Non-Binary Constant Weight Coding Technique

Alexandr Kuznetsov [1[0000-0003-2331-6326]], Anastasiia Kiian [1[0000-0003-2110-010X]], Tetiana Kuznetsova [1[0000-0002-5605-9293]] and Oleksii Smirnov [2[0000-0001-9543-874X]]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, nastyak931@gmail.com,
kuznetsova.tatiana17@gmail.com
[2]Central Ukrainian National Technical University, avenue University, 8, Kropivnitskiy, 25006, Ukraine, dr.smirnovoa@gmail.com

Abstract. This paper presents research results of mixed base number systems using a binomial representation of numbers and nonlinear coding techniques by constant weight codes, which are based on a binomial count. Also we propose a technique of non-binary constant weight coding based on a generalized binomial-positional representation, which allows to generalize the known approach to the non-binary case and practically implement computational algorithms for generating non-binary sequences of constant weight. The proposed technique of non-binary constant weight coding can be useful for improving post-quantum code-based cryptographic algorithms.

Keywords: constant weight coding, mixed base number systems, binomial count, code-based cryptographic algorithms.

1 Introduction

The computational efficiency of arithmetic operations directly depends on the technique of representing numbers on which operations are performed, i.e. on the applied number system [1–4]. The most common is the positional number system in which the same numerical sign (digit) in the number record has different meanings, depending on the position where it is located [3, 4]. Among these systems is the modern decimal number system, the occurrence of which is associated with a finger count, the binary number system used in modern computers, etc.

A mixed base number system is a generalization of the positional system, its base is an increasing number sequence and each represented number is expressed through a linear combination of base elements [3–6]. Mixed base number systems include the Fibonacci number system, factorial, binomial and other systems [6–8].

It should be noted that many applications are based on the binomial number system, including the so-called binomial codes that belong to the class of nonlinear binary redundancy codes used to increase the noise immunity of binary asymmetric data transmission channels [3, 6–8]. The main property of binomial codes, an equal Hamming weight (the number of nonzero elements) of all codewords, is used to effectively detect asymmetric distortions of transmitted sequences. In this case, a change of

Hamming weight of the sequence is an adequate criterion for detecting errors in asymmetric binary data channels.

Another, equally demanded application of constant weight codes consists in constructing provably robust cryptosystems [9–12], the security of which is justified by the reducability of the private key calculation task to the solution of the theoretical complexity problem of syndrome decoding [13, 14]. So, for example, in [15–17], provable secure encryption systems are considered. In works [18–20], code-based electronic signature schemes are considered, their parameters and basic properties are investigated. In articles [21, 22], pseudorandom number generators based on codes are studied, as well as promising stream encryption schemes [23–26]. Papers [27–29] are devoted to the study of zero-knowledge proof schemes. The design of fast and secure code-based hash functions is investigated in [25, 30–32].

Thus, code-based cryptography has many important applications. These crypto primitives are post-quantum security algorithms, i.e. they will be strong even under the conditions of possible quantum cryptanalysis [9–12].

Constant weight codes are used as one of the elements of code-based cryptosystems. In particular, in encryption systems, sequences with constant weights are used as a session key [16, 33, 34]. To generate a digital signature using the decoding algorithm, it is necessary to find a sequence with constant weight [18–20, 35]. When generating pseudo-random numbers, constant weight codes are used in the feedback circuit of the generator [21–23]. The input data for a code-based hash function is first converted to a constant weight sequence and then processed by a compression function [30, 32].

It should be noted that all listed applications only use binary constant weight codes. The discrete mathematics literature also describes only binary algorithms [1, 2, 4]. We offer non-binary constant weight coding technique. This will greatly expand the area of possible use of code-based cryptosystems. In particular, the practical implementation of non-binary (for example, over finite field $GF(2^m)$) codes can work faster and more efficiently, while providing a high level of strength of code-based cryptosystems. This determines the relevance of this article, a purpose of which is to develop a technique of non-binary constant weight coding based on a generalized binomial-positional representation.

2 Positional and Mixed Base Number Systems. Binary technique and Algorithm of Constant Weight Coding

The positional number system is based on a positional numbering, i.e. on a local value of digits, and is determined by a certain number $b > 1$ (a base of the number system) such that the b units in each category are combined into one unit of the next highest rank. The number system is also called b-positional system [1, 2, 13].

A number x in a b-ary positional number system is represented as a linear combination of powers of number b

$$x = \sum_{i=0}^{n-1} a_i b^i \ ,$$

where a_i are integers called numbers and they satisfy an inequality:

$$0 \le a_i < b \ ,$$

i is a discharge sequence number, starting from zero, n is a number of bits (length) of the position code.

Each degree b^i in such record is called a rank, the certain rank and the corresponding numbers is determined by the value of the indicator i. Usually, for a nonzero number x, the leading digit a_{n-1} in the b-ary representation is also required to be nonzero.

If there are no discrepancies (for example, when all the numbers are presented in the form of unique written characters), the number is recorded as a sequence of its b-ary digits, listed in ascending order of rank from left to right:

$$x = (a_0 \quad a_1 \quad ... \quad a_{n-1}) \ .$$

A mixed base number system is a generalization of the b-ary system and also often refers to positional number systems. The basis of the mixed base system is an increasing numbers sequence

$$b_0, b_1, b_2, ...$$

and each number is represented as a linear combination:

$$x = \sum_{i=0}^{n-1} a_i b_i \ ,$$

where some code restrictions are imposed on the coefficients a_i.

Numeral x in a mixed base number system is an enumeration of its numbers in decreasing order of the index i, starting with the first nonzero. If for some $b_i = b^i$, then the mixed base number system coincides with the b-ary positional number system.

The binomial number system is based on the representation of numbers through an increasing sequence of binomial coefficients

$$b_0 = \binom{u_1}{1}, b_1 = \binom{u_2}{2}, ..., b_{n-1} = \binom{u_n}{n},$$

$$b_i = \binom{u_{i+1}}{i+1} = \frac{u_{i+1}!}{(i+1)! \cdot (u_{i+1} - i - 1)!} \ ,$$

$$0 \le u_1 < u_2 < ... < u_n = \frac{n!}{w!(n-w)!},$$

where w is number of non-zero elements of binomial code.

A number x in the binomial system is represented as a linear combination:

$$x = \sum_{i=0}^{n-1} a_i b_i = \sum_{i=0}^{n-1} a_i \binom{u_{i+1}}{i+1},$$

where coefficients $a_i \in \{0,1\}$.

In the case when there are no discrepancies in the calculation of binomial coefficients , $b_i = \binom{u_{i+1}}{i+1}$, i.e. when a rule is established for the formation of a numbers set $0 \le u_1 < u_2 < ... < u_n$, the number x is written in increasing order of ranks a_i from left to right:

$$x = (a_0 \quad a_1 \quad ... \quad a_{n-1}).$$

The considered binomial number system is used to construct *binary constant weight codes* consisting of a set of binary sequences with a fixed number of nonzero elements in each sequence (a constant Hamming weight).

We introduce the following notation:

- n is a length of the constant weight code, i.e. the number of elements (bits) of code sequences (code words);
- $C = \{C_0, C_1, ..., C_{M-1}\}$ is a set of code words for the constant weight code, where

$$C_j = (C_{j_0} \quad C_{j_1} \quad ... \quad C_{j_{n-1}}) \in C,\ C_{j_i} \in \{0,1\},$$

$$j = 0,1,...,M-1,\ i = 0,1,...,n-1.$$

For all vectors C_j, $j = 0,1,...,M-1$ we have equal weight Hamming: $\forall j : w(C_j) = const = w$, where

$$w(C_{j_0} \quad C_{j_1} \quad ... \quad C_{j_{n-1}}) = \#(C_{j_0} \quad C_{j_1} \quad ... \quad C_{j_{n-1}})\Big|_{(C_{j_i} \ne 0)},$$

$\#(C_{j_0} \quad C_{j_1} \quad ... \quad C_{j_{n-1}})\Big|_{(C_{j_i} \ne 0)}$ is a number C_{j_i}, $i = 0,1,...,n-1$, where $C_{j_i} \ne 0$.

The power of the constant weight code (the number of elements in the set C) is determined by the number of binary vectors of length n and weight w:

$$|C| = M = \frac{n!}{w!(n-w)!}.$$

The well-known binomial (binary constant weight) coding technique [6, 7, 13] is based on the presentation of information data in the form of a numerical equivalent (denoted by a number A) with further decomposition into a linear combination of binomial coefficients. Such system of code restrictions on the length of sequences of constant weight n, codeword weights w and code cardinality M are satisfied:

$$\begin{cases} \forall j : w\left(C_j\right) = const = w; \\ 0 \le A < M; \\ 0 \le w \le n. \end{cases}$$

The number A is presented as binary sequence $C_A = \left(C_{A_0} \quad C_{A_1} \quad ... \quad C_{A_{n-1}}\right)$ of constant weight and $A = \sum_{i=0}^{n-1} C_{A_{n-i-1}} b_i$, where $b_i = \binom{n-i-1}{w-l}, l$ is a nonzero element number in C_A, $l = 0,1,...,w$.

Nonzero element is a $C_{A_{n-i-1}}$, for which $b_i \le \sum_{m=0}^{i-1} C_{A_{n-m-1}} b_m$.

Obviously, the sum on the right side of the expression is equal to the sum of only b_m those for which the corresponding elements of the vector C_A are not equal to zero ($C_{A_{n-m-1}} \ne 0$).

It should be noted that the considered technique does not imply the formation of non-binary sequences with constant weight (vectors C_A with $C_{j_i} \in \{0,1,...,q-1\}$, $q > 2$) and thus does not allow the implementation of non-binary constant weight coding.

The article proposes a new technique of non-binary constant weight coding based on a generalized binomial-positional representation, which allows us to generalize the above approach to the non-binary case and practically implement computational algorithms for generating non-binary sequences of constant weight.

3 Proposed Technique of Non-Binary Constant Weight Coding

To generalize the considered approach of generating sequences of constant weight to the non-binary case, a new form of a generalized binomial-positional representation of numbers is proposed. The proposed number system belongs to the class of mixed base systems and is based on the representation of numbers through an increasing sequence of binomial coefficients, each of which is encoded by positional numbering, i.e. the representation of digits with binomial coefficients is based on the local value of the digits.

Consider the number x in the proposed generalized binomial-positional number system: $x = \sum_{i=0}^{n-1} a_i b_i$.

Let's introduce the following notation and equalities:

$$a_i \in \{0,1,...,q-1\},\ b_i = \binom{u_{i+1}}{i+1} = \frac{u_{i+1}!}{(i+1)!\,(u_{i+1}-i-1)!},$$

$$0 \le u_1 < u_2 < ... < u_n = \frac{n!}{w!\,(n-w)!},$$

where w is a number of nonzero elements of the generalized binomial-positional code.

Then the number x is represented through an increasing sequence of binomial coefficients $b_0, b_1, ..., b_{n-1}$, and corresponding sequence $a_0, a_1, ..., a_{n-1}$.

Let's consider nonzero elements $a_i \neq 1,\ i = 0,1,...,n-1$, sequences $a_0, a_1, ..., a_{n-1}$ and renumber them, i.e. we denote them as elements of the sequence $a_0, a_1, ..., a_{w-1}$, $l = 0,1,..., w-1$ and $\forall l : a_l \in \{1,..., q-1\}$.

A sequence $a_0, a_1, ..., a_{w-1}$ and all its elements a_l (nonzero elements of a sequence $a_0, a_1, ..., a_{n-1}$ numbered according to the increasing digits order) are formed using a positional number system on the base $q-1$, i.e. $q-1$ units in each rank are combined into one unit of the next highest rank. A set of nonzero elements sets a_l, $l = 0,1,..., w-1$ defines the number x_P that is represented in the positional system as follows:

$$x_P = \sum_{l=0}^{w-1} (a_l - 1) h^l,$$

where $h = q-1$ is a base of used positional system, $1 \le a_l < q$.

The increasing sequence of binomial coefficients $b_0, b_1, ..., b_{n-1}$ sets a number x_B, which is represented in the binomial number system as $x_B = \sum_{i=0}^{n-1} a_{Bi} b_i$, where coefficients $a_{Bi} \in \{0,1\}$.

The number x in the proposed generalized binomial-positional number system satisfies the following equality:

$$x = x_B \cdot (q\text{-}1)^w + x_P,$$

which sets a main code restriction on the elements of the generalized binomial-positional code.

Thus, the number x in the proposed system of generalized binomial-positional counting is represented as a linear combination:

$$x = \sum_{i=0}^{n-1} a_i b_i = x_B \cdot (q\text{-}1)^w + x_P =$$
$$= (q\text{-}1)^w \sum_{i=0}^{n-1} a_{Bi} b_i + \sum_{l=0}^{w-1} (a_l - 1)(q-1)^l .$$

The proposed generalization of the binomial-positional way of representing numbers consists in the complex use of the positional number system and the binomial counting system: the first term on the right side of the equality, through the increasing sequence of binomial coefficients, determines the placement of nonzero elements of the generalized binomial-positional code, the second term defines the values of nonzero elements of the sequence in positional code.

The proposed technique of representing numbers is based on the technique of non-binary constant weight coding. For the abstract definition of a non-binary constant weight code, we introduce the following formal notation:

- n is a code length;
- $C = \{C_0, C_1, ..., C_{M-1}\}$ is a set of code words,

$$C_j = \left(C_{j_0} \quad C_{j_1} \quad ... \quad C_{j_{n-1}}\right) \in C, \; C_{j_i} \in \{0,1,...,q-1\},$$

$$j = 0,1,...,M-1, \;\; i = 0,1,...,n-1, \;\; \forall j : w\left(C_j\right) = const = w.$$

The cardinality of a non-binary constant weight code defined in this way is determined by the number of length n and weight w vectors with elements from the set $\{0,1,...,q-1\}$:

$$|C| = M = (q-1)^w \frac{n!}{w!(n-w)!}.$$

The proposed technique is based on the presentation of information data in the form of a numerical equivalent A with further decomposition into a linear combination of binomial coefficients, each of which is encoded by positional numbering so that a system of code restrictions on the length of n sequences of constant weight, the weight w of code words and code cardinality M is satisfied:

$$\begin{cases} \forall j : w\left(C_j\right) = const = w; \\ 0 \le A < M; \\ 0 \le w \le n; \\ 0 \le C_{j_i} < q. \end{cases}$$

The number A is presented as non-binary sequence of constant weight $C_A = \left(C_{A_0} \quad C_{A_1} \quad ... \quad C_{A_{n-1}}\right)$ and $A = A_B \cdot (q\text{-}1)^w + A_P$, where $A_B = \sum_{i=0}^{n-1} a_{Bi} b_i$, $b_i = \binom{n-i-1}{w-l}$, $A_P = \sum_{l=0}^{w-1} (a_l - 1) h^l$, $h = q-1$.

The process of generating a non-binary sequence of constant weight is presented in four stages.

1. Representation of number A in the form of numbers A_B and A_P:

$$A_B = \left\lfloor \frac{A}{(q\text{-}1)^w} \right\rfloor, \; A_P = (A) \, mod \left((q\text{-}1)^w\right),$$

where $\lfloor y \rfloor$ is the integer part of number y.

The uniqueness of the representation of number A in the form of numbers A_B and A_P is justified by the Chinese remainder theorem [13].

The number A_B lies within $0 \le A_B < \frac{M}{(q-1)^w}$ and can be represented in a binomial number system with code restrictions:

$$\begin{cases} \forall j : w(c_j) = const = w; \\ 0 \le A_B < \dfrac{n!}{w!(n-w)!}; \\ 0 \le w \le n. \end{cases}$$

The number A_P lies within $0 \le A_P < (q-1)^w$ and, accordingly, can be represented in the positional number system on the basis of $h = q-1$.

1. Representation of numbers in a binomial number system:

$$A_B = \sum_{i=0}^{n-1} a_{Bi} b_i, \; b_i = \binom{n-i-1}{w-l}.$$

2. Representation of a number A_P in a positional number system:

$$A_P = \sum_{l=0}^{w-1} (a_l - 1) h^l, \; h = q-1.$$

Generating of sequence $C_A = \left(C_{A_0} \quad C_{A_1} \quad ... \quad C_{A_{n-1}}\right) \in C$:

$$C_{A_i} = a_l a_{Bi}, \; i = 0,1,...,n-1, \; l = 0,1,...,w-1,$$

i.e.,

- if we have $a_{Bi} = 0$ for some $i = 0,1,...,n-1$ in the A_B representation, then we get $C_{A_i} = 0$;
- if $a_{Bi} = 1$, then we get $C_{A_i} = a_l$, i.e. the required element is equal to the corresponding nonzero element in the view A_P.

Example. Let's $n = 3$, $w = 1$, $q = 4$. The result of the proposed algorithm in the form of the obtained correspondence of all numbers A, their binary representations $I_A = \left(I_{A_0} \quad I_{A_1} \quad ... \quad I_{A_{k-1}}\right)$ in a positional binary code of length $k = \lceil \log_2 M \rceil = \lceil \log_2 9 \rceil = 4$, numbers A_B and A_P, corresponding vectors $\left(a_{B_0} \quad a_{B_1} \quad a_{B_2}\right)$ and $\left(a_0\right)$ and generated non-binary vectors $C_A = \left(C_{A_0} \quad C_{A_1} \quad C_{A_2}\right)$ of constant weight are shown in table 1.

Table 1. An example of the formation of non-binary sequences of constant weight

A	I_A	A_B	$\left(a_{B_0} \quad a_{B_1} \quad a_{B_2}\right)$	A_P	$\left(a_0\right)$	$\left(C_{A_0} \quad C_{A_1} \quad C_{A_2}\right)$
0	(0000)	0	(100)	0	(1)	(100)
1	(1000)	0	(100)	1	(2)	(200)
2	(0100)	0	(100)	2	(3)	(300)
3	(1100)	1	(010)	0	(1)	(010)
4	(0010)	1	(010)	1	(2)	(020)
5	(1010)	1	(010)	2	(3)	(030)
6	(0110)	2	(001)	0	(1)	(001)
7	(1110)	2	(001)	1	(2)	(002)
8	(0001)	2	(001)	2	(3)	(003)

The formed set of 9 non-binary vectors $C_A = \left(C_{A_0} \quad C_{A_1} \quad C_{A_2}\right)$ of constant weight forms a non-binary constant weight code $C = \{C_0, C_1, ..., C_8\}$.

Thus, the proposed number system based on the generalized binomial-positional representation of numbers allows complex use of both the local value of the digits of the code sequence and the values of binomial coefficients specified by the placement of nonzero elements of the sequence. Application of the developed number system allows us to build effective techniques and algorithms of non-binary constant weight coding for their use in various practical applications. For example, the proposed technique can be useful for improving post-quantum code-based cryptographic algorithms (ciphers, electronic digital signatures, key encapsulation schemes, pseudorandom number generators, etc.) [19, 21, 23, 31, 32, 36]. The use of constant weight codes is also one of the basic transformations for the functioning of code-based cryptosystems. In particular, constant weight codes are used in the McEliece [33] and Niederreiter [17] public key encryption schemes, as well as in electronic signature schemes and

code-based pseudorandom numbers generators. It is worth noting that at the moment, code-based cryptography is considered one of the most optimal ways of developing post-quantum cryptography. A good example of the use of constant weight codes in cryptosystems is a Niederreiter encryption process, which consists of several basic steps. First, user generates key and system parameters. Next, an information sequence e that needs to be encrypted is converted using constant-weight codes into a sequence of fixed length n and constant weight t. Then vector syndrome $s = e \cdot H_x^T$ must be calculated.

This vector is a ciphertext, i.e. an encrypted message that can be decrypted only by the user who has a secret key. Decryption consists in removing the action of masking matrices, after which the sequence is decoded using a fast algebraic technique. The found error vector is a sequence of constant weight e. To restore the information sequence, the conversion is used, the inverse of what was used. As you can see, each possible information sequence should be uniquely associated with the corresponding constant weight sequence, i.e. to build a code-based cryptosystem, it is necessary to implement an algebraic rule of this correspondence, implemented through an constant weight account system.

Thus, it is necessary to realize a one-to-one correspondence between all possible information sequences and various constant weight vectors. In the other words, for an arbitrary countable set (in advance of a given power), it is required to implement a new recording technique (number system) in the form of a set of constant weight vectors. At the moment, resistance versions of the constructions of code-based cryptosystems are based on the use of binary Goppa codes. In this simplest case, it is possible to use the well-known binomial count to convert information sequences into constant weight binary vectors. In the general case, code-based cryptosystems can be built for arbitrary base. And for this general case, we offer a generalized binomial-positional number system and a new technique of non-binary constant weight coding (binomial-positional counting). This will not only increase the strength of code-based cryptosystems, but also provide additional useful properties, such as the control of non-binary errors during transmission.

In addition, this study can be useful in other practical applications, for example, to improve channel coding techniques, to prevent interference in telecommunication networks, etc.

4 Conclusions

As a result of the research, a new number system based on the generalized binomial-positional representation of numbers is proposed. It is that the complex use of the binomial counting system (through the increasing binomial coefficients sequence defines a position of nonzero element) and the positional number system (the values of nonzero elements are specified through the local value of numbers).

For the first time, a technique of non-binary constant weight coding based on a generalized binomial-positional representation of numbers is proposed, which allows us to generalize the well-known approach to the non-binary case and practically im-

plement computational algorithms for generating non-binary sequences of constant weight.

The proposed non-binary constant weight coding technique is a generalization of the well-known binary case. In fact, a well-known binary code is used to represent a number in the binomial number system. Nonzero elements of the resulting binomial sequence are additionally encoded with a positional code. Thus, the complexity of the implementation of the proposed technique is defined as the total complexity of the known techniques of binomial and positional coding.

The developed technique can be used in various practical applications, for example, in code-based cryptosystems: ciphers, electronic digital signatures, key encapsulation schemes, pseudorandom number generators, etc. These cryptosystems are expected to be safe even in the conditions of the possible application of quantum cryptographic analysis techniques, i.e. focused on the post-quantum period.

References

1. Anderson, J.A.: Discrete Mathematics With Combinatorics. Prentice Hall, Upper Saddle River, N.J (2003)
2. Knuth, D.E.: The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms. Addison-Wesley Longman Publishing Co., Inc., USA (1997)
3. Borisenko, A.A., Kalashnikov, V.V., Protasova, T.A., Kalashnykova, N.I.: A New Approach to the Classification of Positional Numeral Systems. In: IDT/IIMSS/STET (2014)
4. Wolfram Demonstrations Project brings ideas to life with over 11k interactive #WolframNotebooks for education, research, recreation & more. #WolframDemo #WolfLang, http://demonstrations.wolfram.com/NumberSystemsUsingAComplexBase/
5. Stakhov, A.: Numeral Systems with Irrational Bases for Mission-Critical Applications. World Scientific Publishing Co Pte Ltd, New Jersey (2017)
6. Borisenko, A., Kalashnykova, N., Kalashnikov, V., Gutenko, D.: Binomial Numeral Systems: Description and Applications to Numeration Problems(<Special Issue>Variational Inequality and Combinatorial Problems). International Journal of Biomedical Soft Computing and Human Sciences: the official journal of the Biomedical Fuzzy Systems Association. 17, 11–17 (2012). https://doi.org/10.24466/ijbschs.17.2_11
7. Borisenko, A., Kalashnikov, V., Kalashnykova, N.: BINOMIAL CALCULUS: ADVANTAGES AND PROSPECTS. 8 (2008)
8. Borysenko, O.A., Kalashnikov, V.V., Kalashnykova, N.I., Matsenko, S.M.: The Fibonacci Numeral System for Computer Vision. In: Favorskaya, M.N. and Jain, L.C. (eds.) Computer Vision in Control Systems-3: Aerial and Satellite Image Processing. pp. 321–343. Springer International Publishing, Cham (2018)
9. Overbeck, R., Sendrier, N.: Code-based cryptography. In: Bernstein, D.J., Buchmann, J., and Dahmen, E. (eds.) Post-Quantum Cryptography. pp. 95–145. Springer, Berlin, Heidelberg (2009)
10. Bernstein, D.J.: Introduction to post-quantum cryptography. In: Bernstein, D.J., Buchmann, J., and Dahmen, E. (eds.) Post-Quantum Cryptography. pp. 1–14. Springer, Berlin, Heidelberg (2009)

11. Ding, J., Tillich, J.-P. eds: Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings. Springer International Publishing, Cham (2020)

12. Ding, J., Steinwandt, R. eds: Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers. Springer International Publishing, Cham (2019)

13. The Theory of Error-Correcting Codes. Elsevier (1977)

14. Blahut, R.E.: Theory and Practice of Error Control Codes. Addison-Wesley, Reading, MA (1983)

15. Sendrier, N.: Niederreiter Encryption Scheme. In: van Tilborg, H.C.A. and Jajodia, S. (eds.) Encyclopedia of Cryptography and Security. pp. 842–843. Springer US, Boston, MA (2011)

16. Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications. 2, 439–444 (1992). https://doi.org/10.1515/dma.1992.2.4.439

17. NIEDERREITER, H.: Knapsack-type cryptosystems and algebraic coding theory. Prob. Contr. Inform. Theory. 15, 157–166 (1986)

18. Courtois, N.T., Finiasz, M., Sendrier, N.: How to Achieve a McEliece-Based Digital Signature Scheme. In: Boyd, C. (ed.) Advances in Cryptology — ASIACRYPT 2001. pp. 157–174. Springer, Berlin, Heidelberg (2001)

19. Finiasz, M.: Parallel-CFS. In: Biryukov, A., Gong, G., and Stinson, D.R. (eds.) Selected Areas in Cryptography. pp. 159–170. Springer, Berlin, Heidelberg (2011)

20. Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskyi, D., Smirnov, O., Kuznetsova, T.: Code-Based Schemes for Post-Quantum Digital Signatures. In: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). pp. 707–712 (2019)

21. Fischer, J.-B., Stern, J.: An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding. In: Maurer, U. (ed.) Advances in Cryptology — EUROCRYPT '96. pp. 245–255. Springer, Berlin, Heidelberg (1996)

22. Kuznetsov, A., Kiian, A., Smirnov, O., Cherep, A., Kanabekova, M., Chepurko, I.: Testing of Code-Based Pseudorandom Number Generators for Post-Quantum Application. In: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 172–177 (2020)

23. Gaborit, P., Lauradoux, C., Sendrier, N.: SYND: a Fast Code-Based Stream Cipher with a Security Reduction. In: 2007 IEEE International Symposium on Information Theory. pp. 186–190 (2007)

24. Meziani, M., Hoffmann, G., Cayrel, P.-L.: Improving the Performance of the SYND Stream Cipher. In: Mitrokotsa, A. and Vaudenay, S. (eds.) Progress in Cryptology - AFRICACRYPT 2012. pp. 99–116. Springer, Berlin, Heidelberg (2012)

25. Implementation of code-based hash-functions and stream-ciphers - Pierre-Louis Cayrel, http://www.cayrel.net/?Implementation-of-code-based-hash

26. Meziani, M., Cayrel, P.-L., El Yousfi Alaoui, S.M.: 2SC: An Efficient Code-Based Stream Cipher. In: Kim, T., Adeli, H., Robles, R.J., and Balitanas, M. (eds.) Information Security and Assurance. pp. 111–122. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)

27. Aguilar, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification scheme with reduced communication. In: 2011 IEEE Information Theory Workshop. pp. 648–652 (2011)

28. Aguilar, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification scheme with reduced communication. arXiv:1111.1644 [cs]. (2011)

29. Brunetta, C., Liang, B., Mitrokotsa, A.: Code-Based Zero Knowledge PRF Arguments. In: Lin, Z., Papamanthou, C., and Polychronakis, M. (eds.) Information Security. pp. 171–189. Springer International Publishing, Cham (2019)

30. Finiasz, M., Gaborit, P., Sendrier, N.: Improved Fast Syndrome Based Cryptographic Hash Functions. Presented at the (2005)

31. Bernstein, D.J., Lange, T., Peters, C., Schwabe, P.: Really Fast Syndrome-Based Hashing. In: Nitaj, A. and Pointcheval, D. (eds.) Progress in Cryptology – AFRICACRYPT 2011. pp. 134–152. Springer, Berlin, Heidelberg (2011)

32. Augot, D., Finiasz, M., Sendrier, N.: A Family of Fast Syndrome Based Cryptographic Hash Functions. In: Dawson, E. and Vaudenay, S. (eds.) Progress in Cryptology – Mycrypt 2005. pp. 64–83. Springer, Berlin, Heidelberg (2005)

33. McEliece, R.J.: A Public-Key Cryptosystem Based On Algebraic Coding Theory. Deep Space Network Progress Report. 44, 114–116 (1978)

34. Kuznetsov, A., Svatovskij, I., Kiyan, N., Pushkar'ov, A.: Code-based public-key cryptosystems for the post-quantum period. In: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). pp. 125–130 (2017)

35. Kuznetsov, A., Kiian, A., Babenko, V., Perevozova, I., Chepurko, I., Smirnov, O.: New Approach to the Implementation of Post-Quantum Digital Signature Scheme. In: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 166–171 (2020)

36. Meziani, M., Dagdelen, Ö., Cayrel, P.-L., El Yousfi Alaoui, S.M.: S-FSB: An Improved Variant of the FSB Hash Family. In: Kim, T., Adeli, H., Robles, R.J., and Balitanas, M. (eds.) Information Security and Assurance. pp. 132–145. Springer, Berlin, Heidelberg (2011)