RELATED KEY–RECTANGLE AND BOOMERANG COMBINED ATTACK ON MDA

B. Srinivasa Rao[1], P. Premchand[2]
[1]Professor, [2]Professor
[1]Department of Computer Science and Engineering Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India.
[2]Department 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 cryptanalysis 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 efficient 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 etal (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 deferential and the number of related keys. The first type of distinguisher is applicable when related-key deferential are used in the first sub-cipher, and regular deferential (or related-key deferential 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 deferent 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 $P^* = P \oplus \alpha$ and $P'^* = P' \oplus \alpha$ for a constant α.
2.With a chosen plaintext attack scenario, obtain the corresponding cipher-texts $C = E_K(P)$, $C^* = E_K^*(P^*)$, $C' = E_K'(P')$ and $C'^* = E_K'^*(P'^*)$, where $K^* = K \oplus \Delta K$, $K' = K \oplus \Delta K'$, $K'^* = K \oplus \Delta K \oplus \Delta K'$ (i.e., $K \oplus K^* = K' \oplus K'^* = \Delta K$ and $K \oplus K' = K^* \oplus K'^* = \Delta K'$) and $\Delta K, \Delta K'$ are key deference chosen by the cryptanalyst.
3. Check if $C \oplus C' = C^* \oplus C'^* = \delta$ or $C \oplus C'^* = C^* \oplus C' = \delta$.

As stated, the related-key rectangle distinguisher checks if the two pairs chosen from the ciphertext quartet have the same difference δ. If this difference δ holds with a higher probability than for a random cipher, then the related-key rectangle distinguisher can be applied electively to the underlying cipher. In the above process the deference among the three types of distinguishers is on the condition of the key difference ΔK and ΔK'. Namely, in TYPE 1 $\Delta K \neq 0$ and $\Delta K' = 0$ (or $\Delta K = \Delta K' \neq 0$), in TYPE 2 $\Delta K = 0$ and $\Delta K' \neq 0$ and in TYPE 3 $\Delta K \neq 0$, $\Delta K' \neq 0$ and $\Delta K \neq \Delta K'$. 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 differential conditions.

Differential Condition 1: $P \oplus P^* = P' \oplus P'^* = \alpha$

Differential Condition 2: $I \oplus I^* = I' \oplus I'^* = \beta$ (for some β)

Differential Condition 3: $I \oplus I' = \gamma$ (or $I \oplus I'^* = \gamma$) (for some γ)

Differential Condition 4: $C \oplus C' = C^* \oplus C'^* = \delta$ (or $C \oplus C'^* = C^* \oplus C' = \delta$)

where $I = E^0_k(P)$, $I^* = E^0_{k^*}(P^*)$, $I' = E^0_{k'}(P')$ and $I'^* = E^0_{k'^*}(P'^*)$. 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 $I^* \oplus I'^* = \gamma$ (or $I^* \oplus I' = \gamma$) 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 $\alpha \rightarrow \beta$ for E^0 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 $I \oplus I' = \gamma$ with a probability of 2^{-n} and $I \oplus I'^* = \gamma \rightarrow \delta$ with a probability of 2^{-n}. If we take into account the difference of the I, I' pair, the regular differential $\gamma \rightarrow \delta$ with probability q for E^1 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 $\gamma \rightarrow \delta$ with probability q^* for $E^1$is used twice in this distinguisher. On the other hand, the expected number of right quartets for a random cipher is about $m^2.2^{-2n}$, 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^{-n}. Therefore, if $p^*.(\frac{1}{2}.(q^2 + q^{*2}))^{1/2} > 2^{-n/2}$ and m is sufficiently large, we can distinguish between E and a random cipher. In this distinguisher, we can use either regular differentials $\gamma \rightarrow \delta$ (related to the probability q) or related-key differentials $\gamma \rightarrow \delta$ (related to the probability q^*). By using both of them, we increase the probability for a random cipher to succeed. However, if we take only the maximum of q and q^*, then the ratio of the expected number of right quartets between E and a random cipher is optimal. In this case, the expected number of right quartets for the E cipher is about $m^2.2^{-1}.2^{-n}.(p^*.q)^2$ or $m^2.2^{-1}.2^{-n}.(p^*.q^*)^2$. On the other hand, the expected number of right quartets for a random cipher is about $m^2.2^{-1}.2^{-2n}$. Thus, $p^*.q > 2^{-n/2}$ or $p^*.q^* > 2^{-n/2}$ 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 and key.

2.2 Related-Key Rectangle Distinguisher of TYPE 2

If we have m_1 pairs (P; P*) and m_2 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 $m_1.p$ pairs together with $m_2.p$ pairs satisfying the regular differential $\alpha \rightarrow \beta$ for E^0. Similarly, we get $I \oplus I' = \gamma$ with a probability of 2^{-n} and $I \oplus I'^* = \gamma$ with a probability of 2^{-n}. Since the probability that both pairs (I; I') and (I*; I'*) (or both pairs (I; I'*) and (I*; I')) are right pairs with respect to the related key differential $\gamma \rightarrow \delta$ for E^1 is q^{*2} (here, $q^* = Pr_{X,K}[E_K^1(X) \oplus E_{K^1 \oplus \Delta K'}(X \oplus \gamma) = \delta]$), the expected number of right quartets is about $\sum(m_1.p).(m_2.p).2^{-n}.2.q^{*2} = m_1.m_2.2^{-n+1}.(p.q^*)^2$. Since the expected number of right quartets for a random cipher is about $m_1.m_2.2^{-2n+1}$, we can distinguish between E and a random cipher if $p.q^* > 2^{-n/2}$ and m_1, m_2 are sufficiently large.

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, $q^* = Pr_{X,K}[E_K^1(X) \oplus E_{K^1 \oplus \Delta K}(X \oplus \gamma) = \delta])^2)^{1/2}$, and $q'^* = Pr_{X,K}[E_K^1(X) \oplus E_{K^1 \oplus \Delta K \oplus \Delta K'}(X \oplus \gamma) = \delta])^2)^{1/2}$. In our analysis, we assume $q^* > q'^*$. To begin with, we also assume that we have m_1 pairs of (P; P*) and m_2 pairs of (P'; P'*) with difference α, where P; P*; P' and P'* are encrypted with the keys K, K*, K'and K'*, respectively. Then about $m_1.p$ and $m_2.p^{*2}$ pairs will satisfy the related-key differential $\alpha \rightarrow \beta$ for E^0 under the key difference ΔK. Thus, we have about $m_1.m_2.p^{*2}$ quartets satisfying the differential conditions 1 and 2. Moreover, we get $I \oplus I' = \gamma$ with probability 2^{-n}. These assumptions enable us to obtain about $m_1.m_2.2^{-n}.p^{*2}$ quartets satisfying the differential conditions 1, 2 and 3. As stated above, the differential conditions 2 and 3 allow us to get $I^* \oplus I'^* = \gamma$ with probability 1, and each of the pairs (I; I') and (I*; I'*) satisfies the related-key differential $\gamma \rightarrow \delta$ for E^1 with probability q^*. Therefore, the expected number of right quartets is about $\sum m_1.m_2.2^{-n}.p^{*2}.q^{*2} = m_1.m_2.2^{-n}.(p^*)^2.(q^*)^2$ For a random cipher the expected number of right quartets is about $m_1.m_2.2^{-2n}$. Thus, $p^*.q^* > 2^{-n/2}$ must hold for the related-key rectangle distinguisher to work.

2.4 Related-Key Boomerang Distinguishers

In order to get at least one right quartet in the related-key rectangle distinguishers, we need at least $2^{n/2}$ 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 $2^{n/2}$ 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 $P \oplus P' = \alpha$ and obtain the corresponding ciphertexts $C = E_K(P)$ and $C' = E_K^*(P^*)$, where $K \oplus K^* = \Delta K$.

Compute other two ciphertexts' $= C \oplus \delta$ and $C'^* = C^* \oplus \delta$, and obtain the corresponding plaintexts $P' = E_K^{-1}(C')$ and $P'^* = E_K^{-1,*}(C'^*)$, where $K' \oplus K'^* = \Delta K$ and $K \oplus K' = K^* \oplus K'^* = \Delta K'$.

Check if $P' \oplus P'^* = \alpha$. Similarly, we can classify the three types of distinguishers 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 $I \oplus I^* = \beta$ is p^* (in the encryption direction) and the probability that $I \oplus I' = I^* \oplus I'^* = \gamma$ is q^{*2} (in the decryption direction). Therefore, for any β and γ, $I \oplus I' = \beta$ and $I \oplus I' = I^* \oplus I'^* = \gamma$ (as in these cases $I' \oplus I'^* = \beta$) hold with probability $p^*.\ q^{*2}$. Since the probability of the related-key differential $\beta \rightarrow$ for α $(E^0)^{-1}$ under the related key difference ΔK is p^*, the probability that $P' \oplus P'^* = \alpha$ is $\sum p^{*2} \cdot q^{*2} = \langle p^{*2} \rangle . \langle q^{*2} \rangle$. 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 $C' = C^* \oplus \delta$ and $C'^* = C^* \oplus \delta$, then about $m.p^{*2}.q^{*2}$ quartets satisfy the α test. Since, for a random cipher α test holds with probability 2^{-n}, $\langle p^* \rangle \cdot \langle q^* \rangle > 2^{-n/2}$ boomerang distinguisher works.

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 $M^0||M^1||.... ||M^{n-1}$, where t is specified. Then the l-bit hash value I^n for the message M is computed as follows:$I^0 = IV$; $I^{i+1} = com(I^i; M^i) = E(I^i; M^i) + I^i$ for $0 < i < n$; Where IV is a fixed l-bit initial value, **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 l-bit input I^i is loaded into l/32 32-bit registers denoted (A^0; B^0; ....) and the t-bit message block is divided into t/32 32-bit words denoted (X^0; X^1; ... ; $X^{t/32}$). The l/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) ={ (Br&Cr)| (¬Br&Dr) if 0<= r <=15
(Br&Dr)|(Cr&¬Dr) if 16<= r <=31
Br ⊕Cr ⊕Dr if 32<= r <=47
Cr ⊕(Br|¬Dr) if 48 <= r <=63

The rotation amount sr is specified as follows:

sr = {
7; 12; 17; 22; 7; 12; 17; 22; 7; 12; 17; 22; 7; 12; 17; 22
5; 9; 14; 20; 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; 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 (a_{31}; c_{31}; d_{31}) of C or ($a^¤_{31}$; $c^¤_{31}$; $d^¤_{31}$) of C¤ is in f(0; 0; 0); (0; 1; 0); (1; 0; 1); (1; 1; 1)g. Then the adaptively chosen ciphertext pair (C ⊕±; C¤ ⊕±) cannot satisfy our boomerang distinguisher, where = (e_5; e_5; e_5; e_5). That is, in this case ¢A^{63} cannot be of the form e_5 since the difference induced by the Boolean function of the last round is 0 for (C⊕±; C¤⊕±). This is the reason 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)

Round (i)	A^i	B^i	C^i	D^i	K^i	Prob.
0	0	0	$e31$	0	0	1
1	0	0	0	$e31$	0	$_2{}_i$1
2	$e31$	0	0	0	$e31$	1
3	0	0	0	0	0	1
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
28	0	0	0	0	0	1
29	0	0	0	0	$e31$	$_2{}_i$1
30	0	e_8	0	0	0	$_2{}_i$2
31	0	e_8	e_8	0		$p^¤ = 2^{i4}$
31	$e11;31$	$e31$	$e31$	0	0	$_2{}_i$1
32	0	0	$e31$	$e31$	0	1
33	$e31$	0	0	$e31$	0	1
34	$e31$	0	0	0	$e31$	1
35	0	0	0	0	0	1
.	.	.	.	.	.	.
.	.	.	.	.	.	.
60	0	0	0	0	0	1
61	0	0	0	0	$e31$	$_2{}_i$1
62	0	e_9	0	0	0	$_2{}_i$2
63	0	e_9	e_9	0	0	$_2{}_i$2
64	0	e_9	e_9	e_9		$q^¤ = 2^{i6}$
BOO-4		$(0\ !\ 30)$, $(63\ !\ 31)^2$, $(30\ !\ 2)$				Pr[BOO-4] ¼ $2^{i11;6}$
BOO^W *-4*	Fixed $K^{0;1;2;9;11}$, $(2\ !\ 30)$, $(60\ !\ 31)^2$, $(30\ !\ 2)$					Pr[BOO-4] ¼ $2^{i0:6}$

Table-2 Differential for Rounds 0-32 of MD5

Round (i)	A^i	B^i	C^i	D^i	¢m^i	Prob.
0	0	0	0	0	0	1
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
7	0	0	0	0	0	1
8	0	0	0	0	$e24$	$_2{}_i$1
9	0	$e31$	0	0	$e19$	$_2{}_i$2
10	0	0	$e31$	0	0	$_2{}_i$1
11	0	0	0	$e31$	0	$_2{}_i$1
12	$e31$	0	0	0	$e31$	1
13	0	0	0	0	0	1
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
23	0	0	0	0	0	1
24	0	0	0	0	$e19$	$_2{}_i$2
25	0	$e24$	0	0	0	$_2{}_i$2
26	0	$e24$	$e24$	0	0	$_2{}_i$3
27	0	$e6;24$	$e24$	$e24$	$e24$	$_2{}_i$5
28	$e24$	$e6;24$	$e6;24$	$e24$	0	$_2{}_i$6
29	$e24$	$e6;11;24$	$e6;24$	$e6;24$	0	$_2{}_i$7
30	$e6;24$	$e6;11;24$	$e6;11;24$	$e6;24$	0	$_2{}_i$9
31	$e6;24$	$e6;11;24$	$e6;11;24$	$e6;11;24$	$e31$	$_2{}_i$9

32	*e*6;11;24	*e*6;11;19;24	*e*6;11;24	*e*6;11;24	0	¿8
33	*e*6;11;24	*e*6;11;23	*e*6;11;19;24	*e*6;11;24		
0-32	¿56, ¿47:6					

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

[1] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Advances in Cryptology { Proceedings of CRYPTO 1990, LNCS 537, pp 2-21, Springer-Verlag, 1990.
[2] L.R. Knudsen, Truncated and Higher Order Differential, Proceedings of FSE 1994, LNCS 1008, pp. 196-211, Springer-Verlag, 1995.
[3] J. Daemen, L.R. Knudsen and V. Rijmen, The Block Cipher Square, Proceedings of FSE 1997, LNCS 1267, pp. 149-165, Springer-Verlag, 1997.
[4] S.K. Langford and M.E. Hellman, Differential-Linear Cryptanalysis, Advances in Cryptology {Proceedings of CRYPTO 1994, LNCS 839, pp. 17-25, Springer-Verlag, 1994.
[5] E. Biham, A. Biryukov and A. Shamir, Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differential, Journal of Cryptology, Vol. 18, No. 4, pp. 291-311, 2005.
[6] D. Wagner, the Boomerang Attack, Proceedings of FSE 1999, LNCS 1636, pp156-170, Springer-Verlag, 1999.
[7] E. Biham, O. Dunkelman and N. Keller, The Rectangle Attack - Rectangling the Serpent, Advances in Cryptology { Proceedings of EUROCRYPT 2001, LNCS 2045, pp. 340-357, Springer-Verlag, 2001.
[8] M. Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology Proceedings of EUROCRYPT 1993, LNCS 765, pp. 386-397, Springer-Verlag, 1994.
[9] B.S. Kaliski Jr. and M.J.B. Robshaw, Linear Cryptanalysis Using Multiple Approximations, Advances in Cryptology {Proceedings of CRYPTO 1994, LNCS 839, pp. 26-39, Springer-Verlag, 1994.
[10] L.R. Knudsen and M.J.B. Robshaw, Non-Linear Approximations in Linear Cryptanalysis, Advances in Cryptology {Proceedings of EUROCRYPT 1996, LNCS 1070, pp. 224-236, Springer-Verlag, 1996.
[11] L.R. Knudsen and J.E. Mathiassen, A Chosen-Plaintext Linear Attack on DES, Proceedings of FSE 2000, LNCS 1978, pp. 262-272, Springer-Verlag, 2001.
[12] N.T. Courtois, Feistel Schemes and Bi-Linear Cryptanalysis, Advances in Cryptology {Proceedings of CRYPTO 2004, LNCS 3152, pp. 23-40, Springer-Verlag, 2004.
[13] L.R. Knudsen, Cryptanalysis of LOKI91, Advances in Cryptology { Pro-ceedings of AUSCRYPT 1992, LNCS 718, pp. 196-208, Springer-Verlag, 1993.
[14] E. Biham, New Types of Cryptanalytic Attacks Using Related Keys, Journal of Crytology, Vol. 7, No. 4, pp. 229-246, 1994.
[15] J. Kelsey, B. Schneier and D. Wagner, Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES, Advances in Cryptology { Proceed-ings of CRYPTO 1996, LNCS 1109, pp. 237-251, Springer-Verlag, 1996.
[16] R. C.-W. Phan and H. Handschuh, On Related-Key and Collision Attacks: The Case for the IBM 4758 Cryptoprocessor, Proceedings of ISC 2004, LNCS 3225, pp. 111-122, Springer-Verlag, 2004.
[18] FIPS 180-1: Secure Hash Standard, Federal Information Processing Stan-dards Publication, NIST, April 1995.
[19] R.L. Rivest, The MD5 Message Digest Algorithm, Request for Comments (RFC 1320), Internet Activities Board, Internet Privacy Task Force, 1992.
[20]ISO/IEC 9797, Data Cryptographic Techniques { Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm, 1989.
[21] K. Kurosawa and T. Iwata, TMAC: Two-Key CBC MAC, Topics in Cryp-tology { Proceedings of CT-RSA 2003, LNCS 2612, pp. 33-49, Springer-Verlag, 2003.
[22] E. Jaulmes, A. Joux and F. Valette, On the Security of Randomized CBC-MAC Beyond the Birthday Paradox Limit: A New Construction, Proceedings of FSE 2002, LNCS 2365, pp. 237-251, Springer-Verlag, 2002.
[23] T. Iwata and K. Kurosawa, OMAC: One-Key CBC MAC, Proceedings of FSE 2003, LNCS 2887, pp. 129-153. Springer-Verlag, 2003.
[24] M. Bellare, R. Canetti and H. Krawczyk, Keying Hash Functions for Mes-sage Authentication, Advances in Cryptology { Proceedings of CRYPTO 1996, LNCS 1109, pp. 1-15, Springer-Verlag, 1996.
[25] B. Preneel and P.C. van Oorschot, On the Security of Iterated Message Authentication Codes, IEEE Transactions on Information Theory, Vol. 45, No. 1, pp. 188-99, 1999 (Preliminary version, entitled MDx-MAC and Building Fast MACs from Hash Functions, Advances in Cryptology { Proceedings of CRYPTO 1995, LNCS 963, pp. 1-14, Springer-Verlag, 1995).
[26] I. Damg°ard, A Design Principle for Hash Functions, Advances in Cryptology { Proceedings of CRYPTO 1989, LNCS 435, pp. 416-427, Springer-Verlag, 1989.

[27] R.C. Merkle, One Way Hash Functions and DES, Advances in Cryptology { Proceedings of CRYPTO 1989, LNCS 435, pp. 428-446, Springer-Verlag, 1989.

[28] J.Kim and A. Biryukov, B.preneel and S.Lee On the security of encryption modes of MD4, MD5 and HAVAL, Proc. of ICICS 2005, LNCS3783pp147-158 springer-verlag:2005.