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.

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].

Basic algebraic structure

We will use polynomials of degree $n-1$ modulo $x^n - 1$ with coefficients modulo a large prime p:

$F = \mathbb{F}_p[x] \backslash (x^n - 1)$

We will operate on this field and applying parametrization.

$a \in F$, $a(x^e)$ is the application of x^e to the polynomial a. We remind that $a, b \in F$, $a(x^e) \cdot b(x^e) = (a \cdot b)(x^e)$.

Basic entropic operator

The entropic operation we will work with is:

$a \circ b = a \cdot b \cdot b(x^e)$. As an example we can take $e = n - 1$.

It's straightforward to see that:

$(a \circ b) \circ (c \circ d) = a \cdot b \cdot b(x^e) \cdot c \cdot d \cdot d(x^e) \cdot c(x^e) \cdot d(x^e) \cdot (d(x^e))(x^e)$

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

Due to the fact that $-a \cdot -b = a \cdot b$, and so $-b \cdot (-b)(x^e) = b \cdot b(x^e)$, 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.

Entropic operator mixing

We will define a mixing process $r = m(t, k)$, where r, t and k are pairs of elements in F.

So we have:

$r = (r_1, r_2)$, $t = (t_1, t_2)$ and $k = (k_1, k_2)$, $r_1, r_2, t_1, t_2, k_1, k_2 \in F$

First we join t and k values to get an initial state:

$r = (t_1 \circ k_1, t_2 \circ k_2) = (r_1, r_2)$

Next at each step we mix the two values of the tuple:

$r := (r_1 \circ r_2, r_2 \circ (r_1 \circ r_2))$

And as a final step we mix again k to prevent mixing's reversal:

$r := (r_1 \circ k_1, r_2 \circ k_2)$

Now, it's proven in [NN21] that the operation $r = m(t, k)$ is as well entropic if $\circ$ is. Also, finding k knowing t and r is assumed to be infeasible.

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.

Non linearizability and Gaussian elimination

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.

On the side of a possible pseudo Gaussian elimination for exponentiation we assert that a and $a(x^n)$ must be treated as different unknowns, so if we trace the mixing process we can end with a system of equations, but due to this assertion we got at least half equations than unknowns, making this Gaussian elimination unfeasible if p is chosen big enough as we must guess half of those unknowns.

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.