Curriculum Vitae

Cheikh Thiecoumba Gueye
Professeur Titulaire
Equipe de Recherche en Codes Correcteurs et Implantations Sécurisées Post-quantiques (ERCISpq)
Laboratoire d'Algèbre de Géométrie Algébrique et Applications (LACGAA)
Département de Mathématiques et Informatique
Faculté des Sciences et Techniques
Université Cheikh Anta Diop-Dakar Sénégal
Email: cheikht,gueye@ucad.edu,sn
Tel : 00 221 77 630 47 70

I) RESPONSABILITE ACADEMIQUE

- Directeur École Doctorale Mathématiques et Informatique (2022-2025)
- Directeur du Laboratoire d'Algèbre de Géométrie Algébrique et Applications (LACGAA)
- Responsable de l'Équipe de Recherche en Codes Correcteurs et Implantations Sécurisées Post-quantiques (ERCISpq)
- Secrétaire Scientifique de l'École Doctorale Mathématiques et Informatique (EDMI)(2015-2022)
- Responsable Scientifique et Technique du projet de recherche Cryptographie basée sur les codes (CBC) avec le CEA-MITIC
- Responsable Scientifique et Technique du projet de Recherche Implantation Sécurisée Post quantique (ISPQ) avec le Ministère de l'Enseignement Supérieur de la Recherche et de l'innovation
- Responsable du Master Sécurité des Systèmes Embarques
- Responsable de la Licence Cryptographie et Informatique TDSI
- Responsable de la Licence Mathématique Cryptographie et `Sécurité TDSI
- Responsable de l'UE Cryptographie Appliquée et Mathématiques Discrètes de L3TDSI
- Responsable de l'UE théorie des codes et cryptographie du MAGA
- Responsable de l'EC Codes Correcteur d'erreurs du MAGA
- Responsable de l'UE MTDSI-411 Cryptographie - Théorie des Codes
- Responsable des UE Algèbre 1 et 2 de la L1MPI

II) PUBLICATIONS :

II.1) Articles scientifiques indexés

2025

- "*Survey on Side-Channel Attacks on Code-Based Key Encapsulation Mechanism"*, Moroccan Journal of Algebra and Geometry with Applications, volum 4 (pp 109-137). 2025

2023

- Software implementation of a code-based key encapsulation mechanism from Binary QD generalized Srivastava code . In: CBCrypto2022. Springer. 2023, p. 77-89.

2021

- Security Analysis of a Cryptosystem based on Subspace Subcodes in: Wachter-Zeh,A., Bartz, H., Liva, G. (eds) Codes based Cryptography. CBCrypto 2021. Lecture Notes in Computer Sciences, vol 13150. Springer, Cham, pp 42-59

2019

- Quasi-Dyadic Girault Identification Scheme, In: C. Carlet , S. Guilley, A. Nitaj and A. Souidi (Eds), *Codes, Cryptology, and Information Security. C2SI* 2019*.* Lecture Notes in Computer Science, vol 11445, Springer, Cham, pp. 307–321.

- Generalized subspace subcodes with application in cryptology, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 65, NO. 8, AUGUST 2019

- DAGS: Reloaded Revisiting Dyadic Key Encapsulation, In: M. Baldi, P. Santini and E. Persichiti (Eds), Codes Based Cryptography, CBC 2019. Lecture Notes in Computer Science, vol 11666, Springer, PP. 69-85

- Designing a public key cryptosystem based on quasi-cyclic subspace subcodes of Reed Soloman (accepted for publication In: C. T. Gueye, E. Persichiti, P. L. Cayrel and J. Buchmann (Eds), Algebra, Codes and Cryptology A2C 2019 – Communications in Computer and Information Sciences, vol 1133, Springer, PP 97–113
- Improvement of binary and non-binary Statistical Decoding Algorithm, Inforamtion Security and Cryptology, Dec 2019, Seoul Korea, pp 194-207.

2018

- On the Performance and Security of Multiplication in $GF(2N)$. Cryptography 2(3): 25 (2018)

- DAGS: Key Encapsulation from Dyadic GS codes, J. Math. Cryptol. 2018 ; 12(4) : 221–239

2017

- Generalization of BJMM-ISD Using May-Ozerov Nearest Neighbor Algorithm over an Arbitrary Finite Field Fq, In : S El Hajji, A. Nitaj and A. Souidi (Eds), *Codes, Cryptology, and Information Security. C2SI 2017.* Lecture Notes in Computer Science, vol 10194, Springer, Cham, pp. 96–109.

- NP-Complet Problem in Coding Theory with Application to Code-based Cryptography, , In : S El Hajji, A. Nitaj and A. Souidi (Eds), *Codes, Cryptology, and Information Security. C2SI 2017.* Lecture Notes in Computer Science, vol 10194, Springer, Cham, pp. 230–237.

- Efficient Implementation of Hybrid Encryption from Coding Theory, In: S El Hajji, A. Nitaj and A. Souidi (Eds), *Codes, Cryptology, and Information Security. C2SI 2017.* Lecture Notes in Computer Science, vol 10194, Springer, Cham, pp. 254–264.

- NP-completeness of the Goppa parameterized random binary quasi-dyadic Syndrome Decoding Problem, International Journal of Information and Coding Theory Vol. 4, No. 4, pp.276–288, 2017.

2016

- NP-completeness of the random binary quasi-dyadic Coset Weight problem and the random binary quasi-dyadic Subspace Weight problem, Gulf Journal of Mathematics Vol 4, Issue 4 pp. 206-216, 2016.

- A new secret function for modular lattices, BJMCS, 18(3): 1-10, 2016.

- On cyclic codes over Fpk +vFpk + v2Fpk+…+vrFpk, Gulf Journal of Mathematics Vol 4, Issue 4 pp. 130-139, 2016.

2015

- Critical attacks in code-based cryptography Int. J. Information and Coding Theory, Vol. 3, No. 2, 158-176, 2015.

2014

- On Perfect Commutative EIFA-rings. BJMCS. 4(8) : 1166-1169, 2014.

- On Commutative EKFN-ring with Ascending Chain on Annihilators. BJMCS. 4(3) : 426-431, 2014.

2013

- Secure Cryptographic Scheme based on Modified Reed Muller Codes, International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013.
- On Mono-corect Modules, British Journal of Mathematics & Computer Sciences 3(4): 598-604, 2013`

2012

- *A* New Characterization of Commutative Strongly Pi-Regular Rings, Journal of Mathematics Research; Vol. 4, No. 5; 2012

2011

- Erasure Decoding for Gabidulin Codes, J. Math. Model. Algor, (2011) 10: PP. 277-291 DOI 10.1007/s10852-011-9155-3. **http://www.springer.com/mathematics/applications/journal/10852**
- Decoding Algorithm for Gabidulin Codes, International Journal of Mathematics and Computer Science, 6(2011), no.1, PP. 45–54
- New families of two weight of cyclic projective codes construct as the direct sum of two one weight cyclic codes, International J. of Math. Sci. & Engg. Appls. (IJMSEA) ISSN 0973-9424, Vol 5, No. II, (March, 2011), pp, 339-352.

2010

- Gabidulin Codes that are Generalized Reed Solomon Codes. *International journal of Algebra vol. 4, 2010, n° 3, 119-142.* MR2577461, Zbl 1195.94094.

2006

- Affine Invariant Codes over $Z 4$ with Linear Gray image. Global Journal of Pure and Applied Mathematics, Vol. 2 N° 1 (2006), PP. 61-72.
- Binary Image of Affine Invariant Codes over Z4, J. Sci. Vol. 6 N° 2 (2006), pp.75-87.

2004

- Affine invariant codes over $Z 4$ and their binary image, *Math. Sci. Res. J.* **8** (2004), no.11, 328--335.
- On commutative FGS-rings. *Comm. Algebra* **32** (2004), no. 5, 1715—1727

2000

- On commutative FGS-rings with ascending condition on annihilators. Lect. Not. in Pure and Appl. Math.Vol. 217(2000) pp. 227-229.
-

1997

- On commutative FGI-rings. Extracta Mathematicae Vol 12, Num 3, 255-259(1997).

II.2) Chapitres de Livres

- **Codes Based Cryptography, CBCrypto 2022** Deneuville, JC. (eds) Code-Based Cryptography. CBCrypto 2022. Lecture Notes in Computer Science, vol 13839. Springer PP 77-89, Cham. https://doi.org/10.1007/978-3-031-29689-5_5
- **Codes Based Cryptography, CBCrypto 2021**, Wachter-Zeh,A., Bartz, H., Liva, G. (eds) Codes based Cryptography. CBCrypto 2021. Lecture Notes in ComputerSciences, vol 13150. Springer, Cham, pp 42-59

- **Algebre, Codes, Cryptology A2C 2019** C. T. Gueye, E. Persichiti, P. L. Cayrel and J. Buchmann (Eds), Communications in Computer and Information Sciences, vol 1133, Springer, PP 97–113.

- **Codes Based Cryptography, CBC 2019**, M. Baldi, P. Santini and E. Persichiti(Eds), Lecture Notes in Computer Science, vol 11666, Springer, PP. 69-85.
- **22nd International Conference on Information Security and Cryptology, ICISC 2019,** Seo, Jae Hong(Ed.), Inforamtion Security and Cryptology, Vol 11975, Springer, pp 194-207.
- **Codes, Cryptology, and Information Security C2SI 2019** Claude Carlet, Sylvain Guilley, Abderrahmane Nitaj, El Mamoun Souidi (Eds.), Lecture Notes in Computer Science, Vol. 11445, Springer, pp. 307–321.
- **Codes, Cryptology, and Information Security C2SI 2017**, Said El Hajji, Abderrahmane Nitaj, El Mamoun Souidi (Eds.), Lecture Notes in Computer Science, Vol. 10194, Springer, (pp. 230–237, pp. 254–264, pp.276–288)

- **Coding and Cryptography"**, USTHB, Alger, 2-5 Novembre 2015, Sihem Mesnager, Kenza Guenda and Kamel Betina (Eds)
www.latn.usthb.dz/spip.php?article35
- **Codes, Cryptology, and Information Security C2SI 2018** Claude Carlet, Sylvain Guilley, Abderrahmane Nitaj, El Mamoun Souidi (Eds.), Lecture Notes in Computer Science, Vol. 11445, Springer Online version
- **Geometry and combinatorial Aspects of commutative Algebra** Marcel Dekker New York (2001), pp. 227 – 230.

II.3) Editor General Chair

- **Mathematics of Computer Science, Cybersecurity and Artificial Intelligence** Six Scientific Days of the Doctoral School of Mathematics and Computer sciences 2024 (S2DSMCS) Proceedings in Mathematics & Statistics, Springer

- **Mathematics of Computer Science, Cybersecurity and Artificial Intelligence** Fifth Scientific Days of the Doctoral School of Mathematics and Computer sciences 2023 (S2DSMCS) Proceedings in Mathematics & Statistics, Springer

- **Non-Associative and Non-Commutative Algebra and Operator Theory NANCAOT 2014**, Gueye Cheikh Thiecoumba, Siles Molina Mercedes (Eds), Springer Proceedings in Mathematics & Statistics, Springer ISBN 13: 978-3319239000

- **Algebre, Codes, Cryptology A2C 2019** C. T. Gueye, E. Persichiti, P. L. Cayrel and J. Buchmann (Eds), Communications in Computer and Information Sciences, vol 1133, Springer ISBN 978-3-030-36237-9)

III) COMMUNICATION

- 5eme Journée des doctoriales de l'Ecole Doctoriale PCSTUI du 17 au 19 Novembre 2025 : Synergie transdisciplinaire et défis sociaux complexes.

- Semaine de l'innovation et l'entreprenariat de l'UCAD du 27 au 31 Janvier 2025 : La recherche au service de l'innovation et de l'entreprenariat.

- Séances Académiques du vendredi 30 Septembre 2022 de l'Académie Nationale des Sciences et techniques : La cryptographie post-quantique : enjeux et perspectives

- C2SI 2019 International Conference on Codes, Cryptology, and Information Security 2019, Rabat (Morocco), Avril 22-24, 2018;

Exposé: Quasi-Dyadic Girault Identification Scheme.

- C2SI 2017 International Conference on Codes, Cryptology, and Information Security 2017, Rabat (Morocco), Avril 10-12, 2017;

Exposé: Generalization of BJMM-ISD Using May-Ozerov Nearest Neighbor Algorithm.

- C2SI 2017 International Conference on Codes, Cryptology, and Information Security 2017, Rabat (Morocco), Avril 10-12, 2017;

Exposé: NP-Complet Problem in Coding Theory with Application to Code-based Cryptography.

- C2SI 2017 International Conference on Codes, Cryptology, and Information Security 2017, Rabat (Morocco), Avril 10-12, 2017;

Exposé: Efficient Implementation of Hybrid Encryption from Coding Theory.

- Journées Mathématiques du Sénégal 2017 (JMS2017), UGB- St Louis,

Exposé: Cryptographie Post-quantique

- *On International Colloquium of Number Theory Cryptography and Information Security. Taza (Maroc) November 11-12, 2016.*

Exposé: NP-completeness of random binary quasi-dyadic coset weight problem and the random binary quasi-dyadic subspace weight problem.

- Colloque International sur la théorie du Codage et de la Cryptographie (ICCC 2015), USTHB, Alger, 2-5 Novembre 2015 ;

Exposé: NP-completeness of the Coset Weight Problem for Quasi-dyadic codes.

- Colloque sur la Cryptographie et les Codes Correcteurs d'Erreurs- Université Cheikh Anta Diop- 03-11 Decembre 2015 à Dakar :

Exposé: McEliece Hypothese de Securité

- Dakar's Workshop in honor of Professor Amin Kaidi on Non Associative and Non Commutative Algebra and Operator theory took place May 23-25, 2014 in Dakar.

Exposé: Some properties of mono-correct and epi-correct modules

- Journée Commission Nationale de la Cryptologie, 18 Mars 2014, Présidence de la Republique

Exposé : Implémentations Sécurisées Post-quantique

- 06/2010 CMMSE 2010 (International Conference on Computational and Mathematical Methods in Science and Engineering), Almeria (Espagne), 26-30 Juin 2010;

Exposé intitulé: "Erasure Decoding for Gabidulin codes".

- 04/2008 12ème Atelier d'Algèbre et de Logique(AAL-12), Yaoundé (Cameroun), 03-04 Avril 2008 ;

Exposé Intitulé : « Invariant affine codes on Z_4 ».

- 08/2007 Ecole d'Eté de Calcul Formel et Théorie des Nombres, Faculté des Sciences de Monastir, Monastir (Tunisie) du 27 Août au 07 Septembre 2007 ;

Exposé intitulé : « Codage Algébrique »

- 11/2005 Rencontre Internationale Algèbre Commutative, Codes Correcteurs et Cryptographie, Bamako (Mali), 18 - 25 Novembre,

Exposé intitulé :« les Codes Linéaires sur un Modules «.

- 08/2003 Summer School and Conference on Real Algebraic and its Applications, Trieste (Italie), 04-22 Aout 2003;

Exposé intitulé : " On Commutative FGS-rings "

- 06/1999 Conference on Commutative Algebra and Algebraic Geometry, Messina (Italie), 16-20 Juin 1999;

Exposé intitulé: « On commutative FGS-rings with ascending condition on annihilators »

IV) ACTIVITE D'ENCADREMENT

IV.1) Encadrement de Thèses

IV. 1.1 Thèses en cours

- **Khaly Dieng :** Première année de thèse
  Résistance des implémentations cryptographiques AES face aux attaques par canaux auxiliaires basées sur l'apprentissage automatique.
- **Lobe Guilel Dia :** Première année de thèse
  Résilience du Cryptosystème de McEliece face aux Attaques par canaux auxilliaires.
- **Fallou Diaw :** Deuxième année de thèse
  Intitulé de la thèse : Sécurité des réseaux de neurone implémenté dans les cartes à puce.

- **Mamadou Loum :** Deuxième année de thèse
  Intitulé de la thèse : Gestion des Feux de circulation et de la pollution atmosphérique avec IA et Big Data.
- **Massamba Sow :** Deuxième année de thèse
  Primitives cryptographiques basées sur les codes à symétrie non triviales.
- **Mamadou Cherif Kasse** : Troisième année de thèse
  Intitulé de la thèse : L'utilisation de la cryptographie basée sur les codes dans la technologie Blockchain.

IV. 1.2 Thèses soutenues

- ***Régis Freguin BABINDAMANA*****,** inscrit en thèse depuis Novembre 2 007 sous ma direction, il a soutenu le 02 Novembre 2010 sa thèse

Intitulé de la thèse : Lien entre codes de Gabidulin et codes de Reed Solomon Généralises

- ***Mohamed Sall*****,** inscrit en thèse depuis octobre 2006 sous ma direction, il a soutenu sa thèse le 28 Decembre 2011.

Intitulé de la thèse : Nouvelle construction, par somme directe, de codes cycliques à deux poids. Et dénombrement de codes cycliques irréductibles.

- ***Anta Niane Gueye*****,** inscrit en thèse depuis octobre 2010 sous ma direction, elle a soutenu sa thèse en Decembre 2013

Intitulé du sujet de thèse : Sur la monocorrectivité des modules : Une nouvelle caractérisation des anneaux commutatifs

- **Ousmane Ndiaye,** inscrit en thèse en octobre 2013 sous ma direction, il a

Soutenu sa thèse le 13 Aout 2016.
Intitule de la thèse : Protocoles *cryptographiques post-quantiques* et attaques critiques.

- ***Modou M'boup*****,** inscrit en thèse depuis octobre 2013, sous ma direction, il a soutenu sa these le 13 Janvier 2018

Intitule du sujet de thèse : Chiffrement hybride basé sur les codes

- **Jean Belo klamti,** inscrit en thèse en Juin 2015 sous ma direction, il a soutenu sa these le 29 Janvier 2018

Intitule de la thèse : Conception des cryptosystèmes post-quantiques et généralisation de l'attaque de décodage par ensemble d'informations

- **Gilbert Ndollane Dione ,** inscrit en thèse en Juin 2016 sous ma direction, il a soutenu sa these le 30 Novembre 2020
  Intitule de la thèse : Mécanisme d'Encapsulation et Schéma d'Identification basé sur les codes.

IV.2) Encadrement de mémoire de DEA

- **Yakhya Diop**

Sujet : Modules avec condition de chaine sur les endo-images et les endo-noyaux (soutenu en Aout 2011)

- **Ibrahima Mbaye**

Sujet : La théorie des codes correcteurs d'erreurs (soutenu en Juin 2009)

- **Mohamed Val ould Mohamed Mahmoud**

Sujet : Démonstration du lemme dce Hensel dans un anneau local noetherien(soutenu en Septembre 2007)

- ***Mohamed Yahya ould Mohamed Abdellahi*,**

Sujet : Code negacycliques sur Z4 (soutenu en Janvier 2006).

IV.3) Encadrement de mémoire de Master

- **Abdoulaye Ndongo** (soutenu en Décembre 2025)

Sujet : Conception et mise en œuvre d'un SOC industriel avec integration SOAR pour la protection des infrastructures critiques

- **Bineta Diagne** (soutenu en Décembre 2025)

Sujet : Conception d'un système IIoT de gestion intelligence de la consommation d'eau des lacs de SOCOCIM Industries basé sur la prévision

- **Oumar Coundoul** (soutenu en Décembre 2025)

Sujet : Mise en place d'un SOC pour la surveillance des infrastructures reseau et serveurs critiques

- **Gora Gueye** (soutenu en Octobre 2025)

Sujet : Etude de robustesse des systèmes de détection d'intrusions bases sur le Deep Learning : Attaques adverses et mécanismes de défense dans les réseaux IoT

- **Khaly Dieng** (soutenu en Octobre 2025)

Sujet : Vérification et analyse de la sécurité des systèmes embarques étude expérimentale de l'AES-128 sur microcontrôleur STM32

- **Lobe Guilel Dia** (soutenu en Octobre 2025)

Sujet : Récupération de la clé privée de Classic McEliece à partir des fuites de poids de Hamming

- **Aida Gueye** (soutenu en Octobre 2025)

Sujet : Etude du schéma HQC : fondements, sécurité et implémentation

- **Aminta Cisse** (soutenu en Octobre 2025)

Sujet : Détection et prévention des attaques par Fuzzing sur les Systèmes embarqués

- **Abdou Khadre Ba** (soutenu en Octobre 2025)

Sujet : Conception d'un système de pointage biométrique multimodal sécurisé dans le cadre du New Deal Technologique du Sénégal

- **Khady Sylla** (soutenu en Octobre 2025)

Sujet : Détection d'intrusions IoT basée sur les LLM

- **Moussa Ndiaye** (soutenu en Octobre 2025)

Sujet : Etude conception et mise en œuvre d'une plateforme virtuelle basée sur Proxmox

- **Fallou Diaw** (soutenu en Octobre 2024)

Sujet : Apprentissage multitâches appliqué au contexte des attaques par canaux auxiliaires

- **Serigne Ahmadou Niang** (soutenu en Décembre 2018)

Sujet : Cryptanalyse algébrique sur le cryptosystème de McEliece utilisant les Bases de Grobner

- **Modou Ndiaye** (soutenu en Mai 2017)

Sujet : Codes Quasi Dyadiques : Réduction de la taille des clefs du cryptosystème de McEliece

- **Abdou Mbar Ly** (soutenu en Février 2017)

Sujet : Etudes et implémentation du chiffrement homomorphe DA-Encryp

- **Ababcar Aziz Kane** (soutenu en Février 2016)

Sujet : Cryptosystème de McElice basé sur les Codes MDPC

- **Gilbert Ndollane Dione** (soutenu en Décembre 2015)

Sujet : Signature basée sur les codes quasi dyadiques

- **Jean Klamti Bello** (soutenu en Avril 2015)

Sujet : Application de la borne de Gilbert –Varshamov sur les codes quasi dyadiques

- **Mbouye Khady Diagne** (soutenu en Juin 2014)

Sujet : Simulation d'un d'encodeur utilisant les codes de Hamming de longueur 7 sur F2

- **Fatimatou Mint El Bachir** (soutenu en Avril 2013)

Sujet : Implémentation de la transformation permettant de passer d'un code de Gabidulin à un code de RSG

- **Ameth N'diaye** (soutenu en Mars 2012)

Sujet : Module endo artinien et endo noethérien

- **Ousmane Ndiaye** (soutenu en Mars 2012)

Sujet : Cryptanalyse Algébrique du cryptosystème de McElliece.

- **Ould Mohamed Yehdhih Mohamed** (soutenu en Aout 2011)

Sujet : Etudes de nouveaux paramètres des fonctions courbes

- **Ali Yacine Sangharé** (soutenu en Novembre 2009)

Sujet : Algorithme d'Euclide Etendu : Application aux décodage des codes BCH

- **Thialy Badiane** (soutenu en Septembre 2009)

Sujet : Fonctions Courbes et théorie des codes correcteurs d'erreurs

- **Ibrahima Yade** *(soutenu en juillet 2008)*

Sujet : Code Z4 linéaires

- **Modou Mboup** (soutenu en Juillet 2008)

Sujet : Technique de traitement d'erreurs par les codes de Reed Muller d'ordre 1.

- **Alzouma Aicha** (soutenu novembre 2007)

Sujet : Codes Affines invariant sur Z4 et Leur image par l'application de Gray.

- **Bocar Diaw** (soutenu en Novembre 2007)

Sujet : Masquer la structure des codes GRS pour un usage cryptographique

- ***Régis Freguin Babindamana*** (soutenu en Octobre 2007)

Sujet : Nouvelle classe de code cyclique à deux poids.

V.) PARTICIPATION AUX JURY

V.1) Participation Jury de Thèse

Membre du jury de soutenance de thèse de doctorat unique de :

- **Aminata NGOM** en de qualité Président du Jury.

  Thèse soutenue le 29-03-2024,

Sur le sujet : « **Techniques de stéganographie basées sur les Ondelettes et Méthodes Cryptographiques pour la sécurité des données patient et l'aide au diagnostic médical** ».

- **El Veth SIDI** en qualité de Président du jury.

  Thèse soutenue le 18-02-2023,

Sur le sujet : « **Contributions à l'amélioration de la sécurité de données dissimulées : Modélisation et simulation des modelés S-CCR et M-S-CCR** ».

- **Boubacar Issoufou Djibo** en qualité de Président du Jury.

  Thèse soutenue le 12-12-2022,

Sur le sujet : « **Modèle d'Accès Optique pour accompagner l'atteinte des objectifs du Développement Durable dans le contexte Africain** ».

- **Edgard NDASSIMBA** en qualité de Président du Jury.

  Thèse soutenue le 26-11-2022,

Sur le sujet : « **Etude d'impact de la TV White Space dans la relance de l'éducation, de la santé et de l'agriculture des zones rurales en Afrique-cas de la République centrafricaine** ».

- **Ghislain Mervyl Saint-Juste KOSSINGOU** en qualité de Président du Jury.

  Thèse soutenue le 26-11-2022,

Sur le sujet : « **Etude de l'impact des technologies émergentes dans la remédiation des années de ruptures des activités pédagogiques des zones rurales des pays en situation de post conflit : cas de la République centrafricaine** ».

- **Abdoulaye Maiga** en qualité de Président du jury.

  Thèse soutenue le 24-06-2022,

Sur le sujet : « **Relèvement canonique de surfaces abéliennes** ».

- **Soda DIOP** en qualité de Président du jury.

  Thèse soutenue le 11-06-2022,

Sur le sujet : « **Résolution libre sur les entiers et bases de Gröbner – Shirshov sur les DA-anneaux** ».

- **Sèmou DIOUF** en qualité de Président du jury.

  Thèse soutenue le 28-03-2022,

Sur le sujet : **« Suites récurrentes linéaires sur les corps finis : détermination de la période et coût algorithmique de la fonction d'autocorrèlation ».**

- **François Kassémé GOMIS** en qualité de Président du jury.

  Thèse soutenue le 26-03-2022,

Sur le sujet : **« Etudes des techniques d'apprentissage-machine pour la stéganalyse universelle ».**

- **Amar FALL** en qualité de Président du jury.

  Thèse soutenue le 03-03-2022,

Sur le sujet : **« Quelques Classes d'Algèbres Réelles de Division Ayant Peu d'Automorphismes » « Algèbres absolument Valuées Qui Satisfont A (x^2, y, x^2) = 0 ».**

- **Pagdame TIEBEKABE** en qualité d'Examinateur.

  Thèse soutenue le 22-02-2022,

Sur le sujet : **« Formes linéaires de logarithmes et Equations Diophantiennes ».**

- **El Hadji Ousseynou Diallo** soutenu en Aout 2014

Sujet : Hopficité et co-Hopficité dans la catégorie COMP des complexes

- **Sidi Mouhamed ould Mouhamed** soutenu en Juillet 2014

Sujet : Sur les duo-anneaux artiniens à idéaux principaux

- **André Saint Eudes Mialebama** soutenu en Mars 2014

Sujet : Généralisation des bases de Grobner comm et non comm sur certains types d'anneaux

- **Abdoulaye Mbaye** soutenu en Fevrier 2014

Sujet : Contribution à l'études des anneaux à idéaux principaux

- **Anta Niane Gueye** soutenu en Janvier 2014

Sujet : Sur la monocorrectivité des modules : Une nouvelle caractérisation des anneaux commutatifs

- **Fagueye Ndiaye** soutenu en Novembre 2014

Sujet : Etude du problème de localisation : Identification de sites et de données

- **Mame Cheikh** Diouf soutenu en Mars 2016

Sujet : Les algèbres de Poisson graduées

- **Daouda Faye** soutenu en Mai 2016

Sujet : Localisation et algèbre des polynômes dans un duo anneau

- **Ousmane Ndiaye** soutenu en Aout 2016

Sujet : Protocoles Post-quantiques et Attaques Critiques

- **Ibrahima Labou** soutenu en Aout 2016

Sujet : Nouvelle caractérisation des anneaux commutatifs AIP

- **Mohamed Traoré** soutenu en Novembre 2016

Sujet : Algèbres à puissance 3 associatives réelles de division

- **Babbacar Alassane Ndao** soutenu en Décembre 2016

Sujet : Générateur d'aléa et sécurité : Loi des présences-conception d'un distingueur d'aléa.

- **Ould Cheikh Ahmed youssef** soutenu en Décembre 2016

Sujet : Calculs sur les courbes elliptiques de genre < ou = 2 et cryptographie

- **Ibrahima Gaye** soutenu en

Sujet : Analyse des réseaux sociaux : Contribution à la détection de semences dans la maximisation de l'influence.

- **Nafissatou Diarra** soutenu en Aout 2017

Sujet : Fonction de hachage sur les courbes (hyper)Ellyptiques et bases de Grobner non commutatives sur les D-A anneaux

- **El Hadji Modou Mboup** soutenu en Janvier 2018

Sujet : Chiffrement Hybrides et Authentification Forte basée sur les codes correcteurs d'erreurs

V.2) Participation Jury de Mémoire de Master

- **Cheikh MBENGUE** soutenu le 30 Avril 2023

Sujet : Cryptographie sur les courbes elliptiques et systèmes d'authentification par NFC

- **Penda DIAKHATE** soutenu le 30 Avril 2023

Sujet : Attaque par injection de fautes dans le cryptosystème Classique de McEliece pour retrouver le message clair.

- **Soda NDIAYE** soutenu le 30 Avril 2023

Sujet : Cryptanalyse sur les subcodes espace basé sur les GRS quasi cyclique

- **Ababacar DIBA** soutenu le 30 Avril 2023

Sujet : Signature Caméléon

- **Oumar Kabogari** soutenu en Novembre 2016

Sujet : Audit de sécurité des Systèmes de Gestion de Base de Données.

- **Mohamed El Mehdi Ahmed EL HADJ** soutenu en Novembre 2016

Sujet : Etude et mise en place d'une base de données secours sous Oracle 11gR2.

- **Moussa DIEDHIOU** soutenu en Novembre 2016

Sujet : Audit de sécurité avec Kali Linux et Etude des solutions contre les attaques des malwares (virus, trojan, vers).

- **Awa Diagne** soutenu en Novembre 2016

Sujet : Déploiement de Cisco Network Admission Control (PacketFense)

- **Youssou NDIONE** soutenu en Fevrier 2017

Sujet : Etude et mise en en place d'une solution d'authentification unique

- **Ousmane COULIBALY** soutenu en Fevrier 2017

Sujet : Knapsack Problem and Cryptanalyze

- **Khadidiatou BA** soutenu en Fevrier 2017

Sujet **:** Analyse de la QoS du réseau de la Sonatel

- **Modou Fall KANE** soutenu en fevrier 2017

Sujet : Etude et mise en œuvre d'un réseau sécurisé de Paiement par carte : E-Transaction

- **Abdoulaye MBAYE** soutenu en Fevrier 2017

Sujet : Etude et mise en place d'une solution pour sécuriser les payements en ligne

- **Gora Seye** soutenu en Décembre 2017

Sujet : Conception et réalisation d'un lecteur de carte à puce

- **Lemneya Badda** soutenu en Décembre 2017

Sujet : Etude et mise en place des solutions d'accès à DataCentre

- **Bounama Abdoul Hakim Niang** soutenu en Décembre 2017

Sujet : Etude et mise en place d'une solution de monitoring du mobile money

- **Bounda Toure** soutenu en Février 2018

Sujet : Application de messagerie SMS intégrant l'authentification et la confidentialité (Android et iOS)

- **Mouhamadou Lamine Ba** soutenu en Février 2018

Sujet : Sécurité du mobile money

- **Assane Diop** soutenu en Février 2018

Sujet : Etude de la politique de Sécurité de la Dématérialisation des procédures de passation des marchés publics

- **Seydou Cisse** soutenu en Février 2018

Sujet : Audit et politique de sécurité du Système d'Information du Centre National d'Etat Civil du Sénégal

- **Ousseynou Diankha** soutenu en Février 2018

Sujet : Etude et mise en place d'une solution d'interconnexion sécurisée pour des entreprises Multi-sites

- **Ndèye Fatou NDOUR** soutenu en Décembre 2018

Sujet : Etude et mise en œuvre d'une solution de gestion de la sécurité des SI et des événements : SIEM

- **Abdoulaye CISSE soutenu en Décembre 2018**

Sujet : Analyse en temps réel de données et visualisation avec Streaming Analytics Manager et SuperSet (Bigdata)

- **Serigne Ahmadou NIANG** soutenu en Décembre 2018

Sujet : Cryptanalyse algébrique sur le cryptosystèmes de McEliece utilisant les Bases de Grobner

- **Moustapha DIAGNE** soutenu en Décembre 2018

Sujet : Etude et mise en place d'une politique de défense en profondeur contre les attaques de types "zéro day"

- **Seydou CISSE** soutenu en Décembre 2018

Sujet : Étude et mise en place d'un système de management de la sécurité de

l'information (SMSI) basé sur ISO/IEC 27001 pour le compte de InTouch SA

- **Babacar Ema NDIAYE** soutenu en Décembre 2018

Sujet **:** Etude sur la sécurité du cloud

- **Aichétou Djimé GALLEDOU** soutenu en Décembre 2018

Etude et implémentation d'un outil d'aide à la Décision Médicale sur l'intelligence artificielle

- **Ndèye Yacine NDAO** soutenu en Décembre 2018

Sujet : Conception et mise en place d'un CRM de gestion des contrats pour l'ONG ALIMA

- **Fatou Bintou DIEYE** soutenu en Décembre 2018

Sujet : Audit continue des systèmes d'information et assurance à temps réel sur la qualité

- **Ndèye Téning NDIAYE** soutenu en Décembre 2018

Sujet : Implémentation des contrôles de sécurité dans les systèmes existants.

- **Sokhna NDIAYE** soutenu en Décembre **2018**

Sujet : Etude et conception d'une solution de gestion des identités basée sur la technologie des cartes à puce.

VI) DEVELOPPEMENT INSTITUTIONNEL

VI.1) Promotion de la Recherche

- Organisation Doctoriales EDMI 2023 du 20 au 23 Décembre 2023
- Organisation Doctoriales EDMI 2024 du 17 au 19 Décembre 2024

- Programm Committee of C2SI 2023 fourth International Conference on Codes, Cryptology, Rabat (Morocco), Mai 29-31, 2023
- Organisation du Conseil Scientifique numéro 50 du25 Juillet 2022
- Organisation du Conseil Scientifique numéro 49 du 18 Mars 2022
- Organisation du Conseil Scientifique numéro 48 du 18 Janvier 2022
- Programm Committee of I4CS International Conference on Cryptography, Coding Theory and Cyber Security, 26-28 October, Casablanca (Morocco) 2022
- Projet Codes Based Cryptography (CBC) financé par le Centre d'Excellence Africain en Mathématiques Informatique et TIC.
- Projet Implantations Sécurisés Post-quantiques (ISPQ) en collaboration avec la Commission Nationale de Cryptologie et financé par le Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation.

- Standardisation Post-Quantique de DAGS :
- Organisation de séminaire de recherche hebdomadaire de l'équipe ERCISpq (vendredi de 17h – 19h)
- Organisation d'un séminaire sur Side channel attack du 11 Janvier au 13 Janvier 2017
- Organisation d'un séminaire sur les attaques algébriques basées sur les codes du 02 au 05 Octobre 2018 FST-Dakar
- Programm Committe of C2SI 2019 International Conference on Codes, Cryptology, and Information Security 2019, Rabat (Morocco), Avril 22-24, 2019 ;
- General Chair de la conférence **Non-Associative and Non-Commutative Algebra and Operator Theory NANCAOT 2014,** Gueye Cheikh Thiecoumba, Siles Molina Mercedes (Eds), Springer Proceedings in Mathematics & Statistics, Springer ISBN 13: 978-3319239000
- General Chair de la conference **Algebre, Codes, Cryptology A2C 2019** C. T. Gueye, E. Persichiti, P. L. Cayrel and J. Buchmann (Eds), Communications in Computer and Information Sciences, vol 1133, Springer)

VI.2) Promotion de la Pédagogie

- Responsable du comité de pilotage de la mise en place du Master Sécurité des Systèmes embarqués
- Responsable équipe pédagogique de la LTDSI
- Participation au séminaire de DMI en 2016 sur l'évaluation des masters
- Participation au séminaire de DMI en 2017 sur l'élaboration des syllabus des cours des licences
- TD d'Algèbre de licence de Mathématiques de la Faculté des Sciences et Techniques UCAD.
- Cours de Cryptographie - Théorie des Codes Master Recherche TDSI 1ère et 2ème année de la Faculté des Sciences et Techniques UCAD.
- Cours de Cryptographie - Théorie des Codes Master MAGA1ère et 2ème année de
- Cours d'Introduction à *la théorie des Codes Correcteurs d'Erreurs* de Master Professionnel TDSI 1ère année de la Faculté des Sciences et Techniques. UCAD
- Cours Codes Correcteurs et fonctions Booléennes de la Formation doctoral Codage Cryptographie, Algèbre et Applications de l'école doctorale EDMI de l'UCAD.
- TD d'Algèbre en première année de MPI
- TD d'Algèbre en première année de PCSM
- Cours Magistral L1MP

VI.3) Promotion de la gouvernance

- Membre de la commission d'élaboration et de partage des procédures clés de l'Ecole doctorale EDMI (octobre 2017)
- Membre de la commission chargé de la rédaction du règlement intérieur actualisé de EDMI
- Membre de la commission chargé de proposer un organigramme de l'EDMI
- Responsable de la Bonne Gouvernance de PACER II

- Membre de la commission Assurance qualité de DMI
- Participation en 2015 au séminaire de DMI sur la Gouvernance et l'élaboration d'un plan stratégique
- Participation en 2018 au séminaire de DMI sur la validation des programmes de bonne gouvernance et sur la conception d'un plan quinquennal.

VI.4) Service à la communauté

- Commission institutionnelle du CAMES de l'Université Cheikh Anta Diop de Dakar depuis 2021

- Participation à l'autoévaluation de la licence TDSI en 2015 en tant que Responsable de l'équipe Pédagogique de l'auto évaluation
- Identification des éléments de preuves et des personnes ressources en tant Responsable du comité de pilotage de la préparation du dossier d'auto-évaluation de la LTDSI (2015)
- Participation à l'évaluation externe du programme LTDSI par ANAQ-SUP en 2017
- Instruction de plus de 200 thèses de EDMI à l'attention du curateur de l'Ecole Doctorale Mathématiques et Informatique.
- Représentant de l'Ecole Doctorat Mathématique et Informatique à l'atelier de formation au montage de projet de recherche Horizon 2020 de l'Union Européenne du 26 au 27 Mai 2015.
- Responsable de la coopération Interuniversitaire du Laboratoire d'Algèbre, de Cryptologie, de Géométrie Algébrique et Applications (LACGAA) ;
- Représentant de l'UCAD au projet « Action intégrée pour le renforcement institutionnel et l'internationalisation des mathématiques au Sénégal » (projet Université de Malaga et Université Cheikh Anta Diop)
- Membre du comité d'organisation de la conférence **Non-Associative and Non-Commutative Algebra and Operator Theory NANCAOT 2014**
- Instructeur au Conseil Africain et Malgache pour l'Enseignement Supérieur (CAMES) ;
- Referee au journal "Journal of Mathematical, modeling and Algorithm";
- Referee à la revue « Africaine de la Recherche en Informatique et mathématiques Appliquées (ARIMA) » ;
- Referee au journal « Designs, Codes and Cryptography »;
- Reviewer à American Mathematical Society;