# Macedonian - Chinese Scientific and Technological Cooperation

New Project Proposal for 2016-2017



| **Title of project proposal:**<br><br>Application of Quasigroups in Cryptography and Data Communications | **Project number** |
|---|---|
| **Macedonian organization:**<br>University "Goce Delčev", Republic of Macedonia | |
| **Chinese organization:**<br>Ningbo University, Peoples Republic of China | |
| **Project period:** 01.01.2016 – 31.12.2017 | |
| **Expected period of stay in China for the Macedonian Researchers:**<br>2016: 2 persons, x 7 days, from 13.06.2016 to 19.06.2016<br>2017: 2 persons, x 7 days, from 12.06.2017 to 18.06.2017 | |
| **Expected period of stay in Macedonia for the Chinese Researchers:**<br>2016: 1 person, x 14 days, from 16.08.2016 to 29.08.2016<br>2017: 1 person, x 14 days, from 16.08.2017 to 29.08.2017 | |
| **Address of Macedonian organization:**<br>"Krste Misirkov" 10-A<br>P.O. Box 201<br>2000, Štip<br>Republic of Macedonia<br><br>**Name and signature of contact person:**<br>**Name:** Aleksandra Mileva **Title:** Associate Professor<br>**Tel.:** ++389 78 222 460 **Fax:** ++389 32 390 700<br>**E-mail:** aleksandra.mileva@ugd.edu.mk<br>**Signature:** | |
| **Address of Chinese organization:**<br>Fenghua Road #818<br>Ningbo 315211<br>Peoples Republic of China<br><br>**Name and signature of contact person:**<br>**Name:** Yunqing Xu **Title:** Professor<br>**Tel.:** +86-13989318968 **Fax:** +86-574-87600744<br>**E-mail:** xuyunqing@nbu.edu.cn<br>**Signature:** | |

# Macedonian - Chinese Scientific and Technological Cooperation

New Project Proposal for 2016-2017



**Project description:**

Cryptography and coding theory are the pillars of the secure data communications, and quasigroups are very suitable for application in these two fields, because of their structure, their features, their big number and because they lead to particular simple and yet efficient primitives. This can be supported by several existing cryptographic primitives based on quasigroups, like: one of the few left unbroken eSTREAM finalists – the stream cipher Edon80; Pi-Cipher – an authenticated encryption second round candidate in the ongoing CAESAR competition for authenticated ciphers; two first round candidates to the NIST SHA-3 competition - hash functions Edon-$\mathcal{R}$ and NaSHA; the trapdoor one-way functions and public key cryptosystems based on multivariate quadratic quasigroups (MQQ); a digital signature variant of the original MQQ public key algorithm - MQQ-SIG, which is 300-3500 times faster than RSA or ECDSA in software, and 10,000 times in hardware; an identity based scheme LMQQ-ID, etc. Additionally, quasigroups have successfully been implemented in error correcting codes as well, for example, Random Codes Based on Quasigroups (RCBQ). In this project we plan several activities:

***1. Design of new cryptosystems or their building blocks based on quasigroups***

*1.1 Classification of quasigroups*

The selection of quasigroups in a cryptosystem is very important. The number of quasigroups of a given order is huge, e.g., there are more than $10^{21}$ quasigroups of order 8. But only a part of the quasigroups are suitable for encryptions and it is not easy to select suitable ones. The most important indexes to choose a quasigroup are the period factor and randomness. Two classifications are planed:

(1) Classification based on period factor: The period factor of a quasigroup is a random variable which increase the period of the keystream in each transformation. We use the theory of permutation groups, matrix and probability to classify the quasigroups of different orders. Due to the huge number of quasigroups, we will use a supercomputer in the searches and calculations.

(2) Classification based on randomness: To classify the quasigroups with larger period factors according to the randomness of the result keystream. The main random indexes are frequency, block frequency, cumulative Sums, discrete Fourier transform and runs, etc. The main tools are the probability theory and the NIST-STS software.

*1.2 Obtaining optimal 8–bit S-boxes by small quasigroups*

S-boxes have a fundamental role for the security of modern block ciphers because they are usually the main non-linear part in the block ciphers. Optimal S-boxes can make the cipher resistant against various kinds of attacks. There is a method for generating optimal 4x4 S-boxes by quasigroups of order 4, by which a more optimized hardware implementation of the given S-box can be obtained. We will try to obtain an optimal 8x8 S-boxes from small quasigroups of order 4 or 8, with similar methods, with the final goal of obtaining their more optimized hardware implementation. We will investigate differential and linear characteristics of produced S-boxes. The experiments will include several quasigroup transformations, like e-, d-, OT and quasigroup reverse string transformations, and their combinations. For this activity we plan to use a supercomputer and/or parallel programming.

*1.3 Design of stream cipher and block cipher based on quasigroups*

(1) Design a stream cipher based on a 3-quasigroup of order four to improve the Edon80, a binary additive synchronous stream cipher submitted to the last phase of the eSTREAM project, to resist the key recovery attack, the most advanced attack on Edon80.

(2) Design lightweight stream or block ciphers with low power consumption suitable for low powered systems such as smart phones, tablets and sensor networks with low computational power and low memory capacity. As nonlinear part of the lightweight block cipher will be used optimal 4x4 S-box obtained by quasigroup of order 4, and for linear part will be used recursive perfect diffusion layer obtained by r-ary recursively r-differentiable quasigroups.

***2. Cryptanalysis of some cryptosystems based on quasigroups***

Linear and differential cryptanalysis, since their emergence in cryptology, have proven to be the most viable tool for estimating the security of symmetric cryptographic primitives. First introduced by Biham and Shamir, differential cryptanalysis investigates how a difference in the input propagates through the cipher and influences the output. Serious deviations from uniformly random differentials implicate weaknesses in the cipher that can be used to devise distinguishers or key recovery attacks. For this reason, differential cryptanalysis has become a primer tool for gaining confidence in ciphers that are to be used in practice. While there is a myriad of research done on the topic of differential cryptanalysis for Substitution-Permutation networks, very little is known about the differential properties of ARX based designs. ARX (addition, rotation and XOR) ciphers have become increasingly popular in the last few

years, mainly because of their performance advantages and easy implementation not prone to errors. However, the classical analysis suitable for SP networks, does not apply here. Two groups of researchers have pioneered automated investigation of the differential properties for such ciphers, but so far, the tools are either dedicated or restricted to a small set of operations. Recently, researchers from FCSE, Macedonia and NTNU, Norway have proposed a new authenticated cipher, the Pi-Cipher, that has entered the second round of the current CAESAR competition. Pi-Cipher has an ARX based design, arising from particular quasigroup of order 2^64. From quasigroup theory perspective, the design was carefully made to reduce highly probable differentials. However, only a detailed cryptanalysis can prove the security of the cipher, and increase the confidence in it. Due to its structure the known tools can not be used for analysis. Therefore, our goals can be summarized as follows:

- Modify and improve the existing ARX based tools, so that they can be used for analysis of Pi-Cipher.
- Use the developed tools to prove the resistance of Pi-Cipher to differential cryptanalysis.
- Use the developed tool to analyze the security of the Edon-R hash function that shares a similar structure as Pi-Cipher.
- Create generic analyzers that can be applied to other ciphers with ARX design.
- Use the developed tool in the design of subsequent proposals based on quasigroups, in particular for the planned design from Section 1.3.

***3. Codes based on quasigroups***

*3.1 Designs of error correcting codes based on combinatorial structures and quasigroups*

Optical orthogonal codes (OOCs) have important applications in a fiber-optic code-division multiple-access (CDMA) channel. Recent work has been done on using OOCs for multimedia transmission in fiber-optic local-area networks (LANs) and in multi-rate fiber-optic CDMA systems. Nonlinear cyclic constant-weight codes (CWCs) is another kind of binary cyclic constant-weight code. These two kinds of codes are closely related to combinatorial designs such as group divisible designs and quasigroups. We will design OOCs and CWCs with good auto-correlation property and good correlation properties.

*3.2 Improvement and evaluation of Random Codes Based on Quasigroups (RCBQ)*

Crypt-codes are error-correcting codes resistant to an intruder attack. In a few papers, these codes are obtained by applying known ciphers on the codewords, before sending them through an insecure channel. In this case, two algorithms are used, one for error-correcting codes and another for obtaining information security. In order to obtain more efficient design, some authors give one algorithm where a block cipher and an error-correcting code are combined. One type of such codes are Random Codes Based on Quasigroups (RCBQ).

RCBQ were proposed by D. Gligoroski, S.Markovski and Lj.Kocarev. These error-correcting codes are defined by using a cryptographic algorithm during the encoding/decoding process. Therefore, they allow not only correction of certain amount of errors in the input data, but they also provide an information security, all built in one algorithm.

RCBQ codes are designed using the algorithms for encryption/decryption of Totally Asynchronous Stream Ciphers (TASC) by quasigroup string transformations. These cryptographic algorithms use the alphabet Q and a quasigroup operation * on Q together with its parastrophe \.

Our goals can be summarized as follows:

- We will investigate the performances of the crypt-codes based on quasigroup transformations, known as Random Codes Based on Quasigroups (RCBQ), for transmission through Gaussian channel. We will consider codes with different parameters and analyze the influence of the parameters on the code performances.
- We will investigate the performances of these codes for coding/decoding images and audio files transmitted through Gaussian channel. Also, we will try to define a filter for correcting the images and audio files decoded with RCBQ.
- In order to improve the performances of RCBQ, we will propose some new modifications in the decoding algorithms.

***4. Algebraic curves over finite fields with their cryptographic applications***

We will utilize several tools, such as P-adic analysis, Newton polyhedron and exponential sums, to investigate the rational points on algebraic curves over finite fields and to estimate the sets of points (explicit formulae will be given in some cases); for the nonsingular algebraic curve, we will also study the Jacobian group formed by its divisor classes and compute its order and express the elements in it and implement fast arithmetic. Finally, we will explore the applications of the theoretical results mentioned above in cryptography.

# Macedonian - Chinese Scientific and Technological Cooperation

New Project Proposal for 2016-2017

| | | MACEDONIAN PRINCIPAL RESEARCHER | CHINESE PRINCIPAL RESEARCHER |
|---|---|---|---|
| FIRST AND LAST NAME | | Aleksandra Mileva | Yunqing Xu |
| DEGREE | | PhD | PhD |
| POSITION | | Associate Professor | Full Professor |
| INSTITUTIONs | NAME | Faculty of Computer Science,<br>University "Goce Delčev" | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Krste Misirkov" 10-A<br>P.O. Box 201<br>2000, Štip<br>Republic of Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |
| | TELEPHONE | ++38978222460 | +86-13989318968 |
| | FAX | ++38932390700 | +86-574-87600744 |
| | E-MAIL | aleksandra.mileva@ugd.edu.mk | xuyunqing@nbu.edu.cn |
| | | **OTHER MACEDONIAN PARTICIPANT** | **OTHER CHINESE PARTCIPANT** |
| LAST NAME | | Dimitrova | Cao |
| FIRST NAME | | Vesna | Wei |
| DEGREE | | PhD | PhD |
| POSITION | | Assistant Professor | Associate Professor |
| INSTITUTI | NAME | Faculty of Computer Science and Engineering, "Ss Cyril and Methodius" University | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Rugjer Boshkovikj" 16,<br>P.O. Box 393,<br>1000 Skopje, Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |

| | | | |
|---|---|---|---|
| O N 's | TELEPHONE | ++38978853582 | +86-13858375042 |
| | FAX | ++38923088222 | +86-574-87600744 |
| | E-MAIL | vesna.dimitrova@finki.ukim.mk | caowei@nbu.edu.cn |

| | | **OTHER MACEDONIAN PARTICIPANT** | **OTHER CHINESE PARTCIPANT** |
|---|---|---|---|
| LAST NAME | | Bakeva | Wang |
| FIRST NAME | | Verica | Xiaomiao |
| DEGREE | | PhD | PhD |
| POSITION | | Full Professor | Lecturer |
| I N S T I T U T I O N 's | NAME | Faculty of Computer Science and Engineering, "Ss Cyril and Methodius" University | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Rugjer Boshkovikj" 16, P.O. Box 393, 1000 Skopje, Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |
| | TELEPHONE | ++38970616517 | +86-15968033104 |
| | FAX | ++38923088222 | +86-574-87600744 |
| | E-MAIL | verica.bakeva@finki.ukim.mk | wangxiaomiao@nbu.edu.cn |

| | | **OTHER MACEDONIAN PARTICIPANT** | **OTHER CHINESE PARTCIPANT** |
|---|---|---|---|
| LAST NAME | | Samardziska | Lan |
| FIRST NAME | | Simona | Liantao |
| DEGREE | | PhD | PhD |
| POSITION | | Junior Assistant | Junior Assistant |
| I N S T I T U T I O N 's | NAME | Faculty of Computer Science and Engineering, "Ss Cyril and Methodius" University | Faculty of Science, Beijing Jiaotong University |
| | ADDRESS | "Rugjer Boshkovikj" 16, P.O. Box 393, 1000 Skopje, Macedonia | No.3 Shangyuancun<br>Haidian District<br>Beijing 100044<br>China |
| | TELEPHONE | ++38970275735 | +86-18811795142 |
| | FAX | ++38923088222 | |
| | E-MAIL | simona.samardziska@finki.ukim.mk | llt05404@163.com |

| | | OTHER MACEDONIAN PARTICIPANT | OTHER CHINESE PARTCIPANT |
|---|---|---|---|
| LAST NAME | | Popovska - Mitrovikj | Fang |
| FIRST NAME | | Aleksandra | Zenghui |
| DEGREE | | PhD | MSc |
| POSITION | | Assistant Professor | Assistant |
| INSTITUTION's | NAME | Faculty of Computer Science and Engineering, "Ss Cyril and Methodius" University | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Rugjer Boshkovikj" 16, P.O. Box 393, 1000 Skopje, Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |
| | TELEPHONE | ++38971277039 | +86-17855847671 |
| | FAX | ++38923088222 | +86-574-87600744 |
| | E-MAIL | aleksandra.popovska.mitrovikj@finki.uki | 1051625606@qq.com |

| | | OTHER MACEDONIAN PARTICIPANT | OTHER CHINESE PARTCIPANT |
|---|---|---|---|
| LAST NAME | | Mihajloska | Guo |
| FIRST NAME | | Hristina | Jinli |
| DEGREE | | MSc | MSc |
| POSITION | | Assistant | Assistant |
| INSTITUTION's | NAME | Faculty of Computer Science and Engineering, "Ss Cyril and Methodius" University | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Rugjer Boshkovikj" 16, P.O. Box 393, 1000 Skopje, Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |
| | TELEPHONE | ++38975633242 | +86-17855847621 |
| | FAX | ++38923088222 | +86-574-87600744 |
| | E-MAIL | hristina.mihajloska@finki.ukim.mk | 1214541797@qq.com |

| | OTHER MACEDONIAN PARTICIPANT | OTHER CHINESE PARTCIPANT |
|---|---|---|
| LAST NAME | Bikov | Xie |
| FIRST NAME | Dušan | Shaohua |
| DEGREE | MSc | MSc |

| | | | |
|---|---|---|---|
| POSITION | | | Assistant |
| INSTITUTION's | NAME | Faculty of Computer Science,<br>University “Goce Delčev” | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Krste Misirkov" 10-A<br>P.O. Box 201<br>2000, Štip<br>Republic of Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |
| | TELEPHONE | ++38978382230 | +86-17855847673 |
| | FAX | ++38932390700 | +86-574-87600744 |
| | E-MAIL | dusan.bikov@ugd.edu.mk | 1209490052@qq.com |

| | | **OTHER MACEDONIAN PARTICIPANT** | **OTHER CHINESE PARTCIPANT** |
|---|---|---|---|
| LAST NAME | | Markovski | Zhao |
| FIRST NAME | | Smile | Yaohui |
| DEGREE | | PhD | MSc |
| POSITION | | Professor in retirement | Assistant |
| INSTITUTION's | NAME | Faculty of Computer Science and Engineering, “Ss Cyril and Methodius” University | Faculty of Science,<br>Ningbo University |
| | ADDRESS | "Rugjer Boshkovikj" 16, P.O. Box 393,<br>1000 Skopje, Macedonia | Fenghua Road #818<br>Ningbo 315211<br>China |
| | TELEPHONE | ++38970589191 | +86-18892614946 |
| | FAX | ++38923088222 | +86-574-87600744 |
| | E-MAIL | smile.markovski@finki.ukim.mk | 1293420130@qq.com |