Specification of STABS Cipher

Ohad Amon

14/5/2019

General Description:

STABS (**S**titched-**T**ogether **A**malgamation of **B**etter **S**tandards) is an SPN Block cipher with a block size of 64 bits and a key size of 64 bits. Each block of the cipher is divided into 16 nibbles, which for the sake of this specification are represented as a 4x4 matrix. It has 20 rounds, where each round consists of:

1. SubBytes
2. ShiftRows
3. MixColumns
4. AddRoundKey

similarly to AES.

Round Function:

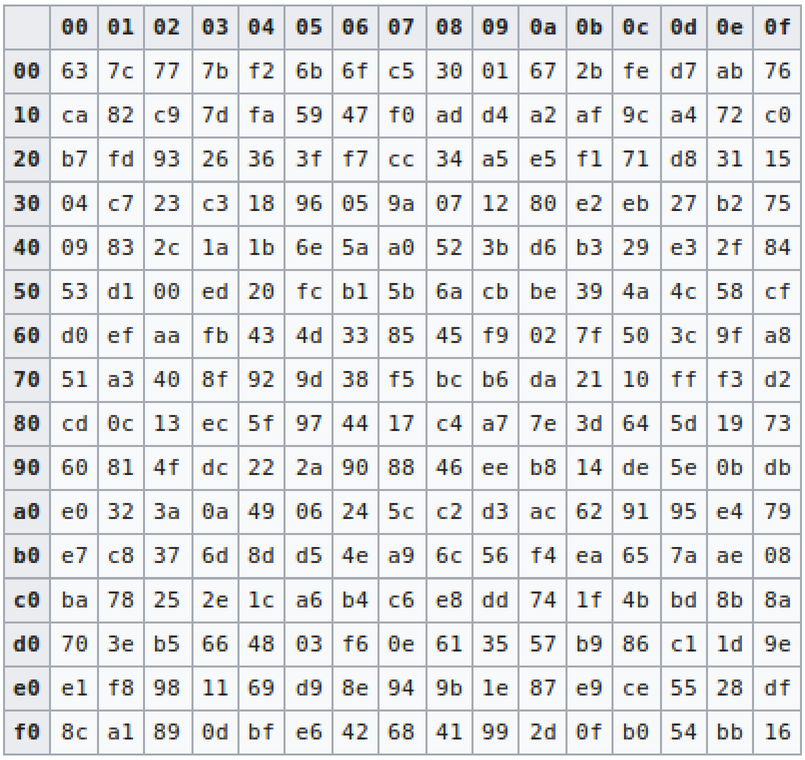
To demonstrate the round function, we shall show each step on the matrix

0	1	2	3
4	5	6	7
8	9	A	B
C	D	E	F

Using the key 0xFEDCBA9876543210.

1. SubBytes:

The sbox used is the 8-bit sbox used by AES. In this round every two nibbles are substituted using the sbox (nibbles 0 and 1 together, nibbles 2 and 3 together, etc.). Below is the sbox pictured such that for every two nibbles, the row is determined by the most significant nibble and the column by the least significant.



	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

After SubBytes the state is:

7	C	2	6
6	E	8	5
A	7	6	2
B	D	D	F

2. ShiftRows

The ShiftRows is performed similarly to AES and TC02, but right instead of left. Each row is rotated 0, 1, 2, 3 nibbles right respectively.

7	C	2	6
5	6	E	8
6	2	A	7
D	D	F	B

3. MixColumns

MixColumns is done by multiplying each column by the following matrix (taken from the Skinny cipher):

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

After MixColumns the state is:

C	3	7	A
7	C	2	6
3	4	4	F
1	E	8	1

4. AddRoundKey

Similarly to TC02, we XOR the 32 most significant bits of the keystate with the cipher state.

After AddRoundKey the state is:

3	D	A	6
C	6	B	E
3	4	4	F
1	E	8	1

Key Schedule:

The key schedule is similar to TC02's, but in order to minimize keystate repetition it utilizes a round a constant (RC). The keystate for round i is defined such:

$k_0 = K$

$k_i = (k_{i-1} \oplus RC) <<< 16$

RC_i is defined:

$RC_1 = 0x3$

$RC_i = RC_{i-1} <<< 1$

The roundkey for each round is the 32 leftmost bits of the keystate

$rk_i = k_i \,\&\, 0xFFFFFFFF00000000$

Test Vectors:

Plaintext	Ciphertext	Key
0x0000000000000000	0x7F94F802DBCC4972	0x0000000000000000
0x1234567890ABCDEF	0x54FCD9CC468B04A1	0x1234567890ABCDEF

Design Rationale:

Once the cipher type was chosen to be an SPN, I needed a nonlinear layer, a diffusion layer and a roundkey layer. I chose the form of AES, using SubBytes, ShiftRows, MixColumns and AddroundKey, in that order.

SubBytes is the cipher's nonlinear layer. It's implemented using a premade sbox. The sbox chosen is AES's 8-bit box, which was used although the cipher uses 4-bit cells because the 8-bit box allows for less predictability of the substitutions, thus harming any differential attack.

ShiftRows and MixColumns together were chosen to be the ones used in the Skinny lightweight cipher. That is because the MixColumns provided uses a binary matrix, which is both easier to implement and quicker to calculate than the MixColumns used in AES. While the matrix is simple, its form ensures quick diffusion over several rounds. ShiftRows in STABS goes right instead of left because that's how it's used in Skinny.

The Key schedule is loosely based on that used in TC02, because both standards have the same size for the block and for the key. Using only part of the key in each round (as opposed to XORing all 64 bits) protects us from having to create the keys in subsequent rounds from the same pool of bits, thus protecting us from attacks on the key schedule. One flaw of the key schedule of TC02 is that it XORing 0x3 to each 16 bits cancels out after over eight rounds, so a changing round constant is introduced in order to reduce roundkey repetition.

The number of rounds was decided to be 20 in order to protect against MitM attacks and differential cryptanalysis. According to Beierele et al.[1] the skinny MixColumns matrix reaches full diffusion in 6 rounds. That means that in order to protect against MitM the cipher needs at least (6-1)+(6-1) = 10 rounds. This is doubled for safety, while only increasing the time required for computation by a factor of 2.

Looking at Table 7 provided in Beierle et al.[1] 19 rounds of the Skinny permutation guarantee at least 92 4-bit sbox activations (using Skinny sboxes). This is equivalent to approximately 5 nibbles per round, making differential cryptanalysis difficult.

Sources:

[1] Beierle, Jean, Kolble, Leander, Moradi, Peyrin, Sasaki, Sasdrich, Siang, *The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS,* https://eprint.iacr.org/2016/660.pdf

[2] Lambooij, E., *Specification of TC02*, https://cryptanex.hideinplainsight.io/media/exercise_file/4/TC02_spec_QZKhUjz.pdf

[3] Wikipedia, *Rijndael S-box*, https://en.wikipedia.org/wiki/Rijndael_S-box