Differential Analaysis of Block Ciphers SIMON and SPECK

Alex Biryukov, Arnab Roy, Vesselin Velichkov

UNIVERSITÉ DU LUXEMBOURG

Outline

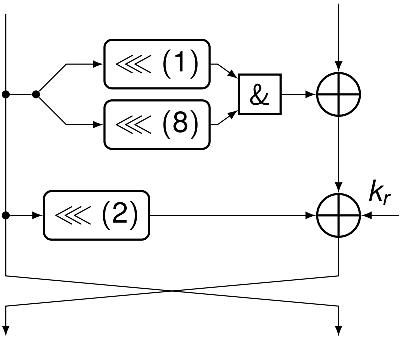
Outline

SIMON AND SPECK

- SIMON , SPECK - proposed in 2013, by a group of researchers from the NSA
- Competitive designs – Simplicity, Efficiency
- Both are constructed on ARX principle
- SIMON – Feistel design with ARX based function
- SPECK – ARX, Resemblance with *Threefish*

SIMON

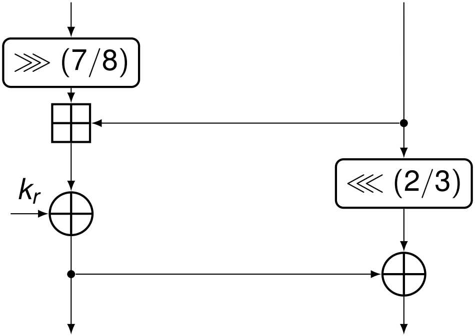
Feistel design with very simple *F*-function



Block Size – 32, 48, 64 with key size 64, 72 or 96, 96 or 128 respectively.

Speck

Round function is similar to Threefish XOR round-key instead of (modular)adding the round-key



Block Size – 32, 48, 64 with key size 64, 72 or 96, 96 or 128 respectively.

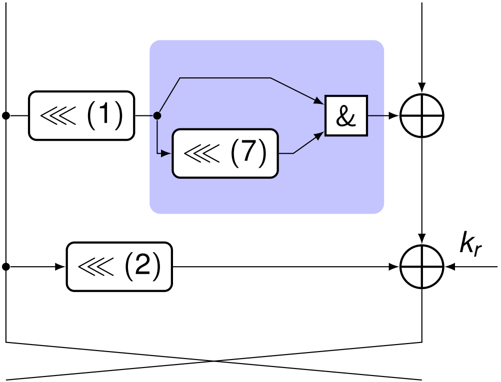
Outline

Outline

SIMON: DP of A(nd)RX round function

$$\Pr(\alpha \to \gamma) =$$

$$\frac{\left|\{x : (x \wedge (x \lll r)) \oplus ((x \oplus \alpha) \wedge ((x \oplus \alpha) \lll r)) = \gamma\}\right|}{2^n}$$



DP: Path counting in DAG

Find DP $\iff$ Count paths in a DAG

DP: Path counting in DAG

Find DP $\iff$ Count paths in a DAG (Example: n=5, r=2)

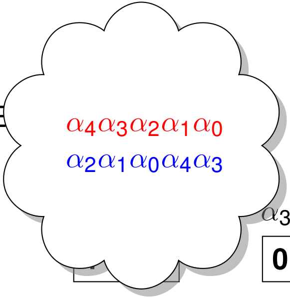
DP: Path counting in DAG

Find DP $\iff$ Count paths in a DAG (Example: n=5, r=2)

$\alpha_0\alpha_3$	γ_0	$\alpha_2\alpha_0$	γ_2	$\alpha_4\alpha_2$	γ_4	$\alpha_1\alpha_4$	γ_1	$\alpha_3\alpha_1$	γ_3
0 0	**0**	**1 0**	**0**	**0 1**	**0**	**1 0**	**0**	**0 1**	**0**

DP: Path counting in DAG

Find DP $\iff$ Count paths in a DAG (E



$\alpha_0\alpha_3$	γ_0
0 0	**0**

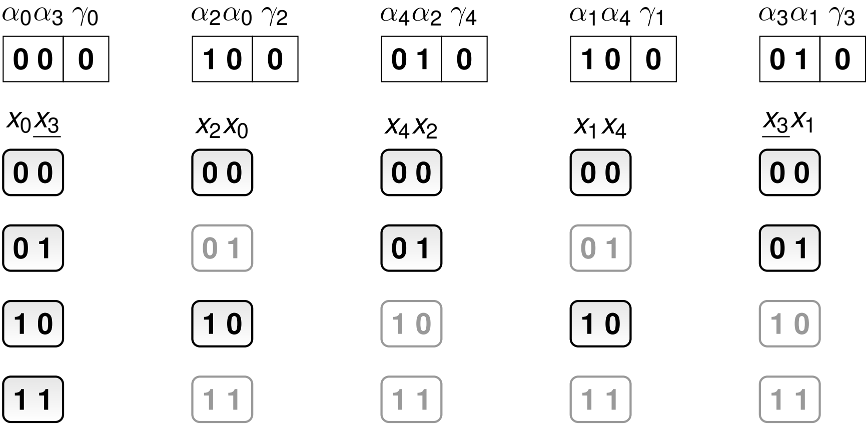
$\alpha_2\alpha_0$	γ_2
1 0	**0**

$\alpha_4\alpha_2$	γ_4
0 1	**0**

$\alpha_3\alpha_1$	γ_3
0 1	**0**

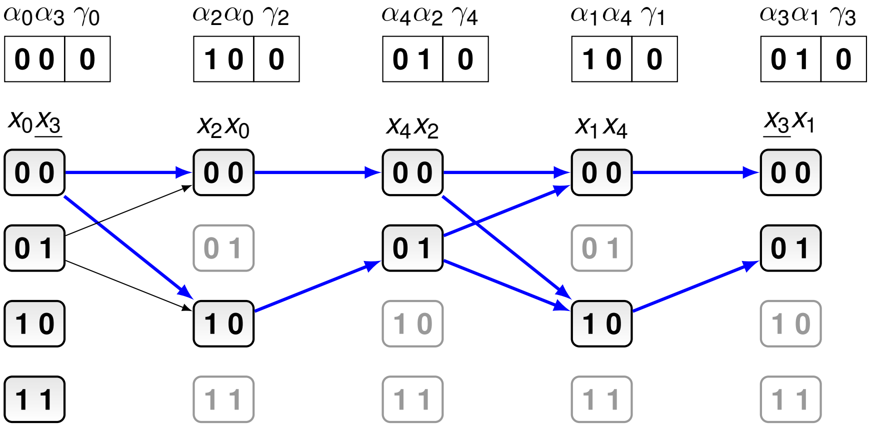
DP: Path counting in DAG

Find DP $\Longleftrightarrow$ Count paths in a DAG (Example: n=5, r=2)

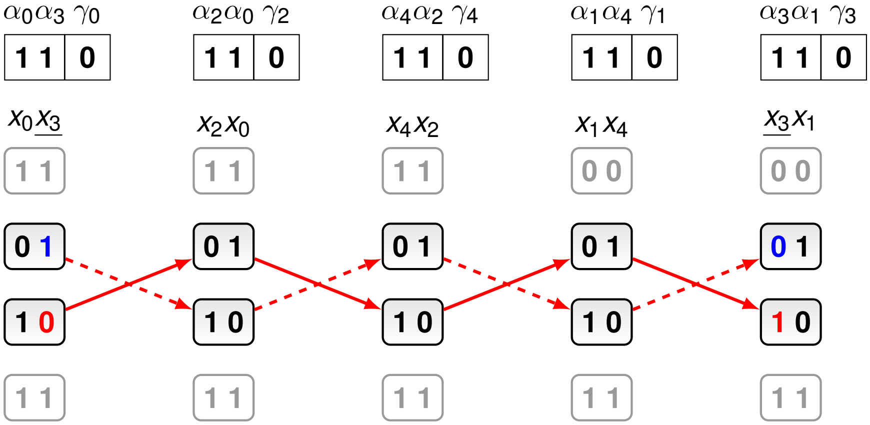


DP: Path counting in DAG

Find DP $\iff$ Count paths in a DAG (Example: n=5, r=2)



Example: Impossible I/O Difference



Outline

About Extending Matsui's Search for ARX

- **Matsui**[EuroCrypt'94] : while selecting DP of round ℓ check $p = p_1 \cdot p_2 \ldots p_\ell \cdot B_{n-\ell} \geq \overline{B_n}$, if $p \geq \overline{B_n}$ update the bound
- Problem: DDT requires exponential memory for ARX designs

About Extending Matsui's Search for ARX

- **Matsui**[EuroCrypt'94] : while selecting DP of round ℓ check $p = p_1 \cdot p_2 \ldots p_\ell \cdot B_{n-\ell} \geq \overline{B_n}$, if $p \geq \overline{B_n}$ update the bound
- Problem: DDT requires exponential memory for ARX designs
- **Biryukov-Velichkov** [CT-RSA'14]: Use partial DDT table for ARX (*Threshold Search*)
- The pDDT - $\mathcal{D}$ contains $\alpha \to \beta$ iff $p(\alpha \to \beta) \geq p_\tau$

About Extending Matsui's Search for ARX

- **Matsui**[EuroCrypt'94] : while selecting DP of round ℓ check $p = p_1 \cdot p_2 \ldots p_\ell \cdot B_{n-\ell} \geq \overline{B_n}$, if $p \geq \overline{B_n}$ update the bound
- Problem: DDT requires exponential memory for ARX designs
- **Biryukov-Velichkov** [CT-RSA'14]: Use partial DDT table for ARX (*Threshold Search*)
- The pDDT - $\mathcal{D}$ contains $\alpha \rightarrow \beta$ iff $p(\alpha \rightarrow \beta) \geq p_\tau$
- While searching, if some $(\alpha \rightarrow \beta) \notin \mathcal{D}$, then it is possible to take several options e.g. Choose greedily, Search all possible, Highway-Country Road approach

Using the *Threshold Search* for ARX

- Parameters in *Threshold Search*: Size of pDDT (and p_τ), precomputaion time for pDDT
- Lower p_τ can intuitively lead to better result; But increases the search complexity and size of the pDDT table

Using the *Threshold Search* for ARX

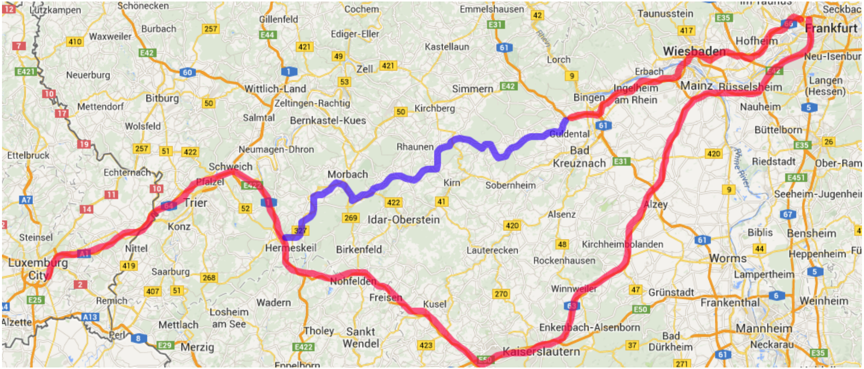
- Parameters in *Threshold Search*: Size of pDDT (and p_τ), precomputaion time for pDDT
- Lower p_τ can intuitively lead to better result; But increases the search complexity and size of the pDDT table
- *Including New Entries*: The new transitions $(\alpha \rightarrow \beta) \notin \mathcal{D}$ are added to a *secondary* table – $\mathcal{D}'$

Using the *Threshold Search* for ARX

- Parameters in *Threshold Search*: Size of pDDT (and p_τ), precomputaion time for pDDT
- Lower p_τ can intuitively lead to better result; But increases the search complexity and size of the pDDT table
- *Including New Entries*: The new transitions $(\alpha \to \beta) \notin \mathcal{D}$ are added to a *secondary* table – $\mathcal{D}'$
- Restrict size of $\mathcal{D}'$ – By Hamming weight of the differences; Used for SPECK
- Another way – select $(\alpha \to \beta)$ at round ℓ such that at round $\ell + 1$ there is at least one transition $\in \mathcal{D}$; Used for SIMON together with Hamming weight

Highway-Country Road Analogy

Route: Luxembourg to Frankfurt



The Highway only route – 2hr 46min
Highway-Country Road – 2hr 31min

Outline

Extension for Differential: Clustering Trails

- We extend the *Threshold Search* for clustering trails.
- **Main Idea**: for round ℓ select transition with p_ℓ:
  $(p_1 \cdot p_2 \ldots p_{\ell-1} p_\ell \cdot B_{n-\ell}) \geq \epsilon \cdot B_n$
- Input: Best trail found by *threshold Search*, pDDT table, ϵ

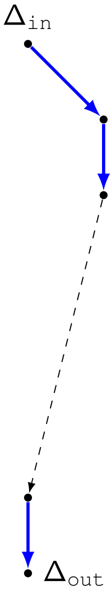
Extension for Differential: Clustering Trails

- We extend the *Threshold Search* for clustering trails.
- **Main Idea**: for round ℓ select transition with p_ℓ:
  $(p_1 \cdot p_2 \ldots p_{\ell-1} p_\ell \cdot B_{n-\ell}) \geq \epsilon \cdot B_n$
- Input: Best trail found by *threshold Search*, pDDT table, ϵ
- **Efficiency**: Hamming weight and probability constraints can be applied
- Difference with branch-and-bound – We prune the search tree by limiting the search to ϵ region of the best known probability

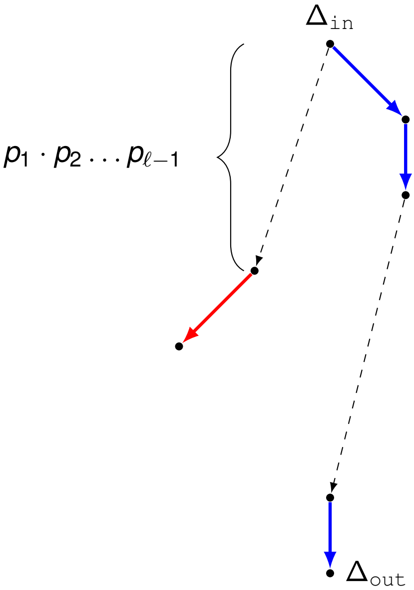
Extension for Differential: Clustering Trails

- We extend the *Threshold Search* for clustering trails.
- **Main Idea**: for round ℓ select transition with p_ℓ:
  $(p_1 \cdot p_2 \ldots p_{\ell-1} p_\ell \cdot B_{n-\ell}) \geq \epsilon \cdot B_n$
- Input: Best trail found by *threshold Search*, pDDT table, ϵ
- **Efficiency**: Hamming weight and probability constraints can be applied
- Difference with branch-and-bound – We prune the search tree by limiting the search to ϵ region of the best known probability
- We apply this technique to both SIMON and SPECK

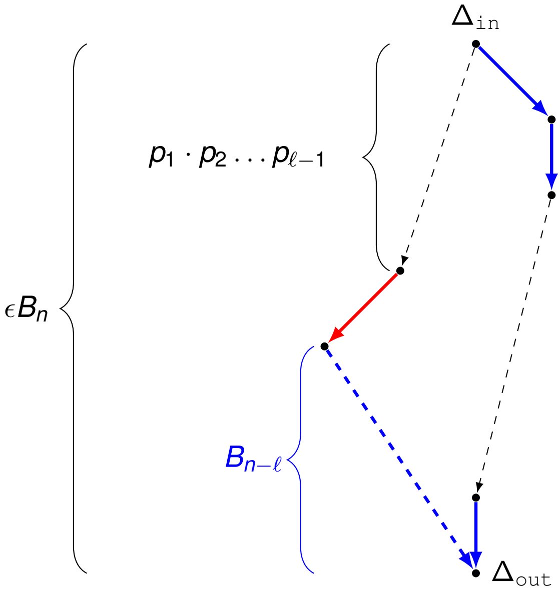
An overview: Differential Search



An overview: Differential Search



An overview: Differential Search



Search Results

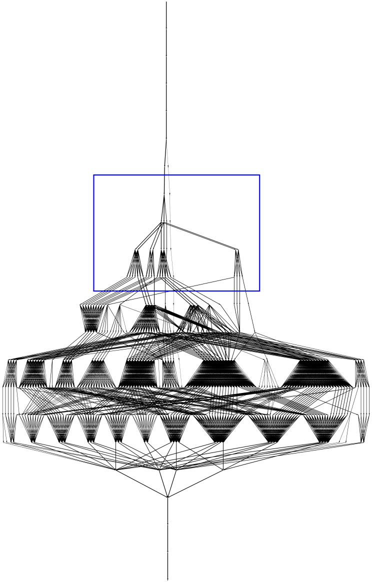
Cipher	# rounds	$\log_2 p$, trail	$\log_2 p$, diff.	# trails
SIMON32	13	**−36**	**−29.69**	**45083**
			−28.11	full search
		−36	−30.20	–
	14		**−30.94**	full search
SIMON48	15	**−48**	**−42.11**	**112573**
		−52	−43.01	–
SIMON64	20	**−70**	**−58.68**	**210771**
		−70	−59.01	–
	21	−72	**−60.53**	**337309**
		−72	−61.01	–
SPECK32	9	**−30**	**−30**	1
SPECK48	10	**−40**	**−39.75**	**137**
			−40.55	–
	11	**−47**	**−46.48**	**384**
SPECK64	13	**−58**	**−57.70**	48
			−58.90	–
	14	**−60**	**−59.11**	**125**

Outline

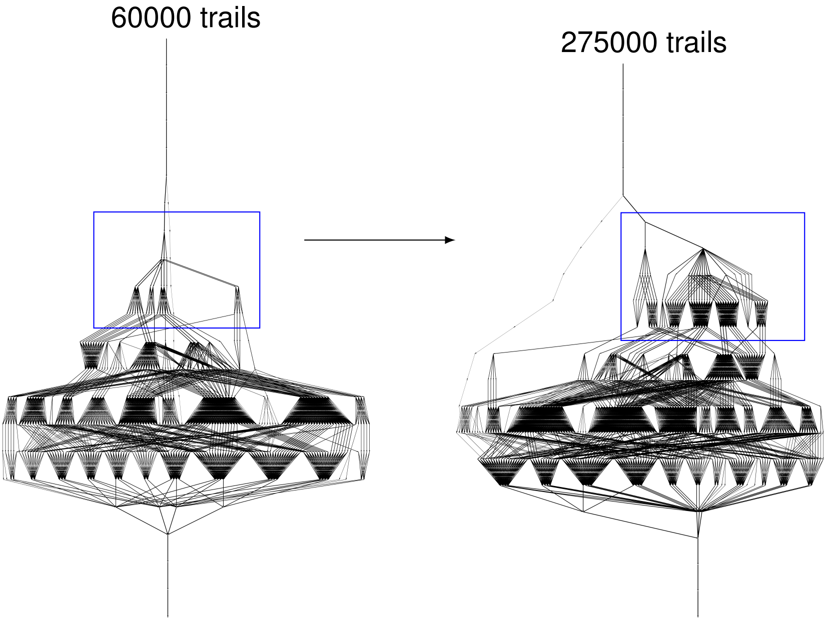
Outline

The differential graph for SIMON

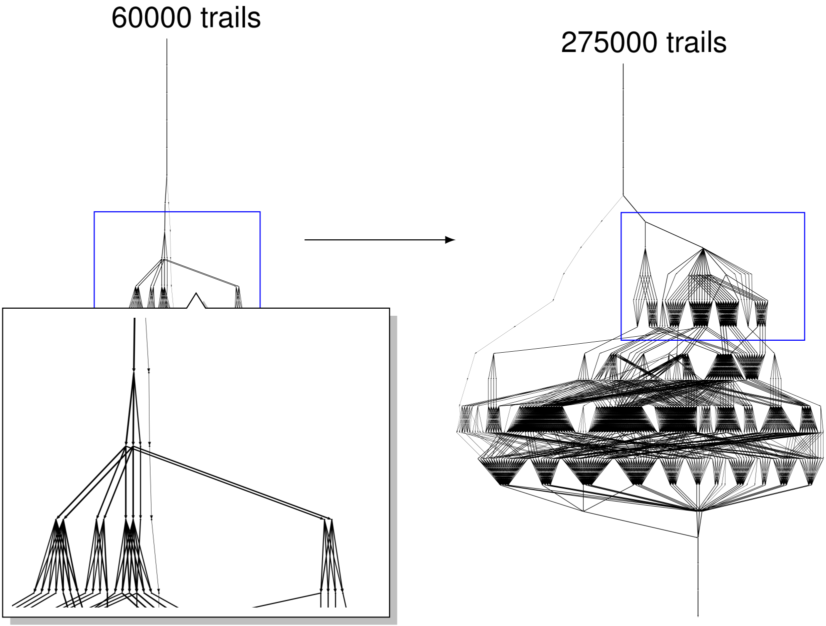
60000 trails



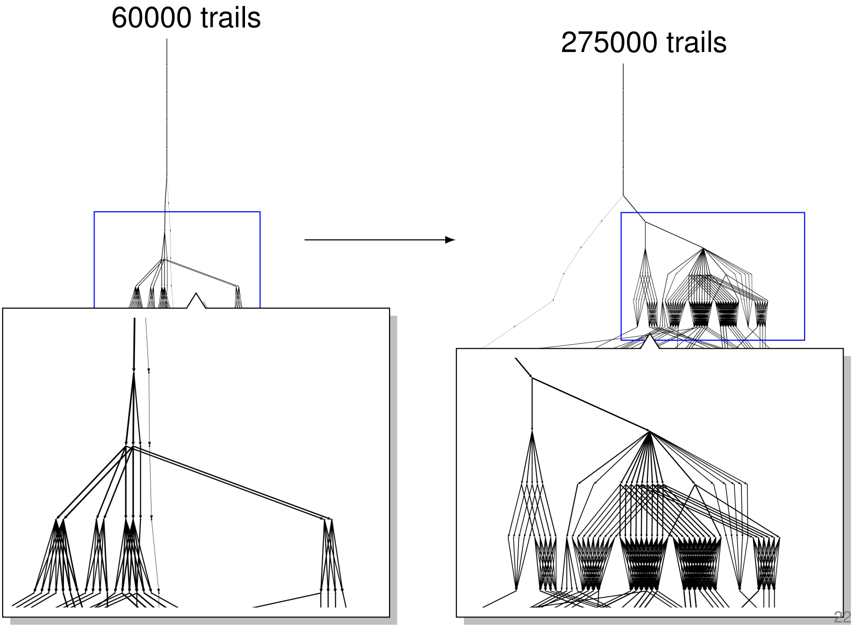
The differential graph for SIMON



The differential graph for SIMON



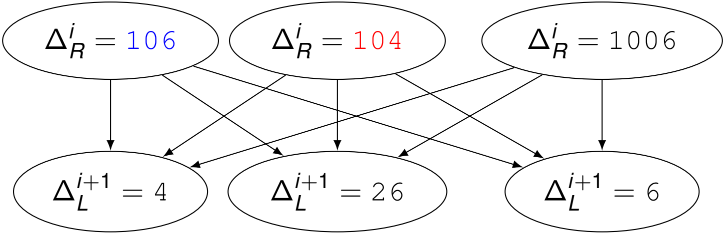
The differential graph for SIMON



Bipartite Subgraph of Trails

Feistel: $\Delta_L^i = 11 \implies \Delta_R^{i+1} = 11$

$\Delta_L^i \xrightarrow{f} \nabla = \{000{*}\ \ 000{*}\ \ 00{*}0\ \ 00{*}0\}$



$$\nabla \oplus (\Delta_L^i \lll 2) \oplus \Delta_R^i) = \Delta_L^{i+1}$$

$$120 \oplus (22) \oplus 106 = 4$$

$$122 \oplus (22) \oplus 104 = 4$$

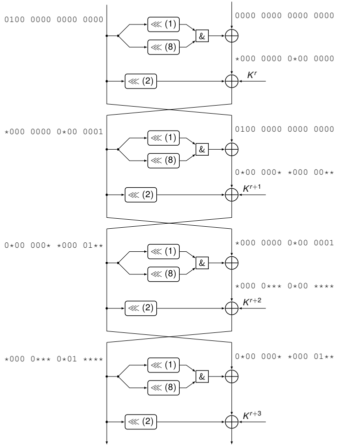
Outline

uni.lu UNIVERSITÉ DU LUXEMBOURG

Outline

19 Round SIMON32: Practical Attack

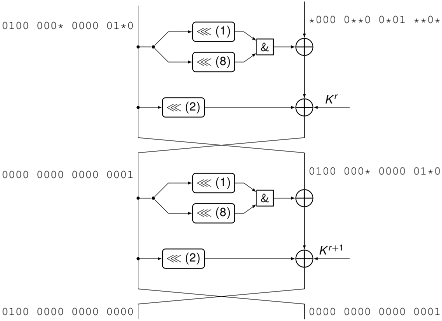
Use 13 round differential with probability $\approx 2^{-28.11}$, Add 2 rounds on top, 4 rounds at the end



Guess 25 bits(and linear combinations) from K^{18}, K^{17}, K^{16}

Attack on SIMON32

- Identify pairs satisfying top 2 rounds truncated difference – guess 2 bits of K^0



Attack on SIMON32

We use four differentials

$$\mathcal{D}_1 : (\texttt{2000}, \texttt{8000}) \rightarrow (\texttt{2000}, \texttt{0})$$
$$\mathcal{D}_2 : (\texttt{4000}, \texttt{0001}) \rightarrow (\texttt{4000}, \texttt{0})$$
$$\mathcal{D}_3 : (\texttt{0004}, \texttt{0010}) \rightarrow (\texttt{0004}, \texttt{0})$$
$$\mathcal{D}_4 : (\texttt{0008}, \texttt{0020}) \rightarrow (\texttt{0008}, \texttt{0})$$

Truncated diffrence for top 2 round

$$(\texttt{0010 0000 }\star\texttt{000 001}\star, \star\star\texttt{00 00}\star\star\texttt{ 00}\star\texttt{0 1}\star\star\texttt{0})$$
$$(\texttt{0100 000}\star\texttt{ 0000 01}\star\texttt{0}, \star\texttt{000 0}\star\star\texttt{0 0}\star\texttt{01 }\star\star\texttt{0}\star)$$
$$(\texttt{000}\star\texttt{ 0000 01}\star\texttt{0 0100}, \texttt{0}\star\star\texttt{0 0}\star\texttt{01 }\star\star\texttt{0}\star\texttt{ }\star\texttt{000})$$
$$(\texttt{00}\star\texttt{0 0000 1}\star\texttt{00 1000}, \star\star\texttt{00 }\star\texttt{01}\star\texttt{ }\star\texttt{0}\star\star\texttt{ 0000})$$

Attack on SIMON32

- Data Collection: Encrypt structure of size 2^{30}
- Filtering: $2^{30-18} = 2^{12}$ pairs remain for any $\mathcal{D}_i$
- Counting : For each $\mathcal{D}_i$
  - 2^{12} pairs, 25 bit guessing
  - 2^{17} candidates for 25 bits
- Intersection of Counters:
  - $\mathcal{D}_1, \mathcal{D}_2$ – 19 common bits (guessed) $\implies$ 2^{15} for 35 bits
  - Intersection: $\mathcal{D}_3, \mathcal{D}_1, \mathcal{D}_2$ – 20 bits common
- 2^{12} candidates for 42 bits
- Intersection with $\mathcal{D}_4$ $\implies$ 2^7 candidates for 47 bits **But** 39 from last 4 rounds
- By brute-forcing rest — total $2^{25+7} = 2^{32}$ key guesses

Attack on SIMON32

UNIVERSITÉ DU LUXEMBOURG

- Data Collection: Encrypt structure of size 2^{30}
- Filtering: $2^{30-18} = 2^{12}$ pairs remain for any $\mathcal{D}_i$
- Counting : For each $\mathcal{D}_i$
  - 2^{12} pairs, 25 bit guessing
  - 2^{17} candidates for 25 bits
- Intersection of Counters:
  - $\mathcal{D}_1, \mathcal{D}_2$ – 19 common bits (guessed) $\implies$ 2^{15} for 35 bits
  - Intersection: $\mathcal{D}_3, \mathcal{D}_1, \mathcal{D}_2$ – 20 bits common
- 2^{12} candidates for 42 bits
- Intersection with $\mathcal{D}_4$ $\implies$ 2^7 candidates for 47 bits **But** 39 from last 4 rounds
- By brute-forcing rest — total $2^{25+7} = 2^{32}$ key guesses

Attack on SIMON32

- Data Collection: Encrypt structure of size 2^{30}
- Filtering: $2^{30-18} = 2^{12}$ pairs remain for any $\mathcal{D}_i$
- Counting : For each $\mathcal{D}_i$
  - 2^{12} pairs, 25 bit guessing
  - 2^{17} candidates for 25 bits
- Intersection of Counters:
  - $\mathcal{D}_1, \mathcal{D}_2$ – 19 common bits (guessed) $\implies$ 2^{15} for 35 bits
  - Intersection: $\mathcal{D}_3, \mathcal{D}_1, \mathcal{D}_2$ – 20 bits common
- 2^{12} candidates for 42 bits
- Intersection with $\mathcal{D}_4$ $\implies$ 2^7 candidates for 47 bits **But** 39 from last 4 rounds
- By brute-forcing rest — total $2^{25+7} = 2^{32}$ key guesses

Attack on SIMON32

- Data Collection: Encrypt structure of size 2^{30}
- Filtering: $2^{30-18} = 2^{12}$ pairs remain for any $\mathcal{D}_i$
- Counting : For each $\mathcal{D}_i$
  - 2^{12} pairs, 25 bit guessing
  - 2^{17} candidates for 25 bits
- Intersection of Counters:
  - $\mathcal{D}_1, \mathcal{D}_2$ – 19 common bits (guessed) $\implies$ 2^{15} for 35 bits
  - Intersection: $\mathcal{D}_3, \mathcal{D}_1, \mathcal{D}_2$ – 20 bits common
- 2^{12} candidates for 42 bits
- Intersection with $\mathcal{D}_4$ $\implies$ 2^7 candidates for 47 bits **But** 39 from last 4 rounds
- By brute-forcing rest — total $2^{25+7} = 2^{32}$ key guesses

Attack on SIMON32

- Data Collection: Encrypt structure of size 2^{30}
- Filtering: $2^{30-18} = 2^{12}$ pairs remain for any $\mathcal{D}_i$
- Counting : For each $\mathcal{D}_i$
  - 2^{12} pairs, 25 bit guessing
  - 2^{17} candidates for 25 bits
- Intersection of Counters:
  - $\mathcal{D}_1, \mathcal{D}_2$ – 19 common bits (guessed) $\implies$ 2^{15} for 35 bits
  - Intersection: $\mathcal{D}_3, \mathcal{D}_1, \mathcal{D}_2$ – 20 bits common
- 2^{12} candidates for 42 bits
- Intersection with $\mathcal{D}_4$ $\implies$ 2^7 candidates for 47 bits **But** 39 from last 4 rounds
- By brute-forcing rest — total $2^{25+7} = 2^{32}$ key guesses

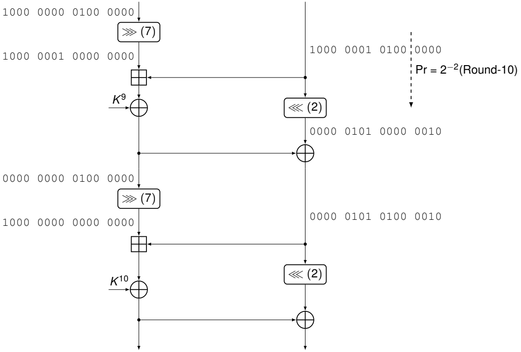
Attack on SIMON32

- Data Collection: Encrypt structure of size 2^{30}
- Filtering: $2^{30-18} = 2^{12}$ pairs remain for any $\mathcal{D}_i$
- Counting : For each $\mathcal{D}_i$
  - 2^{12} pairs, 25 bit guessing
  - 2^{17} candidates for 25 bits
- Intersection of Counters:
  - $\mathcal{D}_1, \mathcal{D}_2$ – 19 common bits (guessed) $\implies$ 2^{15} for 35 bits
  - Intersection: $\mathcal{D}_3, \mathcal{D}_1, \mathcal{D}_2$ – 20 bits common
- 2^{12} candidates for 42 bits
- Intersection with $\mathcal{D}_4$ $\implies$ 2^7 candidates for 47 bits **But** 39 from last 4 rounds
- By brute-forcing rest — total $2^{25+7} = 2^{32}$ key guesses

Outline

Attack on SPECK32

- Use 9 round differential with $p = 2^{-30}$; Add one round each on top and at the end



- Guess 16 bits from K^{10}, 11 bits from K^9, 1 carry bit

Attack on SPECK32

- Verify the difference at the end of round 9
- Keep a counter of size 2^{28}
- Expect 2^{18} counters with 4 increments
- Bruteforce rest of the $64 - 27 = 37$ bits of last 4 round-keys
- Total number of key guessing $2^{18+37} = 2^{55}$

Outline

Summary of Attacks

Cipher	Key Size	Rounds Total	Rounds Attacked	**Our Results** Time	Data	Known Result Time	Data
SIMON32	64	32	19	2^{32}	2^{31}	–	–
SIMON48	72	36	20	2^{52}	2^{46}	–	–
	96	36	20	2^{75}	2^{46}	–	–
SIMON64	96	42	26	2^{89}	2^{63}	2^{94}	2^{63}*
	128	44	26	2^{121}	2^{63}	2^{126}	2^{63}*
SPECK32	64	22	11	2^{55}	2^{31}	–	–
SPECK48	72/96	22	12	2^{43}	2^{43}	$2^{45.3}$	2^{45}
SPECK64	96	26	16	2^{63}	2^{63}	–	–
	128	27	16	2^{63}	2^{63}	–	–

Outline

Summary

- Analysis and Linear time (in word size) Algorithm to find DP of SIMON round function
- Threshold Search with Highway-Country road approach for analysing SIMON and SPECK
- Extend the *Threshold Search* technique for **Differential Search**
- Improved differentials for SIMON and SPECK
- All these methods are generic and can be used to analyse ARX designs
- Additionally, use the differentials for key recovery attack on reduced round SIMON and SPECK