International Journal of Cryptology Research 6(2): 27 - 44 (2016)

Statistical-based Repeated Differential Properties in the AES and PRESENT Key Schedules

Alya Geogiana Buja[*1,2], **Shekh Faisal Abdul Latip**[1], **Pang Kok An**[1], and **Rabiah Ahmad**[1]

[1]*INSFORNET, Faculty of ICT, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, 76100 Melaka.*
[2]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Melaka Kampus Jasin, 77300 Merlimau, Melaka.*

E-mail: geogiana@melaka.uitm.edu.my, shekhfaisal@utem.edu.my, rabiah@utem.edu.my, pangkokan@gmail.com
[*]*Corresponding author*

ABSTRACT

This paper investigates the repeated differential properties in key schedules of the Advanced Encryption Standard (AES) block ciphers and PRESENT. The concept of statistical-based repeated differential pattern for the PRESENT and AES key schedules are defined and introduced. Our study shows that there is a repeated differential property in the AES and PRESENT key schedules. For AES-192 and AES-256,the initial differential patterns were found repeated in first and second round for AES-192 while only in the first round for AES-256. Meanwhile, for AES-128, the initial differential pattern was not found in any of the rounds. In the PRESENT key schedule, the differential patterns were found repeated inconsistently for PRESENT-80 throughout the 32 rounds (including the final round). Meanwhile, the differential pattern was found repeated consistently and clearly for PRESENT-128. In addition, the round-keys with the repeated differential pattern have a large number of bytes in common. From the result, we found that the key schedule for AES-128, AES-192 and AES-256 are more ideal compared to PRESENT-80 and PRESENT-128. The key schedule of AES achieves randomness property compared to PRESENT. With more than half initial differential bits, it affects all bits of the round-key for AES-128, began after round 3 in AES-192 and after round 2 in AES-256. However, for PRESENT the key schedule of PRESENT-80 and PRESENT-128, found that the key schedule of PRESENT-80 is more ideal compared to PRESENT-128 because with about 36 bits (more than half) initial differential bits, 81.25% bits of the round-key affected compared to only 75% for PRESENT-128.

Keywords: AES, block cipher, key schedule, PRESENT, repeated differential properties

1 INTRODUCTION

Advanced Encryption Standard (AES) also known as Rijndael algorithm was developed by Joan Daemen and Vincent Rijmen and submitted to NIST in 1998 (Daemen and Rijmen, 1998). Later in 2001, AES has been adopted as the encryption standard by the U.S. government and is now used worldwide (Federal Information Processing Standards Publication 197, 2001). There are three variants of AES namely AES-128, AES-192 and AES-256. Since proposed, there are several works have been done on the AES key schedules (Biryukov and Khovratovich, 2009, Biryukov et al., 2009, Bogdanov et al., 2011, Dunkelman et al., 2010, Nikolic, 2009, Sasaki, 2011). Another block cipher that was chosen as a standard is named PRESENT is an ultra-lightweight block cipher proposed by Bogdanov et al in 2007 (Bogdanov et al., 2007). It has been chosen as an international standard by ISO/IEC in year 2012 (ISO/IEC 29192-2:2012, 2012). The design considerations of the cipher suit the requirement of todays technology that employing small embedded system as in mobile big data computing environment (Buja et al., 2015). Like AES, PRESENT has two variants namely PRESENT-80 and PRESENT-128 with the key length of 80 bits and 128 bits respectively. As proposed in the original proposal (Bogdanov et al., 2007), the key schedule of the PRESENT block cipher was designed with the round-dependent counter to create asymmetry properties. Asymmetry in the key schedule prevents against related-key and slide attacks (Biham, 1993). Since proposed in 2007, there have been many efforts aiming to attack this cipher such as in (Standaert et al., 2003)(Huang et al., 2014)(Abdul-Latip et al., 2011). Some recent results of key schedule analysis on PRESENT and other block ciphers were presented in (Cho, 2010). In 2011, Hernandez-Castro et al (Hernandez-Castro et al., 2011) investigated the strength of PRESENT key schedule. Previously in 2009, Ozen et al (Ozen et al., 2009) and Ohkuma (Ohkuma, 2009) studied the weak keys of the reduced-round PRESENT.

THIS PAPER. Our work in this paper extends the previous works on AES-128 and AES-256 as presented in (Huang et al., 2011) and (Buja et al., 2016) for PRESENT-80 and PRESENT-128. In this paper, the repeated differential properties of both block ciphers are analyzed and presented in the terms of statistical-based.

ORGANIZATION OF THE PAPER. In Section 2 we provide a brief description of the key schedules of AES and PRESENT block cipher. The found repeated differential properties in the previous works are further explained in Section 3. In Section 4, some statistical-based repeated differential properties of AES-128, AES-256, PRESENT-80 and PRESENT-128 key schedules are presented. Finally, the conclusion are presented in Section 5.

2 A BRIEF DESCRIPTION OF THE AES AND PRESENT KEY SCHEDULES

Details on AES and PRESENT key schedules are presented in 2.1 and 2.2.

2.1 AES Key Schedules

AES is a byte-oriented cipher, and has 10 rounds for 128-bit, 12 rounds for 192-bit and 14 rounds for 256-bit keys. As mentioned in the original proposal, in each round of AES, the internal state (128 bits) can be presented in a 4×4 matrix of bytes, which will be processed by using the following four basic transformations: First, named SubBytes: byte-wise application of

S-boxes, abbreviated as SB. Second, named ShiftRows: cyclic shift of each row of the state matrix by some amount, abbreviated as SR. Third, named MixColumns: column-wise matrix multiplication, abbreviated as MC. Lastly, named AddRoundKey: XOR of the subkey to the state, abbreviated as ARK. An additional AddRoundKey operation is performed before the first round (the whitening key) and the MixColumns operation is omitted in the last round. The key schedule of AES is required to produce 11, 13 or 15 128-bit subkeys from master keys of size 128, 192 or 256 bits respectively. Each 128-bit subkey contains four words (a word is a 32-bit quantity which is denoted by W). Call the number of rounds Nr, and the number of 32-bit words in the master key Nk. Algorithm 1 presents the AES key update algorithm.

Algorithm 1 AES Key Schedule

Input: $128/192/256$ bits secret key, Nk and round constant
Output: 128 bits round-key, Rk

for $i = 0, \ldots,$ Nk - 1 **do** W[i] = K[i] //(e.g., for AES-128, Nk = 4)
  for i = Nk, ..., 4(Nr + 1) - 1 **do** //(e.g., for AES-128, Nr = 10)
    $temp \rightarrow W$[i - 1]
    if i mod Nk == 0 **then** $temp \rightarrow SB(RotWord(temp)) \oplus RCON[I/$Nk]
    end if
    if Nk = 8 and i mod 8 == 4 **then** $temp \rightarrow SB(temp)$
    end if
    $W[i] \rightarrow W$[i - Nk] $\oplus\, temp$
  end for
  Generate the left most 128 bits Rk
end for

As in Algorithm 1, RCON are round constants, and RotWord() rotates four bytes by one byte position to the left. The subkey used in the AddRoundKey at the end of round r is denoted by Kr . The whitening key is K0 . Each subkey is represented as a byte matrix of size 4x4 (corresponding to the state matrix), and the jth byte in the ith row of the matrix is denoted by Kr i,j (0 ¡ i, j ¡ 4). The equivalent key obtained when the MixColumns and AddRoundKey operations are interchanged is denoted by K r = MC1 (Kr). Details on AES can be found in (Daemen and Rijmen, 1998).

2.2 PRESENT Key Schedules

PRESENT is a Substitution-Permutation Network (SPN) block cipher. The encryption block length is 64 bits and the key lengths of 80 bits for PRESENT-80 and 128 bits for PRESENT-128. This cipher takes 64-bit plaintext and 64-bit round key for the encryption which completed after 31 rounds.

Input $x_3x_2x_1x_0$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Output $y_3y_2y_1y_0$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Figure 1: PRESENT 4-bit S-box

Each round consists of three layers: addRoundKey, substitution layer (S-box Layer) and bit permutation layer (P-box Layer). The addRoundKey is a 64-bit XOR operation of the intermediate state with a round key. The S-box Layer as illustrated in Table 1 is a 64-bit nonlinear transform using a single S-box 16 times in parallel. PRESENT uses a single 4-bit S-box. Denote the input value of S-box S as and the output value as . Four bits input will be substituted with four bits output, i.e. . The round key for each round is extracted from the user-provided 80-bit secret key.

Algorithm 2 PRESENT-80 Key Schedule

Input: 80 bits secret-key, K
Output: 64 bits round-key, Rk

for i = 1 to 31 **do**
  Rotate left 61 bits
  $[k_{79}, k_{78}, k_{77}, k_{76}] = SB[k_{79}, k_{78}, k_{77}, k_{76}]$
  $[k_{19}, k_{18}, k_{17}, k_{16}, k_{15}] = [k_{19}, k_{18}, k_{17}, k_{16}, k_{15}] \oplus roundcounter$
  Generate the left most 64 bits Rk
end for

After each round, the secret key in the key register is updated by using the key scheduling algorithm. Algorithm 2 and Algorithm 3 describe the key update algorithm for PRESENT-80 and PRESENT-128 respectively. Both algorithms apply a corresponding rotation function, call the 4-bit S-box of

PRESENT and XOR five bits with the round-dependent counter. The different between key update algorithms of these two variant are, first, the length of the secret key; PRESENT-80 has 80 bits secret key while PRESENT-128 has 128 bits. Second, the key schedule algorithm for PRESENT-80 has three layers; rotation layer, substitution layer and round counter XOR layer.

Algorithm 3 PRESENT-128 Key Schedule

Input: 128 bits secret-key, K
Output: 64 bits round-key,Rk

for i = 1 to 31 **do**
  Rotate left 61 bits
  [k_{127},k_{126},k_{125},k_{124}]= SB[k_{127},k_{126},k_{125},k_{124}]
  [k_{123},k_{122},k_{121},k_{120}]= SB[k_{123},k_{122},k_{121},k_{120}]
  [k_{66},k_{65},k_{64},k_{63},k_{62}]= [k_{66},k_{65},k_{64},k_{63},k_{62}]$\oplus roundcounter$
  Generate the left most 64 bits Rk
end for

Meanwhile, PRESENT-128 has four layers as well as it calls the S-box twice. Finally, the positions of the updated bits are different for all layers of both key schedule algorithms. Details on PRESENT can be read in (Bogdanov et al., 2007).

3 THE REPEATED DIFFERENTIAL PROPERTY OF AES AND PRESENT KEY SCHEDULES

Details of previous works, refer (Huang et al., 2011) for AES and (Buja et al., 2016) for PRESENT. Both AES and PRESENT key schedules (for 64 and 128 bits only) are reperesented in 4 x 4 box with 16 cells. However, for the initial presentation of the secret key for PRESENT is presented with 5-bits key. For AES, the keys are represented in one bute (8-bits). The initial pattern for AES-128 both AES-256 and PRESENT-80 and PRESENT-128 are as in Figure 1. Variable v, x, y and z in the reperesntation (repreesent the intial differential pattern) can be any value from 0 to 255. In this investigatation, we choose the value ”all-ones” for all variables.

Definition 3.1. Initial differential pattern (IDP) is defined as the initial difference of two 80-bits (for PRESENT-80) or 128-bits (for AES-128 and PRESENT-128) or 192-bits (for AES-192) or 256-bits (for AES-256) keys appeared in each round during the updating process is called a Initial Differential Pattern (RDP). The IDP is the value for AES is between 0 and 15 while for PRESENT is between 0 and 31.

Definition 3.2. Repeated differential pattern (RDP) is defined as a difference of two 128-bits (for AES) or 64-bits (for PRESENT) round-keys appeared in each round during the updating process is called a Repeated Differential Pattern (RDP). The RDP is the value between 0 and 15.

x	0	x	0
y	y	0	0
z	0	0	0
v	v	v	v

AES-128

x	0	x	0	0	0	0	0
y	y	0	0	0	0	0	0
z	0	0	0	0	0	0	0
v	v	v	v	0	0	0	0

AES-256

x	0	x	0
y	y	0	0
z	0	0	0
v	v	v	v

PRESENT-80

x	0	x	0
y	y	0	0
z	0	0	0
v	v	v	v

PRESENT-128

Figure 2: Initial Differential Pattern in AES and PRESENT Key Schedules

4 STATISTICAL-BASED REPEATED DIFFERENTIAL PROPERTIES OF AES AND PRESENT KEY SCHEDULES

Table 1 summarizes our statistical findings on diffusion related property of AES and PRESENT. As applied in the previous work (Huang et al., 2011), there are 72-bits of differential pattern used for both AES variants and 36-bits of initial differential pattern appliedfor PRESENT. AES-128 key schedule achieves its randomness property at the first round. By applying 72-bits initial differential pattern, the key schedule algorithm of AES-128 changed all bits of the round-key for all 10-rounds, 68.75% bits of the round-key in first two rounds of AES-192 and 75% for AES-256. Meanwhile, for PRESENT-80 about 81.25% bits of round-keys affected and only 75% for PRESENT-80. Obviously seen, there is no zero difference found in round-keys generated by AES-128 key schedule. There are five zero difference in the first round-key produced by AES-192 key schedule and three in the second round-key. Meanwhile, only four zero difference found in the first round-key of AES-256 key schedule. For PRESENT-80, there is between three to seven zero difference found in the 32 round-keys. PRESENT-128 key schedule yields between four to six zero difference in the 32 round-keys.

Theorem 4.1. *A key schedule algorithm is called random if there is at least 50% of the round-key bits affected. If the randomness achieved is100% in the very first round, then the algorithm is strongly random as the randomness properties successfully propagates through the entire rounds of the algorithm. In addition, a random key schedule algorithm has more positive correlation than negative correlation.*

Proof. Let Sk1 and Sk 2 are two secret keys of length m bits. Let a is the initial difference of Sk1 and Sk2 where d bit(s) of m bits SK2 is made difference from Sk1. a is computed by XORing the updated Sk1 and Sk2. Let Rk1, Rk2...Rk_n are the generated round key of length n bits. By updating the key schedule with an update algorithm, n/2 bits in the generated round-key changed from the initial round-key. Therefore, by the theorem, we have shown that a key schedule is random if the changed bit is equal or more than 50%. □

To show the propagation of the differential pattern in AES (refer Figure 4 to 6) and PRESENT (refer Figure 7 and 8) key schedules, we define the presentation of the round-keys bit for AES and PRESENT as in Figure 3 for both AES and PRESENT. For AES, each cell contains 8 bits while for PRESENT is 4 bits. For instances, the representation for AES-128 secret key (in byte) in row 0 in column 0 is presented as K15 as in Figure 3. Secret key in row 3 in column 2 is presented as K2.

The repeated differential pattern is shown propagate very closely in the

Cipher	Have Pattern ? (Yes / No)	Number of Bit of the Initial Differential Pattern	Percentage of Affected Bit (%)	Number of Zero Difference
AES-128	No	72	100	0
AES-192	No	72	$68.75 \sim 100$	$3 \sim 5$
AES-256	No	72	$75 \sim 100$	4
PRESENT-80	Yes	36	$56.25 \sim 81.25$	$3 \sim 7$
PRESENT-128	Yes, very clear (refer fig. 8)	36	$62.5 \sim 75$	$4 \sim 6$

Table 1: Summary on Differential Relationship in AES and PRESENT Key Schedules.

K15	K14	K13	K12
K8	K9	K10	K11
K7	K6	K5	K4
K0	K1	K2	K3

Figure 3: Byte Presentation of Master Key for AES and PRESENT Block Cipher

generated round-keys. Based on the correlation computed for AES key schedules, there is a strong relation between each round in the algorithm. No zero correlation found in AES-128 but AES-192 and AES-256 have two and three zero correlation respectively. In addition, AES-192 has more than 30 negative correlation compared to AES-256 which has only 29 negative correlation (refer Figure 10 and 11). That is the effect of rotation of the four words in AES key update algorithm. No clear RDP found in AES key schedules.

The propagation in PRESENT key schedule was found having some pattern. Since the PRESENT key schedule algorithm yields less randomness in updating the master key, therefore, after a few round, some repeated differential pattern can be found in the generated round-keys. The correlation shown in Figure 13 (in Appendix) clearly shown that there is pattern for PRESENT-128. The correlation between each round in PRESENT-128 key schedule algorithm

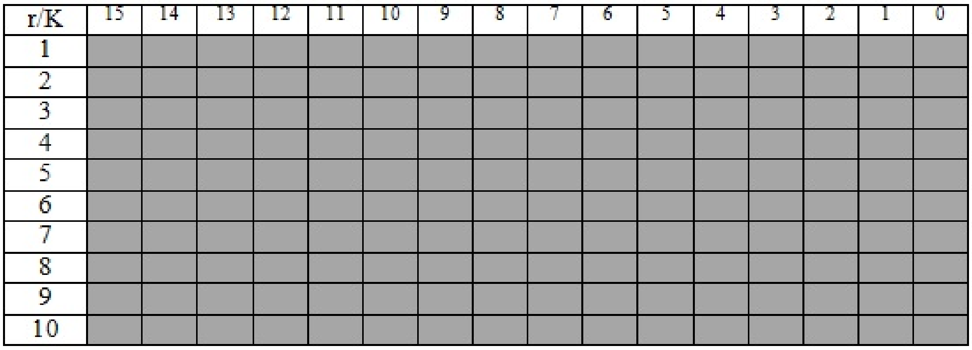

Figure 4: Propagation of RDP in AES-128

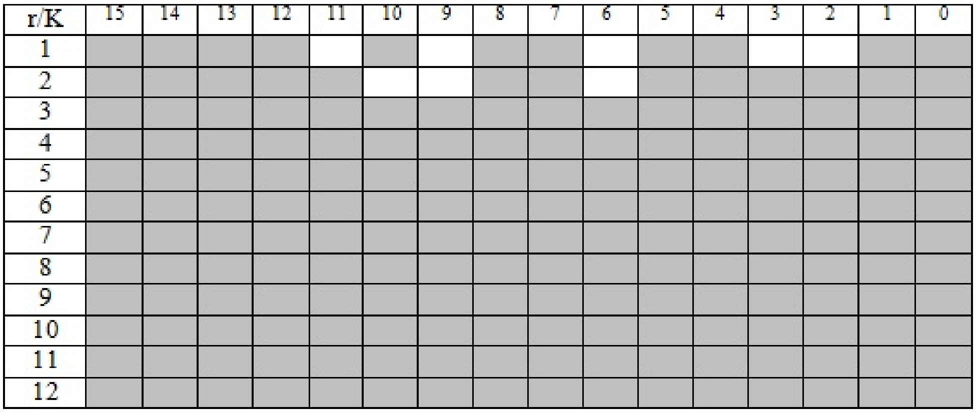

Figure 5: Propagation of RDP in AES-192

affects the randomness in the generated round-keys compared to the correlation computed for PRESENT-80 (refer Figure 12) in Appendix.

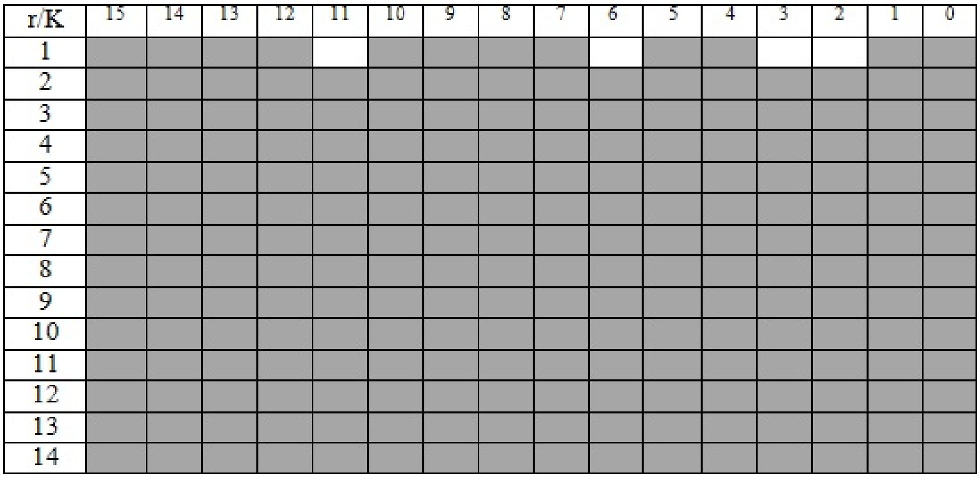

Figure 6: Propagation of RDP in AES-256

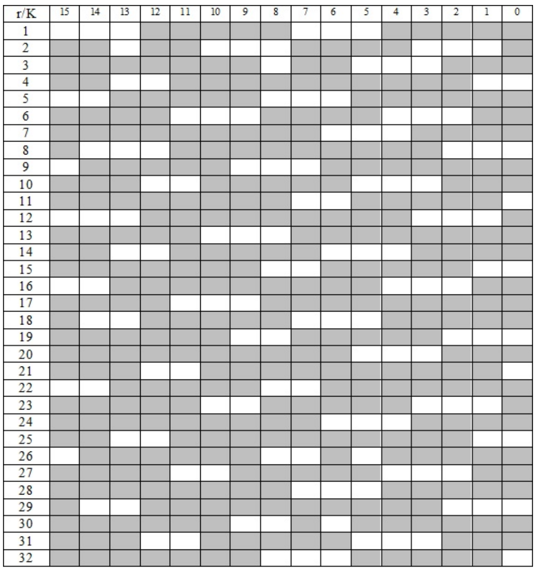

Figure 7: Propagation of RDP in PRESENT-80

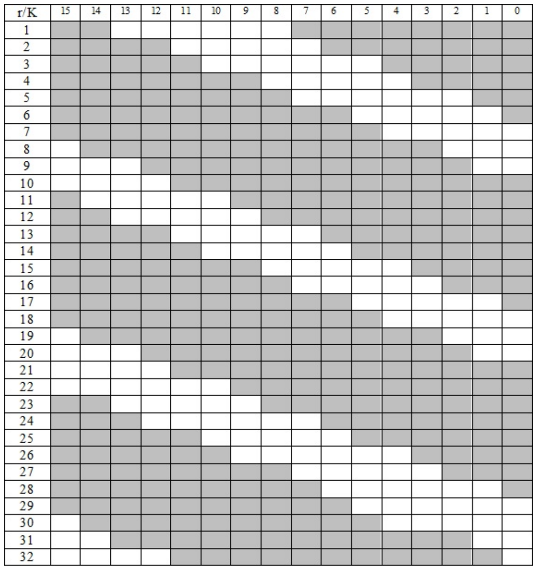

Figure 8: Propagation of RDP in PRESENT-128

5 CONCLUSION

This paper describes some statistical analysis of repeated differential patterns of the AES and PRESENT key schedules. We found that the key scheduling algorithm for AES-128 are more ideal compared to AES-192, AES-256, PRESENT-80 and PRESENT-128 because the key update algorithm for AES has achieved the randomness property successfully (refer fig.4). More than 75% of the round-key bits changed for AES-192 and AES-256 compared to PRESENT which is only 56.25% to 81.25% of round-key bits changed. In addition, less than five zero difference found for AES compared to PRESENT. However, key schedule for PRESENT-80 is more ideal compared to PRESENT-128. Besides, there are large numbers of byte in common found for PRESENT-128 compared to PRESENT-80. In agreement with (Biham, 1993), a cipher is secure from related-key attacks if there is no two different cipher keys contain large number of round keys in common. Future research can be done on investigating the potential further analysis of the weaknesses of the key schedule algorithms for AES and PRESENT.

ACKNOWLEDGMENTS

This work was supported by Universiti Teknologi MARA (UiTM) Malaysia under SLAB Scholarship and Fundamental Research Grant Scheme of UTeM FRGS/1/2015/ICT05/FTMK/02/F00293 funded by Ministry of Higher Education, Malaysia.

A APPENDICES

	r1	r2	r3	r4	r5	r6	r7	r8	r9	r10
r1	1									
r2	0.091267	1								
r3	0.090598	0.114682	1							
r4	-0.12414	-0.05986	-0.0906	1						
r5	-0.07451	-0.00248	-0.06164	-0.11497	1					
r6	-0.04374	0.02615	-0.00198	-0.05062	-0.07914	1				
r7	0.001958	0.005897	0.291918	-0.03328	0.070169	0.008859	1			
r8	-0.0938	0.031388	0.031497	0.062531	-0.04735	0.015719	-0.09393	1		
r9	0.048417	-0.04272	-0.16751	0.076782	-0.06986	-0.03664	-0.04996	0.015642	1	
r10	-0.01712	0.011293	-0.02168	-0.10808	-0.21452	-0.02631	0.143994	0.015642	0.002202	1

Figure 9: Correlation of RDP in AES-128

	r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12
r1	1											
r2	0.238095	1										
r3	-0.15749	-0.0315	1									
r4	-0.08679	0.039448	0.062622	1								
r5	-0.01186	-0.01186	0.156941	0.005897	1							
r6	-0.06911	-0.1323	-0.01567	0.042203	-0.07133	1						
r7	0.129989	0.035451	-0.21886	0.029369	-0.02846	-0.08085	1					
r8	0.100705	0.005924	-0.01567	0.020611	-0.05461	-0.0253	-0.2014	1				
r9	0.195485	0.069111	-0.20375	0.052018	-0.05461	-0.11963	0.112214	0.088185	1			
r10	-0.05726	0.069111	-0.14106	-0.07361	0.008363	0.006141	-0.04459	-0.13191	0.213952	1		
r11	-0.12599	-0.15749	0	0	-0.09416	0.10971	-0.15633	-0.04702	-0.01567	-0.01567	1	
r12	0.037517	0.005924	-0.10971	-0.0108	-0.02312	0.037583	-0.01323	0.025301	-0.00614	0.119627	-0.04702	1

Figure 10: Correlation of RDP in AES-192

	r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12	r13	r14
r1	1													
r2	-0.17534	1												
r3	0.149954	0.358613	1											
r4	0.142316	0.001958	0.090016	1										
r5	0.129199	0.052018	0.098678	0.170036	1									
r6	-0.04996	-0.06667	-0.0852	-0.09202	0.114833	1								
r7	0.042715	-0.03735	-0.01688	0.065751	-0.10282	-0.0688	1							
r8	0.003677	-0.0422	-0.02826	-0.04949	0.056743	0.020611	0.180544	1						
r9	0.078211	0	0.063277	-0.03127	0.078365	0.062622	0.031388	-0.04702	1					
r10	-0.07414	-0.15135	0.016882	-0.03435	0.008363	-0.1199	-0.05419	-0.08609	0.031388	1				
r11	-0.0022	0.075426	0.181627	-0.04548	-0.0277	0.169463	-0.02013	0.129199	-0.04693	-0.04272	1			
r12	0.154392	-0.04996	0.054934	0.111016	0.035058	0.106771	-0.17724	-0.0277	-0.1095	0.02013	0.029117	1		
r13	0.084741	0.00789	0.075736	0.059086	-0.08886	0.00789	-0.11468	-0.12045	0	0.019773	0.116273	0.084741	1	
r14	-0.04272	-0.057	-0.20557	-0.03435	-0.11757	0.068796	-0.02266	0.102816	0	-0.13498	0.02013	0.051553	0.114682	1

Figure 11: Correlation of RDP in AES-256

	r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11
r1	1										
r2	-0.43251	1									
r3	0.236229	-0.30056	1								
r4	-0.31109	0.185477	-0.37749	1							
r5	0.654547	-0.27715	0.274757	-0.46794	1						
r6	-0.7809	0.33353	-0.12023	0.2805	-0.43432	1					
r7	0.168653	-0.49574	0.33477	-0.3818	0.275301	-0.17612	1				
r8	-0.08845	0.025553	-0.40311	0.46794	-0.37255	0.115553	-0.34056	1			
r9	0.171894	0.085444	0.081026	-0.37749	0.531464	-0.25064	0.201279	-0.46729	1		
r10	-0.24335	-0.07192	0.149779	0.185477	-0.52875	0.33353	-0.10324	0.151352	-0.42923	1	
r11	0.200324	-0.00207	-0.04004	-0.15428	0.177171	-0.3391	0.349241	-0.24309	0.297106	-0.3325	1
r12	0.059863	0.065751	-0.07109	0.251222	-0.15859	0.037798	-0.40013	0.534509	-0.45559	0.191366	-0.37234
r13	-0.26228	0.26228	-0.24232	-0.02263	0.111247	0.196763	-0.06213	-0.30902	0.566818	-0.20032	0.168831
r14	0.261084	-0.45025	0.149779	0.059863	-0.08845	-0.11384	0.158432	0.088452	-0.3649	0.432512	-0.26641
r15	-0.10025	0.226045	-0.17448	-0.15467	0.184314	-0.0518	-0.05098	0.003922	0.274757	-0.40295	0.440867
r16	0.059863	-0.05986	0.185239	0.063539	-0.03328	0.101457	-0.07432	0.095937	-0.19926	0.191366	-0.37234
r17	-0.10025	0.100246	-0.1103	0.15859	-0.00392	0.13946	-0.18149	0.066667	0.082226	0.100246	-0.08653
r18	0.535787	-0.27845	0.181538	0.057074	0.302834	-0.33623	0.199194	-0.1103	-0.01538	-0.14978	0.174892
r19	-0.33614	0.525955	-0.06859	-0.1615	-0.05523	0.232477	-0.06154	-0.13412	0.189638	-0.10677	0.107762
r20	0.019773	-0.14632	0.326823	-0.02757	-0.07101	0.152312	0.258473	0.00789	-0.12508	0.170046	-0.04145
r21	-0.12856	0.065751	-0.26334	0.251222	-0.22124	-0.02586	-0.07432	0.283897	-0.00701	0.065751	-0.0432
r22	0.450246	-0.19803	0.149779	-0.19137	0.414743	-0.36948	0.093015	-0.03735	0.342783	-0.26108	0.196193
r23	-0.46135	0.26962	0.075396	0.089521	-0.17931	0.352227	-0.24243	-0.07571	0.010189	0.20571	-0.20514
r24	0.025553	-0.40295	0.274757	-0.02937	0.121569	0.075707	0.275301	-0.12157	-0.04613	0.163145	0.111247
r25	-0.05419	-0.00887	-0.49357	0.373899	-0.21425	0.07789	-0.03782	0.277151	-0.30056	-0.00887	-0.00207
r26	0.254173	-0.19137	0.071092	-0.43891	0.409203	-0.16512	0.139485	-0.03328	0.199257	-0.31698	0.109026
r27	-0.42923	-0.02111	-0.21231	0.185239	-0.40311	0.31585	-0.06779	0.082226	-0.08103	0.107559	-0.22968
r28	0.311092	-0.12267	-0.07109	-0.37439	0.154675	-0.34416	0.316641	-0.15467	0.185239	0.065751	0.154283
r29	0.056731	0.20261	-0.1075	0.153381	-0.17786	-0.115	-0.36155	0.436564	-0.2398	0.008104	0.016988
r30	0.002944	0.248285	0.071092	-0.06354	0.15859	-0.16512	-0.056	-0.34655	0.327422	-0.12856	0.109026
r31	-0.11222	-0.0149	0.100311	0.12167	-0.4022	0.066433	-0.15145	0.021794	-0.28878	0.430004	-0.18111
r32	0.128558	-0.12856	0.007009	-0.06354	0.095937	-0.22878	0.009163	-0.15859	0.135174	-0.31698	0.372336

	r12	r13	r14	r15	r16	r17	r18	r19	r20	r21	r22
r12	1										
r13	-0.50399	1									
r14	0.191366	-0.39858	1								
r15	-0.15859	0.309019	-0.52875	1							
r16	0.43695	-0.43816	0.254173	-0.34655	1						
r17	-0.15859	0.440867	-0.21425	0.121569	-0.2839	1					
r18	-0.05707	-0.22968	0.300563	-0.21058	0.199257	-0.1464	1				
r19	-0.02757	0.240393	-0.42314	0.323477	-0.15362	0.197242	-0.38331	1			
r20	-0.03545	-0.24039	0.233318	-0.32348	0.216648	-0.32348	0.189638	-0.11111	1		
r21	0.124145	0.022628	0.002944	-0.03328	-0.25122	0.217328	-0.24932	-0.02757	-0.1615	1	
r22	-0.12267	0.064021	-0.07192	0.100246	0.002944	-0.21425	0.171894	-0.35986	0.0435	-0.18548	1
r23	0.037798	0.12978	-0.17775	0.075707	0.101457	0.203213	-0.33623	0.168345	-0.23248	0.101457	-0.17775
r24	-0.09594	-0.08653	0.100246	-0.00392	0.029369	0.058824	0.302834	-0.11835	-0.00789	-0.2839	0.163145
r25	0.191366	-0.00207	0.054187	-0.08845	0.002944	0.037347	0.107559	0.146318	-0.08305	0.128558	-0.32414
r26	-0.06158	0.174854	-0.12856	0.34655	-0.24927	0.15859	-0.00701	0.153623	0.035451	-0.12414	0.059863
r27	0.007009	0.107464	0.107559	-0.21058	0.199257	-0.08223	-0.1159	-0.06052	0.189638	0.199257	-0.27845
r28	-0.18866	-0.0432	0.191366	-0.03328	-0.06354	-0.03328	0.007009	0.035451	0.027573	-0.00098	0.254173
r29	0.234107	-0.25482	-0.05673	0.080845	0.040363	0.016169	-0.02481	-0.09759	0.03253	0.169526	0.07294
r30	-0.06158	0.043199	-0.25417	0.033284	0.000978	-0.02937	-0.00701	0.216648	-0.21665	0.063539	0.12267
r31	0.004946	0.018735	0.048661	-0.3388	-0.12167	0.168409	-0.16516	-0.05182	0.115597	0.004946	-0.14201
r32	-0.06158	0.043199	0.059863	0.095937	-0.24927	-0.27998	0.249321	-0.1615	0.098476	-0.06158	0.12267

	r23	r24	r25	r26	r27	r28	r29	r30	r31	r32
r23	1									
r24	0.011954	1								
r25	-0.17775	-0.08845	1							
r26	-0.3561	0.033284	-0.19137	1						
r27	0.055019	-0.21058	0.171894	-0.13517	1					
r28	-0.08952	-0.09594	-0.12267	0.188661	-0.12116	1				
r29	0.213574	-0.17786	-0.05673	-0.23411	-0.09096	-0.02422	1			
r30	0.025862	0.095937	-0.12856	-0.1261	-0.26334	0.1261	-0.10494	1		
r31	-0.06241	-0.02179	0.112218	-0.25818	-0.03546	-0.05836	0.057183	-0.00495	1	
r32	-0.22878	-0.02937	-0.12856	0.249267	-0.00701	-0.06158	-0.04036	0.124145	-0.19487	1

Figure 12: Correlation of RDP in PRESENT-80

	r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12	r13	r14	r15	r16
r1	1															
r2	0.6	1														
r3	0.2	0.6	1													
r4	-0.2	0.2	0.6	1												
r5	-0.6	-0.2	0.2	0.6	1											
r6	-0.6	-0.6	-0.2	0.2	0.6	1										
r7	-0.54132	-0.54132	-0.54132	-0.12888	0.283547	0.695978	1									
r8	-0.54132	-0.54132	-0.54132	-0.54132	-0.12888	0.283547	0.574751	1								
r9	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132	-0.12888	0.149502	0.574751	1							
r10	0.214808	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132	-0.27575	0.149502	0.574751	1						
r11	0.533333	0.133333	-0.26667	-0.6	-0.6	-0.6	-0.54132	-0.12888	0.283547	0.695978	1					
r12	0.933333	0.533333	0.133333	-0.26667	-0.6	-0.6	-0.54132	-0.54132	-0.12888	0.283547	0.6	1				
r13	0.666667	0.933333	0.533333	0.133333	-0.26667	-0.6	-0.54132	-0.54132	-0.54132	-0.12888	0.2	0.6	1			
r14	0.266667	0.666667	0.933333	0.533333	0.133333	-0.26667	-0.54132	-0.54132	-0.54132	-0.54132	-0.2	0.2	0.6	1		
r15	-0.13333	0.266667	0.666667	0.933333	0.533333	0.133333	-0.19762	-0.54132	-0.54132	-0.54132	-0.6	-0.2	0.2	0.6	1	
r16	-0.53333	-0.13333	0.266667	0.666667	0.933333	0.533333	0.214808	-0.19762	-0.54132	-0.54132	-0.6	-0.6	-0.2	0.2	0.6	1
r17	-0.6	-0.53333	-0.13333	0.266667	0.666667	0.933333	0.627239	0.214808	-0.19762	-0.54132	-0.6	-0.6	-0.6	-0.2	0.2	0.6
r18	-0.54132	-0.54132	-0.47258	-0.06015	0.352285	0.764717	0.929125	0.503876	0.078627	-0.34662	-0.54132	-0.54132	-0.54132	-0.54132	-0.12888	0.283547
r19	-0.54132	-0.54132	-0.54132	-0.47258	-0.06015	0.352285	0.645626	0.929125	0.503876	0.078627	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132	-0.12888
r20	-0.26636	-0.54132	-0.54132	-0.54132	-0.47258	-0.06015	0.220377	0.645626	0.929125	0.503876	0.214808	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132
r21	0.146069	-0.26636	-0.54132	-0.54132	-0.54132	-0.47258	-0.20487	0.220377	0.645626	0.929125	0.627239	0.214808	-0.19762	-0.54132	-0.54132	-0.54132
r22	0.466667	0.066667	-0.33333	-0.6	-0.6	-0.6	-0.47258	-0.06015	0.352285	0.764717	0.933333	0.533333	0.133333	-0.26667	-0.6	-0.6
r23	0.866667	0.466667	0.066667	-0.33333	-0.6	-0.6	-0.54132	-0.47258	-0.06015	0.352285	0.666667	0.933333	0.533333	0.133333	-0.26667	-0.6
r24	0.733333	0.866667	0.466667	0.066667	-0.33333	-0.6	-0.54132	-0.54132	-0.47258	-0.06015	0.266667	0.666667	0.933333	0.533333	0.133333	-0.26667
r25	0.333333	0.733333	0.866667	0.466667	0.066667	-0.33333	-0.54132	-0.54132	-0.54132	-0.47258	-0.13333	0.266667	0.666667	0.933333	0.533333	0.133333
r26	-0.06667	0.333333	0.733333	0.866667	0.466667	0.066667	-0.26636	-0.54132	-0.54132	-0.54132	-0.53333	-0.13333	0.266667	0.666667	0.933333	0.533333
r27	-0.46667	-0.06667	0.333333	0.733333	0.866667	0.466667	0.146069	-0.26636	-0.54132	-0.54132	-0.6	-0.53333	-0.13333	0.266667	0.666667	0.933333
r28	-0.6	-0.46667	-0.06667	0.333333	0.733333	0.866667	0.558501	0.146069	-0.26636	-0.54132	-0.6	-0.6	-0.53333	-0.13333	0.266667	0.666667
r29	-0.56061	-0.56061	-0.42471	-0.01699	0.39073	0.798447	0.895516	0.475127	0.054738	-0.36565	-0.56061	-0.56061	-0.56061	-0.49266	-0.08494	0.322777
r30	-0.54132	-0.54132	-0.54132	-0.40384	0.008592	0.421024	0.716501	0.85825	0.433001	0.007752	-0.26636	-0.54132	-0.54132	-0.54132	-0.47258	-0.06015
r31	-0.3351	-0.54132	-0.54132	-0.54132	-0.40384	0.008592	0.291251	0.716501	0.85825	0.433001	0.146069	-0.26636	-0.54132	-0.54132	-0.54132	-0.47258
r32	0.077331	-0.3351	-0.54132	-0.54132	-0.54132	-0.40384	-0.134	0.291251	0.716501	0.85825	0.558501	0.146069	-0.26636	-0.54132	-0.54132	-0.54132

	r17	r18	r19	r20	r21	r22	r23	r24	r25	r26	r27	r28	r29	r30	r31	r32
r17	1															
r18	0.695978	1														
r19	0.283547	0.574751	1													
r20	-0.12888	0.149502	0.574751	1												
r21	-0.54132	-0.27575	0.149502	0.574751	1											
r22	-0.6	-0.54132	-0.12888	0.283547	0.695978	1										
r23	-0.6	-0.54132	-0.54132	-0.12888	0.283547	0.6	1									
r24	-0.6	-0.54132	-0.54132	-0.54132	-0.12888	0.2	0.6	1								
r25	-0.26667	-0.54132	-0.54132	-0.54132	-0.54132	-0.2	0.2	0.6	1							
r26	0.133333	-0.19762	-0.54132	-0.54132	-0.54132	-0.6	-0.2	0.2	0.6	1						
r27	0.533333	0.214808	-0.19762	-0.54132	-0.54132	-0.6	-0.6	-0.2	0.2	0.6	1					
r28	0.933333	0.627239	0.214808	-0.19762	-0.54132	-0.6	-0.6	-0.6	-0.2	0.2	0.6	1				
r29	0.730494	0.965581	0.545192	0.124803	-0.29559	-0.56061	-0.56061	-0.56061	-0.56061	-0.15289	0.254824	0.662541	1			
r30	0.352285	0.645626	0.929125	0.503876	0.078627	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132	-0.12888	0.283547	0.615257	1		
r31	-0.06015	0.220377	0.645626	0.929125	0.503876	0.214808	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132	-0.12888	0.194868	0.574751	1	
r32	-0.47258	-0.20487	0.220377	0.645626	0.929125	0.627239	0.214808	-0.19762	-0.54132	-0.54132	-0.54132	-0.54132	-0.22552	0.149502	0.574751	1

Figure 13: Correlation of RDP in PRESENT-128

REFERENCES

Abdul-Latip, S., Reyhanitabar, M., Susilo, W., and Seberry, J. (2011). Extended cubes: Enhancing the cube attack by extracting low-degree non-linear equations. pages 296–305.

Biham, E. (1993). New types of cryptanalytic attacks using related keys. 765:398–409.

Biryukov, A. and Khovratovich, D. (2009). Related-key cryptanalysis of the full aes-192 and aes-256. 5912:1–18.

Biryukov, A., Khovratovich, D., and Nikolic, I. (2009). Distinguisher and related-key attack on the full aes-256. 5677:231–249.

Bogdanov, A., Khovratovich, D., and Rechberger, C. (2011). Biclique cryptanalysis of the full aes. `http://eprint.iacr.org/2011/449`.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., Seurin, Y., and Vikkelsoe, C. (2007). Present: An ultra-lightweight block cipher. 4727:450–466.

Buja, A., Abdul-Latip, S., and Ahmad, R. (2015). The direction of lightweight ciphers in mobile big data computing. 72:469–476.

Buja, A., Abdul-Latip, S., and Ahmad, R. (2016). Repeated differential properties of present key schedules. In *Proceedings of the 4th International Conference of Information and Network Security (ICINS 16)*, pages 24–28, Kuala Lumpur, Malaysia.

Cho, J. (2010). Linear cryptanalysis of reduced-round present. 5985:302317.

Daemen, J. and Rijmen, V. (1998). AES Proposal : Rijndael.

Dunkelman, O., Keller, N., and Shamir, A. (2010). Improved single-key attacks on 8-round aes-192 and aes-256. 6477:158–176.

Federal Information Processing Standards Publication 197 (2001). Announcing the Advanced Encryption Standard. `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

Hernandez-Castro, J., Peris-Lopez, P., and Aumasson, J.-P. (2011). On the key schedule strength of presents. page 25363.

Huang, J., Susilo, W., and Seberry, J. (2011). Repeated differential properties of the aes-128 and aes-256 key schedules. In *10th international conference on trust, security and privacy in computing and communications (TrustCom)*, page 525532.

Huang, J., Vaudenay, S., and Lai, X. (2014). On the key schedule of lightweight block ciphers. 8885:124142.

ISO/IEC 29192-2:2012 (2012). Information technology Security techniques Lightweight cryptography. Part 2: Block ciphers. `https://www.iso.org/standard/56552.html`.

Nikolic, I. (2009). Distinguisher and related-key attack on the full aes-256. pages 231–249.

Ohkuma, K. (2009). Weak keys of reduced-round present for linear cryptanalysis. 5867:249–265.

Ozen, O., Varici, K., Tezcan, C., and Kocair, C. (2009). Lightweight block ciphers revisited: Cryptanalysis of reduced round present and hight. 5594:90–107.

Sasaki, Y. (2011). Meet-in-the-middle preimage attacks on aes hashing modes and an application to whirlpool. In *FSE11 Preproceedings*.

Standaert, F., Piret, G., and Quisquater, J. (2003). Cryptanalysis of block ciphers: a survey. Technical Report CG-2003/2, Universite Catholique de Louvain.