Results from a Search for the Best Linear Approximation of a Block Cipher

Kashif Ali and Howard M. Heys
Electrical and Computer Engineering
Memorial University of Newfoundland
St. John's, Newfoundland, Canada
{alikashif, howard}@engr.mun.ca

Abstract: In this paper, we investigate the application of an algorithm to find the best linear approximation of a basic Substitution-Permutation Network block cipher. The results imply that, while it is well known that the S-box used for the Advanced Encryption Standard has good nonlinear properties, it is straightforward to randomly select other S-boxes which are able to provide a similar level of security, as indicated by the exact bias of the best linear approximation found by the algorithm, rather than a simple upper bound on the maximum bias.

Introduction

A classical approach to the design of symmetric-key block ciphers is based on a structure referred to as a Substitution-Permutation Network (SPN) [1][2]. Block ciphers typically encrypt a block of plaintext data by iteratively executing a number of rounds of basic operations on the block of data. In an SPN, a round consists of 3 layers of operations: substitution, permutation, and key mixing. The substitution layer maps the inputs of small sub-blocks to the outputs in a nonlinear manner, using a fixed mapping referred to as an S-box, thereby creating a mathematical complexity to the relationship of plaintext bits and ciphertext bits. In this paper, we assume that the same S-box is used for all substitutions in the cipher. The permutation layer transposes the positions of bits within the data block, resulting in a mixing of plaintext bits across the full ciphertext block. The key mixing is typically achieved by exclusive-or'ing subkey bits derived from the master cipher key. The widely deployed Advanced Encryption Standard (AES) [3] is structured similarly to an SPN, except that the permutation layer is replaced by the more general concept of a linear transformation layer.

S-boxes are typically studied for their cryptographic properties independently of the cipher structure. In this paper, we investigate S-boxes directly within the context of an SPN structure based on a 64-bit data block, with 8×8 S-boxes and a permutation layer which maps the output bit *i* of S-box *j* in a round to the input bit *j* of S-box *i* in the next round. Such a permutation provides an effective diffusion of bits throughout the data block.

The applicability of linear cryptanalysis [4] to the 64-bit SPN is studied by considering the effect of using different S-boxes for the network. Linear cryptanalysis is an important fundamental attack applied to block ciphers which exploits the likelihood of a linear relationship (using modulo-2 mathematics) between a set of plaintext bits and ciphertext bits. Using this relationship, it is possible to extract information about the cipher key bits. In order to approximate a linear relationship, the properties of the cipher S-box must be analyzed and exploited. For this purpose, a bias distribution table is determined. For an 8×8 S-box, the bias table consists of 256 rows and 256 columns. Each row corresponds to an S-box 8-bit input mask, α, and each column to an S-box 8-bit output mask, β. Each element in the table corresponds to the value $|(\delta_{\alpha,\beta}-128)|$, where $\delta_{\alpha,\beta}$ is the number of times, out of all possible 256 input values, the subset of input bits (indicated by the ones in α) exclusive-or'ed together are equal to the subset of output bits (indicated by the ones in β) exclusive-or'ed together. The bias of an S-box (for a given α and β) can be determined from $\varepsilon_{\alpha,\beta}=|(\delta_{\alpha,\beta}-128)|/256$. In cases where there are strong linear relationships, $\delta_{\alpha,\beta} << 128$ or $\delta_{\alpha,\beta} >> 128$, so that $\varepsilon_{\alpha,\beta} \rightarrow 1/2$.

Using appropriate assumptions [2], an attacker can concatenate linear approximations of S-boxes to derive an overall linear approximation for the cipher and, consequently, estimate the bias of the cipher approximation from the biases of the S-boxes actively involved in the approximation using the piling-up lemma [4]. The resulting complexity of the linear attack, in terms of the number of required known plaintext/ciphertext pairs, is inversely proportional to the square of the bias of the linear approximation.

Two-Round Iterative Search Algorithm

In order to make use of linear weaknesses within the S-boxes, an attacker must concatenate approximations from one round to the next to ensure that an overall linear approximation involves only plaintext and ciphertext bits. In doing this, an attacker must have an effective approach to selecting which S-boxes are actively involved in the approximation to maximize the bias of the overall linear approximation. It is well known, based on the piling-up lemma, that minimizing the number of active S-boxes and maximizing the bias of the active S-box approximations increases the bias of the overall cipher linear approximation.

An algorithm developed by Matsui [5] successfully found the best possible linear approximation of the Data Encryption Standard. However, when applied to the 64-bit SPN, we found the algorithm not efficient enough to finish the search for the best linear approximation. Hence, we have developed an algorithm that efficiently searches through the set of possible cipher linear approximations to find the one with the largest bias or one that is close to the largest bias. The intuition behind the approach is to collect a large list of the best approximations that can be found after two rounds and then to base the search over the next two rounds on this list. For example, for four rounds, each result in the list for the first two rounds is concatenated to all possible approximations for the next two rounds and the combinations giving the best approximations for all four rounds are used to prepare the list of results to be used in deriving approximations for six rounds. The process is iteratively repeated after every two rounds until the best approximation is obtained for n rounds. The assumption in the approach is that by basing the result for n rounds, on a list of good results for $n-2$ rounds, the overall result will be good, if not optimal.

We refer to this algorithm as the Two-Round Iterative (TRI) algorithm and note that the algorithm is very efficient and linear in terms of the number of rounds of the cipher. While the algorithm is not guaranteed to find the optimal linear approximation (i.e., the one with the largest bias), experiments on small ciphers support the conjecture that there is a high probability that the outcome of the algorithm is optimal and, in virtually all cases, the outcome is close to optimal [6]. Note that typically, linear cryptanalysis employs linear approaches of $n-1$ rounds where n is the number of rounds in the cipher. Details of the relatively trivially issues for applying the TRI algorithm to an odd number of rounds are given in [6].

Analysis of a Block Cipher

In this section, we examine the results obtained by running the TRI algorithm on the 64-bit SPN block cipher. In studying the bias tables of 8×8 S-boxes, it was found that, by considering the maximum value in the bias table for 10000 randomly selected S-boxes, approximately 94% of the S-boxes have maximum bias around 32/256 to 38/256. Since the largest biases for a linear approximation of a cipher typically occur when a small number of S-boxes are active in the approximation (as was supported by the results from smaller networks [6]), we conjecture that not more than 3 S-boxes are involved in each round in the best linear approximation of the 64-bit SPN cipher. Hence, this constraint is used when applying the TRI algorithm and is necessary to make the algorithm run in a practical amount of time on the 64-bit cipher. Consequently, we have studied the maximum value from the bias table when only one S-box is active per round during the approximation, i.e., when $wt(\alpha) = wt(\beta) = 1$ where $wt(\cdot)$ represents the Hamming weight operator. It was discovered that 65% of the 10000 S-boxes tested have maximum biases for $wt(\alpha) = wt(\beta) = 1$ concentrated around 18/256 to 22/256. The implications of this result are that it seems likely that the best cipher linear approximation will be significantly influenced by the low bias values for $wt(\alpha) = wt(\beta) = 1$. As a result, simple upper bounds on the bias computed based on the maximum S-box bias (for any values of α and β) and the minimum number of possible S-boxes in an approximation (eg. one S-box per round in the 64-bit SPN) are dramatically pessimistic for many ciphers. Nevertheless, simple bounding techniques have been typically used when analyzing the level of cipher security [2][3].

The TRI algorithm was run for 10 ciphers differentiated by using 10 random S-boxes labeled R_1 to R_{10} as the cipher S-box and results from the S-box bias tables are shown in Table 1. The table also includes the results for mathematically structured S-boxes, known to have good nonlinear properties, such as the AES and Camellia [7] S-boxes. As well, four randomly found "good" S-boxes that have low bias values for $wt(\alpha) = wt(\beta) = 1$, labeled from R_1^* to R_4^*, are shown. From the table, we can see that for the 10 random S-boxes the maximum bias value in the table is high compared to the S-boxes of AES and Camellia. The "good" S-boxes have a bias of 12/256 to 14/256, comparable to AES and Camellia, for $wt(\alpha) = wt(\beta) = 1$; however they differ significantly for overall maximum value in the bias table. This occurs because the AES and Camellia S-boxes have good values spread out consistently in the tables, while the "good" S-boxes are randomly generated and selected to have low values when $wt(\alpha) = wt(\beta) = 1$.

S-box	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}
Max Value in Bias Table	38	38	34	36	34	32	42	38	36	34
Max Value for $wt(\alpha) = wt(\beta) = 1$	22	22	20	26	22	18	22	18	20	22

S-box	AES	Cam	R_1^*	R_2^*	R_3^*	R_4^*
Max Value in Bias Table	16	16	32	32	34	36
Max Value for $wt(\alpha) = wt(\beta) = 1$	16	14	14	12	12	14

Table 1. Maximum Value in Bias Table for Different S-boxes
(bias = value / 256)

A seven round approximation (targeted to attack an 8 round cipher) is determined using the TRI algorithm and the resulting biases are shown in Table 2. The TRI algorithm is run with a list size of 8000 for all of the ciphers and takes just a few minutes on a PC. From the table, we can see that ciphers using "good" S-boxes have particularly low biases and can be even lower than the AES and Camellia S-box based networks. Similarly, it can be seen that, in all cases, a random S-box based network gives a comparable result (that is, within an order of magnitude) to the AES and Camellia S-box based networks. The results vary from about 8% of the bias of the AES-based cipher for a "good" S-box to about 8 times the AES-based cipher bias for a purely randomly selected S-box. The resulting implication is that the bias for an AES-based cipher is not significantly better and is, in a few cases, potentially worse than the bias for other ciphers with randomly selected S-boxes. In comparison, the simple upper bounds calculated based on one active S-box per round using the largest bias for the S-box (regardless of the input and output mask values) vary even more significantly. Although the upper bounds for the AES-based and Camellia-based ciphers are quite tight, for other S-boxes, the biases can be hundreds, or even thousands, of times smaller than implied by the upper bound. Hence, the calculated simple upper bound can not be considered to be a very good indicator of the actual relative strength of a cipher.

Cipher	**Maximum Bias** (ε)	**Upper Bound** ($\Gamma = 2^6\lambda^7$)	**Relative Bias** ($\varepsilon / \varepsilon_{AES}$)	**Relative Upper Bound** (Γ / ε)
AES	1.788e-7	2.384e-7	1	1.3
Camellia	1.223e-7	2.384e-7	0.68	1.9
R_1	1.337e-6	1.016e-4	7.48	76.0
R_2	4.754e-7	1.016e-4	2.66	213.7
R_3	3.830e-7	4.665e-5	2.14	121.8
R_4	1.344e-6	6.960e-5	7.52	51.8
R_5	3.781e-7	4.665e-5	2.11	123.4
R_6	4.516e-7	3.052e-5	2.53	67.6
R_7	9.104e-7	2.047e-4	5.09	224.8
R_8	1.432e-6	1.016e-4	8.01	70.9
R_9	1.230e-6	6.960e-5	6.88	56.6
R_{10}	1.208e-6	4.665e-5	6.76	38.6
R_1^*	2.737e-7	3.052e-5	1.53	111.5
R_2^*	4.638e-8	3.052e-5	0.26	658.0
R_3^*	1.349e-8	4.665e-5	0.08	3458.1
R_4^*	1.720e-7	6.960e-5	0.96	404.7

Table 2. Bias for 7 Round Linear Approximation Found Using TRI Algorithm
(λ = maximum value in bias table / 256)

Conclusions

We have used a two-round iterative algorithm to find good linear approximations and the corresponding biases in a basic 64-bit SPN. The results indicate that it is quite possible to have low biases in ciphers which do not use the AES S-box, an S-box mathematically structured to have good properties. Similar results have been found for differential cryptanalysis [6] in the same set of random S-boxes. This is significant because it is conceivable that the mathematical structure of the AES S-box, used to give good nonlinear properties, may actually make the cipher susceptible to other mathematical attacks; using S-boxes without mathematical structure (i.e., randomly selected) may make a cipher less vulnerable to attacks based on mathematical properties.

References

[1] A. J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[2] H.M. Heys and S.E. Tavares, "Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis", *Journal of Cryptology*, vol. 9, no. 1, pp. 1-19, 1996.

[3] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.

[4] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", *Lecture Notes in Computer Science, vo. 765: Advances in Cryptology - EUROCRYPT '93*, Springer-Verlag, pp. 386-397, 1994.

[5] M. Matsui, "On Correlation Between the Order of S-boxes and the Strength of DES", *Lecture Notes in Computer Science, vol. 950: Advances in Cryptology - EUROCRYPT '94*, Springer-Verlag, pp. 366-375, 1995.

[6] K. Ali, “An Algorithm to Analyze Substitution-Permutation Networks Resistance to Linear and Differential Cryptanalysis”, *M.Eng. Thesis*, Memorial University of Newfoundland, St. John's, Newfoundland, Canada, 2007.

[7] K. Aoki, T. Ichikawa, M. Kansa, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia: A 128-Bit Block Ciphers Suitable for Multiple Platforms – Design and Analysis", *Lecture Notes in Computer Science, vol. 2012: Selected Areas in Cryptography (SAC 2000)*, pp. 39-56, 2001.