Proceedings of the International Conference IMCS-60, MSU
October 10–13, 2024, Chisinau, Republic of Moldova

Some Hash Functions Based on Quasigroups

Vladimir Cernov, Victor Shcherbacov

Abstract

In this paper, we consider the construction of hash functions based on finite quasigroups.

Keywords: quasigroup, Latin square, encryption, one-way function, cryptology, block cipher, symmetric-key encryption.

1 Introduction

Hashing plays a key role in modern information technologies, providing efficient storage, retrieval and integrity checking of data. Traditional hashing methods such as MD5, SHA-1 and their variants, although widely used, face limitations in the case of large data volumes and increased security requirements.

In the recent years, there has been an increased interest in alternative hashing methods based on abstract algebraic structures. Quasigroups and groupoids are important representatives of these structures with unique properties for hashing applications. The high degree of uniqueness of hash values and computational efficiency of their use should be especially noted.

Definitions and basic properties of quasigroups and loops are available in [1, 2, 3].

Definition 1. *A function H() that maps an arbitrary length message M to a fixed length hash value H(M) is a OneWay Hash Function (OWHF), if it satisfies the following properties:*

1.The description of H() is publicly known and should not require any secret information for its operation.

©2024 by Vladimir Cernov, Victor Shcherbacov

2.Given M, it is easy to compute H(M).

3. Given H(M) in the rang of H(), it is hard to find a message M for given H(M), and given M and H(M), it is hard to find a message $M_0(\neq M)$ *such that* $H(M_0) = H(M)$. [4, 5]

Definition 2. *A OneWay Hash Fucntion H() is called Collision Free Hash Function (CFHF), if it is hard to find two distinct messages M and* M_0 *that hash to the same result* $(H(M) = H(M_0))$. [4, 5]

2 The considered hash function

We give a construction of hashing functions based on quasigroups.

Definition 3. *Let* $H_Q() : Q \to Q$ *be a projection defined as follows:*

$$H_Q(q_1q_2...q_n) = ((...(a \star q_1) \star q_2 \star ...) \star q_n$$

Then $H_Q()$ *is said to be a hash function over the quasigroup* $(Q; \star)$. *The element a is a fixed element from Q.*

Example 1. *Let a quasigroup of order 10 be randomly determined. Suppose that this quasigroup has the following multiplication table:*

$\star$	0	1	2	3	4	5	6	7	8	9
0	0	7	9	1	3	4	5	7	2	6
1	7	9	5	2	4	6	3	0	1	8
2	4	1	2	5	6	7	8	9	3	0
3	6	4	0	8	7	5	2	1	9	3
4	3	0	6	9	2	8	7	4	5	1
5	8	2	3	6	9	1	4	7	0	5
6	9	6	4	3	1	2	0	5	8	7
7	1	5	8	4	0	3	6	2	7	9
8	2	8	7	0	5	9	1	3	6	4
9	5	3	1	7	8	0	9	6	4	2

The value of the hash function for the message $M = 0013145123$ would be as follows

$H_2 = ((((((((((2 \star 0) \star 0) \star 1) \star 3) \star 1) \star 4) \star 5) \star 1) \star 2) \star 3) = 3.$

In the first step, we generate a list of quasigroups of order $n, n \in N$. This step is important to ensure the diversity of possible transformations that will be used in the hashing.

Random quasigroups are selected from the generated list. These selected quasigroups will be used in the hashing process to increase persistence and variability of hash values.

For each of the selected quasigroups, the hash value of the original message is calculated. This step allows to obtain intermediate values which will be later combined to form the final hash.

The final step uses a chain hashing method where intermediate hash values are concatenated to produce a final hash value of a given length. This method ensures that the final hash is unique and collision-resistant.

3 Conclusion

In this paper we propose and discuss an approach to constructing a hash function based on quasigroups and the chain hashing method. By randomly selecting quasigroups from a large number of possible variants and using the chain method of combining intermediate hashes, it was possible to create a convenient mechanism for obtaining hash values. In the future, it is planned to further study the optimization of the proposed algorithm and its adaptation for use in systems with higher performance requirements.

Thus, the proposed quasigroup-based hashing method is a promising direction for the development of new cryptographic algorithms and can find wide application in the field of data protection and authentication.

Acknowledgments. The Institutional Research Program of the Moldova State University for 2024–2027 years, subprogram 011303 has supported part of the research for this paper.

References

[1] V. D. Belousov. *Foundations of the Theory of Quasigroups and Loops.* Nauka, Moscow, 1967. (in Russian).

[2] V. D. Belousov. *Elements of Quasigroup Theory: a Special Course.* Kishinev State University Printing House, Kishinev, 1981. (in Russian).

[3] V. A. Shcherbacov. *Quasigroups in cryptology.* Comput. Sci. J. Moldova, vol.17, no.2(50), 2009, pp. 193–228.

[4] J. Dvorsky, E. Ochodkova, and V. Snasel. *Hash functions based on large quasigroups.* Velokonocni kryptologie, pp. 1–8, 2002.

[5] J. Dvorsky, E. Ochodkova, and V. Snasel. *Hashovaci funkce zalozena na kvazigrupach.* In Workshop Milkulasska kryptobesidka, Praha, 2000 (in Czech).

Vladimir Cernov[1], Victor Shcherbacov[2]

[1]Moldova State University, Vladimir Andrunachievici Institute of Mathematics and Computer Science
E–mail: volodya.black@gmail.com
ORCID: https://orcid.org/0009-0004-7695-1141

[2]Moldova State University, Vladimir Andrunachievici Institute of Mathematics and Computer Science
E–mail: scerb@math.md
ORCID: https://orcid.org/0000-0002-5319-5951