an id verifier transfer protocol. *J. Medical Systems*, 38(10), 116. URL http://dblp.uni-trier.de/db/journals/jms/jms38.html. -.

Ibrahim, Alaauldin e Dalkiliç, G. (2017a). An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for rfid, proven on wisp. *J. Sensors*, 2017, 2367312:1–2367312:10. URL http://dblp.uni-trier.de/db/journals/js/js2017.html. -.

Ibrahim, Alaauldin e Dalkiliç, G. (2017b). Review of different classes of rfid authentication protocols. *Wireless Networks*, 25(3), 961–974. URL http://dblp.uni-trier.de/db/journals/winet/winet25.html9. -.

Ju, S. (2012). A lightweight key establishment in wireless sensor network based on elliptic curve cryptography. In -, 138–141. doi:10.1109/ICADE.2012.6330115.

Kaur, Kuljeet e Kumar, N.e.S.M.e.O.M.S. (2016). Lightweight authentication protocol for rfid-enabled systems based on ecc. In *GLOBECOM*, 1–6. IEEE. URL http://dblp.uni-trier.de/db/conf/globecom/globecom2016.html. -.

Kim, Cheol-Joong e Yun, S.Y.e.P.S.C. (2010a). A lightweight ecc algorithm for mobile rfid service. *Ubiquitous Information Technologies and Applications (CUTE), 2010 Proceedings of the 5th International Conference on*, 6, 1–6. doi:10.1109/ICUT.2010.5678170.

Kim, Cheol-Joong e Yun, S.Y.e.P.S.C. (2010b). A lightweight ecc algorithm for mobile rfid service. *Ubiquitous Information Technologies and Applications (CUTE), 2010 Proceedings of the 5th International Conference on*, 6, 1–6. doi:10.1109/ICUT.2010.5678170.

Kim, SungJin e Kim, Y.e.P.S. (2007). Rfid security protocol by lightweight ecc algorithm. In *ALPIT*, 323–328. IEEE Computer Society.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9(3), 49–51.

Lara-Nino, Carlos e Díaz-Pérez, A.e.M.S.M. (2018). Elliptic curve lightweight cryptography: a survey. *IEEE Access*, PP, 1–1. doi:10.1109/ACCESS.2018.2881444.

Li, Zhongke e Zhao, H.e.S.X.e.W.C. (2018). Asymmetric cryptography based unidirectional authentication method for rfid. In -, 374–3743. doi:10.1109/CyberC.2018.00073.

Mansoor, Khwaja e Ghani, A.e.C.S.e.S.S.e.G.S.e.M.A. (2019). Securing iot-based rfid systems: A robust authentication protocol using symmetric cryptography. *Sensors*, 19, 4752. doi:10.3390/s19214752.

Menezes, Alfred J. e van Oorschot, P.C.e.V.S.A. (2001). *Handbook of Applied Cryptography*. CRC Press.

Pinol, Oriol Pinol e Raza, S.e.E.J.e.V.T. (2015). Bsd-based elliptic curve cryptography for the open internet of things. In M. Badra, A. Boukerche, and P. Urien (eds.), *NTMS*, 1–5. IEEE. URL http://dblp.uni-trier.de/db/conf/ntms/ntms2015.html. -.

Refsdal, Atle e Solhaug, B.e.S.K. (2015). *Cyber-systems*, 25–27. doi:10.1007/978-3-319-23570-7_3.

Shen, Zuming e Zeng, P.e.Q.Y.e.C.K.K.R. (2018). A secure and practical rfid ownership transfer protocol based on chebyshev polynomials. *IEEE Access*, 6(-), 14560–14566. doi:10.1109/access.2018.2809480. URL https://app.dimensions.ai/details/publication/pub.1101227543andhttps://doi.org/10.1109/access.2018.2809480. -.

SIEMENS (2020). Um guia prático sobre a indústria 4.0.

Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Prentice Hall Press, USA, 5th edition.

Unemyr, M. (2017). *The Internet of Things – The Next Industrial Revolution Has Begun: How IoT, big data, predictive analytics, machine learning and AI will change our lives forever n.* publisher.

Wei, Lili e Luo, Z.e.Q.Q. and He, Qing e Xu, J. (2014). A low-cost pkc-based rfid authentication protocol and its implementation. In *CIS*, 415–419. IEEE Computer Society. URL http://dblp.uni-trier.de/db/conf/cis/cis2014.html. -.

Xiao, Liang e Xu, H.e.Z.F.e.W.R.e.L.P. (2020). Skinny-based rfid lightweight authentication protocol. *Sensors*, 20, 1366. doi:10.3390/s20051366.

YÁñEZ, F. (2017). *The Goal is Industry 4.0: Technologies and Trends of the Fourth Industrial Revolution*.

Yoonjeong, KIM e OHM, S.e.K.Y. (2009). Privacy-preserving rfid authentication using public exponent three rsa algorithm. *IEICE Transactions on Information and Systems*, E92.D(3), 545–547. doi:10.1587/transinf.e92.d.545. URL https://app.dimensions.ai/details/publication/pub.1068093387andhttps://www.jstage.jst.go.jp/article/transinf/E92.D/3/E92.D_3_545/_pdf. -.

Zelbst, P. (2012). *RFID for the Supply Chain and Operations Professional (The Supply and Operations Management Collection)*. Business Expert Press.