# Session : Cryptography and Codes

# Circulant matrices and logistic maps to share keys

S. ADOUI
s.adoui@univ-batna2.dz

Laboratoire d application des Mathématiques et l électroniques : LAMIE,
University of Mostefa Ben Boulaïd, Batna 2 -Algeria

**Abstract**

With the development of the usage of Internet, and the revolution of the information and communication technology, when we exchange our data we are obliged to protect them and the way to do this is cryography systems whoose assure security of their information system and to master the control access to resources and the authentication of the users and the transmitted documents.

In this abstract we present a new system using the set of circulantS matrices to share a key ; this key will be used to encrypt and decrypt a text or an image using Diffie Hellman protocol.
The circular matrices give us a good property ; it is the commutativity of multiplication(A.B = B.A) which allows us to exchange and share a secret key in complete security.
We suppose that to encrypt/decrypt a text message or image we have to convert them to a matrix then we will encrypt/decrypt them with a matrix-key.
Let's assume ; two person wants to share a key(square matrix)between them secretly :
(a) The two person agreeing on a common square random matrix of order "n" rated "G".
(b) Now ; each of them selects two secrets circulants matrices with the same order of G "$A_1$" and "$A_2$" (successive "$B_1$" and "$B_2$" with the same order of G)
(c) Each of them calculates and sends to the other the encrypted "$C_1$" with :

$$C_1 = A_1.G.A_2 \qquad (successive C_2 = B_1.G.B_2)$$

(d) Now ;each of them reveived "$C_1$" (successive $C_2$)and calculate :

$$K_1 = A_1.C_2.A_2 \qquad (successive K_2 = B_1.C_1.B_2)$$

(e) Hence ; their agreed on a secret matrix is : K= $K_1 = K_2$ ; so they were able to share the same key.
This secret key K will be used to encrypt/decrypt a text message or image.
If we supose that M is the converted image to a matrix ; the first person encrypt M to ME using the formula ME=K.M.$K^1$ and the second person received ME and decryt them to MD using the formula MD=$K^1$.ME.K whoose MD=M initial converted image.
And to strengthen the security of our system we have worked to manage the public matrix G and make it secret to share between the two persons using the chaotic logistics sequences using a protocol of exchange known in the field quantum which is protocol BB84.

**Références**

[1] M. Kumar, S. Kumar, R. Budhiraja, M.K. Das, *A cryptographic model based on logistic map and a 3-d matrix*, Journal of Information Security and Applications , Supplement C(2017) : 47-58.

[2] A. Kanso and N. Smaoui , *Logistic chaotic maps for binary numbers generations*, Chaos, Solitons and Fractals , 40(5)(2009) :p 2557 ? 2568.

[3] Guihua Zeng, *Quantum Private Communication*, Springer Publishing Company, Incorporated, 1st edition, 2010.

# A two-stages pipelining implementation of the SHA-3 hash function for single and multi-message hashing

F. Assad[1], F. Elotmani[1] , M. Fettach[1], A. Tragha[2]

[1]Laboratoire Traitement de l'information, Université Hassan II, Casablanca
[2]Laboratoire Traitement et modélisation de l'information, Université Hassan II, Casablanca

## Résumé /Abstract :

Security has become a very demanding parameter in today's world of speed communication, one of the methods to ensure information integrity is the use of hash function which generates a stream of bytes (hash) which must be unique. The Keccak hash function is one of more than fifty candidates accepted by the NIST (national institute of standard and technology) for the SHA-3 hash function competition. It is based on a sponge construction and has thus a quite different structure from hash functions that belong to the MD4 family, such as SHA1 and SHA-2. With this structure, Keccak is more secure and efficient than the existing standards [1].

In this work we propose a new design for the Keccak hash function, the novelty of this architecture lies in the fact that it can efficiently serve multiple multi-block messages. This technique is very effectual in the case where the algorithm is supposed to process several messages at the same time, as in the case of a network card servicing multiple secure streams of packets that require hashing. The easiest way to implement pipelining in hash functions is to first unroll, and then introduce pipeline registers between rounds. The simplest case is the architecture that is two times unrolled, and has two pipeline stages. Unlike several works, our design processes data completely including padding and preprocessing parts. Moreover, it is not based on any FPGA resources such as Digital signal processors (DSPs). Additionally we have also taken into account all different output lengths (128, 256, 384 and 512) to build a complete design of Keccak hash algorithm.

The two-stage pipeline design allows to output a first block after exactly 24 clock cycles and can process a new block every 12 clock cycles. This allowed processing multiple messages for hashing simultaneously. This core implements the five sub-rounds Theta, Rho, Pi, Chi and Iota [2]. The output generated by the core will be stored in a register then the output register is fed as input to the following stage multiplexer. At the last round, the output is fed to the truncate unit in order to produce the final hash value.

The proposed design is coded in VHDL and implemented on Virtex 5 FPGA. The FPGA implementation results show that the proposed architecture achieves good performance in terms of maximum frequency, consumed area, throughput and efficiency, it utilizes 1613 slices and thus it has a maximum frequency of 362.450 MHz on virtex 5.

## Références :

[1] G. Bertoni, J. Daemen, M. Peeters, G.V. Assch e, "Keccak sponge function family main document.".

[2] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

# On recurrent sets of operators

M.Amouch[1] and O.Benchiheb[1]

[1]Laboratory LMF, University Chouaib Doukkali. Department of Mathematics, Faculty of science Eljadida, Morocco

**Résumé/Abstract**

An operator $T$ acting on a Banach space $X$ is said to be recurrent if for each $U$ ; a nonempty open subset of $X$, there exists $n \in \mathbb{N}$ such that $T^n(U) \cap U \neq \emptyset$. In the present work, we generalize this notion from a single operator to a set $\Gamma$ of operators. As application, we study the recurrence of $C$-regularized group of operators.

**Références**

[1] M. Amouch and O. Benchiheb, *On cyclic sets of operators*, Rend. Circ. Mat. Palermo, 2. Ser (2018), https ://doi.org/10.1007/s12215-018-0368-4.

[2] M. Amouch and O. Benchiheb, *On linear dynamics of sets of operators*, Turk. J. Math, 43(1)(2019) : 402–411.

[3] G. Costakis, A. Manoussos and I. Parissis, *Recurrent linear operators*, Complex. Anal. Oper. Th, 8(2014) : 1601–1643.

# Quasi-cyclic codes

*Youssef BENSALIH*[1], *Mohammed SABIRI*[2]

[1]Département de mathématique et informatique, Faculté des sciences et techniques, Errachidia.
[2] Département de mathématique et informatique, Faculté des sciences et techniques , Errachidia.

## Abstract :

Quasi cyclic codes over finite commutative rings areviewed as cyclic codes over a noncommutative rings of matrices over finite ring. In this talk we study construction of some quasi- cyclic codes and their properties.

.

## Références :

[1] Pierre-Louis Cayrel,Cristophe Chabot, Quasi-cyclic codes as codes over rings of matrices, Finite _eld and their applications,16 (2010), 100-115.
[2] C.Chabot Factorisation in $M_l(F_q)[X]$: contruction of quasi-cyclic codes.in Workshop on coding and cryptography, WCC 2011 .

# Cryptographie basée sur les courbes éléptiques

Hayat BENSELLA [1]

Laboratoire algèbre et théorie des nombres ,
Université de scieces et de la technologie
Houari Boumedien , Algérie

## Résumé /Abstract :

Méthode de construction d'une courbe hypereleptiques adapté à la cryptographie et aux appareils cryptographiques utilisant une telle méthode .

## Références :

[1] Henri Cohen. A Course in Computational Algebraic Number Theory. Springer,1993..
[2] René Schoof. Elliptic curves over finite fields and the computation of square roots. Mathematics of Computation, Vol. 44, N°382, avril 1985..

# the discovery of the sequence of pseudo remains to generate prime numbers facilitates the cracking of RSA-encryption

Ahmed. Hafdi ,

Université Mohammed V - Agdal, Rabat

## Résumé /Abstract :

La découverte des nombres premiers a créé une révolution dans le monde des mathématiques. Depuis l'ère d'Euclide, celui à l'origine de cette grande découverte, tous les mathématiciens se débattent afin de trouver une formule qui permettrait de manipuler ces nombres et donc de prédire leur comportement.
La complexité des nombres premiers est ce qui fait leur particularité. En effet, grâce à cet atout indéniable, l'algorithme de cryptage *RSA* est considéré comme le plus sécurisé en vue de son utilisation de grands nombres premiers car la génération de ces derniers requiert une grande complexité au niveau de la mémoire et du temps.
Le fruit de ma recherche tourne autour des nombres premiers ainsi que le RSA - algorithme et plus précisément de son craquage grâce à la découverte des pseudos restes qui permettent de générer des nombres premiers de grande valeur en un temps raccourci. Effectivement, le travail accompli sur les nombres premiers permet de générer une suite de pseudos restes qui réduisent la complexité des nombres premiers qui sont considérés comme la base de la cryptographie, ce qui mène à la génération rapide et facile de grands nombres premiers. Cette découverte facilite le craquage non seulement de l'algorithme RSA, mais également de tout algorithme de cryptage basé sur les nombres premiers.

## Références :

[1] Gardiner, Anthony (1997). The Mathematical Olympiad Handbook: An Introduction to Problem Solving Based on the First 32 British Mathematical Olympiads 1965–1996. Oxford University Press. p. 26. ISBN 978-0-19-850105-3.
[2] The Original RSA Patent as filed with the U.S. Patent Office by Rivest; Ronald L. (Belmont, MA), Shamir; Adi (Cambridge, MA), Adleman; Leonard M. (Arlington, MA), December 14, 1977, U.S. Patent 4,405,829 .
[3] PKCS #1: RSA Cryptography Standard (RSA Laboratories website) The PKCS #1 standard "provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; sign ature schemes with appendix; ASN.1 syntax for representing keys and for identifying the schemes"

# On the Classification of Elliptic curves over particular rings

M. Sahmoudi[1], A. Chillali[2]

[1]Electric Engineering and computing and Mathematical sciences Laboratory , Ibn Tofail university, Kenitra
[2]Engineering Sciences Laboratory, Sidi Mohamed Ben Abdellah university , Taza

**Résumé/Abstract**

Let $L/\mathbb{Q}$ be a Sextic extension, namely $L = \mathbb{Q}(\sqrt{d}, \beta)$ which is a rational quadratic over a pure cubic subfield $K = \mathbb{Q}(\beta)$ where d is a rational square free integer and $\beta$ is a root of monic irreducible polynomial of degree 3. We are interested in finding a commutative and associative ring denoted by $\mathbb{Z}_q[\sqrt{d}, \beta]$ using the integral closure $O_L$ of sextic extension $L$. Furthermore, we study the elliptic curve over this ring. Consequently, we will prove the following principal result :

$$E^q_{t,s}(\alpha, \beta) \cong \mathbb{F}^q_5 \oplus E^q_{a_0,b_0}(\alpha, \beta).$$

**Références**

[1] A. Chillali *Elliptic curves of the ring* $\mathbb{F}_q(\epsilon),\ \epsilon^n = 0$, Int. Math Forum, 6 (2011), 1501-1505

[2] A. Chillali and M. Sahmoudi, *Cryptography over sextic extension with cubic subfield*, World Academy Sci. Engrg. Technol. **9** (2015), 246-249.

[3] A. Tadmori, A. Chillali and M. Ziane, *Cryptography over the elliptic curve* $E_{a,b}(A_3)$, Journal of Taibah University for Science, **9** 3, (2015), 326-331.

[4] H. Hassib, A. Chillali and M. Abdou Elomary, *Elliptic curves over a chain ring of characteristic 3*, Journal of Taibah University for Science, **9** 3, (2015), 276-287.

[5] JH.Silverman , *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 2009

[6] M. E. Charkani and M. Sahmoudi, *Sextic extension with cubic subfield*, JP J Algebra, Number Theory Appl. **34** (2014), 139-150.

[7] M. Sahmoudi, *Explicit integral basis for a family of sextic field*, Gulf J. Math. **4** (2016), 217-222.

[8] M. Sahmoudi and A. Chillali, *Key exchange over particular algebaic closure ring*, Tatra Mt. Math. Publ. **70** (2017), 151-162.

[9] M. Sahmoudi and A. Soullami, *On Sextic Integral Bases Using Relative Quadratic Extention*, Bol. Soc. Paran. Mat.. (3s.)v.**38** 4 (2020), 175-180.

[10] M. Virat, *Courbe elliptique sur un anneau et applications cryptographiques*, Thèse Docteur en Sciences, Nice-Sophia Antipolis, (2009).

# Proof Zero Knowledge Based On Elliptic Curves

Mohamed Souhail[1], Seddik ABDELALIM[2] and Abdelhak CHAICHAA[1,2]

Laboratory of Topology Algebra, Geometry and Discrete Mathematics.
Department of Mathematical and Computer Sciences,
Faculty of Sciences Ain Chock,
Hassan II University of Casablanca, Morocco

**Résumé/Abstract**

Zero-Knowledge Proofs has a very important role in many areas such as electronic voting, Electronic Cash. In this paper we will talk about Zero-Knowledge Proofs based on elliptic curves over fields and over the rings $\mathbb{F}_p[e_1, ..., e_n]$, which will be a more secure proof against which based on other mathematical problems.

**Références**

[1] S.Abdelalim, A. Chilali. *The Eliptic Curves* $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ Gulf Journal of Mathematics Vol 3, Issue 2 (2015) 49-53.

[2] M. Virat. *Courbe elliptique sur un anneau et applications cryptographiques.* Thèse Docteur en Sciences, Nice-Sophia Antipolis. (2009).

[3] D. Mumford, J. Fogarty, and F. Kirwan.*Geometric Invariant Theory* , volume 34 of A Series of Modern Surveys in Mathematics . Springer-Verlag, 3e edition, 1994.

[4] N.M. Katz and B.Mazur. *Arithmetic Moduli of Elliptic Curves.* Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.

[5] H.Lange and W.Ruppert. *Complete systems of addition laws on abelian varieties.* Invent.Math. 79, 603-610(1985).

[6] Douglas Stinson.*Cryptography - Theory and Practice* CRC Press, Inc., 1995.

# A Secure Electronic Voting protocol for Multiple Elections based on a Variant of the ElGamal digital Signature

L. Zahhafi and O.Khadir

Laboratory of Mathematics, Cryptography, Mechanics and Numerical Analysis
University Hassan II of Casablanca, Fst Mohammedia, Morocco

**Abstract**

In this work, we propose a new electronic voting scheme inspired from the Mu and Varadharajan method [5]. The protocol is based on the RSA blind digital signature to protect anonymity of all transactions. We used a variant of the ElGamal [3] digital signature to make the protocol valid for multiple elections. The security and complexity of our voting scheme are analysed.

**Références**

[1] T. ElGamal : A public key cryptosystem and a signature scheme based on discrete logarithm problem. IEEE Trans. Info. Theory , IT-31 (1985)

[2] Chaum, D. : Blind signatures for untraceable payments, Advances in Cryptology, Crypto'82, 199–203 (1982)

[3] O. Khadir : New variant of ElGamal signature scheme, Int. J. Contemp. Math. Sciences, Vol. 5, no. 34, 1653–1662 (2010)

[4] R. Rivest, A. Shamir, & L. Adeleman L. : A method for obtaining digital signatures and public key cryptosystems. Communication of the ACM Vol. no 21 (1978)

[5] Y. Mu & V. Varadharajan : Anonymous Secure E-Voting over a Network. IEEE Computer Society, 293–299 (1998)

[6] K. SakoK. & j. Kilian : Secure voting using partially compatible homomorphisms. CRYPTO '94 : 14th International Cryptology Conference, volume 839 of LNCS, 411-424 (1994)