On Noekeon*
NES/DOC/UIB/WP3/009/1

Lars R. Knudsen and Håvard Raddum
Dept. of Informatics, University of Bergen, Norway

April 24, 2001

Abstract

In this note we analyse Noekeon, a 128-bit block cipher submitted to the NESSIE project. It is shown that for six of seven S-boxes which satisfy the design criteria of the Noekeon designers the resulting block ciphers are vulnerable to either a differential attack, a linear attack or both. One conclusion is that Noekeon is not designed according to the wide trail strategy.

Also, it is shown that there exist many related keys for which plaintexts of certain differences result in ciphertexts of certain differences with high probabilities. Noekeon has two key-schedules, one for applications where related-key attacks are not considered dangerous and one for applications where related-key attacks can be mounted. In this paper it is shown that for any given user-selected keys there are many related keys independently of which key-schedule is used.

1 Introduction

Noekeon is an iterated 128-bit block cipher with 128-bit keys, which runs in 16 rounds. Each round consists of some subfunctions, a linear function called Theta, three rotations called Pi1, 32 parallel 4-bit S-box lookups called Gamma and three rotations called Pi2. All functions take a 128-bit text input. The function Theta takes as input also the 128-bit round key. To avoid round symmetries a round constant is added to 32 bits of the ciphertexts in each round. After the 16 rounds, an output transformation is applied. This consists of the addition of a round constant and a final application of Theta. The output transformation and the nature of the individual round function components allow for very similar encryption and decryption routines. Figure 1 illustrates the round function in Noekeon, where C_i is a round dependent constant and $K_0, \ldots, K_3$ are the 32-bit subkeys. The reader is referred to [3] for more details.

*This work was supported by the European Union fund IST-1999-12324 - Nessie.

2 Differential and Linear Attacks

Let e_i denote a 32-bit string with a one-bit in the ith position and zeros elsewhere. Consider first differential attacks [1] and the following one-round differentials, where the differences are split into four 32-bit differences.

$$\begin{array}{cccc} (e_i & 0 & e_i & 0) \\ (e_i & 0 & e_i & 0) \\ (e_i & 0 & e_{i+5} & 0) \\ (e_i & 0 & e_{i+5} & 0) \\ (e_i & 0 & e_i & 0), \end{array} \begin{array}{c} \stackrel{\text{Theta}}{\rightarrow} \\ \stackrel{\text{Pi1}}{\rightarrow} \\ \stackrel{\text{Gamma}}{\rightarrow} \\ \stackrel{\text{Pi2}}{\rightarrow} \\ \\ \end{array}$$

where indices are computed modulo 32. The differentials require that two inputs to the 4-bit S-box, S4, in Gamma with difference 8_x can lead to outputs of difference 8_x, and that two inputs with difference 2_x can lead to outputs of difference 2_x.

Consider also the following one-round differentials.

$$\begin{array}{cccc} (0 & e_i & 0 & e_i) \\ (0 & e_i & 0 & e_i) \\ (0 & e_{i+1} & 0 & e_{i+2}) \\ (0 & e_{i+1} & 0 & e_{i+2}) \\ (0 & e_i & 0 & e_i). \end{array} \begin{array}{c} \stackrel{\text{Theta}}{\rightarrow} \\ \stackrel{\text{Pi1}}{\rightarrow} \\ \stackrel{\text{Gamma}}{\rightarrow} \\ \stackrel{\text{Pi2}}{\rightarrow} \\ \\ \end{array}$$

The differentials require that two inputs to S4 with difference 4_x can lead to outputs of difference 4_x, and that two inputs with difference 1_x can lead to outputs of difference 1_x.

Consider next linear attacks [5]. If one considers the above listed differences (the e_is and 0s) as bitmasks, one gets possible one-round (iterative) linear approximations for the round function of Noekeon.

The requirements are for the first approximation, that the most significant bit of the input of S4 equals most significant bit of the output of S4 with a probability different from 1/2, and that the second least significant bit of the input of S4 equals the second least significant bit of the output of S4 with a probability different from 1/2.

The requirements for the second approximation are, that the second most significant bit of the input of S4 equals the second most significant bit of the output of S4 with a probability different from 1/2, and that the least significant bit of the input of S4 equals the least significant bit of the output of S4 with a probability different from 1/2.

Let us introduce some notation. We shall write $h_x \rightarrow j_x$ to denote that inputs of exclusive-or difference h_x to S4 lead to outputs of exclusive-or difference 4_x with probability greater than 0, and use a similar notation for linear approximations, where h_x and j_x will denote bit masks [5].

By inspection of the differential distribution tables for the S-box in Noekoen, S4, (see e.g. Table 3 in [3]) it follows that $4_x \rightarrow 4_x$ with probability 2/16, but $1_x \rightarrow 1_x$, $2_x \rightarrow 2_x$, and $8_x \rightarrow 8_x$, all have probability zero.

From the linear approximation table of S4, (see e.g. Table 4 in [3]) it follows that $1_x \rightarrow 1_x$ and $2_x \rightarrow 2_x$ have positive biases, but both $4_x \rightarrow 4_x$ and $8_x \rightarrow 8_x$ have a zero bias. Therefore none of the above differentials exists and the linear approximations all hold with probability 1/2.

In the design of Noekeon it was not explicitly required that the above differential and linear combinations should not exist in the used S-box.

We implemented a simple search for self-inverse S-boxes, where the differential probabilities through the S-box were at most 4/16 and where the maximum bias in the linear approximations were 4/16. For 8,600 of 10,000 such S-boxes at least one of the above four structures exists.

The above differentials and linear approximations repeat themselves after one round, we say they are 1-round iterative differentials and approximations. These can be iterated to any number of rounds. In each round there are two active S-boxes. Since the probability of a (non-trivial) differential through one Noekeon S-box is either 2/16 or 4/16, it holds that if the above differentials exist they have one of three possible probabilities, and similarly for the linear approximations. In the following it is assumed that the probability of an i-round differential can be approximated by the product of i one-round differentials and similarly for linear approximations.

For the differential attack, in the worst case (for the attacker) the probability of a one-round differential of the above form is 2^{-6}. Thus, when iterated to 15 rounds the probability is 2^{-90}. In the best cases, the one-round differentials have probability 2^{-4}, which iterated to 15 rounds gives a probability of 2^{-60}. In the third case, the probability for a 15-round differential is 2^{-75}. In addition, if there is one differential there is in total at least 32 differentials with similar probabilities. Such phenomenon exist only with a very small probability for a randomly chosen permutation.

For the linear attack, in the worst case (for the attacker) the bias of a one-round linear approximation of the above form is 2^{-5}. Thus, when iterated to 15 rounds the bias is 2^{-61}. In the best case, the bias of a one-round linear approximation of the above form is 2^{-3}, and when iterated to 15 rounds the bias is 2^{-31}. In the third case the bias for 15 rounds is 2^{-46}. In addition, if there is one such linear approximation there is in total at least 32 approximations with similar biases. Such phenomenon exist only with a very small probability for a randomly chosen permutation.

The wide trail strategy was introduced by Daemen [2], see also [3, 4]. Here the nonlinear components are generated independently of the linear components. One constructs a linear diffusion layer such that there are no multiple-round differentials or linear approximations involving only few S-boxes. Then one generates an S-box with only low probability differentials and low biases. The result should be a cipher which is strong against differential and linear attacks. It is clear from the above that Noekeon is not designed according to this strategy. It was shown that for about 86% of the S-boxes generated according to the constraints given, a differential attack or a linear attack is possible (at

least in theory).

3 Related Keys

The round keys in Noekeon are very easy to compute. The user-selected 128-bit key is encrypted using Noekeon with the all-zero key, and the resulting 128-bit ciphertext is used as the round key in all rounds. This key-schedule is constructed to thwart related-key attacks, where an attacker is able to get encryptions under several keys. The idea is that even though the attacker knows a relation between two (or more) user-selected keys, the fact that the keys are encrypted leaves little hope for the attacker to predict the differences in the round keys. In applications where the related-key attacks are not applicable it is recommended to use the so-called *direct-key mode* where the user-selected key is used directly as the round key in all rounds. In the following we ignore the output transformation of Noekeon, which has no effect on the findings presented here.

In the following it will be shown that for every user-selected key there are many related keys. Consider *related-key differentials.* These are pairs of plaintexts of a certain difference, where one plaintext is encrypted under one key and the second plaintext under a second, different key, and the corresponding pairs of ciphertexts. The two keys involved have a certain difference.

By a closer look at the round function one finds that there are many related keys for any given key. In fact, take any input difference ϕ_1 to the Gamma function (the S-box layer). Find a likely output difference ϕ_2 with probability p. Compute the difference Φ=Pi2(ϕ_2). Then there exists a unique difference, Ψ, between two round keys such that two inputs of difference Φ encrypt to a difference Φ after one round of encryption with probability p when encrypted with a pair of keys of difference Ψ.

It follows by inspection of the round function of Noekeon, that this phenomenon holds also for word-wise rotated values of Φ and Ψ, that is, where the same rotation amount is applied to all involved 32-bit words. Therefore, for any given user-selected key if there is one related key, then there are 31 other related keys of a similar form.

As an example, consider two texts of difference

$$\Phi = (00000020_x, 00000010_x, 00000001_x, 00000008_x).$$

Consider two keys $K = k_0, k_1, k_2, k_3$ and $K' = k'_0, k'_1, k'_2, k'_3$, such that $\Psi_1 = k_1 \oplus k'_1 = k_3 \oplus k'_3 = 0x21002121$ and $\Psi_2 = k_0 \oplus k'_0 = k_2 \oplus k'_2 = 0x18001818$. Then it holds that after i rounds of encryption, the difference in the ciphertexts is Φ with a probability of $1/4^i$, (where we tacitly assume that the probability of an i-round differential is well approximated by the product of the i involved one-round differentials). It follows by a closer look at this differential that there is only one active S-box in the S4-mapping, and that the input difference is f_x. For the differential to hold it is required that the output difference of the active S-box is again f_x. From the difference distribution table of Noekeon (see e.g. Table 3 in [3]) it follows that this combination has a probability of 1/4. This

means, that for any given key K, if a randomly chosen plaintext x encrypts to the ciphertext y, then the key $K \oplus \Psi$ will encrypt $x \oplus \Phi$ to $y \oplus \Phi$ with a probability of 2^{-32} after 16 rounds of encryption, where $\Psi = \Psi_2, \Psi_1, \Psi_2, \Psi_1$ (where '$\oplus$' is defined as a wordwise exclusive-or). Since there are 2^{128} different inputs, it can be expected that this phenomenon holds for 2^{96} texts. Or put differently, for a pair of texts of difference Φ one can expect that there are 2^{96} pairs of keys of difference Ψ which encrypt these texts to ciphertexts after 16 rounds of difference Φ.

As mentioned above, this phenomenon holds also for rotated values of Φ and Ψ, where rotation is word-wise (32-bit words). Therefore, for every user-selected key there are 32 related keys of a form similar to the above, where in each case, there is only one active S-box per round in the involved differential, every time with input and output difference f_x.

According to Table 3 of [3] there are 24 combinations of input and output differences through S4 of probability 1/4. For each of these one gets a related-key differential over i rounds of probability $1/4^i$. Because of the rotation symmetry explained above it holds that for each such differential there are 31 other differentials with the same probability. This means that for each user-selected key there are 768 other keys for which there exists a related-key differential of probability 2^{-32} over 16 rounds of Noekeon.

In the above differentials there is only one active S-box in each round. According to Table 3 of [3] there are 72 combinations of input and output differences through S4 of probability 1/8. Each of these (at their 31 rotation variants) gives rise to a related-key differential over 16 rounds of probability 2^{-48}. In total there are 2,304 such differentials.

Next we consider differentials with two active S-boxes per round. For each two of the 24 S4-differentials of probability 1/4 and their rotated variants, there is a related-key differential over 16 rounds of Noekeon of probability 2^{-64}. This means that there are about

$$\left(\begin{array}{c} 768 \\ 2 \end{array} \right) = 2^{18}$$

such differentials. One can go one step further and find differentials with two active S-boxes where for each round one combination has probability 1/4 and the other probability 1/8. There are $768 \times 2,304$ such differentials each of probability 2^{-80}. Table 1 lists the probabilities of related-key differentials with probabilities larger than 2^{-128} which we have detected.

Note that since the round key is generated from the user-selected key by a bijective mapping, the related-key differentials exist both in the direct-key mode and when the key-schedule is used. The existence of the related keys is mainly due to the fact that the round keys are all equal.

Although it is unclear how to exploit these related keys in cryptanalytic attacks on Noekeon when used for encryption, such relations could easily be avoided using a slightly more complex key-schedule. Also, it is clear that Noekeon should not be used in hashing modes or in any other modes where an attacker has influence on the choice of the key.

Probability	# related keys
2^{-32}	768
2^{-48}	2,304
2^{-64}	2^{18}
2^{-80}	2^{21}
2^{-96}	2^{26}
2^{-112}	2^{29}

Table 1: Related-key differentials for Noekeon with 16 rounds based on 1-round iterative differentials. First column gives the probabilities of the differentials, the second column states for any given key the number of related keys for which such a differential exists.

Finally we note that the above related keys are effects of the existence of 1-round iterative differentials. There might be other differentials, e.g. i-round iterative differentials for $i > 1$, which give rise to more such keys. This is a topic for further research.

4 Conclusion

In this note it has been shown that for 86% of the S-boxes generated according to the design strategy of Noekeon, efficient differential and/or linear attacks can be mounted. This means that Noekeon is not designed according to the wide trail strategy. The particular choice of the S-box in Noekeon falls outside the mentioned 86%.

In the second part of the paper large classes of related keys were reported. The existence of these classes of related keys is independent of which of the two proposed key-schedules is used.

References

[1] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer Verlag, 1993.

[2] J. Daemen. *Cipher and Hash Function Design*. PhD thesis, Katholieke Universiteit Leuven, March 1995.

[3] J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen. Nessie proposal: NOEKEON. Submitted as an NESSIE Candidate Algorithm. Available from `http://www.cryptonessie.org`.

[4] J. Daemen and V. Rijmen. AES proposal: Rijndael. Submitted as an AES Candidate Algorithm. Available from `http://www.nist.gov/aes`.

[5] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93, LNCS 765*, pages 386–397. Springer Verlag, 1993.

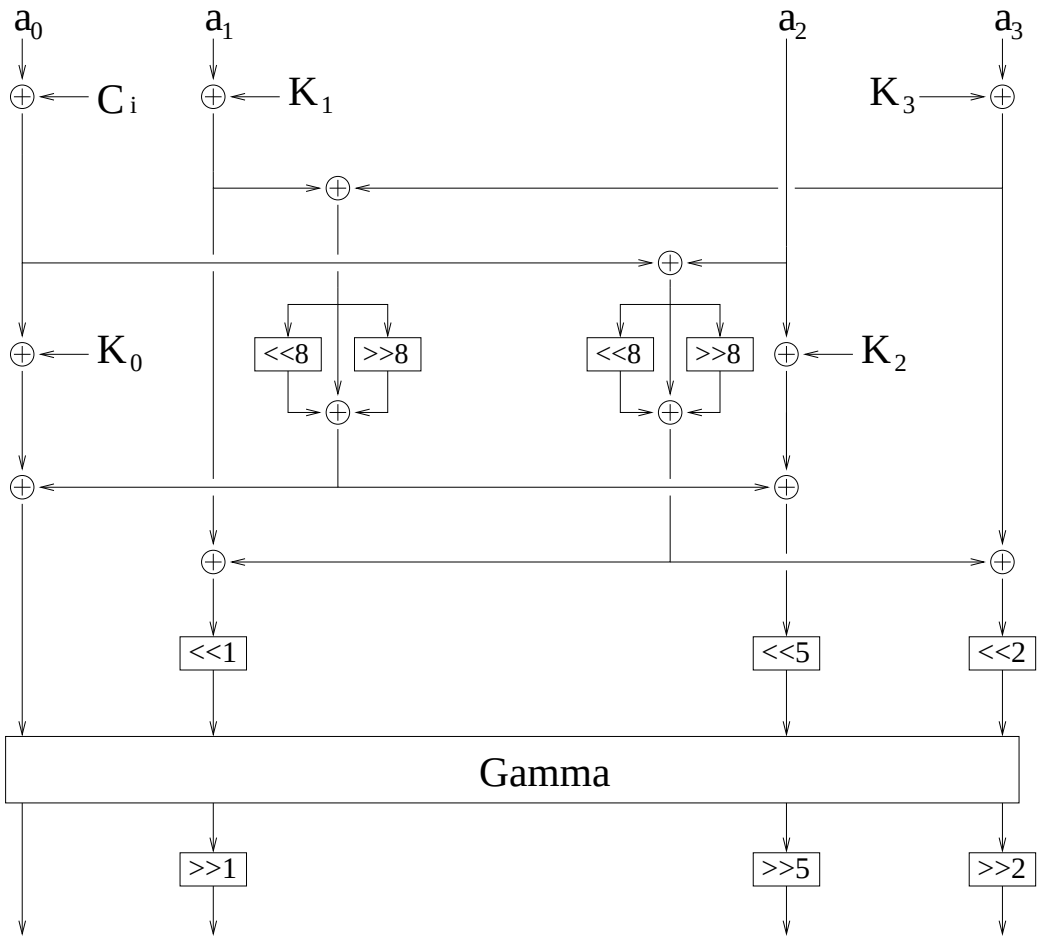

Figure 1: The Noekeon round function.