Crypto-World

Informační sešit GCUCMP

Ročník 4, číslo 12/2002 **17. prosinec 2002**

12/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/

(383 e-mail výtisků)

Obsah : **Str.**

Příloha : EAL4.jpg
(certifikát operačního systému W2k podle CC na EAL4)

A. Rijndael: beyond the AES

H. Joan Daemen
joan.daemen@protonworld.com
ERG Group – Proton World
Belgium

Vincent Rijmen
vincent.rijmen@cryptomathic.com
Cryptomathic NV, Belgium, and IAIK
Graz University of Technology,
Austria

I. Paulo S.L.M. Barreto
pbarreto@larc.usp.br
Laborat´orio de Arquitetura e Redes de Computadores (LARC),
Escola Polit´ecnica, Universidade de S˜ao Paulo, Brazil.

J. Abstract

In October 2000, after a 3-year evaluation process, NIST announced its decision to propose the Belgian algorithm Rijndael for the AES. In this paper, we discuss some of the work that has been done on Rijndael since its selection as the AES. We also outline briefly the design of a related cipher, called Anubis, and compare both designs.

Keywords: Rijndael, AES, Anubis

1 Introduction

In October 2000, after a 3-year evaluation process, NIST announced its decision to propose the Belgian algorithm Rijndael for the AES. In this paper, we discuss some of the work that has been done on Rijndael since its selection as the AES. The contributions can be divided into three groups. The first group consists of studies regarding implementations with improved performance. The second group consists of the study of the algorithm's resistance against newly developed cryptanalytic attacks. Lastly, we discuss some proposed changes to the algorithm, that we incorporated in the new block cipher 'Anubis', which was submitted to the NESSIE evaluation process. This paper doesn't contain a description of Rijndael. For a full specification, we refer the reader to [DR02a].

The paper is organized as follows. Section 2 treats the improvements in performance, both of software and dedicated hardware implementations. Section 3 discusses key length and Section 4 gives an overview of the most important cryptanalysis performed on Rijndael. In Section 5 we briefly discuss some techniques to protect against side channel attacks. The design of Anubis is summarized in Section 6.

2 Performance improvements

2.1 Software

Since the adoption of Rijndael as AES, many people have been implementing it in their favourite programming languages. In this section, we briefly mention two of the fastest software implementations available for a PC platform. The performance is shown in Table 1.

The implementation of B. Gladman is freely available from [Gla]. The implementation of H. Lipmaa is for sale. The implementations fix both the block length and the key length of Rijndael to 128 bits.

Author	CPU cycles/input block	Performance
B. Gladman	280	57 Mbytes/sec
H. Lipmaa	229	70 Mbytes/sec

Table 1: Performance of two hand-optimised software implementations of Rijndael. The figures given are for a 1GHz Pentium IV PC.

2.2 Hardware

The main challenge for compact or high-speed hardware implementations of Rijndael seems to be the efficient implementation of the S-box. The S-box is a nonlinear function with 8 input bits and 8 output bits. Commercially available optimisers are incapable of finding the optimal circuit fully automatically. For compact implementations, the S-box can't be implemented as a 256-byte table: instead a dedicated logical circuit has to be designed. In order to achieve maximal performance, 16 instances of the S-box have to be hardwired (neglecting the key schedule). Since 16 256-byte tables would occupy too much area, also here a dedicated logical circuit is required.

The S-box is defined as the inversion map in the finite field GF(256), followed by an affine transformation:

$$S[x] = f(x^{-1}). \tag{1}$$

Different representations for the field elements can be adopted. It is well known that the representation of the field elements influences the complexity of the inversion map $I(x) = x^{-1}$ over the field. In [Rij00], we described how a change of representation could decrease the gate complexity of a combinatorial implementation of $I(x)$. This technique has been worked out in [WOL02, SMTM01].

In these implementations, $I(x)$ is replaced by three operations:

$$I(x) = \phi^{-1}\left(i\left[\phi(x)\right]\right). \tag{2}$$

The change of representation is denoted by $\phi(x)$, and the more efficiently implementable inversion map is denoted by $i(x)$. The maps ϕ and ϕ^{-1} have to be repeated in every round. Although the implementation of ϕ^{-1} can be combined with the implementation of the affine map $f(x)$, there is still a considerable amount of overhead involved. In [SMTM01], a performance of 2.6 Gb/s is reported. This performance is obtained using 224 kgates and with a clock frequency of 224 MHz.

The authors of [RDJ+01] propose to do the change of field element representation only once, at the beginning of the cipher. Subsequently, all steps of the cipher are redefined to work with the new representation. At the end of the encryption, the data is transformed back to the original representation. This eliminates the overhead in every round. The authors report a performance of 7.5 Gb/s for a clock frequency of 32 MHz. The circuit uses 256 kgates.

3 Key length and exhaustive key search

Exhaustive key search is the basic technique of trying all key values one by one until the correct key is found. To identify the correct key it is sufficient to know a small amount of plaintext and its corresponding ciphertext. If the plaintext has some known form of redundancy, such as consisting of ASCII coded text, a small amount of ciphertext is sufficient. When a key is used for authentication, the knowledge of the MACs corresponding to few known messages is required. Exhaustive key search can in principle be mounted on any cipher. Its expected workload however is of the order 2^k executions of the block cipher if k is the length of the key. This makes exhaustive key search prohibitively expensive when the key length is large enough.

When DES was designed in the seventies, its key length of 56 bits was considered secure against exhaustive key search without a vast financial investment in hardware. However, advances in technology and computing performance have changed this and nowadays, exhaustive key search for keys of 56 bits has become practical. The current rate of increase in computing power is such that an 80-bit key should offer an acceptable level of security for another 10 or 15 years [LV01]. By 2020, an 80-bit key will be as vulnerable to exhaustive search as a 64-bit key is today, assuming a halved cost of processing power every 18 months. If we do a simple extrapolation, the shortest key length of AES, 128 bits, will become vulnerable only by the end of this century.

4 Cryptanalysis of Rijndael

Exhaustive key search is an attack that doesn't exploit the internal structure of a cipher. In this section we discuss attacks that exploit structural properties of the block cipher. These types of attack are denoted

by the term *cryptanalysis*. A cryptanalytic attack *breaks* a cipher in the academical sense if its expected workload is below that of exhaustive key search. Such an attack is called a *shortcut* attack. A paradoxical consequence of this definition is that a cipher with a longer key is easier to break in the academical sense: since the expected workload to recover a longer key by exhaustive key search is growing, it is easier to find an attack that has a lower expected workload. Hence, the existence of a shortcut attack for a given cipher does not necessarily mean that the cipher has no longer any security to offer, because most shortcut attacks described in cryptographic literature still have a prohibitively high workload, or cannot be implemented at all in a practical setting.

While exhaustive key search only requires a few plaintext-ciphertext pairs, or some ciphertext that corresponds with redundant plaintext, most shortcut attacks tend to be much more demanding. Some need huge quantities of plaintext-ciphertext pairs (*known plaintext*), in other attacks the cryptanalyst must have ciphertext values corresponding with plaintext that he has chosen (*chosen plaintext*). In so-called *related-key attacks*, the cryptanalyst must even be in a position to encipher chosen plaintexts with different (unknown) key values that have certain relations, chosen by the cryptanalyst.

Still, the presence or absence of shortcut attacks for a cipher is a quality criterion that is widely accepted in the cryptographic community. Indeed, the foremost criterion for being selected among the finalists in the AES competition was the absence of shortcut attacks. Finding shortcut attacks for the competing ciphers was the name of the game.

For many modern ciphers, no shortcut attacks are known. Nevertheless, the resistance of iterative block ciphers with respect to a specific cryptanalytic method can be evaluated by performing it on reduced-round versions of the block cipher. Attacks on reduced-round versions allow to get an idea of the *security margin* of a cipher. If for a cipher with R rounds there exists a shortcut attack against a reduced-round version with $R - r$ rounds, the cipher has an absolute security margin of r rounds or a relative security margin of r/R. Note that the discovery of an attack on a reduced-round version with $R/2$ rounds doesn't mean that the cipher is half-broken. Indeed, the complexity of most academic attacks increases exponentially in the number of rounds.

As advances in cryptanalysis of a cipher tend to enable the breaking of more and more rounds over time, the security margin indicates the resistance of the cipher against improvements of known types of cryptanalysis. However, it says nothing about the likelihood of these advances in cryptanalysis or about the resistance of the cipher against unknown attacks.

Often, for new types of cryptanalysis it is not trivial to accurately estimate the complexity of the attack. In these cases, one can get a better idea of this complexity by implementing the attack on reduced-round versions of the target cipher, where it is often infeasible to implement the attack for the full cipher.

4.1 Differential and linear cryptanalysis

Differential and linear cryptanalysis are the two most powerful general purpose cryptographic attacks known to date. Providing lower bounds for the complexity of these attacks was the main cryptographic criterion in the design of Rijndael.

In their basic form, both attacks retrieve key information from the last *round* by statistically analysing (large) amounts of plaintext/ciphertext pairs. The key information acquired is then used to find even more key bits until the full key is found. Differential cryptanalysis is a chosen-plaintext attack where plaintexts are applied in pairs that have a fixed difference. Differential cryptanalysis exploits large propagation probabilities between difference patterns in the plaintext and difference patterns at the input of the last round. Linear cryptanalysis is a known-plaintext attack that exploits large correlations between parities (linear combinations of bits) at the input of the last round with which a parity in the plaintext. Many smart techniques have been published to make these basic attacks more efficient. However, in all cases, the ability to predict large-probability difference propagations and large correlations over multiple rounds are essential for their success.

For Rijndael, we have proven an upper bound of 2^{-150} for the probability of any 4-round differential trail and of 2^{-75} for the correlation of any 4-round linear trail. In combination with the number of rounds in Rijndael, these bounds provide a high security margin against both differential and linear cryptanalysis. For a detailed treatment of these aspects, we refer to [DR02a].

4.2 Variants

After their publication, linear and differential attacks have been extended in several ways and new attacks have been published that are related to them. The best known extension is known as *truncated differentials*. We already took into account these attacks in the design of Rijndael from the start [DR02a].

Other attacks use difference propagation and correlation in different ways. This includes impossible differentials [BBS99], boomerang attacks [BDK02] and rectangle attacks [BDK02]. Thanks to the upper bounds for 4-round trails and the actual number of rounds, none of these methods of cryptanalysis have lead to shortcut attacks in Rijndael.

4.3 Saturation attacks

The most powerful cryptanalysis of Rijndael to date is the *saturation attack*. This is a chosen-plaintext attack that exploits the byte-oriented structure of the cipher and works on any cipher with a round structure similar to the one of Rijndael. It was first described in the paper presenting a predecessor of Rijndael, the block cipher Square [DKR97] and was often referred to as the Square attack.

The original saturation attack can break round-reduced variants of Rijndael up to 6 (128-bit key and state) or 7 rounds faster than exhaustive key search. N. Ferguson et al. [FKS+00] proposed some optimizations that reduce the work factor of the attack. In [Luc00], S. Lucks proposes the name *'saturation attack'* for this type of attacks. More recently, these attacks have been called 'Structural attacks' by A. Biryukov and A. Shamir [BS01] and 'Integral Cryptanalysis' by L. Knudsen and D. Wagner [KW02].

H. Gilbert and M. Minier developed also an attack that exploits the byte-oriented structure of AES [GM00]. Their attack can break a reduced version of AES with seven rounds, but it seems to be faster than exhaustive key search for 256-bit keys only.

4.4 Algebraic Structure

The round transformation of Rijndael can be decomposed into a sequence of steps in several different ways. S. Murphy and M. Robshaw observed that the decomposition can be defined in such a way that the steps of the round transformation have a low algebraic order [MR00].

The algebraic order of a transformation f equals the number of different transformations that can be constructed by repeated application of f: f, $f \circ f$, $f \circ f \circ f$, ... Until now, this observation on *some of the components* of the round transformation hasn't led to any cryptanalytical attack. On the contrary, R. Wernsdorf proved recently that the *full round transformation* of Rijndael generates the alternating group [Wer02]. This shows that the algebraic order of the round transformation isn't low.

J. Fuller and W. Millan made an observation on the structure of the S-box that is used in Rijndael [FM]. The S-box can be described as 8 Boolean functions f_i with 8 common input bits. J. Fuller and W. Millan observed that the 8 Boolean functions are related to one another:

$$f_i(x) \equiv f_j(g_{ij}(x)) + c_{ij} \quad . \tag{3}$$

Here the c_{ij} are constants and the functions g_{ij} are linear functions. This implies Rijndael can be described by means of one non-linear Boolean function and some linear/affine operations. The observation is a consequence of the mathematical definition of the S-box. In the same way as the repeated use of a single S-box doesn't lead to an attack, also this observation is by no means a weakness, but rather an illustration of the simplicity of the design of the cipher.

4.5 Algebraic attacks

The transparent algebraic structure of Rijndael has encouraged several teams of researchers to investigate the security of Rijndael against algebraic solving methods. Typically, an algebraic attack consists of two steps.

1. Collecting step: The cryptanalyst expresses the cipher as a set of *simple* equations in a number of variables. These variables include bits (or bytes) from the plaintext, ciphertext and the key, and typically also of intermediate computation values and round keys. The term *simple* can be defined very loosely as *suitable for the next step.*

2. Solving step: the cryptanalyst uses some data input such as plaintext-ciphertext pairs, substitutes these values in the corresponding variables in the set of equations collected in step 1 and tries to solve the resulting set of equations, thereby recovering the key.

Rijndael can be expressed with elegant equations in several ways. Whereas in many other cipher designs the structure is obscured by the addition of many complex operations, in Rijndael the inner structure is very simple and transparent, clearly facilitating the expression of the cipher as a set of simple equations. The key issue to be judged however, is whether equations that look elegant to the mathematician's mind, are also simple to solve. Several attempts have been made to construct algebraic attacks for Rijndael. None have resulted in shortcut attacks as yet, and most of the papers conclude that more research is required. In the following sections we discuss a number of attempts.

4.5.1 Continued fractions

Ferguson, Schroeppel and Whiting [FSW01] derive a closed formula for Rijndael that can be seen as a generalisation of continued fractions. Any byte of the intermediate result after 5 rounds can be expressed as follows.

$$x = K + \sum \frac{C_1}{K^* + \sum \frac{C_2}{K^* + \sum \frac{C_3}{K^* + \sum \frac{C_4}{K^* + \sum \frac{C_5}{K^* + p_*^*}}}}} \tag{4}$$

Here every K is some expanded key byte, each C_i is a known constant and each $*$ is a known exponent or subscript, but these values depend on the summation variables that enclose the symbol.

A fully expanded version of (4) has 2^{25} terms. In order to break 10-round Rijndael, a cryptanalyst could use 2 equations of this type. The first one would express the intermediate variables after 5 rounds as function of the plaintext bytes. The second equation would cover rounds 6–10 by expressing the same intermediate variables as a function of the ciphertext bytes. Combining both equations would result in an equation with 2^{26} unknowns. By repeating this equation for $2^{26}/16$ known plaintext/ciphertext pairs, enough information could be gathered to solve for the unknowns, in an information-theoretic sense. It is currently unknown what a practical algorithm to solve this type of equations would look like.

4.5.2 XSL

Courtois and Pieprzyck [CP] observe that the S-box used in Rijndael can be described by a number of implicit quadratic Boolean equations. If the 8 input bits are denoted by $x_1, \ldots x_8$, and the 8 output bits by $y_1, \ldots y_8$, then there exist equations of the form

$$f(x_1, \ldots, x_8, y_1, \ldots y_8) = 0, \tag{5}$$

where the algebraic degree of f equals two.

In principle, 8 equations of the type (5) suffice to define the S-box, but Courtois and Pieprzyck observe that more equations of this type can be constructed. Furthermore, they claim that these extra equations can be used to reduce the complexity of the solving step.

In the first step of the XSL method, equations are collected that describe the output of every sub-block of the cipher as a function of the input of the same sub-block. As a result, the cryptanalysts get a system of 8000 quadratic equations in 1600 unknowns, for the case of Rijndael, where the linear steps are ignored for sake of simplicity.

The most difficult part of the XSL method is to find an efficient elimination process. Courtois and Pieprzyck estimate that for Rijndael the complexity would be 2^{230} steps. For Rijndael with 256-bit keys, the complexity would be 2^{255} steps. As an extension, they propose to use cubic equations as well. For that case, the complexity for Rijndael with 256-bit keys may drop to 2^{203} steps in their most optimistic estimation. All these complexity estimations are made under the (optimistic) assumption that the Gaussion elimination method for linear equations can be implemented in a complexity $\mathcal{O}(n^{2.4})$. It is still a topic of debate whether the assumptions of Courtois and Pieprzyck are valid and the XSL attack will work at all.

4.5.3 Embedding

Murphy and Robshaw [MR02] define the block cipher BES, which operates on data blocks of 128 bytes instead of bits. According to Murphy and Robshaw, the algebraic structure of BES is even more elegant and simple than that of Rijndael. Furthermore, Rijndael can be *embedded* into BES. There is a map ϕ such that:

$$\text{Rijndael}(x) = \phi^{-1}\left(\text{BES}\left(\phi(x)\right)\right). \tag{6}$$

Murphy and Robshaw proceed with some observations on the properties of BES. However, these properties of BES do not translate to properties of Rijndael.

Murphy and Robshaw believe that when the XSL method is applied to BES, the complexity of the solving step could be significantly smaller than in the case where XSL is directly applied to Rijndael (cf. Section 4.5.2).

5 Side-channel attacks

Besides mathematical-cryptanalytic attacks on the *algorithm*, also the resistance of *implementations* against side-channel attacks, is of importance. Side-channel attacks exploit weaknesses of the implementation of the algorithms rather than those in the algorithms themselves and are particularly important for smartcards. The best-known examples of these attacks are: timing analysis, simple power analysis, differential power analysis and electro-magnetic analysis.

Implementing Rijndael in a way that resists timing analysis and simple power analysis, was explained already in [DR02a]. Security against differential power analysis seems more difficult to achieve. All currently proposed techniques are variations on the *masking* approach: instead of processing the actual inputs x, only the values a and $x \oplus a = b$ are processed, where a is a randomly generated *mask*. Only at the end of the encryption operation, both values are recombined to compute the output. In general, different masks have to be used for different types of operations.

In [Mes01], it is proposed to implement Rijndael using two operations only:

binary XOR: this operation can easily be protected, and

table lookup: the author proposes to replace every table T by a table T', with

$$T'[x] = T[x \oplus a] \oplus b, \tag{7}$$

where a is the input mask, and b the output mask. Both masks are chosen at the beginning of the encryption and used to compute the version of T' that will be used for that encryption.

In [AG01], the authors propose to implement Rijndael using operations the finite field operations 'addition' (XOR) and 'multiplication'. A conversion rule is given to compute 'multiplicative' masks from 'additive' masks. Alas, in [GT], the authors describe a weakness found in the method of [AG01].

Since the study of electro-magnetic analysis has only started, it is too early to evaluate the danger it represents for modern smartcards, and how it can be countered.

6 Anubis

Anubis is another block cipher designed according to the Wide Trail design strategy [BR00, Anu]. It is in many ways similar to Rijndael and its predecessor, Square. Similar to Rijndael and Square, Anubis encrypts blocks of 128 bits, which are internally represented as 16 bytes arranged in a 4-by-4 matrix. The round transformation of Anubis is composed of similar steps as in Rijndael and Square.

The most important differences between Anubis and Rijndael are the following:

The involutional structure: In Anubis, all steps are involutions. This implies that the implementation of the decryption operation can be the same as the encryption operation, except for a change in the key schedule. This should in principle reduce the code size or area in software, respectively hardware applications that implement both encryption and decryption.

The different S-box: The S-box of Anubis is generated in a pseudo-random way. The advantage of this method is that providing a simple mathematical description seems more difficult. The polynomial expansion of the S-box is certainly more involved. The disadvantages are the suboptimal differential and linear properties, and possibly a more complex hardware implementation.

A more complex key scheduling: The advantage is the improved resistance against key based attacks, in particular the shortcuts for long keys. The disadvantage is the higher cost: slower execution, a reduced key agility, larger code or gate count.

Two versions of Anubis have been defined. Their only difference lies in the choice of the S-box used (cf. Section 6.1.4).

We will now discuss some components of Anubis in more detail. Space restrictions forbid us to explain all components in detail. For a complete treatment, we refer the reader to [BR00].

6.1 Round transformation

The round transformation of Anubis is composed of 4 steps, with a similar functionality as the steps in the round transformation of Rijndael. For ease of reading, we use the nomenclature of Rijndael in order to denote the steps. In the design document of Anubis, different names are used [BR00].

One encryption with Anubis consists of $8 + N$ iterations of the round transformation, where N denotes the key length in 32-bit words. Similar to Rijndael, the last round uses a slightly modified round transformation, and there is one additional iteration of the step AddRoundKey.

6.1.1 AddRoundKey

The round key addition, is exactly the same in Anubis as in Rijndael: bit-wise addition with the round key. This transformation is an involution.

6.1.2 MixColumns

In Rijndael, the MixColumns step is defined as a multiplication of the columns with the matrix M. In Anubis, the matrix H is used instead.

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}, \qquad H = \begin{bmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{bmatrix}. \tag{8}$$

Exactly as with Rijndael, all operations on bytes are defined as operations in the finite field $\mathrm{GF}(2^8)$, using the polynomial representation. The reduction polynomial for Anubis however, is different from the used in Rijndael. The matrix H is symmetric and unitary: $H^{-1} = H^T = H$. Consequently, multiplication with H is an involution. The branch number of this step equals 5, like for MixColumns in Rijndael. The matrix H has small coefficients, in order to retain the good performance of implementations on smart-cards.

6.1.3 ShiftRows

The purpose of the step ShiftRows is to spread the bytes of each input column to different output columns.

Anubis doesn't use the ShiftRows step of Rijndael. Instead, the state matrix is transposed, as is done in Square. Clearly, matrix transposition is an involution.

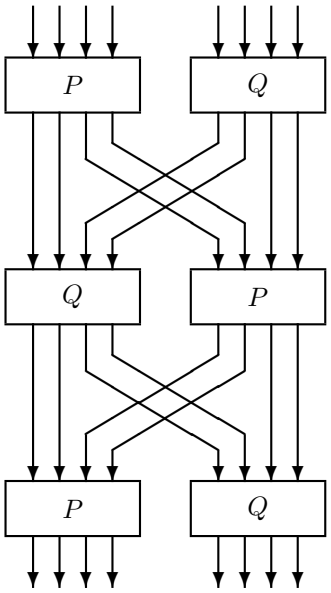
6.1.4 SubBytes

The S-box used in Anubis is a self-inverse S-box: $S[S[x]] = x, \forall x$. The following design criteria for the S-box were used:

- The propagation probability of all non-zero input differences must not exceed 8×2^{-8}.
- The correlation between input bits and output bits must not exceed 16×2^{-6}.
- The nonlinear order of all linear combinations of the output functions must not be below 7.

In the first version of Anubis, the S-box was generated in a pseudo-random way, and had no further structure. However, we learned that the lack of structure hinders efficient hardware implementation. Moreover, a flaw in the random search program resulted in the selection of an S-box with a correlation 17×2^{-6}, violating a design criterion.

Therefore, we defined a new version of Anubis, using an alternative S-box that, besides exactly satisfying the design conditions, is amenable to much more efficient implementation in hardware. This S-box is illustrated in figure 1. The P and Q tables are pseudo-randomly generated involutions with similar design criteria as the S-box, and chosen so that the S-box satisfies the design criteria. Table 2 shows the involutions found by the searching algorithm.



[htb]

Figure 1: Structure of the Anubis S-box. Both P and Q are pseudo-randomly generated involutions; the output from the upper and middle nonlinear layers are mixed through a simple linear shuffling.

Table 2: Mini-boxes P and Q.

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P[u]$	3	F	E	0	5	4	B	C	D	A	9	6	7	8	2	1
$Q[u]$	9	E	5	6	A	2	3	C	F	0	4	D	7	B	1	8

6.2 Key scheduling

Anubis is defined to operate with key lengths of $32N$ bits, with $4 \leq N \leq 10$. The key schedule consists of two steps. In the first step, the *key evolution function* ψ is used repeatedly to expand the key K into $9 + N$ intermediate keys κ_r of $32N$ bits:

$$\kappa_0 = K, \quad \kappa_1 = \psi(K), \quad \kappa_2 = \psi(\kappa_1), \ldots \ . \tag{9}$$

In the second step, the *key selection function* ϕ is used to extract the round keys k_r from the intermediate keys:

$$k_r = \phi(\kappa_r), \ \ \forall r \ . \tag{10}$$

The purpose of this scheme is to make key guessing attacks as in [Luc00] impossible.

6.3 Involutional structure

With Rijndael, the decryption operation differs significantly from the encryption operation. Although it is possible to implement the decryption operation in such a way that it has the same succession of steps as the encryption operation, the components used in the steps (S-box, matrix, shift offsets) are different.

With Anubis, all the individual steps are involutions. Hence, it becomes possible to implement the decryption operation in such a way that only the key scheduling is different from the encryption operation. We call this an *involutional structure*.

Involutional structure is found as part of many cipher designs. All classical Feistel networks have this property, as do some more general iterated block ciphers like IDEA [LMM91]. Self-inverse ciphers similar to Anubis were described and analyzed in [YTH96, YMT97].

Besides the advantages for implementation, an involutional structure also automatically implies equivalent security of encryption and decryption [KW].

7 Conclusions

Efficient implementations of Rijndael have been realised in software and dedicated hardware. On top of that, research has been done on techniques to make these implementations secure against side channel attacks.

We have discussed the complexity of exhaustive key search and shown that applying this attack to Rijndael is not expected to be feasible in the foreseeable future. Many attempts have been made to find weaknesses in Rijndael. Although this has lead to some interesting research providing new insights in Rijndael, it has not resulted in any shortcut attacks.

The design of Anubis follows the structure of Rijndael, but several components have been replaced by alternatives. We discussed some advantages and disadvantages of these alternative choices.

References

[AES00] *Proceedings of the third AES candidate conference*, New York, April 2000.

[AG01] Mehdi-Laurent Akkar and Christophe Giraud. An implementation of DES and AES, secure against some attacks. In Çetin K. Koç and Paar [ÇKKP01], pages 309–318.

[Anu] Homepage of the block cipher anubis. http://planeta.terra.com.br/informatica/paulobarreto/AnubisPage.html.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *Advances in Cryptology, Proceedings of Eurocrypt '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–24. Springer-Verlag, 1999.

[BDK02] Eli Biham, Orr Dunkelmann, and Nathan Keller. New results on boomerang and rectangle attacks. In Daemen and Rijmen [DR02b], pages 1–16.

[BR00] Paulo S.L.M. Barreto and Vincent Rijmen. The Anubis block cipher. In *First open NESSIE Workshop*, Leuven, November 2000.

[BS01] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In Birgit Pfitzmann, editor, *Advances in Cryptology, Proceedings of Eurocrypt '01*, volume 2045 of *Lecture Notes in Computer Science*, pages 394–405. Springer-Verlag, 2001.

[ÇKKP01] David Naccache Çetin K. Koç and Christophe Paar, editors. *CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*. Springer-Verlag, 2001.

[CP] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. Available from IACR's e-Print server.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *Fast Software Encryption '97*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer-Verlag, 1997.

[DR02a] Joan Daemen and Vincent Rijmen. *The design of Rijndael, AES — the advanced encryption standard*. Springer-Verlag, 2002.

[DR02b] Joan Daemen and Vincent Rijmen, editors. *Fast Software Encryption '02*, volume 2365 of *Lecture Notes in Computer Science*. Springer-Verlag, 2002.

[FKS+00] Niels Ferguson, John Kelsey, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In AES3 [AES00], pages 213–231.

[FM] Joanne Fuller and William Millan. On linear redundancy in the AES S-box. Available from IACR's e-Print server.

[FSW01] Niels Ferguson, Richard Schroeppel, and Doug Whiting. A simple algebraic representation of Rijndael. draft, 2001.

[Gla] Brian Gladman. Implementations of AES (Rijndael) in C/C++ and Assembler. http://fp.gladman.plus.com/cryptography_technology/rijndael/.

[GM00] Henri Gilbert and Marine Minier. A collision attack on 7 rounds of Rijndael. In AES3 [AES00], pages 230–241.

[GT] J. Dj. Goliç and C. Tymen. Multiplicative masking and power analysis of AES. In Çetin K. Koç, editor, *CHES 2002*, Lecture Notes in Computer Science, *to appear*.

[KW] Lars R. Knudsen and David Wagner. On the structure of Skipjack. to appear in Discrete Applied Mathematics.

[KW02] Lars Knudsen and David Wagner. Integral cryptanalysis. In Daemen and Rijmen [DR02b], pages 112–127.

[LMM91] Xuija Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *Advances in Cryptology, Proceedings of Eurocrypt '91*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer-Verlag, 1991.

[Luc00] Stefan Lucks. Attacking 7 rounds of Rijndael under 192-bit and 256-bit keys. In AES3 [AES00], pages 215–229.

[LV01] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255–293, 2001.

[Mes01] Thomas S. Messerges. Securing the AES finalists against power analysis attacks. In Bruce Schneier, editor, *Fast Software Encryption '00*, volume 1978 of *Lecture Notes in Computer Science*, pages 150–164. Springer-Verlag, 2001.

[MR00] Sean Murphy and Matt J.B. Robshaw. New observations on rijndael. http://www.isg.rhbnc.ac.uk/∼sean/rijn_newobs.pdf, August 2000.

[MR02] Sean Murphy and Matt J.B. Robshaw. Essential algebraic structure within the aes. In Moti Yung, editor, *Advances in Cryptology, Proceedings of Crypto 2002*, Lecture Notes in Computer Science. Springer-Verlag, 2002.

[RDJ+01] Atri Rudra, Pradeep K. Dubey, Charanjit S. Jutla, Vijay Kumar, Josyula R. Rao, and Pankaj Rohatgi. Efficient Rijndael encryption implementation with composite field arithmetic. In Çetin K. Koç and Paar [ÇKKP01], pages 171–184.

[Rij00] Vincent Rijmen. Efficient implementation of the Rijndael S-box. http://www.esat.kuleuven.ac.be/∼rijmen/rijndael/sbox.pdf, 2000.

[SMTM01] Akashi Satoh, Sumio Morioka, Kohji Takano, and Seiji Munetoh. A compact Rijndael hardware architecture with S-box optimization. In Colin Boyd, editor, *Advances in Cryptology, Proceedings of Asiacrypt 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 239–254. Springer-Verlag, 2001.

[Wer02] Ralph Wernsdorf. The round functions of Rijndael generate the alternating group. In Daemen and Rijmen [DR02b], pages 143–148.

[WOL02] Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger. An ASIC implementation of the AES S-boxes. In Bart Preneel, editor, *Topics in Cryptology — CT-RSA 2002*, Lecture Notes in Computer Science, pages 67–78. Springer-Verlag, 2002.

[YMT97] A.M. Youssef, S. Mister, and S.E. Tavares. On the design of linear transformations for substitution permutation encryption networks. In *Workshop on Selected Areas in Cryptography, SAC'97*, Workshop record, pages 40–48, 1997.

[YTH96] A.M. Youssef, S.E. Tavares, and H.M. Heys. A new class of substitution-permutation networks. In *Workshop on Selected Areas in Cryptography, SAC'96*, Workshop record, pages 132–147, 1996.

B. Kryptografie a normy - Digitální certifikáty. IETF-PKIX.
Část 7. Protokol OCSP v2. (Online Certificate Status Protocol). Protokoly DPV (Delegated Path Validation) a DPD (Delegated Path Discovery).

Jaroslav Pinkava, PVT, a.s.
Jaroslav.pinkava@pvt.cz

1. Verze 2 protokolu OCSP

V minulé části byl popsán protokol OCSP (dle RFC 2560, lit. [2]), který umožňuje zjišťovat aktuální stav (platnost) digitálního certifikátu bez nutnosti užití CRL. Klient protokolu OCSP dává požadavek (vzhledem k statutu certifikátu) vůči odpovídající straně (OCSP responder) a pozdrží akceptaci certifikátu do té doby než dostane odpověď na svůj požadavek. Samotný protokol specifikuje obsah a formát dat, která budou vyměněna mezi aplikací, která ověřuje statut certifikátu a serverem, který poskytuje tento statut. Nedávno (říjen 2002) vyšel nový draft (draft-ietf-pkix-ocsp-v2-ext-00.txt, lit. [3]), který specifikuje rozšíření OCSP protokolu a definuje verzi 2 protokolu. Tato verze dává k dispozici další pracovní prostředky a umožňuje rovněž tak zjišťovat revokační statut jak certifikátů veřejného klíče, tak atributového certifikátu.

Rozšíření serviceLocator lze využít při vytváření požadavku pro server OCSP (který zodpovídá za identifikaci certifikátu). Klient vyplní toto rozšíření kopií pole AuthorityInfoAccess (AIA) z certifikátu, které specifikuje adresu serveru OCSP.

Pokud však CA, která tento certifikát vydala, vydává pouze CRL a klient chce komunikovat s daným OCSP serverem, pak tento server nemusí znát, kde je příslušné CRL přístupné. Z tohoto důvodu je definováno nové rozšíření, které toto (tj. alokaci CRL) serveru OCSP umožní. Toto rozšíření nese označení crlLocator. Klient toto rozšíření může vyplnit kopií pole CDP (CRLDistributionPoints) z certifikátu (zde je adresa úložiště CRL).

V praxi je v řadě případů efektivnější nejprve se přesvědčit, zda certifikát není odvolán (než bude budována certifikační cesta a podnikán přístup do úložiště – např. pomocí LDAP). Cílem daného rozšíření je tedy umožnit serveru OCSP naplnění služby a to i v situacích, kdy server nezná adresu certifikační autority.

Protokol OCSP v2. umožňuje stejně jako první verze práci s pouhým CertID (z důvodů zpětné kompatibility), ale umožňuje také následující dvě možnosti:

a) odeslání celého certifikátu;
b) odeslání jména vydávající strany, pořadového čísla certifikátu, hashe nad polem tbsCertificate (kódování DER) a podpisu certifikátu (tj. vybraných částí certifikátu – důvodem může být ochrana informací).

Odpověď serveru OCSP je pak konstituována stejným způsobem.
Takto OCSP servery mohou využít informace obsažené v CRL a transformovat je do svých odpovědí. Toto umožňuje klientům podporovat OCSP protokol i v situacích, kdy CA vydává CRL

2. Protokol DPV

Účelem tohoto protokolu (a protokolu DPD, o kterém bude řeč v odstavci 3) je provést určitou analýzu certifikační cesty (pro certifikát veřejného klíče). Přitom protokol DPV (dotaz – odpověď) požaduje na serveru provést ověření této certifikační cesty (a nevyžaduje získání žádných dat). Naproti tomu protokol DPD (dotaz – odpověď) lze použít pro získání veškeré potřebné informace (např. získání kořenového certifikátu, certifikátů certifikační autority, kompletního CRL, delta-CRL, odpovědí OCSP), která je nezbytná pro místní ověření platnosti certifikátu.

Protokol DPV umožňuje serveru provést ověření certifikátu v reálném čase pro definovaný časový moment T (přitom T může být aktuální čas nebo čas, který již nastal – tj. v minulosti).

Pro ověření certifikátu může být vyžadován řetězec několika certifikátů (ten se nazývá certifikační cestou). Přenesení požadavku ověření této cesty na server může být požadováno klientem, který momentálně nedisponuje potřebnými kapacitami (procesními či komunikačními) pro jeho provedení. Samozřejmě klient v této situaci důvěřuje příslušnému serveru ve stejné míře, v jaké by důvěřoval vlastnímu softwaru pro ověření certifikátu (pokud by takový provozoval).

Klienti přitom mohou uložit serveru provést ověření certifikátu v rámci dané specifikované politiky pro ověřování certifikátů. Server, pokud tuto politiku nepodporuje vrací jako svůj výsledek chybu. Pokud požadavek neobsahuje specifikaci ověřovací politiky, pak server ve své odpovědi indikuje, kterou politiku použil. Definice politik mohou být poměrně dlouhé a komplexní, mohou požadovat některé vstupní parametry (např. kořenové certifikáty). Klient může požadovat časový moment ověření, který je odlišný od aktuálního času. Pokud není informace o revokačním statutu v daném okamžiku (obsaženém v požadavku) dostupná, musí DPV server vrátit jako odpověď, že certifikát je neplatný. Informaci lze doplnit důvody, které vedly k tomuto závěru. DPV server musí mít certifikát, který ověřuje, ať již ho získá přímo od klienta, resp. získá ho jinou cestou.

Výstupem je jedna z následujících čtyř odpovědí DPV serveru:
- certifikát je platný dle dané ověřovací politiky;
- certifikát není platný dle dané ověřovací politiky (+důvod);
- platnost certifikátu dle dané ověřovací politiky není známa;
- platnost nelze ověřit vzhledem k chybě.

Protokol musí obsahovat ochrany proti znovuzaslání (replay attack), odpověď musí být autentizována příslušným DPV serverem – digitálně podepsána pomocí serverového certifikátu.

3. Protokol DPD

Protokol DPD má význam pro ty klienty, kteří provádí sami patřičné procesy v rámci PKI a požadují na serveru pouze, aby jim získal všechny potřebné informace. Důvěra v server spočívá v tom, že klient spoléhá na to, že server získá nejaktuálnější potřebné informace.

Ověření cesty pak provede sám klient. Vzhledem k tomu, že požadovaná data jsou digitálně podepsaná, klient nemusí věřit serveru více než věří příslušným úložištím.

Užitečnost protokolu DPD je několikerá. Místo vícenásobného požadavku na přístup k potřebným informacím je formulován pouze jediný požadavek (přitom řada informací může být uložena v cache samotného serveru). Klientský software nemusí přitom obsahovat diverzifikované procedury pro získání informací různých typů, z různorodých úložišť a pomocí celé řady protokolů různých typů. Klient musí umět specifikovat své potřeby včetně politiky pro ověřování a DPD server musí být schopný tuto politiku použít. Standardně vrací DPD server jako odpověď jednu certifikační cestu ke každému koncovému certifikátu. Musí však umět naplnit i další požadavky klienta (např. více cest ke koncovému certifikátu, požadavek na přítomnost určitých rozšíření atd.).

Odpověď DPD musí indikovat jednu z následujících pěti možností:
- jedna či více certifikačních cest byla nalezena dle politiky ověřování cest, spolu se vší požadovanou informací;
- jedna či více certifikačních cest byla nalezena dle politiky ověřování cest, spolu s podmnožinou požadovaných informací;
- jedna či více certifikačních cest byla nalezena dle politiky ověřování cest, bez požadovaných informací;
- nebyla nalezena žádná certifikační cesta ve smyslu dané politiky ověřování cest;
- cesta nemohla být zkonstruována v důsledku chyby.

Odpověď může být autentizována.

Oba protokoly (DPV a DPD) mohou probíhat v zabezpečeném režimu nižší úrovně. Dokument (lit. [4]) se dále v odstavcích 7 a 8 zabývá pojmy politika ověřování certifikátů a politika ověřování certifikačních cest, jejich komponentami a dalšími souvisejícími otázkami.

1. Literatura

[1] PKIX Working Group:
http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html.

[2] RFC 2560-Online Certificate Status Protocol - OCSP:
http://www.ietf.cnri.reston.va.us/rfc/rfc2560.txt

[3] draft PKIX: Online Certificate Status Protocol, version 2,
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-ocspv2-ext-00.txt

[4] RFC 3379: Delegated Path Validation and Delegated Path Discovery
Protocol Requirements, http://www.ietf.cnri.reston.va.us/rfc/rfc3379.txt

C. Profil kvalifikovaného certifikátu
Část I.

Jan Hobza, ÚOOÚ , Odbor elektronického podpisu
Jan.Hobza@uoou.cz

Abstrakt

Tento příspěvek se zabývá právní analýzou požadavků na obsah kvalifikovaného certifikátu podle Směrnice Evropského parlamentu a Rady o zásadách společenství pro elektronické podpisy 1999/93/ES (dále jen Směrnice) a zákona č. 277/2000 Sb., o elektronickém podpisu (dále jen Zákon) a návrhem implementace těchto požadavků do ASN.1 struktury certifikátu v3 X.509.

Směrnice obsahuje v příloze č. I seznam povinných položek kvalifikovaného certifikátu. Jedná se o slovní popis obsahu položek, které musí minimálně obsahovat každý kvalifikovaný certifikát vydaný v intencích Směrnice. Možným řešením struktury certifikátu ve smyslu směrnice 1999/93/ES se zabývá dokument TS 101862 „Qualified certificate profile“ vydaný ETSI. V tomto dokumentu je navržena doporučovaná struktura čtyř položek kvalifikovaného certifikátu podle zmíněných požadavků směrnice. Implementace ostatních požadavků na kvalifikovaný certifikát musí odpovídat RFC 3039. Oba tyto dokumenty vycházejí z RFC 2459, respektive RFC 3280.

Zákon o elektronickém podpisu stanoví požadavky na údaje obsažené v kvalifikovaném certifikátu v §12. Některé tyto požadavky se ovšem přesně nekryjí s výše uvedenými požadavky směrnice na obsah kvalifikovaného certifikátu. Ač měl zákonodárce zjevný úmysl držet se co možná pevně dikce Směrnice, ne ve všech ustanoveních Zákona se mu to podařilo. Autor se v příspěvku zabývá zkoumání především těchto odchylek § 12 Zákona od Směrnice a snaží se nalézt jejich řešení v rámci platného práva a best-practices v oboru.

Text příspěvku obsahuje srovnání a rozbor jednotlivých bodů § 12 Zákona a přílohy č.I Směrnice. U každého bodu je nastíněno řešení požadavků Směrnice v rámci již existujících technických dokumentů a navrženo řešení požadavků Zákona. U každého návrhu je uvedena ASN.1 struktura podle X.680 (1997). Účelem uvádění příkladných struktur položek v ASN.1 není snaha o přímou implementaci řešení, ale snaha přiblížit problematiku na názorných příkladech. Tam, kde je to smysluplné, jsou uvedeny i konkrétní hodnoty atributů či položek certifikátu. V bodech, kde se oba předpisy shodují, je pouze informativní oznámení o způsobu řešení, které volí TS 101 862, nebo vychází RFC, neboť je podle autora zbytečné zatěžovat posluchače rešerší z dostupných standardů.

Příspěvek podává návrh na vytvoření profilu kvalifikovaného certifikátu v rámci platných právních předpisů. Výhodou vytvoření takového profilu znamená možnost jasně definovat požadavky na produkt a pro poskytovatele certifikačních služeb jasně deklarovat připravenost produktu – kvalifikovaného certifikátu – pro akreditační schéma a rozvíjející trh. Zároveň je i impulsem pro vývoj kompatibilních aplikací a krokem k interoperabilitě s produkty elektronického podpisu v Evropské unii. Zároveň je třeba podotknout, že stejně jako v Evropské unii, znamená vytvoření profilu kvalifikovaného certifikátu jen možnost přistoupení subjektů na trhu k plnění takového dokumentu. Jeho dodržování tedy není závazné, pokud si ho sám poskytovatel jako závazné nepřijme, ale má být výhodou, podobně jako dodržování řady standardů ISO (např. ISO 9000).

Cílem příspěvku je také dát podnět k obecné diskusi na toto téma, zvážit opodstatněnost požadavků na vytvoření profilu pro kvalifikované certifikáty mezi experty a případně začít sbírat komentáře a připomínky k obsahu příspěvku. Samotný text ještě nemůže

být hotovým Profilem kvalifikovaného certifikátu. Autor ale doufá, že může být platformou pro budoucí diskuse nad nastíněným problémem.

Klíčová slova: kvalifikovaný certifikát, položka, atribut, rozšíření, prohlášení, zákon o elektronickém podpisu, směrnice Evropského parlamentu 1999/93/ES, syntaxe, identifikátor, klíč.

1. Úvod

Zákon o elektronickém podpisu stanoví požadavky na údaje obsažené v kvalifikovaném certifikátu v §12. Některé tyto požadavky se ovšem přesně nekryjí s požadavky směrnice na obsah kvalifikovaného certifikátu:

Příloha I Směrnice 1999/93/ES:	**§ 12 zákona č. 227/2000 Sb.:**
a) označení, že certifikát je vydán jako kvalifikovaný certifikát,	a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,
b) označení poskytovatele certifikačních služeb a státu, ve kterém má poskytovatel sídlo,	b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,
c) jméno podepisující osoby nebo pseudonym, který je jako takový označen,	c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,
d) zvláštní znaky podepisující osoby, pokud jsou důležité pro účel, pro nějž je certifikát určen,	d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, která jsou pod kontrolou podepisující osoby;	e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
f) označení počátku a konce doby platnosti certifikátu,	h) počátek a konec platnosti kvalifikovaného certifikátu,
g) identifikační kód certifikátu,	g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,
h) zaručený elektronický podpis poskytovatele certifikačních služeb, který certifikát vydává,	f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,
	i) případně údaje o tom, zda se používání

Na rozdíl od situace v Evropské unii, kde ETSI vydal dokument TS 101862, neexistuje u nás žádný obdobný dokument, který by se s těmito odlišnostmi (po technické stránce) vypořádal. Hlavním cílem tohoto příspěvku je tedy navrhnout koncept profilu kvalifikovaného certifikátu, který by odpovídal požadavkům zákona o elektronickém podpisu, nebyl by v rozporu s požadavky směrnice 1999/93/ES a zároveň byl v souladu s doporučeními příslušných dokumentů ETSI a RFC. Díky platnému znění zákona o elektronickém podpisu a díky uvedeným rozdílům v § 12 a příloze č. I směrnice zde stojíme ale před několika problémy.

V některých částech ustanovení § 12 jsou spojeny údaje požadované v kvalifikovaném certifikátu s právními pojmy, na jejichž výkladu je pak závislý i způsob implementace údajů ve struktuře certifikátu. V těchto bodech se kvalifikovaný certifikát vydaný podle zákona liší

od kvalifikovaného certifikátu ve smyslu směrnice a poměrně komplikované je zde i naplnění doporučení příslušných RFCs.

Některé položky kvalifikovaného certifikátu odkazují na objekty, které jsou mimo rámec jeho vydavatele. Vzhledem k odlišnému českému akreditačnímu schématu nad poskytovateli certifikačních služeb vydávajících kvalifikované certifikáty od evropského akreditačního schématu není možné tyto objekty zaměnit. Příspěvek se zabývá i řešením odlišností v těchto objektech.

2. Obsah položek

2.1 Bod a) Směrnice - označení, že certifikát je vydán jako kvalifikovaný certifikát

Požadavek na označení, že daný certifikát je vydán jako kvalifikovaný certifikát, je pro oba předpisy téměř shodný. Označení se bude pouze lišit v identifikaci předpisu, podle kterého je vydán [2,4]. Do doby, než bude české akreditační schéma v souladu se Směrnicí, než bude náš právní řád odpovídat požadavkům Směrnice, než budou u nás nastaveny technické požadavky na poskytovatele, produkty a certifikáty odpovídající požadavkům příloh I, II a III, nebude možné označovat české kvalifikované certifikáty jako kvalifikované certifikáty podle Směrnice.

V našem prostředí je požadavek bodu a) možné naplnit dvěma následujícími způsoby, případně jejich kombinací:

1. Certificate Policies extension:

Pokud má tato položka sloužit k naplnění bodu a), Certifikační politika identifikovaná v certificatePolicies extension [5,6] musí jasně vyjadřovat, že poskytovatel vydal tento certifikát jako kvalifikovaný podle platných právních předpisů. V zájmu zachování co nejširší interoperability kvalifikovaných certifikátů je vhodné identifikovat certifikační politiku v této položce pouze pomocí OID. Pokud poskytovatel či zúčastněná strana požaduje kvalifikátor certifikační politiky, je vhodné používat jen CPS Pointer ve formě URI [4]. Pokud certifikát neobsahuje další označení, že je vydán jako kvalifikovaný (viz bod 2), tato položka by měla být kritická a to v závislosti na uživatelské aplikaci (aplikace, které zachází s certifikáty podle RFC 3280 musí umět rozpoznat tuto položku, a tedy neodmítnout certifikát, pokud je *certificatePolicies* kritická).

```
certificatePolicies EXTENSION ::= {
        SYNTAX  CertificatePoliciesSyntax
        IDENTIFIED BY id-ce-certificatePolicies }

id-ce-certificatePolicies OBJECT IDENTIFIER ::=  { id-ce 32 }
--odpovídá hodnotě OID „2.5.29.32“

        critical ::= BOOLEAN TRUE

CertificatePoliciesSyntax ::= SEQUENCE OF
                PolicyInformation

 PolicyInformation-1 ::= SEQUENCE {
            policyIdentifier   CertPolicyId,
            policyQualifiers   SEQUENCE SIZE OF
       PolicyQualifierInfo OPTIONAL }
```

```
CertPolicyId ::= OBJECT IDENTIFIER
        --OID certifikační politiky

PolicyQualifierInfo ::= SEQUENCE {
            policyQualifierId   PolicyQualifierId,
                                qualifier                   CPSuri  OPTIONAL }

              PolicyQualifierId ::= OBJECT IDENTIFIER
--odpovídá hodnotě OID „1.3.6.1.5.5.7.2.1“

              CPSuri ::= IA5String
```

2. Qualified Certificate Statements extension:

Položka QCStatements je Private Internet Extension zavedená RFC 3039. Obsahuje jedno nebo více prohlášení vystavitele certifikátu. Mezi možná prohlášení vystavitele patří i prohlášení, že daný certifikát je vydaný jako kvalifikovaný podle platných právních předpisů. Toto prohlášení obsahuje jeho identifikátor ve formě OID. QCStatements extension může být nastavena jako kritická. V takovém případě jsou jako kritická označena všechna obsažená prohlášení [6]. Pokud certifikát neobsahuje další označení, že je vydán jako kvalifikovaný (viz. bod 1), tato položka by měla být kritická.

Poskytovatelé certifikačních služeb, kteří vydávají kvalifikované certifikáty v souladu platnými právními předpisy, které jsou v souladu se Směrnicí 1999/93/ES, mohou v položce QCStatements uvádět prohlášení identifikované pomocí id-etsi-qcs-QcCompliance (viz ASN.1 struktura) [6]. Toto se netýká poskytovatelů, kteří vydávají kvalifikované certifikáty podle českého zákona č. 227/2000 Sb., o elektronickém podpisu.

Pro přiblížení české koncepce kvalifikovaných certifikačních služeb evropským standardům a s vizí na úspěšnou a kompletní implementaci požadavků Směrnice 1999/93/ES je možné vytvořit na úrovni centrálního dozorového orgánu vlastní prohlášení o vydávání kvalifikovaných certifikátů podle zákona č. 227/2000Sb., o elektronickém podpisu ve znění pozdějších předpisů a toto prohlášení (objekt) zaregistrovat u některé z registračních agentur ISO[1]. Dozorový/akreditační orgán by zveřejnil OID tohoto prohlášení a jeho znění na veřejně dostupném místě.

```
qcStatements EXTENSION ::= {
 SYNTAX                 QCStatements,
 IDENTIFIED BY          id-pe-qcStatements}

   id-pe-qcStatements OBJECT IDENTIFIER ::= { id-pe 3 }
   --odpovídá hodnotě OID „1.3.6.1.5.5.7.1.3“

   critical ::= BOOLEAN TRUE

           QCStatements ::= SEQUENCE OF QCStatement

   QCStatement-1 ::= SEQUENCE {
            IDENTIFIED BY id-etsi-qcs-QcCompliance}

                    id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= {
                    id-etsi-qcs 1}
```

--odpovídá hodnotě OID „0.4.0.1862.1.1“. Pro účely kvalifikovaných certifikátů vydávaných podle zákona o elektronickém podpisu autor navrhuje vytvořit vlastní prohlášení.

[1] Příslušné OID by mělo být odvozené od OID akreditačního či dozorového orgánu. V případě ČR tyto dvě úlohy plní stále jeden subjekt, kterým od roku 2003 má být Ministerstvo informatiky.

2.2 Bod b) Směrnice - označení poskytovatele certifikačních služeb a státu, ve kterém má poskytovatel sídlo

Požadavek na obsah certifikátu se v tomto bodě pro oba předpisy (příloha I Směrnice 1999/93/ES a zákon č. 227/2000 Sb., o elektronickém podpisu) částečně liší. Požadavek Směrnice je možné jednoznačně splnit informací uloženou v položce Vydavatel (Issuer) podle RFC 3036. Požadavek českého Zákona na uvedení obchodního jména a sídla poskytovatele je možné též splnit informací uloženou v položce Vydavatel (Issuer) podle RFC 3039, ovšem pomocí širší škály atributů. Vždy se bude jednat o strukturu Name podle RFC 2247.

TS 101862 vyžaduje jako povinný atribut položky Issuer countryName (viz níže). Dále doporučuje vhodnou kombinaci atributů uvedenou v RFC 3039. V praxi se mezi zahraničními poskytovateli[2], kteří prohlašují kompatibilitu se Směrnicí, ne nejvíce ujala kombinace atributů countryName, commonName a organizationName, případně organizationalUnitName. V případě požadavků českého zákona musí položka Issuer obsahovat minimálně atributy countryName, organizationName či commonName [3]. Dále je třeba zvolit atributy pro uvedení sídla. Z důvodu ověřitelnosti a spolehlivosti je pravděpodobně nejvhodnější (z pohledu spoléhajících stran) vycházet z údajů zapisovaných do obchodního rejstříku. Možným řešením by bylo zahrnutí atributů postalAddress a postalCode. Tyto atributy ovšem byly původně určeny pro účely poštovních služeb jako specifikace doručovacího místa. Jako výhodnější se jeví zahrnutí označení celého sídla do atributu localityName případně stateOrProvinceName, se kterými doporučuje pracovat i RFC 3280. Volba atributů položky Issuer je zásadní i z toho důvodu, že slouží k řetězení certifikátů v certifikační cestě (přímo nadřízený certifikát musí obsahovat v položce Subject identické údaje, jako podřízený certifikát v položce Issuer).

Výrazně komplikovanější je naplnění požadavku na uvedení údaje o tom, že certifikát byl vydán v České republice (tento požadavek obsahuje jen český zákon o elektronickém podpisu, v žádném jiném obdobném předpisu se takový požadavek nevyskytuje). Místo vydání certifikátu je pojem, který není zákonem definován. Mohou vznikat pochybnosti, zda se místem vydání certifikátu rozumí místo předání certifikátu jeho držiteli, nebo místo generování certifikátu systémem certifikační autority, nebo místo sídla poskytovatele certifikačních služeb. Problémy vznikají například v situaci, kdy místo generování a místo předání certifikátu nejsou na území stejného státu, nebo kdy poskytovatel certifikačních služeb se sídlem v ČR generuje certifikáty na serveru umístěném v zahraničí a předává je klientům například opět v České republice.

Vyjděme ze samotného ustanovení § 12 odst. 1 písm. b). Z něho vyplvá, že kvalifikované certifikáty je možné vydávat pouze na území České republiky. Proto je výklad tohoto pojmu zásadní.

Vydání kvalifikovaného certifikátu je právní úkon, který má místo v čase, místo v prostoru a musí existovat subjekt, který jej vykonává. Určení jedné z těchto náležitostí nám může pomoci určit i místo vydání certifikátu. Zákon o elektronickém podpisu v § 6 odst. 1 ukládá QPCS v písmenu f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat. V § 6 odst. 1 písm. h) ukládá zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát vydán nebo zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám. A podstatný je § 6 odst. 1 písm. d): zjistit, zda v okamžiku vydání kvalifikovaného certifikátu měla podepisující osoba

[2] Například A-Trust AG (Rakousko), Belgacom E-Trust (Belgie), Deutsche Post (Německo)

data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát [2]. Tuto povinnost může poskytovatel splnit pouze v součinnosti s žadatelem o certifikát, protože pouze on disponuje daty pro vytváření elektronických podpisů. Žadatel může součinnost poskytnout při podávání žádosti o certifikát (ten v té době však ještě neexistuje, a tedy nelze zjistit, zda soukromý klíč odpovídá veřejnému klíči v něm uloženému) a dále ji může poskytnout v době od vygenerování certifikátu do jeho předání. Okamžik generování certifikátu certifikační autoritou se dá z časového hlediska velmi dobře zaznamenat (určení datumu a času s uvedením hodiny, minuty a sekundy podle § 6 odst. 1 písm h) ovšem v tuto chvíli nedochází k součinnosti s žadatelem. Žadatel poskytuje součinnost až při předávání certifikátu. V tuto chvíli je možné i ověřit, zda sobě odpovídají soukromý a veřejný klíč (§ 6 odst. 1 písm. d) a je možné také určit čas tohoto úkonu (§ 6 odst. 1 písm. h). Zdá se tedy, že vydání certifikátu je úkon jeho předání žadateli, respektive jeho zpřístupnění žadateli. Místo vydání certifikátu je tedy místo, kde se tento úkon uskuteční. Podle zákona o elektronickém podpisu je tedy možné kvalifikované certifikáty předávat (zpřístupňovat) pouze na území ČR.

Možné způsoby řešení jsou podle autora opět dva:

1. Celý problém je možné považovat za vyřešený, pokud přistoupíme na myšlenku, že označení, že daný certifikát byl vydán jako kvalifikovaný podle českého zákona o elektronickém podpisu (podle bodu a)), zároveň splňuje i požadavek bodu b). Tedy požadavek na obsažení údaje o tom, že byl vydán v ČR. Jako odůvodnění slouží závěr minulého odstavce, ze kterého vyplývá, že kvalifikované certifikáty ve smyslu zákona č. 227/2000 Sb. lze vydávat (předávat/zpřístupňovat) jen na území ČR. Pokud tedy byl certifikáty vydán jako kvalifikovaný podle zákona o elektronickém podpisu, zároveň musel být vydán na území ČR. Pokud by poskytovatel předával kvalifikované certifikáty podle českého zákona na území cizího státu, porušoval by tím zákon o elektronickém podpisu (respektive tento výklad).

Požadavek na uvedení údaje, že kvalifikovaný certifikát byl vydán v České republice je tedy splněn, pokud je splněn požadavek bodu a), tedy že certifikát obsahuje údaj o tom, že byl vydán jako kvalifikovaný podle zákona o elektronickém podpisu.

2. Závěr první varianty může být z právního hlediska sporný. Vezmeme-li v úvahu zásadu zákazu synonyma, můžeme tvrdit, že pokud by zákonodárce zamýšlel spojit požadavky bodu a) a bodu b) v jeden, jistě by tak učinil[3]. Tímto způsobem se k variantě č. 1 může postavit soud a může vyložit požadavek bodu b) odlišně[4]. Pokud bychom i my postupovali podle právních zásad, problém údaje o vydání v ČR bychom mohli vyřešit v položce Qualified Certificate Statements extension. Autor v takovém případě navrhuje obdobný postup jako u bodu a). Tedy dozorovým orgánem definované prohlášení (například ve znění: „tento certifikát byl vydán v České republice“) a registrované OID.

Issuer Name

Name ::= CHOICE { RDNSequence }

[3] Jedná se o teoretickou zásadu, kterou soudy mohou uplatnit při výkladu zákona. Čtenáře jistě napadne praktická stránka věci, tedy že „zákonodárce“ spíše nevěděl, co činí…

[4] Nezbývá než konstatovat, že nám i pro tento účel chybí judikáty a soudní praxe, ze které bychom mohli vycházet.

```
   RDNSequence ::=SEQUENCE OF RelativeDistinguisedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

    type   AtributeType,
    value  AttributeValue }

     id-at-countryName      AttributeType ::= { id-at 6 }
--odpovídá hodnotě { 2.5.4.6 }
X520countryName ::= PrintableString 'CZ'

          RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

    type   AtributeType,
    value  AttributeValue }

id-at-commonName                AttributeType ::= { id-at 3 }
--odpovídá hodnotě { 2.5.4.3 }
X520CommonName ::= utf8String[5]

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

    type   AtributeType,
    value  AttributeValue }

id-at-organizationName    AttributeType ::= { id-at 10 }
-- odpovídá hodnotě { 2.5.4.10 }
X520OrganizationName ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

    type   AtributeType,
    value  AttributeValue }

id-at-localityName          AttributeType ::= { id-at 7 }
-- odpovídá hodnotě { 2.5.4.7 }
X520LocalityName ::= utf8String

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

  AttributeTypeAndValue ::= SEQUENCE {

    type   AtributeType,
    value  AttributeValue }

id-at-stateOrProvinceName AttributeType ::= { id-at 8 }
--odpovídá hodnotě { 2.5.4.8 }
```

[5] Aplikace, které odpovídají RFC 2459, resp. RFC 3280, musí od roku 2004 používat kódování UTF8 podle RFC 2279. Autor tedy doporučuje doporučit toto kódování.

```
X520StateOrProvinceName ::= utf8String

qcStatements EXTENSION ::= {
  SYNTAX                QCStatements,
  IDENTIFIED BY         id-pe-qcStatements}

   id-pe-qcStatements OBJECT IDENTIFIER ::= { id-pe 3 }
   QCStatements ::= SEQUENCE OF QCStatement

QCStatement-2 ::= SEQUENCE {
                  statementId OBJECT IDENTIFIER }
```

--autor navrhuje vytvořit prohlášení a registrovat OID, které by identifikovalo prohlášení o místě vydání daného kvalifikovaného certifikátu. OID by se odvozovalo od OID dozorového orgánu.

Pokračování v příštím čísle e-zinu Crypto-World 1/2003

OBSAH celého příspěvku

References

[1] Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách společenství pro elektronické podpisy

[2] Zákon č. 227/2000 Sb., o elektronickém podpisu

[3] ITU-T Recommendation X.509 (1997): ISO/IEC 9594-8: Information Technology - Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks.

[4] ETSI TS 101 862 v1.2.1 (2001): Qualified certificate profile.

[5] RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

[6] RFC 3039: Internet X.509 Public Key Infrastructure Qualified Certificate Profile.

[7] RFC 2247: Using Domains in LDAP/X.500 Distinguished Names.

[8] ISO/IEC 8824-1 (1998): ITU-T Recommendation X.680 (1997): Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[9] ISO 4217 (1995): Codes for the representation of currencies and funds.

D. Nový útok (XSL) na AES

Nicolas Courtois a Josef Pieprzyk ukázali, že algoritmus Rijndael má zcela zvláštní algebraickou strukturu a může být zapsán jako systém předdefinovaných multivarietních kvadratikých rovnic (MQ). Autoři předvedli, že např. pro 128-bit Rijndael se problém nalezení tajného klíče při znalosti jednoho otevřeného textu dá popsat jako systém 8000 kvadratických rovnic s 1600 binárními neznámými. Bezpečnost Rijndaelu tím však ohrožena nebyla. Není totiž znám dostatečně výkonný algoritmus, který by takovýto systém byl schopen řešit. Známý kryptolog Shamir ve své práci, kterou publikoval na Eurocryptu 2000, popsal algoritmus XL, který řeší takovéto systémy v subexponenciálním čase. To by však znamenalo, že bezpečnost Rijndaelu se nezvyšuje exponenciálně s počtem rund! Připomeňme, že klasické útoky na blokové šifry jako např. lineární, diferenční nebo Jakobsen-Knudsenův útok mají složitost exponenciální v závislosti na počtu rund.

Josef Pieprzyk - Pragocyrpt 1996

V praxi algoritmus XL není tak výkonný a nedokáže rozbít Rijndael. Systém kvadratických rovnic "popisující" Rijndael není ale zcela náhodný, má mnoho speciálních vlastností: získaná matice je řídká a je výrazně strukturovaná. Právě tuto strukturu Nikolas Courtois a Josef Pieprzyk studovali a navrhli zlepšení obecné XL metodu a její přizpůsobení právě této specifické struktuře. Ve svém příspěvku na Asiacryptu 2002 (prosinec 2002) navrhli novou třídu útoků, nazvanou XSL útok. Celý princip je zatím vysoce heuristický, a je velmi obtížné zhodnotit jeho složitost a obecnost. Ve svém příspěvku však předvedli, že by útok mohl být schopen rozbít i 256 bitový AES.

Nicolas Courtois and Josef Pieprzyk: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations ; to appear at Asiacrypt 2002, New Zealand, LNCS, Springer.

Dvě rozdílné verze XSL útoku můžete nalézt v archivu IACR : http://eprint.iacr.org/2002/044

A co píší o tomto ohlášeném výsledku v běžném tisku?
http://www.stuff.co.nz/inl/print/0,1478,2125066a28,00.html

Cryptologists claim weakness in new US system
FRIDAY, 29 NOVEMBER 2002

Two of the world's top code-breakers may have found a way to tap into American government computer systems and are due to unveil their findings in Queenstown next week. The pair are among more than 130 cryptologists from 20 countries due to attend the five-day Asia Crypt 2002 conference starting on Sunday.

Among papers to be presented is work by Josef Pieprzyk, of Australia's Macquarie University, and Nicolas Courtois, of Schlumberger Sema in France, who believe they may have found a way of "attacking" encryption methods recently installed by the United States government and American businesses, Prof Wolfe said.

"They have found what looks to be a way of attacking it. If the standard has been broken, it may render it useless," Prof Wolfe said.

If the cryptologists were able to find a weakness in the system, so too could America's enemies.

E. Operační systém Windows 2000 získal certifikát bezpečnosti Common Criteria

Firma Microsoft získala pro své produkty Windows 2000 Professional, Server, Advanced Server certifikát stvrzující, že bylo dosaženo míry záruky hodnocení EAL 4 (Evaluation Assurance Level) podle Common Criteria.

Hodnocení bylo provedeno proti profilu ochrany CAPP/EAL4 (Controlled Access Protection Profile, version 1d) s nainstalovaným Service Packem 3 a Hotfixem Q326886. Evaulační platforma : Compaq Proliant ML570, ML330, Compaq Professional Workstation AP550, Dell Optiplex GX400, Dell PE 2500, 6450, 2550, 1550. Hodnocení proběhlo podle metodologie IT Security Evaluation (Version 1) podle Common Criteria v. 2.1 (totožné s ISO 15408, resp. ČSN ISO 15408). Validační zpráva má číslo : CCEVS-VR-02-0025. Datum vydání : 25.října 2002.

Připomeňme si zde stručnou charakteristiku EAL 4 , tak je uvedena ve 3 části ISO 15408 (Evaluation criteria for IT security - Part 3: Security assurance requirements) :

Míra záruky hodnocení EAL4 – metodicky navrženo, testováno a revidováno

EAL4 je použitelná v takových situacích, kdy vývojáři nebo uživatelé vyžadují střední až vysokou nezávislou záruku bezpečnosti z oblasti obvyklých výrobků a jsou připraveni na dodatečné technické náklady, týkající se především bezpečnosti.

Na úplný závěr uvedeme řadu odkazů, které se k dělení tohoto certifikátu vztahují :

Windows 2000 Security Configuration Guide
http://www.microsoft.com/technet/security/issues/W2kCCSCG/default.asp

Windows 2000 Evaluated Configuration User's Guide
http://www.microsoft.com/technet/security/issues/W2kCCUG/default.asp

Windows 2000 Evaluated Configuration Administrator's Guide
http://www.microsoft.com/technet/security/issues/W2kCCAdm/default.asp

Windows 2000 CC evaluation information
Windows 2000 CC News Bulletins –
http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/cccert.asp

Windows 2000 CC Overview White Paper –
http://www.microsoft.com/technet/security/issues/W2KCCWP.asp.

The above guides and security configuration templates (in inf format) would be available for download as pdf and inf files after NIAP posts the validated Windows 2000 security target.
Windows 2000 CC Security Target –
http://download.microsoft.com/download/win2000srv/CCSecTar/2.0/NT5/EN-US/W2KCCST.pdf

Článek v odlišném duchu než předchozí oficiální sdělení Microsoftu:
Understanding the Windows EAL4 Evaluation, Jonathan S. Shapiro, Ph.D.
http://eros.cs.jhu.edu/~shap/NT-EAL4.html

F. O čem jsme psali v prosinci 1999 - 2001

Crypto-World 12/1999

Crypto-World 12/2000

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

Crypto-World 12/2001

Příloha: uloha7.wav

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprochází jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :
http://www.mujweb.cz/veda/gcucmp

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@ct.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@ct.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@ct.cz
vondruska.p@seznam.cz
pavel.vondruska@post.cz