UNIVERSITY of
SOUTH
FLORIDA

Post-Quantum Group-based Cryptography: Breaking Xifrat

Kianna Cabral, Dmytro Savchuk
Northeastern University, University of South Florida

ABSTRACT

In recent years, The National Information Technology Laboratory (NIST) has been calling for a transition to post-quantum cryptography. With the rapid advancement of quantum computers, established cryptographic methods are at risk of being compromised. Traditional public-key cryptosystems can no longer ensure the confidentiality and integrity of digital communications.
As a potential solution to this challenge, Xifrat1-Sign, a digital signature scheme based on quasigroups, has been proposed to NIST. By leveraging the special properties of the algebraic structure of quasigroups, and particularly, the restricted-commutativity, this cryptographic scheme aims to achieve a quantum resistant security.
To assess its effectiveness, we conducted a cryptanalysis of the Xifrat cryptosystem using computational group theory and differential statistical analyses. As a result, we have identified several vulnerabilities in its design—a step towards breaking the full system.
This study makes a significant contribution to the improvement of the Xifrat cryptosystem and other quasigroup-based schemes, but also to the reinforcement of new cryptographic frameworks in the face of emergent quantum technologies.

Keywords: public-key cryptography, post-quantum cryptography, digital signature key exchange, quasigroups, “entropic” quasigroup, “entropoids”, group theory.

CONTACT

Kianna Cabral
Northeastern University
Email: cabral.ki@northeastern.edu
Phone: +1(508)904-4062

INTRODUCTION

Xifrat1-Sign[1], a quasigroup-based cryptographic system, was recently proposed as a candidate to NIST’s Post-Quantum Cryptography Standardization project[2]—an effort to develop post-quantum cryptographic algorithms that ensure data confidentiality, authenticity, and integrity in the quantum era.
Xifrat1-Sign1, if proven secure, could be the most compact and efficient post-quantum cryptosystem proposed to date, achieving a minimum of 192-bit post-quantum security. The algorithm relies on a discrete-logarithm-like problem, but the mathematical structure of quasigroups seems resistant to Shor's algorithm. Despite being in its early stages with limited research and scrutiny, group-based cryptography is gaining popularity due to its promising properties.

Quasigroups

Quasigroup, an algebraic structure with one binary operation, differs from a group since it does not require associativity, nor an identity element, and whose multiplication is given by a Latin Square. In addition, Xifrat is based on a quasigroup with the special property of restricted-commutativity[3].

Properties of the considered quasigroup:

i. Non-Associative *In General*: (ab)c ≠ a(bc)
ii. Non-Commutative *In General*: ab ≠ ba
iii. Restricted-Commutativity: (ab)(cd) = (ac)(bd)
iv. Generalized Restricted-Commutativity

$$(x_{1,1}x_{1,2}\dots x_{1,n})(x_{2,1}x_{2,2}\dots x_{2,n})\dots(x_{m,1}x_{m,2}\dots x_{m,n}) =$$
$$(x_{1,1}x_{2,1}\dots x_{m,1})(x_{1,2}x_{2,2}\dots x_{m,2})\dots(x_{1,n}x_{2,n}\dots x_{m,n})$$

Additional properties needed for basic security:

- The quasigroup table should overall be not symmetric.
- The quasigroup table should not have any fixed points.

While non-associativity ensures one-way functions, non-commutativity provides quantum security.

Xifrat algorithm

The construction of Xifrat relies upon three core mixing functions based on multiplication in quasigroup: BLK, VEC, and DUP (D) that use 64-,384-,768-bit vectors as inputs, respectively, with each function built upon the previous. These functions shuffle, randomize, and confound the message.
Xifrat1-Sign. key generation scheme is the following:

1. Uniformly randomly generate three 768-bit vectors: c,k, and q,
2. Compute $p_1 = D(c,k)$, $p_2 = D(k,q)$,
3. Return public-key $pk = (c, p_1, p_2)$ and secret-key $sk = (c,k,q)$

Purpose: We aim to conduct a cryptanalysis of the Xifrat cryptosystem to verify the security and reliability of its algorithm against quantum threats and other attacks.

METHODS

The implementation of the Xifrat algorithm was performed in GAP including Loops Package[4]. The multiplication table of the quasigroup Q utilized in Xifrat is given by a Latin Square represented in GAP as:

```
Q:= QuasigroupByCayleyTable([
  [10,11,0,3,12,4,1,5,15,6,8,14,2,9,7,13],
  [15,8,9,7,2,13,5,1,10,14,11,6,12,0,3,4],
  [2,3,6,11,15,5,13,4,12,0,7,9,10,14,8,1],
  [0,5,10,4,14,3,8,11,9,2,1,12,6,15,13,7],
  [8,15,1,12,3,14,0,9,11,13,10,4,7,5,2,6],
  [6,4,2,5,9,11,7,3,14,10,13,15,0,12,1,8],
  [13,14,7,9,5,15,2,12,4,8,6,11,1,3,0,10],
  [12,7,14,8,10,1,4,13,2,9,3,0,15,6,11,5],
  [5,0,11,6,13,2,15,10,1,3,9,7,4,8,14,12],
  [14,13,12,1,0,8,3,7,6,15,4,10,9,2,5,11],
  [1,9,8,14,4,12,10,15,5,7,0,3,13,11,6,2],
  [7,12,13,15,11,9,6,14,3,1,2,5,8,4,10,0],
  [9,1,15,13,6,7,11,8,0,12,5,2,14,10,4,3],
  [4,6,3,0,1,10,12,2,13,11,14,8,5,7,9,15],
  [11,10,5,2,7,6,9,0,8,4,15,13,3,1,12,14],
  [3,2,4,10,8,0,14,6,7,5,12,1,11,13,15,9]
  ]);
```

Two approaches to the assault of Xifrat were devised:

- Differential cryptanalysis
- Exploiting algebraic properties of Q

The statistical tests were executed to gauge the overall performance of the system as it detects for any non-randomness and predictability of the output given the inputs.
Additionally, newly discovered algebraic properties of the quasigroup Q effectively allowed us to comprise the main block of the system.

RESULTS

Differential cryptanalysis

Avalanche test is used to measure the sensitivity of the output of the mixing functions given a certain change in the input.

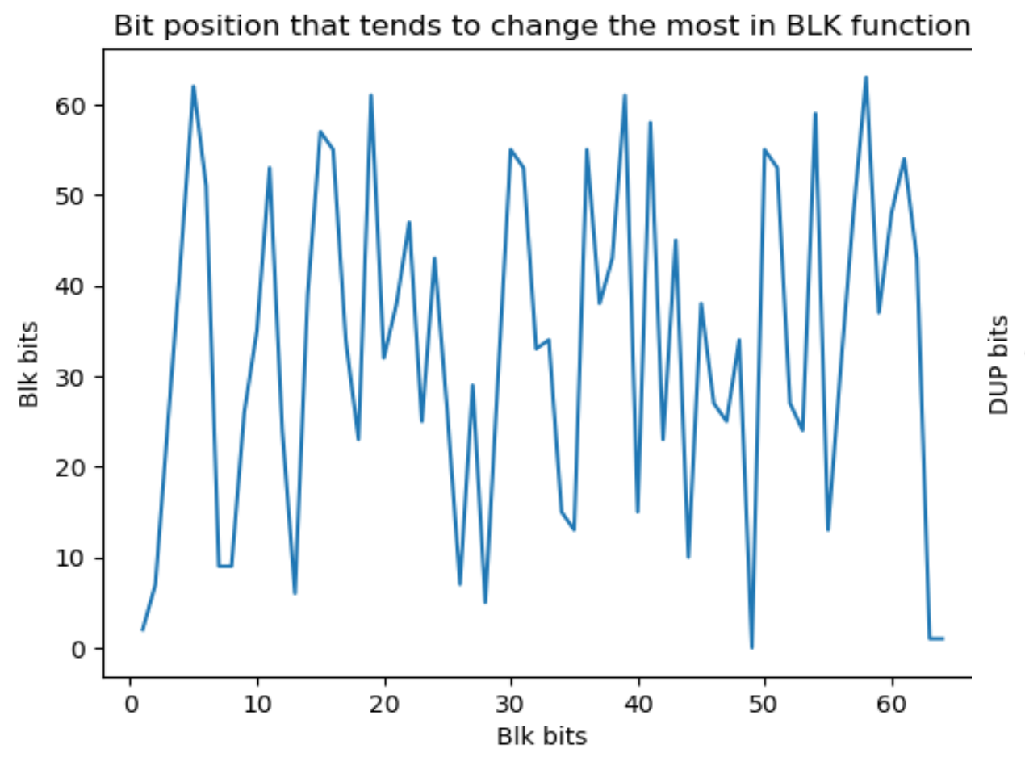

Figure 1. Variability of BLK.

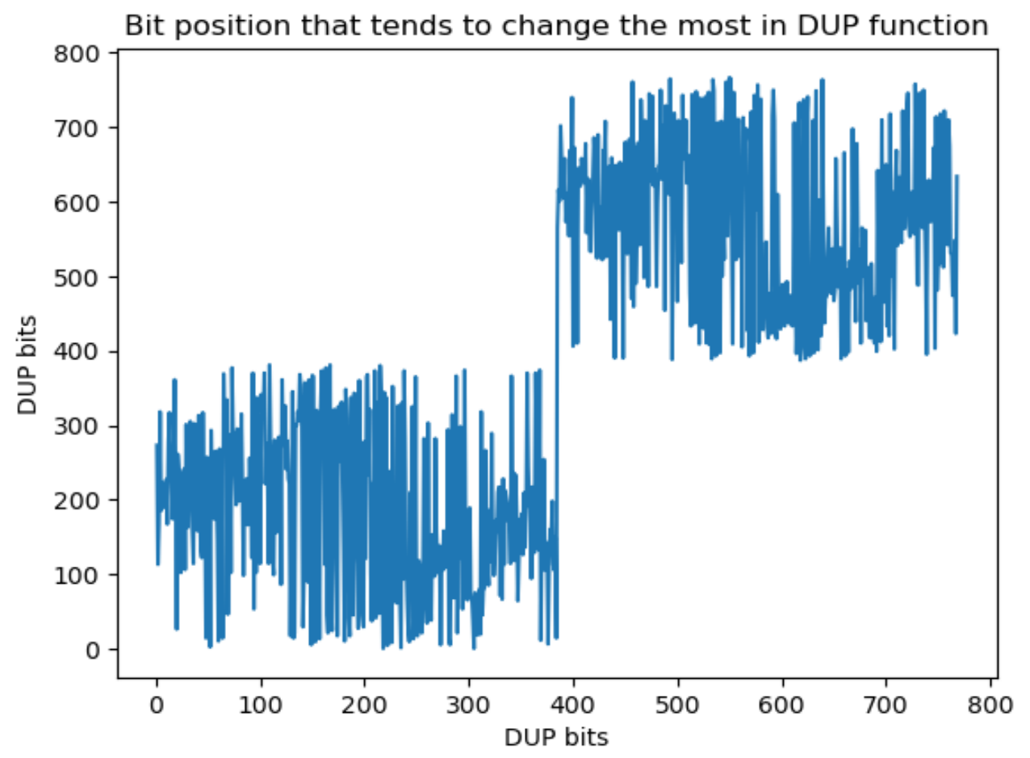

Figure 2. Variability of DUP.

While the intermediate ciphertext resulting from the BLK function manifests a random variability, the final ciphertext generated by the DUP function exhibits a limitation. Lower-range bits are insensitive to changes to upper-range bits and vice-versa, as shown below.

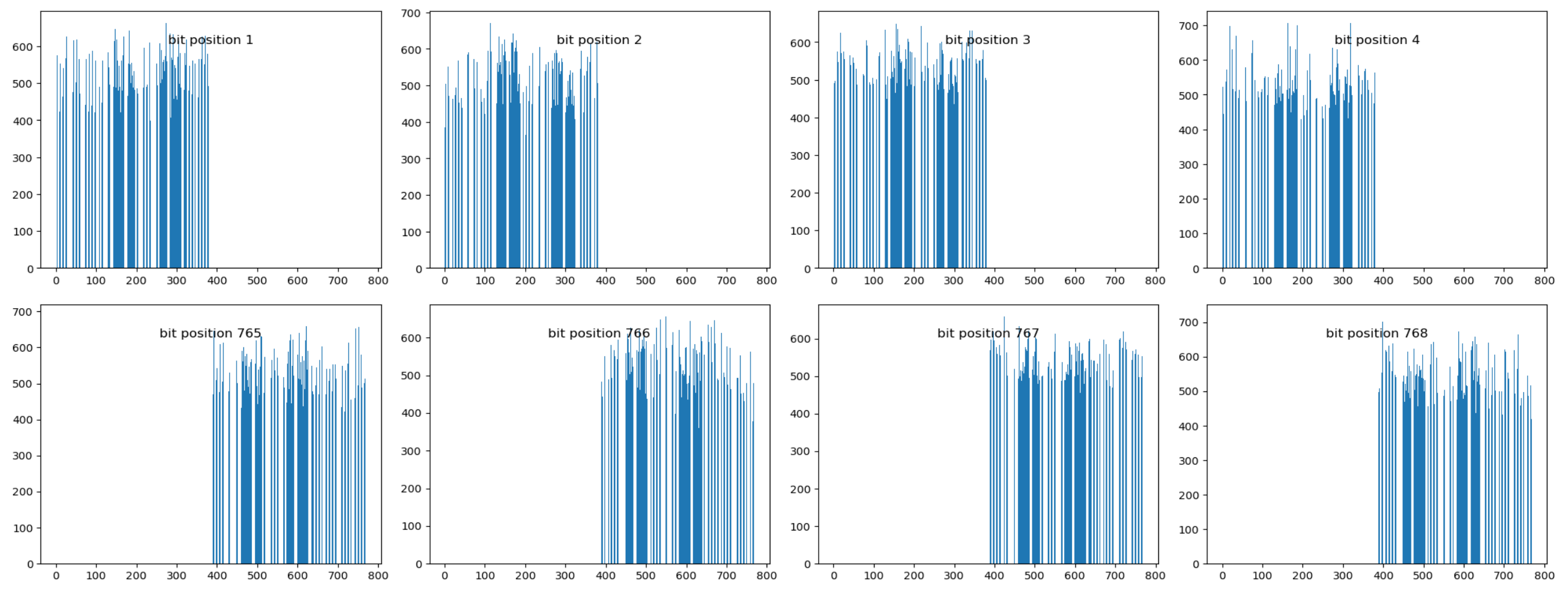

Figure 3. Bits flipped in DUP outputs.

RESULTS

Algebraic cryptanalysis

By exploiting the generalized restricted commutativity of this quasigroup, the mixing functions were simplified.

Theorem 1
Given vectors $A = (a_i)$, $B = (b_i)$ over Q,
let $X = (x_i)$ be a vector with components $x_i = a_i b_i a_i b_i$.
Then $BLK(A,B) = \sigma(x)$, where

$$\sigma\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 x_2 \dots x_{16} \\ x_2 x_3 \dots x_1 \\ \vdots \\ x_{16} x_1 \dots x_{15} \end{pmatrix}$$

Proposition
$\sigma^{16} = id$, so for each vector C $\sigma^{-1}(C) = \sigma^{15}(C)$.

Theorem 2.
Given A, $C = BLK(A,B) = \sigma(X)$, there is an algorithm to find B.

The security of the system is based on the complexity to find B from A and DUP(A,B). In other words, on the assumption that DUP is a one-way function.

CONCLUSIONS

We have demonstrated that the Xifrat public-key cryptosystem is less secure than anticipated. The avalanche tests reveal the limitations of the DUP mixing function in effectively shuffling the inputs for randomization. Furthermore, the restricted number of bits flipped not only undermines the initially promised security extent but also introduces a substantial security risk.
We also showed that using algebraic properties of Q we can undo the first layer of shuffling, thus seriously compromising the security of the system.

REFERENCES

1. Niu, J. Xifrat1-sign.i dss specification document. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/xifrat1-sign-i-spec.pdf (2023).
2. Round 1 Additional Signatures - Post-Quantum Cryptography: Digital Signature Schemes | CSRC | CSRC — csrc.nist.gov
(2023).
3. D.Gligoroski. Entropoid Based Cryptography. https://eprint.iacr.org/2021/469
4. Nagy, G. P. & Vojtechovský, P. The LOOPS Package Computing with quasigroups and loops in GAP (2022). https://docs.gap-system.org/pkg/loops/doc/manual.pdf).

ACKNOWLEDGEMENTS

I thank the National Science Foundation (NSF) for funding this REU and the University of South Florida for welcoming us. A heartfelt thank you to Dr. Biasse and Dr. Savchuk for making this happen and offering us this exceptional opportunity! Another thank you to the rest of my cohort for the good advice and encouragement along the way. Finally, I would like to express my sincerest gratitude to my advisor Dr. Savchuk for all the effort, patience, and unwavering support.