Xifrat Cryptanalysis - Compute the Mixing Function Without the Key

Xifrat was a cryptosystem proposed about half a month ago. This paper demonstrate an attack that computes the mixing function without knowing its key.

Authors:

"Danny" Niu Jianfang
(Family name is "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

Xifrat [NN21] is a public-key cryptosystem proposed in earlier 2021 by D.Nager with parameters and instantiation selected by DannyNiu/NJF. We demonstrate in this paper that its possible to compute its mixing function $m(r,k)$ without knowing k

2. The Attack on $m(r,k)$

We import the definitions, propositions, and notations used in the proof of correctness in [NN21].

Due to the "restricted-commutative" property of the underlaying the mixing function $m(r,k)$ can be re-written as $(s'\ j'\ k)$ where $s' = e(r)$ and $j' = e(k)$. This results in the output of $m()$ can be re-written as r operating element-wise with 131 independent pairs of tritets.

Finding such set of pairs of tritets requires only collecting a few pairs of cryptogram, and searching only for $131 \cdot 2^{3 \cdot 2} \approx 2^{13}$ numbers.

The attack completely breaks Xifrat-Sign, and can recover the private key used by the peer in Xifrat-Kex.

Annex A. References

- [NN21] D.Nager, DannyNiu/NJF, *Xifrat - Compact Public-Key Cryptosystems based on Quasigroups* https://eprint.iacr.org/2021/444