Entropic Quasigroup Based Secret Agreement Using Large Order Automorphisms

Daniel Nager
daniel.nager@gmail.com

August 2023

Abstract

In this paper a method to build Secret Agreement algorithms is presented, which only requires an abelian group and at least one automorphism of the operator of this group. An example of such an algorithm is also presented. Knowledge of entropic quasigroups and Bruck-Murdoch-Toyoda theorem on how to build a quasigroup with these two elements is assumed.

Expanding complexity of an entropic quasigroup

Let $E = (G, *)$, an entropic quasigroup. We want to do a mixing process in order to achieve complexity, we will compute the following mixing:

Let $c = (c_1, c_2), k = (k_1, k_2)$, $c_1, c_2, k_1, k_2 \in G$ we define $r = c\bar{*}k$ as:

First we mix the parameters:

$s_1 \leftarrow c_1 * k_1$, $s_2 \leftarrow c_2 * k_2$

For a fixed number of times n we operate the state:

$s_1 \leftarrow s_1 * s_2$
$s_2 \leftarrow s_2 * s_1$

Finally we mix the second parameter k:

$r_1 \leftarrow s_1 * k_1, r_2 \leftarrow s_2 * k_2, r = (r_1, r_2)$

It's not hard to prove that $c\bar{*}k$ is an entropic quasigroup operation as well, and, with a fixed c is a bijection. n can be as large as needed in order to match security requirements.

Construction of the entropic quasigroup

We will use the result of Bruck-Murdoch-Toyoda theorem to build $*$ operation of E taking into consideration some security constraints.

So, provided γ an automorphism of G, we define:

$a, b \in G,\ a * b = a \cdot \gamma(b)$

γ must have a big order under composition so the smallest n such where $\gamma^n(a) = a$ must big enought taking into consideration security parameters.

Let's note now that any number of applications of the quasigroup operation of automorphisms results in an automorphism. The same happens with composition, so we can use any combination of automorphisms:

$\gamma(b) = \alpha(b) \cdot \beta(b)$ or $\gamma(b) = \alpha(\beta(b))$

as an example. This allows a lot of combinations that increases complexity and makes the theoretic scheme seemingly hard to break just using γ and not its definition, together with $\bar{*}$.

Secret agreement

We profit from the fact that $(c\bar{*}k)\bar{*}(q\bar{*}c) = (c\bar{*}q)\bar{*}(k\bar{*}c)$, so k and q can be exchanged.

Let's state that when using $\bar{*}$ operation we're assuming elements are in $G \times G$.

Let's denote A and B the partners, A chooses a secret k and publishes $c\bar{*}k$ and B chooses a secret q and publishes $c\bar{*}q$, c is an agreed public constant. With these public values and the secret information, with the equality above a common secret can be computed.

Let's note that $c\bar{*}k \neq k\bar{*}c$, or in other words, if we isolate from constants k in $c\bar{*}k$ and in $k\bar{*}c$ both values are different due to the asymmetry in mixing with nested composed automorphisms, so the fact is that one cannot be used to deduce easily the other.

A practical proposal

We will use the finite field $F = \mathbb{F}_{p^4}$ as the group and composition of polynomials, with at least one degree one polynomial, as automorphisms. Degree one polynomials are well know as being the iterating function of LGCs and it's period under composition in F is easy to find.

So an instance of $*$ can be:

$a, b \in \mathbb{F}_{(2^{64}+24195)^4}$, using primitive polynomial $x^4 + x + 1$ as a modulo for computations, $a * b = a \cdot (b \circ (2x+1) \cdot (b \circ (x^2 + 6x + 1)$, where $\cdot$ here is the product, and applying the mixing described above with $n = 256$ steps we can get a strong function $c\bar{\cdot}k$ to be used with the secret agreement described.

In this case public value's size is 512 bits.

Conclusion

We've presented a general method to build secret agreements, and two examples on how to do it. While the examples can be broken with some method, the hope is the general method will be not so easy to break, as there is a wide range of abelian groups and automorphisms on these groups, so there's actually two proposals to break in this document, the practical proposal and the general method. Let's note that the main point of all this is that those automorphisms, or at leas one of them have an order under composition large enough to reach security requirements.