IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2016, No. 2, pp. 226–247. DOI:10.13154/tosc.v2016.i2.226-247

# Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs

Alex Biryukov[1], Dmitry Khovratovich[2] and Léo Perrin[3]

[1] Interdisciplinary Centre for Security, Reliability and Trust (SnT), Computer Science and Communications Research Unit (CSC), University of Luxembourg, Luxembourg, Luxembourg
alex.biryukov@uni.lu
[2] University of Luxembourg, Luxembourg, Luxembourg
dmitry.khovratovich@uni.lu
[3] Interdisciplinary Centre for Security, Reliability and Trust (SnT), Computer Science and Communications Research Unit, University of Luxembourg, Luxembourg, Luxembourg
leo.perrin@uni.lu

**Abstract.** We devise the first closed formula for the number of rounds of a blockcipher with secret components so that these components can be revealed using multiset, algebraic-degree, or division-integral properties, which in this case are equivalent.
Using the new result, we attack 7 (out of 9) rounds of Kuznyechik, the recent Russian blockcipher standard, thus halving its security margin.
With the same technique we attack 6 (out of 8) rounds of Khazad, the legacy 64-bit blockcipher. Finally, we show how to cryptanalyze and find a decomposition of generic SPN construction for which the inner-components are secret. All the attacks are the best to date.

**Keywords:** Generic SPN · Algebraic attack · Multi-set · Integral · Division property · Kuznyechik · Khazad

## 1 Introduction

### 1.1 Multiset, integrals, division, and algebraic degree

Multiset attacks originated in the late 1990s with application to byte-oriented blockciphers [BS01] and are also known as Square [DKR97], integral [KW02], and saturation [Luc01] attacks. For years, they remained the most efficient method to attack AES [FKL+00, DF13], Camellia, and other popular designs. However, finding a multiset property has been heuristic, and the number of rounds that can or can not be attacked remained an open question.

The connection of the multiset attacks to the algebraic degree of the blockcipher as a function of plaintext and key became apparent in the recent works by Boura, Canteaut, et al. [BCC11, BC13]. It was demonstrated that the algebraic degree is incomplete for about the same number of rounds as the multiset attacks can penetrate. This suggests similarity, if not equivalence, of the algebraic and the integral property. However, the recent division property attack by Todo can break more rounds than the algebraic method [Tod15], which may suggest that the division method is superior. The division property is tedious to find by hand, so Todo devised a search algorithm supposed to run on a PC.

Our contribution is a single closed formula that calculates the number of rounds that can be attacked using either division or algebraic method. We plug ciphers Kuznyechik and Khazad into it, as well as the secret SPN constructions, and derive the best attacks to date.


Received: 2016-06-01, Revised: 2016-09-01, Accepted: 2016-11-01, Published: 2017-02-03

Consider an $n$-bit SPN with, in total, $r$ S-Box layers consisting in the parallel application of $m$-bit bijective S-Boxes. A naive approach shows that such a structure has degree about $(m-1)^r$ and thus that about $\log_{m-1}(n)$ rounds are needed to achieve full degree. However, we found that this quantity should be multiplied by 2: in fact, about $2\log_{m-1}(n)$ rounds are necessary! For instance, if $n > 2(m-1)^q$, then the $2q$-round structure has degree at most $n-2$. A more generic statement is given by Theorem 1 which links the base $(m-1)$ expansion of the block size $n$ and the number of SPN rounds needed to reach full degree.

## 1.2 Kuznyechik and Khazad

Khazad [BR00] is a 64-bit blockcipher with 128-bit key, a NESSIE finalist, designed by Barreto and Rijmen in 2000. It is notable for the linear layer that achieves full diffusion over one round. The best attack on Khazad in the single-key setting dates back to 2003 and breaks 5 out of 8 rounds [Mul03]. For the sake of completeness, we mention an attack against 5 rounds in the weak-key setting [Bir03] and related-key attacks against 7 and 8 rounds [BN10].

Kuznyechik is a more recent design and is a new Russian standard blockcipher [Fed15], which replaces the old [Dol10] and broken [Iso13] GOST 28147-89, now called "Magma". It is a 9-round 128-bit block, 256-bit key cipher. In contrast to its counterpart, the hash function Streebog [Fed12], Kuznyechik has not been officially submitted for the third-party cryptanalysis. Neither design rationale nor security analysis accompanies the specification. The rationale elements we are aware of include the claim that the S-box was selected almost randomly [SB15], and the linear layer is an iterative MDS construction based on [CGMN99]. Very recently, a non-trivial decomposition of the Kuznyechik S-box (which it shares with Streebog) was found, which in absence of design rationale puts the security of the cipher into question. This situation somewhat resembles that with DES S-boxes, which had additional unexplained structure due to hidden design criteria. Given the recent efforts to make Kuznyechik an IETF standard [Dol16], it seems urgent to analyze it from the cryptanalytic point of view.

Our unified division-algebraic formula implies the existence of a 4-round property for Kuznyechik and a 3-round property for Khazad, which can be turned into 7-round and 6-round attacks, respectively, using the partial sum technique [FKL+00]. The only third-party cryptanalysis of Kuznyechik breaks 5 rounds, so we halve the security margin at once.

We compare these attacks with the state of the art in Table 1.

Table 1: The best attacks against Khazad and Kuznyechik.

| Target | Rounds | Data Comp. | Time Comp. | Mem. Comp. | Ref. |
|---|---|---|---|---|---|
| Kuznyechik | 5 | $2^{113}$ | $2^{140.3}$ | $2^{153.3}$ | [AY15] |
| | 6 | $2^{120}$ | $2^{146.5}$ | $2^{132}$ | Section 3.3 |
| | 7 | $2^{128}$ | $2^{155}$ | $2^{140}$ | Section 3.2 |
| Khazad | 4 | $2^{9}$ | $2^{80}$ | $2^{8}$ | [BR00] |
| | 5 | $2^{64}$ | $2^{91}$ | $2^{11}$ | [Mul03] |
| | 6 | $2^{64}$ | $2^{90}$ | $2^{68}$ | Section 4 |

## 1.3 Secret SPN: SASA...S

A block cipher with secret nonlinear layers $S$ and secret affine transformations $A$ is a fundamental concept in both symmetric and asymmetric cryptography, as it determines an

essential lower bound for the security of traditional SPN ciphers with public components and only key being secret. In addition, a small secret-component cipher can be used to build an S-box with hidden representation [BP15], for the purpose of backdoor or efficient hardware implementation [BPU16]. Finally, the secret-component cipher is a crucial security element of white-box cryptography [CEJvO02], where groups of internal transformations are masked with secret operations and then are exposed as lookup tables. It was demonstrated in [BBK14] that the multiple attempts to construct a white-box AES implementation boil down to the SASA cipher – a four-layer scheme with two secret S-box layers (S) and two secret affine layers (A). The AES diffusion properties make it impossible to obfuscate more than 1.5 rounds of AES and add more secret layers to SASA.

One of the first structural attacks against a bijective SPN targets SASAS with practical complexity [BS01]. This attack recovers S-boxes and affine layers up to affine equivalence (as equivalent layers produce identical ciphers). Independently, Minaud et al. [MDFK15] and Dinur et al. [DDKL15] found decomposition attacks for black- and white-box versions of ASASA both for large and small block sizes. These results suggest the insecurity of generic 5-layer SPN with secret layers but give little insight on the security of longer variants, nor do they expose the requirements on the S-box width and the state size. Todo analyzed several concrete SPNs in [Tod15], but did not provide any closed formula for the scheme parameters that can be broken.

We provide sufficient conditions on $n$ as a function of $m$ and $q$ such that the secret components in schemes AS...AS and SA..AS with $q$ layers can be found faster than $2^n$. We note that since the entire S-boxes are unknown, the exhaustive search would take far more computations than $2^n$.

### 1.4 Paper structure

Section 2 presents our main theorem bounding the number of SPN rounds having degree strictly less than maximal. Sections 3, 4 and 5 present our attacks against Kuzneychik, Khazad and generic structures respectively. Finally, we revisit the division property and expose its multiple links to algebraic attacks in Section 6.

## 2 Degree bounds on generic SPN

### 2.1 Basic Proposition

We use the following notation:

$$A(SA)^q = A\underbrace{SASA\dots SA}_{2q \text{ layers}}.$$

Consider the $A(SA)^q$ scheme with secret bijective S-boxes of size $m$ and degree $m-1$ and secret affine transformations over $\mathbb{F}_2$. The S-Boxes and the linear layers used may be different.

It is well known that the algebraic degree of an $n$-bit permutation $P$ is at most $n-1$. If it does not reach this maximum, this provides a distinguisher. If the degree is $d$ then the sum of $P(x)$ for all $x$ in a cube of dimension $d+1$ is equal to 0, which is unlikely for a random permutation if $d < n-1$.

Our results are based on the following theorem by Boura et al., which we apply recursively to derive the degree bounds.

**Proposition 1** ([BCC11]). *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 $m$-bit bijective Sboxes of degree $m-1$. Then*

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

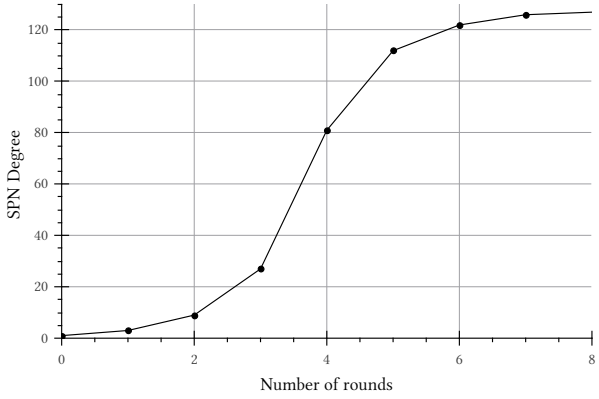


Figure 1: Evolution of the maximum algebraic degree of a SPN with 128-bit blocks and 4-bit S-Boxes as bounded by Proposition 1.

This proposition captures the influence of the fact that an S-Box layer consists of the parallel application of several smaller functions. Note in particular that if $m = n$, which corresponds to the case where one S-Box is applied to the full state, this bound does not give new information: it merely states that $\deg(G \circ F) \leq n - 1$, which is obviously the case since it is a permutation. When the S-Box layers consists in several smaller S-Boxes however, it implies a degree discrepancy as illustrated in Figure 1 which shows the evolution of the maximum degree of a SPN with $m = 4$ and $n = 128$: starting from $r = 4$, the degree increase is much slower. It reaches the maximum of 127 only after 8 rounds, meaning that a simple integral distinguisher exists for up to 7 rounds.

The maximum number of rounds for which there exists such a distinguisher is obviously related to the block and the S-Box size. Is there a general pattern for how many rounds are necessary? And which distinguisher is the best: a simple one based on exploiting an algebraic degree of at most $n - 2$ or one which exploits a degree bounded by $n - (m + 1)$ and adds another S-Box layer for free?

To answer these questions, we derive a theorem bounding the degree of a SPN depending on its number of rounds, its block size $n$ and the S-Box size $m$. Then, we derive simple corollaries linking the expansion in base $m - 1$ of $n$ with the number of rounds for which integral distinguishers of each type exists.

It is assumed that all S-Boxes have maximum algebraic degree $d = m - 1$ but they may be distinct (so do the linear layers). We use $\overline{x_\ell ... x_0}^d$ to denote the base $d$ expansion of $x$, where $\ell = \lfloor \log_d(x) \rfloor$:

$$x = \overline{x_\ell ... x_1 x_0}^d, \text{ where } x = \sum_{i=0}^{\ell} x_i d^i.$$

## 2.2 A Bound on the Algebraic Degree of a SPN

The following theorem allows us to study the evolution of the algebraic degree of a SPN based on Proposition 1.

**Theorem 1.** *For all $\ell \leq \lfloor \log_d(n) \rfloor$, it holds that:*

$$\deg\left(A(SA)^{\ell+r}\right) \leq n - \left(\psi_r + \left\lfloor \frac{n}{d^r} \right\rfloor - \frac{d^\ell}{d^r}\right),$$

*where*

$$\psi_i = \begin{cases} 0 \text{ if } n_{i-1} = n_{i-2} = ... = n_0 = 0, \\ 1 \text{ otherwise.} \end{cases}$$

*Furthermore, if* $\ell = \lfloor \log_d(n) \rfloor$ *and* $n_\ell ... n_1 n_0$ *is the base* $d$ *expansion of* $n$*, we have*

$$\left\lfloor \frac{n}{d^r} \right\rfloor = \sum_{i=r}^{\ell} n_i d^{i-r} \quad \textit{and} \ ,$$

*so that in this case, if we need* $\deg\left(A(SA)^{\ell+r}\right) \leq n-k$*, then it is sufficient that*

$$\psi_r + \left\lfloor \frac{n}{d^r} \right\rfloor - \frac{d^\ell}{d^r} \geq k \quad \textit{or, equivalently,} \quad (n_\ell - 1)d^{\ell-r} + \sum_{i=r}^{\ell-1} n_i d^{i-r} \ \geq \ k - \psi_r.$$

The proof of this theorem is given in Section A.1. The best bounds are derived for $\ell = \lfloor \log_d(n) \rfloor$ but the theorem holds for any $\ell \leq \lfloor \log_d(n) \rfloor$.

Note that unless $n$ is a power of $d$ we have that $\psi_r$ is equal to 1 at least for $r \geq \ell - 1$. Furthermore, it is likely to be equal to 1 even for lower values of $r$. The algebraic degree of $r + \ell$ SPN rounds is bounded by $n + d^{\ell-r} - \lfloor n/d^r \rfloor$. This observation has some interesting corollaries.

**Corollary 1.** *Let* $\ell = \lfloor \log_d(n) \rfloor$*,* $n = \overline{n_\ell ... n_0}^d$ *be the block size and* $m = d + 1$ *be the size of the S-Boxes. Assume that there exists* $i < \ell - 2$ *such that* $n_i \neq 0$*. Then the maximum number of rounds for which the degree is at most* $n - 2$ *is equal to*

$$\begin{cases} 2\ell & \textit{if} \ \ n_\ell > 1, \\ 2\ell - 1 & \textit{if} \ \ n_\ell = 1, \ n_{\ell-1} \geq 1, \\ 2\ell - 2 & \textit{if} \ \ n_\ell = 1, \ n_{\ell-1} = 0, \ n_{\ell-2} \geq 1. \end{cases}$$

*The same results can be expressed using intervals rather than the expansion in base* $d$ *of* $n$*. The maximum number* $r_s$ *of rounds for which* $\deg(A(SA)^{r_s - 1}) \leq n - 2$ *is equal to*

$$\begin{cases} 2\ell & \textit{if} \ \ 2d^\ell < n < d^{\ell+1}, \\ 2\ell - 1 & \textit{if} \ \ d^\ell + d^{\ell-1} < n \leq 2d^\ell, \\ 2\ell - 2 & \textit{if} \ \ d^\ell + d^{\ell-2} < n \leq d^\ell + d^{\ell-1}. \end{cases}$$

*Proof.* Using the assumptions of the corollary along with Theorem 1, we deduce that the degree is at most $n - 2$ if $\lfloor n/d^r \rfloor - d^{\ell-r} \geq 1$, which can also be written $\sum_{i=r}^{\ell-1} n_i d^{i-r} + (n_\ell - 1)d^{\ell-r} \geq 1$.

If $r = \ell$, then we need that $n_\ell - 1 \geq 1$, which implies the first case.

If $n_\ell = 1$ then the inequality becomes $\sum_{i=r}^{\ell-1} n_i d^{i-r} \geq 1$. For $r = \ell - 1$, it is equivalent to $n_{\ell-1} \geq 1$. For $r = \ell - 2$ and $n_{\ell-1} = 0$, it is equivalent to $n_{\ell-2} \geq 1$.

These results are easily turned into intervals. For example, $n_\ell > 1$ and $\psi_\ell = 1$ if and only if $n > 2d^\ell$. Furthermore, if $n = d^\ell$ then $r_s = 2\ell - 1$ as in this case $\psi_\ell = 0$. The other intervals are deduced identically. □

We deduce from Corollary 1 that a good rule of thumb to estimate the number of SPN rounds necessary to achieve full degree is to use $2 \times \lfloor \log_{m-1}(n) \rfloor$ rounds. Interestingly, this result is very similar to what is stated in Theorem 1 of [PU16]. Indeed, in this paper, the existence of integral distinguishers for about $2\log_d(n)$ rounds of Feistel Network are derived, where $d$ is the degree of the Feistel function.

Corollary 1 tells us a bound on the number of rounds for which the maximum algebraic degree can not be reached. It is also worth looking at round bounds for smaller degrees. Let us look for the maximum number of rounds $r_s$ such that $\deg(A(SA)^{r_s-1}) \leq n-(m+1)$. It is then possible to attack $(SA)^{r_s}$ by fixing $d + 1 = m$ bits corresponding to an S-Box input.

**Corollary 2.** *Let $\ell = \lfloor \log_d(n) \rfloor$, $n = \overline{n_\ell \ldots n_0}^d$ be the block size and $m = d+1$ be the size of the S-Boxes. Assume that there exists $i < \ell - 3$ such that $n_i \neq 0$. Then the maximum number $r_s$ of rounds for which $\deg(A(SA)^{r_s-1}) \leq n - (m+1)$ is equal to*

$$\begin{cases} 2\ell & \text{if } n_\ell > 2 \text{ or } n_\ell = 2,\ n_{\ell-1} \geq 1, \\ 2\ell - 1 & \text{if } n_\ell = 2,\ n_{\ell-1} = 0 \text{ or } n_\ell = 1, n_{\ell-1} \geq 2 \text{ or } n_{\ell-1} = 1, n_{\ell-2} \geq 1 \\ 2\ell - 2 & \text{if } n_\ell = 1, n_{\ell-1} = 0,\ n_{\ell-2} \geq 1. \end{cases}$$

*The same results can be expressed using intervals rather than the expansion in base $d$ of $n$. The maximum number $r_s$ of rounds for which $\deg(A(SA)^{r_s-1}) \leq n - (m+1)$ is equal to*

$$\begin{cases} 2\ell & \text{if } 2d^\ell + d^{\ell-1} < n < d^{\ell+1}, \\ 2\ell - 1 & \text{if } d^\ell + d^{\ell-1} + d^{\ell-2} < n \leq 2d^\ell + d^{\ell-1} \\ 2\ell - 2 & \text{if } d^\ell + d^{\ell-2} < n \leq d^\ell + d^{\ell-1} + d^{\ell-2}. \end{cases}$$

*Proof.* We want $\lfloor n/d^r \rfloor - d^{\ell-r} > d$, which is equivalent to

$$\sum_{i=r}^{\ell} n_i d^{i-r} \geq d + d^{\ell-r} + 1.$$

- It is impossible to have $r = \ell$. Indeed, in this case, we would have $n_\ell > d+1$ which is impossible ($n_i < d$, for all $i$).
- In order to have $r = \ell - 1$, it is necessary and sufficient to have $dn_\ell + n_{\ell-1} > 2d$. It is the case if and only if $n_\ell \geq 3$ or $n_\ell = 2$ and $n_{\ell-1} > 0$.
- If it is not the case, then we may have $r = \ell - 2$. In order for this to happen, we need $d^2 n_\ell + dn_{\ell-1} + n_{\ell-2} > d + d^2$. It is the case if $n_\ell = 2$. Otherwise, as $n_\ell = 1$, we need either $n_{\ell-1} \geq 2$ or both $n_{\ell-1} = 1$ and $n_{\ell-2} > 0$.

This concludes the proof for the base $d$ expansions. Intervals are deduced from those in the same fashion as for Corollary 2. □

In most cases, approach relying on fixing the input of a whole S-Box to leverage a distinguisher on $q-1$ rounds to attack $q$ rounds leads to the best attacks. Indeed, it is usually true that $r_s = r_i$, meaning that both distinguishers cover an equal number of rounds. Since the data complexity of the second approach is lower, as the whole input of an S-Box is fixed instead of just 1 bit, it is a better attack.

However, there are cases where the simpler distinguisher based on a degree bound of $n-2$ covers one more round. Using Corollary 1 and Corollary 2, we can see that the case $n_\ell = 2, n_{\ell-1} = 0$ yields such a case. Indeed, for such values, $r_i = 2\ell$ which means that $2\ell$ rounds have algebraic degree at most $n-2$, but $r_s = 2\ell - 1 = r_i - 1$. This actually occurs with $d = 7$ and $n = 104 = \overline{206}^7$. For these values, the progression of the bound on the degree as deduced from Proposition 1 is $1 \to 7 \to 49 \to 96 \to 102 \to 103$. Since $96 = 108 - 8$, it is impossible to extend a 4-round distinguisher using the fixed-S-Box method. And yet, since $102 < 103$, a simple distinguisher on 5-round exists. Similarly, for $d = 3$ and $n = 512 = \overline{200222}^3$, we have that $r_s = 9$, and $r_i = 10$. Indeed, the last steps of the progression of the algebraic degree are $502 \to 508 \to 510 \to 511$ and 508 is too high to allow a fixed-S-Box integral distinguisher.

We applied these corollaries to several S-Box size/block size combinations and obtained the results in Table 2. The maximum number of rounds such that $\deg(A(SA)^r) \leq n-2$ obtained with Corollary 1 is denoted $r_i$. The actual value of $\deg(A(SA)^{r_i})$ is also given: it can be computed either directly from Theorem 1 or by recursively applying the formula

Table 2: Theorem 1 and its Corollaries 1 and 2 for some $m, n$.

| S-box size $m$ | Block size $n$ | $(n_\ell, n_{\ell-1}, n_{\ell-2})$ | $r_i$ | $\deg(A(SA)^{r_i})$ | $r_s$ | $c_{\min}$ |
|---|---|---|---|---|---|---|
| 4 | 16 | (1, 2, 1) | 3 | 13 | 3 | 12 |
| | 24 | (2, 2, 0) | 4 | 22 | 4 | 20 |
| | 32 | (1, 0, 1) | 4 | 29 | 4 | 24 |
| | 48 | (1, 2, 1) | 5 | 45 | 5 | 44 |
| | 64 | (2, 1, 0) | 6 | 62 | 6 | 60 |
| | 128 | (1, 1, 2) | 7 | 126 | 7 | 124 |
| | 512 | (2, 0, 0) | 10 | 510 | 9 | 504 |
| 8 | 64 | (1, 2, 1) | 3 | 61 | 3 | 56 |
| | 104 | (2, 0, 6) | 4 | 102 | 3 | 56 |
| | 128 | (2, 4, 2) | 4 | 126 | 4 | 120 |
| | 256 | (5, 1, 4) | 4 | 251 | 4 | 232 |
| | 512 | (1, 3, 3) | 5 | 508 | 5 | 488 |

from Proposition 1. We also computed the number $r_s$ of rounds having a degree at most equal to $n - (m + 1)$ using Corollary 2. We then compute $\deg(A(SA)^{r_s})$ and deduce the minimum dimension of a cube $c_{\min}$ summing to zero over $SA(SA)^{r_s}$ by rounding $\deg(A(SA)^{r_s-1})$ up to its closest multiple of $m$.

# 3 Cryptanalysis of 7-round Kuznyechik

Kuznyechik[1], also known as GOST 34.12-2015, is a new 128-bit blockcipher developed in Russia and recently adopted as a Russian official standard [Fed15]. It is described in an informational IETF RFC [Dol16]. The hash function Streebog [Fed12], designed by the same team, has already been standardized by the IETF [DD13].

Kuznyechik is an SPN cipher with 9 rounds. Its linear layer is an $16 \times 16$ MDS matrix, and the S-box, borrowed from the earlier Streebog, is 8-bit. The design principles of Kuznyechik are barely known: we only know, as it is specified in the standard, that the matrix is a power of some specific matrix corresponding to the 16-block LFSR. The S-box design rationale is not known: the designers claimed (regarding Streebog) that it was selected randomly, whereas the recent reverse-engineering attack demonstrated a decomposition of it into a sort of 2-round Feistel Network using finite field multiplications instead of xors [BPU16].

The third-party cryptanalysis of Kuznyechik is limited to the already mentioned reverse-engineering attack and the 5-round meet-in-the-middle attack [AY15]. In this section we outline the first 6- and 7-round attacks on Kuznyechik.

## 3.1 Description of Kuznyechik and Notations

Kuznyechik is a 9-round 128-bit blockcipher with 256-bit key, where the 128-bit plaintext $P$ is first XORed with the whitening round key $K_0$. Then the 128-bit state undergoes 9 identical rounds with round function denoted by $\mathcal{XLS}$:

- first, $\mathcal{S}$ applies the 8-bit S-box bytewise;

[1] Literally, "grasshopper" in English.

- then $\mathcal{L}$ is a linear transformation over $\mathbb{F}_{2^8}^{16}$ based on a $16 \times 16$ MDS matrix $M$ over $\mathbb{F}_{2^8}$,
- finally, $\mathcal{X}$ is the XOR with the round key.

The round keys are produced as follows:

1. The initial key $K = (K_0||K_1)$ is a concatenation of the first two round keys $K_0$ and $K_1$.
2. The 256-bit state $(K_0||K_1)$ undergoes a 8-round Feistel network with the 128-bit round function being $\mathcal{XLS}$ where round keys are round constants from 1 to 8. The output of the network is the concatenation $(K_2||K_3)$ of the next two round keys.
3. In the same way and increasing the constants, we produce $(K_4||K_5)$ out of $(K_2||K_3)$, then $(K_6||K_7)$ from the former, and finally $(K_8||K_9)$ from $(K_6||K_7)$.

Let us denote the bytes of the internal state $X$ and the key $K$ as $X[0], X[1], \ldots, X[15]$ and $K[0], K[1], \ldots$.

## 3.2 Attack on 7-round Kuznyechik

By applying Corollary 1 with $m = 8, d = 7$ and $n = 128 = \overline{242}^7$, we obtain that the algebraic degree of the 4-round subcipher $\mathcal{E}_K$ as a function of the plaintext is at most 126. Let $V$ be a linear space of states of dimension 127. Then we obtain

$$\bigoplus_{v \in V} \mathcal{E}_K(v) = 0. \tag{1}$$

Now we demonstrate how to use this 4-round property in the 7-round attack. The attack proceeds as follows.

1. Guess the key byte $K_0[0]$.
2. Let $\mathcal{P}$ be a structure of $2^{127}$ plaintexts, where the first byte takes $2^7$ values $\{S^{-1}(0) \oplus K_0[0], S^{-1}(1) \oplus K_0[0], \ldots, S^{-1}(127) \oplus K_0[0]\}$, and the other bytes take all possible values.
3. Ask for encryption of $\mathcal{P}$ under the unknown $K$, get ciphertexts $\mathcal{C}$.
4. Decrypt $\mathcal{C}$ by two rounds (let us denote the decryption function for the last 2 rounds by $\mathcal{D}^2$), guessing the round keys, and check if
$$\bigoplus_{c \in \mathcal{C}} \mathcal{D}^2(c) = 0.$$
5. Test all remaining key candidates on four (plaintext, ciphertext) pairs, pick the right one.

The attack works since $\mathcal{P}$ becomes an affine space of dimension 127 after the first S-box layer and remains so after the linear transformation and the key addition. After the next 4 rounds it becomes a multiset that XORs to 0 thanks to Equation (1). We then test this property on the decrypted ciphertexts and keep only the key candidates that satisfy it. We note that the attack is deterministic and always gives the correct answer.

**Complexity and optimization.** Since $\mathcal{D}^2$ involves two round keys $K_6$ and $K_7$ and thus 256 bits of key material, a naive implementation of this attack would give a complexity far higher than the exhaustive search. To cope with that, we apply the tricks well known from the integral cryptanalysis of AES, although the case of AES is easier due to incomplete diffusion at the linear layer.

Let us denote the output of the fifth round by $X_5$ so that we analyze the $2^{127}$ states $\{X_5^i,\ i < 2^{127}\}$. First, we test the balanced property on separate bytes. For the first byte we have to compute the sum

$$\bigoplus_{c \in \mathcal{C}} S^{-1}(M^{-0}(\mathcal{S}^{-1}(\mathcal{L}^{-1}(c \oplus K_7)) \oplus K_6)), \tag{2}$$

where $M^{-i}, i < 16$, is the $i$-th row of matrix $M^{-1}$, which determines the value of byte 0 after the application of $\mathcal{L}^{-1}$.

Then we use the *partial sum* technique from [FKL+00], which reduces the complexity greatly. We consider equivalent round keys $K_i' = \mathcal{L}^{-1}(K_i)$ and equivalent ciphertexts $c'^i = \mathcal{L}^{-1}(c^i)$. Then Equation (2) is rewritten as

$$\bigoplus_{c' \in \mathcal{C}'} S^{-1}(q_0\mathcal{S}^{-1}(c'[0] \oplus K_7'[0]) \oplus q_1\mathcal{S}^{-1}(c'[1] \oplus K_7'[1]) \oplus \ldots \\ \ldots \oplus q_{15}\mathcal{S}^{-1}(c'[15] \oplus K_7'[15])) \oplus K_6'[0]), \tag{3}$$

where $q_j$ are coefficients of $M^{-1}$.

Note that only 17 key bytes are involved in Equation (3). The crucial property of the partial sum technique is that it allows guessing them sequentially and reuse the intermediate calculations in a dynamic programming fashion. Concretely, we proceed as follows:

1. We prepare table $T_1$ of $2^{136}$ bit counters, initialized with 0, that correspond to all the possible tuples $(K_7'[0], K_7'[1], x_1, c'[2], c'[3], \ldots, c'[15])$, where $x_1$ is a byte value.

2. For each pair of key bytes $K_7'[0], K_7'[1]$ and each ciphertext $c'$ we calculate $x_1 = q_0\mathcal{S}^{-1}(c'[0] \oplus K_7'[0]) \oplus q_1\mathcal{S}^{-1}(c'[1] \oplus K_7'[1])$ and change the parity of the corresponding counter.

3. We prepare another table $T_2$ of $2^{136}$ counters for tuples $(K_7'[0], K_7'[1], K_7'[2], x_2, c'[3], c'[4], \ldots, c'[15])$.

4. For every $K_7'[2]$ and every entry in $T_1$ we compute $x_2 = x_1 \oplus q_2\mathcal{S}^{-1}(c'[2] \oplus K_7'[2])$ and update the corresponding parity counter in $T_2$.

5. We proceed up to table $T_{15}$, which contains the counters for tuples $(K_7'[0], K_7'[1], \ldots, K_7'[15], x_{15})$.

6. For every $K_6'[0]$ and every entry from $T_{15}$ we compute $x_{15} \oplus K_6'[0]$ and the parities of occurences of all values entering $S^{-1}$. Then we check if the balanced property is satisfied and keep all tuples $(K_7'[0], K_7'[1], \ldots, K_7'[15], K_6'[0])$ for which it does.

7. We repeat all the steps above for the other 15 S-boxes and derive the whole round keys $K_6', K_7'$, from which we recover a candidate $K$ and test it.

Since the balanced property for a single byte is a $2^{-8}$ filter, we expect that for every $K_7'$ on average one $K_6'$ will be suggested and thus $2^{128}$ key candidates $K$ will be generated, of which $2^{120}$ will remain after filtering on $K_0[0]$. We need the complexity of $2^{122}$ encryptions to test them.

The complexity of the partial sum step is calculated as follows. At the first step we make 2 S-box inversions for each of $2^{16}$ guesses and $2^{127}$ ciphertexts, or $2^{144}$ S-box inversions in total. At each other step we make $2^{144}$ inversions. Thus to check the property on a single byte we need $2^{148}$ S-box inversions, and for all bytes we need $2^{152}$ inversions. Since each 7-round cipher call uses $2^{6.5}$ S-boxes, the testing-filtering phase is equivalent to $2^{146.5}$ blockcipher calls. To get the full attack complexity, we have to accomodate for the guess of $K_0[0]$, which raises the complexity to $2^{154.5}$ time and about $2^{140}$ bytes of memory. We also need the entire codebook, though if we have partial key knowledge (any byte of $K_0$), we could live with $2^{127}$ chosen plaintexts.

### 3.3 6-round attack

For the 6-round attack we exploit the fact that the 3-round subcipher has degree at most 116. Thus we encrypt $2^{120}$ plaintexts, which take all possible values in the first 15 bytes.

The second phase of the attack is the same as in the 7-round version, only the table $T_1$ takes less time to produce. The time complexity becomes $2^{146.5}$ and the data complexity is $2^{120}$.

## 4 Cryptanalysis of reduced Khazad

### 4.1 Description of Khazad

Khazad is a 64-bit blockcipher with using a 128-bit key designed by Rijmen and Barreto in 2000 [BR00]. It was later selected as a finalist of the NESSIE project.

Khazad is an 8-round SPN network where S-boxes are 8-bit permutations of degree 7 and the linear layer is given by a $8 \times 8$ matrix over $\mathbb{F}_2$. The plaintext is initially XORed with the whitening key $K_0$, and then undergoes 8 identical rounds, each consisting of

- The S-box layer $\mathcal{S}$ of 8 S-boxes $S$.
- Linear transformation $\mathcal{L}$ based on the involutive matrix $H$.
- XOR with the round key, an operation denoted $\sigma$.

The 64-bit round keys $K_i$ are derived from the initial key $K$ as follows. The key $K$ enters the Feistel network with the blockcipher round function $\sigma \circ \mathcal{L} \circ \mathcal{S}$ where the round keys are constants. Each round a new round key is produced:

$$K_i = \sigma \circ \mathcal{L} \circ \mathcal{S}(K_{i-2}) \oplus K_{i-1}, \quad K = K_0 || K_1.$$

The best attack on Khazad is the 5-round attack by Muller with $2^{91}$ time and $2^{64}$ time complexity [Mul03].

### 4.2 Attack on the 6-round Khazad

Khazad and Kuznyechik are quite similar in structure, even though the Kuznyechik state is twice as large. For parameters $m = 8, d = 7$ and $n = 64 = \overline{121}^7$, Corollary 1 implies that the algebraic degree of 3-round Khazad is strictly less than $n - 1$. In fact, by recursively applying Proposition 1, we find that it is at most equal to $64 - \lceil \frac{64-49}{7} \rceil = 61$.

We proceed similarly to the attack on Kuznyechik:

1. Guess the key byte $K_0[0]$.
2. Prepare the $2^{62}$ plaintexts that form an affine space of dimension 62 after the first S-box layer by taking all possible values in the last 7 bytes and values from 0 to 63 in the first byte.

3. Encrypt the plaintexts and get ciphertexts $C$.

4. Test the balanced property by partial decryption of the ciphertexts for the 2 rounds.

The partial decryption procedure is again the same as for Kuznyechik. We prepare a set of tables with $2^{72}$ bit counters each and guess the key bytes sequentially. The time complexity of the attack is $2^{90}$ and the data complexity is $2^{64}$. Thus we attack 6 rounds of Khazad with the same complexity as the best existing attack processes 5 rounds.

# 5 Attacks on secret SPNs

We proceed to the analysis of SPN ciphers with secret components, which generalizes the integral distinguishers in [BCC11, BC13, Tod15] and dedicated attacks in [MDFK15, DDKL15, BS01, BK15].

## 5.1 Decomposition attack on AS..AS

**Attack 1.** *The $(AS)^{2q+1}$ scheme with secret bijective (possibly different) S-boxes of degree $m-1$ such that $3(m-1)^q+1 \le n$ and secret affine transformations over $\mathbb{F}_2$ can be decomposed with data and time complexity*

$$C_{(AS)^{2q+1}} \le 2^n.$$

**Recovery of the outer S-layer.** In Theorem 1 we set $l = r = q$. By the condition of the attack we have either $\psi_q = 1$ and $\frac{n}{d^q} \ge 3$, or $\psi_q = 0$ and $\frac{n}{d^q} \ge 4$. In both cases we have

$$\deg(A(SA)^{2q}) = D \le n-3.$$

Therefore, an affine space of dimension $D+1$ is encrypted to ciphertexts that sum to 0. Since in this space the $n-D-1$ variables take fixed values, it is a *cube* of dimension $D+1$. Now consider the encryption of this cube $\{P_1, P_2, \dots, P_{2^{D+1}}\}$ by the longer scheme $A(SA)^{2q}S = (AS)^{2q+1}$ and look, w.l.o.g., at the first S-box $S_0$ of size $m$. As noticed in [BS01], we get an equation:

$$S_0^{-1}(C_1^0) \oplus S_0^{-1}(C_2^0) \oplus \dots \oplus S_0^{-1}(C_{2^{D+1}}^0) = 0, \tag{4}$$

where $C_j^0$ are the bits of ciphertext $C_j = (AS)^{2q+1}(P_j)$ outputted by $S_0$.

We encrypt $2^m$ such multisets (cubes) and collect $2^m$ equations of type (4). 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[2] $2^m - m - 1$. Since any solution is good for us, we can fix $S^{-1}(C_i^0)$ at $(m+1)$ arbitrary points, get a full rank system, and solve it in $2^{3m}$ time.

**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 $\mathcal{A}$ of dimension $D' > D+1$, where $(n-D')$ variables are fixed and the other are free. Let us compute how many linearly independent equations (4) we can obtain fron using only the plaintexts from this space.

Linearly independent equations (4) correspond to linearly independent indicator functions of the plaintext sets. For example, in 3-dimensional space the 2-dimensional sets

[2] In practice it is usually equal to this value, as confirmed both by [BS10] and our experiments

$\{(*,*,0)\},\{(*,*,1)\},\{(0,*,*)\}$ and $\{(1,*,*)\}$ are linearly dependent. However, any three of them are linearly independent.

We can guarantee the linear independence as follows. Consider subspaces of $\mathcal{A}$ of dimension $D'-1$, which are formed by fixing any variable (out of $D'$) 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 $(D+3) \le n$ contains at least $D^2+5D$ spaces of dimension $D+1$. For all $d,m,n$ that we consider the condition $D^2+5D > 2^m$ holds as $D \approx n$ and $m \approx \log_q n$, so the total complexity of the first step is upper bounded by $2^{D+3} \le 2^n$.

**Recovery of the A-layers.** Thus we are left with the subcipher $A(SA)^{2q}$, which has incomplete degree $D \le n-3$. The affine layers can then be recovered with the technique from [MDFK15] (even though defined for incomplete-degree ASASA it works equally well for other incomplete degree SPN). The main idea (for the technical details of the attack we refer the reader to [MDFK15]) is that we have to encrypt $n^2/2$ linearly independent cubes of dimension $D+1$ and then solve a linear system over $\mathbb{F}_2$ with $n^2/2$ equations.

We have already demonstrated that the full codebook contains at least $(n-3)^2+5(n-3) \ge n^2/2$ linearly independent cubes of dimension $n-2$, so the total complexity of the affine-recovery step does not exceed $2^n$. For smaller $D$ the complexity is around $2^{D+3}$.

**Attack 2.** *The $(AS)^{2q}$ scheme with secret bijective S-boxes of degree $m-1$ (possibly different) such that $2(m-1)^q+1 \le n$ and secret affine transformations over $\mathbb{F}_2$ can be attacked with data and time complexity*

$$C_{(AS)^{2q}} \le 2^{n-m+3}.$$

The proof for the even number of S-layers repeats the previous one with $l=q, r=q-1$, so we omit it.

Briefly, we have a bound $\deg(AS)^{(2q-1)} \le n-(1+2(m-1)-(m-1)) = n-m$, which is smaller by $(m-3)$ than in Attack 1. This difference is deducted from the complexity exponent in $2^n$.

## 5.2 Decomposition attack on SAS..AS

For a scheme starting with an S-layer we obtain a different result.

**Attack 3.** *The $S(AS)^{2q+1}$ scheme with secret bijective $m$-bit S-boxes of degree $m-1$ (possibly different) such that $(m+1)(m-1)^q+1 \le n$ and secret affine transformations over $\mathbb{F}_2$ (thus $4q+3$ layers in total) can be decomposed with complexity*

$$C_{S(AS)^{2q+1}} \le 2^n.$$

*Proof.* We have that $n \ge (m+1)(m-1)^q+1 = (m-1)^{q+1}+2(m-1)^q+1$. Thus, by applying Corollary 2 with $q=\ell-1$, we deduce that $\deg(A(SA)^{2q}) = D \le n-m-1$. Therefore, it is sufficient to encrypt cubes of dimension $n-m$. Such cubes can be produced before the A layer by fixing the input to a single S-box and varying the others.

The rest of the attack is identical to the attack on $(AS)^q$. We take arbitrary $2^m-m-1$ values $V$ and fix one of S-boxes to $v \in V$, whereas the other take all possible values. The total data complexity is slightly less than $2^n$ encryptions.

□

*Remark* 1. Again, we stress that the time complexity of $2^n$ is not a natural upper bound for this kind of attacks (even though the data complexity can not be higher). 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 for small $q$ and some interesting $m, n$ in Table 3 and give the equivalent key size for the AS pair of layers (about $(n - 1.45n/m)2^m + n^2$ bits).

Table 3: Summary of the complexity of our decomposition attacks with concrete $q, m, n$.

| S-box | Block | Key size | ASASAS | SASASAS | ASASASAS | SASASASAS |
|---|---|---|---|---|---|---|
| 4 | 12 | 270 | $2^{11}$ | - | - | - |
| 4 | 16 | 420 | $2^{11}$ | $2^{15}$ | $2^{15}$ | - |
| 4 | 24 | 1060 | $2^{11}$ | $2^{15}$ | $2^{15}$ | $2^{24}$ |
| 6 | 12 | 728 | $2^{12}$ | - | - | - |
| 6 | 18 | 1200 | $2^{17}$ | - | - | - |
| 6 | 24 | 1744 | $2^{21}$ | - | - | - |
| 6 | 36 | 3048 | $2^{28}$ | $2^{36}$ | $2^{36}$ | - |
| 6 | 120 | $2^{14}$ | $2^{28}$ | $2^{36}$ | $2^{106}$ | $2^{114}$ |
| 8 | 128 | $2^{15}$ | $2^{52}$ | $2^{64}$ | $2^{118}$ | $2^{128}$ |
| 8 | 256 | $2^{17}$ | $2^{52}$ | $2^{64}$ | $2^{230}$ | $2^{240}$ |

## 5.3 Exploiting lower-degree linear combinations

Even if the attacked primitive has maximal degree, it still can be attacked under some circumstances. This effectively adds one more affine layer to a generic SPN structure vulnerable to decomposition attacks described above. We present a distinguisher that exposes a property that is unlikely to occur in a random permutation.

The key observation allowing our attack is the following.

**Lemma 1.** *Let $f$ be an $n$-bit function and $z(f, n)$ be the number of non-zero $b$ in $\mathbb{F}_2^n$ such that $\deg\left(x \mapsto b \cdot f(x)\right) \leq n - 2$. Then the expected value of $z(f, n)$ is $1 - 2^{-n} \approx 1$.*

*Proof.* We consider the high-degree indicator matrix (HDIM) of $f$, as introduced in [PU16]. It is defined as a $n \times n$ binary matrix where the coefficient at line $i$ and column $j$ is equal to 1 if and only if the monomial $\prod_{k \neq j} x_k$ of degree $n - 1$ is present in the ANF of the $i$-th output bit of $f$.

We consider each of the coordinates independently and assume that a monomial appears in the ANF of a coordinate of a random permutation with probability 1/2. The expected number of solutions $b$ of the equation $M \times b = 0$ where $M$ is such a matrix is given by Theorem 3.2.4 and the preceding comments of [Kol99]: it is equal to $1 - 2^{-n}$ and thus converges to 1 as $n$ goes to infinity.

Such solutions correspond to linear combinations of the coordinates of $f$ such that the monomials of degree $n - 1$ cancel each other. In other words, such $b$ are such that $\deg\left(x \mapsto b \cdot f(x)\right) \leq n - 2$ and their expected number is $1 - 2^{-n}$.

□

Consider now an $n$-bit permutation $P$ with degree $n - m + 1$ and a layer $S$ of $m$-bit S-Boxes with degree $m - 1$. Then $S \circ P$ has degree $n - 1$. However, because of Lemma 1, we can expect each of the S-Boxes to have a linear combination of its coordinates with lower degree. Hence, we expect the existence of about $n/m$ linearly independent linear combinations of the coordinates of $S \circ P$ with an algebraic degree at most equal to $n - 2$.

These can be detected using the following method. For all cube $c_i$ where only bit $i$ is fixed to 0, compute the sum $\bigoplus_{x \in c_i} (S \circ P)(x) = s_i$. Then, build the $n \times n$ matrix where row $i$ is equal to $s_i$, i.e. the HDIM of $S \circ P$.

If a linear combination of the output bits has algebraic degree $n-2$, then the corresponding linear combination of the rows of this matrix is equal to the all-zero row because each row is a sum over a space of size $2^{n-1}$ which is equal to 0 for the lower-degree linear combinations. Hence, the rank of this matrix will be close to $n - n/m$ while the rank of a random binary matrix is expected to be $n-1$. As the number of S-Boxes in the layer increases, the rank of this matrix decreases. Furthermore, the application of an affine layer after $S \circ P$ does not change the presence of low-degree linear combinations, it merely shuffles them. Thus, the same discrepancy in rank would be observed in $A \circ S \circ P$.

**Attack 4.** *A scheme PSA where $P$ is a secret permutation with* $\deg(P) = n - m + 1$*, $S$ is a secret layer of $m$-bit S-Boxes with degree $m-1$ (possibly different) and $A$ is a secret affine transformation can be distinguished from a random permutation with high probability with complexity*

$$C_{PSA} \leq n2^{n-1}.$$

The *High Degree Indicator Matrix (*HDIM*)* which we use here was first introduced in [PU16]. It was used in the same paper to prove the existence of integral distinguisher against Feistel Networks depending on the number of rounds and the algebraic degree of the Feistel functions.

## 5.4 Why ASASA can not be secure

Now we note that an ASASA structure with equal-size S-boxes cannot reach a full degree. Indeed, even if we take an ASASA instance with maximum degree, namely one with 2 S-Box layers where each consists in 2 S-Boxes of size $m = n/2$, then the decomposition of $n$ in base $d$ is simply $n = 2d + 2$. This implies that the algebraic degree is at most $n-2$ as this puts us in the situation of Corollary 1.

**Corollary 3.** *The $n$-bit ASASA scheme with equal-size S-Boxes has algebraic degree at most $n-2$.*

As a result, we deduce a distinguisher on the ASASA scheme for any $m$ with a complexity of $2^{n-1}$: the sum over any cube of this size must be equal to 0. For comparison, the best attack in [DDKL15, MDFK15] has complexity $2^{3n/2}$. However, our attack is only a distinguisher.

## 5.5 Experimental verification

We have verified our attack experimentally. We considered the ASASASAS scheme with 16-bit block and four 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 (4), 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 these unknowns, the S-box is recovered precisely.

We also tried the rank based distinguisher against the ASASASASA scheme (addition of 1 secret affine layer) with the same parameters. As the degree of ASASASA is equal to 13 and $m = 4$, we expect the presence of 4 linear combinations of the output bits with algebraic degree 14 instead of 15. We ran the matrix based method to count these linear

combinations. We found that, the average number of low-degree linear combinations over ten ASASASASA schemes is 4.5 while the average of this quantity is equal to 0.7 for the same number of permutations generated with a Knuth shuffle.

# 6 Similarity to the division property

We use the following notations.

**Kronecker's function** For the predicate $P$ we write

$$[P] = \begin{cases} 1, & \text{if } P \text{ is true;} \\ 0, & \text{if } P \text{ is false.} \end{cases} .$$

**Polynomial Notations** We denote the Hamming weight of $x$ by $\mathrm{wt}(x)$. The algebraic normal form (ANF) of function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u^f x^u,$$

where $a_u^f \in \mathbb{F}_2$ and $x^u$ is defined as

$$(x_1 x_2 \dots x_n)^{u_1 u_2 \dots u_n} = \prod_i x_i^{u_i} = \prod_i (1 + (x_i + 1)u_i).$$

The ANF coefficients $a_u$ can be found with the *Moebius transform*:

$$a_u^f = \bigoplus_{x \le u} f(x),$$

where $a \le b$ if $a_i \le b_i$ for every $i$.

## 6.1 Division property revisited

In the seminal paper [Tod15] on the security of generic Feistel and SPN schemes to integral attacks, Todo introduced the following notion.

**Definition 1.** A multiset $\mathcal{X}$ on $\mathbb{F}_2^n$ has *division property* $\mathcal{D}_k^n$ if

$$\bigoplus_{x \in \mathcal{X}} x^u = 0. \tag{5}$$

for all $u \in \mathbb{F}_2^n$ such that $\mathrm{wt}(u) < k$.

If we set $k$ bits to take all possible values, and the other to constant, we get a multiset with division property $\mathcal{D}_k^n$ (in other words, a cube of dimension $k$). If the multiset sums to 0 over all $n$ bits, it has division property $\mathcal{D}_2^n$. Todo found distinguishers of the form

$$\mathcal{D}_k^n \mapsto \mathcal{D}_2^n$$

(meaning that multisets of a certain property are mapped to multisets of another property) for generic SPN constructions with $n$-bit block and $m$-bit S-boxes of degree $m - 1$, the number of rounds $r$ and cube dimension $k$ given in Table 4. Since these attacks outperform the existing degree bounds so far, it seems that the division property method is more effective than the algebraic one.

Table 4: Todo's best division attacks on generic SPN.

| n | m | r | k | Target |
|---|---|---|---|---|
| 64 | 4 | 6 | 60 | Present |
| 128 | 4 | 7 | 124 | Serpent |
| 128 | 8 | 4 | 120 | AES |
| 256 | 4 | 8 | 252 | Minalpher |
| 512 | 4 | 10 | 509 | Prost-512 |
| 512 | 8 | 5 | 488 | Whirlpool |

We claim that the same results can be found using the algebraic degree bounds from our Theorem 1 and the techniques from Section 5.2. The idea is first to demonstrate that the algebraic degree of the $(r-1)$-round primitive is at most $n-m-1$. Therefore, the encryptions of any cube of dimension $r-1$ sum to 0 over $r-1$ rounds.

Then we apply the technique from Section 5.2: we let all the S-boxes but one take all possible values, and the last one be constant. This property holds after the first round, thus we can distinguish $r$ rounds using $2^{n-m}$ plaintexts.

Table 2 implies that this procedure applies for all cases in Table 4. For instance, we have

$$2 \cdot 3^3 + 3^2 + 1 \leq 64,$$

which by Theorem 1 implies that the 5-round PRESENT has degree 59, which is exactly what we require. For other primitives it is similar.

## 6.2 Algebraic view on the division property

In order to demonstrate why the division property covers as many rounds as the algebraic distinguisher, we introduce an equivalent definition of the division property.

It might seem that checking the division property requires evaluation of the entire multiset for every $u$. However, as we will see, for multisets with compact description it becomes much easier. A reader may notice that Equation (5) ignores the order of the elements of the multiset. Moreover, it is unimportant how many times an element occurs; it matters only whether this number is odd or even[3].

Now we define the *multiset indicator* boolean function, which is true if and only if the argument $y$ is present in the multiset an odd number of times:

$$\mathbb{I}_X(y) = \bigoplus_{x \in \mathcal{X}} [x = y]$$

**Proposition 2.** *Multiset $\mathcal{X}$ has division property $\mathcal{D}^n_k$ if and only if its indicator function has degree at most $n-k$.*

*Proof.* Suppose that multiset $\mathcal{X}$ has division property $\mathcal{D}^n_k$. Consider the dual multiset $\overline{\mathcal{X}}$:

$$x \in \overline{\mathcal{X}} \Leftrightarrow \overline{x} \in \mathcal{X},$$

where $\overline{x}$ denotes the negation of $x$. It is evident that the algebraic degree of $\mathbb{I}_X$ and $\mathbb{I}_{\overline{\mathcal{X}}}$ are the same. Now consider the ANF $\bigoplus_u a_u^{\mathbb{I}_{\overline{\mathcal{X}}}} x^u$ of $\mathbb{I}_{\overline{\mathcal{X}}}$ and some coefficient $a_u$ with

[3] A similar approach was independently taken in [BC16].

$\mathrm{wt}(u) > n - k$. From the Moebius transform we get

$$a_u^{\mathbb{I}_{\overline{\mathcal{X}}}} = \bigoplus_{y \le u} \mathbb{I}_{\overline{\mathcal{X}}}(y) = \bigoplus_{y \le u} \bigoplus_{x \in \overline{\mathcal{X}}} [x = y] = \bigoplus_{x \in \overline{\mathcal{X}}} \bigoplus_{y \le u} [x = y] = \bigoplus_{x \in \overline{\mathcal{X}}} [x \le u] =$$
$$= \bigoplus_{x \in \overline{\mathcal{X}}} [\overline{u} \le \overline{x}] = \bigoplus_{\overline{x} \in \overline{\mathcal{X}}} [\overline{u} \le \overline{x}] = \bigoplus_{x \in \mathcal{X}} [\overline{u} \le x] = \bigoplus_{x \in \mathcal{X}} x^{\overline{u}} = 0.$$

The last equation holds from the division property definition since $\mathrm{wt}(\overline{u}) < k$. This ends the proof. □

Thus, looking at the division property of a multiset boils down to studying the algebraic degree of the indicator function of the multiset. The decrease of $k$ in $\mathcal{D}_k^n$ when the multiset undergoes the cipher gets then a natural algebraic explanation: the multiset description becomes more sophisticated and is described by a function of increasing algebraic degree.

### 6.3 Evolution of the multiset degree

Suppose now that the multiset $\mathcal{X}$ given by the indicator function $\mathbb{I}_{\mathcal{X}}$ undergoes an S-box $S$ of degree $d$ and becomes $\mathcal{Y} = S(\mathcal{X})$. Then for the indicator $\mathbb{I}_{\mathcal{Y}}$ and its ANF $\bigoplus_v a_v^{\mathbb{I}_{\mathcal{Y}}} y^v$ we get the following equation on $a_v$ from the Moebius transform:

$$a_v = \bigoplus_{y \le v} \mathbb{I}_{\mathcal{Y}}(y) = \bigoplus_{y \le v} \bigoplus_{x} [S(x) = y] \mathbb{I}_X(x) = \bigoplus_{x} \underbrace{[S(x) \le v]}_{\text{has degree} \le d(n - \mathrm{wt}(v))} \mathbb{I}_X. \quad (6)$$

The degree bound follows from the fact that $S(x) \le v$ if and only if $S(x)$ is equal to 0 on certain $n - \mathrm{wt}(v)$ coordinates. For

$$d(n - \mathrm{wt}(v)) + \deg(\mathbb{I}_X) < n$$

the function $[S(x) \le x]\mathbb{I}_X(x)$ has incomplete degree in $x$, so it sums to 0 over $x \in \mathbb{F}_2^n$ and $a_v = 0$ for such $v$. Therefore

$$\deg(\mathbb{I}_Y) \le n - \left\lceil \frac{n - \deg(\mathbb{I}_X)}{d} \right\rceil, \quad (7)$$

which is equivalent to $\mathcal{D}_k^n$ becoming $\mathcal{D}^n_{\lceil \frac{k}{d} \rceil}$. Now let us note that Equation (7) is the same as in Proposition 1! Therefore, the multiset degree grows at the same speed as the algebraic degree of the primitive.

*We conclude that the evolution of the division property is the same process as the algebraic degree growth.* It is even possible to present an equivalent of Theorem 1 for the division property, but we leave it as a simple exercise to the reader.

## 7 Conclusion

We have identified a simple closed formula bounding the number of rounds necessary for a $A(SA)^q$ structure to achieve full degree. We also used it to identify round-reduced version of some block ciphers with incomplete degrees, namely for Kuznyechik (the last Russian standard block cipher), the legacy cipher Khazad and generic such constructions. This lead us to presenting the best attacks against those primitives by attacking 7 out of 9 rounds of Kuznyechik and 6 out of 8 rounds of Khazad.

We also rephrased our findings within the framework of Todo's division property and showed that the two methods lead to similar results.

## Acknowledgement

The work of Léo Perrin is supported by the CORE project ACRYPT (ID C12-15-4009992) funded by the Fonds National de la Recherche, Luxembourg.

## References

[AY15] Riham AlTawy and Amr M Youssef. A meet in the middle attack on reduced round Kuznyechik. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 98(10):2194–2198, 2015.

[BBK14] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key (extended abstract). In *ASIACRYPT'14*, volume 8873 of *Lecture Notes in Computer Science*, pages 63–84. Springer, 2014.

[BC13] 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.

[BC16] Christina Boura and Anne Canteaut. Another view of the division property, 2016. http://materials.dagstuhl.de/files/16/16021/16021.AnneCanteaut1.Slides.pdf.

[BCC11] Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of Keccak and Luffa. In *FSE'11*, volume 6733 of *Lecture Notes in Computer Science*, pages 252–269. Springer, 2011.

[Bir03] Alex Biryukov. Analysis of involutional ciphers: Khazad and anubis. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 45–53. Springer, 2003.

[BK15] Alex Biryukov and Dmitry Khovratovich. Decomposition attack on sasasasas. Cryptology ePrint Archive, Report 2015/646, 2015. http://eprint.iacr.org/2015/646.

[BN10] Alex Biryukov and Ivica Nikolic. Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to aes, camellia, khazad and others. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 322–344. Springer, 2010.

[BP15] Alex Biryukov and Léo Perrin. On reverse-engineering S-Boxes with hidden design criteria or structure. In *CRYPTO'15*, volume 9215 of *Lecture Notes in Computer Science*, pages 116–140. Springer, 2015.

[BPU16] Alex Biryukov, Léo Perrin, and Aleksei Udovenko. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1. In *Advances in Cryptology-Eurocrypt 2016*, page To appear. Springer, 2016.

[BR00] PSLM Barreto and Vincent Rijmen. The Khazad legacy-level block cipher. *Primitive submitted to NESSIE*, 97, 2000.

[BS01] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In *EUROCRYPT'01*, volume 2045 of *Lecture Notes in Computer Science*, pages 394–405. Springer, 2001.

[BS10] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. *J. Cryptology*, 23(4):505–518, 2010.

[CEJvO02] Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. White-box cryptography and an AES implementation. In *Selected Areas in Cryptography'02*, volume 2595 of *Lecture Notes in Computer Science*, pages 250–270. Springer, 2002.

[CGMN99] Elena Couselo, Santos González, Viktor T. Markov, and Alexander A. Nechaev. Recursive mds-codes and pseudogeometries. In *AAECC*, volume 1719 of *Lecture Notes in Computer Science*, pages 211–220. Springer, 1999.

[DD13] V. Dolmatov and A. Degtyarev. GOST R 34.11-2012: Hash Function. RFC 6986 (Informational), August 2013.

[DDKL15] Itai Dinur, Orr Dunkelman, Thorsten Kranz, and Gregor Leander. Decomposing the ASASA block cipher construction. *IACR Cryptology ePrint Archive*, 2015:507, 2015.

[DF13] Patrick Derbez and Pierre-Alain Fouque. Exhausting demirci-selçuk meet-in-the-middle attacks against reduced-round AES. In *FSE*, volume 8424 of *Lecture Notes in Computer Science*, pages 541–560. Springer, 2013.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher square. In *FSE '97*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

[Dol10] V. Dolmatov. GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms. RFC 5830 (Informational), March 2010.

[Dol16] V. Dolmatov. GOST R 34.12-2015: Block Cipher "Kuznyechik". RFC 7801 (Informational), March 2016.

[Fed12] Federal Agency on Technical Regulation and Metrology. GOST R 34.11-2012: Streebog hash function, 2012. https://www.streebog.net/.

[Fed15] Federal Agency on Technical Regulation and Metrology. Block ciphers, 2015. http://www.tc26.ru/en/standard/draft/ENG_GOST_R_bsh.pdf.

[FKL+00] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In *FSE'00*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.

[GPT15] Henri Gilbert, Jérôme Plût, and Joana Treger. Key-recovery attack on the ASASA cryptosystem with expanding s-boxes. In *CRYPTO'15*, volume 9215 of *Lecture Notes in Computer Science*, pages 475–490. Springer, 2015.

[Iso13] Takanori Isobe. A single-key attack on the full gost block cipher. *Journal of cryptology*, 26(1):172–189, 2013.

[Kol99] V.F. Kolchin. *Random Graphs*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1999.

[KW02] Lars R. Knudsen and David Wagner. Integral cryptanalysis. In *FSE'02*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127. Springer, 2002.

[Luc01] Stefan Lucks. The saturation attack - A bait for twofish. In *FSE*, volume 2355 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2001.

[MDFK15] 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/2015/516, to appear at ASIACRYPT'15.

[Mul03] Frédéric Muller. A new attack against khazad. In *Advances in Cryptology-ASIACRYPT 2003*, pages 347–358. Springer, 2003.

[PU16] Léo Perrin and Aleksei Udovenko. Algebraic Insights into the Secret Feistel Network. In Thomas Peyrin, editor, *Fast Software Encryption: 23rd International Workshop, FSE 2016, Bochum, 2016.*, Lecture Notes in Computer Science, page To Appear. Springer Berlin Heidelberg, 2016.

[SB15] Markku-Juhani O. Saarinen and Billy Bob Brumley. Whirlbob, the whirlpool based variant of STRIBOB. In Sonja Buchegger and Mads Dam, editors, *Secure IT Systems, 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19-21, 2015, Proceedings*, volume 9417 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2015.

[Tod15] Yosuke Todo. Structural evaluation by generalized integral property. In *EUROCRYPT'15*, volume 9056 of *Lecture Notes in Computer Science*, pages 287–314. Springer, 2015.

# A New SA...S challenges

In order to stimulate further cryptanalysis and research on the security of generic SPN structures, we present a set of parameters for the SA...S schemes, which we deem secure in the light of previous results [MDFK15, DDKL15, GPT15] and new analysis presented in this paper. They are given in Table 5. Notice 24 and 32-bit instances which are *memory-hard*.

Table 5: Secure secret-SPN variants. "BB mem." and "WB mem." correspond to the memory needed to implement such structures in the Black-Box and White-Box settings respectively.

| Block | Layers | Structure | $S$-layer | BB mem. | WB mem. | Security |
|---|---|---|---|---|---|---|
| 12 bits | 7 | $SASASAS$ | 2×(6 bits) | 512 B | 8 KB | 64 bits |
| 16 bits | 7 | $SASASAS$ | 2×(8 bits) | 2 KB | 132 KB | 64 bits |
| 24 bits | 7 | $SASASAS$ | 3×(8 bits) | 3 KB | 50 MB | 128 bits |
| 32 bits | 7 | $SASASAS$ | 4×(8 bits) | 4 KB | 18 GB | 128 bits |
| 64 bits | 7 | $SASASAS$ | 8×(8 bits) | 8 KB | – | 128 bits |
| 128 bits | 11 | $S(AS)^5$ | 16×(8 bits) | 24 KB | – | 128 bits |

## A.1 Proof of Theorem 1

We bound the algebraic degree of $r$ SPN rounds using $\theta_r$:

$$\deg(A(SA)^r) \leq \theta_r.$$

Obviously, $\theta_0 = 1$ holds as $(SA)^0$ is the identity. For larger values, $\theta_r$ is bounded in three different ways: the natural bounds $d^r$ and $n-1$, and the one from Proposition 1:

$$\theta_r \leq n - \left\lceil \frac{n - \theta_{r-1}}{d} \right\rceil.$$

As long as the first bound prevails, the expression of $\theta_r$ is very simple: $\theta_r = d^r$.

We now consider a larger number of rounds. Let $\ell$ be such that $\ell \leq \log_d(n)$. It holds that

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

which, using the base $d$ expansion of $n$, is equal to

$$\theta_{\ell+1} \leq n - \left\lceil \frac{\sum_{i=0}^{\infty} n_i d^i - d^\ell}{d} \right\rceil.$$

Because all coefficients in the numerator except $n_0$ can be divided by $d$, this quantity is equal to:

$$\theta_{\ell+1} \leq n - \left( \sum_{i=1}^{\infty} n_i d^{i-1} - d^{\ell-1} + \left\lceil \frac{n_0}{d} \right\rceil \right).$$

Finally, we note that $\sum_{i=1}^{\infty} n_i d^{i-1} = \lfloor n/d \rfloor$ and conclude that

$$\theta_{\ell+1} \leq n - \left( \left\lfloor \frac{n}{d} \right\rfloor - d^{\ell-1} + \left\lceil \frac{n_0}{d} \right\rceil \right).$$

In fact, we can generalize this equality using a simple induction for $r \leq \ell$. To simplify its writing, we define $\psi_i$ as follows:

$$\psi_1 = \lceil n_0/d \rceil \ , \quad \psi_{i+1} = \left\lceil \frac{n_i + \psi_i}{d} \right\rceil .$$

Our induction hypothesis is then

$$\theta_{\ell+r} \leq n - \left( \left\lfloor \frac{n}{d^r} \right\rfloor - d^{\ell-r} + \psi_r \right), \tag{8}$$

and we have established that it holds for $r = 1$. Suppose now that it holds for some $r$. Using Proposition 1, we deduce that

$$\theta_{\ell+r+1} \leq n - \left\lceil \frac{n - \left(n - \lfloor n/d^r \rfloor + d^{\ell-r} - \psi_r\right)}{d} \right\rceil ,$$

which implies

$$\theta_{\ell+r+1} \leq n - \left\lceil \frac{\sum_{i=r}^{\infty} n_i d^{i-r} - d^{\ell-r} + \psi_r}{d} \right\rceil .$$

Using again that all $d^{i-r}$ for $i \geq r$ are divisible by $d$ except for $d^0$, we can rewrite this inequality as

$$\theta_{\ell+r+1} \leq n - \left( \sum_{i=r}^{\infty} n_i d^{i-r-1} - d^{\ell-r-1} + \left\lceil \frac{n_r + \psi_r}{d} \right\rceil \right).$$

We simplify this expression using that $\sum_{i=r}^{\infty} n_i d^{i-r-1} = \lfloor n/d^{r+1} \rfloor$ and the definition of $\psi_{r+1}$ and obtain

$$\theta_{\ell+r+1} \leq n - \left( \left\lfloor \frac{n}{d^{r+1}} \right\rfloor - d^{\ell-r-1} + \psi_{r+1} \right).$$

Let us simplify this expression. First, the quantity $\lfloor n/d^r \rfloor - d^{\ell-r}$ can be written using the base $d$ expansion of $n$:

$$\lfloor n/d^r \rfloor - d^{\ell-r} \leq \sum_{i \geq r,\ i \neq \ell} n_i d^{i-r} + (n_r - 1) d^{\ell-r}.$$

Furthermore, all $n_i$ for $i > \ell$ are equal to 0. Using this, the inequality becomes:

$$\lfloor n/d^r \rfloor - d^{\ell-r} \leq \sum_{i=r}^{\ell-1} n_i d^{i-r} + (n_r - 1) d^{\ell-r}.$$

Second, we can easily compute $\psi_i$ using the base $d$ expansion of $n$. We again proceed inductively using the following hypothesis:

$$\psi_i = \begin{cases} 0 \text{ if } \ n_{i-1} = n_{i-2} = \ldots = n_0 = 0, \\ 1 \text{ otherwise.} \end{cases}$$

The equality obviously holds for $i = 0$ as $\lceil n_0/d \rceil = 0$ if and only if $n_0 = 0$, otherwise it is equal to 1 because $n_j < d$ for all $j$. Assuming the equality holds for $i$, let us now compute $\psi_{i+1}$. By definition,

$$\psi_{i+1} = \left\lceil \frac{n_i + \psi_i}{d} \right\rceil ,$$

which, given that $n_i < d$ and $\psi_i \leq 1$, is at most equal to 1. Thus, $\psi_{i+1} = 1$ if and only if either $\psi_i$ or $n_i$ is strictly greater than 0. This concludes the induction.

We deduce Theorem 1.