The Return of the Cryptographic Boomerang

S. Murphy

***Abstract*—The boomerang analysis, together with its offspring the amplified boomerang analysis and the rectangle analysis, are techniques that are widely used in the analysis of block ciphers. We give realistic examples which demonstrate that the boomerang analysis can commonly give probability values that are highly inaccurate. Thus any complexity estimates for the security of a block cipher based on the boomerang or rectangle analysis must be viewed extremely sceptically.**

***Index Terms*—Block Ciphers, Boomerang Analysis, Rectangle Analysis.**

I. Introduction

The *boomerang* analysis of [1] is an adaptation of differential cryptanalysis [2], [3] in which quartets of encryptions and decryptions are used. Two related plaintexts are encrypted, and the resulting pair of ciphertexts is then used to generate two new related ciphertexts. These two new ciphertexts are then decrypted to give two new plaintexts. The aim of the boomerang analysis is to use such quartets of plaintexts and of ciphertexts to find key information. Furthermore, enhanced versions of the boomerang analysis based on this idea have also been developed, such as the *amplified boomerang* analysis [4] and the *rectangle* analysis [5].

There is however no *a priori* reason for the probabilistic argument of [1] concerning the boomerang analysis, and therefore for the related analyses, to be correct. We demonstrate this by giving simple examples using the Data Encryption Standard (DES) [6] and the Advanced Encryption Standard (AES) [7].

The motivation for the use of the word *boomerang* to describe such an analysis of quartets is given in [1].

> *This is why we call it the boomerang attack: when you send it properly, it always comes back to you.*

We send a DES or an AES boomerang, but our boomerang won't come back.

II. The Boomerang Analysis

We describe the basic boomerang analysis in the manner of [1], and a schematic diagram of the boomerang analysis, based on Figure 1 of [1], is given in Figure 1. We base our notation on that of [1], so we suppose that E represents the block cipher encryption under a fixed key. The basic boomerang analysis is based on a quartet of encryptions and decryptions, and the process for generating such a quartet is described below.

- Choose values $\triangle$ and ∇.
- Choose a pair of plaintexts P and P' such that $P + P' = \triangle$.

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.

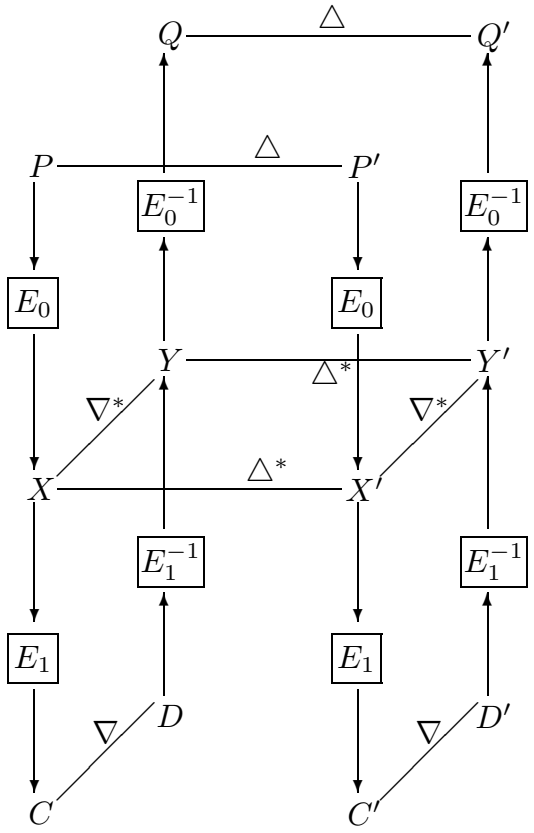

Fig. 1. Schematic Diagram of the Basic Boomerang Analysis.

- Encrypt P and P' to obtain ciphertexts $C = E(P)$ and $C' = E(P')$.
- Obtain two further ciphertexts $D = C + \nabla$ and $D' = C' + \nabla$.
- Decrypt D and D' to obtain plaintexts $Q = E^{-1}(D)$ and $Q' = E^{-1}(D')$.

The boomerang analysis is an attempt to use the ideas of differential cryptanalysis [2], [3] to analyse the plaintext quartet (P, P', Q, Q') and ciphertext quartet (C, C', D, D'). To this end, we consider the encryption operation in two parts, so we may write $E = E_1 \circ E_0$. Thus E_0 represents the initial part of the encryption operation, and E_1 represents the final part. We let (X, X', Y, Y') denote the intermediate result of the encryption and decryption operations, so we have:

$$\begin{aligned} X &= E_0(P) = E_1^{-1}(C), \qquad & X' &= E_0(P') = E_1^{-1}(C'), \\ Y &= E_0(Q) = E_1^{-1}(D), \qquad & Y' &= E_0(Q') = E_1^{-1}(D'). \end{aligned}$$

The basic boomerang analysis uses two differential characteristics [2], [3]. The differential characteristic $\triangle \to \triangle^*$ is used for the initial part E_0 of the overall encryption E and the differential characteristic $\nabla^* \to \nabla$ is used for the final

part E_1 of the overall encryption E, for some values $\triangle^*$ and ∇^*. A quartet of encryptions and decryptions, or equivalently the corresponding plaintext and ciphertext quartets, is called a *right quartet* if the following conditions hold:

$$\begin{array}{ll} P+P'=Q+Q'=\triangle, & X+X'=Y+Y'=\triangle^*, \\ X+Y=X'+Y'=\nabla^*, & C+D=C'+D'=\nabla. \end{array}$$

A motivation for using this quartet of encryptions and decryptions, and for the definition of a right quartet is given in [1].

> *We want to cover the pair P, P' with the characteristic for E_0, and to cover the pairs P, Q and P', Q' with the characteristic for E_1^{-1}. Then (we claim) the pair Q, Q' is perfectly set up to use the characteristic $\triangle^* \to \triangle$ for E_0^{-1}.*

It is the case that

$$\begin{array}{rcl} E_0(Q)+E_0(Q') = & Y+Y' & \\ = & (Y+X)+(X+X')+(X'+Y') & \\ = & \nabla^*+\triangle^*+\nabla^*=\triangle^* & \end{array}$$

is indeed a condition required to start the characteristic $\triangle^* \to \triangle$ for E_0^{-1}, the inverse of the initial part of the encryption operation. However, whilst this condition is a necessary condition, it is not a sufficient condition, as the examples of Section III and VI demonstrate.

The statistical reasoning of the boomerang analysis given in Section 4 of [1] states that the probability p of a right quartet satisfies

$$p \geq p_0^2 p_1^2,$$

where p_0 is the probability of the differential characteristic $\triangle \to \triangle^*$ under E_0 and p_1 is the probability of the differential characteristic $\nabla \to \nabla^*$ under E_1. The complexity estimates for the boomerang analysis given in [1] are based on this estimate of p. However, in both Sections III and VI we give examples of a boomerang analysis with $p_0, p_1 > 0$, but for which a right quartet can never occur, that is $p = 0$.

III. A DES Boomerang

We consider a boomerang analysis on a block cipher that consists of four rounds of the Data Encryption Standard (DES) [6]. Thus E is the encryption under some fixed key of four rounds of the DES (without IP and IP^{-1}), and we suppose that E_0 is the initial two rounds of this encryption and that E_1 the final two rounds of this encryption. We use the two differential characteristics used in the iterated differential cryptanalysis of the DES [2], [3]. Thus we define

$$\begin{array}{rcl} \triangle & = & \triangle^* = \texttt{19600000 00000000} = (\gamma_9, 0) = \delta_9 \\ \text{and} \quad \nabla & = & \nabla^* = \texttt{1B600000 00000000} = (\gamma_{\texttt{B}}, 0) = \delta_{\texttt{B}}, \end{array}$$

so in particular we have:

$$\begin{array}{rcl} E_0(Z)+E_0(Z+\triangle) = & \triangle^* & \text{with probability } p_0 \approx \frac{1}{234}, \\ E_1(Z)+E_1(Z+\nabla^*) = & \nabla & \text{with probability } p_1 \approx \frac{1}{234}. \end{array}$$

The reasoning of Section 4 of [1] would now assert that the probability of a right quartet is at least $p_0^2 p_1^2 \approx \left(\frac{1}{234}\right)^4$.

We now consider the conditions required for a right quartet to occur. Accordingly, we let c, c', d, d' denote the four 6-bit inputs to DES S-Box 2 in the fourth round of this cipher. Thus c, c', d, d' are a selection of six bits of C, C', D, D'. For a right quartet, we require that $X + X' = Y + Y' = \triangle^* = \delta_9$ and $X + Y = X' + Y' = \nabla^* = \delta_{\texttt{B}}$. Allowing for the expansion phase of the DES round function [6], a right quartet therefore satisfies

$$c + c' = d + d' = \texttt{110010} \text{ and } c + d = c' + d' = \texttt{110110},$$

which gives the following relationship between the four 6-bit S-Box inputs:

$$\begin{array}{rcl} c' & = & c + \texttt{110010}, \\ d & = & c + \texttt{110110}, \\ \text{and} \quad d' & = & d + \texttt{110010} = c + \texttt{000100}. \end{array}$$

In the classical differential cryptanalysis of the DES, we require that the outputs of the respective pairs of S-Boxes are identical. Thus we have

$$S_2(c) = S_2(d) \text{ and } S_2(c') = S_2(d'),$$

where $S_2 : \mathbb{Z}_2^6 \to \mathbb{Z}_2^4$ is the 6-bit to 4-bit function given by DES S-Box 2. For a right quartet to exist, we therefore require that there exists a 6-bit value c such that

$$\begin{array}{rcl} S_2(c) & = & S_2(c + \texttt{110110}) \\ \text{and } S_2(c + \texttt{110010}) & = & S_2(c + \texttt{000100}). \end{array}$$

It is easy to verify by a direct search of all $2^6 = 64$ possibilities for c that no such value for c exists.

It is is not therefore possible for a right quartet to exist in this boomerang analysis. In other words, a right quartet exists in this boomerang analysis with probability zero, rather than than the probability of at least $p_0^2 p_1^2 \approx \left(\frac{1}{234}\right)^4 > 0$ asserted by [1]. This DES boomerang *never* comes back.

IV. The Amplified Boomerang Analysis

The *amplified boomerang* analysis of [4] is an adaptation of the basic boomerang analysis that only uses encryptions and no decryptions in a chosen plaintext analysis. The idea is to encrypt pairs (P, P') or (Q, Q') of plaintexts satisfying $P + P' = Q + Q' = \triangle$. As before, we let $(X, X') = (E_0(P), E_0(P'))$ and $(Y, Y') = (E_0(Q), E_0(Q'))$ denote the intermediate values of encryptions under E. Such intermediate values (X, X') or (Y, Y') then satisfy $X + X' = \triangle^*$ or $Y + Y' = \triangle^*$ with probability p_0. Thus if we start with N such plaintext pairs, we expect to obtain Np intermediate pairs with difference $\triangle^*$, and so we expect to obtain about $\frac{1}{2}(Np)^2$ intermediate quartets (X, X', Y, Y') satisfying $X + X' = Y + Y' = \triangle^*$. It is then asserted by [4] that such an intermediate quartet also satisfies $X + Y = X' + Y' = \nabla^*$, the other part of the boomerang condition, uniformly at random. The example of Section III shows this is not the case. There is no *a priori* reason to assume that amplified boomerang analysis works in the manner described by [4].

V. The Rectangle Analysis

The basic idea of the *rectangle* analysis is mentioned in [1], but was developed by [5] as an adaptation of the amplified boomerang analysis that considers all values for the appropriate intermediate values. We suppose that we are considering an n-bit block cipher and we let

$$\begin{array}{rcl} \mathbf{P} & = & (P, P', Q, Q')^T, \\ \mathbf{X} & = & (X, X', Y, Y')^T \\ \text{and} \quad \mathbf{C} & = & (C, C', D, D')^T \end{array}$$

denote the quartet vectors at the plaintext, intermediate and ciphertext stages respectively, so $\mathbf{P}$, $\mathbf{X}$ and $\mathbf{C}$ are vectors over $\mathrm{GF}(2)$ of length $4n$. We now let

$$S = \begin{pmatrix} I & I & 0 & 0 \\ 0 & 0 & I & I \end{pmatrix}, T = \begin{pmatrix} I & I & 0 & 0 \\ 0 & 0 & I & I \\ I & 0 & I & 0 \\ 0 & I & 0 & I \end{pmatrix}$$

$$\text{and} \quad U = \begin{pmatrix} I & 0 & I & 0 \\ 0 & I & 0 & I \end{pmatrix}$$

denote the matrices over $\mathrm{GF}(2)$ giving the required differences at these stages, where the defining sub-blocks are $n \times n$ matrices. Thus S and U are matrices of rank $2n$ and T is a matrix of rank $3n$. We let

$$\widetilde{\triangle} = \begin{pmatrix} \triangle \\ \triangle \end{pmatrix}, \ \mathbf{z} = \begin{pmatrix} z \\ z \\ z' \\ z' \end{pmatrix} \text{ and } \widetilde{\nabla} = \begin{pmatrix} \nabla \\ \nabla \end{pmatrix}$$

denote the required differences at these stages, so the probability of interest for the analysis of plaintext and ciphertext quartets is then given by

$$\mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, S\mathbf{P} = \widetilde{\triangle}\right).$$

Under the assumption that the sequence of difference values $(S\mathbf{P}, T\mathbf{X}, U\mathbf{C})$ forms a Markov process [8], this probability $\mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, S\mathbf{P} = \widetilde{\triangle}\right)$ is given by

$$\sum_{\mathbf{z}} \mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, T\mathbf{X} = \mathbf{z}\right) \mathbb{P}\left(T\mathbf{X} = \mathbf{z} \,\middle|\, S\mathbf{P} = \widetilde{\triangle}\right).$$

The first term $\mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, T\mathbf{X} = \mathbf{z}\right)$ of the above summand would be evaluated by the method of the analysis of [5] as $\mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, S\mathbf{X} = (z, z)^T\right)$. We now consider the DES example of Section III and take $z = \delta_9$ and $z' = \delta_{\mathtt{B}}$. We show in Section III that

$$\begin{array}{rl} & \mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, T\mathbf{X} = \mathbf{z}\right) = 0, \\ \text{whereas} \quad & \mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, S\mathbf{X} = (z, z)^T\right) = p_1^2 > 0. \end{array}$$

The analysis of [5] would therefore give $\mathbf{z} = (\delta_9, \delta_9, \delta_{\mathtt{B}}, \delta_{\mathtt{B}})^T$ as the dominant term when evaluating the above summation for $\mathbb{P}\left(U\mathbf{C} = \widetilde{\nabla} \,\middle|\, T\mathbf{X} = \mathbf{z}\right)$, whereas in fact this term is zero in this summation. As with other analyses based on the boomerang idea, there is no *a priori* reason to assume the rectangle analysis works in the manner described by [5].

VI. An AES Boomerang

We now give another similar cautionary example about the boomerang analysis, basing this example on the Advanced Encryption Standard (AES) [7], [9]. We consider a block cipher based on two (complete) rounds of the AES. Thus E is the encryption under some fixed key of two rounds of the AES, and we suppose that E_0 is the initial round of this encryption and that E_1 the final round of this encryption.

The only nonlinear part of an AES round is the SubBytes phase, which consists of the application of an S-Box to each byte of the 16-byte state, where an S-Box is formally a function $S\colon \mathbb{Z}_2^8 \to \mathbb{Z}_2^8$. The nonlinear part of an S-Box is an "inversion" operation on bytes, given by $z \mapsto z^{2^8-2}$ in $\mathrm{GF}(2^8)$, and there exist many nonzero input byte differences α and output byte differences β such that the differential probability for the AES S-Box is 2^{-7} [9], [10]. One such pair of input and output differences for SubBytes is given by $\alpha = \mathtt{02}$ and $\beta = \mathtt{EE}$, so we have

$$\mathbb{P}\left(S(z + \mathtt{02}) + S(z) = \mathtt{EE}\right) = 2^{-7}.$$

Allowing for the effect of the ShiftRows and MixColumns operations, we can base a boomerang analysis on the differences:

$$\begin{array}{l} \triangle = \nabla^* = \mathtt{02000000\ 00000000\ 00000000\ 00000000}, \\ \triangle^* = \nabla = \mathtt{C7EEEE29\ 00000000\ 00000000\ 00000000}. \end{array}$$

This gives the following differential probabilities for the two parts of the block cipher:

$$\begin{array}{ll} E_0(Z) + E_0(Z + \triangle) = \triangle^* & \text{with probability } p_0 = 2^{-7}, \\ E_1(Z) + E_1(Z + \nabla^*) = \nabla & \text{with probability } p_1 = 2^{-7}. \end{array}$$

We now consider the effect of the right quartet restrictions on the possibilities for the intermediate values. A similar analysis to Section III shows that:

$$\begin{array}{rcrcl} X' & = & X + & \triangle^* & = X + \mathtt{C7EEEE29\ 00\ldots00}, \\ Y & = & X + & \nabla^* & = X + \mathtt{02000000\ 00\ldots00}, \\ Y' & = & X + & \triangle^* + \nabla^* & = X + \mathtt{C5EEEE29\ 00\ldots00}. \end{array}$$

If we let x denote the first byte of X, then for a right quartet we require that

$$S(x) + S(x + \mathtt{02}) = \mathtt{EE} \text{ and } S(x + \mathtt{C7}) + S(x + \mathtt{C5}) = \mathtt{EE}.$$

A search through all 2^8 possible byte values for x quickly shows that there is no byte value x which satisfies the two above equations.

We have therefore shown that it is not possible for a right quartet to exist in this boomerang analysis, even though the reasoning of Section 4 of [1] would give a lower bound for the probability of a right quartet of at least $p_0^2 p_1^2 = 2^{-28}$. Just like the DES boomerang of Section III, this AES boomerang *never* comes back.

VII. A High Probability DES Boomerang

We have given a DES boomerang and an AES boomerang (Sections III and VI) which cannot occur, that is they happen with probability zero. In both cases, this was demonstrated by giving a pair of S-Box equations which had no solution. Of course, if we had set up a different potential boomerang, that

is other difference values, we would have obtained other pairs of S-Box equations, which may well have had many solutions. In such a case, it is entirely possible that the boomerang probability may greatly exceed that given by [1].

We illustrate this point about boomerang probabilities with a striking contrast to the zero-probability non-returning DES boomerang of Section III. We simply make a minor modification of the boomerang differences for Section III. Thus we take $\nabla = \nabla^* = \triangle^* = \triangle = \delta_9$ rather than $\nabla = \nabla^* = \delta_{\mathtt{B}}$ and $\triangle^* = \triangle = \delta_9$ as for Section III. As for this Section III example, the statistical reasoning of Section 4 of [1] now asserts that the probability of a right quartet is $\left(\frac{1}{234}\right)^4$. The condition for a right quartet in this case is simply then given by

$$\begin{aligned} P' &= Q = Q' + \delta_9 = P + \delta_9, \\ X' &= Y = Y' + \delta_9 = X + \delta_9 \\ \text{and} \quad C' &= D = D' + \delta_9 = C + \delta_9. \end{aligned}$$

This right quartet is therefore simply the repeated use of a *right pair* [2], [3] in differential cryptanalysis. Thus in this case a right quartet occurs with the same probability as a right pair based on this characteristic, namely $\left(\frac{1}{234}\right)^2$. The true probability of this boomerang occurring is very much greater than the probability value for this boomerang occurring given by the statistical reasoning of [1].

VIII. Conditional Probability and the Boomerang Analysis

A boomerang analysis requires the use of conditional probability. The condition for a right quartet is a *Rank-3n* condition, as is illustrated by the matrix T (Section V) of rank $3n$, and we denote this event by R_3. However, the boomerang-type analysis of [1], [4], [5] instead uses an algebraically less onerous *Rank-2n* condition, as illustrated by the matrix U (Section V) of rank $2n$, and we denote this event by R_2. The justification for the application of a boomerang or a related analysis in the manner of [1] essentially asserts for any cryptographic event A under consideration that

$$\mathbb{P}(A|R_3) = \mathbb{P}(A|R_2).$$

There is simply no probabilistic justification for this assertion.

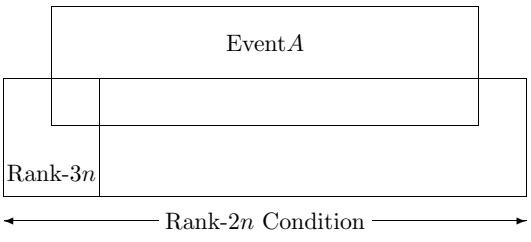

Fig. 2. Rank-$2n$ and Rank-$3n$ Conditions in the Boomerang Analysis.

The application of conditional probability to a boomerang-type analysis is illustrated by the Venn diagram of Figure 2. The boomerang-type analysis of [1], [4], [5] uses

$$\mathbb{P}(A|R_2) = \frac{\#\left(A \bigcap R_2\right)}{\#R_2},$$

whereas the correct condition for a boomerang-type analysis is

$$\mathbb{P}(A|R_3) = \frac{\#\left(A \bigcap R_3\right)}{\#R_3}.$$

There is no *probabilistic* reason why these two quantities are related in any way. We can illustrate this by using a fair dice roll with six outcomes $\{1, 2, 3, 4, 5, 6\}$ as an example. If the dice throw is at most 2, then the conditional probabilities that the dice roll is odd and that the dice roll is even are given by

$$\begin{aligned} &\mathbb{P}(\text{ Dice is Odd} \mid \text{Dice} \leq 2\ ) = \ \tfrac{1}{2} \\ \text{and} \quad &\mathbb{P}(\text{ Dice is Even} \mid \text{Dice} \leq 2\ ) = \ \tfrac{1}{2}\ . \end{aligned}$$

If we replace the condition that the dice throw is at most 2 with the less onerous condition that the dice throw is at most 3, we obtain the following different conditional probabilities that the dice roll is odd and the dice roll is even:

$$\begin{aligned} &\mathbb{P}(\text{ Dice is Odd} \mid \text{Dice} \leq 3\ ) = \ \tfrac{2}{3} \\ \text{and} \quad &\mathbb{P}(\text{ Dice is Even} \mid \text{Dice} \leq 3\ ) = \ \tfrac{1}{3}\ . \end{aligned}$$

This simple example shows the central importance of the conditioning event. Arbitrarily replacing one conditioning event by another conditioning event is a fundamental error in the application of conditional probability.

In the DES and AES boomerang examples which occur with zero probability (Sections III and VI), we have $A \bigcap R_3 = \emptyset$ even though $A \bigcap R_2 \neq \emptyset$, so

$$\begin{gathered} \frac{\#\left(A \bigcap R_2\right)}{\#R_2} > \frac{\#\left(A \bigcap R_3\right)}{\#R_3} = 0, \\ \text{that is } \mathbb{P}(A|R_2) > \mathbb{P}(A|R_3) = 0. \end{gathered}$$

By contrast, in the DES boomerang example of Section VII, the cryptographic event A is actually a subset of R_3, so we have

$$\begin{gathered} \frac{\#\left(A \bigcap R_2\right)}{\#R_2} = \frac{\#\left(A \bigcap R_3\right)}{\#R_2} < \frac{\#\left(A \bigcap R_3\right)}{\#R_3}, \\ \text{that is } \mathbb{P}(A|R_2) < \mathbb{P}(A|R_3). \end{gathered}$$

For a boomerang-type analysis to be correct, we require that

$$\mathbb{P}(A|R_2) = \mathbb{P}(A|R_3) = \frac{\#\left(A \bigcap R_2\right)}{\#R_2} = \frac{\#\left(A \bigcap R_3\right)}{\#R_3}.$$

Loosely speaking, we require that the event A occurs with the same frequency in the Rank-$3n$ subset as it does in the Rank-$2n$ subset. As stated above, there is no probabilistic reason for this to be the case, and as the examples of this paper demonstrate, there is no general cryptographic reason for this to be the case. A cryptographic boomerang-type analysis that merely swaps the Rank-$2n$ condition for the Rank-$3n$ condition cannot be regarded as having been substantiated.

IX. Comments on a Rectangle Analysis of the AES

An analysis of the AES [7] in a specific related key model is given in [11], and this analysis makes use of a number of different techniques based on the cryptographic boomerang. The correctness of the boomerang probabilities given by [1] is asserted by [11], and such values for boomerang probabilities are the foundations of the analysis of the AES given by [11]. As we have shown, such foundations are not necessarily sound.

We discuss the dubious nature of the AES analysis given by [11] by considering a critical technique used in this analysis termed the *Feistel switch*. A value for the probability that a Feistel switch occurs is given in [11] based on the usual boomerang reasoning of [1], that is based on a Rank-$2n$ condition rather than the correct Rank-$3n$ condition. Thus the value given by [11] for the probability that a Feistel switch occurs is not generally correct. This is illustrated by the DES boomerang example of Section III, which is actually a Feistel switch, with $\Delta_X = \gamma_9$, $\Delta_Y = 0$ and $\Delta_Z = \gamma_{\text{B}}$ in the notation of [11]. Thus it would be asserted by [11] that this DES example of a Feistel switch, which can never happen, occurs with nonzero probability.

Another technique used by [11] is termed the *S-box switch*, which essentially considers the cryptographic boomerang when $\nabla^* = \triangle^*$. However, whilst the Rank-$2n$ condition is used by [11] to give a probability value for the Feistel switch, the Rank-$3n$ condition is used by [11] to give a probability value for the S-box switch. This is problematic as the DES boomerang example of Section VII is essentially both an S-box switch and a Feistel switch, with $\Delta_X = \Delta_Z = \gamma_9$ and $\Delta_Y = 0$ in the notation of [11].

These examples show that the justifications for the probability values for various cryptographic boomerang-type events given by [11] are not really convincing. The data requirements for the related key analysis of the AES given by [11] cannot therefore be regarded as having been soundly demonstrated.

X. Conclusions

We have given counterexamples that clearly demonstrate that the justification for the boomerang analysis given by [1] is highly questionable. These counterexamples are based on the two most important block ciphers, the DES and the AES, so they are not just artificially contrived. Such counterexamples can also be adapted to show that the justifications for derived analyses, such as the amplified boomerang analysis [4] and the rectangle analysis [5], are also highly questionable. Furthermore, the claims given made by [11] for a related key analysis of the AES must be regarded as unsubstantiated.

The correct condition for a right quartet in a boomerang-type analysis is a Rank-$3n$ condition. The boomerang-type analysis replaces the correct right quartet Rank-$3n$ condition with an algebraically less onerous Rank-$2n$ condition. Whilst it is possible that, for a particular block cipher and a particular collection of differences, a probability conditional on the Rank-$3n$ event and a probability conditional on the Rank-$2n$ event are equal, there is no *a priori* probabilistic or cryptographic reason for these two conditional probabilities to be equal. The justification for the application of a boomerang or a related analysis in the manner of [1] to a particular block cipher and a particular collection of differences does clearly require the demonstration that the Rank-$3n$ and Rank-$2n$ conditions give the same probability.

We have shown that the usual probabilistic argument used to justify the so-called boomerang effect is unsound. A probability value for a boomerang-type analysis derived in the manner of [1], [4], [5] can be highly inaccurate and is at best an arbitrary guess for the true probability. In terms of the original motivation for the use of the word *boomerang* to describe this style of cryptographic analysis, the contribution of this paper can best be summarised as follows:

> *A cryptographic boomerang need not return from whence it came.*

Acknowledgment

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

References

[1] D. Wagner, "The Boomerang Attack," in *Fast Software Encryption, FSE '99*, ser. LNCS, L. Knudsen, Ed., vol. 1636. Springer–Verlag, 1999, pp. 156–170.

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

[3] ——, "Differential Cryptanalysis of the DES-like Cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3–72, 1993.

[4] J. Kelsey, T. Kohno, and B. Schneier, "Amplified Boomerang Attacks against Reduced-Round MARS and Serpent," in *Fast Software Encryption, FSE 2000*, ser. LNCS, B. Schneier, Ed., vol. 1978. Springer–Verlag, 2001, pp. 75–93.

[5] E. Biham, O. Dunkelman, and N. Keller, "The Rectangle Attack – Rectangling the Serpent," in *Advances in Cryptology – EUROCRYPT 2001*, ser. LNCS, B. Pfitzmann, Ed., vol. 2045. Springer–Verlag, 2001, pp. 340–357.

[6] National Bureau of Standards, "The Data Encryption Standard," Federal Information Processing Standards Publication (FIPS) 46, 1977.

[7] National Institute of Standards and Technology, "The Advanced Encryption Standard," Federal Information Processing Standards Publication (FIPS) 197, 2001.

[8] S. Murphy and F. Piper and M. Walker and P. Wild, "Maximum Likelihood Estimation for Block Cipher Keys," Royal Holloway (University of London)," *Technical Report RHUL-MA-2006-3*, 1994, http://www.ma.rhul.ac.uk/techreports.

[9] J. Daemen and V. Rijmen, *The Design of Rijndael*. Springer–Verlag, 2002.

[10] W.-A. Jackson and S. Murphy, "Projective Aspects of the AES Inversion," *Designs, Codes and Cryptography*, vol. 43, pp. 167–179, 2007.

[11] A. Biryukov and D. Khovratovich, "Related-key Cryptanalysis of the Full AES-192 and AES-256," in *Advances in Cryptology – ASIACRYPT 2009*, ser. LNCS, M. Matsui, Ed., vol. 5912. Springer–Verlag, 2009, pp. 1–18.

Biography. S. Murphy is a Professor of Mathematics at Royal Holloway, University of London. He has a B.A. and a Ph.D. in Mathematics.