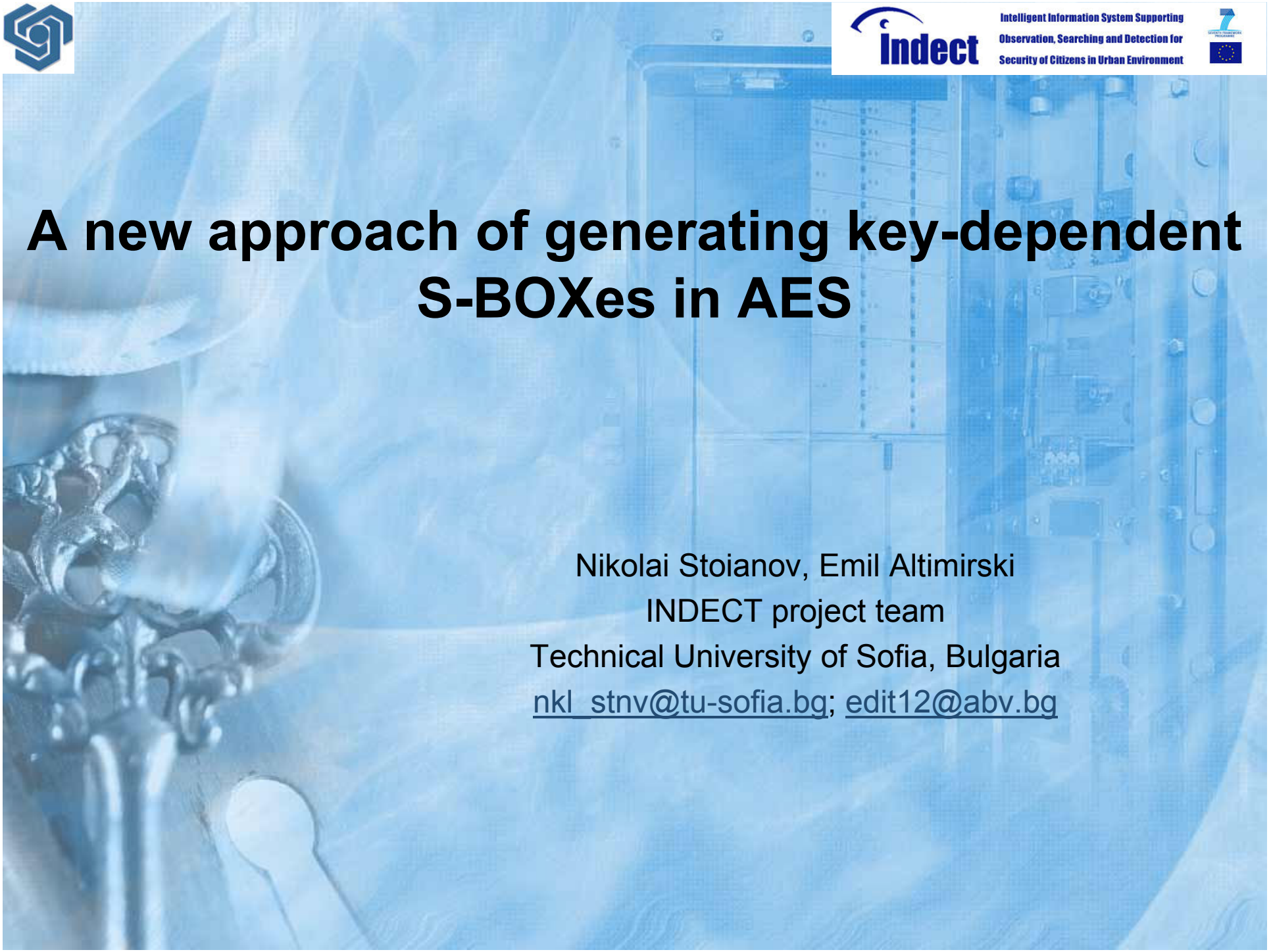


Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment

A new approach of generating key-dependent S-BOXes in AES

Nikolai Stoianov, Emil Altimirski
INDECT project team
Technical University of Sofia, Bulgaria
nkl_stnv@tu-sofia.bg; edit12@abv.bg

Problem definition

- AES – standard;
- SubBytes function - non-linear substitution;
- S-BOX and $S\text{-}BOX_{INV}$ – relation between input and output – FIXED;
- 256!=8.57817775342842654119082271681 23e+506 numbers of S-BOXes ≈7.78659901640563707754315717353 88e+494 TBytes

Criteria [5], [6], [7],[8]

•Balancing;

It ensures that S-boxes do not discriminate against any of the bits, so no value is favored.

•Nonlinearity;

Function that meets this criterion is one that is not linear. Linear functions satisfy following properties:

Additivity: $f(x)+f(y)=f(x+y)$

Homogeneity: $af(x)=f(ax)$

•Completeness;

Bijective function $f:\{0,1\}^t \mapsto \{0,1\}^t$ is completeness if for all $i,j \in \{0,1,...,t-1\}$ exist vector S(X) such that $S(X \oplus e_j)$ and $X \in \{0,1\}^t$ differ in at last bit j. e_j is t-bit unit vector with “1” in position i. In other words, function is complete, when every output bit depends upon every input bit.

Criteria [5], [6], [7],[8]

•The Strict Avalanche Criterion (SAC);

SAC is satisfied if for all $i, j \in \{0,1,...,t-1\}$, input bit i changes output bit j with probability exactly 0,5.

•Low XOR Table;

For any n x n S-box, S-box XOR table entries are defined throughout position [i,j] in XOR table which contains value:

$$\left|\left\{X \in \{0,1\}^n : S(X) \oplus S(X \oplus i) = j\right\}\right|$$

S-box is secure when has low XOR table entries, ideally — “0” and “2”.

•Diffusion Order;

It ensures that even if the value of the output bits change is large, the number of changes to entry is relatively low. Diffusion order specifies the minimum number of changes to the entry, which occurs when a single input bit changes.

Criteria [5], [6], [7],[8]

•Invertability;

Each n x n S-BOX meet the requirements for invertability if $S(X_1)=S(X_2)$ if $X_1=X_2$ for all inputs X_1 and X_2.

•Static criteria:

- Independence between the input and output data;

  Each S-BOX meets the requirement for independence between input and output data of the row r, where r<n if:

  $$P(y_i \mid a_1x_1, a_2x_2, ..., a_nx_n) = P(y_i)$$

  for $\forall x_i, y_j, a_k \mid 1 \le i, j, k \le n; (x_i, y_j, a_k) \in \{0,1\}; A = [a_1, a_2, ..., a_n]$

- Independence between the output and input data;

  Each S-BOX meets the requirement for independence between output and input data from the row r, where r<n if: $P(x_i \mid a_1y_1, a_2y_2, ..., a_ny_n) = P(x_i)$

  for $\forall x_i, y_j, a_k \mid 1 \le i, j, k \le n; (x_i, y_j, a_k) \in \{0,1\}; A = [a_1, a_2, ..., a_n]$

Criteria [5], [6], [7],[8]

•Dynamic criteria

- Dynamic Independence between the input and output data;

  Each S-BOX meets the requirements for independence between the input and output data of the row r, with r<n if: $P(\Delta y_i \mid a_1\Delta x_1, a_2\Delta x_2, ..., a_n\Delta x_n) = P(\Delta y_i)$

  for $\forall \Delta x_i, \Delta y_j, a_k \mid 1 \le i, j, k \le n; (\Delta x_i, \Delta y_j, a_k) \in \{0,1\}; A = [a_1, a_2, ..., a_n]$

- Dynamic Independence between the output and input data;

  Each S-BOX meets the requirement for independence between the output and input data of the row r, with r<n if: $P(\Delta x_i \mid a_1\Delta y_1, a_2\Delta y_2, ..., a_n\Delta y_n) = P(\Delta x_i)$

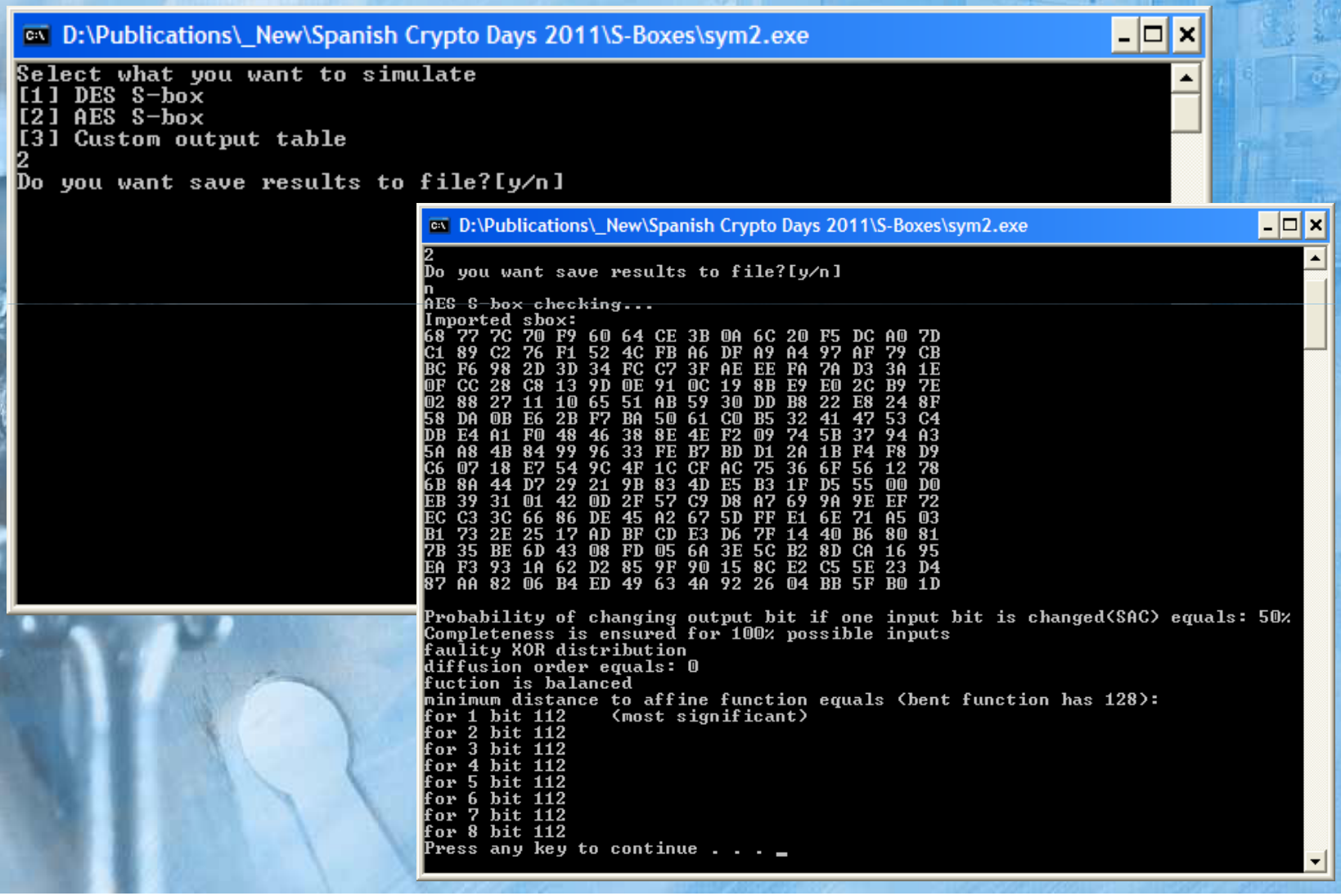
  for $\forall \Delta x_i, \Delta y_j, a_k \mid 1 \le i, j, k \le n; (\Delta x_i, \Delta y_j, a_k) \in \{0,1\}; A = [a_1, a_2, ..., a_n]$

•Non-contradiction

The S-BOX which is tested will have only one non repeated value in each cell of the table.

A new approach of generating key-dependent S-BOXes in AES

Software simulator



Characteristics of AES S-BOX and S-BOX$_{INV}$

Probability of changing output bit if one input bit is changed (SAC) equals: 50%

Completeness is ensured for 100% possible inputs

Faultily XOR distribution

Diffusion order equals: 0

Function is balanced

Minimum distance to affine function equals (bent function has 128):

For 1 bit 112 (most significant)

For 2 bit 112

For 3 bit 112

For 4 bit 112

For 5 bit 112

For 6 bit 112

For 7 bit 112

For 8 bit 112

Generating method

- First of all choose one byte from used key - Key[i];
- Calculating new $S\text{-}BOX_{xor}$, where each cell is equal to exclusive or (XOR) with chosen byte, $S\text{-}BOX_{xor}[x,y]=S\text{-}BOX_{AES}[x,y] \oplus Key[i]$;
- A newly calculated substitution matrix is used for data encryption.

For decryption process the following approach is used:

- Choose same byte from key - Key[i];
- Calculating new S-BOXxor, where each cell is equal to exclusive or (XOR) with chosen byte, S-BOXxor[x,y]=S-BOXAES[x,y] ⊕ Key[i];
- Calculating inverse matrices by using S-BOXxor, S-BOXxor INV=INV (S-BOXxor);
- A newly calculated inverse S-BOX is used for data decryption.

Indect
Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment

Table 1. S-BOX$_{24}$ (S-BOX $\oplus$ 24$_{hex}$)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	47	58	53	5F	D6	4F	4B	E1	14	25	43	0F	DA	F3	8F	52
1	EE	A6	ED	59	DE	7D	63	D4	89	F0	86	8B	B8	80	56	E4
2	93	D9	B7	02	12	1B	D3	E8	10	81	C1	D5	55	FC	15	31
3	20	E3	07	E7	3C	B2	21	BE	23	36	A4	C6	CF	03	96	51
4	2D	A7	08	3E	3F	4A	7E	84	76	1F	F2	97	0D	C7	0B	A0
5	77	F5	24	C9	04	D8	95	7F	4E	EF	9A	1D	6E	68	7C	EB
6	F4	CB	8E	DF	67	69	17	A1	61	DD	26	5B	74	18	BB	8C
7	75	87	64	AB	B6	B9	1C	D1	98	92	FE	05	34	DB	D7	F6
8	E9	28	37	C8	7B	B3	60	33	E0	83	5A	19	40	79	3D	57
9	44	A5	6B	F8	06	0E	B4	AC	62	CA	9C	30	FA	7A	2F	FF
A	C4	16	1E	2E	6D	22	00	78	E6	F7	88	46	B5	B1	C0	5D
B	C3	EC	13	49	A9	F1	6A	8D	48	72	D0	CE	41	5E	8A	2C
C	9E	5C	01	0A	38	82	90	E2	CC	F9	50	3B	6F	99	AF	AE
D	54	1A	91	42	6C	27	D2	2A	45	11	73	9D	A2	E5	39	BA
E	C5	DC	BC	35	4D	FD	AA	B0	BF	3A	A3	CD	EA	71	0C	FB
F	A8	85	AD	29	9B	C2	66	4C	65	BD	09	2B	94	70	9F	32

Indect
Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment

Table 2. $S\text{-}BOX_{6F}$ ($S\text{-}BOX \oplus 6F_{hex}$)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0C	13	18	14	9D	04	00	AA	5F	6E	08	44	91	B8	C4	19
1	A5	ED	A6	12	95	36	28	9F	C2	BB	CD	C0	F3	CB	1D	AF
2	D8	92	FC	49	59	50	98	A3	5B	CA	8A	9E	1E	B7	5E	7A
3	6B	A8	4C	AC	77	F9	6A	F5	68	7D	EF	8D	84	48	DD	1A
4	66	EC	43	75	74	01	35	CF	3D	54	B9	DC	46	8C	40	EB
5	3C	BE	6F	82	4F	93	DE	34	05	A4	D1	56	25	23	37	A0
6	BF	80	C5	94	2C	22	5C	EA	2A	96	6D	10	3F	53	F0	C7
7	3E	CC	2F	E0	FD	F2	57	9A	D3	D9	B5	4E	7F	90	9C	BD
8	A2	63	7C	83	30	F8	2B	78	AB	C8	11	52	0B	32	76	1C
9	0F	EE	20	B3	4D	45	FF	E7	29	81	D7	7B	B1	31	64	B4
A	8F	5D	55	65	26	69	4B	33	AD	BC	C3	0D	FE	FA	8B	16
B	88	A7	58	02	E2	BA	21	C6	03	39	9B	85	0A	15	C1	67
C	D5	17	4A	41	73	C9	DB	A9	87	B2	1B	70	24	D2	E4	E5
D	1F	51	DA	09	27	6C	99	61	0E	5A	38	D6	E9	AE	72	F1
E	8E	97	F7	7E	06	B6	E1	FB	F4	71	E8	86	A1	3A	47	B0
F	E3	CE	E6	62	D0	89	2D	07	2E	F6	42	60	DF	3B	D4	79

Table 3. $S\text{-}BOX_{80}$ ($S\text{-}BOX \oplus 80_{hex}$)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E3	FC	F7	FB	72	EB	EF	45	B0	81	E7	AB	7E	57	2B	F6
1	4A	02	49	FD	7A	D9	C7	70	2D	54	22	2F	1C	24	F2	40
2	37	7D	13	A6	B6	BF	77	4C	B4	25	65	71	F1	58	B1	95
3	84	47	A3	43	98	16	85	1A	87	92	00	62	6B	A7	32	F5
4	89	03	AC	9A	9B	EE	DA	20	D2	BB	56	33	A9	63	AF	04
5	D3	51	80	6D	A0	7C	31	DB	EA	4B	3E	B9	CA	CC	D8	4F
6	50	6F	2A	7B	C3	CD	B3	05	C5	79	82	FF	D0	BC	1F	28
7	D1	23	C0	0F	12	1D	B8	75	3C	36	5A	A1	90	7F	73	52
8	4D	8C	93	6C	DF	17	C4	97	44	27	FE	BD	E4	DD	99	F3
9	E0	01	CF	5C	A2	AA	10	08	C6	6E	38	94	5E	DE	8B	5B
A	60	B2	BA	8A	C9	86	A4	DC	42	53	2C	E2	11	15	64	F9
B	67	48	B7	ED	0D	55	CE	29	EC	D6	74	6A	E5	FA	2E	88
C	3A	F8	A5	AE	9C	26	34	46	68	5D	F4	9F	CB	3D	0B	0A
D	F0	BE	35	E6	C8	83	76	8E	E1	B5	D7	39	06	41	9D	1E
E	61	78	18	91	E9	59	0E	14	1B	9E	07	69	4E	D5	A8	5F
F	0C	21	09	8D	3F	66	C2	E8	C1	19	AD	8F	30	D4	3B	96

Characteristics of new S-BOXes

Probability of changing output bit if one input bit is changed (SAC) equals: 50%
Completeness is ensured for 100% possible inputs
Faultily XOR distribution
Diffusion order equals: 0
Function is balanced
Minimum distance to affine function equals (bent function has 128):
For 1 bit 112 (most significant)
For 2 bit 112
For 3 bit 112
For 4 bit 112
For 5 bit 112
For 6 bit 112
For 7 bit 112
For 8 bit 112

Encryption:

1.Select a key for AES;

2.The first byte of the Key (it could be anyone else) is selected – Key[1];

3.Calculating new $S\text{-}BOX_{key[1]} = S\text{-}BOX_{AES} \oplus Key[1]$;

4.Continue according to the algorithm set out in AES by using new calculated $S\text{-}BOX_{key[1]}$.

Decryption:

1.Select a key for AES;

2.The first byte of the Key (it could be anyone else) is selected – Key[1];

3.Calculating new $S\text{-}BOX_{key[1]} = S\text{-}BOX_{AES} \oplus Key[1]$;

4.Calculating inverse $S\text{-}BOX_{key[1]INV}$=INV (S-BOXkey[1])=INV (S-BOXAES⊕Key[1]);

5.Continue according to the algorithm set out in AES by using new calculated $S\text{-}BOX_{key[1]INV}$.

Conclusion

- New substitution matrices were developed by XOR operation with chosen byte from key and existing AES S-BOX;
- Matrices were tested with the software simulator;
- Characteristics of the new 256 S-BOXes are identical with original AES S-BOX;
- An algorithm for using these matrices is proposed.

Acknowledgments. This work has been funded by the EU Project INDECT (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*) — grant agreement number: 218086.

References

1.Bruce Schneier, AES Announced, October 15, 2000

2.FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

3.Advanced Encryption Standard (AES), National Institute of Standards and Technology http://csrc.nist.gov/archive/aes/index.html

4.Bruce Schneier. AES News, Crypto-Gram Newsletter, September 15, 2002. http://www.schneier.com/crypto-gram-0209.html. Retrieved 2007-07-27.

5.M. H. Dawson and S. E. Tavares, ”An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation of Differential-Like Attacks”, Advances in cryptology – Eurocrypt ‘91, LNCS, vol. 547, pp. 352-367, Springer (1991)

6.Nikolai Stoianov, AES S-BOX generator: analysis of requirements, International Science Conference 2009” Communication and information systems”, Shoumen, Bulgaria, 2010

7.INDECT Consortium, D8.2: Evaluation of Components, June, 2010, http://www.indect-project.eu/files/deliverables/public/deliverable-8.2

8.Nikolai Stoianov, One Approach of Using Key-Dependent S-BOXes in AES, MCSS 2011, CCIS 149, pp. 331–337, 2011. Springer-Verlag Berlin Heidelberg, 2011

Future work

- Test new S-BOXes with additional metrics;
- Implementation of new S-BOXes in AES* and test results with comparison of AES;
- Creating new AES mode of operation.

Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment

Thank you!