Advanced Lightweight Cryptography for Automotive Security: Surveys, Challenges and Solutions

Phuc Tran and Duc Cuong Nguyen
HCL Vietnam, Vietnam

Keywords: Lightweight Cryptography, Automotive Security, Authenticated Encryption, CEASAR.

Abstract: Recently, automotive embedded systems have become strong principles of computing, along with an increasing need for secure communication. The rapid development of the V2X (Vehicle-to-Everything) technology for the entity's interconnection leads to the rise of attack surface and the demand for cryptographic security standard. In addition, the requirement of having secure automotive services and devices against not only current but also future attacks are emerged. Unfortunately, providing robust, secure solutions for automotive embedded systems still faces big challenges. Because of the distinctive characteristics and infrastructures of the vehicular networks, the requirements for automotive security are far more complicated as compared to other type of networks, such as conventional wireless networks, and mobile networks. In this paper, we present a comprehensive survey of the developments in automotive security from the perspective of lightweight cryptographic solutions, including lightweight algorithms and lightweight protocols. Furthermore, security challenges, issues and their cryptographic countermeasures as well as limitations of future automotive industry are also discussed. These strategies can be flexibly adapted to meet strict security levels of automotive security in the future.

1 INTRODUCTION

In recent years, the swift progress of technology for automotive industry from the high extent of automation and the remarkable attempt for the goal of autonomous driving, confronts a dramatic change. This transformation leads to the requirements of providing secure hyper-connectivity among the entities in vehicular networks. Consequently, automotive security becomes key concern for automotive embedded systems in the future.

Authentication and verification of data, especially of big data exchanged among vehicles and their related entities (devices or applications) deserve utter attention. Besides, the secrecy and confidentiality of entity's information also needs to be evaluated as it can only be accessed and transferred by trusted parties. The difference between conventional networks, like wireless network or mobile network and vehicular network is the continuity and availability over time, as the automotive entities (services and applications) need to be accessed and all the time when authorities needed, while other networks' programs can be disconnected on specific occasion.

Although certain cryptographic algorithms, such as public-key infrastructure (PKI) and elliptic curve cryptography (ECC) offer strong protection against different network attacks, they may not be employed straightly in vehicular networks because of their high mobility and particular network characteristics.

Furthermore, the tight requirements in constrained environments inhere the mass developments of smart devices that impedes the development of new lightweight cryptographic algorithms for automotive security. New lightweight standards are required to perform strong security mechanism, encryption/ decryption, with low power applications and other functionalities for the automotive embedded systems.

This paper aims at giving an overview on the advancements of vehicular network and providing visions on the lightweight cryptographic solutions. Based on our study of the latest lightweight cryptography in automotive systems, our paper includes necessary aspects to consider when designing a suitable lightweight standard for automotive security, and covers most of the effective lightweight methods such as lightweight block cipher, lightweight stream cipher, lightweight hashes, dedicated authenticated encryption, and lightweight protocols employed for VANET architecture as well. We further present a compre-

Tran, P. and Nguyen, D.
Advanced Lightweight Cryptography for Automotive Security: Surveys, Challenges and Solutions.
DOI: 10.5220/0011109500003194
In *Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS 2022)*, pages 304-311
ISBN: 978-989-758-564-7; ISSN: 2184-4976

hensive understanding of challenges and countermeasures in security of automotive embedded systems.

The paper is organized as follows: In Section 2, we present the background of automotive embedded systems as well as their challenges, and discuss countermeasures and related limitations of the current automotive security. Lightweight cryptographic solutions for automotive security are characterized in Section 3. Section 4 presents discussions of future directions of lightweight cryptography for automotive. Finally, we give concluding remarks in Section 5.

2 BACKGROUND

In this section, we briefly present automotive embedded system architecture and summarize primary challenges and issues related to vehicular networks applied to this architecture. Certain solutions and limitations are discussed afterwards.

2.1 Challenges and Issues of Automotive Networks

Automotive networks require the corresponding systems to provide (close-to) instant responses. Hence, one of the key points to consider is the real-time functionalities that can assist in controlling systems. The systems, necessarily, should provide two main features: predictability and reliability. To this end, preserving the predictability with ECUs faces principal challenges as calling for low data rates and low computational resources when providing security. Although many existing proposals that provided security with advancements in computational capacity and bandwidth were presented, their application to the automotive systems is still under consideration.

Furthermore, in automotive networks, multicasting and broadcasting are generally used for message transmission between multiple receivers, simultaneously. As the result, the functional capabilities of existing automotive communication protocols are required to be improved in terms of messages' authorization for all targeted receivers.

Additionally, intermittent connectivity is another challenge for automotive security. Employing asymmetric cryptography and security certificates is a method to address this challenge, as enabling modules to ensure their own security approaches without asking for any external connections between in-vehicle components and external devices (such as a central server).

Last but not least, most internal transmission in vehicular network is also insecure. Components do not typically use cryptographic techniques within their features and, if possible, they generally employ encryption/ decryption procedure across a wide variety of vehicles and ECUs with the same keys. Although authentication process is essentially applied when re-executing ECUs, conventional data transmissions are rarely encrypted or authenticated. This leads to high possibility for attackers to exploit, as presented in (Checkoway et al., 2011), (Miller and Valasek, 2014a), (Othmane et al., 2014).

2.2 Countermeasures and Limitations

2.2.1 Intrusion Detection, Network Analysis and Verification

An Intrusion Detection System (IDS) for vehicle was presented in (Miller and Valasek, 2014b) to discover irregularities in the vehicular network by regularly comparing traffic to a standard.

Entropy-based approach (Muter and Asaj, 2011) was employed to detect attacks without calling for any predefined models of the attacks. The attackers, conversely, can make the intrusion detection works remarkable harder as they make an effort to confuse their attacks by masking or hiding their purposes with some firmware modification or injection techniques, as in (Miller and Valasek, 2015) and (Miller and Valasek, 2016).

To authenticate the internal transmission in vehicular networks, (Sojka et al., 2014) proposed an architecture which combines assessment of safety and security requirements, called AUTomotive Open System ARchitecture (AUTOSAR). And, in (Mundhenk et al., 2015b), a probabilistic checking framework which depends on the standard security assessment AUTOSAR, was presented to estimate the automotive security.

2.2.2 Security Integration

Existing approaches often employed symmetric cryptography to limit the overhead when adding security in vehicular networks as well as in automotive embedded systems. One of the effective techniques was to use Message Authentication Codes (MACs). It allowed fast and efficient computation, especially on ECUs with limited computational power (Lin et al., 2013). In (Han et al., 2014), a proposal which mapped the MACs with FlexRay protocol was presented, called TESLA. Although this protocol supported delivering authentication for targeted symmetric mechanisms, it could not provide authorization as well as validation for communication streams and communication partners. Moreover, the concept of integrating a CMAC with Cyclic Redundancy Check (CRC) to automotive systems was proposed in (Zalman and Mayer, 2014). This model supported the vehicular networks in reducing the overhead and adapting to the requirements of authentication and integrity. Furthermore, another approach was presented by (Jiang et al., 2012), as utilizing a pre-shared key in symmetric cryptography each automotive systems' phase, to ensure real-time response. Other models, such as in (Herber et al., 2014) leveraged the advantages of Virtual CANs (VCANs) to split network traffic in the consumer and corporate domain.

2.2.3 Limitations

The requirement of real-time response in the vehicular networks leads to the failure of existing protocols that were proposed for conventional networks, as these protocols cannot deliver high throughput performance, low latency, and message reliability. In addition, the connected ECUs in CAN protocols which broadcast information through CAN bus, require data/payload sizes as small as 64-bit block. In this manner, a lightweight standard with 64-bit block size and 128-bit key size is considered as the best instance to meet real-time requirements in constrained environment of vehicular networks and automotive systems. Recently, many researchers have paid attention to developing lightweight cryptographic standards and key generation schemes that ensure the security for vehicular networks with high performance (Mundhenk et al., 2017), (Shen et al., 2018).

3 LIGHTWEIGHT CRYPTOGRAPHIC SOLUTIONS FOR AUTOMOTIVE SECURITY

Lightweight cryptography separates into various instances, including lightweight stream cipher, lightweight block cipher, lightweight hashing, and dedicated authenticated encryption version, with specific security requirements for each instance. In this section, we present a summary of various lightweight algorithms and lightweight protocols for automotive embedded systems, which can be found in the literature.

3.1 Lightweight Block Cipher

Hong et al.'s research (Hong et al., 2013) presented a lightweight algorithm `LEA` which is suitable for multiple devices with constrained resources. Besides, several block ciphers have been proposed in existing research to meet better performance results in hardware and software implementations such as `mCrypton` (Lim and Korkishko, 2005), `SEA` (Standaert et al., 2006), `CLEFIA` (Shirai et al., 2007), `KLEIN` (Gong et al., 2011), `XTEA` (Yu et al., 2011), `LED` (Guo et al., 2011b), `PICCOLO` (Shibutani et al., 2011), `PRINCE` (Borghoff et al., 2012), `RoadRunneR` (Baysal and Sahin, 2015), `RECTANGLE` (Zhang et al., 2015), `SPARX` (Dinu et al., 2016) and `SKINNY` (Beierle et al., 2016).

Extensively, some of these were tailored and enhanced by optimizing structural components of traditional block ciphers to upgrade their performance. For example, `DESL` (Leander et al., 2007) is a `DES` lightweight instance, which is designed from conventional `DES` construction. In `DESL`, the authors utilized a single S-box in a round function instead of iterating eight rounds, which makes a difference to initial and final permutation generation to improve hardware implementation. Additionally, `SIMON` and `SPECK` (Beaulieu et al., 2015), which are other lightweight block ciphers, are constructed in various block sizes and key sizes. Both proposals are flexible with multiple platforms and result well across a variety of lightweight applications. Furthermore, some lightweight block ciphers are also presented in (Université du Luxembourg, 2017).

Small Block Size and Small Key Size. Corresponding to the structure of lightweight block cipher, the block size and key size are required to be small for constrained resource adaption and performance benefits. Generally, it should be less than 64-bits rather than 128-bits. In particular, the more block size and key size decreases, the more plaintext and power consumption limits. For instance, `PRESENT` (Bogdanov et al., 2007) is designed with 80-bits key size, and `TWINE` (Hosseinzadeh and Hosseinzadeh, 2016) is tailored with 80/128-bits key size.

Simple Key Schedule and Simple Function. Due to the fact that the lightweight block ciphers perform simpler computation operations rather conventional block cipher models, the structural functions and rounds should be constrained in lightweight rational designs. For instance, a single S-box 4-bit S-boxes can be utilized instead of 8-bit S-boxes for lightweight target. In addition, a simple key schedule which generates sub-keys, is also needed as low-resource limitation. In this manner, some lightweight cryptography proposals are as follows: `PRESENT` uses 4-bit S-boxes, while `Hummingbird2` (Mohd et al., 2015) and

Iceberg (Standaert et al., 2004) have only four function rounds, or (Yu et al., 2011) divides 128-bits master key into four 32-bits sub-keys.

3.2 Lightweight Stream Cipher

Stream ciphers are also motivating primitives for lightweight standards. The eSTREAM (ECRYPT 2017) was organized by the European Network of Excellence for Cryptology for finding novel stream models that may be appropriate for boundless adoption. Among the final candidates in 2008, the three stream ciphers of Trivium (Cannière, 2006), Grain (Hell et al., 2007) and MICKEY (Babbage and Dodd, 2008) performed good results for hardware applications with limited resources. Some other lightweight stream ciphers are Enocoro-80 (Watanabe et al., 2008), A2U2 (David et al., 2011), WG-8 (Fan et al., 2013) and Sprout (Armknecht and Mikhalev, 2015).

3.3 Lightweight Hash Function

It is more difficult to develop and perform a lightweight hash function than a lightweight ciphers. The hash functions generally require a larger internal state which is suitable for conventional systems than other cryptographic algorithms, but this feature would be costly on limited resource systems.

In 2010, Armknecht and Mikhalev proposed using lightweight hash function in RFID protocols (Armknecht and Mikhalev, 2010). A traditional hash function uses internal state with large size and costly power consumption, which may not be suitable for resource-constrained applications. Therefore, Guo et al. presented lightweight algorithm PHOTON in 2011 (Guo et al., 2011a) based on block cipher model. Some other lightweight hash functions are Armadillo (Badel et al., 2010), SPONGENT (Bogdanov et al., 2011), QUARK (Aumasson et al., 2013a) and BLAKE2S/B (Aumasson et al., 2013b).

Small Output Size. One of the critical requirements when designing a secure lightweight hash function is large size enough to offering collision resistance, especially birthday attack protection. For applications do not require collision resistance in structure, internal and stabilize sizes may be used. On the other hands, the secure hash functions not only pay attention to collision resistance, but also need to provide strong protection against preimage, second image and impact attacks. This feature can decrease the range of internal state.

Small Message Size. The large capacity of conventional hash functions can be used to support the advantages of 264-bits size utilizing in structure. From a lightweight hash viewpoint, the size should be much smaller (e.g., at most 256-bits). In this manner, hash functions that are improved for short messages may be more suitable for lightweight applications.

3.4 Dedicated Authenticated Encryption

Authenticated encryption (AE) is a type of symmetric key cryptography. This model ensures security approaches, as confidentiality, authenticity, and integrity as well. The specific characteristics of the AE architecture leads to a smaller area and lower power consumption for hardware implementation. These features are advantageous for constrained devices, as only the encryption procedure is required to encrypt/decrypt the data (as no decryption procedure is needed to verify the integrity of the message), combining with MAC function (in terms of block or hash) to provide the integrity and authenticity.

- **POET/ POE** (Abed et al., 2014): is a family of On-Line Authenticated Encryption proposals. This approach is suitable for low end applications since it allows using a single core processor. POET/POE is efficient for high end devices and provides high throughput on multi core architecture. POET is ensure security against nonce misuse and decryption misuse.
- **AES-GCM** (Arun et al., 2015) is a standardized authenticated Galois/Counter mode (GCM). This approach provides authenticity and confidentiality, achieved by a universal hash function and AES model, respectively. A unique nonce is used in AES-GCM for each key. AES-GCM are high speed at low cost, low latency, parallelism, and efficient software and hardware implementation.
- **AEGIS** (Wu and Preneel, 2016): AEGIS is a dedicated authenticated encryption proposal. This approach is constructed from AES encryption round functions, but not the last round. Its speed is faster than AES in both the CTR mode and CBC mode. AEGIS supports Parallel AES round functions at each step, so it's suitable for fast software and hardware implementations. Furthermore, AEGIS protects a packet as leaving the packet header unencrypted.
- **ACORN** (Wu, 2016): ACORN is an authenticated encryption proposal which depends on linear feedback shift registers (LFSR). This approach used for lightweight applications that has limited

resources and for high performance applications. ACORN separates the processing of associated data and the plaintext/ ciphertext, as no requirements of checking the message length (associated data, plaintext or ciphertext) and message padding to a multiple of block size which lowers the cost of hardware implementation.

- **MORUS** (Wu and Huang, 2016): MORUS is an approach of dedicated authentication cipher. The design of MORUS depends on stream ciphers' design which covers a small number of operations in the state update function. The generated key and nonce aim to shield only one message, while the state size and key generation function contribute to enhancing security against cipher attacks. This proposal shows good results in hardware performance by employing only AND, XOR, and rotation operations in the update function. For the software implementation results, MORUS is also efficient model as presenting good performance across platforms.
- **ASCON** (Dobraunig et al., 2016): Ascon has been selected as the primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR competition (2014–2019) and is currently competing in the NIST Lightweight Cryptography competition (2019).
- **Deoxys** (Tean et al., 2016): Deoxys is a family of authenticated encryption proposal which depends on a tweakable block cipher (Deoxys-BC). This approach has two authentication and encryption models: (a) Deoxys-I for non-repeating nonce, and (b) Deoxys-II for the nonce repeating version. Deoxys performs well for small messages which is suitable for lightweight applications. It shows reasonable results on hardware and software implementation, and ensures good security for all its parameters.
- **AEZ** (Hoang et al., 2017): AEZ is presented as an authentication encryption scheme. This approach provides strong security and usability features. AEZ is parallelizable proposal which performs with a computational cost close to the AES-CTR model. Additionally, the associated data of AEZ can be an arbitrary strings while the nonce and key cover a variable length.
- **SAEAES** (Naito et al., 2018): This approach belongs to a family of authenticated encryption algorithm, and was submitted to the Lightweight Cryptography Project of National Institute of Standards and Technology (NIST). It has a minimum state size since the state size equals to a block size. There is no demand for an inverse to do decryption. Besides, only XOR is needed for a block cipher encryption and it is an online cipher, i.e. a data block is processed only once.

3.5 Lightweight Cryptography Used for VANET Security

VANETs are ad hoc routing protocols that implement wireless transmission by mixing the concepts of both ad hoc network proposal and wireless communication medium. The two fundamental wireless terminals of the VANETs, On-Board Unit (OBU) and Road Side Unit (RSU), take action as nodes within a wireless network to support in receiving and relaying messages. Hence, the connections between the OBUs and RSUs are established to achieve safety services, such as traffic or weather information in real-time and cautions of collision, as the targeted RSUs act as wireless access points and the embedded OBUs support in communicating with other RSUs or OBUs.

Furthermore, every sent messages and received messages are validated in a vehicular network through the nodes to add the security approach to all automotive services and devices.

Corresponding to the asymmetric and symmetric cryptography, some lightweight protocols have been proposed to improve the automotive security and to satisfy the VANET's security requirements in the future.

- **OTC** (Dacosta et al., 2012): One-Time Cookie (OTC) protocol is an approach which aims at protecting the vehicular system from SID theft and session hijacking. This protocol ensures security features as providing tokens for every request and also applying HMAC with them for the request to avoid token reuse.
- **Adriadne** (Hu et al., 2005): This approach is based on Dynamic Source Routing (DSR) protocol. The Ariadne model ensures security between nodes' communication by using one-way hash function and MAC. Authentication is enabled by using shared key.
- **RobSAD** (Chen et al., 2009): The RobSAD protocol provides an efficient approach for Sybil attack detection. In Sybil attack, several replications of a node, with numerous identities and various positions, are sent simultaneously that leading to network confusion and illegal agreement. In RobSAD approach, Sybil node is recognized when more than one node have same motion routes, as different vehicles driven by different drivers cannot carry same motion models.

- **SEAD** (Mutalik et al., 2016): Secure and Efficient Ad hoc Distance (SEAD) protocol depends on active destination sequenced distance vector (DSDV) routing. This approach protects against incorrect routing and ensures authentication using one-way hash function. Particularly, to elude continuing route and to guarantee route freshness, destination-sequence number is utilized. In addition, the SEAD protocol executes median node hashing to certify the authenticity of each route.
- **ECDSA** (Manvi et al., 2009): Elliptical Curve Digital Signature (ECDS) algorithm utilizes digital signature. This approach ensures security and authenticity for automotive system by using asymmetric operations with hash function. The agreement is required for both sender and receiver upon elliptical curve parameters.
- **ARAN** (Sanzgiri et al., 2002): Authenticated Routing for Ad hoc Network (ARAN) was inspired from Ad hoc On-demand Distance Vector (AODV) protocol. A new node that wants to access to the vehicular network has to send a certificate request to the third-party CA for a signed certificate. All certified nodes are issued with the CA's public-key. ARAN ensures the authentication's discovery and the freshness of the vehicular route by using asymmetric algorithms and timestamps, respectively.

4 DISCUSSIONS

The life span of cars is much longer than other related-IT systems that benefits in frequently updated technologies and services. Hence, although deploying cryptographic algorithms are important for ensuring security purpose of the cars, there are still areas to be considered in future research works, as the cryptanalysis possibility is increased due to outdated employed technologies, when the automotive devices applied on cars are not easy to be substituted.

Furthermore, the key security concerns for future automotive industry are to construct comprehensive methods of both utilization and optimization targets applied for vehicular networks extensively. There is an urgent demand for realizing malicious threats and exploring effective solutions to ensure automotive security by either developing new lightweight cryptographic standards or employing existing proposals in efficient ways. Some directions could be considered as the following:

- *Cipher construction and performances:* A key concern should be considered comprehensively on the security features of the standard is to evaluate the increase of round number and round complexity within architecture design of the cipher.
- *Security metrics for new security standard:* There does not exist any security metrics that can accurately ensure cryptographic security. Recently, many attackers with advanced cryptanalysis techniques can break encryption/ decryption procedures. It calls for clear lightweight standards for enhancing the security of constrained applications in automotive systems.

5 CONCLUSION

In this study, we presented a comprehensive survey on the role of lightweight cryptography for automotive security. In addition, we discussed challenges, issues, and countermeasures as well as limitations of future directions for open research. We also have gone over lightweight cryptographic solutions, including lightweight algorithms and lightweight protocols in terms of algorithm name and type, cryptanalysis, and security metrics. It is important to develop more secure and lightweight encryption algorithms that have a smaller key size, fast processing, and require less computation power.

Our work calls for actions to validate how effective these solutions are and if it is possible to implement them in automotive systems. In addition, algorithms for automotive embedded systems which suitable for cutting-edge security standards like ISO 21434 and ISO26262 should be developed.

REFERENCES

Abed, F., Weimar, B., Foley, J., Forler, C., List, E., Lucks, S., and Wenzel, J. (2014). The poet family of on-line authenticated encryption schemes. In *CAESAR*.

Armknecht, F. and Mikhalev, V. (2010). A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-lw. In *International Conference on Information Security and Cryptology*. Springer.

Armknecht, F. and Mikhalev, V. (2015). On lightweight stream ciphers with shorter internal states. In *Inter. Workshop on Fast Software Encryption*. Springer.

Arun, V., Vanisree, K., and Reddy, D. L. (2015). Implementation of aes-gcm encryption algorithm for high performance and low power architecture using fpga. In *International Journal of Research and Applications*.

Aumasson, J., Henzen, L., Meier, W., and Naya-Plasencia, M. (2013a). Quark: A lightweight hash. In *Journal of Cryptology*.

Aumasson, J., Neves, S., Wilcox-O'Hearn, Z., and Winnerlein, C. (2013b). Blake2: Simpler, smaller, fast as md5. In *International Conference on Applied Cryptography and Network Security*. Springer.

Babbage, S. and Dodd, M. (2008). The mickey stream ciphers. In *New Stream Cipher Designs*. Springer.

Badel, S., Dagtekin, N., Nakahara, J., Ouafi, K., Reffé, N., Sepehrdad, P., Susil, P., and Vaudenay, S. (2010). Armadillo: A multi-purpose cryptographic primitive dedicated to hardware. In *Workshop on Cryptographic Hardware and Embedded Systems*. Springer.

Baysal, A. and Sahin, S. (2015). Roadrunner: A small and fast bitslice block cipher for low cost 8-bit processors. In *Lightweight Cryptography for Security and Privacy*. Springer.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L. (2015). The simon and speck lightweight block ciphers. In *52nd Design Automation Conference*. IEEE.

Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., and Sim, S. M. (2016). The skinny family of block ciphers and its low-latency variant mantis. In *Annual International Cryptology Conference*. Springer.

Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., and Verbauwhede, I. (2011). Spongent: A lightweight hash function. In *Workshop on Cryptographic Hardware and Embedded Systems*. Springer.

Bogdanov, A., Knudsen, L., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., and Vikkelsoe, C. (2007). Present: An ultra-lightweight block cipher. In *International workshop on cryptographic hardware and embedded systems*. Springer.

Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S., and Yalçin, T. (2012). Prince–a low-latency block cipher for pervasive computing applications. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer.

Cannière, C. (2006). Trivium: A stream cipher construction inspired by block cipher design principles. In *International Conference on Information Security*. Springer.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., and Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *USENIX*.

Chen, C., X.Wang, W. H., and Zang, B. (2009). A robust detection of the sybil attack in urban vanets. In *Conference on Distributed Computing Systems*. IEEE.

Dacosta, I., Chakradeo, S., Ahamad, M., and Traynor, P. (2012). Onetime cookies: preventing session hijacking attacks with stateless authentication tokens. In *ACM Transactions on Internet Technology*.

David, M., Ranasinghe, D., and Larsen, T. (2011). A2u2: a stream cipher for printed electronics rfid tags. In *International Conference on RFID*. IEEE.

Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., and Biryukov, A. (2016). Design strategies for arx with provable bounds: Sparx and lax. In *Conference on the Theory and Application of Cryptology and Information Security*. Springer.

Dobraunig, C., Eichlseder, M., Mendel, F., and Schläffer, M. (2016). Ascon. In *CAESAR competition*.

Fan, X., Mandal, K., and Gong, G. (2013). Wg-8: A lightweight stream cipher for resource-constrained smart devices. In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*. Springer.

Gheraibia, Y., Kabir, S., Djaffi, K., and Krimou, K. (2018). An overview of the approaches for automotive safety integrity levels allocation. In *Journal of Failure Analysis and Prevention*.

Gong, Z., Nikova, S., and Law, Y. W. (2011). Klein: a new family of lightweight block ciphers. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Springer.

Guo, J., Peyrin, T., and Poschmann, A. (2011a). The photon family of lightweight hash functions. In *Annual Cryptology Conference*. Springer.

Guo, J., Peyrin, T., Poschmann, A., and Robshaw, M. (2011b). The led block cipher. In *Workshop on Cryptographic Hardware and Embedded Systems*. Springer.

Han, G., Zeng, H., Li, Y., and Dou, W. (2014). Safe: Security-aware flexray scheduling engine. In *DATE*.

Hell, M., Johansson, T., and Meier, W. (2007). Grain: a stream cipher for constrained environments. In *International Journal of Wireless and Mobile Computing*.

Herber, C., Richter, A., Wild, T., and Herkersdorf, A. (2014). A network virtualization approach for performance isolation in controller area network (can). In *Real-Time and Embedded Technology and Applications Symposium (RTAS)*. IEEE.

Hoang, V. T., Krovetz, T., , and Rogaway, P. (2017). Aez v5: Authenticated encryption by enciphering. In *CAESAR*.

Hong, D., J. Lee, D. K., Kwon, D., Ryu, K., and Lee, D. (2013). Lea: A 128-bit block cipher for fast encryption on common processors. In *International Workshop on Information Security Applications*. Springer.

Hoppe, T., Kiltz, S., and Dittmann, J. (2008). Adaptive dynamic reaction to automotive it security incidents using multimedia car environment. In *Information Assurance and Security*.

Hosseinzadeh, J. and Hosseinzadeh, M. (2016). A comprehensive survey on evaluation of lightweight symmetric ciphers: Hardware and software implementation. In *Advances in Computer Science Journal*.

Hu, Y. C., Perrig, A., and Johnson, D. B. (2005). Ariadne: a secure on-demand routing protocol for ad hoc networks. In *Wireless Networks*.

Jiang, K., Eles, P., and Peng, Z. (2012). Co-design techniques for distributed real-time embedded systems with communication security constraints. In *DATE*.

Leander, G., Paar, C., Poschmann, A., and Schramm, K. (2007). New lightweight des variants. In *International Workshop on Fast Software Encryption*. Springer.

Lim, C. and Korkishko, T. (2005). mcrypton – a lightweight block cipher for security of low-cost rfid tags and sensors. In *International Workshop on Information Security Applications*. Springer.

Lin, W., Zhu, Q., Phung, C., and Sangiovanni-Vincentelli, A. (2013). Security-aware mapping for canbased real-time distributed automotive systems. In *Conference on Computer-Aided Design*. IEEE.

Manvi, S. S., Kakkasageri, M. S., , and Adiga, D. G. (2009). Message authentication in vehicular ad hoc networks: Ecdsa based approach. In *International Conference on Future Computer and Communication*.

Miller, C. and Valasek, C. (2014a). A survey of remote automotive attack surfaces. In *Black Hat*.

Miller, C. and Valasek, C. (2014b). Survey of remote automotive attack surfaces. In *Black Hat*.

Miller, C. and Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. In *http://illmatics.com*.

Miller, C. and Valasek, C. (2016). Advanced can injection techniques for vehicle networks. In *Blackhat*.

Mohd, B., Hayajneh, T., and Vasilakos, A. (2015). A survey on lightweight block ciphers for low-resource devices: comparative study and open issues. In *Journal of Network Computing Application*.

Mundhenk, P., Paverd, A. J., Mrowca, A., Steinhorst, S., Lukasiewycz, M., Fahmy, S. A., and Chakraborty, S. (2017). Security in automotive networks: Lightweight authentication and authorization. In *ACM Transactions on Design Automation of Electronic Systems*.

Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S. A., and Chakraborty, S. (2015a). Lightweight authentication for secure automotive networks. In *Conference on Design, Automation and Test in Europe*.

Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S. A., and Chakraborty, S. (2015b). Security analysis of automotive architectures using probabilistic model checking. In *Design Automation Conference*.

Mutalik, P., Nagaraj, S., Vedavyas, J., Biradar, R. V., , and Patil, V. G. C. (2016). A comparative study on aodv, dsr and dsdv routing protocols for intelligent transportation system (its) in metro cities for road traffic safety using vanet route traffic analysis (vrta). In *International Conference on Advances in Electronics, Communication and Computer Technology*. IEEE.

Muter, M. and Asaj, N. (2011). Entropy-based anomaly detection for in-vehicle networks. In *Intelligent Vehicles Symposium*. IEEE.

Naito, Y., Matsui, M., Sugawara, T., and Suzuki, D. (2018). Saeb: A lightweight blockcipher-based aead mode of operation. In *IACR Transactions on Cryptographic Hardware and Embedded Systems*.

Nilsson, D., Phung, P., and Larson, U. (2008). Vehicle ecu classification based on safety security characteristics. In *IET Road Transport Information and Control*.

Othmane, L. B., Fernando, R., Ranchal, R., Bhargava, B., , and Bodden, E. (2014). Likelihood of threats to connected vehicles. In *International Journal of Next-Generation Computing (IJNGC)*.

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. In *International Conference on Network Protocols*. IEEE.

Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., , and Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. In *Journal of Network and Computer Applications*.

Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., and Shirai, T. (2011). Piccolo: an ultra-lightweight blockcipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. (2007). The 128-bit blockcipher clefia. In *International Workshop on Fast Software Encryption*. Springer.

Sojka, M., Krec, M., and Hanzalek, Z. (2014). Case study on combined validation of safety amp; security requirements. In *International Symposium on Industrial Embedded Systems (SIES)*. IEEE.

Standaert, F.-X., Piret, G., Gershenfeld, N., and Quisquater, J. (2006). Sea: A scalable encryption algorithm for small embedded applications. In *International Conference on Smart Card Research and Advanced Applications*. Springer.

Standaert, F.-X., Piret, G., Rouvroy, G., Quisquater, J., and Legat, J. (2004). Iceberg: An involutional cipher efficient for block encryption in reconfigurable hardware. In *International Workshop on Fast Software Encryption*. Springer.

Tean, J., Nikolic, L., T.Peyrin, and Y.Seurin (2016). Deoxys. In *CAESAR competition*.

Université du Luxembourg (2017). Lightweight block ciphers. In *https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers*.

Watanabe, D., Ideguchi, K., Kitahara, J., Muto, K., Furuichi, H., and Kaneko, T. (2008). Enocoro-80: a hardware oriented stream cipher. In *International Conference on Availability, Reliability and Security*.

Wu, H. (2016). Acorn: a lightweight authenticated cipher. In *CAESAR competition*.

Wu, H. and Huang, T. (2016). The authenticated cipher morus. In *CAESAR competition*.

Wu, H. and Preneel, B. (2016). Aegis: A fast authenticated encryption algorithm. In *CAESAR competition*.

Yu, J., Khan, G., and Yuan, F. (2011). Xtea encryption based novel rfid security protocol. In *24th Canadian Conference on Electrical and Computer Engineering*.

Zalman, R. and Mayer, A. (2014). Secure but still safe and low cost automotive communication technique. In *Design Automation Conference*.

Zapata, M. G. and Asokan, N. (2002). Securing ad hoc routing protocols. In *ACM Workshop on Wireless Security*.

Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., and Verbauwhede, I. (2015). Rectangle: A bit-slice lightweight block cipher suitable for multiple platforms. In *Science China Information Sciences 58, 12*. Springer.