

Overestimates for the Gain of Multiple Linear Approximations in Symmetric Cryptology

S. Murphy

Abstract—This paper shows that Corollary 1 of “On Multiple Linear Approximations” (Crypto 2004 – LNCS 3152) is incorrect. In particular, the value given for the gain by Corollary 1 is likely to be a significant overestimate of this quantity. Thus any data requirements for linear cryptanalysis with multiple linear approximations based on this value for the gain are highly questionable.

Index Terms—Linear cryptanalysis, multiple linear approximations, gain, Jensen’s inequality.

I. INTRODUCTION

Linear cryptanalysis [1] of a block cipher in its basic form uses a linear approximation of the form

$$\alpha^T \begin{pmatrix} \mathbf{p} \\ \mathbf{c} \end{pmatrix} = k \text{ with probability } \frac{1}{2} (1 + \epsilon),$$

where α is a data mask, k is one bit of key information, \mathbf{p} is a plaintext and \mathbf{c} is a corresponding ciphertext. The value ϵ is known as the *imbalance* or *correlation* (twice the *bias*) of the linear approximation. If $\epsilon \neq 0$, then it is possible to estimate the key bit k reasonably accurately if the number N of plaintext-ciphertext pairs is at least ϵ^{-2} [1].

Enhanced forms of linear cryptanalysis [2], [3] use a collection of m such linear approximations. Such a situation with multiple linear approximations is also considered by [4], where the *gain* of such a linear cryptanalysis is defined. The gain is an attempt to quantify the advantage of such a linear cryptanalysis over exhaustive search.

This paper is concerned with the values given for the gain by [4]. In particular, there are two results given for the value of the gain, namely *Theorem 1* and *Corollary 1* of [4], where it is claimed that the value for the gain given by *Corollary 1* is an accurate (asymptotic) approximation of that given by *Theorem 1*. We show the value for the gain given by *Corollary 1* generally greatly exceeds the value for the gain given by *Theorem 1*, so this claim is not correct.

II. MULTIPLE LINEAR APPROXIMATIONS

We consider a linear cryptanalysis based on N plaintext-ciphertext pairs. We suppose that we have m linear approximations

$$\alpha_i^T \begin{pmatrix} \mathbf{p} \\ \mathbf{c} \end{pmatrix} = k_i \text{ with probability } \frac{1}{2} (1 + \epsilon_i)$$

S. Murphy is with the Information Security Group, Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K.

Manuscript received XX; revised XX.

for distinct data masks α_i , individual bits of key information k_i and imbalances ϵ_i ($i = 1, \dots, m$). The *capacity* \bar{c}^2 of this collection of linear approximations is given by Definition 2 of [4] to be $\bar{c}^2 = \sum_{i=1}^m \epsilon_i^2$.

For simplicity, we suppose that the m key bits k_1, \dots, k_m give m bits of information about the block cipher key. We let $\mathbf{z} = (k_1, \dots, k_m)^T$ denote the *key class*, and we denote the set of all key classes by \mathcal{Z} , so $\mathcal{Z} = \mathbb{Z}_2^m$ and $|\mathcal{Z}| = 2^m$. We let \mathbf{z}^* denote the key class containing the true key, and, without loss of generality, we suppose that $\mathbf{z}^* = 0$. We let $\mathcal{Z}^* = \mathcal{Z} \setminus \{\mathbf{z}^*\} = \mathbb{Z}_2^m \setminus \{0\}$ denote the set of key classes not containing the true key, so $|\mathcal{Z}^*| = 2^m - 1$. We denote the m -dimensional *imbalance vector* corresponding to key class \mathbf{z} by \mathbf{c}_z , so

$$\mathbf{c}_z = ((-1)^{z_1} \epsilon_1, \dots, (-1)^{z_m} \epsilon_m)^T.$$

We note that the squared distance from such an imbalance vector to the imbalance vector for the true key class is given by

$$|\mathbf{c}_z - \mathbf{c}_{\mathbf{z}^*}|^2 = \left| -2(z_1 \epsilon_1, \dots, z_m \epsilon_m)^T \right|^2 = 4 \sum_{i=1}^m z_i^2 \epsilon_i^2.$$

III. STATEMENT OF *Theorem 1* AND *Corollary 1*

For completeness, we now state *Theorem 1* and *Corollary 1* of [4], but using $\tilde{\gamma}$ to denote the value for the gain given by the expression of *Corollary 1*.

Theorem 1 [4]. Given m linear approximations and N independent pairs (P_i, C_i) , an adversary can mount an attack with a gain equal to:

$$\gamma = -\log_2 \left[2 \frac{1}{|\mathcal{Z}|} \sum_{\mathbf{z} \in \mathcal{Z}^*} \phi \left(-\frac{1}{2} N^{\frac{1}{2}} |\mathbf{c}_z - \mathbf{c}_{\mathbf{z}^*}| \right) + \frac{1}{|\mathcal{Z}|} \right],$$

where ϕ is the standard normal cumulative distribution function, $\mathbf{c}_z = ((-1)^{z_1} \epsilon_1, \dots, (-1)^{z_m} \epsilon_m)^T$, and $|\mathcal{Z}|$ is the number of key classes induced by the approximations.

Corollary 1 [4]. If $|\mathcal{Z}|$ is sufficiently large, then the value γ for the gain given in *Theorem 1* can be accurately approximated by

$$\tilde{\gamma} = -\log_2 \left[2 \frac{|\mathcal{Z}| - 1}{|\mathcal{Z}|} \phi \left(-\left(\frac{1}{2} N \bar{c}^2 \right)^{\frac{1}{2}} \right) + \frac{1}{|\mathcal{Z}|} \right],$$

where $\bar{c}^2 = \sum_{i=1}^m \epsilon_i^2$.

IV. CONCEPTS USED TO DEFINE GAIN VALUES

The value γ given for the gain by *Theorem 1* and the value $\tilde{\gamma}$ given for the gain by *Corollary 1* can both be expressed in terms of two functions, g and H_m , and a random variable X , which we now define.

The function g on the positive real numbers is defined by

$$g(x) = \phi\left(-\frac{1}{2} N^{\frac{1}{2}} x^{\frac{1}{2}}\right),$$

where ϕ denotes the cumulative distribution function for a standard normal $N(0; 1)$ random variable. We note that $g(x)$ is a convex function of x for $x > 0$ as

$$g''(x) = \frac{1}{32} \frac{1}{\sqrt{2\pi}} N^{\frac{1}{2}} e^{-\frac{Nx}{8}} (N + 4x^{-1}) x^{-\frac{1}{2}} > 0 \text{ for } x > 0.$$

The function H_m on the positive real numbers is defined by

$$\begin{aligned} H_m(x) &= -\log_2(2(1 - 2^{-m})x + 2^{-m}) \\ &= -\log_2\left[2\frac{|Z^*|}{|Z|}x + \frac{1}{|Z|}\right]. \end{aligned}$$

We note that $H_m(x)$ is a decreasing function of x for $x > 0$ as

$$H'_m(x) = -\frac{1}{\log 2} \left(\frac{2(1 - 2^{-m})}{2(1 - 2^{-m})x + 2^{-m}} \right) < 0 \text{ for } x > 0.$$

The random variable X on \mathcal{Z}^* is defined for $\mathbf{z} \in \mathcal{Z}^*$ by

$$X(\mathbf{z}) = |\mathbf{c}_{\mathbf{z}} - \mathbf{c}_{\mathbf{z}^*}|^2,$$

so X is the random variable giving the squared distance of an imbalance vector for an incorrect key class from the imbalance vector for the true key class. Thus the distribution of X is given by

$$\mathbf{P}(X = x) = \frac{\#\{\mathbf{z} \in \mathcal{Z}^* \mid |\mathbf{c}_{\mathbf{z}} - \mathbf{c}_{\mathbf{z}^*}|^2 = x\}}{(2^m - 1)}.$$

V. COMPARISON OF VALUES FOR THE GAIN

We now compare the two values γ and $\tilde{\gamma}$ given for the gain in *Theorem 1* and *Corollary 1*. We show in Appendix A that the value γ given for the gain by *Theorem 1* can be expressed as

$$\gamma = H_m(\mathbf{E}[g(X)]),$$

and we show in Appendix B that the value $\tilde{\gamma}$ given for the gain by *Corollary 1* can be expressed as

$$\tilde{\gamma} = H_m(g(2\bar{c}^2)) = H_m(g((1 - 2^{-m})\mathbf{E}[X])).$$

However, this value $\tilde{\gamma}$ for the gain can be well approximated by $\hat{\gamma}$, where

$$\hat{\gamma} = H_m(g(\mathbf{E}[X])).$$

We now use Jensen's inequality [5] to compare γ and $\hat{\gamma}$. As g is a convex function of the positive real numbers, Jensen's inequality shows that

$$g(\mathbf{E}[X]) \leq \mathbf{E}[g(X)].$$

Furthermore H_m is a decreasing function of the positive real numbers, so

$$\hat{\gamma} = H_m(g(\mathbf{E}[X])) \geq H_m(\mathbf{E}[g(X)]) = \gamma.$$

However, $\tilde{\gamma}$ is usually extremely well-approximated by $\hat{\gamma}$, so giving Lemma 1.

Lemma 1: The value $\tilde{\gamma}$ for the gain given by *Corollary 1* generally exceeds the value γ given for the gain by *Theorem 1*.

VI. EXAMPLE VALUES FOR THE GAIN

The important issue in the use of the value $\tilde{\gamma}$ given by *Corollary 1* to approximate the value γ of the gain given by *Theorem 1* is whether the overestimate of γ by $\tilde{\gamma}$ referred to in Lemma 1 is significant. The following examples show that it is generally the case that the use of $\tilde{\gamma}$ given in *Corollary 1* gives a large overestimate of the value γ given for the gain by *Theorem 1*.

For simplicity, we assume that all m linear approximations have the same imbalance ϵ , that is $\epsilon_1 = \dots = \epsilon_m = \epsilon$. The capacity of such a collection of linear approximations is clearly $\bar{c}^2 = m\epsilon^2$. In this situation, using the result given in Section II, we have

$$|\mathbf{c}_{\mathbf{z}} - \mathbf{c}_{\mathbf{z}^*}|^2 = 4\epsilon^2 \sum_{i=1}^m z_i^2 = 4\epsilon^2 |\mathbf{z}|^2.$$

As there are $\binom{m}{l}$ such vectors $\mathbf{z} \in \mathbb{Z}_2^m$ with $|\mathbf{z}|^2 = l$, the random variable X is given by

$$X = 4\epsilon^2 l \text{ with probability } \binom{m}{l} (2^m - 1)^{-1} \quad [l = 1, \dots, m].$$

Thus X is a multiple of a censored $\text{Bin}(m, \frac{1}{2})$ random variable with 0 removed, so the mean of X is given by $\mathbf{E}[X] = 4\epsilon^2 \frac{m}{2} \frac{2^m}{2^m - 1}$. We therefore obtain $g(\mathbf{E}[X])$, used to define $\hat{\gamma}$, as

$$\begin{aligned} g(\mathbf{E}[X]) &= \phi\left(-\frac{1}{2} N^{\frac{1}{2}} \epsilon \left(2m \frac{2^m}{2^m - 1}\right)^{\frac{1}{2}}\right) \\ &= \phi\left(- (N\epsilon^2)^{\frac{1}{2}} \left(\frac{m}{2}\right)^{\frac{1}{2}} \left(\frac{2^m}{2^m - 1}\right)^{\frac{1}{2}}\right). \end{aligned}$$

By contrast, the mean of $g(X)$ is given by

$$\begin{aligned} \mathbf{E}[g(X)] &= \frac{1}{2^m - 1} \sum_{l=1}^m \binom{m}{l} \phi\left(-\frac{1}{2} N^{\frac{1}{2}} 2\epsilon l^{\frac{1}{2}}\right) \\ &= \frac{1}{2^m - 1} \sum_{l=1}^m \binom{m}{l} \phi\left(- (N\epsilon^2)^{\frac{1}{2}} l^{\frac{1}{2}}\right). \end{aligned}$$

We now consider the values of these two expressions for a particular example. We suppose that there are $m = 8$ linear approximations, so the capacity $\bar{c}^2 = 8\epsilon^2$. We further suppose that we have $N = 2\epsilon^{-2}$ plaintext-ciphertext pairs, so $N\epsilon^2 = 2$. In this case we have

$$g(\mathbf{E}[X]) = 0.0023, \text{ whereas } \mathbf{E}[g(X)] = 0.0074.$$

For this example, we have $g(\mathbf{E}[X]) < \frac{1}{3} \mathbf{E}[g(X)]$, so illustrating Jensen's inequality. We now calculate the various values given for the gain in this situation, so

$$\gamma = H_8(g(\mathbf{E}[X])) = 5.75 \text{ and } \hat{\gamma} = H_8(\mathbf{E}[g(X)]) = 6.88.$$

Furthermore, a direct calculation gives $\tilde{\gamma} = 6.87$, so $\hat{\gamma}$ is obviously a very good approximation of $\tilde{\gamma}$. In this situation, *Corollary 1* overestimates the gain as given by *Theorem 1* by over one bit in six.

More generally, we can consider the situation as the number m of linear approximations increases. As above, we suppose we have $N = 2\epsilon^{-2}$ plaintext-ciphertext pairs, each of which has imbalance ϵ , so the capacity $\bar{c}^2 = m\epsilon^2$. The following Table compares values γ for the gain given by *Theorem 1* with the values $\tilde{\gamma}$ for the gain given by *Corollary 1* for $m = 8, 16, 24, 32$ linear approximations. It can be clearly seen that the overestimate for value of the gain of *Theorem 1* given by *Corollary 1* increases both in absolute and relative terms as the number m of linear approximations increases.

Linear Approximations	8	16	24	32
<i>Theorem 1</i> Value γ	5.75	10.68	15.36	19.95
<i>Corollary 1</i> Value $\tilde{\gamma}$	6.87	13.64	19.90	25.93
Overestimate of γ by $\hat{\gamma}$	1.12	2.95	4.54	5.98

VII. THE ‘‘PROOF’’ OF *Corollary 1*

Appendix A.1 of [4] is entitled *Proof of Corollary 1*, and *Appendix A.1* essentially asserts that $g(\mathbf{E}[X]) = \mathbf{E}[g(X)]$, Jensen’s inequality notwithstanding. The examples of Section VI shows that this assertion, which is the basis of the ‘‘proof’’ of *Corollary 1*, is simply wrong. *Appendix A.1* attempts to justify this assertion by considering the Taylor series for $g(x)$ about the point $\mathbf{E}(X)$ (in our terminology), taking expectations, and then implicitly assuming that: *the higher order [second and above] moments of X are sufficiently small* [4]. However, the second order moment $\mathbf{E}((X - \mathbf{E}(X))^2)$ is simply the variance of X , and this is generally not negligible. For example, in the cases considered in Section VI in which all imbalances are equal to ϵ , the second order moment of X is given by

$$\begin{aligned} \mathbf{E}(X - \mathbf{E}(X))^2 &= \text{Var}(X) \\ &= (4\epsilon^2)^2 \frac{m}{4} \left(1 - \frac{m-1}{2^m-1} - \frac{m}{(2^m-1)^2}\right) \\ &\approx 4m\epsilon^4, \end{aligned}$$

which is never negligible and indeed increases with m . As with the discussion by [4] of probabilities for dependent data masks [6], the given ‘‘proof’’ of *Corollary 1* by [4] is not correct.

VIII. CONCLUSIONS

We have shown that the value for the gain given by *Corollary 1* of [4] is not reliable, and is in general a large overestimate of the value of the gain given by *Theorem 1*. Furthermore, the ‘‘proof’’ given of *Corollary 1* simply ignores Jensen’s inequality, a fundamental result in probability and theoretical statistics. Any result based on this value for the gain given by *Corollary 1*, such as the theoretical data requirements for such a linear cryptanalysis, is therefore highly questionable.

APPENDIX A

VALUE FOR THE GAIN GIVEN BY *Theorem 1*

The value γ given for the gain given by *Theorem 1* of [4] is

$$\gamma = -\log_2 \left[2 \frac{1}{|\mathcal{Z}|} \sum_{\mathbf{z} \in \mathcal{Z}^*} \phi \left(-\frac{1}{2} N^{\frac{1}{2}} |\mathbf{c}_{\mathbf{z}} - \mathbf{c}_{\mathbf{z}^*}| \right) + \frac{1}{|\mathcal{Z}|} \right].$$

Thus we have

$$\gamma = -\log_2 \left[2 \frac{(1 - 2^{-m})}{2^m - 1} \sum_{\mathbf{z} \neq 0} g(|\mathbf{c}_{\mathbf{z}} - \mathbf{c}_0|^2) + 2^{-m} \right].$$

However, the mean value of $g(X)$ is given by

$$\mathbf{E}[g(X)] = \frac{1}{2^m - 1} \sum_{\mathbf{z} \neq 0} g(|\mathbf{c}_{\mathbf{z}} - \mathbf{c}_0|^2),$$

so we have shown that the value γ given for the gain by *Theorem 1* is given by

$$\gamma = -\log_2 [2(1 - 2^{-m}) \mathbf{E}[g(X)] + 2^{-m}] = H_m(\mathbf{E}[g(X)]).$$

APPENDIX B

VALUE FOR THE GAIN GIVEN BY *Corollary 1*

The value $\tilde{\gamma}$ given for the gain by *Corollary 1* of [4] is

$$\begin{aligned} \tilde{\gamma} &= -\log_2 \left[2 \frac{|\mathcal{Z}|-1}{|\mathcal{Z}|} \phi \left(-\left(\frac{1}{2} N \bar{c}^2 \right)^{\frac{1}{2}} \right) + \frac{1}{|\mathcal{Z}|} \right] \\ &= H_m \left(\phi \left(-\frac{1}{2} (2N\bar{c}^2)^{\frac{1}{2}} \right) \right) = H_m(g(2\bar{c}^2)). \end{aligned}$$

We express this quantity in terms of the mean of X , which is given by

$$\mathbf{E}[X] = \frac{1}{|\mathcal{Z}^*|} \sum_{\mathbf{z} \neq \mathbf{z}^*} |\mathbf{c}_{\mathbf{z}} - \mathbf{c}_{\mathbf{z}^*}|^2 = (2^m - 1)^{-1} \sum_{\mathbf{z} \neq 0} |\mathbf{c}_{\mathbf{z}} - \mathbf{c}_0|^2.$$

However, $|\mathbf{c}_{\mathbf{z}} - \mathbf{c}_0|^2 = 4 \sum_{i=1}^m z_i^2 \epsilon_i^2$ (Section I), so we have

$$\mathbf{E}[X] = (2^m - 1)^{-1} \sum_{\mathbf{z} \neq 0} \sum_{i=1}^m 4z_i^2 \epsilon_i^2 = \frac{4}{2^m - 1} \sum_{i=1}^m \epsilon_i^2 \sum_{\mathbf{z} \neq 0} z_i^2.$$

As the two summations in the above expression can be evaluated to give

$$\sum_{\mathbf{z} \neq 0} z_i^2 = \sum_{\mathbf{z} \neq 0} z_i = 2^{m-1} \text{ and } \sum_{i=1}^m \epsilon_i^2 = \bar{c}^2,$$

we have

$$\mathbf{E}[X] = \frac{4 \cdot 2^{m-1}}{2^m - 1} \bar{c}^2.$$

Thus we can give the capacity in terms of the mean of X as

$$\bar{c}^2 = \frac{1}{2} (1 - 2^{-m}) \mathbf{E}[X],$$

so we can obtain

$$\begin{aligned} \phi \left(-\left(\frac{1}{2} N \bar{c}^2 \right)^{\frac{1}{2}} \right) &= \phi \left(-\frac{1}{2} N^{\frac{1}{2}} ((1 - 2^{-m}) \mathbf{E}[X])^{\frac{1}{2}} \right) \\ &= g((1 - 2^{-m}) \mathbf{E}[X]). \end{aligned}$$

This means we can express the value $\tilde{\gamma}$ given for the gain by *Corollary 1* as

$$\tilde{\gamma} = H_m(g((1 - 2^{-m}) \mathbf{E}[X])).$$

If we now define the value

$$\hat{\gamma} = H_m(g(\mathbf{E}[X])),$$

then clearly $\hat{\gamma}$ is a very good approximation of $\tilde{\gamma}$ when m is moderately large.

ACKNOWLEDGMENT

The author would like to thank the referees for their comments.

REFERENCES

- [1] M. Matsui, "Linear Cryptanalysis for the DES Cipher," in *Advances in Cryptology – EUROCRYPT 1993*, ser. LNCS, T. Hellesest, Ed., vol. 765. Springer-Verlag, 1993, pp. 386–397.
- [2] B. Kaliski and M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations," in *Advances in Cryptology – CRYPTO 94*, ser. LNCS, Y. Desmedt, Ed., vol. 839. Springer-Verlag, 1994, pp. 26–39.
- [3] —, "Linear Cryptanalysis Using Multiple Approximations and FEAL," in *Fast Software Encryption 1994*, ser. LNCS, B. Preneel, Ed., vol. 1008. Springer-Verlag, 1995, pp. 249–264.
- [4] A. Biryukov, C. D. Cannière, and M. Quinquater, "On Multiple Approximations," in *Advances in Cryptology – CRYPTO 04*, ser. LNCS, M. Franklin, Ed., vol. 3152. Springer-Verlag, 2004, pp. 1–22.
- [5] S. Silvey, *Statistical Inference*. Chapman and Hall, 1975.
- [6] S. Murphy, "The Independence of Linear Approximations in Symmetric Cryptology," *IEEE Transactions on Information Theory*, vol. 52, pp. 5510–5518, 2006.