Differential Cryptanalysis of Round-Reduced Simon and Speck

Farzaneh Abed Eik List Stefan Lucks Jakob Wenzel

Bauhaus-Universität Weimar

FSE 2014
March 27, 2014

Agenda

- Motivation
- Simon and Speck
- Our Method
- Results
- Discussion

Section 1

Motivation

Motivation

- June 2013, two lightweight ciphers SIMON, SPECK by NSA
- Intensively optimized
- Performant in both hard- and software
- No security analysis for both ciphers $\Rightarrow$ left as a task to the community

Section 2

SIMON and SPECK

SIMON

- Uses ARX construction
- Families of Feistel-network
- Three simple operations: AND, rotations, XOR
- State size $2n$ and key size k, 10 family members

SIMON (cont'd)

Require: (L^0, R^0) {Plaintext}
Ensure: (L^r, R^r) {Ciphertext}

1: **for** $i = 1, \ldots, r$ **do**
2: $\quad L^i \leftarrow R^{i-1} \oplus K^{i-1} \oplus f(L^{i-1}) \oplus (L^{i-1} \lll 2)$
3: $\quad R^i \leftarrow L^{i-1}$
4: **end for**
5: **return** (L^r, R^r)

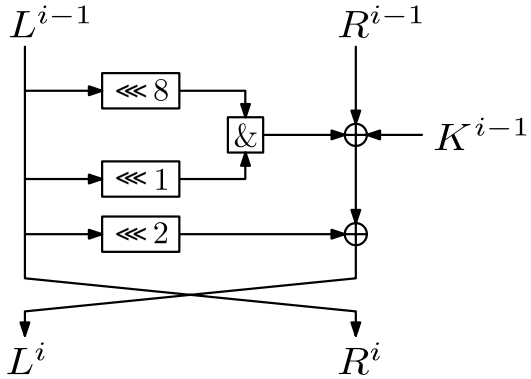


Figure: SIMON encryption

SPECK

- Three operations: Addition, rotations, XOR
- Support variety of block and key sizes, 10 family members
- Similar to ThreeFish but much faster

SPECK (cont'd)

Require: (L^0, R^0) {Plaintext}
Ensure: (L^r, R^r) {Ciphertext}

1: **for** $i = 1, \ldots, r$ **do**
2: $\quad L^i \leftarrow (L^{i-1} \ggg \alpha) + R^{i-1} \bmod 2^n$
3: $\quad L^i \leftarrow L^i \oplus K^{i-1}$
4: $\quad R^i \leftarrow (R^{i-1} \lll \beta) \oplus L^i$
5: **end for**
6: **return** (L^r, R^r)

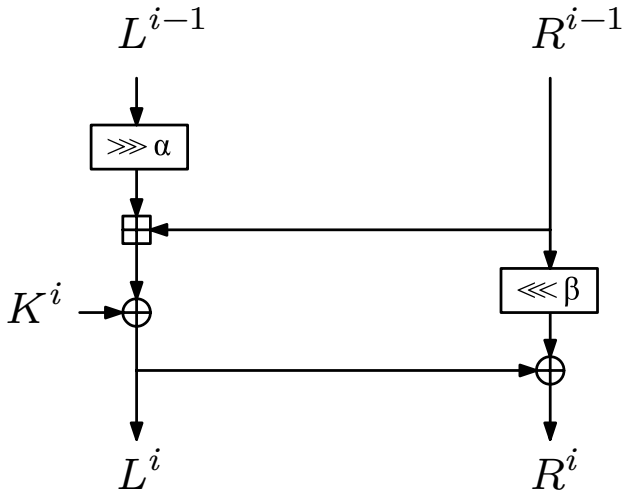


Figure: SPECK encryption

Section 3

Method

Why Differential Attacks

- Slide: XOR of 1-bit constant with round keys
- Linear: Difficulties to linearise AND
- MITM: Fast diffusion in key schedule
- Splice and Cut: Fast diffusion in key schedule

Methods for Differential Characteristic and Probability

Twofold approach:

1. Matsui's Algorithm:
   - Finds the best r-round characteristic in depth-first manner
   - Usse as reference trail for the Branch-and-Bound
2. Branch and bound (B&B) Algorithm:
   - Prunes the search
   - Finds the optimal solution

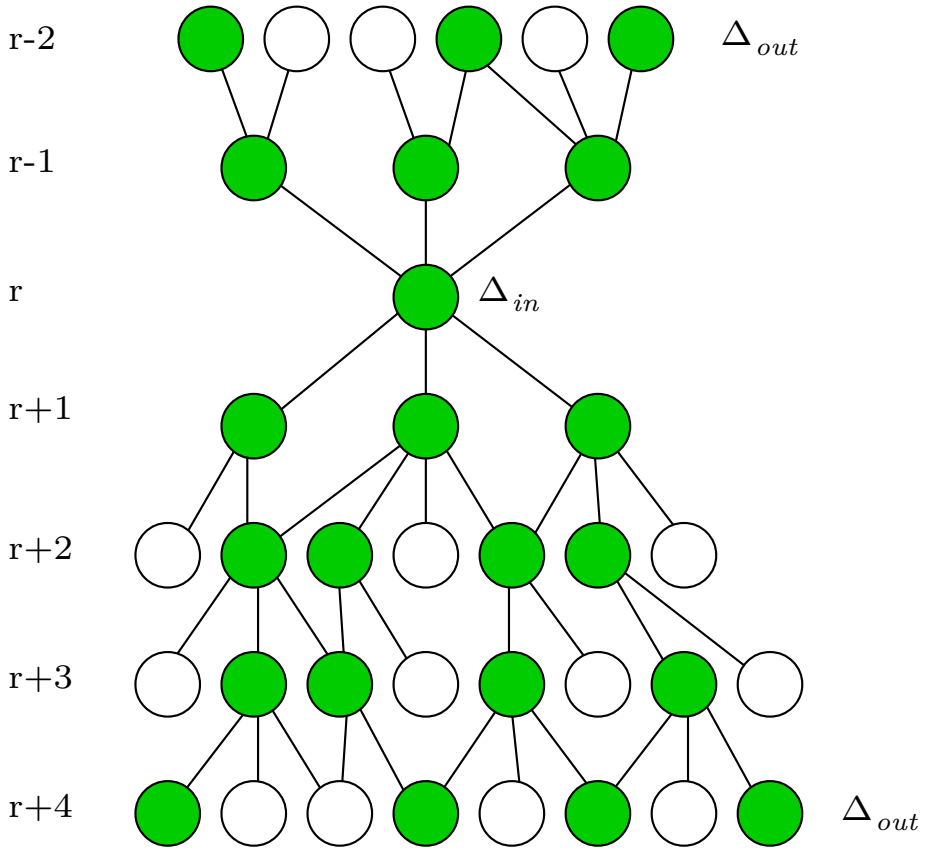
How to Apply Matsui and B&B

- Start from the input difference α
- Propagate in forward and backward direction
- Collect all output difference $\alpha \rightarrow \beta$ and their P
- Use as starting point for the next round in depth-first manner

How to Apply Matsui and B&B (cont'd)

- Searching all possible paths is infeasible
- Prune the search tree
- Define P threshold
- Consider pairs with $P \gg 2^{p-threshold}$ and
- maximum number of characteristics

Branch-and-Bound



Differential Attacks Procedure

1. Collect text pairs
2. Filter out pairs
3. Filter out round keys
4. Test all remaining key candidates by brute-force

Differential Attacks (cont'd)

1. **Collection phase**:
   1. Collect plaintext pairs (P_i, P'_i)
   2. Obtain (C_i, C'_i) ciphertext pairs from encryption oracle

Differential Attacks (cont'd)

2. **Filtering phase**:
   3. Derive all pairs (C_i, C_i') with the correct difference
   4. Store all correct pairs in a list

Differential Attacks (cont'd)

3. **Key Guessing phase**:

5. Guess some key bits
6. For all ciphertext in the list partially decrypt (C_i, C_i')
7. Test for the match, if yes increment the counter
8. Output key candidates with highest counter

Differential Attacks (cont'd)

4. **Brute-force phase**:
   9. Identify correct values for all remaining keys

Section 4

Results

Differential Attacks on Simon

Cipher	Total Rds	Attacked Rds	Data (CP)	Memory (Bytes)	Success Rate
SIMON32/64	32	18	$2^{31.2}$	$2^{15.0}$	0.63
SIMON48/k	36	19	$2^{46.0\dagger}$	$2^{20.0}$	0.98
SIMON64/k	42,44	26	$2^{63.0}$	$2^{31.0}$	0.86
SIMON96/k	52,54	35	$2^{93.2}$	$2^{37.8}$	0.63
SIMON128/k	68,72	46	$2^{125.6}$	$2^{40.6}$	0.63

- CP = chosen plaintexts
- † = chosen ciphertexts

Differential Attacks on Speck

Cipher	Total Rds	Attacked Rds	Data (CP)	Memory (Bytes)	Success Rate
SPECK32/64	22	10	2^{29}	2^{16}	0.99
SPECK48/k	22,23	12	2^{45}	2^{24}	0.99
SPECK64/k	26,27	15	2^{61}	2^{32}	0.99
SPECK96/k	28,29	15	2^{89}	2^{48}	0.99
SPECK128/k	32-34	16	2^{116}	2^{64}	0.99

Rectangle Attack on Speck

Cipher	Total Rds	Attacked Rds	Data (CP)	Memory (Bytes)	Success Rate
SPECK32/64	22	11	$2^{30.1}$	$2^{37.1}$	≈ 1
SPECK48/k	22,23	12	$2^{43.2}$	$2^{45.8}$	≈ 1
SPECK64/k	26,27	14	$2^{63.6}$	$2^{65.6}$	≈ 1
SPECK96/k	28,29	16	$2^{90.9}$	$2^{94.5}$	≈ 1
SPECK128/k	32-34	18	$2^{125.9}$	$2^{121.9}$	≈ 1

Comparison for SIMON

Cipher	Total Rds.	Biryukov		Alkhzaimi		Us	
		Rds.	Pr	Rds.	Pr	Rds.	Pr
SIMON32/64	32	14	$2^{-30.94}$	16	$2^{-29.48}$	18	$2^{-30.22}$
SIMON48/k	36	15	$2^{-42.11}$	18	$2^{-42.6}$	15	$2^{-43.01}$
SIMON64/k	42,44	21	$2^{-61.17}$	24	$2^{-62.0}$	21	$2^{-61.01}$
SIMON96/k	52,54	-	–	29	$2^{-87.5}$	35	$2^{-92.2}$
SIMON128/k	68,72	-	–	40	$2^{-124.8}$	46	$2^{-124.6}$

Comparison for SPECK

Cipher	Total Rds.	Biryukov		Us	
		Rds.	Pr	Rds.	Pr
SPECK32/64	22	9	2^{-31}	10	$2^{-30.99}$
SPECK48/k	22,23	10	$2^{-43.87}$	12	$2^{-40.55}$
SPECK64/k	26,27	13	$2^{-57.70}$	15	$2^{-58.9}$
SPECK96/k	28,29	-	—	15	$2^{-83.98}$
SPECK128/k	32-34	-	—	16	$2^{-111.16}$

Section 5

Conclusion

Conclusion

- Differential attacks on up to half of the rounds for SIMON and SPECK
- SIMON is highly vulnerable against differential cryptanalysis
- Any new analysis on addition-based ARX would be a threat to SPECK
- ThreeFish, 2010, only 24/72 rounds up to now, SPECK, 2013, up to half

Differentials for SIMON32/64

Rd.	ΔL^i	ΔR^i	$\log_2(p)$	**Rd.**	ΔL^i	ΔR^i	$\log_2(p)$
0	0	Δ_6		8	Δ_4	$\Delta_{2,6,14}$	-6
1	Δ_6	0	0	9	$\Delta_{2,14}$	Δ_4	-2
2	Δ_8	Δ_6	-2	10	Δ_0	$\Delta_{2,14}$	-4
3	$\Delta_{6,10}$	Δ_8	-2	11	Δ_{14}	Δ_0	-2
4	Δ_{12}	$\Delta_{6,10}$	-4	12	0	Δ_{14}	-2
5	$\Delta_{6,10,14}$	Δ_{12}	-2	13	Δ_{14}	0	0
6	$\Delta_{0,8}$	$\Delta_{6,10,14}$	-6	14			
7	$\Delta_{2,6,14}$	$\Delta_{0,8}$	-4	15			
Σ							-36
Σ_{acc}							-30.22

- $\sum$: the total probability of the full characteristic
- $\sum_{acc}$: the accumulated probability of all found trails from start to the end

Differentials for SPECK32/64

Rd.	ΔL^i	ΔR^i	$\log_2(p)$	**Rd.**	ΔL^i	ΔR^i	$\log_2(p)$
0	$\Delta_{5,6,9,11}$	$\Delta_{0,2,9,14}$		6	Δ_{15}	$\Delta_{1,3,10,15}$	-2
1	$\Delta_{0,4,9}$	$\Delta_{2,9,11}$	-5	7	$\Delta_{1,3,8,10,15}$	$\Delta_{5,8,10,12,15}$	-4
2	$\Delta_{11,13}$	Δ_{4}	-4	8	$\Delta_{1,3,5,15}$	$\Delta_{3,5,7,10,12,14,15}$	-6
3	Δ_{6}	0	-2	9	$\Delta_{3,5,7,8,15}$	$\Delta_{0,1,3,8,9,12,14,15}$	-7
4	Δ_{15}	Δ_{15}	0	10			
5	$\Delta_{8,15}$	$\Delta_{1,8,15}$	-1				
Σ							-31
Σ_{acc}							-30.99