RELATED KEY–RECTANGLE AND BOOMERANG COMBINED ATTACK ON MDA

B. Srinivasa Rao¹, P. Premchand²

¹Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India.
²Department of Computer Science Engineering, University College of Engineering, Osmania University, Hyderabad, India.

Abstract: In the present research work a combined cryptanalysis technique namely Related Key–Rectangle and Boomerang Combined Attack has been discussed and implemented on some message digest algorithms for their evaluation. The evaluated results of various rounds of the implemented algorithms are presented. The experimentally tested results show that the encryption modes of all the message digest algorithms are vulnerable to the related-key rectangle and boomerang combined attack. Thus the present work proposes an improved combined cryptanalytic attack.

Index Terms - Combined attacks, Cryptanalysis, Message Digest Algorithms, Related Key Cryptanalysis.

I. INTRODUCTION

The cryptanalytic tools play significant role in inferring the vulnerabilities and assessment of strength of cryptographic systems. The evaluation of cryptographic systems using cryptanalytic attack mechanisms prove the security of the cryptosystems against possible attacks in a more accurate and reliable way. Differential cryptanalysis, linear cryptanalysis and related key cryptanalysis are the widely used cryptanalytic tools to evaluate the security of the cryptographic algorithms. Differential cryptanalysis introduced by Biham and Shamir is one of the most powerful chosen plaintext attacks in symmetric key cryptography. Linear cryptanalysis is an efficient cryptographic tool for block ciphers and stream ciphers. Related key cryptanalysis is applicable to ciphers with different but related unknown keys. This attack is based on the key scheduling algorithm and encryption/decryption algorithm. Various variations of these attacks have been proposed to meet the different contexts of the emerging cryptosystems. The variations of differential cryptanalysis are truncated differential cryptanalysis, higher order differential cryptanalysis, square cryptanalysis, impossible differential cryptanalysis, boomerang cryptanalysis and rectangle cryptanalysis. Multiple linear cryptanalysis, nonlinear cryptanalysis and bilinear cryptanalysis are the variations of linear cryptanalysis. For effective and efficient cryptanalytic combined attacks are designed from the above cryptanalytic tools and their variations and applied for various security systems to study the possibility their vulnerability to the attacks. Continuous research is being done in the direction of designing and developing combined attacks and their implementation and the present research also makes an attempt to implement a new combined attack on some crypto systems like Message Authentication Code algorithm. Message digest (MD) algorithms are important type of cryptographic algorithms and are extensively used in applications such as digital signature, data authentication, e-cash etc. The important MD algorithms are MD4, MD5, HAVAL, SHA-0 and SHA-1. Earlier several attempts have been made for cryptanalysis of MD algorithms using techniques such as collision attacks, neutral-bit, message modification etc. Differential cryptanalysis and their variations were also implemented to investigate the non-randomness of the MD functions. In order to have an improved attack over the earlier ones, in our present research work, we propose an improved attack by introducing related-key rectangle and boomerang combined cryptanalytic attack for evaluation of the security of various message digest algorithms like MD4, MD5, HAVAL, SHA-0 and SHA-1. Based upon the previously existing techniques four types of related-key rectangle and boomerang distinguishers are designed and implemented for the above mentioned message digest algorithms. The evaluated results of various rounds of the implemented algorithms are presented.

II. THE RELATED-KEY RECTANGLE AND BOOMERANG ATTACKS

In this section, based upon the earlier work proposed by J. Kim et al. (2005) we introduce the related-key rectangle and boomerang attacks. In these attacks, there exist three types of related-key rectangle and boomerang distinguishers according to the usage of related-key differential and the number of related keys. The first type of distinguisher is applicable when related-key differential are used in the first sub-cipher, and regular differential (or related-key differential with the same key deference as those used in the first sub-cipher) in the second sub-cipher. The second type uses related-key deferential in the second sub-cipher and regular deferential for the first sub-cipher. The third type uses related-key deferential in both sub-ciphers. The first and second types of distinguishers use two related keys, but they use different methods for selecting plaintexts to work with. On the other hand, the third type of distinguisher uses four related keys. We call these three types of distinguisher related-key rectangle and boomerang distinguishers of TYPE 1, TYPE 2 and TYPE 3, respectively. We first introduce the three types of related-key rectangle distinguishers and then of related-key boomerang distinguishers. The related-key rectangle distinguishers of TYPE 1, TYPE 2 and TYPE 3 work as follows:

1. Choose two random n-bit plaintexts P and P’ and compute two other plaintexts P” = P ⊕ α and P’” = P’ ⊕ α for a constant α.
2. With a chosen plaintext attack scenario, obtain the corresponding cipher-texts C = EK (P), C’ = EK* (P’), C” = EK’ (P) and C’” = EK*” (P’”), where K” = K ⊕ ΔK, K = K ⊕ ΔK, K” = K ⊕ ΔK ⊕ ΔK (i.e., K ⊕ K = K ⊕ K” = ΔK and K ⊕ K = K” ⊕ K” = ΔK) and ΔK, ΔK are key deference chosen by the cryptanalyst.
3. Check if C ⊕ C” = C’ ⊕ C’” = δ or C ⊕ C” = C’ ⊕ C’” = δ.
As stated, the related-key rectangle distinguisher checks if the two pairs chosen from the ciphertext quarter have the same difference 8. If this difference δ holds with a higher probability than for a random cipher, then the related-key rectangle distinguisher can be applied eectively to the underlying cipher. In the above process the deference among the three types of differentiators is on the condition of the key difference ΔK and AK.

Namely, in TYPE 1 AK 0 and AK 0 (or ΔK 0), in TYPE 2 ΔK 0 and ΔK 0 and in TYPE 3 ΔK 0, ΔK 0 and ΔK 0. If the plaintext quartet (P; P; P; P) satisfies the last δ test, we call such a quartet a right quartet.

The related-key rectangle distinguishers can be formed by building quartets of plaintexts (P; P; P; P) that satisfy the following four differentials.

Differential Condition 1: P ⊕ P ⊕ P = α
Differential Condition 2: I(X) = I(X) (for some β)
Differential Condition 3: I(X) = γ (or I(X) = γ) (for some γ)
Differential Condition 4: C⊙C = C⊙C = δ (or C⊙C = C⊙C = δ)

where I = E′(P), I = E′(P), I = E′(P), and I = E′(P). In these four differential conditions, α and δ represent specific differences, and β and γ represent arbitrary differences. Note that the differential conditions 2 and 3 imply I(X) = γ (or I(X) = γ) with probability 1. If these four differential conditions are satisfied, such a quartet (P; P; P; P) is a right quartet.

2.1 Related-Key Rectangle Distinguisher of TYPE 1

Assume that we have m plaintext pairs with difference α, where one plaintext of each pair is encrypted with the key K and the other plaintext with the key K′. Then we have about mp pairs satisfying the related-key differential α → β for E′ under the key difference ΔK.

The mp pairs generate about (mp)2/2 quartets satisfying conditions 1 and 2. Assuming that the intermediate encryption values are uniformly distributed over all possible values, we get I(X) = γ with a probability of 2 and I(X) = γ → δ with a probability of 2. If we take into account the difference of the I, I, pair, the regular differential γ → δ with probability q for E′ is used twice in this distinguisher. On the other hand, if we take into account the difference of the I, I, pair, the related-key differential γ → δ with probability q for E′ is used twice in this distinguisher.

On the other hand, the expected number of right quartets for a random cipher is about m 2 2 since there are (m/2) 2 possible quartets and each of the pairs (C, C) and (C, C) (or the pairs (C, C) and (C, C)) satisfies the δ difference with probability 2. Therefore, if p α 2 2 or p 2 q 2 2 must hold for the related-key rectangle distinguisher to work. Note that our estimated expectations are approximate values since the actual values of the expectations depend on the values of the chosen plaintexts and the used differential probabilities are average ones over the text key.

2.2 Related-Key Rectangle Distinguisher of TYPE 2

If we have m, pairs (P; P), and m, pairs (P; P) with difference α, where P and P are all encrypted under the key K and P and P are all encrypted under the key K′, then we have about m, pairs together with m, pairs satisfying the regular differential α → β for E′. Similarly, we get I(X) = γ with a probability of 2 and I(X) = γ with a probability of 2. Since the probability that both pairs (I, I) (or (I, I′) and (I, I′)) are right pairs with the related key differential γ → δ for E′ is q (here, q = PrXK[E′(X) ⊕ E′(X)] (X ⊕ γ) = δ)], the expected number of right quartets is about m, (m, p). 2 2 2 m, 2 2 1 m, 2 2 1 (p q) 2. Since the expected number of right quartets for a random cipher is about m 2 2 2 1, 2 m, 2 2 1, then we have about m, pairs between E and a random cipher. Therefore, if p > q 2 2 or p 2 q 2 2 must hold for the related-key rectangle distinguisher to work. Note that our estimated expectations are approximate values since the actual values of the expectations depend on the values of the chosen plaintexts and the used differential probabilities are average ones over the text key.

2.3 Related-Key Rectangle Distinguisher of TYPE 3

In order to optimize the ratio of the expected number of right quartets between E and a random cipher, we should only consider the maximum of q and q in the related-key rectangle distinguisher of TYPE 3, where q = PrXK[E′(X) ⊕ E′(X)] (X ⊕ γ) = δ)] 1/2 and q = PrXK[E′(X) ⊕ E′(X)] (X ⊕ γ) = δ)] 1/2. In our analysis, we assume q > q. To begin with, we also assume that we have m, pairs of (P; P) and m, pairs of (P; P) with difference α, where P, P, and P are encrypted with the keys K, K′, K, and K′, respectively. Then about m, p and m, p pairs will satisfy the related-key differential α → β for E′ under the key difference ΔK. Thus, we have about m, m, p pairs satisfying the differential conditions 1 and 2. Moreover, we get I(X) = γ with probability 2. These assumptions enable us to obtain about m, m, 2 2 p, 2 2 m, m, 2 2 (p q) 2. For a random cipher the expected number of right quartets is about m 2 2 1. Thus, p q > 2 2 must hold for the related-key rectangle distinguisher to work.

2.4 Related-Key Boomerang Distinguishing

In order to get at least one right quartet in the related-key rectangle distinguishers, we need at least 2w 2 plaintext queries. However, under an adaptive chosen plaintext and ciphertext attack scenario we can make a related-key boomerang distinguisher which can remove the factor 2w 2 in the data requirement. As a compensation of a smaller data requirement, this attack works only in a stronger attack model; it requires access to both the encryption box and the decryption box. The related-key boomerang distinguishers based on two or four related keys work as follows.

Choose two n-bit plaintexts P and P such that P ⊕ P = α and obtain the corresponding ciphertexts C = EK(P) and C = EK(P), where K K = ΔK.

Compute other two ciphertexts C = C ⊕ δ and C = C ⊕ δ, and obtain the corresponding plaintexts P = EK(C) and P = EK(C), where K K = ΔK and K K = K K = K K = ΔK.

Check if P ⊕ P = α. Similarly, we can classify the three types of differentiators by the condition of the key differences ΔK and ΔK. Note that the difference between the related-key rectangle and boomerang distinguishers of the same TYPE is on the encryption and decryption process.
for the plaintexts (P; P') and the ciphertexts (C'; C'). In a similar way, we can analyze the three types of the related-key boomerang distinguishers. Let us consider the related-key boomerang distinguisher of TYPE 3. The probability that I(G1) = β is p' (in the encryption direction) and the probability that I(G2) = γ is q' (in the decryption direction). Therefore, for any β and γ, I(G1) = β and I(G2) = γ (as in these cases I(G1) and I(G2) hold with probability p', q'). Since the probability of the related-key differential β to a for α (E^i)^j under the related key difference ΔK is p', the probability that P(β → α) = \sum q_{p'}^2 \cdot q_{p'}^2 > \cdot q_{p'}^2. Therefore, if we have m chosen plaintext pairs (P; P') with difference α and we have another m adaptively chosen ciphertext pairs (C; C') such that C = C°°° and C' = C°°°, then about m.p^2.q^2 quartets satisfy the α test. Since, for a random cipher α test holds with probability 2^-a, \( \sum q_{p'}^2 > \cdot q_{p'}^2 \) boomerang distinguisher.

III. HASH FUNCTIONS

Hash functions are an important type of cryptographic algorithms; they are widely used in cryptographic applications such as digital signature, data authentication and e-cash. Hash functions are at work in the millions of transactions that take place on the internet every day. The purpose of the use of hash functions in many cryptographic protocols is to ensure their security as well as improve their efficiency. The most widely used hash functions are cryptographic hash functions such as MD5 [112] and SHA-1 [41], which follow the design principle of MD4. Hash functions are message digest algorithms which compress any arbitrary bit length message into a hash value with a small and fixed bit-length. The cryptographic hash functions such as MD4, MD5, HAVAL, SHA-0 and SHA-1 are performed based on the well-known Davies-Meyer construction, which is described as follows. Before the hash function is applied to a message M of arbitrary bit length, it is padded to a multiple of t-bit and divided into n t-bit sub-messages M1[M2][...][Mt-1], where t is specified. Then the 1-bit hash value F is computed as follows: F^i = IV; I^i+1 = \text{com}(I^i; M^i) = E(I^i; M^i) + F^i for 0 < i < n. Where IV is a fixed 1-bit initial value, \text{com} is a compression function and E is an iterative step function. In MD4, MD5, HAVAL, SHA-0 and SHA-1, the function E is composed of 3; 4 or 5 passes and in each pass there are 16, 20 or 32 rounds that use only simple basic operations and Boolean functions on 32-bit words. The 1-bit input I^i is loaded into I^i/32 32-bit registers denoted (A^i; B^i; ... ; X^i). The I^i/32 registers are updated through a number of rounds. In each pass, a fixed Boolean function f and 32-bit constants Cst are used.

IV. IMPLEMENTATION OF RELATED-KEY, RECTANGULAR BOOMERANG ATTACK

MD5 is a strengthened version of MD4, which increases the number of passes from 3 to 4 (i.e., it extends the number of rounds from 48 to 64) and uses the round function. In MD5 four types of Boolean functions f are used; two of them are the same as the Boolean functions of MD4 used in rounds 1-15 and 32-47.

\[
fr(Br; Cr; Dr) = \begin{cases} 
(Br\&Cr)\oplus(\neg Br\&Dr) & \text{if } 0 \leq r \leq 15 \\
(Br\&Dr)\oplus(Cr\&\neg Dr) & \text{if } 16 \leq r \leq 31 \\
Br \oplus Cr \oplus Dr & \text{if } 32 \leq r \leq 47 \\
Cr \oplus (Br\neg\&Dr) & \text{if } 48 \leq r \leq 63 
\end{cases}
\]

The rotation amount sr is specified as follows:

\[
sr = \{ \\
7; 12; 17; 22; 12; 7; 17; 22; 7; 12; 17; 22; 7; 12; 17; 22 \\
5; 9; 14; 20; 5; 9; 14; 20; 5; 9; 14; 20 \\
4; 11; 16; 23; 4; 11; 16; 23; 4; 11; 16; 23 \\
6; 10; 15; 21; 6; 10; 15; 21; 6; 10; 15; 21 
\}
\]

MD5 uses the following message expansion algorithm for a 512-bit message

\[
M = X0||X1||...; ||X15
\]

Xr = \{ \\
X0; X1; X2; X3; X4; X5; X6; X7; X8; X9; X10; X11; X12; X13; X14; X15 \\
X1; X6; X11; X0; X5; X10; X15; X4; X9; X14; X3; X8; X13; X2; X7; X12 \\
X5; X8; X11; X14; X1; X4; X7; X10; X13; X0; X3; X6; X9; X12; X15; X2 \\
X0; X7; X14; X5; X12; X3; X10; X1; X8; X15; X6; X13; X4; X11; X2; X9 
\}

In the MD5 attacks, we first find consecutive two related-key differentials with high probabilities which are independent of each other, and then we estimate the probability Pr[BOO k] on the basis of those differentials by a series of simulations, where k is the number of source keys (k is equal to 2 or 4). The related-key boomerang attacks on MD5 and HAVAL are slightly different from those of MD4. The boomerang attack works by finding not only a chosen plaintext pair but also an adaptively chosen ciphertext pair that satisfy a boomerang distinguisher. For MD5 once we obtain a ciphertext pair by asking for the encryption of a chosen plaintext pair, we know whether or not the adaptively chosen ciphertexts can be a boomerang candidate. Assume that the ciphertext pair obtained by asking for the encryption of a chosen plaintext pair is (C; C') and (a0; c0; d0) of C or (a0; c0; d0) of C' is in f(0; 0; 0); (0; 1; 0); (1; 0; 1); (1; 1; 1)l. Then the adaptively chosen ciphertext pair (C \oplus z; C' \oplus z) cannot satisfy our boomerang distinguisher, where = (e2; e3; e2; e3). That is, in this case \( e^A \) cannot be of the form \( e_3 \) since the difference induced by the Boolean function of the last round is 0 for \( (C \oplus z; C' \oplus z) \). This is why the required number of queries for the decryption process is smaller than that for the encryption process. During our simulations, we have observed that the simulation results correspond to our estimation of success rate. As an example of our simulations, we give in Tabl-1 a related-key quartet, a chosen plaintext pair and an adaptively chosen ciphertext pair of MD5 obtained by the boomerang distinguisher. The differential rounds 0-32 for MD5 is shown in Table-2.
Table 1: Boomerang Distinguishers of MD5 (Four Related Keys)

<table>
<thead>
<tr>
<th>Round (i)</th>
<th>A'</th>
<th>B'</th>
<th>C'</th>
<th>D'</th>
<th>K'</th>
<th>Prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>0</td>
<td>i/1</td>
</tr>
<tr>
<td>2</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>29</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>i/1</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td>e8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>i/2</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td>e8</td>
<td>e8</td>
<td>0</td>
<td></td>
<td>i/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>e11;31</td>
<td>e31</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>i/1</td>
</tr>
<tr>
<td>33</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>34</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>1</td>
</tr>
<tr>
<td>35</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>61</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>i/1</td>
</tr>
<tr>
<td>62</td>
<td>0</td>
<td>e9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>i/2</td>
</tr>
<tr>
<td>63</td>
<td>0</td>
<td>e9</td>
<td>e9</td>
<td>0</td>
<td></td>
<td>i/2</td>
</tr>
<tr>
<td>64</td>
<td>0</td>
<td>e9</td>
<td>e9</td>
<td>e9</td>
<td></td>
<td>i/4</td>
</tr>
</tbody>
</table>

BOO-4: (0 ; 30), (63 ; 31), (30 ; 2) \(P_{[BOO-4]} \approx 2^{-13.8}\)

BOO-W-4: Fixed \(K^{0;1;2;9;11} ; (2 ; 30), (60 ; 31), (30 ; 2)\) \(P_{[BOO-W-4]} \approx 2^{-6}\)

Table 2: Differential for Rounds 0-32 of MD5

<table>
<thead>
<tr>
<th>Round (i)</th>
<th>A'</th>
<th>B'</th>
<th>C'</th>
<th>D'</th>
<th>cmr</th>
<th>Prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e24</td>
<td>i/1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>e19</td>
<td>i/2</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>i/2</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>0</td>
<td>i/2</td>
</tr>
<tr>
<td>12</td>
<td>e31</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e31</td>
<td>i</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>e19</td>
<td>i/2</td>
</tr>
<tr>
<td>25</td>
<td>0</td>
<td>e24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>i/2</td>
</tr>
<tr>
<td>26</td>
<td>0</td>
<td>e24</td>
<td>e24</td>
<td>0</td>
<td>0</td>
<td>i/3</td>
</tr>
<tr>
<td>27</td>
<td>0</td>
<td>e6;24</td>
<td>e24</td>
<td>e24</td>
<td>e24</td>
<td>i/5</td>
</tr>
<tr>
<td>28</td>
<td>e24</td>
<td>e6;24</td>
<td>e6;24</td>
<td>e24</td>
<td>0</td>
<td>i/6</td>
</tr>
<tr>
<td>29</td>
<td>e24</td>
<td>e6;11;24</td>
<td>e6;24</td>
<td>e6;24</td>
<td>0</td>
<td>i/7</td>
</tr>
<tr>
<td>30</td>
<td>e6;24</td>
<td>e6;11;24</td>
<td>e6;11;24</td>
<td>e6;24</td>
<td>0</td>
<td>i/9</td>
</tr>
<tr>
<td>31</td>
<td>e6;24</td>
<td>e6;11;24</td>
<td>e6;11;24</td>
<td>e6;11;24</td>
<td>e31</td>
<td>i/9</td>
</tr>
</tbody>
</table>
V. CONCLUSION

In the present work we have applied the related-key boomerang attack to MD5. The MD5 used in encryption modes is vulnerable to the related-key boomerang attack and are very much close to the earlier simulation by Kim et al. However, a more detailed study and simulation is required not only on MD5 but also other systems like HAVAL and MD4 etc. against the present combined attack. The comparative studies can give a better picture of the general vulnerability of the crypto systems for combined attacks.

VI. ACKNOWLEDGEMENTS

B. Srinivasa Rao is very much thankful to Dr. L. Pratap Reddy, Professor, Department of ECE, JNTUH, Hyderabad, for his valuable suggestions. Also thankful to the Management of GRIET for their encouragement and cooperation for pursuing his Ph.D. work.

REFERENCES
