From: oleg.oleshko@excite.com
Date: Sun, 14 May 2000 01:50:34 -0700 (PDT)
To: AESround2@nist.gov
Subject: Comments to AES Conf
X-Mailer: Excite Inbox
X-Sender-Ip: 62.244.22.30

Title: PROPERTIES OF EXPANDED KEYS OF THE AES CANDIDATES
Organiztaion: Kharkov State Technical University of Radioelectronics, Ukraine

Dr. M. Bondarenko, Dr. I. Gorbenko, T. Grinenko,
S. Golovashich, O. Oleshko, A. Bondarenko

Kharkov State Technical University of Radioelectronics

PROPERTIES OF EXPANDED KEYS OF THE AES CANDIDATES

The results of an estimation of the key expansion schemes on the criterion of «error» propagation are presented. We came to a conclusion, that best on this criterion are AES algorithms RC6 and TWOF. AES algorithms RIJN and SERP are considered as an unsatisfactory algorithms on this criterion. It is proposed in the choice of the standard to take into account properties and performances of the key expansion schemes.

Introduction

Today in the field of information safety the important problem of making of cryptography standards of 21 century is solved. Its solution was initiated by USA NIST. The development began in 1997 with project of making comprehensive analysis of a candidate ciphers for standard of the block symmetric cryptoalgorithm (AES) of 21 century [1]. For this purpose NIST has declared competition of cryptoalgorithms, claiming to be standards of the block cryptoalgorithm of 21 century. Three stages of submitting of the candidates were planned. In April, 2000 the third round was held.

The purpose of the present message is to set forth opinion and to represent the results obtained by authors, first of all in a part of a research of properties of the expanded keys, which in our mind should be considered in choice of one or several cryptoalgorithms as standards of XXI century.

As a result of numerous investigations we came to opinion, that the candidates can be ranked according to priority (efficiency) in the following order: RC6, MARS, TWOF (USA), RIJN (Belgium), CRYPTON (Korea), CAST-256 (Canada), E2 (Japan), SERP (Great Britain, Israel etc.), HPC (USA), DFC (Francium), SAFER (USA), LOKI197 (Australia), DEAL (USA), FROG (Costa Rica) and Magenta (Germany). On the 3 Conference holding in April as a result of ratings of voting most high priority was received by algorithms RIJN (Belgium) and SERP (Great Britain, Israel etc.).

In our investigations we have given the special attention to properties of the expanded keys. In our mind the fact is that (and this requires the special considerations) expanded keys should possessed a number of properties - to be generated randomly, equiprobably, and independently, i.e. to have the same properties, as initial keys.

1. Analysis of algorithms and properties of the expanded keys

In our mind, all five candidate ciphers falling into the second round, are possessed the actual security (safety), i.e. for them there are not exist or unknown cryptoanalitic attack, which on computational complexity would be better than attack such as «rough force» - exhaustive search on space of all possible keys. As seen from investigations, all of them have a good statistical safety (but only under condition that $n_{\ddot{o}} \geq n_g$, where n_g is permissible number of cycles of transformation).

Therefore crucial in ranking of algorithms is the computational complexity of the forward and reverse transformations, reliability of mathematical basis, and also complexity of the key expansion for processors with different digit capacity. On our estimates and results of experimental investigations, from a point of view of computational complexity, cryptoalgorithms can be placed in

above order - RC6, MARS, TWOF, RIJN, SERP. Though, for different platforms of the software implementation in Assembly language there is possibility for the reduction of computational complexity by tens clocks.

To AES claimed the requirements on complexity of key expansion and equiprobability of occurrence of initial keys with length of 128, 192 and 256 bits. Equiprobability of occurrence of keys allows to reach maximum strength, since in attack "rough force" all keys are equiprobable and any reduced exhaustive search is impossible. That is equiprobability of occurrence of the keys is a necessary condition of actual safety. The sufficient conditions are provided by appropriately designed algorithm.

The analysis has conducted shows that in the candidate ciphers for AES - RÑ6, MARS, TWOF, RIJN and SEPR satisfied (practically) the necessary conditions for providing computational strength.

In the AES analysis we came to conclusion, that the particular requirements should be claimed to the expanded keys also. In particular in our mind it is necessary, that the change on each of a bit position of an initial key results in uniform varying of bits (error propagation) in the expanded key. The experimental investigations an effect of error propagation for the finalists of the second round RC6, MARS, TWOF, RIJN and SERP were performed. In essence was studied effect of error propagation in the expanded K^p key in change of each bit of initial key Kj. For all algorithms the procedure of key expansion is possible to present as

$$K_j^p = X\left(K_j, C_V\right), \tag{1}$$

where $\tilde{N}_V$ means the V-th constant of algorithm of key expansion. Next, the number of modified n_i bits in the expanded key is possible to present as function φ of the number of modified bit of an initial key and constants, i.e.

$$n_i = \varphi_r\left(i, C_V\right), \tag{2}$$

Where r is a type of AES algorithm.

Thus, in experiment was varied the i-th bit of an initial key, and for each r (RC6, MARS, TWOF, RIJN, SERP) the amount of modified bits was determined by following technique:

1. Was built an initial key K_j, and then the respective expanded key K_j^p.

2. In each initial key K_j was varied the i bit, $i = \overline{1, l_p}$, and then according to (1) was built the respective expanded key K_{j1}^p, where l_p is length of the expanded key.

3. Hamming distance n_i between the expanded keys K_j^p for each i-th position and different keys was computed.

In our opinion as the best key expansion algorithm it is possible to consider algorithm, for which, at first, distribution $\overline{n_i}$, $i = \overline{1, l_p}$ submits to the uniform law, and secondly, the expectation of distribution $\bar{n}$ is closer to $l_p/2$. Physically in the first case it means, that the change of each bit results in avalanche effect with uniform error propagation, and in second, that the change of one bit results on the average in change of half of bits of the expanded key. As a whole at satisfy of both conditions the expanded keys differ in half of bits, therefore it is possible to consider them as independent.

Fig. 1-5 present the histograms of error propagation factors in the expanded key depending on a position of modified bit in an initial key for all of five algorithms.

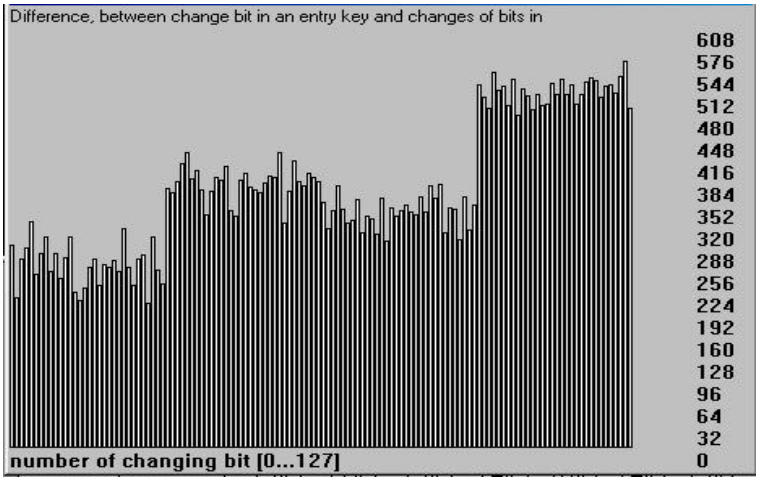

Fig.1. Dependence of "error" propagation factor in the expanded key on a position number of modified bit for RIJN, key length of 128 bits

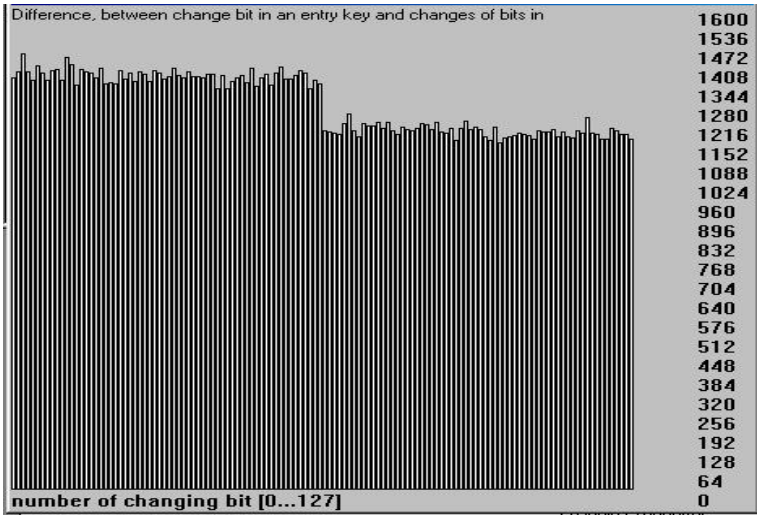

Fig.2. Dependence of "error" propagation factor of the expanded key of the expanded key on the first 128 positions of an initial key for SERP, key length of 192 bits

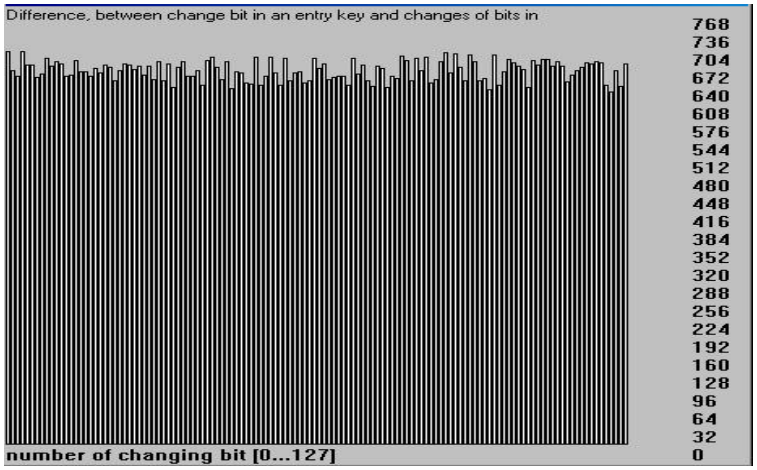

Fig.3. Dependence of "error" propagation factor in the expanded key on a position number of modified bit for RC6, length of an initial key of 128 bits

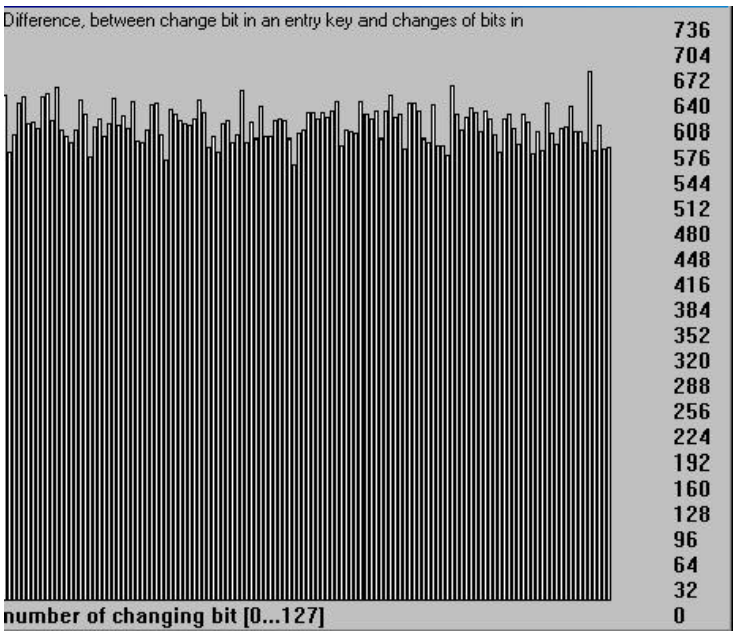

Fig.4. Dependence of "error" propagation factor in the expanded key on a position number of modified bit for TWOFISH, length of an initial key of 128 bits

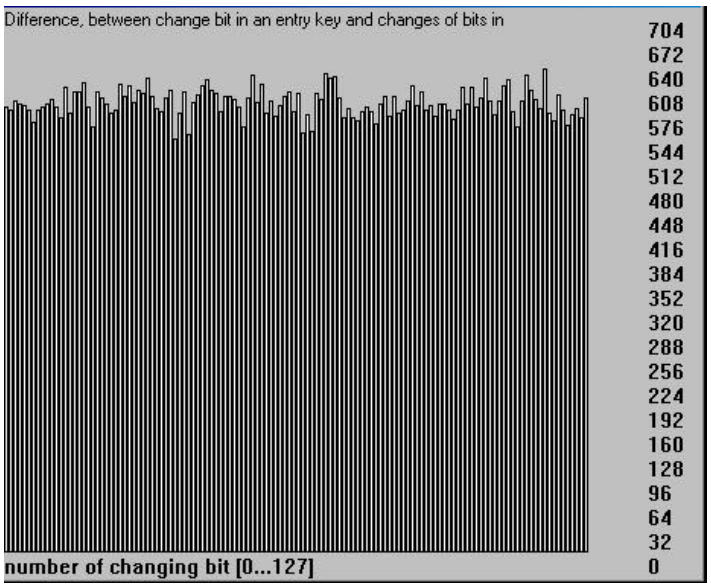

Fig.5. Dependence of "error" propagation factor in the expanded key on a position number of modified bit for MARS, length of an initial key of 128 bits

The data analysis of a fig. 1-5 shows, that for algorithms RIJN and SERP the "error" propagation factor depending on a position number of modified bit is essentially nonuniform. The nature of nonuniformity is explained by feature of algorithm of key expansion.

As followed from Fig. 3 - 5 error propagation factors for algorithms RC6, TWOFISH and MARS are close to uniform and have the same character for different initial keys and different lengths of initial keys.

In Table 2 shown the values of expectation of a correlation function of errors propagation factor of the expanded keys, initial keys, which differ on one bit, for five candidates in AES.

Table 2

Error propagation factor for AES.

AES type	length of an initial key	length of the expanded key	Errors propagation factor (depending on a bit position), intervals
RIJN	128	1408	216/580
SERP	192	4224	1200/1490
RC6	128	1408	640/720
MARS	128	3072	560/640
TWOF	128	1280	616/674

The data analysis of the Table 2 allows to make a conclusion, that the algorithms RC6 and TWOF permit to build the expanded keys with best decorrelation of two expanded keys, for which the initial keys differ on one bit.

Above pointed out allows to make the conjecture that the best key expansion schemes are the schemes of algorithms RC6 and TWOF

Conclusion

The analysis of the concepts of making of standards of a cryptography security of the information shows, that the implementation of AES project will allow to create effective algorithms, available at a world level. The holding of competitions and opened takeoff of the candidates practically will allow to eliminate an opportunity of embedding "trapdoors" in algorithms.

In the choice one or several block symmetric cryptoalgorithms as standards of XXI century in our mind is necessary for taking into account performances of the key expansion schemes. More preferable are the schemes of algorithms RC6 and TWOF, since the expanded keys in them are good decorrelated even in case if the initial keys differ in one bit. Also the mean of a error propagation factor in these algorithms is close to half of length of the expanded keys.

References

[1]. AES discussion forum: http://aes.nist.gov