Decomposition attack on SASASASAS

Alex Biryukov and Dmitry Khovratovich
University of Luxembourg

alex.biryukov@uni.lu, khovratovich@gmail.com

June 2015

Abstract

We demonstrate the first attacks on the SPN ciphers with 6, 7, 8, and 9 secret components. In particular, we show a decomposition attack on the SASASASAS scheme when the S-box size m and the block length n satisfy the condition $m^2 \leq n$ (for example, 8-bit S-box and 128-bit block).

1 Introduction

A block cipher with secret nonlinear layers S and secret affine transformations A is a fundamental concept in both symmetric and asymmetric cryptography. For years, only up to 5-layer schemes could be analyzed in a generic, structural way. The so called "ASASA" structure with two S-box layers and three affine layers was suggested by Patarin in 1997 [12] and broken by Biham in 2000 [2] due to non-bijectivity of S-boxes. The SASAS structure was attacked with practical complexity in 2001 by Biryukov and Shamir [4, 5]. The attack recovered S-boxes and affine layers up to affine equivalence (as equivalent layers produce identical ciphers).

The ASASA scheme with injective S-boxes and schemes with more layers were considered secure since then and motivated Biryukov et al. to propose a number of schemes based on the generic ASASA for black-box, white-box, and public-key cryptography in 2014 [3]. However, it turned out that this variant is also insecure, even though the attack complexity is practical for small block sizes only. Independently, Minaud et al. [11] and Dinur et al. [8] found decomposition attacks for several instances of ASASA both for large and small block sizes. These results suggest the insecurity of generic 5-layer schemes with secret layers, but give little insight on the security of longer variants.

The structural decomposition attacks are supposed to be difficult since the secret components are described with much more than n bits of information, where n is the block size. In some cases the attacks with complexity 2^n and higher are not a surprise [8]. Moreover, for small block lengths n, which is a typical setting in the white-box cryptography, a scheme can be called secure only if the decomposition complexity is far larger than 2^n. It is unclear whether this can be achieved for 6-layer and longer schemes.

Our contributions. In this work we combine the existing techniques altogether and demonstrate attacks on 6-, 7-, 8-, and 9-layer schemes. As a groundbreaking result, we demonstrate a decomposition attack on the SASASASAS scheme (which is a generic 5-round substitution affine network) with total complexity of 2^n or less for certain parameters (e.g., 2^{240} for secret 8-bit S-boxes and 256-bit block size). Our methods apply for certain (but natural) combinations of S-box size and block size, and, to little surprise, for smaller S-boxes we can attack even more layers.

Related work. Our attacks are purely algebraic but highlight the links between the Square/multiset/integral attack and the high-order differential attack. In this context, a reader might be interested in the schemes with very small S-boxes [1] and attacks on them [9, 10]. The degree deficiency effect, that we exploit, was noticed in [7] and used in [6] to demonstrate that Rijndael-256 achieves full degree only after 7 rounds.

2 Algebraic degree of iterative functions

The following result originated in the discussion on the security of Keccak permutation. The small size (5 bits) and low degree (2) of Keccak S-boxes warned cryptographers that the full-round permutation

might be insecure to algebraic attacks or distinguishers. Indeed, after some point, the algebraic degree of the multi-round SPN structure does not grow as fast as expected. For m-bit bijective S-boxes that have maximum possible degree $(m-1)$, the following result holds.

Theorem 1 ([7]). *Let G be an arbitrary function on $\mathbb{F}_2^n$. Let F be a bijection on $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller bijective Sboxes.*

1. *If the degree of all S-boxes is $m-1$, then*

$$\deg(G \circ F) \leq n - \left\lceil \frac{n - \deg(G)}{m-1} \right\rceil.$$

In other words, the difference between n and the scheme degree decreases at maximum by the factor of $(m-1)$ with each new layer. Due to rounding the fraction in the equation, the degree deficiency is even larger.

3 Attack on SASASASAS

We proceed to our main result and then derive some interesting implications. Consider the ASASASA scheme with secret bijective m-bit S-boxes (possibly different) and secret affine transformations over $GF(2)$. Apparently, if there are at least m such S-boxes in each layer, then the scheme does not have the maximum possible degree.

Theorem 2. *If $m^2 \leq n$, then*

$$\deg(ASASASA) \leq n - 3.$$

Proof. The degree of the ASA subscheme does not exceed $m-1$, and the degree of the ASASA subscheme does not exceed $(m-1)^2 < n$. If we add one more S-layer, Theorem 1 implies that

$$\deg(ASASAS) \leq n - \left\lceil \frac{n-(m-1)^2}{m-1} \right\rceil = n - \left\lceil \frac{n}{m-1} \right\rceil + m - 1. \tag{1}$$

From the theorem condition we get

$$m^2 \leq n \implies m^2 - 1 < n \implies \frac{n}{m-1} > m+1 \implies -\left\lceil \frac{n}{m-1} \right\rceil \leq -m-2.$$

We substitute this to Eq. (1) and obtain that

$$\deg(ASASAS) \leq n - 3.$$

Clearly, the degree does not change if we add one more A-layer. This ends the proof. □

For ASASA-like schemes the degree growth is shown in Table 1. It can be seen that ASASASA schemes with 4-bit S-boxes and 16-bit block, or 8-bit S-boxes and 128-bit block, do not have the maximum possible degree.

3.1 Decomposition attack on ASASASAS

Procedure. Consider now the ASASASAS scheme (one more S-layer). Denote $\deg(ASASASA)$ by d. If we encrypt any affine subspace of dimension

$$d+1 \leq n + m - \left\lceil \frac{n}{m-1} \right\rceil,$$

the inputs to the last S-layer would sum to zero. Consider, w.l.o.g., the first S-box S_0. As noticed in [5], we get an equation:

$$S_0^{-1}(x_1) \oplus S_0^{-1}(x_2) \oplus \cdots \oplus S_0^{-1}(x_{2^{d+1}}) = 0, \tag{2}$$

where x_j is the output of S_0 at j-th encryption.

We encrypt 2^m such subspaces (cubes) and collect 2^m equations of type (2). The resulting system is linear w.r.t. new variables $y_j = S_0^{-1}(j), j \in Z_2^m$. However, it has multiple solutions, as for any affine invertible transformation B if $\mathcal{S}$ is a solution then $\mathcal{S}(B())$ is a solution as well. Thus our system of

equations has rank at most[1] $2^m - m - 1$. Since any solution is good for us, we can fix $S^{-1}(x_i)$ at $(m+1)$ arbitrary points, get a full rank system, and solve it in 2^{3m} time.

Using the technique from [11], the ASASASA scheme can then be decomposed with complexity $n^2 2^{d+1}$.

Complexity. The complexity of peeling off the final S-layer is determined by the number of encryptions, which is upper bounded by 2^{d+m+1}. However, this bound can be improved significantly. Consider an affine space of dimension $d' > d+1$, where $(n-d')$ variables are fixed and the other are free. How many spaces of dimension $(d+1)$ are inside? Note that we should exclude linearly dependent spaces.

Consider subspaces of dimension $d'-1$, which are formed by fixing any of d' variables to 1. These d' subspaces are linearly independent. Within each, we can select $(d'-1)$ subspaces of dimension $(d'-2)$ in the same fashion. Therefore, a space of dimension $(d+3)$ contains at least d^2+5d spaces of dimension $d+1$. For all m, n that we consider the condition $d^2+5d > 2^m$ holds, so the total complexity of the attack is upper bounded by

$$C_{\text{Decompose ASASASAS}} \leq 2^{d+3} \leq 2^{n+m+2-\lceil \frac{n}{m-1} \rceil}.$$

For certain parameters, like $m = 4, n = 16$ we can take into account the fact that $(2^m - m - 1)$ spaces are sufficient, and $d + 1 \geq 2^m - m - 1$. In this case the complexity of the attack is smaller by the factor of 2.

3.2 Attack on SASASASAS

Now let us make the final step and consider a scheme with yet another S-layer, i.e. SASASASAS. The observation here (also used in [9]) is that by fixing an input to a single S-box and varying the others we also get an affine space, even if we do not know its constant bits. In the terms of the multiset attack, the S-box layer preserves the multiset property, which has the affine property that we need. As long as $d + 1 \leq n - m$, i.e. at least one S-box can be fixed, this approach works. Unfortunately, we can not fix arbitrary bits anymore to reduce the data complexity.

The attack procedure is very similar to that for ASASASAS. Let k be maximum such that $d + 1 \leq n - km$. Then one of k S-boxes takes $2^m - m - 1$ values, and the other take all possible values. The total data complexity is slightly less than $2^{n-(k-1)m}$.

For some extreme cases the complexity is almost 2^n. However, we stress that this not an upper bound for this kind of attacks. Indeed, we recover the secret components, which are described with more than n bits of information (about $m2^m$ bits for an S-box and n^2 bits for the affine layer). We summarize our attacks in Table 2 and give the equivalent key size for the AS pair of layers $(m2^m + n^2)$.

[1] In practice it is usually equal to this value, as confirmed both by [5] and our experiments

S-box size	Block size	ASA	ASASA	ASASASA
Verified experimentally				
3	12	2	4	8
3	15	2	4	8
4	12	3	9	11
4	16	3	9	13
6	12	5	10	11
6	18	5	15	17
Theorem 1 implications				
8	128	7	49	116
8	256	7	49	227
6	120	5	25	104
10	120	9	106	118
16	128	15	120	127

Table 1: Degree evolution

S-box	Block	Key size	ASASAS	SASASAS	ASASASAS	SASASASAS
4	12	208	2^{11}	-	-	-
4	16	312	2^{11}	2^{15}	2^{15}	-
6	12	500	2^{12}	-	-	-
6	18	700	2^{17}	-	-	-
6	24	960	2^{21}	-	-	-
6	36	2^{10}	2^{28}	2^{36}	2^{36}	-
6	120	2^{14}	2^{28}	2^{36}	2^{106}	2^{114}
8	128	2^{14}	2^{52}	2^{64}	2^{118}	2^{128}
8	256	2^{16}	2^{52}	2^{64}	2^{230}	2^{240}

Table 2: Summary of our decomposition attacks

3.3 Even more layers

Our results can be further extended to more esoteric scenarios, where $m \ll n$. For example, if $m^3 \leq n$ (4-bit S-boxes, 64-bit block) the 11-layer scheme can be decomposed with complexity less than 2^n. In general, at least $(2 \log_m n + 7)$ secret layers are needed to achieve security against this sort of attacks.

4 Experimental verification

We have verified our attack by experiments. We considered the ASASASAS scheme with 16-bit block and 4 4-bit S-boxes. The inputs to the last S-layer have degree 13, thus they sum to zero over a cube of dimension 14.

We need 2^4 linearly independent equations to recover the S-box. We encrypted 2^{15} plaintexts that start with the zero bit. Within this structure, we consider 15 substructures $\{\mathcal{S}_i\}$, where i-th bit is zero in $\mathcal{S}_i$. We got a system of 15 equations (2), which has rank 11 (in most cases). We assigned arbitrary distinct values to 5 unknowns and solved the resulting system. As a result, we got an S-box, which is affine-equivalent to the original one. When we take true values of this unknowns, the S-box is recovered precisely.

References

[1] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Computer Science*, pages 430–454. Springer, 2015.

[2] Eli Biham. Cryptanalysis of patarin's 2-round public key system with S boxes (2R). In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 408–416. Springer, 2000.

[3] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key (extended abstract). In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014*, volume 8873 of *Lecture Notes in Computer Science*, pages 63–84. Springer, 2014.

[4] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 394–405. Springer, 2001.

[5] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. *J. Cryptology*, 23(4):505–518, 2010.

[6] Christina Boura and Anne Canteaut. On the influence of the algebraic degree of f^{-1} on the algebraic degree of G $\circ$ F. *IEEE Transactions on Information Theory*, 59(1):691–702, 2013.

[7] Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of keccak and *Luffa*. In Antoine Joux, editor, *FSE'2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 252–269. Springer, 2011.

[8] Itai Dinur, Orr Dunkelman, Thorsten Kranz, and Gregor Leander. Decomposing the ASASA block cipher construction. *IACR Cryptology ePrint Archive*, 2015:507, 2015.

[9] Itai Dinur, Yunwen Liu, Willi Meier, and Qingju Wang. Optimized interpolation attacks on lowmc. Cryptology ePrint Archive, Report 2015/418, 2015. `http://eprint.iacr.org/`.

[10] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. Higher-order cryptanalysis of lowmc. Cryptology ePrint Archive, Report 2015/407, 2015. `http://eprint.iacr.org/`.

[11] Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman. Key-recovery attacks on ASASA. Cryptology ePrint Archive, Report 2015/516, 2015. `http://eprint.iacr.org/`.

[12] Jacques Patarin and Louis Goubin. Asymmetric cryptography with s-boxes. In Yongfei Han, Tatsuaki Okamoto, and Sihan Qing, editors, *ICICS'97*, volume 1334 of *Lecture Notes in Computer Science*, pages 369–380. Springer, 1997.