Differential-Linear Cryptanalysis of ASCON: Theory vs. Practice

Assoc. Prof. Dr. **Cihangir TEZCAN**

MIDDLE EAST TECHNICAL UNIVERSITY

Informatics Institute, Department of Cyber Security

NIST Lightweight Cryptography Workshop

22 June 2023

This work has been supported by TUBITAK 1001 Project under the grant number 121E228 and by Middle East Technical University Scientific Research Projects Coordination Unit under grant number AGEP-704-2023-11294.

Theory vs. Pratice

“In theory, theory and practice are the same. In practice, they are not.”

Many cryptanalysis results are obtained theoretically but

1. they may **not** work in practice

Theory vs. Pratice

"In theory, theory and practice are the same. In practice, they are not."

Many cryptanalysis results are obtained theoretically but

1. they may **not** work in practice
2. they may require **more** data/time/memory than expected

Theory vs. Pratice

"In theory, theory and practice are the same. In practice, they are not."

Many cryptanalysis results are obtained theoretically but

1. they may **not** work in practice
2. they may require **more** data/time/memory than expected
3. they may require **less** data/time/memory than expected

Theory vs. Pratice

"In theory, theory and practice are the same. In practice, they are not."

Many cryptanalysis results are obtained theoretically but

1. they may **not** work in practice
2. they may require **more** data/time/memory than expected
3. they may require **less** data/time/memory than expected

Toy versions of the distinguishers and attacks must be experimentally verified

ASCON

ASCON

- Designed by Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schlaffer
- First choice for *Lightweight Applications* in CAESAR Competition
- Type: Sponge construction
- Primitive: SPN
  - **Block size:** 64 or 128 bits
  - **State size:** 320 bits
  - **Key:** 128 bits (initial version supported 96 bits)
  - **Nonce:** 128 bits
  - **Tag:** 128 bits
  - **Rounds:** 12 (initialization) or 6 (encryption)

DryGASCON

DryGASCON

- Designed by Sebastien Riou
- Type: Sponge construction
- Primitive: ASCON (slightly different permutation) and DrySponge
  - **Block size:** 128 bits
  - **State size:** 320 or 576 bits
  - **Key:** 128 or 256 bits
  - **Nonce:** 128 or 256 bits
  - **Tag:** 128 bits
  - **Rounds:** 11 or 12 (depends on key length)

ASCON

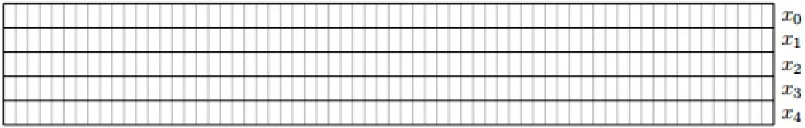

Figure: 320-bit state ASCON

ASCON

round	constant	round	constant
0	0x0000000000000000000f0	6	0x0000000000000000000096
1	0x0000000000000000000e1	7	0x0000000000000000000087
2	0x0000000000000000000d2	8	0x0000000000000000000078
3	0x0000000000000000000c3	9	0x0000000000000000000069
4	0x0000000000000000000b4	10	0x000000000000000000005a
5	0x0000000000000000000a5	11	0x000000000000000000004b

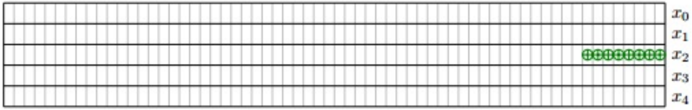

Figure: Adding constants

ASCON

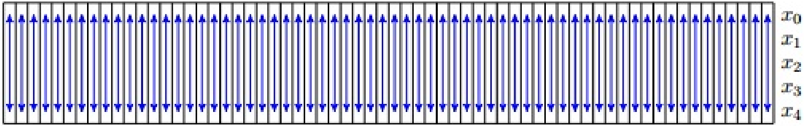

Table: ASCON's 5 × 5 S-box in hexadecimal notation

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	4	B	1F	14	1A	15	9	2	1B	5	8	12	1D	3	6	1C
x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
S(x)	1E	13	7	E	0	D	11	18	10	C	1	19	16	A	F	17

ASCON

$$
\begin{aligned}
\Sigma_0(x_0) &= x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)\\
\Sigma_1(x_1) &= x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)\\
\Sigma_2(x_2) &= x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)\\
\Sigma_3(x_3) &= x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)\\
\Sigma_4(x_4) &= x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)
\end{aligned}
$$

Figure: Linear Diffusion layer ASCON

ASCON

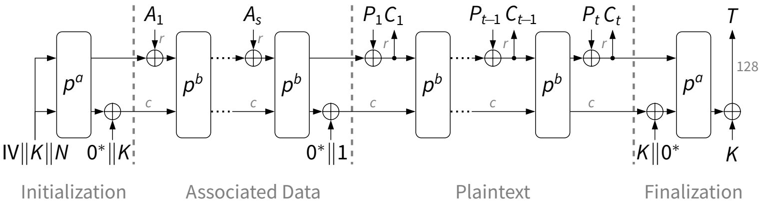

Figure: The encryption of ASCON. p^a means the permutation operation p is performed a times. We have $a = 12$ and $b = 6$.

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis

- **Differential cryptanalysis** introduces an input difference and after r_1 rounds of encryption, aims to observe some output difference with probability p

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis

- **Differential cryptanalysis** introduces an input difference and after r_1 rounds of encryption, aims to observe some output difference with probability p
- **Linear cryptanalysis** uses an r_2-round linear approximation where XOR of masked input and output bits equal to zero with probability $1/2 + q$

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis

- **Differential cryptanalysis** introduces an input difference and after r_1 rounds of encryption, aims to observe some output difference with probability p
- **Linear cryptanalysis** uses an r_2-round linear approximation where XOR of masked input and output bits equal to zero with probability $1/2 + q$
- Differential-Linear cryptanalysis combines a differential and a linear approximation to obtain an $r_1 + r_2$-round distinguisher

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis

- **Differential cryptanalysis** introduces an input difference and after r_1 rounds of encryption, aims to observe some output difference with probability p
- **Linear cryptanalysis** uses an r_2-round linear approximation where XOR of masked input and output bits equal to zero with probability $1/2 + q$
- Differential-Linear cryptanalysis combines a differential and a linear approximation to obtain an $r_1 + r_2$-round distinguisher
- A differential can be combined with a linear approximation where input masked bits of the linear approximation coincide with the output difference bits that have fixed difference

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis

- **Differential cryptanalysis** introduces an input difference and after r_1 rounds of encryption, aims to observe some output difference with probability p
- **Linear cryptanalysis** uses an r_2-round linear approximation where XOR of masked input and output bits equal to zero with probability $1/2 + q$
- Differential-Linear cryptanalysis combines a differential and a linear approximation to obtain an $r_1 + r_2$-round distinguisher
- A differential can be combined with a linear approximation where input masked bits of the linear approximation coincide with the output difference bits that have fixed difference
- The bias of a differential-linear distinguisher is approximately $2pq^2$

Differential-Linear Cryptanalysis

Differential-Linear Cryptanalysis

- **Differential cryptanalysis** introduces an input difference and after r_1 rounds of encryption, aims to observe some output difference with probability p
- **Linear cryptanalysis** uses an r_2-round linear approximation where XOR of masked input and output bits equal to zero with probability $1/2 + q$
- Differential-Linear cryptanalysis combines a differential and a linear approximation to obtain an $r_1 + r_2$-round distinguisher
- A differential can be combined with a linear approximation where input masked bits of the linear approximation coincide with the output difference bits that have fixed difference
- The bias of a differential-linear distinguisher is approximately $2pq^2$
- Data complexity is $\mathcal{O}(p^{-2}q^{-4})$ chosen plaintexts

Experiment on SERPENT Differential-Linear Distinguisher

Table: Experimental verification of the first r rounds of the 9-round differential-linear distinguisher of (Dunkelman, Indesteege, and Keller, 2008) on SERPENT block cipher. We performed the experiments using 100 randomly chosen keys with 2^{50} random data pairs.

r	Theoretical Bias	Experimental Bias	Gain
4	2^{-15}	$2^{-13.73}$	$2^{1.27}$

Experiment on SERPENT Differential-Linear Distinguisher

Table: Experimental verification of the first r rounds of the 9-round differential-linear distinguisher of (Dunkelman, Indesteege, and Keller, 2008) on SERPENT block cipher. We performed the experiments using 100 randomly chosen keys with 2^{50} random data pairs.

r	Theoretical Bias	Experimental Bias	Gain
4	2^{-15}	$2^{-13.73}$	$2^{1.27}$
5	2^{-19}	$2^{-17.63}$	$2^{1.37}$

Experiment on SERPENT Differential-Linear Distinguisher

Table: Experimental verification of the first r rounds of the 9-round differential-linear distinguisher of (Dunkelman, Indesteege, and Keller, 2008) on SERPENT block cipher. We performed the experiments using 100 randomly chosen keys with 2^{50} random data pairs.

r	Theoretical Bias	Experimental Bias	Gain
4	2^{-15}	$2^{-13.73}$	$2^{1.27}$
5	2^{-19}	$2^{-17.63}$	$2^{1.37}$
6	2^{-27}	$2^{-25.61}$	$2^{1.39}$

Undisturbed Bits of ASCON

Table: Undisturbed bits of DRYGASCON and ASCON's 5x5 S-box

Input Difference	Output Difference	Input Difference	Output Difference
00001	?1???	10000	?10??
00010	1???1	10001	10??1
00011	???0?	10011	0???0
00100	??110	10100	0?1??
00101	1????	10101	????1
00110	????1	10110	1????
00111	0??1?	10111	????0
01000	??11?	11000	??1??
01011	???1?	11100	??0??
01100	??00?	11110	?1???
01110	?0???	11111	?0???
01111	?1?0?		

Table: ASCON's 5 × 5 S-box in hexadecimal notation

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	4	B	1F	14	1A	15	9	2	1B	5	8	12	1D	3	6	1C
x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
S(x)	1E	13	7	E	0	D	11	18	10	C	1	19	16	A	F	17

2-Round Differential Distinguisher for ASCON (Tezcan 2020)

Table: Our 2-round truncated differential Δ_2 with probability one for Ascon. S and P represent the result of substitution and permutation layers, respectively

	2-Round Truncated Differential Δ_2
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
I	0000000000000000000000000000000000000000000000000000000000000000
	0000000001000000000000000000000000000000000000000000000000000000
	0000000001000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
S_1	000000000?000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000?00000000?00000000000000000000000000
	000000?00?00000000000000000000000000000000000000?000000000000000
P_1	000000000??0000?000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	000000000?000000?000000000000000000000000000000000?0000000000000
	000000?00??0000??00000000000?00000000?0000000000?0?0000000000000
	000000?00??0000??00000000000?00000000?0000000000?0?0000000000000
S_2	000000?00??0000??0000000000000000000000000000000?0?0000000000000
	000000?00??0000??00000000000?00000000?0000000000?0?0000000000000
	000000?00?000000?00000000000?00000000?0000000000?0?0000000000000
	0?0?0??00??0?0???00000000?00??0000??0??0000??00??0?00000?0000000
	000?00??0??0??0??000000?0?00?00000?00?0000000?0????000??00000000
P_2	000000??0????00???000??0000000000000000000000000???00?0?00000000
	0?0?00?00??0000??00??00?0????000??000??000000?0??0?000?000?0?000
	00000??00?000??0?000000?0?0??000000?0?000000?00??0?0000?0?000000

2-Round Linear Distinguisher for ASCON

Table: Type-II linear characteristic for 2-round ASCON-128 permutation with bias 2^{-8} in hexadecimal notation

Round	State				
0	....	...........2.4..	...........2.4.1	....2.........8.	....2.........8.
1	....	....	....	1	1
2	9224b6d24b6eda49	....	....	....	....

4-Round Differential-Linear Distinguisher of ASCON

	2-Round Truncated Differential Δ_2
I	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000001000000000000000000000000000000000000000000000000000000 0000000001000000000000000000000000000000000000000000000000000000
S_1	000000000?000000000000000000000000000000000000000000000000000000 000000000?000000000000000000000000000000000000000000000000000000 000000000?000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 000000000?000000000000000000000000000000000000000000000000000000
P_1	000000000?000000000000000000?00000000?00000000000000000000000000 000000?00?00000000000000000000000000000000000000?000000000000000 000000000??0000?000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 000000000?000000?000000000000000000000000000000000?0000000000000
S_2	000000?00??0000??00000000000?00000000?0000000000?0?0000000000000 000000?00??0000??00000000000?00000000?0000000000?0?0000000000000 000000?00??0000??0000000000000000000000000000000?0?0000000000000 000000?00??0000??00000000000?00000000?0000000000?0?0000000000000 000000?00?000000?00000000000?00000000?0000000000?0?0000000000000
P_2	0?0?0??00??0?0???00000000?00??0000??0??0000??00??0?00000?0000000 000?00??0??0??0??000000?0?00?00000?00?0000000?0????000??00000000 000000??0????00???000??0000000000000000000000000????00?0?0000000 0?0?00?00??0000??00??00?0????000??000??000000?0??0?000?000?0?000 00000??00?000??0?000000?0?0??000000?0?000000?00??0?0000?0?000000

Round	State				
0	....	...........2.4..	...........2.4.1	.....2........8.	.....2........8.
1	....	....	....	1	1
2	9224b6d24b6eda49	....	....	....	....

Theory vs Practice

Theory vs Practice

- The 4-round Differential-Linear distinguisher for ASCON has
  - theoretical bias of 2^{-15}

Theory vs Practice

Theory vs Practice

- The 4-round Differential-Linear distinguisher for Ascon has
  - theoretical bias of 2^{-15}
  - practical bias of 2^{-2}

Theory vs Practice

Theory vs Practice

- The 4-round Differential-Linear distinguisher for Ascon has
  - theoretical bias of 2^{-15}
  - practical bias of 2^{-2}
  - DLCT reduces this to 2^{-5}

Theory vs Practice

Theory vs Practice

- The 4-round Differential-Linear distinguisher for ASCON has
  - theoretical bias of 2^{-15}
  - practical bias of 2^{-2}
  - DLCT reduces this to 2^{-5}
- The gap might be due to
  1. multiple distinguishers

Theory vs Practice

Theory vs Practice

- The 4-round Differential-Linear distinguisher for ASCON has
  - theoretical bias of 2^{-15}
  - practical bias of 2^{-2}
  - DLCT reduces this to 2^{-5}
- The gap might be due to
  1. multiple distinguishers
  2. slow diffusion and confusion

Experimentally Obtained Better Distinguishers for DryGASCON

Round	5- Round Differential-Linear Path for $GASCON_{C5R11}$
I	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000001000000000000000000000000000000000000000
	0000000000000000000000001000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
S1	000000000000000000000000?000000000000000000000000000000000000000
	000000000000000000000000?000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	000000000000000000000000?000000000000000000000000000000000000000
P1	000000?00000000000000000?0000000?0000000000000000000000000000000
	00000000000?000000000000?00000000000000000000000000000?000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	000000000000?00000000000?0000000000000000000000000000000000?0000
S2	000000?0000??00000000000?00000000?00000000000000000000?0000?0000
	000000?0000??00000000000?00000000?00000000000000000000?0000?0000
	00000000000??00000000000?00000000000000000000000000000?0000?0000
	000000?0000??00000000000?00000000?00000000000000000000?0000?0000
	000000?0000??00000000000?00000000?00000000000000000000?0000?0000
P2	?0000??0000??0000000?000???000000?00?0000?00000?0000???0000?0000
	?00000?0000??00000000?00???000??0?00?0000??000?00000?0?0000?0000
	0000000000??0??0000000??00??000000000000000??000000000?0??0?00?0
	0000?0?000???000??000000?0000?0???0000?0000000?0000??0?0000?0000
	?0000??0000??00000000000?0?0000?0?0000000??000??00000??0000?0000

Round	State				
0	1......8.21.1.21	....	....	............18.	1......8.21.11a.
1	....	....	....	.......8..1....1	.......8..1....1
2	....	....	....	....	1
3	....	e37c4f1b6e8d53e6	e.8629e8e4b766af	....	....

Round	2- Round Truncated Differantial for $GASCON_{C5R11}$
I	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000100000000000000000000000
	0000000000000000000000000000000000000000100000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
S1	0000000000000000000000000000000000000000?00000000000000000000000
	0000000000000000000000000000000000000000?00000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000?00000000000000000000000
P1	0000000000000000000000000000000?00000000?00000000000000000?00000
	0000000000?00000000000000000000000000000?000000000000?0000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	00000?0000000000000000000000000000000000?00000000000?00000000000
S2	00000?0000?00000000000000000000?00000000?00000000000??0000?00000
	00000?0000?00000000000000000000?00000000?00000000000??0000?00000
	00000?0000?00000000000000000000000000000?00000000000??0000000000
	00000?0000?00000000000000000000?00000000?00000000000??0000?00000
	00000?0000?00000000000000000000?00000000?00000000000??0000?00000
P2	00000?0000???0000?00000?0000?00??00000???000?0000000??0000??0000
	00000?0000?0?00000?000??0000?00???000??00?00000000??0000?00000
	00?00?0??0?000000000??00000000000000??00??0000000??0??000000000
	?0000?0000?0??0000?0000000?0000?0?0?0000?000000??000???000?0?000
	00000?0000??00000??000??0000000???0000?0?00000000000??0000??0000

Round	State				
0	............18.	1......8.21.1.2.	1......8.21.1.21	............18.	....
1	....	....	....	.......8..1....1	.......8..1....1
2	....	....	....	....	1
3	....	....	e.8629e8e4b766af	c587ed1921757a4e	....

Figure: Bias $2^{-7.98}$, Data 2^{29} and Bias $2^{-5.34}$, Data 2^{17}

Experiments on ASCON

Experiments on 5-round Differential-Linear Attacks (to appear in Springer CCIS Book Series)

By keeping the linear approximation fixed, we performed experiments by introducing input difference to every single S-box

Input Difference	Best biases
00011	$2^{-11.91}$, $2^{-14.87}$, $2^{-15.05}$, and $2^{-8.03}$

Experiments on Ascon

Experiments on 5-round Differential-Linear Attacks (to appear in Springer CCIS Book Series)

By keeping the linear approximation fixed, we performed experiments by introducing input difference to every single S-box

Input Difference	Best biases
00011	$2^{-11.91}$, $2^{-14.87}$, $2^{-15.05}$, and $2^{-8.03}$
10011	$2^{-14.45}$, $2^{-12.25}$, $2^{-12.25}$, and $2^{-14.45}$

Experiments on ASCON

Experiments on 5-round Differential-Linear Attacks (to appear in Springer CCIS Book Series)

By keeping the linear approximation fixed, we performed experiments by introducing input difference to every single S-box

Input Difference	Best biases
00011	$2^{-11.91}$, $2^{-14.87}$, $2^{-15.05}$, and $2^{-8.03}$
10011	$2^{-14.45}$, $2^{-12.25}$, $2^{-12.25}$, and $2^{-14.45}$
01100	$2^{-8.52}$, $2^{-7.94}$, $2^{-7.94}$, and $2^{-8.52}$

Symmetric Cryptography on GPUs

Optimized GPU Implementation of Ascon

Parallel computing power of GPUs can be used to optimize symmetric key algorithms to

1. obtain fast encryption

Symmetric Cryptography on GPUs

Optimized GPU Implementation of Ascon

Parallel computing power of GPUs can be used to optimize symmetric key algorithms to

1. obtain fast encryption
2. perform brute force attacks on short keys

Symmetric Cryptography on GPUs

Optimized GPU Implementation of Ascon

Parallel computing power of GPUs can be used to optimize symmetric key algorithms to

1. obtain fast encryption
2. perform brute force attacks on short keys
   - We achieved 2^{35} key trials per second on an RTX 4090

Symmetric Cryptography on GPUs

Optimized GPU Implementation of Ascon

Parallel computing power of GPUs can be used to optimize symmetric key algorithms to

1. obtain fast encryption
2. perform brute force attacks on short keys
   - We achieved 2^{35} key trials per second on an RTX 4090
3. verify theoretical results in practice

Symmetric Cryptography on GPUs

Optimized GPU Implementation of Ascon

Parallel computing power of GPUs can be used to optimize symmetric key algorithms to

1. obtain fast encryption
2. perform brute force attacks on short keys
   - We achieved 2^{35} key trials per second on an RTX 4090
3. verify theoretical results in practice
   - We achieved 2^{35} 5-round Ascon differential-linear distinguisher verifications per second on an RTX 4090

Symmetric Cryptography on GPUs

Optimized GPU Implementation of ASCON

Parallel computing power of GPUs can be used to optimize symmetric key algorithms to

1. obtain fast encryption
2. perform brute force attacks on short keys
   - We achieved 2^{35} key trials per second on an RTX 4090
3. verify theoretical results in practice
   - We achieved 2^{35} 5-round ASCON differential-linear distinguisher verifications per second on an RTX 4090

Our optimized GPU codes are available at
`https://github.com/cihangirtezcan/CUDA_ASCON`

Thanks

Thank You for Your Attention

Mail: cihangir@metu.edu.tr
Udemy: cihangir-tezcan
CihangirTezcan
CihangirTezcan