Archives of
Transport System
Telematics

Volume 11

Issue 3

September 2018

Safety Weaknesses of Digital Signature Used for Safety Critical Applications of E-Government

M. FRANEKOVÁ[a], M. ŠUTÁK[b]
[a] UNIVERSITY OF ŽILINA, Faculty of Electrical Engineering, Department of Control and Information Systems, 010 026 Žilina, Slovak Republic
[b] ALIGA, S. R. O., 036 01 Martin, Slovak Republic
EMAIL: maria.franekova@fel.uniza.sk

ABSTRACT

The authors of this article focus on the analysis of safety weaks of digital signature schemes used within e-Government service in condition of Slovak republic. Main part is orientated on the possibility of attacks on eID card with using RSA digital signature scheme what was in the last months very frequently medialized in Slovakia. In the practical part on the base of mathematically description is analysed possible weaks of RSA digital signature schemes especially complexity of factorization problems dependence of length of key is describe and compare with more effectiveness ECDSA scheme. On the base of studies the authors mentioned the recommendations for parameters selection of very often used digital signature schemes focus on access to safety- critical applications supported during process of digitalization of e-Government in Slovak republic.

KEYWORDS: E-Government, safety-critical, services, eID card, authorization, qualified certificate, digital signature, RSA, ECDSA, complexity of factorization

1. Introduction

It is well known that in a cyberspace is the electronic signature an innovative alternative to the traditional hand-written signature when you perform on-line transactions. Issuing and utilization of the electronic signature is in Slovak Republic (SR) governed by the Act No.272/2016 Coll. on Trust Services [1]. In terms of this Act is the electronic signature issued by using the classified equipment (CE) with using the qualified certificate (QC). Qualified electronic signature (QES) offers to their clients authenticity (ability to unambiguously validate the subject identity), integrity (ability to evidence, that after document signing there was not any change of the document) and non-repudiation (client can not declare, that they do not sign document). Within countries in European Union (EU) belong to pioneer of electronics signature using Austria and Estonia. In Slovak republic was by adoption of the Trust services Act [1] repealed Act No.215/2002 Coll. [2] and the term guaranteed electronical signature has modified to qualified electronic signature. In Slovak republic is QES used for communication with governmental organizations through the Central Government Portal, access to services of the Business and Trade Register, communication with the financial administration (tax and customs authorities) and for communication with the courts of law in SR.

It is clear, that access to these applications also with issuing and utilization of QES as well as QC issued by the accredited certification authority must provide appropriate high level of security. In Slovak republic is security of electronic services in accordance with e-Government act implemented through electronic identification card (eID) with chip, where are stored (by using electronic signatures with asymmetric cryptography schemes) public key (*PK*), secret key (*SK*) and qualified certificate, that are used for QES generation [3].

In connection to act on e-Government in SR is eID secure device for cryptography key storing (public and secret) and qualified certificate too, that are aimed at qualified electronic signature creation. For QES issuing through electronic identification card must be fulfilled these conditions:

- it is necessary to own eID with valid qualified certificate, which is stored in chip,
- it is necessary to have computer with chip card reader and with relevant drivers, SW tools for eID and application for QES generation,
- the citizen must know its personal security code) PSC and personal identification number (PIN) for QES,
- for on-line communication is there needed internet connection and browser with installed application for QES creation.

In last months the researchers in Slovak and Czech Republic [4, 5] has pointed out weaknesses in eID with chip. The problem was found in key issuing in SW library, which was created by company Infineon Technologies AG. It is very often used library, which we can found at highest levels of security not only in applications in Slovak republic, but also in Estonia and Austria. The weaknesses connected to key management, which is needed for the RSA (Rivest Shamir Adleman) signature scheme [6], which is used by eID they discovered also researchers from Enigma Bridge in Cambridge and Italian Ca'Foscari University of Venice [7, 8]. It is security weakness, which allows a hackers calculate the secret key from public key because the space of keys is significantly limited (factorization becomes for RSA keys with length 512 bits, 1024 bits and 2048 bits possible and feasible). In Slovak republic was threatened approximately 300.000 clients, whereas from 2.5 million issued eID cards with chip not everyone activated the certificates. The Top-level certification authority in SR – National Security Authority (NSA) reacted to a published evidences of eID security vulnerabilities by revoking of all certificates from 31st October 2017 and clients were requested to apply for issuing new certificate with 3072 bits keys, what however will be only temporary solution.

Authors of the article analysed the possibilities of crypto analytical attack to the RSA algorithm through the attack to factorization. Simultaneously they pointed out to possibility of substitution the RSA algorithm by more effective way of securing - ECDSA (Elliptic Curve Digital Signature Algorithm) signature schemes application. ECC (Elliptic Curve Cryptography) based certificates plan to deploy for securing e-Government services (after revoking till now valid certificates) for example Estonia.

2. Mathematical principle of digital signature schemes and their security

List of approved signature schemes, algorithms and parameters for qualified electronic signature generation are mentioned in the Regulation of the National Security Office No. 135/2009 Coll. [9]. In the regulation are mentioned QES formats, ways of QEP generation, list of approved signature schemes and also ways of generation and verification of timestamps. With reference to [9] it is recommended nine signature schemes (look at Table 1). In Table 1 are presented asymmetric cryptosystem algorithm and type of hash function.

Table 1. List of approved QEP signature schemes with reference to [9]

Signature Scheme	Asymmetric algorithm	Hash Function
001	RSA	SHA1
002	RSA	SHA1
003	RSA	RIMEMD160
004	RSA	RIPEMD160
005	DSA	SHA1
006	ECDSA -	SHA1
007	ECDSA-	SHA1
008	ECGDSA -	SHA1
009	ECGDSA -	SHA1

By implementation QES in Slovak republic are recommended schemes with appendix (signature is added to a document). It is deterministic scheme with the RSA algorithm but it is recommended also stochastic scheme DSA type (Digital Signature Algorithm), which uses modified El Gamal algorithm and ECDSA scheme, which uses ECC algorithm. ECDSA signature schemes are recommended in structure (utilizing prime ECC) and in structure (utilizing binary ECC). It is recommended also German standard ECGDSA (Elliptic Curve German Digital Signature Standard). As a hash functions are recommended American standard SHA (Secure Hash Algorithm) or European standard RIPMED (RACE Integrity Primitives Evaluation Message Digest).We suppose that the length of hash code used by implementation is at least 256 bits and not as it is mentioned in Appendix 1 of the regulation [9] (it is difficult for legislation to keep abreast of the fast trends in crypto-analysis). We also suppose that for implementation is in case of the RSA algorithm utilized safer modification of the RSA.

For the purpose of security weaknesses analysis in case of deterministic schemes with the RSA and stochastic ECDSA it is necessary to start from their mathematical description.

The mathematical description consists from parts generation of keys, signature creation and their verification {*Gen*, *Sign*, *Vrf*}. Particular parts represents:

- {*Gen*} – probabilistic polynomial algorithm for key pair generation – secret key (*SK*) and public key (*PK*).
- {*Sign*} – effective algorithm for signature $Sign_{SK}$ generation from digital document (message)xn, with using *SK*.
- {*Vrf*} – typically deterministic polynomial algorithm, which validate the signature $Vrf_{PK}(M,Sign)$ with using PK.

Signature scheme correctness is generally defined:

$$\{PK,SK\} \leftarrow \{Gen\} \quad Vrf_{PK}\left(M,Sign\right) \in tru \tag{1}$$

2.1. RSA signature scheme

Today there exist various modifications of RSA signature scheme with the aim to increase security on stochastic elements enhancing basis. Examples of such approach are RSA-FDH (Full Domain Hash) scheme and RSA-PSS (Probabilistic Signature Scheme) [10].

Original digital signature scheme on the RSA basis is characterized as a deterministic scheme, i.e. for the same message (document) with the same RSA parameters is generated the same digital signature. This principle is based on the fact, that on the side of the message sender (citizen) *A* (when the digital signature is generated) is from message *M* created hash code *h=M(H)* by the hash function *H*. This code is encrypted by sender's secret key E_{SK_A} and joined to message *M*. Through the communication channel is then transmitted open message *M* and digital signature *sign*=E_{SK_A} *(H(M))*.To the signature is added in addition certificate issued by accredited certification authority (ACA). One of the first ACA in SR, which issues qualified certificates (QC) also with timestamp is PSCA (First Slovak Certification Authority).

In original RSA signature scheme the recipient (appropriate authority) *B* after receiving signed message validates the digital signature by the deciphering it with using the public key of sender *A* (PK_A) whereby it get hash code, which is compared with calculated hash code from received message *M'*, i.e. *h'=H(M')* If are these two codes equal *(h'=h)*, the message is authentic.

Basic techniques for signature generation and its verification are described in standard PKCS#1 [10].

Key generation procedure, signature generation and its verification in the RSA scheme (from sender *A* towards receiver *B*) can be mathematically described as follows [3]:

- generating of key pair for sender *A* - {*Gen*}:
  - generate two different, but approximately the same length primes *p* and *q*, *p<q*; prime generation can be based for example on probabilistic Rabin-Miller algorithm; according to the ANSI X9. 31 [11] it is required so called strong primes; for primality are tested not only *p* and *q*, but also *(p–1), (q–1), (p+1), (q+1)*. Primes and are not used in next procedure, but the must stay confidential.
  - calculate modulus *N* (it means length of the key and Euler function *φ(N)*):

$$N = p \cdot q;\ \varphi(N) + (p-1) \cdot (q-1) \tag{2}$$

  - choose cipher exponent so that 1<s< *φ(N)*; number must be incommensurable with *φ(N)*:

$$gcd(s,\ \varphi(N))) = 1 \tag{3}$$

  - number pair *s, N* represents public key ~*PK* ={*s*, *N*};
  - calculate decrypt exponent so that congruence is achieved:

$$t.s \equiv 1 mod \varphi\left(N\right) \tag{4}$$

Note: In described original procedure are sometimes primes and not generated randomly, but first of all is chosen special value of cypher exponent (public element), for example $s = 17$ *or* $s = 2^{16} + 1$ and accordingly to this is adapted selection of primes *p* and *q*.

- digital signature generation on side of sender *A* -{*Sign*}:
  - original message - *M*;
  - generated signature:

$$sign = H\left(M\right)^{t_A} modN \tag{5}$$

- signature verification on side of sender *B* {*Vrf*}:
  - received message - *M'*;
  - signature - *sign*;
  - signature validity:

$$sign^{s_A} modN = H\left(M'\right) \tag{6}$$

Correctness of this signature scheme results from the fact that in the RSA algorithm are encrypt and decrypt transformation are mutually inverse functions. Similar as the encryption and decryption scheme is security of the RSA scheme of digital signature based on big numbers factorization difficulty (big modulus *N*).

The RSA laboratories, as the authority in this area, recommends substitute till now used signature schemes with the RSA algorithm (PKCS # 1 v1.5) by more robust schemes, which brings into the process of digital signature creation some random elements.

In many cases is a question of RSA algorithm security often limited only to discussion about key length. The security of such system is also influenced by right implementation, size of encryption and decryption exponent and many other details. From the time, when was the RSA published for the first time, many scientist have explored the robustness of this algorithm and many of the attacks against RSA have been successful, none of them has been critical. Mainly there has been pointed out to possible threat of unsuitable use of this cryptosystem, because secure implementation of the RSA is not simple task. Today is as a most critical attack to the RSA algorithm taken attack to a concrete implementation and its concrete weaknesses, where are applicable well known techniques side channels.

The most known attacks on the RSA can be sorted out into the four groups [12]:

- attacks on RSA algorithm structure;
- attacks on small decryption exponent;
- attacks on small encryption exponent;
- attacks on implementation.

In studies [13] are published new attacks based on possibility to create fictitious signature by attacker for selected message (existential forgery), when the attacker is able to generate a number of message and signature couples {*M, Sign*}. Then consequently are created valid signatures, or more precisely attacks of EUF-CMA type (existentially unforgeable under the chosen message attack).

2.2. ECDS signature schemes

Cryptography based on elliptic curves is a new perspective trend in modern asymmetric cryptography. Basic algebraic structure, which is used in ECC, is the elliptic curve group of points. They are complex mathematical objects, described by multiple expressions, definitions and theorems that can be found for example in [14]. Gradual implementation of the ECDSA (as a substitute for the RSA) comes from advantageous characteristics of these schemes. These are mainly higher security of the ECC by smaller bit's key length utilization which leads to smaller computational complexity. The ECDSA signature schemes faster for signature generation (suitable for on-line signing). It is well known that ECDSA algorithm security is dependent on discrete logarithm problem solving (Elliptic Curve Discrete Logarithm Problem). For the SW application of eID are suitable elliptic curves over the finite ring F_p. At the present time are standardized NIST (National Institute of Standards and Technology) curves: P-256, P-384 and P-521 [15]. The ECDSA P-256 has its equivalent from the perspective of modulus *N* in the RSA algorithm RSA 3072.

Procedure of generation and verification of ECDSA digital signature over the finite field can be mathematically described this way [3]:

- generating of key pair for sender (citizen) - {*Gen*}:
  - selection of parameters $F_p(a,b)$ – for expression $y^2 = x^3 + ax + b$; count of points $F_p(a,b)$ should be dividable by the large prime *p* (*p* is a key length);
  - selection of point P∈ $F_p(a,b)$ - *P* is defined by coordinates $[x_p, y_p]$; degree of the point is *n* $(n > 2^{160})$.
  - selection of random number *d* - *d* is number from interval *(1,n – 1)*;
  - calculation of point *Q* - *Q* is defined by coordinates $[x_Q, y_Q]$:

$$Q = d \cdot P \tag{7}$$

  - public key and secret key are:

$$PK_A = \{E, P, n, Q\};\ SK_A = \{d\} \tag{8}$$

  - digital signature generation on the side of sender {*Sign*}:
  - generation of message fingerprint *M* - *H(M)*;
  - selection of k - k is a random number from interval *(1,n – 1)*;
  - calculation of $k \cdot P$ - $k \cdot P = (x1, y1)$;
  - signature calculation:

$$r = x_1 modn \quad s = \left(k^{-1}\left(H\left(M\right) + d \cdot r\right)\right) modn; H(M) \tag{9}$$

  - signature is the couple *(r, s)*, signature length is a double the key length;
  - signed message - *{M, r, s}*;
- digital signage verification {*Vrf*}:
  - received message - *{M', r', s'}*;
  - verification by receiver if the received *r', s'* are integers from interval *(1, n – 1)*
  - calculation of *H(M)*; according to the selected hash function type and *w*:

$$w = \left(s'\right)^{-1} modn \tag{10}$$

  - calculation of u_1, u_2:

$$u_1 = \left(H\left(M'\right) \cdot w\right) modn; u_2 = \left(r' \cdot w\right) modn \tag{11}$$

  - calculation:

$$u_1 \cdot P + u_2 \cdot Q = \left(x_0, y_0\right); v = x_0 modn \tag{12}$$

  - if it is true that $v = r'$ than the signage is valid, if $v \neq r'$, than message was modified or was signed by someone else or the message was signed faulty.

Arithmetical operation of NIST curves are more difficult to implement in comparison with the RSA. Probably there is a reason why process of the ECDSA implementation slowed down. Even in case of correct implementation it is hard to solve problems arising from the side channels attacks or weakening of system by attack. SW application must deal not only with points on ECC but also with the point in zero and infinity *O*. To the problem contributes also slow legislation. The deterministic schemes can use one type of algorithm while in the ECDSA it is possible to use multiple ECC, which makes the process of implementation difficult. Today there exists more alternative ECC, for example Curve 25519 (Montgomery curve), ed 25519 (Twisted Edwards curve). However introducing new standards is slow and today there exist only preliminary versions of IETF standards.

3. Safety weaks of eID based on digital signature in condition of Slovak Republic

Based on research over the implemented technology of eID [16] it appears that by utilization of extension to Coppersmith's factorization attack it is possible to reconstruct secret key from public key by utilizing available (and reachable) computing power.

The problem was discovered in Infineon's RSA library version 1.02.013, which falsely generates key pairs [17], and this fact can help to an attacker to uncover RSA secret key from the relevant public key. As a result is key space so much limited, that for key length bellow 2048 bits is factorization by attack of type "brute force attack" which follows the most unfavourable direction feasible. The part of the library which uses ECC appears as a secure.

As a solution the producer of relevant technology offers Infineon update which addresses the problem. The recommendation of producer is to utilize ECC keys, but change of algorithm is not always possible. In applications where is the RSA required it is recommended to use different method – for example OpenSSL and then use the new secure RSA keys with the old device.

The library is widely used in devices approved by NIST FIPS 140-2 and Common Criteria EAL 5+ and so it represents quite wide area of applications and environments affected by this problem. For example they are eID cards, authentication tokens, TLS/HTTPS keys, PGP. Trust boot devices or SW packet signature.

Prime generation by library brings to the users advantages from perspective of computational power's optimization (primes generation with suitable length and evidence that they are primes is computationally intensive) but simultaneously it brings entropy decreasing for keys generated this way, which can lead into simplifying the task of the potential attacker. This malfunction was addressed in the described case. The Infineon Company utilizes in its products accelerating algorithm "Fast Prime" (in case of time-limited operation). It is SW algorithm connected to the HW where it should be implemented. This algorithm was introduced in year 2000 and was certified by BSI (Federal Office for Information Security) in Germany. In the time of certification there were not identified mathematical weaknesses. The change came with discovered method, described in [16]. Utilizing of this method brings estimated complexity 45 CPU days for cipher braking in case of relevant RSA algorithm with key length 1024 bits and in average 50 CPU years in case of relevant RSA algorithm with key length 2048 bits.

Specific structure of primes that are used in eID (selection from SW library) creates for attacker possibility to make anticipatory fetching of primes and to optimize the time of factorization this way. The factorization can be parallelized, what creates another optimization potential when we take into consideration easy accessibility of computing power. Today is the worst case scenario for reaching a cost equivalent for breaking cipher:

- 1024 bits RSA with utilization of Amazon cloud - 756 USD,
- 2048 bits RSA with utilization of Amazon cloud - 40.000 USD.

Complexity of the factorization attack is not the same for all key lengths and it is not monotonously growing function.

Factorization complexity in dependence on used key length is referred at Fig.1 which is taken from [16].

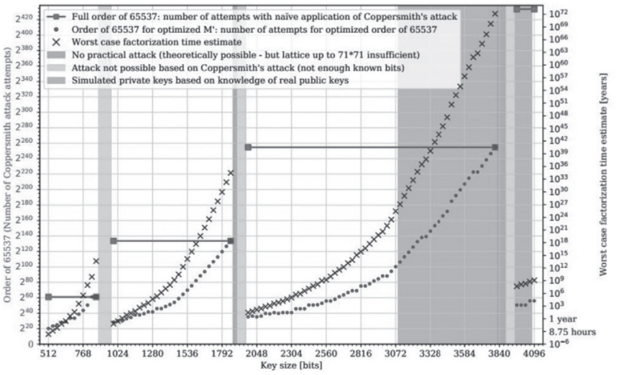

Fig. 1. The complexity of keys factorization produced by the studies RSALib with different key length [own study]

The Estimation of time for cipher breaking according to [16] is referred in Table 2

Table 2. Estimation of time for RSA algorithm breaking [own study]

Key length in bits	Rented computing power Amazon (2xIntel E5-2666 v3@2.90GHz, estimated)	Cost of energy ($0,2/kWh) (2xIntel E5-2666 v3@2.90GHz, estimated)
512 b	0,63 hours, $0,063	$0,002
1024 b	31,71 hours, $76	$1,78
2048 b	45,98 years, $40.305	$944
3072 b	9,28*10^{24} years, $8,13*10^{27}	$1,90*10^{26}
4096 b	4,18*10^{8} years, $3,66*10^{11}	$8,58*10^{9}

Efficiency of the method used for RSA secret key breaking leads to the knowledge, that in this case is the most difficult to break key with length 3072 bits and exactly this key length was chosen as a solution for current state of "eID problem" in Slovak republic.

It is the worst case scenario which leads to the most optimistic parameters of breaking from perspective of the attacker, in case if it is realised.

4. Recommendation

The RSA is today more frequently utilised technique in comparison to the ECC - it was earlier carried into life, so the time historically has built up confidence to its utilization also in connection to system tools for its assisted deployment (existing libraries). The events of the last months however brought a necessity for re-evaluation of this statement - for addressing of the growth computing power and from this fact resulting growth of risk for cipher breaking, must be implemented upgrading to the keys with higher length. This implication brings grow of requirements for storage and transport relevant to cryptographic processes – what is not always easily fulfilled. Logically can be taken as the solution ECC - as a substitution of the RSA, but this replacement is not perfect. ECC is approximately the same age as the RSA, but its deployment is delayed and therefore there is a fewer real deployments. There are many causes of these factors. For example selection of suitable elliptic curve is sensitive decision, because not every curve is suitable and secure and some curves are vulnerable by their nature [18]. More secure then generate the curve by yourself is to use some of standards, for example NIST (FIPS 186-4), ECC Brainpool, SECG, etc. Moreover is significant, relevant factor an existence of patent protection - after discovering of ECC can be recognized quite significant effort to protect by patent developed technologies, which leads into limited widening in compare with RSA for example. This fact is gradually changing because of expiring time for patent protection in case of relevant technologies.

From the perspective of encryption is on the one side the RSA slightly faster than the ECC (if we suppose comparable security), but on the other side is opposite process much faster for the ECC as compared with the RSA. It is the implication of the fact, that for the same security is in case of the ECC required shorter key length as it is for the RSA and this way is process complexity reduced.

Key length comparison in bits for equivalent security (according to the NIST) is in Table 3.

Table 3. Equivalent security for the most utilized symmetric and asymmetric algorithms [own study]

Symmetric scheme (key size in bits)	ECC-based scheme (size of n in bits)	RSA/DSA (modulus size N in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3073
192	384	7680
256	512	15360

Important attribute of a deployment is not only selection of used cryptographic algorithm, but also the way of implementation, where is HW implementation taken as cryptographically more resistant, than it is in case of SW implementation. The key is exact fulfilment of all standard conditions - for example: if some variable should be random, it must be random. There are examples, when it was expected input value, which should be random substituted by constant, which has led into cryptographic compromising of solution (as the example can be taken Sony Playstation 3).

Important aspect for comparing schemes of digital signature is not only equivalent security but also signature length. This parameter is mainly important for devices with limited computational power such as smartcards and sensor networks, where it is very important let the digital signature scheme has a very efficient signing, verifying and in some cases both of them according to the limited storage possibilities.

In Table 4 to Table 6 are referred signature length (in bits) for RSA-FDH, RSA-PSS, DSA and El Gamal and ECDSA in comparison to equivalent security. Also there are in Table 4 to Table 6 referred a hash code lengths (in bits) for individual schemes and level of security.

Table 4. Signature length for RSA-FDH and RSA-PSS schemes for individual level of security [own study]

N	Hash length	Signature length	Security
RSA-FDH			
1024	1024	1024	80
2048	2048	2048	112
3072	3072	3072	128
RSA-PSS			
1024	160-512	1024	80
2048	160-512	2048	112
3072	160-512	3072	128

Table 5. Signature length for DSA and El Gamal schemes for individual level of security [own study]

p	*q*	Hash length	Signature length	Security
DSA				
1024	160	160	320	80
2048	224	224	448	112
3072	256	256	512	128
El Gamal				
1024	-	1024	2048	80
2048	-	2048	4096	112
3072	-	3072	6144	128

Table 6. Signature length for ECDSA scheme for individual level of security [own study]

Key length	Signature length	Hash length	Security
160	320	160	80
224	448	224	112
256	512	256	128

In case of systems, where is the most important performance of digital signature scheme in use and it is not limited by system memory is another important parameter for their comparison also the performance. These applications could be classified according to the characteristic if they require fast signing or fast verification of signature. In practise is today signature verification performed much more frequently than signature generating. In consequence to this it is suitable to have schemes, where is verification not compute-intensive task. In Table 7 is compared performance of the RSA and the ECDSA signature schemes from perspective of number of required operations per second when the signature is generated and verified for individual security levels.

Table 7. Performance comparing for the RSA and the ECDSA signature schemes [own study]

	Signing [operations per second]	Verification [operations per second]
RSA-1024	6 100	93 281
RSA-2048	857	27 496
RSA-4096	118	7 370
ECDSA-224 (nistp224)	15 375	7 349
ECDSA-256 (nistp256)	9 024	3 697
ECDSA-521 (nistp521)	3 252	1 501

Note: Performance comparing was done with these characteristics: I7-2600, 3.40GHz, Ubuntu 12.04 LTS 64-bit, openssl 1.0.1, 8kB blocs

Currently it is recommended form perspective of computational security to apply cryptographic systems with exponential complexity in practise, where is time for algorithm breaking many times higher than it is length of human life according to the available PC performance. The results of experiment are referred in Table 8 [19], which was done under these conditions:

- I7-5600U CPU 2.60GHz x 4 cores,
- Theoretically 2600000000 x 4 ≈ 10000000000,
- ≈ 10.10^9 operations per second,
- Cluster with 1 000 servers,
- The Age of the Universe $13.8 \,.\, 10^9$ years.

Table 8. Computational security of cryptographic algorithm for individual key length [own study]

Strength (bits)	Time
80	3 833 years
112	16 464 665 330 209 years = 1 193 universes
128	78 190 457 universes
140	320 268 112 014 universes
192	1442359349927821335964738119…

This situation is changing in coming quantum computers. It should be noted that potential of big number factorization by using a quantum computers was described already before 20 years [20] and it brings exponential acceleration of this process in comparison to classic algorithms. Practical addressing of quantum technologies problems in its deployment [21] raises an expectation that in a few years term will be classic cryptography changed, respectively it will be transformed into the quantum-proof cryptography (for examples hash based signatures are immune to the application of quantum computers).

As a target becomes a creation of cryptographic system resistant to classic and also quantum computers but with intention of achieving interoperability with existing communication networks. One example of the project addressing this challenge is for example organizing of first PQC (Post-Quantum Cryptography) Standardization Conference announced by NIST [22] to April 2018. Anyhow these are at this moment only expectation that do not need to be completely achieved.

The RSA deployment, respectively the ECC will be definitely vital part of cryptography also for near future. As a fundamental fact can be taken continuing of research in this area, when undiscovery of fast factorization method (for the RSA) or effective discrete logarithm problem solving algorithm (for the ECC) creates an expectation that breaking of basic parts of cryptography achieves acceptable risk. The cryptography of today is based on expected interpretation of well-known open question in complexity theory, the P versus NP. Major part of cryptography belongs to class NP and mentioned expectations leads to the premise that classes P and NP are not equal and so there does not exist polynomial time for relevant algorithm breaking.

5. Conclusion

Classical cryptography reaches gradually the limits. Its original deterministic concept is under the influence of stochastic elements introducing enriched, but it can be expected that this approach will not be sufficient forever - from the perspective of barrier creation for breaking difficulty.

Digital signature signage in connection to eID are based on asymmetry assumption; signature generation (encryption) is simple but decryption is without knowledge of the key difficult (or at least knowledges how to derive it). This premise becomes problematic also because of quantum technologies progress (likewise mistakes in implementation of existing trusted cryptographic methods), as it had been in described digital signature implementation made by Infineon company. Implementation of the RSA signature scheme in the eID technology for the purpose of e-Government services providing has been noted, that by utilization of extension to Coppersmith's factorization attack it is possible to reconstruct secret key from public key by utilizing available computing power. Because of this is transition to the ECDSA signature scheme for e-Government applications mandatory.

Authors pointed out security risks of this application and they introduced comparisons to more effective digital signature schemes as well as recommendation for key length according to the equivalent and computational security in context of performance of these cryptographic systems.

Acknowledgement

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number 016ŽU-4/2018: Modernization of teaching methods of managements of industrial processes based on the concept of Industry 4.0.

Bibliography

[1] Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendment and Supplementing of certain Acts (Trust Services Act), Slovak, 2016

[2] Act No. 215/2004 Coll. on Protection of Classified Information and on Amendment and Supplementing of certain Acts as amended, Slovak, 2002

[3] FRANEKOVÁ M., RÁSTOČNÝ K.: Cryptography in safety-related systems, EDIS Žilina, 203 p., University of Žilina, Slovak, 2017

[4] LACKO Ľ.: How to deal with eID if we want to use it for digital signing, PC Revue 3rd November 2017, Slovak, 2017

[5] GOODIN D.: Millions of high-security crypto keys crippled by newly discovered flaw. Ars Technika Journal (10/2017). In: https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/ [date of access: 20.12.2017]

[6] VAUDENAY S.: A Classical introduction to Cryptography, Springer, 2009

[7] MILLER S.D., NARAYANAN B.: Coppersmith's lattices "focus group": an attack on small - exponent of RSA. August 2017, In: https://eprint.iacr.org/2017/835.pdf [date of access: 20.12.2017]

[8] SEMINARIO C.E., WILSON D.C.: Assessing Impacts of a Power User Attack on a Matrix Factorization Collaborative Recommender System. In: https://pdfs.semanticscholar.org/0764/0f89fe3a97c8b6736f609b7c333be795d69a.pdf [date of access: 20.12.2017]

[9] National Security Authority Decree No. 135/2009 Coll. on the Format and Manner of Completing Advanced Electronic Signature, Slovak 2009

[10] PKCS # 1 v.2.1 RSA Cryptography Standard, 1999

[11] ANSI X.9.31 Pseudorandom number Generator, 2011

[12] LEVICKÝ, D.: Cryptography in communication security, Elfa Košice, Slovak, 2014

[13] VAN TILBORG H.C.A., JAJODIA S.: Encyklopedia of Cryptography and Security, 2011

[14] BOS J.W., et al.: Elliptic Curve Cryptography in practice. In: https://eprint.iacr.org/2013.pdf, 2013 [date of access: 20.12.2017]

[15] RFC 5114: Additional Diffie-Hellman Groups for used of IETF Standards 2008

[16] NEMEC M., et al.: The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli, CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, p. 1631-1648, October 30-November 3, 2017, Dallas, TX, USA, Session H1: Crypto Attacks, 2017

[17] CERT Software Engineering Institute, Carnegie Mellon University, Vulnerability Notes Database, Vulnerability Note VU#307015, Infineon RSA library does not properly generate RSA key pairs, Original Release date: 16 Oct 2017, In: https://www.kb.cert.org/vuls/id/307015 [date of access: 20.12.2017]

[18] JINASENA T., MEEGAMA R., MARASINGHE R.: Access Control of Medical Images using Elliptic Curve Cryptography through Effective Multi-Key Management in a Mobile

[19] Multicasting Environment, Computer Science and Engineering, 7(1): 1-11, doi:10.5923/j.computer.20170701.01, 2017

[20] DAMIEN G.: BlueKrypt: Cryptography key lengths Recommendations. BlueKrypt v 30.4, 2017

[21] SHOR P.W.: Algorithms for quantum computation: Discrete logarithms and factoring, Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press, 1994, p. 124-134

[22] Havard University, HARVARDgazette, Science & Health / Engineering & Technology, Researchers create quantum calculator, 30th November 2017, In: https://news.harvard.edu/gazette/story/2017/11/researchers-create-new-type-of-quantum-computer/ [date of access: 20.12.2017]

[23] NIST - National Institute of Standards and Technology, Information Technology Laboratory, CSRC - Computer Security Resource Centre, Projects: Post-Quantum Cryptography, In: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography [date of access: 20.12.2017]