On Track of Sigfox Confidentiality with End-to-End Encryption

Radek Fujdiak
Brno University of Technology
Brno, Czech Republic
fujdiak@vutbr.cz

Petr Blazek
Brno University of Technology
Brno, Czech Republic
blazekpetr@phd.feec.vutbr.cz

Konstantin Mikhaylov
University of Oulu
Oulu, Finland
konstantin.mikhaylov@oulu.fi

Lukas Malina
Brno University of Technology
Brno, Czech Republic
malina@vutbr.cz

Petr Mlynek
Brno University of Technology
Brno, Czech Republic
mlynek@vutbr.cz

Jiri Misurec
Brno University of Technology
Brno, Czech Republic
misurec@vutbr.cz

Vojtech Blazek
Brno University of Technology
Brno, Czech Republic
xblaze32@stud.feec.vutbr.cz

ABSTRACT

The last years brought many novel challenges for the Internet of Things (IoT). Low capital and operational expenditures, massive deployments of devices, reliability and security are among the most crucial ones. The recently introduced Low-power wide area (LPWA) technologies provide one possible way of addressing these challenges. In the current paper, we focus on one of the most mature LPWA technology, namely Sigfox. We provide a brief security assessment of this technology and highlight the main security imperfections. Notably, we also consider the recent changes introduced in the last revision of the Sigfox specification released in the fourth quarter of 2017. Importantly, this paper discusses the highlighted issues and compares three selected cryptographic encryption solutions (AES, ChaCha and OTP) in respect to the main IoT triad of performance, security and cost. We investigate the encryption solutions and characterize their energy consumption in a real-life implementation. The results herein presented are useful for understanding the cost of enabling security aspects and enable selecting the most efficient encryption protocol.

CCS CONCEPTS

• **Security and privacy → Block and stream ciphers**;

KEYWORDS

IoT, LPWAN, Sigfox, Security, Encryption, Symmetric cipher, AES, ChaCha, One time pad, Low-power

ARES 2018, August 27–30, 2018, Hamburg, Germany

ACM ISBN 978-1-4503-6448-5/18/08…$15.00
https://doi.org/10.1145/3230833.3232805

ACM Reference Format:
Radek Fujdiak, Petr Blazek, Konstantin Mikhaylov, Lukas Malina, Petr Mlynek, Jiri Misurec, and Vojtech Blazek. 2018. On Track of Sigfox Confidentiality with End-to-End Encryption. In *ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3230833.3232805

1 INTRODUCTION

The Internet of Things (IoT), where objects are capable to communicate with each other without any human interaction [7], is a current trend in communication technologies and will become an important component of the future. In the past years, the interest in this area grew exponentially, which is also confirmed by the results from our keyword analysis displayed in Figure 1. Moreover, Figure 1 shows also the growing interest in security related to IoT (more than half of the items found for the keyword "Internet of Things" also refer to security).

The high interest in the IoT Security is caused by the exponential growth of IoT objects and their fast deployment, which often causes various vulnerabilities [10] and gives rise to different security challenges [37]. Nowadays, the Low Power Wide Area Networks (LPWAN) are among the most discussed technologies for IoT

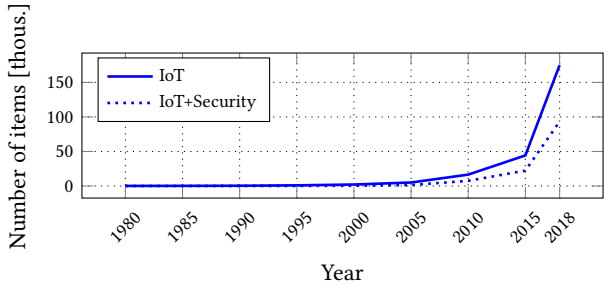

Figure 1: Results of keyword search for the term "Internet of Things" and "Internet of things"+"Security" in Google Scholar for selected years 1980–2018.

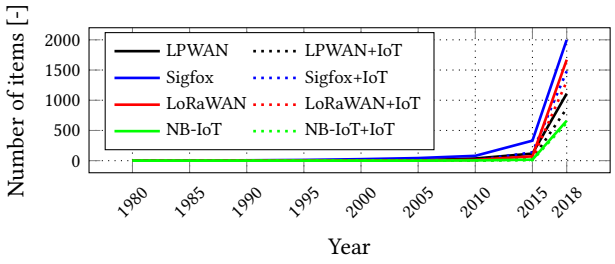

Figure 2: Results of keyword search for LPWAN and IoT in Google Scholar for selected years 1980–2018.

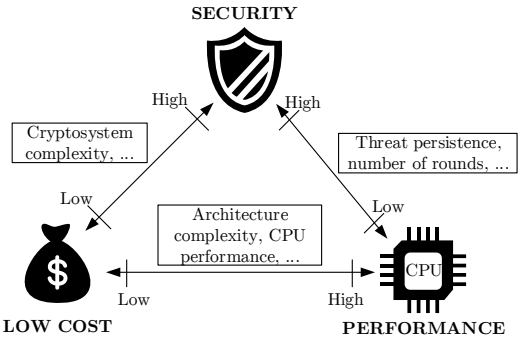

Figure 3: Example of the security, performance, low-cost triad.

and represent a novel communication paradigm [26]. LPWANS are typically characterized among others by limited energy, low cost, and lower security level. The LPWAN was reported by Ericsson in November 2017 mobility report as a communication technology with the highest compound annual growth rate (CAGR) among all other IoT technologies [21]. The growing interest for LPWAN (also in area of IoT) is also displayed in Figure 2. The keyword search was carried out for IoT, LPWAN and three main technologies - Sigfox, Long Range Wide Area Network (LoRaWAN) and Narrowband-IoT (NB-IoT). Most of the items dealing with LPWAN also refer to the Internet of Things.

The LPWANs are low-cost, low-power, long-range communication technologies developed for harvesting information from millions of nodes. However, the LPWAN follows also the trend known from the IoT and entails several security issues such as lack of adequate support of over-the-air updates, no encryption for application payload (potential eavesdropping), and generally low complexity of security [17, 26].

This paper focuses on providing the most up to date information about one of the most adopted LPWAN technology Sigfox together with recent news from Q4/2017. Moreover, we provide security assessment for the cryptographic algorithms used in the communication chain and highlight the imperfections and critical issues. Furthermore, we provide one of the first analysis of consumption and time complexity for the suggested cipher by Sigfox documentation for end-to-end encryption and also provide suggestions of different alternatives. The key contribution of this paper is to bring together original theoretical and practical results, which should help with future research and also address the user issues in this very specific LPWAN technology. Additionally, we provide in-depth discussion on the security issue of Sigfox and propose also future directions of the research.

The remainder of this paper is organized as follows. In the following section, we describe the technical specifics of Sigfox technology and also provide discussion on security issues and challenges. Our proposed solution to deal with unsolved confidentiality is included in Section 3. In Section 4, the laboratory environment and used methods are introduced. The main results of this paper are placed in Section 5. They are followed by a discussion, conclusion and suggestions for future research in Section 6.

2 BACKGROUND

2.1 Description of Sigfox technology

As previously said, we are focusing on one of the most mature LPWAN technology Sigfox, which is a proprietary technology owned by same named French company Sigfox Inc, which follows the business-to-business (B2B) model in order to provide communication service similar to the cellular one across the world. This technology is very limited due to its low data rate of 100 bps, max. payload of 12/8 octets (up/down) and a max. of 140/4 (up/down) transmissions per day [2, 11, 17]. IoT is based on the three main principle so-called triad of security, performance and low cost (Figure 3) [9] as same as to the limited Sigfox. Therefore, there always need to be a good balance between all three parameters of this triad. This paper focuses on improving the security of Sigfox with minimal impact on performance or cost.

2.2 Related Studies

Several papers are discussing the security issues of Sigfox. However, they do not get deep into details. Poursafar *et. al* [24] point out the fact that Sigfox is proprietary solution with higher potential risk. Moreover, Centenaro *et. al* [6] comes to a very similar finding adding that Sigfox is leaving the final security on the user. From a real security assessment point of view, Sigfox security solution is based on the following key components [32–34]:

- Static manufacturer key, the so-called Porting Authorization Code (PAC), which is employed while registering devices to the network (re-generated after use).
- Unique device identifier (ID), which is used together with the unique Network Authentication Key (NAK) generated by the server in a Cipher-based Message Authentication Code function (CMAC) for device authentication.
- Message Integrity Code (MIC) with a size of 2–5 bytes, which is calculated from a message payload and ensures the message integrity together with a sequence number provided by basic counter for message freshness.
- Each message is sent three times to provide service availability, but there is no acknowledgment.

Furthermore, the Sigfox documentation discusses the encryption by means of the symmetric cipher AES-128 in a stream counter mode (CTR) [32]. However, this encryption is not yet implemented and it does not provide the application layer end-to-end encryption from the sensor to the end-user. This imperfection might hinder the usage of Sigfox in the context of more critical applications, where private and sensitive data is transferred.

3 PROPOSED SOLUTIONS

Due to their very specifics and features, the security solution for LPWAN systems in general, and for SigFox in particular, should be [3, 16, 25, 30, 38]:

- Low-power - Sigfox technology uses battery powered sensors with lifetime of several years. This means that is crucial to find ciphers with low computational complexity, and low time and power requirements.
- No heading - Sigfox has payload limitations of 12 B, which leaves no extra space for all sorts of overheads. Therefore, the final ciphers should not increase the message payload by additional or redundant data such as control counts, stamps or others.
- Low data rate and message limitation - Sigfox has data rate of 100/600 bps (uplink/downlink) and max. 140/4 messages per day (uplink/downlink). This means that it is vital to focus on ciphers, which do not require additional communication or information exchange. Moreover, the message delivery is naturally unreliable - any packet may get lost and the system must be able to handle it. This means to focus on ciphers without needs of acknowledgments or public parameters exchange.
- Low price - Sigfox is a low-cost solution for end-users, any increase of device price (even a relatively low one) might exclude the device from the final market.
- Low memory - Most of the Sigfox devices are often simple sensors with very limited memory capacity. Therefore, the final solution should minimize the memory requirements as much as possible.

As one can see from the list above, such often-used solutions as asymmetric cryptography or elliptic curve cryptography do not fit well for LPWANs. The asymmetric cryptography works mostly with high key-lengths, which is not suitable for small Sigfox payload of 12 B. Furthermore, the elliptic curve algorithms are based on the parametric exchanges, which does not suite to the Sigfox limited number of message transmissions. Due to these reasons, the limitations of Sigfox exclude most of the modern algorithms and leave the use of the symmetric ciphers as the only possibility.

The symmetric cryptosystems use one secret keys for both decryption and encryption. The modern symmetric cryptosystems are divided into two categories: (i) the block ciphers, and (ii) the stream ciphers. The block symmetric ciphers see the message as a n-block, where n is a non-zero number of blocks. There are also block ciphers with very small sized blocks such as Tiny Encryption Algorithm (TEA [36], XTEA [20], or XXTEA [29]) or padding techniques, which help to fill empty blocks. However, these techniques add additional complexity to the final solution or impacting the performance/cost (i.e. using only part of the payload). Therefore, we will search in the area of symmetric stream ciphers.

The Advanced Encryption Standard (AES), which is supported and widely used, also supports the stream mode, the so called Counter mode (CTR). AES was recommended in the Sigfox documentation as a one of the options. However, Bernstein [5] introduced the new stream cipher ChaCha in 2008, which is based on the Salsa cipher and should be faster than the AES cipher. In any case, Sigfox is a step back from the traditional continuous communication to ad-hoc periodical communication. Therefore, we might consider also the nontraditional and unconventional ciphers. Shannon *et. al* [31] introduces in 1949 very strong notion of perfect secrecy for the One Time Pad cipher (OTP), which is based on the Vernam Cipher introduces by Miller [4] and reinvented by Vernam in [35]. The proof of perfect secrecy for OTP is discussed in Appendix A. The OTP has very specific requirements:

- all used keys must be truly random, therefore a true random number generator (TRNG) is required,
- the key generation and exchange must be done via a trusted channel,
- each key must be at least as long as the message,
- the keys must remain secret and should be used only once then they should be securely deliminated.

For the modern systems, the major problem referred to the OTP is the number of keys. Nevertheless, Sigfox covers only a limited number of messages and the communication has periodical character. Moreover, Sigfox nodes have limited power and battery life-time, which we can use for computing the maximal number of messages. Counting 5 years of lifetime [19] and a maximum of 140 messages per day, then we get 255 500 of message, which equals 3.066 MB (considering 12 B payload). This stands for maximum number of message, but the typical periodicity of Sigfox communication is even lower, e.g., one message per day. Therefore, the Sigfox naturally deals with the main OTP challenge. In the rest of the paper, we will consider the three selected ciphers: (i) AES-128-CTR, (ii) Cha-Cha20, and (iii) OTP:

- AES-128 was selected as a recommended cipher from many standards (i.e. recommendation for federal information systems and organizations - NIST SP800-53 [27], or by guide to industrial control systems security - NIST SP800-82 [13]) and the CTR mode come out from the recommendation of the last Sigfox technical report on security [32].
- The ChaCha20 was selected as a promising and relatively new stream cipher, which should give better performance compared to the AES cipher [5].
- Last but not least, the selection of OTP cipher was motivated by Occam's Razor, a principle attributed to the logician William of Ockham: "*All things being equal, the simplest solution tends to be the best one.*" and basic thought of theoretical physicist Albert Einstein: *"Everything Should Be Made as Simple as Possible, But Not Simpler"*. We believe that OTP might be the simplest possible answer to the confidentiality imperfection of Sigfox.

4 EXPERIMENTAL SETUP

Sigfox is operator based technology, therefore, the Czech national Sigfox network was used for the presented experimental measurements from operator SimpleCell. The SimpleCell claims to have coverage of 95 % population and coverage of 92 % land. Moreover, the service provide 99+ % availability. The measurement were taken in Brno with 100 % success rate (100 messages sent/received).

As a hardware, we used customized Arduino UNO board with low-power components (see Figure 4). The main parts are: 8-bit AVR CMOS microcontroller ATMEGA328P-PU [1] (up to 0.1 µA in sleep mode, max. 20 MHz), real time clock RTC - MCP7940N-I/P (up to 1.4 µA in sleep mode) [18], temperature sensors DS18B20 (up to 0.75 µA in sleep mode) [8], Sigfox node WISOL SFM10R1 (up to 2 µA sleep mode) [15]. Moreover, the ATMEGA328-PU has function of "Programming Lock for Software Security" to provide simple protection for the firmware. This hardware setup provides an appropriate environment for the implementation with very low power consumption. For the measurement, we were considering the frequency of ATMEGA328P-PU of 4, 8 and 16 MHz.

As a firmware (software), we used an open-source cryptography library for Arduino boards - Arduino Cryptography Library [28]. This library contains, among the others, the block cipher AES-128 with stream mode CTR (128-bit key and 4 B of IV used for block counting) and stream cipher ChaCha20 (8 B nonce, 8/12/20 rounds with 128/256-bit key) [28]. Both encryption algorithms suite the requirements established already in Section 3. Additionally, we also use our own library with implementation of OTP (see Algorithm 1) and own implementation of the communication stack.

We are using the precomputed keys, which are considered to be loaded within the manufacturing process in the secure memory.

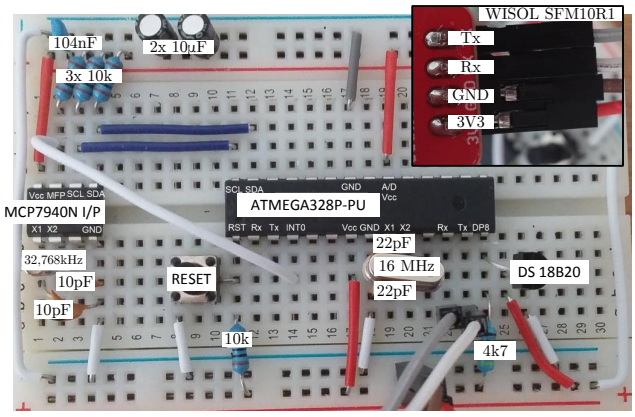

Figure 4: Our low-power hardware setup based on the Arduino UNO board and used for the measurements.

Algorithm 1 One Time Pad Encryption

Require: One time key $k \in \{0,1\}^n$, message $m \in \{0,1\}^n$, where n is size of k, m
Ensure: Ciphertext $c \in \{0,1\}^n$
1: **for** $(i \leftarrow 0)$ **to** $n-1$ **do**
2: $\quad c_i \leftarrow m_i \oplus k_i$
3: **end for**
4: **return** c

This will ensure that the TRNG does not need to be a part of the final sensor. Instead, the keys can be generated in by TRNG placed in server with higher computational capacity. Moreover, each key k is deleted after first use (and the table is shifted). The synchronization between server and client is handled by the message sequence number, which we also use to keep synchronization between client-server key-table.

Finally, the experiment was conducted in laboratory environment with 25°C and the high quality DC Power Analyzer N6705B from Agilent (Keysight) Technologies [14] was used to monitor the current consumption profiles of the test device. The used sample size was 1.00352 ms for initial communication measurements and 81.92 µs for measuring the encryption algorithms. The voltage level was set to 3 V. The monitored values were power consumption represented by average current I_{curr_avr} (the N6705B measure multiple current values and average them) and time consumption t of each method.

5 EXPERIMENTAL RESULTS

5.1 Initial measurements

The initial measurement was focused on the investigation of the encryption general impact in context of the whole communication process. The results are displayed in Figure 5. We compared scenarios without (NON) and with encryption (AES, the AES-128-CTR was selected as a reference of secure system). The experiment was as follows. Firstly, the sensor wake up from deep-sleep, consumption for which is constant (equals value of 9 µA) and then the initialization phase starts (first peak, approx. 10 mA) and data process (second peak, approx. 8 mA), where also the encryption is present. Followed by three main peaks, which are representing the transmission of the three repetitions of one Sigfox message (each approx. 60 mA for 12 B payload). The most power demanding process is the transmission also in comparison to the encryption, which has only negligible impact to the final power consumption. The high power consumption is caused by transmission time (<5 sec) and necessary additive modules such as radio module. We can see that lowering the number of messages per day is the crucial part for the application and battery-life time. Moreover, we show the efficiency of selected algorithms and final impact on the power consumption of additive encryption (which needs just the CPU).

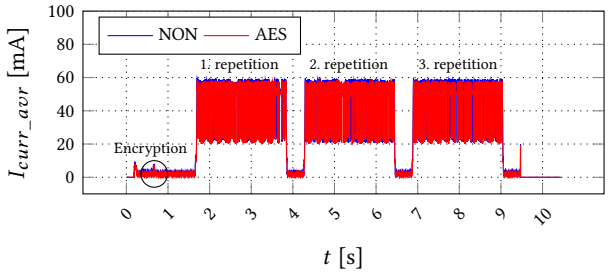

Figure 5: Results of power consumption measurement for communication system with and without encryption.

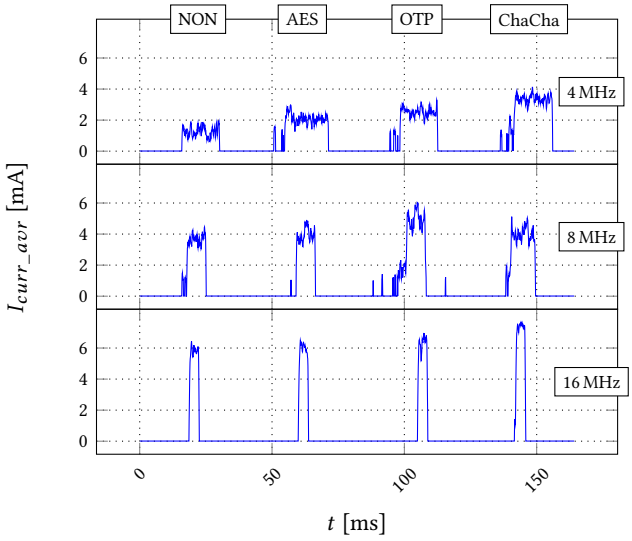

Figure 6: Results for measurement of impact of different ciphers on power consumption of communication stack for 4/8/16 MHz CPU frequency.

5.2 Encryption Consumption Analysis

To clearly see the impact of the encryption, we conducted measurement focused only on the encryption part, where we compared three selected ciphers AES, ChaCha and OTP. Also, different CPU frequency was utilized (4/8/16 MHz) to simulate scenarios of different IoT nodes with different performance. The results are displayed in Figure 6. The CPU frequency has obvious impact on the power consumption. A system without encryption (NON) has mean consumption of 2/4/6 mA consumption for 4/8/16 MHz (linear dependency) with very similar characteristic of systems with encryption. The least power demanding algorithm is AES-128-CTR with power consumption very close to the system without encryption (mean of 2.5/4.5/6.5 mA for 4/8/16 MHz). Followed by OTP with mean of 3/5/7 mA for 4/8/16 MHz and ChaCha20/20 with mean of 3.5/4.5/7.5 mA for 4/8/16 MHz. The mean speed of each cipher was for 4/8/16 MHz as follows: AES-128-CTR - 17.5/8.0/3.8 ms, OTP - 16.3/8.4/3.8 ms and ChaCha20/20 - 16.5/9.5/3.8 ms. The measurements show that OTP is the fastest solution for the lower CPU frequencies and AES the fastest for the higher CPU frequencies.

6 CONCLUSION

The applications that require a stronger SigFox security level must solve end-to-end confidentiality, and data authentication and integrity. The data that is exchanged between end devices and the SigFox infrastructure (i.e. in a radio part) must be secured in the same manner as data on the internet. Using efficient ciphers is important, but the most power consuming process seems to be the message transmission. However, ciphers must adapt to the restricted length of the data payload in the SigFox message.

Based on the result displayed in Figure 5, it is clear that encryption has only minimal impact on the power consumption. This piece of knowledge is essential to the triad from Figure 3. The lower power consumption leads to lower costs, respectively, leads to the possibility of using the higher security level for IoT application. Moreover, the measurements displayed in Figure 6 show that AES-128-CTR might be a least power consumption demanding solution. However, the ChaCha provides, compared to AES, resistance to timing attacks as well as cache-collision attacks. Moreover, the ChaCha is less complex implementation in comparison to AES. Furthermore, the ChaCha is also, contrary to AES, proposed in the IETF protocol and used, e.g., by Google in TLS connections [22]. Additionally, the OTP shows comparable results with regards to power consumption and time complexity. The OTP provides possibly the most secure solution. However, there are still many open questions regarding OTP such as:

- Key storage - The client must ensure the secure key storage in the low-power memory (from our separated measurements, the standard SD cards consume approx. 150 µA) and the server must ensure secure large key storage on multiple places (to avoid simple one-point attacks).
- Sufficient number of keys - Considering the area of IoT in which billions of devices are being connected, even if Sigfox would take only one part of the market, there would have to be a sufficient solution for generating new unique sets of one-time keys for each node.
- Key generation - this paper introduced the possibility of using precomputed key-table. However, there are already low-power, low-cost random number generators (RNG), which might provide better performance and lower power consumption than the introduced solution. These RNG are already getting implemented to microcontrollers or there might be a simple physical way to generate true random bits such as using the radio or ADC noise. Nevertheless, separated and more deep analysis is required.

Another aspect related to the implementation of the security for low-power systems is to make a choice between different software and hardware implementations. For example, Piotrowski *et. al* [23] showed that an appropriate hardware implementation enables significant energy savings. However, the software implementation already brings a sufficient, low-cost and low power solution compared to the long on-air time with high energy consumption for communication. Therefore, the software implementation appears to be a decent compromise for LPWANs, which contributes to a reduction of costs.

Besides application data security, the key management is also important. The current solution offers static key management based on symmetric cryptography. Nevertheless, the system must be able to react to various attacks such as stolen devices, key leakage, and others. Therefore, new key establishing is the required property.

A ONE TIME PAD PERFECT SECRECY

This section provide the proof of the OTP perfect secrecy based on the sources [4, 12, 31, 35].

Definition A.1. Let us have the encryption scheme E and the message space M. Then E over M is perfectly secure just and only if, for all messages $m \in M$ and ciphertext c applies the probability $P[m|c] = P[m]$.

Theorem A.2. *The algorithm OTP is a perfectly secure encryption scheme.*

Proof. Lets define $M = \{0,1\}^n$, where n stands for number of messages. Then for $m \in M$ and also any c applies:

$$P[m|c] = \frac{P[m \wedge c]}{P[c]} = \frac{P[c|m] \cdot P[m]}{P[c]}, \quad (1)$$

Probability of ciphertext $P[c]$ over all messages in the message space is the sum of:

$$P[c] = \sum_{m \in M} P[c|m] \cdot P[m], \quad (2)$$

where for any m, c applies:

$$P[c|m] = P[c \oplus m] = 2^{-n}. \quad (3)$$

Combining the equation 2 and 3:

$$P[c] = \sum_{m \in M} 2^{-n} \cdot P[m] = 2^{-n}. \quad (4)$$

Comparing the equation 1 and 4, we can assume that OTP is perfectly secure. □

However, the perfect secrecy is conditional and there need to be same probability for m, c, also two different messages m_1, m_2 must have same probability, algorithm must use true random k with length at least equal to m, k must differs for each message and must be securely destroyed after use [12].

ACKNOWLEDGMENTS

The National Sustainability Program under Grant no. LO1401 and the Czech Ministry of the Interiornder grant no. VI20172019093 financed the research described in this article. For the research, the infrastructure of the SIX Center was used.

REFERENCES

[1] 2016. 8-bit AVR Microcontrollers: ATmega328/P. (2016). (Technical documentation).
[2] Aloÿs Augustin, Jiazi Yi, Thomas Clausen, and William Mark Townsley. 2016. A study of LoRa: Long range & low power networks for the internet of things. *Sensors* 16, 9 (9 2016), 1466. DOI: http://dx.doi.org/10.3390/s16091466
[3] Victor Baños-Gonzalez, M Shahwaiz Afaqui, Elena Lopez-Aguilera, and Eduard Garcia-Villegas. 2016. IEEE 802.11 ah: A technology to face the IoT challenge. *Sensors* 16, 11 (2016), 1960.
[4] Steven M Bellovin. 2011. Frank Miller: Inventor of the one-time pad. *Cryptologia* 35, 3 (7 2011), 203–222. DOI: http://dx.doi.org/10.1080/01611194.2011.583711
[5] Daniel J Bernstein. 2008. ChaCha, a variant of Salsa20. (2008). http://cr.yp.to/chacha/chacha-20080120.pdf
[6] Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. 2016. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications* 23, 5 (11 2016), 60–67. DOI: http://dx.doi.org/10.1109/MWC.2016.7721743
[7] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. 2018. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* 78 (part 2) (1 2018), 544–546. DOI: http://dx.doi.org/10.1016/j.future.2017.07.060
[8] Dallas Semiconductor 2018. *DS18B20: Programmable Resolution 1-Wire® Digital Thermometer*. Dallas Semiconductor. (Technical documentation).
[9] Thomas Eisenbarth and Sandeep Kumar. 2007. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers* 24, 6 (12 2007). DOI: http://dx.doi.org/10.1109/MDT.2007.178
[10] Alberto Giaretta, Sasitharan Balasubramaniam, and Mauro Conti. 2016. Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks. *IEEE Transactions on Information Forensics and Security* 11, 4 (12 2016), 665–676. DOI: http://dx.doi.org/10.1109/TIFS.2015.2505632
[11] Wael Guibene, Keith E Nolan, and Mark Y Kelly. 2015. Survey on clean slate cellular-iot standard proposals. In *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on*. IEEE, 1596–1599. DOI: http://dx.doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.240
[12] Jonathan Katz and Yehuda Lindell. 2015. *Introduction to modern cryptography*. CRC press. (second edition).
[13] Stouffer Keith, Lightman Suzanne, Pillitteri Victoria, Abrams Marshall, and Adam Hahn. 2015. Guide to Industrial Control Systems (ICS) Security. (5 2015). https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (Rev. 2).
[14] Keysight Technologies 2015. *Keysight N6705 DC Power Analyzer*. Keysight Technologies. http://literature.cdn.keysight.com/litweb/pdf/N6705-90010.pdf (Technical documentation no. N6705-90010).
[15] LPWAN Co., Ltd. 2016. *LPWAN SigFox node*. LPWAN Co., Ltd. (Technical documentation, Version 1.0).
[16] Mahmoud Shuker Mahmoud and Auday AH Mohamad. 2016. A study of efficient power consumption wireless communication techniques/modules for internet of things (IoT) applications. *Advances in Internet of Things* 6, 02 (2016), 19.
[17] George Margelis, Robert Piechocki, Dritan Kaleshi, and Paul Thomas. 2015. Low throughput networks for the IoT: Lessons learned from industrial implementations. In *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 181–186. DOI: http://dx.doi.org/10.1109/WF-IoT.2015.7389049
[18] Microchip Technology Inc. 2014. *MCP7940N*. Microchip Technology Inc. (Technical documentation).
[19] Élodie Morin, Mickael Maman, Roberto Guizzetti, and Andrzej Duda. 2017. Comparison of the device lifetime in wireless networks for the internet of things. *IEEE Access* 5 (4 2017), 7097–7114. DOI: http://dx.doi.org/10.1109/ACCESS.2017.2688279
[20] Roger M Needham and David J Wheeler. 1997. Tea extensions. *Report (Cambridge University, Cambridge, UK, 1997) Google Scholar* (1997).
[21] Hauveldop Niklas. 2017. Ericsson mobility report. (11 2017). https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017-central-and-eastern-europe.pdf
[22] Menachemi Nir and Adam Langley. 2015. Internet Research Task Force (IRTF). (2015).
[23] Steffen Peter, Peter Langendorfer, and Krzysztof Piotrowski. 2008. Public key cryptography empowered smart dust is affordable. *International Journal of Sensor Networks* 4, 1-2 (2008), 130–143. DOI: http://dx.doi.org/10.1504/IJSNet.2008.019258
[24] Noushin Poursafar, Md Eshrat E Alahi, and Subhas Mukhopadhyay. 2017. Long-range wireless technologies for IoT applications: A review. In *Sensing Technology (ICST), 2017 Eleventh International Conference on*. IEEE, 1–6. DOI: http://dx.doi.org/10.1109/ICSensT.2017.8304507
[25] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. 2016. Low power wide area networks: A survey. *arXiv preprint arXiv:1606.07360* (2016).
[26] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. 2017. Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials* 19, 2 (1 2017), 855–873. DOI: http://dx.doi.org/10.1109/COMST.2017.2652320
[27] Blank Rebecca and Gallagher Patrick. 2013. NIST Special Publication 800-53. (2013). DOI: http://dx.doi.org/10.6028/NIST.SP.800-53r4 (Rev. 4).
[28] Weatherley Rhys. 2018. Arduino Cryptography Library. (2018). https://rweather.github.io/arduinolibs/ (software).
[29] Matthew D Russell. 2004. Tinyness: an overview of tea and related ciphers. *Draft v0* 3, 3 (2004).
[30] Ramon Sanchez-Iborra and Maria-Dolores Cano. 2016. State of the art in LP-WAN solutions for industrial IoT services. *Sensors* 16, 5 (2016), 708.
[31] Claude E Shannon. 1949. Communication Theory of Secrecy Systems. *Bell System Technical Journal* 28, 4 (10 1949), 656–715. DOI: http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x
[32] Sigfox 2017. *Secure Sigfox Ready devices: Recommendation guide*. Sigfox. (Technical documentation, rev. 34).
[33] Sigfox 2017. *Sigfox Technical Overview*. Sigfox. (Technical documentation).
[34] Oriol Solà Campillo. 2017. Security issues in Internet of Things. (2017). http://hdl.handle.net/2117/109290
[35] Gilbert Vernam. 1919. Secret signaling system. (7 1919). https://patents.google.com/patent/US1310719 US Patent 1919-07-22 (US1310719A).
[36] David J Wheeler and Roger M Needham. 1994. TEA, a tiny encryption algorithm. In *International Workshop on Fast Software Encryption*. Springer, 363–366. DOI: http://dx.doi.org/10.1007/3-540-60590-8_29
[37] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications* 84 (4 2017), 25–37. DOI: http://dx.doi.org/10.1016/j.jnca.2017.02.009
[38] Juan Carlos Zuniga and Benoit Ponsard. 2016. Sigfox system description. *LPWAN@ IETF97, Nov. 14th* (2016).