УДК 681.3.06:519.248.681

Р.В. Олейников, В.И. Руженцев

НОВЫЙ ПОДХОД К ПОСТРОЕНИЮ СХЕМ РАЗВОРАЧИВАНИЯ КЛЮЧЕЙ ДЛЯ СИММЕТРИЧНЫХ БЛОЧНЫХ ШИФРОВ

Предлагается новый подход построения небиективных схем разворачивания ключей для симметричных блочных алгоритмов шифрования, позволяющий обеспечить стойкость к известным атакам на схемы разворачивания и дополнительную защиту от атак на реализацию. Несмотря на то, что применение небиективных конструкций приводит к возможности существования эквивалентных ключей шифрования, обосновывается низкая вероятность появления такого события.

Симметричный блочный шифр; схема разворачивания ключей; атака на связанных ключах; слайд-атака.

R.V. Oliynykov, V.I. Ruzhentsev

A NEW APPROACH OF KEY SCHEDULE CONSTRUCTION FOR SYMMETRIC BLOCK CIPHERS

A new method of non-bijective key schedule construction for symmetric block ciphers which protects cipher from known key attacks and gives additional strength to implementation attacks is proposed. Although non-bijective key schedule potentially allows existence of equivalent encryption keys, it is proved that probability of such event is negligible small. An example of new type of key schedule for Rijndael-like cipher and its analysis are given.

Key schedule; symmetric block cipher; related key attack; slide attack.

Introduction. Symmetric block ciphers are the most widely used cryptographic transformation in modern commercial information security systems. Besides of encryption, they are used for construction of hashing functions, pseudo random number generators, etc. Iterated symmetric block ciphers exploit Shannon's idea [1]: product of cryptographically weak transformations can give a strong one. Modern block ciphers usually use several types of basic transformation: non-linear layer (*S*-boxes) for diffusion and linear layer for confusion. First generation of block ciphers has very simple key schedule, which usually includes just combination of bits or bytes of encryption key, like in DES [2]. This method of deriving round keys has advantages in implementation in hardware or software, but allows application of some types of cryptanalytical techniques, like slide-attack [3], related keys attack [4], etc., or lead to existence of weak keys. Next generation of symmetric block ciphers, proposed to AES [5] and NESSIE [6] competitions, uses more complex key schedule. But all of them use bijective mapping from the set of encryption keys to the set of sequences of derived round keys and vice versa. In most cases modern ciphers are protected from related keys and slide attacks. But if an attacker already has a value of the round key (via differential fault analysis, side-channel attacks, etc.), it's rather easy to get original encryption key.

For protection from this method of obtaining of master key, we can use non-bijective generation of round keys. This type of key schedule has rather simple construction, but it is almost impossible to compute the encryption key from one or several round keys. Having good key agility and simple implementation and giving protection to symmetric block cipher from additional attacks, this key schedule allows potential collisions in round keys (different encryption keys might generate the same sequence of round keys). This fact usually prevents developers of symmetric block ciphers of using non-bijective constructions in key schedule.

1**. Requirements to round keys of modern symmetric block ciphers.** Cryptographic properties of round keys do not have serious impact to differential or linear properties of block cipher [8], but key schedule determines strength to various types of key attacks and partially, strength to algebraic analysis [8] during defining intermediate variables for values of round keys.

We propose following requirements to key schedule of modern block cipher.

1. Good statistical properties and non-linear dependence of every bit of every round key from any bit of encryption key (protection from related keys and slide attacks).
2. Impossibility (high computational complexity) of encryption key retrieving from one or several round keys (additional protection from differential fault analysis, side-channel attacks, etc.)
3. Simple implementation both in software and hardware, usage of cipher's round function transformations (implementation effectiveness).
4. Good key agility (generation of all round keys takes less time than one encryption).
5. Possibility of round key generation in direct and reverse order (for simplicity and efficiency of smart card implementation).
6. Absence of weak keys which could worsen cryptographic properties of the cipher (implementation of this requirement is dependent on the whole block cipher construction).

As for our opinion, key schedule which satisfy all of these requirements, provides high level of cryptographic security and could be implemented in new effective symmetric block ciphers.

2. Proposed construction of key schedule. Let K_M be the encryption key for symmetric block cipher, and ($(K_1, K_2, ...K_m)$ – round keys generated for K_M by key schedule function. Let number of round keys be some non-prime number $m = l \cdot t$.

Let iterated SPN block cipher has the following construction:

$$Cipher[K_M] = \prod_{i=1}^{N_R} \theta \circ \gamma \circ \sigma_{K_i},$$

where σ_{K_i} – round key addition (usually, XOR with the round key);

γ – non-linear layer (S-boxes);

θ – linear transformation layer (byte permutation and MDS matrix multiplication).

Though we use here typical construction for Rijndael-like SPN block cipher, the same principles are also applicable to Feistel and Lai-Massey scheme.

Let also full diffusion (dependence of all output bytes from all input bytes) be achievable after application of 2 rounds of encryption (this is also property of AES/Rijndael [8]).

Now we can generate an intermediate value, which we call *Key State* or *KS* using the following algorithm:

$$KS[K_M] = \sigma_{K_M} \circ \theta \circ \gamma \circ \sigma_{K_M} \circ \theta \circ \gamma \circ \sigma_{K_M}.$$

As input to this transformation we use some constant C^t. It can be assigned an arbitrary value with the following limitations: for different $KS^t \neq KS^v$ there must be used different $C^t \neq C^v$, and if there are some symmetry inside round function, there

should not be such a symmetry inside constant C^t (like *111…1*). Number of constants depends on number of round keys m and size of the round key. Let the number of round keys generated from one key state denote as $l > 2$ (we generate m round keys from t key states, and each of it forms l round keys).

Round keys $(K_0, K_1, ...K_m)$ can be generated from key states by simple byte permutation (or shifting). Requirement to this function is the following: every round key generated from the same key state should be generated by unique permutation (but permutation can be the same for different key states.

Having such sequence of round keys, we can satisfy requirement 1-5 from the part 2 of present paper. Really, each bit of round key K_i non-linearly depends of each bit of the encryption key K_M with good statistical properties (2 rounds of encryption with full diffusion), there is no reverse function from $\{K_i\}$ to K_M (forward transformation is non-bijective), round keys can be generated both in direct and reverse order, implementation is rather easy and uses functions from round transformations, and key schedule time less than one encryption time (there are more than two round keys from one key state).

3. Analysis of proposed construction. As was mentioned before, proposed construction satisfies the requirement 1-5 from the second part of this paper. Requirement 6 depends on the construction of round function, but for many types of modern ciphers it is enough to use constants without internal symmetry.

Main potential problem of proposed construction is the following: for non-bijective mapping from K_M to $\{K_i\}$, there is non-zero probability of event that for different encryption keys $K_M^{(1)} \neq K_M^{(2)}$ there will be equal round keys: $K_1^{(1)} = K_1^{(2)}, K_2^{(1)} = K_2^{(2)}, ..., K_m^{(1)} = K_m^{(2)}$, or

$$P_{coll}\left(K_1^{(1)} = K_1^{(2)}, K_2^{(1)} = K_2^{(2)}, ..., K_m^{(1)} = K_m^{(2)} \Big/ K_M^{(1)} \neq K_M^{(2)} \right) > 0. \qquad (1)$$

It means that there potentially can be equivalent encryption keys and the cardinal number of the encryption key set can be decreased. Let find the upper bound of probability (1) for proposed construction.

This probability depends on the probability of collision in one key state (which forms l round keys):

$$P_{coll}^{KS}\left(K_{sl+1}^{(1)} = K_{sl+1}^{(2)}, K_{sl+2}^{(1)} = K_{sl+2}^{(2)}, ..., K_{(s+1)l-1}^{(1)} = K_{(s+1)l-1}^{(2)} \Big/ K_M^{(1)} \neq K_M^{(2)} \right) > 0, \qquad (2)$$

$$s \in \{0,1,...t-1\}$$

Let ΔK_M be a difference between encryption keys (for example, $\Delta K_M = K_M^{(1)} \oplus K_M^{(2)}$).

Let $\Delta S_1 = \gamma(\Delta K_M)$ – difference after the first non-linear transformation on S-boxes, $\Delta\theta_1 = \theta(\Delta S_1)$ – difference after the first linear transformation (MDS matrix multiplication), $\Delta_+ = \Delta\theta_1$ – difference after the second key addition, $\Delta S_2 = \gamma(\Delta_+)$ –

difference after the second non-linear transformation on S-boxes, and $\Delta\theta_2 = \theta(\Delta S_2)$ – difference after the second linear transformation.

It is obvious, that for equivalent key states $KS_M^{(1)} = KS_M^{(2)}$ for different encryption keys $K_M^{(1)} \neq K_M^{(2)}$ we need to have $\Delta\theta_2 = \Delta K_M$. Accordingly, we need $\Delta_+ = \gamma^{-1}\left(\theta^{-1}(\Delta K_M)\right)$ and $\Delta\theta_1 = \theta(\gamma(\Delta K_M))$ with $\Delta_+ = \Delta\theta_1$.

So long as θ and θ^{-1} are the linear transformations, correspondence between input and output difference will hold for them with probability 1. But for non-linear (S-boxes) transformations γ and γ^{-1} there will be probabilistic correspondence between input and output difference, or

$$p\left(\Delta\theta_1 \middle/ \Delta S_1\right) = 1,\ p\left(\Delta S_2 \middle/ \Delta\theta_2\right) = 1,\ p\left(\Delta S_1 \middle/ \Delta K_M\right) < 1,\ \ p\left(\Delta_+ \middle/ \Delta S_2\right) < 1. \quad (3)$$

Transformations describable by (3) are independent, so probability of collision (2) can be estimated as

$$\begin{aligned} &P_{coll}^{KS}\left(K_{sl+1}^{(1)} = K_{sl+1}^{(2)}, \ldots, K_{(s+1)l-1}^{(1)} = K_{(s+1)l-1}^{(2)} \middle/ K_M^{(1)} \neq K_M^{(2)}\right) = \\ &= p\left(\Delta\theta_1 \middle/ \Delta S_1\right) \cdot p\left(\Delta S_2 \middle/ \Delta\theta_2\right) \cdot p\left(\Delta S_1 \middle/ \Delta K_M\right) \cdot p\left(\Delta_+ \middle/ \Delta S_2\right). \end{aligned} \quad (4)$$

So, for effective search of equivalent keys we need to maximize the probability (2) taking into account the following limitations:

$$\begin{cases} K_M^{(1)} \neq K_M^{(2)},\ \Delta K_M \neq 0, \\ \Delta\theta_2 = \Delta K_M, \\ p_{coll}^{KS} = p\left(\Delta\theta_1 \middle/ \Delta S_1\right) \cdot p\left(\Delta S_2 \middle/ \Delta\theta_2\right) \cdot p\left(\Delta S_1 \middle/ \Delta K_M\right) \cdot p\left(\Delta_+ \middle/ \Delta S_2\right), \\ p_{coll}^{KS} \to \max. \end{cases} \quad (5)$$

Let $\Delta_{\max}^S$ be a maximal probability of non-zero input difference transformation via single S-box (in the non-linear layer γ), B_M – branch number of θ transformation, $wt(\Delta)$ – number of active (non-zero) bytes in the difference Δ.

Then probabilities (3) can be estimated as follows:

$$\begin{aligned} p\left(\Delta S_1 \middle/ \Delta K_M\right) = \left(\Delta_{\max}^S\right)^{wt(\Delta K_M)} < 1 \; on \; \Delta K_M \neq 0, \\ p\left(\Delta S_2 \middle/ \Delta\theta_2\right) = \left(\Delta_{\max}^S\right)^{wt(\Delta\theta_1)} < 1. \end{aligned} \quad (6)$$

Taking 1 active byte in ΔK_M, or $wt(\Delta K_M) = 1$ we will have $wt(\Delta\theta_1) = B_M - 1$ according to properties of MDS matrix multiplication, and

$wt(\Delta\theta_2)=1$ with respect to the second condition of (4). On $wt(\Delta K_M)=2$ we'll have $wt(\Delta\theta_1)=B_M-2$ and $wt(\Delta\theta_2)=2$ and so on, till $wt(\Delta K_M)=B_M-1$, $wt(\Delta\theta_1)=1$ and $wt(\Delta\theta_2)=B_M-1$. From this follows

$$wt(\Delta K_M)+wt(\Delta\theta_1)=B_M \text{ for any } wt(\Delta K_M)\in\{1,2,...,B_M-1\}. \quad (7)$$

From (4), (6) and (7) it follows that

$$P_{coll}^{KS}\left(K_{sl+1}^{(1)}=K_{sl+1}^{(2)},...,K_{(s+1)l-1}^{(1)}=K_{(s+1)l-1}^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)=$$

$$=p\left(\Delta\theta_1\Big/\Delta S_1\right)\cdot p\left(\Delta S_2\Big/\Delta\theta_2\right)\cdot p\left(\Delta S_1\Big/\Delta K_M\right)\cdot p\left(\Delta_+\Big/\Delta S_2\right)=$$

$$=1\cdot 1\cdot p\left(\Delta S_1\Big/\Delta K_M\right)\cdot p\left(\Delta S_2\Big/\Delta\theta_2\right)=\left(\Delta_{\max}^S\right)^{wt(\Delta K_M)}\cdot\left(\Delta_{\max}^S\right)^{wt(\Delta\theta_1)}=$$

$$=\left(\Delta_{\max}^S\right)^{wt(\Delta K_M)+wt(\Delta\theta_1)},$$

or

$$P_{coll}^{KS}\left(K_1^{(1)}=K_1^{(2)},...,K_m^{(1)}=K_m^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)=\left(\Delta_{\max}^S\right)^{B_M}. \quad (8)$$

As long as for different key states we use different constants $C^i\neq C^j$ for $i\neq j$, non-linear transformations on S-boxes (γ layers) are performed independently. So, for t independent key states probability of finding an equivalent key (1) can be estimated as

$$P_{coll}\left(K_1^{(1)}=K_1^{(2)},K_2^{(1)}=K_2^{(2)},...,K_m^{(1)}=K_m^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)=$$

$$=\left(P_{coll}^{KS}\left(K_{sl+1}^{(1)}=K_{sl+1}^{(2)},K_{sl+2}^{(1)}=K_{sl+2}^{(2)},...,K_{(s+1)l-1}^{(1)}=K_{(s+1)l-1}^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)\right)^t=$$

$$=\left(\Delta_{\max}^S\right)^{B_M\cdot t} \quad (9)$$

Having appropriate small probability of difference transformation on a single S-box, enough big MDS matrix (for big branch number) and several key states, we can get negligible small probability of having equivalent keys for symmetric block cipher.

4. Example of proposed key schedule. Let we have perspective Rijndael-like symmetric block cipher with 128 bits block size and 128 bit key length. It has 12 rounds and uses 128-bits round keys $K_1,K_2,...,K_{12}$ ($m=12$), S-box non-linear layer, ShiftRows (swapping 64-bits halves of State) and MixColums as two 8x8 MDS matrices instead of for 4x4 MDS in AES/Rijndael. For protection of algebraic analysis, it uses random S-boxes with $\Delta_{\max}^S=2^{-5}$ instead of AES/Rijndael S-boxes with $\Delta_{\max}^S=2^{-6}$. Branch number of 8x8 MDS matrix is $B_M=9$.

For key length of 128 bits we have the cardinal number of the encryption keys set is equal to 2^{128}, so the threshold probability (upper bound) is

$$P_{coll}\left(K_1^{(1)}=K_1^{(2)},K_2^{(1)}=K_2^{(2)},...,K_{12}^{(1)}=K_{12}^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)\leq 2^{-128}. \qquad (10)$$

According to proposed construction, pseudo-code of key schedule for generating key states will have the following form:

```
void Cipher_KeyExpansionKS( byte key[ 16  ], const Ci, byte KS[ 16  ])
{
   byte state[ 16  ] = Ci

   XORRoundKey(state, key )

   S_boxes( state )
   ShiftRows( state )
   MixColumns( state )
   XORRoundKey(state,  key )

   S_boxes( state )
   ShiftRows( state )
   MixColumns( state )
   XORRoundKey(state, key)

   KS = state
}
```

Number of required key states t for negligible small probability of having equivalent keys we can be found from the equations (9) and (10):

$$P_{coll}\left(K_1^{(1)}=K_1^{(2)},K_2^{(1)}=K_2^{(2)},...,K_{12}^{(1)}=K_{12}^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)=\left(\Delta_{\max}^{S}\right)^{B_M\cdot t}\leq 2^{-128}$$

or

$$P_{coll}\left(K_1^{(1)}=K_1^{(2)},K_2^{(1)}=K_2^{(2)},...,K_{12}^{(1)}=K_{12}^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)=\left(2^{-5}\right)^{9\cdot t}\leq 2^{-128},$$

and for $t=3$ we get

$$P_{coll}\left(K_1^{(1)}=K_1^{(2)},K_2^{(1)}=K_2^{(2)},...,K_{12}^{(1)}=K_{12}^{(2)}\Big/K_M^{(1)}\neq K_M^{(2)}\right)=2^{-135}.$$

So, having 3 key states (each forms $l=\frac{m}{t}=\frac{12}{3}=4$ round keys), we have negligible small probability equivalent keys in the new cipher with highest strength to all key schedule attacks and all advantages for fast and compact implementation.

Conclusions. Proposed approach allows constructing of block ciphers key schedules of new type, which have very good cryptographic and statistical properties, protect algorithm from all known key attacks and gives additional protection from attacks to implementation of the cipher (like differential fault analysis and side-channel attacks). Implementation of such type of key schedule is fast and compact. Although proposed approach forms non-bijective key schedules which potentially can have equivalent keys, it is shown that the probability of having such keys is negligible small.

BIBLIOGRAPHIC LIST

1. *Shannon C.E.* Communication Theory of Secrecy Systems // Bell Syst. Tech. Journal. – 1949. – Vol. 28.
2. FIPS 46-3. Data Encryption Standard (DES).
3. *Biryukov D.*Wagner. Slide Attacks. Proceedings of FSE'99, LNCS 1636. Springer Verlag. 1999. – P. 245-259.
4. *Biham E.* New Types of Cryptanalytic Attacks Using Related Keys // Journal of Cryptology. – 1994. – Vol. 7. – P. 229-246.
5. Announcing development of a federal information processing standard for Advanced Encryption Standard. Department of Commerce. National Institute of Standards and Technology, USA. 1997. Available at http://csrc.nist.gov/archive/aes/pre-round1/aes_9701.txt.
6. New European Schemes for Signature, Integrity, and Encryption. Call for Cryptographic Primitives. Information Societies Technology (IST) Program of the European Commission, 2000. Available at https://www.cosic.esat.kuleuven.be/nessie/call.
7. *Daemen J., Rijmen V.* The design of Rijndael. AES –The Advanced Encryption Standard. Springer-Verlag, Berlin. 2002.
8. *Courtois N.T., Pieprzyk J.* Cryptanalysis of block ciphers with overdefined systems of equations. Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, 2002.

Олейников Роман Васильевич
ЗАО «Институт информационных технологий».
E-mail: ROliynykov@gmail.com.
Украина, 61166, г. Харьков, ул. Бакулина, 12.
Тел.: +380577142205; +380675733343.

Руженцев Виктор Игоревич
E-mail: vityazik@rambler.ru.

Oliynykov Roman Vasil'evich
JSC "Institute of Information Technologies".
E-mail: ROliynykov@gmail.com.
12, Bakulina street, Kharkov, 61166, Ukraine.
Phone: +380577142205; +380675733343.

Ruzhentsev Viktor Igorevich
E-mail: vityazik@rambler.ru.

УДК 003.26

А.Т. Алиев

ЛИНГВИСТИЧЕСКАЯ СТЕГАНОГРАФИЯ НА ОСНОВЕ ЗАМЕНЫ СИНОНИМОВ ДЛЯ ТЕКСТОВ НА РУССКОМ ЯЗЫКЕ

Рассматриваются методы скрытой передачи информации, основанные на использовании синонимов. Основной задачей является исследование возможности реализации данных методов для текстов на русском языке. Для этого в работе был проведен анализ особенностей русского языка и его частотных свойств, построены специальные словари синонимов для разных частей речи и предложены новые алгоритмы сокрытия и извлечения информации.

Сокрытие информации; скрытая передача информации; стеганография; лингвистическая стеганография; текст; метод синонимичных преобразований; синонимичная замена.