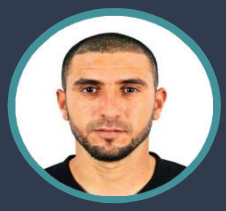
Abdessalem Abidi

Enseignant Chercheur Contractuel

Enseignant chercheur contractuel à la Faculté des sciences et techniques de Sidi- Bouzid FSTSBZ, Université de Kairouan -Tunisie



abdessalemabidi9@gmail.com

+21697243249

Regueb, Sidi-Bouzid, Tunisie

linkedin.com/in/abdessalem-abidi-804261b0

Expériences Professionnelles

Enseignant Chercheur Contractuel

09/2020 - Présent

Faculté des sciences et techniques de Sidi Bouzid – FSTSBZ, Université de Kairouan, Tunisie

Enseignement: *Électronique numérique, Électronique analogique, Fonctions d'électronique analogique, Fonctions d'électronique numérique, Les automates programmables, Sécurité et optimisation dans les réseaux de capteurs sans fil, WSN (Wireless Sensors Network) et protocoles, Communication dans les systèmes embarqués, Bases de données pour les systèmes embarqués, Techniques de test des systèmes sur puce SOC, Mini projet SE/SOC, Programmation en Python.*

Préparation des fascicules des travaux dirigés et des travaux pratiques.

Participation aux réunions pédagogiques et commissions du département Maths-Informatique : *Validation et affectation des sujets des PFE, Délibérations de résultats, Échange avec les autres enseignants pour assurer la cohérence pédagogique de l'ensemble de cours et des travaux pratiques.*

Encadrement et participation aux jurys d'examen des projets de fin d'études.

Conception, tests et diagnostics des cartes électroniques.

Participation à la vie de l'institution : *Conseils, soutenances, membre du club robotique à FSTSBZ, organisation de manifestations scientifiques.*

Enseignant Chercheur Vacataire

09/2018 – 06/2020

Faculté des sciences et techniques de Sidi Bouzid – FSTSBZ, Université de Kairouan, Tunisie

Enseignement : *Électronique analogique, Électronique numérique, Programmation en Assembleur, Microprocesseur et microcontrôleur, Filtrage et conversion analogique numérique, Mini projet électronique.*

Encadrement et participation aux jurys d'examen des projets de fin d'études.

Participation aux réunions pédagogiques et commissions du département Maths-Informatique.

Recherche et développement de composants électroniques.

Participation aux compétitions robotique.

Étalonnage des appareils de mesure.

Formation et Titres Universitaires

Thèse Doctorat

Électronique et Microélectronique

10/2014 - 06/2020

L'école doctorale Matériaux Dispositifs et Microsystèmes - EDMDM

Faculté des sciences de Monastir - FSM

Titre : Contribution à la conception d'un crypto-processeur de chiffrement symétrique à base du mode opératoire CBC prouvé chaotique.

Directeur de thèse : Pr. Mohsen Machhout - Directeur du laboratoire électronique et microélectronique à la faculté des sciences de Monastir.

Diplôme National de Mastère de Recherche

Microélectronique et Nanoélectronique

09/2011 - 01/2014

Faculté des sciences de Monastir - FSM

Titre : Contribution à la conception d'un IP de signature reconfigurable ECDSA

Licence Fondamentale

Électronique, Électrotechnique et Automatique(LFEEA)

09/2008 - 06/2011

Faculté des Sciences de Bizerte - FSB

Baccalauréat

Section Mathématiques

09/2007 - 06/2008

Lycée secondaire de Regueb

Stages de Recherche

Date : *10/2018 – 12/2018*
Lieu : *Équipe* ***AND****, DISC,* ***Institut FEMTO-ST****, Université Bourgogne Franche-Comité,* ***Belfort, France***
Description : *Stage de recherche effectué au sein de l'Equipe Algorithmique Numérique Distribuée (****AND****), Département Informatique des Systèmes Complexes (****DISC****),* ***FEMTO-ST Institute****, UMR 6174 CNRS,* ***Université Bourgogne Franche-Comité, Belfort, France*** *sous la direction des Professeurs* ***Christophe Guyeux*** *et* ***Jean François Couchot***
Objectifs : *Démontrer que l'algorithme de chiffrement symétrique RC5 présente un niveau de sécurité et d'aléa bien supérieur tout en se comportant chaotiquement, notamment lorsqu'il est intégré avec le mode de chiffrement CBC et ceci à travers l'évaluation de la qualité des images chiffrés avec la technique RC5-CBC et l'analyse des résultats de synthèse d'une architecture matérielle implémentant cet algorithme sur un circuit programmable FPGA.*

Date : *07/2017 – 07/2017*
Lieu : *Equipe* ***AND****,* ***DISC****,* ***Institut FEMTO-ST****, Université Bourgogne Franche-Comité,* ***Belfort, France***
Description : *Stage de recherche effectué au sein de l'Equipe Algorithmique Numérique Distribuée (****AND****), Département Informatique des Systèmes Complexes (****DISC****),* ***FEMTO-ST Institute****, UMR 6174 CNRS,* ***Université Bourgogne Franche-Comité, Belfort, France*** *sous la direction du Professeur* ***Jean François Couchot***
Objectifs : *Le comportement imprévisible de l'algorithme RC5-CBC a été vérifié à travers des calculs matériels précis sur une machine dédiée. Le développement de ces analyses nous a permis de valider que RC-CBC présente une extreme sensibilité aux conditions initiales telles que le changement des clés (key sensitivity en anglais) et le changement des messages initiales (plaintext sensitivity en anglais), en plus de satisfaire le phénomène de l'effet d'avanche. Ceci permet donc de confirmer le comportement imprévisible du RC5-CBC.*

Date : *04/2016 – 05/2016*
Lieu : *Département* ***DISC****, Université de Franche-Comité,* ***Besançon, France***
Description : *Stage de recherche effectué au sein du Département Informatique des Systèmes Complexes (****DISC****),* ***FEMTO-ST Institute****,* ***Université de Franche-Comité, Besançon, France*** *sous la direction du Professeur* ***Christophe Guyeux***
Objectifs : *Preuve théorique et expérimentale du chaos de l'algorithme RC5 opérant avec le mode CBC, à savoir l'algorithme RC5-CBC.*

Date : *05/2015 – 05/2015*
Lieu : *Département* ***DISC****, Université de Franche-Comité,* ***Besançon, France***
Description : *Stage de recherche effectué au sein du Département Informatique des Systèmes Complexes (****DISC****),* ***FEMTO-ST Institute****,* ***Université de Franche-Comité, Besançon, France*** *sous la direction du Professeur* ***Christophe Guyeux***
Objectifs : *Modélisation du mode de chiffrement symétrique CBC et l'évaluation de son chaos en opérant avec certains exemples rudimentaires d'algorithmes de chiffrement par bloc extraites à partir de ce qu'on appelle les méthodes de chiffrement par transposition.*

Liste de Publications et Communications Scientifiques

Publications Scientifques :

Salah Dhahri, Abdessalem Abidi, Radhia Bouazizi and Abdelkrim Zitouni. Development, Characterization and Analysis of a magnetic localization algorithm for a wireless endoscopic capsule. Submitted to The journal of supercomputing.

Abdessalem Abidi, Christophe Guyeux and Mohsen Machhout. Evaluation of chaotic properties of CBC mode of encryption embedded with RC5 block cipher algorithm. Discontinuity, Nonlinearity, and Complexity journal Volume 9, Issue 4 pp. 607-618 DOI: 10.5890/DNC.2020.12.013.

Abdessalem Abidi, Anissa Sghaier, Mohammed Bakiri, Christophe Guyeux and Mohsen Machhout. Statistical Analysis and Security Evaluation of Chaotic RC5-CBC Symmetric Key Block Cipher Algorithm. International Journal of Advanced Computer Science and Applications (IJACSA). Volume 10 No 10 October 2019

Abdessalem Abidi, Christophe Guyeux, Jacques Demerjian, Belgacem Bouallègue and Mohsen Machhout. Lyapunov Exponent Evaluation of the CBC Mode of Operation. Chaotic Modeling and Simulation (CMSIM) journal 2: 185–196, 2018.

Abdessalem Abidi, Qianxue Wang, Belgacem Bouallègue, Mohsen Machhout and Christophe Guyeux. Proving chaotic behaior of cbc mode of operation. International journal of bifurcation and chaos. Vol. 26, No. 07, 1650113 (2016).

Communications Scientifques :

Abdessalem Abidi, Christophe Guyeux and Mohsen Machhout. The dynamics of the CBC Mode of Operation. The 2017International Symposium on Nonlinear Theory and its Applications on 4th-7th December 2017. Cancùn, Mexico

Abdessalem Abidi, Christophe Guyeux, Belgacem Bouallègue and Mohsen Machhout. Conditions to have a well-disordered dynamics in the CBC Mode of Operation. Computer Systems and Applications (AICCSA), 2017 IEEE/ACS 14th International Conference on 30 Oct.-3 Nov. 2017. Hammamet, Tunisia.

Abdessalem Abidi, Qianxue Wang, Belgacem Bouallègue, Mohsen Machhout, and Christophe Guyeux. Summary of Topological Study of Chaotic CBC Mode of Operation. Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing And Applications for Business Engineering (DCABES), on 24-26 Aug. 2016, Paris, France.

Abdessalem Abidi, Qianxue Wang, Belgacem Bouallègue, Mohsen Machhout and Christophe Guyeux. Quantitative Evaluation of Chaotic CBC Mode of Operation. International conference on advanced technologies for signal image processing ATSIP'2016, Monastir, Tunisia, March 2016.

Abdessalem Abidi, Belgacem Bouallègue and Fatma Kahri. Implementation of Elliptic Curve Digital Signature Algorithm ECDSA. 2014 Global Summit on Computer & Information Technology (GSCIT), Sousse, 14-16 June 2014.

Synthèse des Activités d'Enseignement

Poste : Enseignant Chercheur Contractuel

Enseignement						
A.U		**Matière**	**Filière**	**Volume horaire**		
				Cours	**TD**	**TP**
2021/2022	**Semestre 1**	*Systèmes logiques et architecture des ordinateurs*	LFSI 1		***21***	
		Fonctions d'Electronique Analogique	LITIC 2	***21***	***10.5***	***10.5***
		WSN et protocoles	LITIC 3	***21***		***21***
		Sécurité et optimisation dans les RCSFs	LITIC 3	***21***	***10.5***	***21***
		Les automates programmables	MPEEAA 2		***10.5***	
	Semestre 2	*Programmation en python*	LFSI 2	***21***		***10.5***
		Fonctions d'électronique numérique	LITIC 1	***21***	***21***	***10.5***
		Fondements des réseaux	LFSI1	***31.5***		***21***

Enseignement						
A.U		**Matière**	**Filière**	**Volume horaire**		
				Cours	**TD**	**TP**
2020/2021	**Semestre 1**	*Communication pour les systèmes embarqués SEs*	LFSI 1		***10.5***	
		Techniques de test SOC	LITIC 2	***21***	***10.5***	***10.5***
		Bases de données pour les SEs	LITIC 3	***21***		***21***
		Mini Projet SE/SOC	LITIC 3	***21***	***10.5***	***21***
	Semestre 2	*Programmation en python*	LFSI 2	***21***		***10.5***
		Fonctions d'électronique numérique	LITIC 1	***21***	***21***	***10.5***

Poste : Enseignant Chercheur Vacataire

Enseignement						
A.U		**Matière**	**Filière**	**Volume horaire**		
				Cours	**TD**	**TP**
2019/2020	**Semestre 1**	*Systèmes logiques et architecture des ordinateurs*	LFSI 1			***10.5***
		Electronique numérique	LITIC 1			***21***
		Atelier d'électronique	LATEC 2			***21***
		Programmation en assembleur	LATEC 2	***10.5***		***21***
		Fonctions d'électronique analogique	LATEC 2		***10.5***	
		Microprocesseur et microcontrôleur	LATEC 2	***21***	***21***	
	Semestre 2	*Programmation en python*	LFSI 1			***21***
		Electronique analogique	LITIC1			***21***
		Fonctions d'électronique numérique	LITIC 1		***21***	***21***
		Filtrage et conversion analogique numérique	LATEC 2	***10.5***	***21***	
		Atelier filtrage et conversion	LATEC2			***21***

Enseignement						
A.U		**Matière**	**Filière**	**Volume horaire**		
				Cours	**TD**	**TP**
2018/2019	**Semestre 1**	*Atelier EEA2 Électronique numérique*	LATEC 1			***21***
		Mini Projet électronique	LATEC 1			***21***
	Semestre 2	*Filtrage et conversion analogique numérique*	LATEC 2	***10.5***	***21***	
		Atelier filtrage et conversion A/N	LATEC 2			***21***

Synthèse des Activités Pédagogiques

Préparation des Fascicules des Travaux Pratiques

09/2021 – Présent

- Fascicule de travaux pratiques de la matière Electronique Numérique.

- Fascicule de travaux pratiques de la matière Fonctions d'électronique analogique.

Examinateur des Projets de Fin d'Études

07/2021 – 07/2021

- Réalisation d'une imprimante intelligente.

- Réalisation d'un système de détection de température dans une salle de conservation des vaccins.

- Réalisation d'un mini robot de lutte contre incendie à base Arduino.

Encadrant des Projets de Fin d'Études

02/2022 – Présent

- Simulation d'un réseau IMS à base des solutions openSource.
- Mise en place d'un système de supervision de réseau.
- Instalation d'une solution fortiproxy sur fortinet.

02/2021 - 06/2021

- Étude et implémentation sur FPGA de l'algorithme de chiffrement RC5 opérant avec le mode opératoire CBC.
- Mise en place d'un système de supervision de réseau.

Co-Encadrant des Projets de Fin d'Études

02/2020 - 06/2020

- Cryptage des images médicales à base de chiffrement symétrique RC5.

- Système d'authentification des étudiants par carte étudiant basé sur l'algorithme de signature numérique ECDSA.

Synthèse des Activités de Recherche

Travaux de Thèse

Titre : Contribution à la conception d'un crypto-processeur de chiffrement symétrique à base du mode opératoire CBC prouvé chaotique.

Résumé : Notre thèse vise à analyser théoriquement le mode de chiffrement symétrique par chaînage de blocs (de l'anglais Cipher Block Chaining CBC), en évaluant ses propriétés de chaos selon la définition réputée de Robert Devaney. Cela se produit lorsque les fonctions de chiffrement envisagées satisfont certaines propriétés liées à un graphe associé bien défini. En effet, la caractérisation de ces fonctions rendant le mode d'opération CBC chaotique, n'était que le point de départ de notre étude de sécurité et d'aléa telle qu'on peut l'entendre avec une approche système dynamique discret. Par la suite, nous avons démontré qu'une telle fonction de chiffrement (à titre d'exemple le Rivest Cipher 5) permet de garantir un niveau de sécurité et d'aléa bien meilleur tout en se comportant chaotiquement, à savoir en opérant avec le mode de chiffrement CBC. À cette fin, nous avons évalué la qualité d`une variété d'images chiffrés avec cet algorithme. Ainsi, nous avons interprété les résultats de synthèse d'une architecture matérielle l'implémentant sur un circuit intégré FPGA. En outre, l'étude topologique de ce mode de chiffrement, prouvé chaotique, a été poursuivie, en considérant plus spécifiquement certaines propriétés quantitatives et qualitatives telles que le niveau d'entropie topologique, le mélange topologique et l'exposant de Lyapunov. Toutes ces propriétés conduisent à un comportement totalement imprévisible pour certains cas de fonctionnement du mode CBC, qui sont précieux pour l'effet avalanche, la diffusion et la confusion souhaitées pour de tels techniques de chiffrement.

Thèmes : microélectronique, cryptographie, sécurité informatique, théorie du choas, théorie des graphes, systèmes dynamiques discrets, modélisation, FPGA.

Travaux de Mastère

Titre : Contribution à la conception d'un IP de signature reconfigurable ECDSA.

Résumé : Dans cette mémoire, nous avons conçu et implémenté successivement deux IPs assurant deux fonctions cryptographiques: Le SHA-256et l'ECC. Chaque IP répond à nos besoins pour le cryptage et l'intégrité des données. Le choix de SHA-256 comme IP de hachage est justifié par le fait que ce dernier est le plus performant du point de vue rapidité (3.864 ns)et espace mémoire occupé (4% occupation en Slices), parmi les IP de hachage disponibles. La principale opération à effectuer lors d'un protocole utilisant les courbes elliptiques est la multiplication d'un point par un scalaire. Pour réaliser cette multiplication nous avons utilisé la multiplication scalaire basée sur le système de coordonnées projectives de Montgomery, la méthode la plus optimale en termes de temps d'exécution (2,618 ms) et de puissance consommée (65,83 mW). En effet, on a choisit d'utiliser le multiplieur de Montgomery vu qu`il est plus performant par rapport au multiplieur série du point de vue occupation de surface sur FPGA (0.4% occupation en Slices, 0.7% pour le multiplieur série) et de point de vue rapidité (2.875 ns, 3.547 ns pour le multiplieur série) pour le type de FPGA Virtex V et dans le corps GF(2 163). Ainsi, nous avons passé des coordonnées affines aux coordonnées projectives afin d'éviter l'opération d'inversion qui est coûteuse de point de vue temps d'exécution et taux d'occupation en CLBs. Enfin, Ces deux IPs ont été regroupés sur une seule puce et implémentés sur FPGA pour constituer notre crypto-processeur ECDSA. En effet, nous avons conçu et implémenté le bloc de génération de signature avec un temps d`exécution de (9.798 ns) ainsi que celui de vérification de signature avec un temps d'exécution de (9.4073 ns).

Thèmes : sécurité, chiffrement, signature numérique, courbes elliptiques, fonctions de hachage, FPGA.

Activité Scientifque

07/2021 – 07/2021

Membre actif du laboratoire électronique et microélectronique à la faculté des sciences de Monastir sous la direction du Professeur Mohsen Machhout

Formations

Formation VDI

10/01/2022 – 14/01/2022

Organisé par : Faculté des sciences et technique de Sidi Bouzid - FSTSBZ

Participation à la formation sur le laboratoire d'étude des réseaux et de la convergence VDI

Formation ATSIP

21/03/2016 – 24/03/2016

Organisé par : Ecole National des Ingénieurs de Sfax - ENIS

Participation à la formation intitulé «2nd International Conference on Advanced Technologies for signal and image processing »

Formation ATURED

21/12/2015 – 26/12/2015

Organisé par : Association Tunisienne de recherche didactique ATURED à l'Institut de Tourisme de Sousse

Participation à la formation intitulé « Logiciel EndNote, Rédaction de l'article, Méthodologie de la thèse »

Formation CANDUST
09/12/2015
Organisé par : CANDUST à la Faculté des médecines de Sfax
Participation à la formation « Author Workshop » .

Formation SETIT
22/02/2015
Organisé par : Research UNIT SETIT & TUNISIAN ASSOCIATION à l'Ecole Supérieure de Commerce de Sfax
Participation à la formation qui traite le domaine de Cloud Computing.

Formation JSMNT
15/01/2015 - 16/01/2015
Organisé par : Institut Supérieure d'informatique et de Mathématiques de Monastir
Participation aux 1ère journées scientifiques (6 conférences plénières) en Microélectronique et Nouvelles Technologies JSMNT 2015.

Formation Presentation in English
12/2014
Organisé par : Faculté des sciences de Monastir
Participation en langue anglaise ayant pour thème « Presentations in English » .

Formation ENIM ROBOTS
05/2014
Organisé par : Ecole Nationale des Ingénieurs de Monastir
Participation aux compétitions nationales de robotiques en Mars, Avril et Décembre 2014 .

Connaissances Techniques

Langages : *MATLAB, VHDL, C, C++, Python, Assembleur*
Packages : *Simulink*
Outils : *MS Office (Word, Excel, Access, PowerPoint), Ares, Isis, System C, MICROC, T-SPICE, EAGLE, Adobe Photoshop, ARES, ISISS, Ubuntu...*
Autres : *Microcontrôleurs PIC, Microcontrôleurs STM, Arduino, Micro-Bit, Rasberry pi, …*

Langues

Arabe : *Langue Maternelle*
Francais : *Lu, écrit, parlé*
Anglais : *Lu, écrit, parlé*