Total Break of Zorro using Linear and Differential Attacks

Shahram Rasoolzadeh[1,2], Zahra Ahmadian[1,2], Mahmood Salmasizadeh[2], and Mohammad Reza Aref[1]

[1] Information Systems and Security Lab (ISSL), Department of Electrical Engineering,
[2] Electronic Research Institute,
Sharif University of Technology, Tehran, Iran
{sh_rasoolzadeh,ahmadian}@ee.sharif.edu,{salmasi,aref}@sharif.edu

Abstract. An AES-like lightweight block cipher, namely Zorro, was proposed in CHES 2013. While it has a 16-byte state, it uses only 4 S-Boxes per round. This weak nonlinearity was widely criticized, insofar as it has been directly exploited in all the attacks on Zorro reported by now, including the weak key, reduced round, and even full round attacks. In this paper, Using some observations discovered by Wang et. al., we present new differential and linear attacks on Zorro, both of which recover the full secret key with practical complexity. These attacks are based on very efficient distinguishers that have only two active sboxes per four rounds. The time complexity of our differential and linear attacks are $2^{52.74}$ and $2^{57.85}$ and the data complexity are $2^{55.15}$ chosen plaintexts and $2^{45.44}$ known plaintexts, respectively. The results clearly show that the block cipher Zorro does not have enough security against differential and linear cryptanalysis.

Keywords: Zorro, Lightweight Block Cipher, Differential Cryptanlysis, Linear Cryptanlysis.

1 Introduction

Block ciphers are the most widely-studied primitives in the area of symmetric cryptography. Among the different types of attacks, differential cryptanalysis [1] and linear cryptanalysis [2] can be regarded as two of the oldest and most important statistical methods to analyse the security of the block ciphers.

Zorro is a newly proposed lightweight block cipher whose design is based on AES [4]. It is basically designed with the aim of increasing the resistance against side-channel attacks while still remaining a lightweight block cipher. In spite of its 16-byte state, the SubByte layer of Zorro uses only 4 similar S-Boxes in the first row, which are different from AES S-Boxes. Similar to LED-64 [5], key addition layer in Zorro is applied only after each four rounds. Besides, Shift Row and Mix Column layers are exactly the same as AES ones.

For both differential and linear cryptanalysis, desingers have evaluated the security of the cipher and found a balance between the number of inactive S-Boxes and the number of freedom degrees for differential or linear paths. The

designers concluded that 14 and 16 rounds are upper bound for any non-trivial differential or linear characteristics, respectively. Furthermore, they show that in the single key model of Zorro, a 12 round meet-in-the-middle attack is the most powerful attack.

1.1 Related work

During the past year, Zorro has attracted the attention of many cryptanalists and some attacks have been lunched against it by now. The first one, proposed by Guo, is a key recovery attack on the full-round version of the algorithm, but it works only for 2^{64} weak keys of the whole key space 2^{128} [6].

In the next attack, Wang et. al. presented a differential key recovery attack and a linear distinguisher for full-round Zorro. They observed an interesting property for the Zorro's MixColumn: the forth power of the MDS matrix is equal to the identity matrix. Using this property of Zorro along with its weak nonlinearity, they found differential and linear distinguishers for Zorro in which only four S-Boxes are activated per four round. The resulted differential cryptanalysis can recover the randomly chosen key with time complexity of 2^{108} and data complexity of $2^{112.4}$ chosen plaintexts, and linear distinguisher use $2^{105.3}$ known plaintexts to successfully distinguish it from the random permutation [7].

Finally, Soleimany proposed a probabilistic variation of slide attack and applied it to 16 rounds of Zorro (out of 24 rounds) [8]. This attack requires $2^{123.62}$ known plaintexts with the time complexity of $2^{123.8}$ encryptions or $2^{121.59}$ known plaintexts with time complexity of $2^{124.23}$ encryptions.

Very recently, Dunkelman et. al. briefly reported their new results on Zorro in FSE'14 rump session which is an improvement of Wang's differential and linear attacks [9]. As they stated, the gain of their attack is not in the probability of distinguishers since the new distinguishers still have two active S-boxes per two rounds (i.e. one Sbox per round in average which is similar to that of Wang's attack). Instead, they achieved some improvements in the key recovery phase. Consequently, a differential attack with time and data complexity of 2^{98} and 2^{95}, and a linear attack with time and data complexity of 2^{88} and $2^{83.3}$ are resulted.

1.2 Our contributions

In this paper, we break the full-round version of Zorro by using differential and linear cryptanalysis. Alongside the weak nonlinearity of Zorro (i.e. the limited number of S-Boxes in each round), we use the fact discovered in [7] that the fourth power of MDS matrix is equal to the identity matrix. We propose very efficient iterated differential characteristics and linear trails that have only two active S-Boxes per four round. Using the 23, 22 and 21-round differential characteristic and linear trail, we can propose a key recovery attack for any randomly chosen secret key of full-round Zorro. Differential cryptanalysis has a time complexity of $2^{52.74}$ full round encryption and data complexity of $2^{55.15}$ chosen plaintexts. And linear cryptanalysis has a time complexity of $2^{57.85}$ full round encryption

and data complexity of $2^{45.44}$ known plaintexts. Either in differential cryptanalysis or in linear cryptanalysis memory complexity is 2^{17}. Tab. 1 summarizes the complexities of existing attacks and ours. Our results show that the theoretical security of the full-round Zorro evaluated by designers does not hold up in practice.

Table 1. Summary of cryptanalytic results on Zorro

Attack Type	Rounds attacked	Time	Data	Memory	Ref.
Differential	Full-round*	$2^{54.3}$	$2^{54.3}$ CP	$2^{54.3}$	[6]
Statistical Slide	16 (out of 24)	$2^{123.8}$	$2^{123.62}$ CP	-	[8]
Statistical Slide	16 (out of 24)	$2^{124.23}$	$2^{121.59}$ CP	-	[8]
Linear (Distinguisher)	Full-round	$2^{105.3}$	$2^{105.3}$ CP	-	[7]
Differential	Full-round	2^{108}	$2^{112.4}$ CP	2^{32}	[7]
Differential	Full-round	2^{98}	2^{95} CP	-	[9]
Linear	Full-round	2^{88}	$2^{83.3}$ KP	2^{80}	[9]
Differential	**Full-round**	$\mathbf{2^{52.74}}$	$\mathbf{2^{55.15}}$ **CP**	$\mathbf{2^{17}}$	**Sec. 3**
Linear	**Full-round**	$\mathbf{2^{57.85}}$	$\mathbf{2^{45.44}}$ **KP**	$\mathbf{2^{17}}$	**Sec. 4**

*This attack works only for 2^{64} keys of the whole key space 2^{128}.
CP: Chosen Plaintext, KP: Known Plaintext.

1.3 Outline

This paper is organized as follows: Section 2 presents a brief description of Zorro. Section 3 represents the outline of the differential attack on full-round Zorro with all details and evaluates its complexities. Also outline and detail of linear attack and evaluation of its complexities are presented in Section 4. Finally, Section 5 concludes this paper.

2 A Brief Description of Zorro

The block cipher Zorro has a 128-bit key and a 128-bit block size. It has 24 rounds which is divided into 6 steps of 4 rounds each.

As in AES-128, the internal state in Zorro is a 4×4 matrix of bytes, and every round consists of four transformations:

1. **SB*** is the S-Box layer where only 4 similar S-Boxes, which are different from AES S-Boxes, are applied to the 4 bytes of the first row in the state matrix.
2. **AC** is the addition of round constants. Specifically, in round i the four constants $(i, i, i, i << 3)$ are added to the four bytes of the first row.
3. **SR** is similar to AES ShiftRow.
4. **MC** is similar to AES MixCol.

The key schedule of Zorro is similar to that of LED. Before the first and after each step (i.e. each four rounds), the master key is xored to the state.

As Wang argued in [7], by focusing on MC layer used in Zorro, we will see an exclusive feature of this layer. The fourth power of MC matrix equals the identity matrix.

$$M = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \Rightarrow M^4 = \begin{pmatrix} 01\ 00\ 00\ 00 \\ 00\ 01\ 00\ 00 \\ 00\ 00\ 01\ 00 \\ 00\ 00\ 00\ 01 \end{pmatrix} \tag{1}$$

Since only 4 S-Boxes are applied to the first row in each round, combined with these features of MDS matrix iterated differential characteristics and linear trails are found for one step of Zorro.

3 Differential Cryptanalysis

In this section, we first find some iterated differential characteristics for one step of Zorro with high probability. Then, using the conventional assumption that the step functions are independent [7], we will construct three groups of distinguishers for 23, 22 and 21 rounds of Zorro. The first distinguisher is used in the first phase of the key recovery attack to reduce the key space of 2^{128} to 2^{96}. Having recovered 32 bits of key in the first phase, we use the second and third distinguishers in the next two phases to recover 64 more bits of the key. Finally the 32 remaining bits of key are retrieved by an exhaustive search.

3.1 Iterated Differential Characteristic

In order to find an efficient iterated differential characteristic for one step of Zorro with the minimum number of active S-Boxes, we enjoy the maximum flexibility in the input difference. To minimize the number of active S-Boxes, it is sensible to set the difference of the first row equal to zero and to bypass the influence of SR transformation, we set the differences of the third and fourth columns equal to that of first and second ones, respectively. We do not impose any more conditions on the remaining six bytes now and let their dependency be utilized in minimizing the number of active S-Boxes in the next rounds. We can extend this input difference to four rounds with only two active S-Boxes as shown in Fig. 1. In this figure the AC transformation is omitted since it does not have any affect on the differentials. The active S-Boxes are shown in gray whose difference value is written inside. For attaining such a differential characteristic, some conditions in MC transformations between states (#3, #4), (#6, #7), (#12, #1), as well as two conditions for SB^* transformation between states (#10, #11) must be satisfied. Satisfying mentioned MC conditions results in 24 independent linear equations in 26 variables $A, \ldots, Z$. Hence, after some simplifications, we can represent all the variables based on A and B:

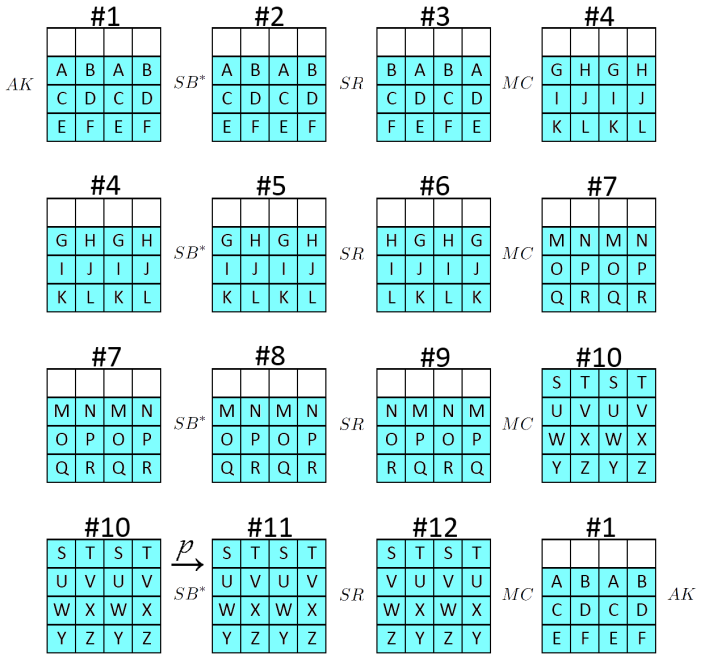

Fig. 1. Iterated differential characteristic of one step of Zorro

$$
\begin{aligned}
C &= D = A \oplus B \\
E &= 2A \oplus B \\
F &= A \oplus 2B \\
G &= 2A \oplus 3B \\
H &= 3A \oplus 2B \\
I &= A \oplus 5B \\
J &= 5A \oplus B \\
K &= 3A \oplus 4B \\
L &= 4A \oplus 3B \\
M &= A \oplus 8B \\
N &= 8A \oplus B \\
O &= P = 13(A \oplus B) \\
Q &= 10A \oplus B \\
R &= A \oplus 10B \\
S &= 20A \oplus 4B
\end{aligned}
$$

$$
\begin{aligned}
T &= 4A \oplus 20B \\
U &= 6A \oplus 31B \\
V &= 31A \oplus 6B \\
W &= 17A \oplus 5B \\
X &= 5A \oplus 17B \\
Y &= 7A \oplus 24B \\
Z &= 24A \oplus 7B
\end{aligned}
$$

Now let's focus on the SB^* transformation of the fourth round. We need that for all the four active S-Boxes, each output difference equals its own input difference. Suppose this happens with the probability of p. Then,

$$p = DP(S \to S)^2 \times DP(T \to T)^2 \tag{2}$$

where $DP(\alpha \to \beta)$ is the differential probability of S-Box with input difference α and output difference β. We will try to maximize p. Also, we still have 2 degrees of freedom, A and B. So we can set one of S or T to zero and confine the number of active S-Boxes to two, per four rounds. Let

$$\begin{cases} S = 0 \Rightarrow B = 5A \\ T = 0 \Rightarrow A = 5B \end{cases} \tag{3}$$

Hence, for the best probability of the proposed 4-round differential characteristic

$$P_{4r} = \max_{1 \le x \le 255} DP(x \to x)^2 \tag{4}$$

According to DDT of S-Box, the maximum probability is equal to $P_{4r} = (6/256)^2 = 2^{-10.83}$ and there are three choices for x to achieve this value. Considering the two cases of $S = 0$ or $T = 0$, there would be, in total, six options for the input difference to construct a differential with this maximum probability. These differentials are shown in Table 2. Furthermore, similar to [7], we can replace the difference of state #1 by that of #4, #7 or #10, to get new sets of iterated differential characteristics.

3.2 Key recovery

The full key recovery attack on full-round Zorro proceeds in three phase. In each phase, we recover 32 bits of the secret key.

Phase 1. Recovering the 32 Bits of Key. Using each of the six 4-round iterated differentials introduced in Tab. 2, we can construct a 23-round (= 5 steps + 3 rounds) differential characteristics with probability of

$$P_{23r} = (P_{4r})^5 \times P_{3r} = 2^{-10.83 \times 5} = 2^{-54.15} \tag{5}$$

Table 2. Six iterated differential characteristics for one step

Number	A	B	C	D	E	F	G	H	I	J	K	L	M
1	136	158	22	22	149	175	178	164	88	0	205	178	20
2	158	136	22	22	175	149	164	178	0	88	178	205	178
3	92	55	107	107	143	50	225	138	183	0	56	225	255
4	55	92	107	107	50	143	138	225	0	183	225	56	225
5	22	78	88	88	98	138	254	166	123	0	25	254	80
6	78	22	88	88	138	98	166	254	0	123	254	25	254

Number	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	178	254	254	185	51	0	123	85	136	0	35	42	131
2	20	254	254	51	185	123	0	136	85	35	0	131	42
3	225	169	169	89	145	0	234	168	92	0	93	113	228
4	255	169	169	145	89	234	0	92	168	93	0	228	113
5	254	213	213	210	204	0	247	79	22	0	140	168	58
6	80	213	213	204	210	247	0	22	79	140	0	58	168

Note that the last three rounds of this characteristics have no cost in probability, i.e. $P_{3r} = 1$. Since P_{23r} is too far from that of a Pseudo Random Permutation, $P_{PRP} = 2^{-128}$, such a 23-round distinguisher can be successfully used to distinguish the correct key from the wrong key in a 24-round attack.

In the following, we explain a key recovery attack on full round Zorro which extracts 32 bits information of the secret key K. Similar to [7], a structure attack which merge all the six differential characteristics simultaneously requires less data here. We also change the order of MC and AK in the last round where the equivalent key $K' = MC^{-1}(K)$ is added before MC. In fact, this attack recovers 32 bits of the first row of K', each of which is a linear function of K, in two (potentially simultaneous) procedures: In the first one, we find the second and fourth bytes of first row by using iterated differential characteristics respected to No. 1, 3 and 5 of Tab. 2; In the other one, the first and third bytes are recovered respected to No. 2, 4 and 6 of Tab. 2. At the end, we will come up with 2^{96} key candidates for the whole 128-bit key.

Step 1. Choosing the Plaintext Pairs
Our Attack is a structural chosen plaintext attack, where we choose some structures and all the plaintexts in every structure are queried from the encryption oracle to get the corresponding ciphertexts. Suppose that we construct M structures which, in total, give N differential pairs with the difference according to #1. The precise relation between M and N can be found in Appendix A.

Step 2. Filtering the Ciphertext Pairs
Partially decrypt all the N ciphertext pairs generated in Step 1 to get their corresponding difference in the output of SB^* of round 24. Keep only those pairs that satisfy the condition in the third row of #10 as well as the two zero differences in the first row (see Fig. 2.). For a pseudo random permutation,

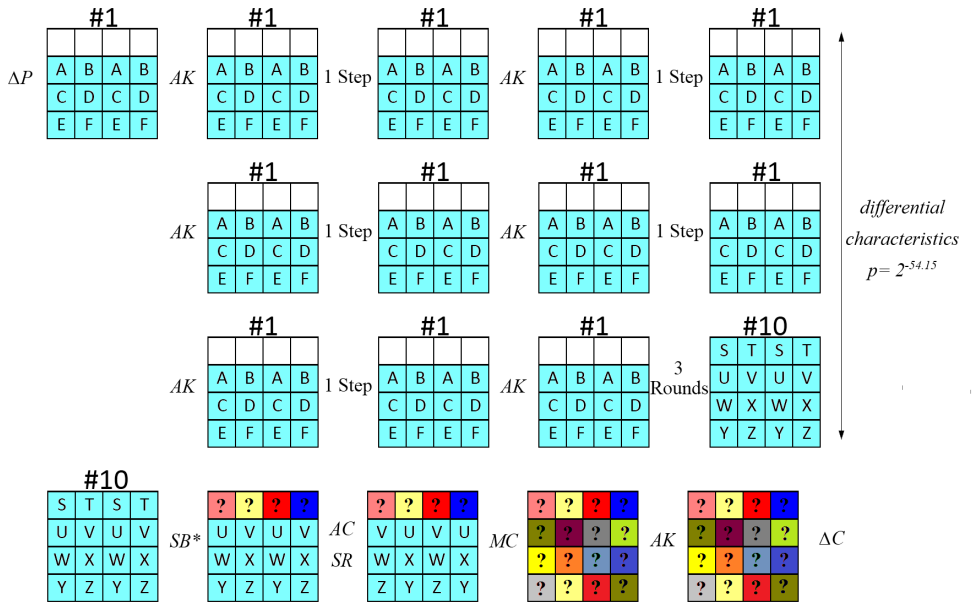

Fig. 2. Differential characteristics on 23-round Zorro

this happens with the probability of 2^{-112}. Whereas for Zorro this probability is $2^{-54.15}$. Therefore, it remains about $N \times 2^{-54.15}$ pairs of data to distinguish the right key from the wrong keys.

Step 3. Recovering 16 bits of K'
Guess the two bytes of the first row of K' corresponding to those two active S-Boxes, and partially decrypt the remaining pairs to get their differences in the first row of the input of round 24. If it is consistent with that of #1, increase the corresponding counter of the guessed key. There are $N \times 2^{-54.15}$ differential pairs to distinguish the right key from the wrong keys. An incorrect key is suggested with a probability of 2^{-16} while it is about one for the right key. Utilizing the probability differences between the correct key and incorrect keys, we can extract the correct candidates for secret key. By this procedure we find two Bytes of K' in the first row. A similar procedure can be repeated for the other two active S-Boxes to find the other two bytes in the first row.

Phase 2 & 3. Recovering the 96 Remaining Key Bits If we replace the state of #1 by #4 or #7 in Figure 1, we will come up with another 6 iterated differential characteristics, which can be used to construct 22 or 21-round differential characteristics with the same probability of $Pr_{22-round} = Pr_{21-round} = 2^{-54.15}$. So, we need the same number of differential pairs (N) to distinguish the right key from the wrong keys.

The steps of Phase 2 are similar to that of Phase 1 with two minor differences: In Step 2, the ciphertext differences are filtered based on their partially decrypted values in the output of SB^* transformation in round 23 (rather than 24). Thanks to the 32 bits of K' retrieved in Phase 1, this can be performed. In Step 3, We need to guess 16 bits of K'', where $K'' = MC^{-1}(SR^{-1}(K'$ with all bits 0 in the first row)).

In this phase, we partially decrypt all the ciphertexts in the structure for one round . But in AC layer, in addition to round constant, we add bitwisely the first row of K' which was found in Phase 1, and continue the rest of the attack similar to Phase 1. We guess all the 2^{16} keys involved in active S-Boxes, and repeat this procedure once more to get the other 2^{16} key bits. So, we can finally find 32 bits of the first row of K''.

Also in Phase 3, we make use of 21-round differentials and find the third 32 bits of K''', where $K''' = MC^{-1}(SR^{-1}(K''$ with all bits 0 in the first row)). We do similar to Phase 2, except that at first all the ciphertexts in the structure are partially decrypted for two rounds, and in AC layers, in addition to round constant, we add the first row of K' in round 23, and the first row of K" in round 22.

Finally, by using the information retrieved from K', K'' and K''', we end up with only 2^{32} candidates for the 128-bit secret key K. With a exhaustive search on these 2^{32} key, we can find the whole 128 bits of secret key.

3.3 Complexities

1. Time Complexity
   For Phase 1, in Step 2, we need to partially decrypt each remaining pair for less than one round. Therefore it takes about $N \times 2^{-54.15}/24$ full-round Zorro encryption. Step 3 requires less than one round encryption for $N \times 2^{-54.15} \times 2^{16}$ times. Thus the time complexity for finding 32 bits of K' is about
   $$T_{ph.1} = 2 \times N \times 1/24 \times (1 + 2^{-54.15} \times 2^{16}) \simeq N/12 \quad (6)$$
   full-round Zorro encryption. As described in [1] and [3], for a differential attack with differential characteristics with probability of p, about c/p differential pairs are needed to distinguish the right key from the wrong keys, where c is a small constant. These all results that N is smaller than $2^{54.15}$ and time complexity is about $T_{ph.1} = 2^{50.57}$ full-round Zorro encryptions.
   Similar to what explained for Phase 1, for the other two phases we have:
   $$T_{ph.2} = N \times 1/24 \times (1 + 2 \times (1 + 2^{-54.15} \times 2^{16})) \simeq N/8 \quad (7)$$
   $$T_{ph.3} = N \times 1/24 \times (2 + 2 \times (1 + 2^{-54.15} \times 2^{16})) \simeq N/6 \quad (8)$$
   All in all, the time complexity for the key recovery attack on full-round Zorro would be $T = T_{ph.1} + T_{ph.2} + T_{ph.3} + 2^{32} = 2^{52.74}$
2. Data Complexity
   For the both attack procedures presented in Phase 1, we need in total $2N$

differential pairs. According to Appendix A, we have $x = 6$ hence each structure has 2^6 plaintexts and $2N = 6 \times 2^5 M$ where M is the number of structures. So the Data complexity of this phase would be $D_{ph.1} = 2/3 \times N \simeq 2^{53.57}$.
The other two phases require also $D_{ph.1} = D_{ph.2} \simeq 2^{53.57}$ chosen data, so for the full key recovery attack we need about $D = 3 \times 2^{53.57} \simeq 2^{55.15}$ chosen plaintexts.

3. Memory Complexity
The memory required for all the three phases of the attack is used to keep the counters of the two 16-bit keys. For the simultaneous attack procedures in three phases, it is $Mem. = 2 \times 2^{16} = 2^{17}$ counters. Note that the memory required for keeping each structure pairs is negligible. So, the memory complexity is independent of N.

4 Linear Cryptanalysis

The procedure of linear attack is very similar to that of differential attack, presented in Sec. 3. We first try to find iterated linear trails with a high correlation for one step of the algorithm. Then we make use of this trail to construct 23, 22 and 21-round linear distinguishers, which are used for a key recovery attack on the full-round Zorro.

4.1 Iterated Linear Trail

Same as the way of finding iterated differential characteristics in section 3.1., we can find iterated linear trails for Zorro. There exists some iterated linear trials for one step of Zorro whose patterns are identical to that of differential characteristics given in Fig. 1, where the gray bytes are the ones with a non-zero mask. Satisfying MixColumn transformation between states of (#3, #4) , (#6, #7) and (#12, #1), the following conditions are forced on the mask values $A, B, \ldots, Z$:

$$
\begin{aligned}
A &= 10Q \oplus R \\
B &= Q \oplus 10R \\
C &= D = 13Q \oplus R \\
E &= Q \oplus 8R \\
F &= 8Q \oplus R \\
G &= 3Q \oplus 4R \\
H &= 4Q \oplus 3R \\
I &= Q \oplus 5R \\
J &= 5Q \oplus R \\
K &= 2Q \oplus 3R
\end{aligned}
$$

$$
\begin{aligned}
L &= 3Q \oplus 2R \\
M &= 2Q \oplus R \\
N &= Q \oplus 2R \\
O &= P = Q \oplus R \\
S &= 20Q \oplus 4R \\
T &= 4Q \oplus 20R \\
U &= 7Q \oplus 24R \\
V &= 24Q \oplus 7R \\
W &= 17Q \oplus 5R \\
X &= 5Q \oplus 17R \\
Y &= 6Q \oplus 31R \\
Z &= 31Q \oplus 6R
\end{aligned}
$$

Since the only nonlinear parts involved in this trail are the active S-Boxes of state #10, the absolute correlation $|c|$ of this four round trail is:

$$|c| = C(S,S)^2 \times C(T,T)^2 \tag{9}$$

where $C(\alpha, \beta)$ is the linear correlation of Zorro S-Box with input mask α and output mask β. Again, we have 2 degrees of freedom, Q and R to maximize $|c|$. So we can set one of S or T to zero.

$$\begin{cases} S = 0 \Rightarrow R = 5Q \\ T = 0 \Rightarrow Q = 5R \end{cases} \tag{10}$$

which in two cases yields

$$|c_{4r}| = \max_{1 \le x \le 255} C(x,x)^2. \tag{11}$$

After searching the LAT of Zorro S-box, the largest linear correlation occurs when $x = 136$. With this setting the absolute of the corresponding correlation would be $|c_{4r}| = (28/128)^2 \simeq 2^{-4.39}$. Also, we can find new linear trails with the same correlation, if we change the relative location of #1 with #4, #7 or #10. The masking values $A, \ldots, Z$ in Fig. 1 are given in Tab. 3.

4.2 Key recovery

Similar to that of differential attack, the full key recovery attack on full-round Zorro proceeds in three phase. In each phase, we recover 32 bits of the of secret key.

Phase 1. Recovering the 32 Bits of Key. Using each of the two 4-round iterated linear trails in Tab. 3, we can construct a 23-round (= 5 steps + 3 rounds) linear trail with the correlation of

$$|c_{23r}| = |c_{4r}|^5 \times |c_{3r}| = 2^{-4.39 \times 5} = 2^{-21.93} \tag{12}$$

Table 3. Two iterated linear trails for one step

Number	A	B	C	D	E	F	G	H	I	J	K	L	M
1	177	97	227	227	191	126	130	126	34	0	126	251	160
2	97	177	227	227	126	191	126	130	0	34	251	126	52

Number	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	52	133	133	234	234	0	136	95	37	0	170	163	234
2	152	133	133	234	234	136	0	37	95	170	0	234	163

This 23-round linear trail is similar to the 23-round differential chararcteristic given in Fig. 2. Since $|c_{23r}|$ is much larger than that of a Pseudo Random Permutation, $|c_{PRP}| = 0$, such a 23-round distinguisher can be successfully used to distinguish the correct key from the wrong key in a 24-round attack.

In the following, we explain a key recovery attack on full round Zorro which extracts 32 bits of the first row of K', in two sequential procedures: First, we find the second and fourth bytes of the first row of K' by using iterated linear trails respected to No. 1 of Tab. 3. Then, first and third bytes of key respected to No. 2 of Tab. 3 gets found.

With the assumption that the secret key is randomly chosen from the whole key space, the amount of plaintext/ciphertext pairs required for this attack would be $N_L = 1/|c_{23r}|^2 \simeq 2^{43.85}$ as discussed in [2] and [3]. The steps of this phase of attack are as follows:

Step 1. Data Collection
Ask the corresponding ciphertexts of N_L randomly generated plaintexts from the encryption oracle.

Step 2. Data Processing
Compute

$$\alpha = \Gamma_{\#1} \cdot P \oplus \Gamma_{\#10,rows\ 2,3,4} \cdot C'_{rows\ 2,3,4} \tag{13}$$

where P is the plaintext, C' is the one-round partially decrypted ciphertext, $\cdot$ represent the dot product, and $\Gamma_{\#n}$ is the linear mask for state #n in No.1 linear trail given in Tab. 3.

Step 3. Recovering the second and fourth bytes of K'
Guess the second and fourth bytes of K', partially decrypt the ciphertext to get the first row of C' for every 2^{16} guesses. Compute

$$\beta = \Gamma_{\#10,row\ 1} \cdot C'_{row\ 1} \tag{14}$$

If $\alpha = \beta$, increase the counter of the corresponding guessed key.

Step 4. Recovering the first and third bytes of K'
Repeat Steps 2 and 3 for these two bytes of key.

At the end of this procedure, all the four bytes of K''s first row are introduced.

Phase 2 & 3. Recovering the 96 Remaining Key Bits Look like full-key recovery attack in Phase 2 and 3 of differential cryptanalysis, we use 22 and 21-round linear distinguishers with $c_{22r} = c_{21r} = 2^{-21.93}$ which works with an amount of $N_L = 2^{43.85}$ known plaintexts. After reducing the key candidates to 2^{32}, we do a exhaustive search on the key candidates to get the secret key.

Complexities

1. Time Complexity
   We actually separated Steps 2 and 3 to avoid some unnecessary repetitions in attack computations in practice. But, to evaluate the time complexity of the attack, we ignore this improvement and give an upper bound for the time complexity assuming that Step 2 is merged with Step 3.

$$T_{ph.1} = N_L \times 2 \times 2^{16} \times 1/24 = 2^{56.27}. \tag{15}$$

$$T_{ph.2} = N_L \times 1/24 \times (1 + 2 \times 2^{16})) \simeq 2^{56.27} \tag{16}$$

$$T_{ph.3} = N_L \times 1/24 \times (2 + 2 \times 2^{16})) \simeq 2^{56.27} \tag{17}$$

2. Data Complexity
   As mentioned before, for each phase we need about $N_L \simeq 2^{43.85}$ known plaintexts.
3. Memory Complexity
   Since the procedure of recovering the two 16 bits of first row of K' are performed in parallel, it is necessary to have enough memory for each 2×2^{16} keys, which is independent of N_L.

All in all, the time, data and memory complexity for the proposed key recovery attack on full-round Zorro are $2^{57.85}, 2^{45.44}$, and 2^{17}, respectively.

5 Conclusions

In this paper, we presented how to break the full-round version of Zorro by using differential and linear cryptanalysis with practical complexities. These attacks works for all the key space and make use of 23, 22 and 21-round differential characteristics or linear trails. Our results on these two attacks show a trade-of between the time and data complexity: While differential cryptanalysis has a time complexity of $2^{52.74}$ full round encryption and data complexity of $2^{55.15}$ chosen plaintexts, linear cryptanalysis has a time complexity of $2^{57.85}$ full round encryption and data complexity of $2^{45.44}$ known plaintexts. As far as we know, this is the first practical attack on full-round Zorro which along with the previous cryptanalyses shows that the low nonlinearity in the design of Zorro obviously has sacrificed the security for efficiency.

Appendix A. Structural Chosen Plaintext

Assume that we have $x > 2$ differential characteristics and we are going to choose minimum number of plaintexts that provide enough pairs for these x differential characteristics. Let's define a graph in which the vertexes are the plaintexts and the edges are the valid differential pairs. For any node we have x edges and the number of nodes are 2^x. So, we have $x \times 2^{x-1}$ differential plaintext pairs, in total. Thus, the ratio of the chosen plaintexts to the differential plaintext pair in a stracture is $2/x$. This method is an extension of what proposed in [7] for generating data.

References

1. Eli Biham and Adi Shamir. *Differential cryptanalysis of DES-like cryptosystems.* In Alfred J. Menezes and Scott A. Vanstone, editors, Advances in Cryptology-CRYPT0 90, volume 537 of Lecture Notes in Computer Science, pages 221. Springer Berlin Heidelberg, 1991.
2. Mitsuru Matsui. *Linear cryptanalysis method for DES cipher.* In Tor Helleseth, editor, Advances in Cryptology-EUROCRYPT 1993, volume 765 of Lecture Notes in Computer Science, pages 386-397. Springer Berlin Heidelberg, 1994.
3. H. M. Heys, *A Tutorial on Linear and Differential Cryptanalysis.* Technical Report CORR 2001-17, Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, Mar. 2001.
4. B. Gerard, Vincent Grosso, M. Naya-Plasencia, and Francois-Xavier Standaert. *Block ciphers that are easier to mask: How far can we go?* In Guido Bertoni and Jean-Sbastien Coron, editors, Cryptographic Hardware and Embedded Systems (CHES) 2013, volume 8086 of Lecture Notes in Computer Science, pages 383-399. Springer Berlin Heidelberg, 2013.
5. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw. *The LED block cipher.* In Bart Preneel and Tsuyoshi Takagi, editors, Cryptographic Hardware and Embedded Systems-CHES 2011, volume 6917 of Lecture Notes in Computer Science, pages 326-341. Springer Berlin Heidelberg, 2011.
6. Jian Guo, Ivica Nikolic, Thomas Peyrin, and Lei Wang. *Cryptanalysis of Zorro.* Cryptology ePrint Archive, Report 2013/713, 2013. `http://eprint.iacr.org/`
7. Yanfeng Wang, Wenling Wu, Zhiyuan Guo, and Xiaoli Yu. *Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro.* Cryptology ePrint Archive, Report 2013/713, 2013. `http://eprint.iacr.org/`
8. Hadi Soleimany. *Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro.* Accepted Papers for 21st International Workshop on Fast Software Encryption. `http://fse2014.isg.rhul.ac.uk/index.php?p=accepted`
9. Ahiya Bar-On, Itai Dinur, Orr Dunkelman, Nathan Keller, Virginie Lallemand, Maria, Naya-Plasencia, Boaz Tsaban and Adi Shamir. *New Results on Zorro.* Rump Session for 21st International Workshop on Fast Software Encryption. `http://fse.2014.rump.cr.yp.to/`