Non Linearizable Entropic Operator

Daniel Nager
daniel.nager@gmail.com

January 2025

Abstract

In [Pan21] a linearization attack is proposed in order to break the cryptosystem proposed in [Gli21]. We want to propose here a non-linearizable operator that disables this attack as this operator doesn't give raise to a quasigrup and doesn't obey the latin square property.

1 Entropic operator definition

As a reminder let's define what an entropic operation is, in particular, if we take $\circ$ as operator it must satisfy:

$(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ c)$

so in this formula b and c can be interchanged without altering the result, but not necessarily other exchanges are possible.

If with a fixed a, every b gives a distinct result, i.e. is a bijection, and the same happens with a fixed b with respect to a variable a, then is a quasigroup. We're not interested on quasigroups since are highly questioned by [Pan21], but in entropic operators that aren't a quasigroup, so the operations cited are many-to-one mappings and not one-to-one. This disables the referenced linearization attack of [Pan21].

2 Definition of two algebraic structures

We will use 4-bit, other amount of bits is possible, binary numbers and will interpret it in two algebraic structures, such as:

$\mathbb{F}_{16}$, the finite field of 16 elements, and in particular its square operation, and

$\mathbb{Z}_2[x]\backslash(x^4+1)$, polynomials on $\mathbb{Z}_2$ modulo x^4+1, and in particular multiplying by x, that results in a bitwise rotation to the left of the 4-bit array. We call this rotation of a value b as $r(b)$.

3 Basic entropic operator

The entropic operation we will work with is:

$a \circ b = a \oplus b^2 \oplus r(b^2)$

It's straightforward to see that:

$(a \circ b) \circ (c \circ d) = a \oplus b^2 \oplus r(b^2) \oplus c^2 \oplus d^4 \oplus r(d^2)^2 \oplus r(c^2) \oplus r(d^2)^2 \oplus r(r(d^2)^2)$

We check that b and c can be swapped so the entropic property holds.

Due to the fact that $\neg a \oplus \neg b = a \oplus b$, we can state that the operator $\circ$ is non-injective, in particular its a two-to-one map, so the resulting mathematical structure is not a quasigrup, but almost.

We must note that, due to the mixing of different algebraic structures, $r(a^2) \neq r(a)^2$, so some simplifications cannot be done in complex formulas.

4 Entropic list operator and mixing

We will be working with lists of 4-bit elements, and define an extension of the basic entropic operator that's entropic as well:

$A \cdot B = A \circ R(B)$,

where in lists $A \circ B$ means element wise operation of the previously defined $\circ$ operation and $R(B)$ means a rotation of the list B itself, one position to the left or to the right item-wise. This operation on lists is entropic as well.

Finally we define, a new structure which is a pair of such lists as just presented and a mixing algorithm that will give as a result a pair of lists $R = m(T, K)$:

$T = [T_1, T_2]$, $K = [K_1, K_2]$, where items of T and K are the lists of 4-bit elements.

First step is to set up an initial state:

$S_0 = [T_1 \cdot K_1, T_2 \cdot K_2]$,

next at each step if we have $S_i = [A_i, B_i]$ we compute $S_{i+1} = [A_i \cdot B_i, B_i \cdot (A_i \cdot B_i)]$.

The final step is to apply again the initial value of the second element:

$S_r = [A_n \cdot K_1, B_n \cdot K_2]$

Now, it's proven in [NN21] that the operation $R = m(T, K)$ is as well entropic if $\cdot$ is. As a debrief finding K knowing T and R is assumed to be infeasible.

5 Protocol for key agreement and digital signature

The secret agreement and digital signature protocols are the same as the ones described in [NN21].

To do signatures, we can profit from the following equality:

$m(m(C,H),m(K,Q)) = m(m(C,K),m(H,Q))$

Then $\langle C, m(C,K)\rangle$ are the signer credentials, and $\langle m(H,Q), m(K,Q)\rangle$ the signature. Q must be different for each signature, while K is always the same. H is the hash to sign and C a constant value.

To do a secret agreement we profit from the equality

$m(m(C,K),m(Q,C)) = m(m(C,Q),m(K,C))$, where C is an agreed constant and K, Q are secret values of each party in the agreeement.

6 Security analysis

The Bruck-Murdoch-Toyoda theorem [Bru44] [Mur41] [Toy41] states that every entropic quasigroup has the form:

$a * b = \sigma(a) \cdot \tau(b) \cdot c$

where $(G,\cdot)$ is an abelian group and σ and τ are commuting automorphisms of $(G,\cdot)$. This is the basis and a prerequisite to apply linearization attack, but in this case the basic operator $a \circ b$ doesn't define a quasigroup so we can assert such automorphisms doesn't exist.

Additionally $r(a)^2 \neq r(a^2)$, so after enough steps of applying the mixing algorithm the resulting formula grows enough to be intractable, so no gaussian-like elimination can be done despite we're working with bits, rotations and xors, due to the interference of squaring.

References

[Pan21] Lorenz Panny. *Entropoids: Groups in Disguise.* Cryptology ePrint Archive, Paper 2021/583. 2021. URL: `https://eprint.iacr.org/2021/583`.

[Gli21] Danilo Gligoroski. *Entropoid Based Cryptography.* Cryptology ePrint Archive, Paper 2021/469. 2021. URL: https://eprint.iacr.org/2021/469.

[NN21] Daniel Nager and "Danny" Niu Jianfang. *Xifrat - Compact Public-Key Cryptosystems based on Quasigroups.* Cryptology ePrint Archive, Paper 2021/444. 2021. URL: https://eprint.iacr.org/2021/444.

[Bru44] Richard H. Bruck. "Some Results in the Theory of Quasigroups". In: *Transactions of the American Mathematical Society* 55.1 (1944), pp. 19–52. ISSN: 00029947. URL: http://www.jstor.org/stable/1990138.

[Mur41] D. C. Murdoch. "Structure of Abelian Quasi-Groups". In: *Transactions of the American Mathematical Society* 49.3 (1941), pp. 392–409. ISSN: 00029947. URL: http://www.jstor.org/stable/1989940.

[Toy41] Kôshichi Toyoda. "On axioms of linear functions". In: *Proceedings of the Imperial Academy* 17.7 (1941), pp. 221–227. URL: https://doi.org/10.3792/pia/1195578751.