Some Security Arguments For Xifrat1

Xifrat1 is a family of cryptosystems based on abelian quasigroups and is the redesigned successor to the previous Xifrat0 cryptosystems. This paper discuss and attempt to argue its security, and provide this as foundation for future reasoning and/or refuting of its security.

Authors: Jianfang "Danny" Niu (dannyniu {at} hotmail {dot} com)

!NOTE! The HTML rendering of this document is not authoritative, and readers seeking a stable reference should look for the PDF version published at official sources.

Table of Contents

1. Introduction

The 3rd round of NIST PQC project had recently completed and first set of candidates to be standardized is announced. Also announced is the NIST's intentions to standardize a more efficient general-purpose signature scheme. For the announced candidates -

- The most efficient and easiest to implement Dilithium has big cryptograms,
- The most compact Falcon has intricate implementation requirements,
- The one with the most confidence in security - SPHINCS+ has huge signatures.

Xifrat1 [Niu22] is a new proposal based on abelian quasigroups, that provides compact cryptograms, and is reasonably efficient. The paper proposing Xifrat1 didn't touch deep on security arguments. This paper will provide some arguments for its security, and serve as future reference for reasoning and/or refuting its security.

2. The Xifrat1 Construction

The cryptograms in Xifrat1 are vectors of 12 64-bit words, built from 3 layers, bootstrapped from a 16x16 randomly chosen abelian quasigroup whose set we call the "quartet". The cryptograms and each layer below it follow the "restricted-commutative" property.

$$P{<}Q{,}n{>} := (\ Q^n\ ,\ O : Q^n \times Q^n \rightarrow Q^n\ )$$

where

$$O(a^n, b^n) = uvuv$$ and

$$a, b \in Q$$

$$u = (a_1\ a_2\ ...\ a_n \mid a_2\ a_3\ ...\ a_1 \mid ... \mid a_n\ a_1\ ...\ a_{n\text{-}1}\ )$$

$$v = (b_1\ b_2\ ...\ b_n \mid b_2\ b_3\ ...\ b_1 \mid ... \mid b_n\ b_1\ ...\ b_{n\text{-}1}\ )$$

We use 1-based indexing here for ease of notation. The Xifrat1 paper [Niu22] uses 0-based indexing

The design of the new O mixing function has 2 phases - the cycling phase where u and v are computed from vector elements of a and b; the alternating phase of $uvuv$. By generalized restricted-commutativity, the cycling and alternating phases can be computed in either order and results in the same value output. The resulting template mixing function preserves the restricted-commutativity property from a lower layer to a higher layer The Xifrat1 cryptosystem uses 3 layers:

The 1st layer is $(B{,}Blk) := P{<}\text{"quartets"}{,}16{>}$
The 2nd layer is $(V{,}Vec) := P{<}B{,}6{>}$
The final outter-mose layer is $(D{,}Dup) := P{<}V{,}2{>}$

3. Attack 1: Evaluate without Full Knowledge of 1 Operand

The first attack we discuss is the "evaluation without full knowledge of either operand" attack. This attack was present in a most fatal form in Xifrat0, and was quickly broken [Niu21] back then.

The same apply to Xifrat1. Recall that the "Blk" function works over a vector of 16 quartets. If we can find either of u or v , then we can use that knowledge to compute that function - because the alternating phase works parallelly over the vector of tritet. This attack has to be blocked at the cycling phase of a higher layer.

The cycling phase at a higher layer mixes together the vector elements of the lower layer, making it necessary to recover the vector in its entirety to be able to compute the mixing function. This is why at 384 bits, we still need a "Dup" layer on top of the "Vec" layer.

4. Attack 2: Group Theoretic Analysis

This section discusses group theoretic cryptanalysis on Xifrat1. I had briefly discussed this with the author of [Panny21] - we hold different opinion over this.

As we said in [Niu22], the 16x16 latin square was chosen randomly; and we assume its quasigroup operation is also random, in the sense that it *behave as if randomly*.

It's a fact [Bruck44] [Murdoch39] [Toyoda41] that, any quasigroup, like that we've been using, can be decomposed into a group with 2 automorphisms:

$f(a,b) = g(a) + h(b) + c$ where f is the quasigroup operation, g and h are 2 automorphisms which we assume *are independent of each other* and *behave as if randomly*, and c is a constant from the quasigroup set, and $+$ is the operation of the decomposed group.

Now let's see an example:

$$g(x) + h(y) = u$$
$$g(y) + h(x) = v$$

If g and h are truely random, then the only way to find x , y from u , v would be to try every possible solution and verify each of them to find out. Because we generated our 16x16 quasigroup randomly, we assume that the underlaying automorphisms fulfills this property. It is further assumed, that composition of randomly-behaving maps are also randomly-behaving.

The Blk function can now be reverted, by first searching 16 independent quartets from the alternating phase, then solving the "cycling" equations system, which consists of 16 group equations, each with 16 automorphisms that we had assumed to be "randomly-behaving".

There are 2 crucial assumptions we make, as the basis for believing that the mixing funcitons at higher layer are more difficult to to invert than the Blk function.

1. The group automorphisms exploitation is the most efficient attack applicable to the cycling-alternating mixing function formula *when assuming* that there is a efficient way to evaluate the automorphisms.
2. There is no efficient way to find or evaluate larger group automorphisms from the group and automorphisms underlaying the smaller abelian quasigroup *assuming* the underlaying abelian quasigroup is randomly-behaving.

Additionally, we assume that the expansion result of abelian quasigroup formula at higher layer into group automorphisms is no more efficiently solvable than applying layer-by-layer approach according to the preceding list, as the expansion of the formula terms is polynomial (which we believe makes the solution of the equasions system super-exponential, but we have yet no way of being sure).

Annex A. References

- [Bruck44] Richard H. Bruck; *Some Results in the Theory of Quasigroups*; In: *Transactions of the American Mathematical Society* 55.1 (1944), pp. 19-52.
- [Murdoch39] David C. Murdoch; *Quasi-Groups Which Satisfy Certain Generalized Associative Laws*; In: *American Journal of Mathematics* 61.2 (1939), pp.509-522.
- [Toyoda41] Koshichi Toyoda; *On axioms of linear functions*; In: *Proceedings of the Imperial Academy* 17.7 (1941), pp.221-227.
- [Panny21] Lorenz Panny; 2021-05 *Entropoids: Groups in Disguise*; https://ia.cr/2021/583
- [NN21] Daniel Nager, and Jianfang "Danny" Niu; 2021-04 *Xifrat - Compact Public-Key Cryptosystems based on Quasigroups*; https://ia.cr/2021/444
- [Niu21] Jianfang "Danny" Niu; 2021-04 *Xifrat Cryptanalysis - Compute the Mixing Function Without the Key*; https://ia.cr/2021/487
- [Niu22] Jianfang "Danny" Niu; 2022-04 *Resurrecting Xifrat - Compact Cryptosystems 2nd Attempt*; https://ia.cr/2022/429