SAFETY EVALUATION OF CRYPTOGRAPHY MODULES WITHIN SAFETY RELATED CONTROL SYSTEMS FOR RAILWAY APPLICATIONS

Maria FRANEKOVA[1], *Marek VYROSTKO*[1]

[1]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Univerzitna 1, 01026 Zilina, Slovakia

maria.franekova@fel.uniza.sk, marek.vyrostko@fel.uniza.sk

Abstract. *The paper deals with the problem of safety evaluation of cryptographic modules used within safety-related control system for applications with increasing safety integrity level. The requirements to cryptographic techniques in safety-related communication for railway application are describe. The mainly part is oriented to description of mathematical apparatus for an error probability of cryptography code with a safety code, used in an additional safety communication layer. The practical results are related with the quantitative evaluation of an average error probability of code word for Euroradio protocol recommended for communication in European Train Control System.*

Keywords

Safety-related communications, safety integrity level, railway applications, cryptographic code, safety code, safety evaluation.

1. Introduction

Nowadays in railway applications, with respect to high requirement to Safety Integrity Level (SIL) of an interlocking and a communication system, the safety of subsystems cannot be demonstrated by tests only, but also by theoretical models based on quantitative analysis [1], [2]. Negative influence also results from the fact, that a generally acceptable theoretical apparatus for risk analysis and safety level evaluation is missing, which would objectify the whole process of safety consideration. Reciprocity information exchange leads to opinion of safety certification unification. It leads to problems minimize by reciprocity acceptation advisement results. The genesis of the problem is based on the fact, that single countries of European space developed philosophical different signaling systems and interlocking systems too. These systems have been developed basically at the national level with different types of signals and devices. Today it is very difficult to harmonize these devices.

Developing the uniform ETCS (*European Train Control System*) in Europe can solve these problems in the future, although implementation of particular application level of ETCS depends on economical situation in individual European country [3], [4]. Application level ETCS L2 assumes communication across GSM-R (*Global System for Mobile - for Railway*) network and communication protocol Euroradio, which content some cryptography mechanisms for keeping of integrity and authentication procedures of railway transport entities, e. g. communication between OBU (*On Board Unit*) in train with RBC (*Radio Block Central*) and communication between RBC-RBC [5]. In several part of cryptography systems within ETCS system is in the phase of evolution and discussions. Concerning to very dynamic developed discipline (as it is cryptography) and with related cryptanalysis several recommended cryptography algorithm in Euroradio system is not computationally safety just now (not resistant against existing attacks) [6]. Therefore it is necessary to create the methodology for safety evaluation of the cryptographic algorithms or the cryptographic modules and to determine computationally safety of recommended cryptographic mechanisms, to consider their selection and in addition to proposal for these algorithms KMS (*Key Management System*). In Europe countries this time KMS is in the phase of developing. With respect of interoperability in railway transport in European countries these procedures and convention must be solved incorporate with railway companies in Europe [3]. The reciprocal acceptance an interlocking and communication systems safety appraisal results bring considerable financial savings and significantly reduce the deployment of new systems into railway operation (the necessary requirement for interlocking system implementation is a positive result of Safety appraisal). In addition more suitable conditions are created for penetration of these systems onto third-party countries (the reference of the systems safety being accepted by several countries organizations acts positively).

These rules are valid for specific part of safety related systems too, which is communication. It is well known that standards for commercial sphere (e. g. financial sector, company information systems, ...) exist but for applications of cryptography with increasing safety integrity level the methodology for safety evaluations absent. E. g. the FIPS 140-2 [7] standard is applicable to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems. For safety evaluation of cryptography modules methods based on the quantitative analyses are recommended in comparison of approach apply in the commercial sphere, where the methods are based on the qualitative analyses.

According to standard FIPS PUB 140-2 cryptographic modules are divided to four qualitative levels:

- Security Level 1 - provides the lowest level of security. No specific physical security mechanisms are required in cryptographic module beyond the basic requirement for production-grade components.
- Security Level 2 – improves upon the physical security mechanisms of a cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module.
- Security Level 3 – attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module, trusted channel for manipulation of critical data – B1 according to TCESEC [8] are used.
- Security Level 4 – provides the highest level of security. The physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

General requirement to cryptography techniques which must be fulfill are described in the norm EN 50159 [9].

2. Requirements for Cryptography Mechanisms within Safety Critical Applications

Cryptographic techniques are recommended to apply within safety-related application (e. g. safety-related control system in railway transport) if malicious attacks within the open transmission network cannot be ruled out. This is usually the case when safety-related communication uses a public network, a radio transmission system and a transmission system with connections to public networks. Cryptographic techniques can eliminate masqueraded of message. Cryptographic techniques can be combined with the safety encoding mechanism or provided separately. The degree of effectiveness of cryptography mechanism depends on the strength of the algorithms and the secrecy of the keys. According to norm for railway applications [9] the safety case shall demonstrate the appropriateness of the following: technical choice of cryptographic techniques (performance of encryption algorithm, key characteristics), technical choice of cryptographic architectures (checking the correct functioning - before and during the operational phase of the cryptographic processes when they are implemented outside the safety-related equipment), management activities (production, storage, distribution and revocation of confidential keys). The cryptographic algorithm shall be applied to all user data and may be applied over an additional data that is not transmitted but is known to the sender and the receiver (implicit data). The basic principle of safety - related communication between two safety-related equipment SRE 1 and SRE 2 is illustrated in Fig. 1. The additional safety layer, certificated in the required safety integrity level (SIL) must be implemented within a safety - related equipment. It is layer of the safety - related transmission in which is implemented the safety mechanism a safety code for elimination of unintentional attack affected by EMI (*Electromagnetic Interferences*) and the safety layer the access protection, which is realized with the use of cryptographic code, or cryptographic techniques. This layer can be component part of safety – related equipment or can be apply in input point to untrusted transmission systems. According to norm [9] within safety - related communication across open transmission system, in which is not possible to eliminate unauthorized access to system, within communication layer of the access protection the block cipher based on secret key is high recommended (model of structure message B0) or cryptography code (model of structure message B1).

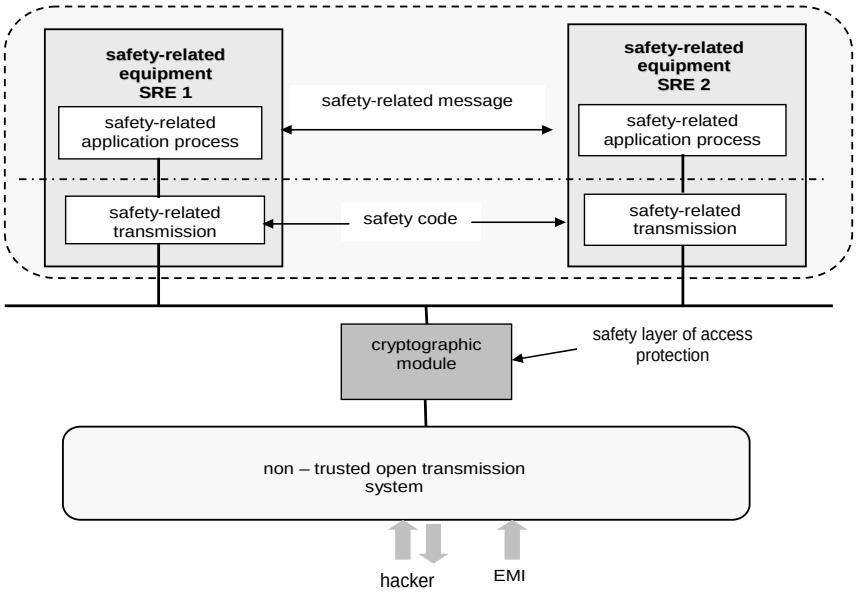

Fig. 1: Location of cryptographic module within communications between two safety - related equipment.

3. Mathematical Apparatus for Error Probability Determination of Cryptographic Code Word

We assume that safety communication layer, as it is illustrated in Fig. 2, will be combined with safety and cryptography code. Further let us assume that conventional block cipher will by apply as cryptography code and communication channel is affected by electromagnetic interferences only.

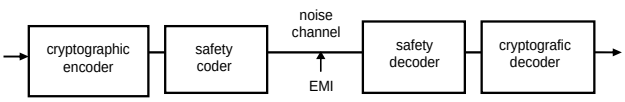

Fig. 2: Combined case of creating safety communication layer.

In the conventional block cipher, a plaintext block of *n* total bits, usually comprising an integral number of code words of *k* bits each, is enciphered by cryptography encoder, as a block of *n* total bits. After transmission and reception, the plaintext block is restored as the output the output of the deciphering system. No output words are in error unless the received cipher text block contains an error in at least one of *n* bits. Assuming the independence of input bit errors,

$$P_{cw} = P(w|be)[1-(1-P_b)^n], \tag{1}$$

where $P(w|be)$ is the probability of an error in an output word, given that there is a block error at the input of the cryptography decoder (deciphering system). Setting $P(w|be)=1$ [10], we obtain:

$$P_{cw} \le 1-(1-P_b)^n \le nP_b . \tag{2}$$

Due the one one-to-one correspondence between the ciphertext blocks, an error in a received ciphertext block is certain to cause at least one erroneous bit in output block. Consequently, over the ensemble of block cipher of size *n*, there are (2^n-1) equally like output blocks corresponding to an erroneous ciphertext block. Consider any fixed bit in these output blocks. In $(2^{n-1}-1)$ of the possible output blocks, this bit is correct, that is, in the same state that it would have been in if no error had occurred in enciphered block. We conclude that given a block error, there is an ensemble-average probability that a bit is correct equal to $(2^{n-1}-1)/(2^n-1)$. Consider a second fixed output bit. Given that there is a block error and that the first fixed output bit is correct, it follows from an extension of the previous reasoning that there is an ensemble-average probability that the second fixed bit is correct equal to $(2^{n-2}-1)/(2^{n-1}-1)$. If $x_1, x_2, \ldots, x_k$ are events, the probability of all these events is equal to the product of conditional probabilities:

$$P(x_1, x_2, \ldots, x_k = P(x_k|x_{k-1}, \ldots, x_1) \ldots P(x_2|x_1)P(x_1) . \tag{3}$$

Using this equation and repeating the analysis for successive output bits, we conclude that for a *k*-bit word contained within a single block,

$$\overline{P}(w|be) = 1-\prod_{i=1}^{k}\frac{2^{n-i}-1}{2^{n+1-i}-1} = \frac{1-2^{-k}}{1-2^{-n}} . \tag{4}$$

Combining this relation with (1), we obtain the ensemble-average cryptographic word error probability for block ciphers,

$$\overline{P}_{cw} = (1-2^{-n})^{-1}(1-2^{-k})[1-(1-P_b)^n]. \quad (5)$$

A Taylor-series expansion yields

$$\overline{P}_{cw} \approx (1-2^{-n})^{-1}(1-2^{-k})nP_b. \quad (6)$$

Which is accurate if

$$P_b << 2(n-1)^{-1}. \quad (7)$$

The ensemble-average cryptographic bit error probability for block ciphers is obtained by setting $k = 1$ in (5) or (6). Although these equations hold for $n \geq k$, it is usually required that $n \geq 4k$ [10], [11] to safeguard against the frequency analysis of block patterns.

The preceding derivations of cryptographic error probabilities depend upon the assumption of independent bit errors at the input of to the deciphering system. When this input is the output from a decoding system that corrects word errors, the input bit errors are not independent, but occur in clusters. Thus the preceding equations for the cryptographic error probabilities do not apply. However, assuming the independence of the input word errors, we can relate the word errors; we can relate the word error probabilities at the outputs of deciphering systems to the word error probabilities at the inputs. This assumption is valid when block codes are used for error correction and the symbol errors at the input to the decoding system are independent.

For block ciphers yield

$$P_{cw} \leq 1-(1-P_w)^{n/k} \leq \frac{n}{k}P_w. \quad (8)$$

Where P_w is word error probability, then

$$\overline{P}_{cw} = (1-2^{-n})^{-1}(1-2^{-k})[1-(1-P_w)^{n/k}], \quad (9)$$

where the integer n/k is the number of words in a block. A Taylor-series expansion yields the approximation:

$$\overline{P}_{cw} \approx (1-2^{-n})^{-1}(1-2^{-k})\frac{n}{k}P_w. \quad (10)$$

Which is accurate if

$$P_w << 2k(n-k)^{-1}. \quad (11)$$

4. Result of Error Probability Determination with Application to Euroradio Protocol

Determination of an average error probability of the cryptography code word was realized for combined communication system, which consists from the safety code and the cryptographic code MAC (*Message Authentication Code*) [12]. The formal notation of MAC calculation is:

$$MAC = C_{Kc}(M), \quad (12)$$

where M is the message, K_c is the shared key and C representing ciphering operation.

This alternative cryptographic technique is well recommended for using in Euroradio safety layer of communication protocol within ETCS system, developed in railway application in Europe. This cryptography code is recommended to apply in CBC (*Cipher Block Chaining*) mode CBC-MAC, which improves the safety of algorithm [13].

CBC-MAC is based on 3-DES block cipher [14], which enciphered the block size of length $k = 64$ bits with applying the secret keys of length 168 bits and is using in secure procedures ensuring message authentication and integrity during transmission.

Let us assume that the safety code is detection cyclic linear block code works in the principle of CRC (*Cycling Redundancy Check*) - CRC-16. Further we assume that probability of undetected error of code word $P_w = 2^{-16}$ (according to norm [9], so called the worst case). The ensemble-average cryptographic word error probability $\overline{P}_{cw}$ was realized according to relation (10). The results of $\overline{P}_{cw}$ for different length of code word in the input of ciphering encoder (k = 64, 128, 192, 256) and different length of input plaintext ($n = 1.10^4$, 5.10^4, 1.10^5, 5.10^5, 1.10^6, 5.10^6) are illustrated in Tab. 1 and Tab. 2.

Graphical results of $\overline{P}_{cw}$ as function of input bit stream of plaintext n for constant value of code words in input of cryptography decoder is illustrated in Fig. 3.

In the graph illustrated in Fig. 4 we can shown how is changed $\overline{P}_{cw}$ dependence of code words $k = 64$, $k = 128$ and $k = 256$ in the input of cryptography encoder.

Tab.1: Result of the average error probability with using cryptography code in accordance with parameter *n*.

Length of input plaintext *n*	Average error probability $\overline{P}_{cw}$ if *k*=64	Average error probability $\overline{P}_{cw}$ if *k*=128	Average error probability $\overline{P}_{cw}$ if *k*=256
$1{,}10^4$	$3{,}13\cdot10^{-14}$	$1{,}56\cdot10^{-14}$	$7{,}81\cdot10^{-15}$
$5{,}10^4$	$1{,}56\cdot10^{-13}$	$7{,}81\cdot10^{-14}$	$3{,}91\cdot10^{-14}$
$1{,}10^5$	$3{,}13\cdot10^{-13}$	$1{,}56\cdot10^{-13}$	$7{,}81\cdot10^{-14}$
$5{,}10^5$	$1{,}56\cdot10^{-12}$	$7{,}81\cdot10^{-13}$	$3{,}91\cdot10^{-13}$
$1{,}10^6$	$3{,}13\cdot10^{-12}$	$1{,}56\cdot10^{-12}$	$7{,}81\cdot10^{-13}$
$5{,}10^6$	$1{,}56\cdot10^{-11}$	$7{,}81\cdot10^{-12}$	$3{,}91\cdot10^{-12}$

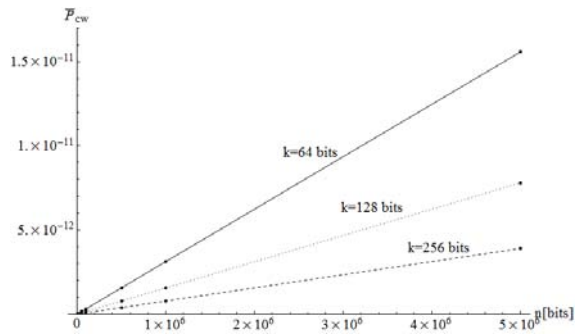

Fig. 3: Caption example.

Tab.2: Result of average error probability with using cryptography code in accordance with parameter *k*.

Length of input block *k*	64	128	192	256
Average error probability $\overline{P}_{cw}$	$3{,}13\cdot10^{-14}$	$1{,}56\cdot10^{-14}$	$1{,}04\cdot10^{-14}$	$7{,}81\cdot10^{-15}$

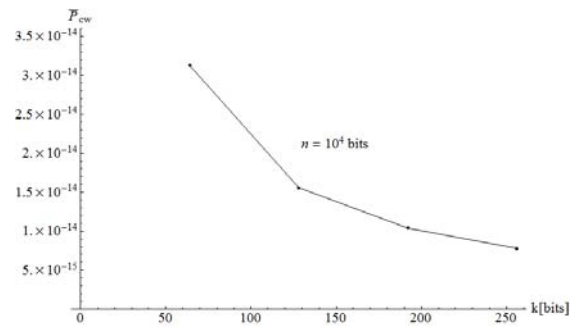

Fig. 4: Average error probability of the cryptography code in dependence on *k*.

This is simulation of changing cryptography algorithms DES or 3-DES to today resistant block cipher to known cryptanalytic attacks AES (*Advanced Encryption Standard*) [15] for constant length of plain text $n = 10^4$.

5. Conclusion

In the paper the mathematical apparatus for an error probability of cryptography code was describe, which can be used within the safety evaluation of cryptography codes used in safety-related communication with combination of a safety code. The authors assumed application of CRC-16 safety code. The results are oriented to determination of an average error probability of message authentication code (MAC) on the base of 3-DES algorithm in CBC mode, which is recommended to apply in Euroradio communication protocol in ETCS system providing affect of electromagnetic interferences only. In Tab. 1 and Tab. 2 and in Fig. 3 and Fig. 4 are illustrated the results of an average error probability of cryptography code in dependence of length of plaintext *n* and of length of code word *k* (in the case of changing the algorithm 3-DES to more prefer algorithms AES). For keeping high diffusion of a cipher text it is necessary the length of message *n* choice more than selected length of block cipher *k* ($n>4k$ is recommended). Results of an average error probability of code word can be changed in dependence on the detection or correction possibilities of safety code. In the paper the authors assume one type of safety code only and determination oriented to safety analyses of cryptography code.

For global safety evaluation of cryptographic module it is necessary to create the model which will be describe the affects of the intentional attacks to safety message transmission.

Acknowledgements

This work was supported by project **Centre of excellence for systems and services of intelligent transport**, ITMS 26220120028, University of Zilina, Zilina, Slovak republic

Project Part-Financed by the European Union

European Regional Development Fund

References

[1] EN 50129. *Railway applications : Safety-related electronic systems*. CENELEC, 2003.

[2] EN 50126. *Railway applications : The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)*. CENELEC, 2001.

[3] *The European Rail Traffic Management System* [online]. 2010. Available at WWW: <www.ertms.com>.

[4] ZAHRADNÍK, J.; RÁSTOČNÝ, K. *Aplication of safety-related systems*. EDIS, ŽU in Žilina, 2006. ISBN 80-8070-546-1.

[5] FRANEKOVÁ, M.; KÁLLAY, F.; PENIAK, P.; VESTENICKÝ, P. *Communication safety of industrial networks*. ŽU in Žilina, EDIS, 2007. ISBN 978 -80 -8070-715-6.

[6] CHRTIANSKY, P. Cryptoanalysis of block cipher used in safety-related comunication protocol. *Proceedings of International Conference ELEKTRO, Žilina*. May 2008, pp. 143-145. ISBN 978-80-8070-845-0.

[7] FIPS 140-2. *Security requirement for cryptographic modules*. Federal Information Processing Standard Publication, 1994.

[8] QIU, L.; ZHANG, Y.; WANG, W.; KYUNG, M.; RATUL MAHAJAN, H. *Trusted Computer System Evaluation Criteria.* National Computer Security Center.

[9] EN 50159. *Railway applications : Communication, signalling and processing systems - Safety - related communication in transmission systems*.

[10] TORRIERI, D. J. *Principle of Secure Communication Systems*. Boston, London : Artech House, 1992. ISBN 0-89006-555-1.

[11] SATTAR, F.; MUFTI, N. On Post Decryption Error Probability in Counter Mode Operation with Explicit Counter Transmittal. *International Journal of Security. International Journal of Network Security*. March 2009, vol.8, no.2, pp.119-124. ISSN 1816-3548.

[12] ISO/IEC 9797-1:1999. *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1 : Mechanisms using a block cipher.*

[13] ISO/IEC 10116:2006. *Information technology – Security techniques – Modes of operation for an n-bit block cipher.*

[14] NIST FIPS PUB 81. *DES Modes of Operation*. 1980, v. 1.1.

About Authors

Maria FRANEKOVA was born in 1961 in Brezno (Slovakia). She received her Assoc. Prof. in 2004 in the field of “Information and Safety-related Systems”. Her research interests include safety data transmission, analysis of safety communication on the base of coding and cryptography tools within safety related applications.

Marek VYROSTKO was born in Kosice, Slovakia in 1985. He received his Master (Ing.) degree in 2008. Currently he is Ph.D. adept. His research interests include communication and management of cryptographic keys within safety- related systems.