Hervé TALE

PhD in Cryptography

National Advanced school of Engineering - Yaounde
Department of Computer Engineering
Po Box. 3614 Yaounde-Messa (Cameroon)
(+237 6 95 38 17 50)
herve.tale@univ-yaounde1.cm
http://perso.prema-a.org/herve.tale-kalachi/

Identification

Name: **TALE KALACHI**

Surname: **Hervé**

Born the: 30^{th} August 1989 at Bafoussam, Cameroon

Languages: My native language is French, but I also speak and write English

Current position

Senior Lecturer, *Department of Computer Engineering*, National Advanced school of Engineering of Yaounde, University of Yaounde 1.
Cameroon

Diplomas and training

2014 - 2017 **PhD in Mathematics and Computer Sciences, on the topic: "Security of cryptographic protocols based on Coding theory"**, University of Rouen & University of Yaounde 1, Supervisors : Ayoub Otmani & Marcel TONGA, Co-supervisor: Sélestin Ndjeya.

2009 - 2012 **Master degree with thesis in Mathematics**, University of Yaounde 1, Cameroon.

2006 - 2009 **Bachelor's degree in Mathematics**, University of Yaoundé 1, Cameroon.

2006 - 2009 **Secondary and High School Teacher's Diploma in Mathematics**, Higher Teacher's Training College of Yaoundé (Cameroon).

Teaching and research experiences

2019 - 2020 Post-doctoral researcher at **Inria** in the **ARIC** team at "ENS de Lyon", involved in the **RISQ-project** and working with Prof. Damien Stehlé on lattice-based cryptography.

2017 - 2019 Teachings of Computer Science at Government High school of Soa - Yaounde (Cameroon)

2016 - 2017 Teachings and research assistant at the department of computer science, University of Rouen-Normandie (France).

2009 - 2015 Mathematics teacher at "Government high school of Bandenkop" (West Cameroon).

2010 - 2015 Pedagogic leader of the mathematics department at "Government high school of Bandenkop".

Publications

- Franck Rivel Kamwa Djomou, Hervé Talé Kalachi, Emmanuel Fouotsa, **Generalization of Low Rank Parity-Check (LRPC) Codes over the Ring of Integers Modulo a Positive Integer** *Arabian Journal of Mathematics, 1-10 DOI 10.1007/s40065-021-00327-z (2021)*
- Hervé Talé Kalachi, **On the Failure of the Smart Approach of the GPT Cryptosystem** *Cryptologia, DOI: 10.1080/01611194.2020.1829181 (2020)*
- Vlad Dragoi and Hervé Talé Kalachi, **Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC** *IEEE Communications Letters 22(2): 264-267 (2018)*
- Philippe Gaborit, Ayoub Otmani and Hervé Talé Kalachi, **Polynomial-Time Key Recovery Attack on the Faure-Loidreau Scheme Based on Gabidulin Codes**, *Design, Codes and Cryptography, 86(7): 1391-1403 (2018).*
- Ayoub Otmani, Hervé Talé Kalachi and Sélestin Ndjeya, **Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes**, *Design Codes and Cryptography 86(9): 1983-1996 (2018).*
- Dominic Bucerzan, Vlad Dragoi and Hervé Talé Kalachi, **Evolution of the McEliece Public Key Encryption Scheme**, *In Innovative Security Solutions for Information Technology and Communications - 10th International Conference, SecITC 2017, Bucharest, Romania, June 8-9, 2017, Revised Selected Papers*
- Ayoub Otmani and Hervé Talé Kalachi, **Square Codes attack on a modified Sidelnikov Cryptosystem**, *International Conference in Codes, Cryptology and Information Security, Rabat, Morocco.* (26-28 May 2015).

Preprints

Low-Rank Parity-Check Codes Over Finite Commutative Rings and Application to Cryptography, *Hermann Tchatchiem Kamche, Hervé Talé Kalachi, Franck Rivel Kamwa Djomou and Emmanuel Fouotsa* , Available via the link *https://arxiv.org/pdf/2106.08712.pdf*.

Solving the Rank Decoding Problem Over Finite Principal Ideal Rings, *Hervé Talé Kalachi and Hermann Tchatchiem Kamche*, Available via the link *https://arxiv.org/abs/2106.11569*.

Scientific activities

Talks in international conferences/workshops

- **On the Failure of the Smart Approach of the GPT Cryptosystem** : Talk given in the **AFRIMath** international seminar on number theory and information theory (June 25, 2021).
- **Introduction to code based cryptography :** African Mathematical School (**AMS**), University of Yaounde 1, Cameroon (16 - 28, July 2018)
- **On the Security of some Cryptosystems Based on Gabidulin Codes:** $6^{ème}$ International workshop on Cryptography, Algebra and Geometry (**CRAG-6**), University of Bamenda-Cameroon (15-17 June 2016).
- **Example of Structural Attack in Code Based Cryptography:** Atelier sur La Cryptographie, Codage et Applications, Brazzaville-Congo (14-18 Décembre 2015).
- **The Overbeck's Attack:** Workshop on Number Theory, Coding and Post-Quantum Cryptography, Cheikh Anta Diop University, Senegal (03-11 December 2015).

- **Square Codes attack on a modified Sidelnikov Cryptosystem**, *International Conference in Codes, Cryptology and Information Security, Rabat, Morocco* (26-28 May 2015).

Seminar Talks

- **On the Failure of the Smart Approach of the GPT Cryptosystem** : Talk given in the weekly seminar of the research team in Algebra and Logic of the University of Yaounde 1 (March 4, 2021).
- **Rank-Metric Cryptography** : Journée **ARCOCRYPT**, University of Rouen Normandie (November 7, 2019).
- **On the security of some variants of the GPT Cryptosystem** : Crypto seminar, ARIC team, ENS de Lyon (May 9, 2019).
- **Around the Faure-Loidreau cryptosystem** seminar of the research team in logic, algebra and geometry, University of Yaounde 1, Cameroon (21 June 2018).
- **On the Security of some Cryptosystems Based on Gabidulin Codes:** African Institute of Mathematical Sciences (AIMS-Limbé), Cameroon (03 April 2018).
- **Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes:** Talk given at "the cryptography seminar" of "université de Rennes 1", France (03 February 2017).
- **Security of Cryptographic Primitives Based on Coding Theory:** Presented at the seminar of the team "Combinatorics and Algorithms" of LITIS, university of Rouen-Normandie, France (2 December 2016).
- **Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes:** Presented at the Crypto seminar, GREYC, University of Caen, France (30 March 2016).
- **Sécurité des Protocoles cryptographiques fondés sur la théorie des Codes:** Doctoriales des Sciences Mathématiques 2015, Ecole Normale Supérieure de Yaoundé-Cameroun (Décembre 2015).
- **Square Code Attack on a Modified Sidelnikov:** Exposé à la journée des doctorants des équipes C & A et TIBS du LITIS, université de Rouen-Normandie, France (25 June 2015).
- **On the use of Random Redundancy In Cryptography:** École Jeunes Chercheurs en Mathématiques et Informatiques, Université d'Orleans, France. (30 Mars - 03 Avril 2015).
- **Cryptographie basée sur les Codes:** Doctoriales des Sciences Mathématiques 2014, Ecole Normale Supérieure de Yaoundé - Cameroun (Décembre 2014).
- **Cryptanalysis of a Modified Sidelnikov Cryptosystem:** CIMPA research school, AIMS-SENEGAL (June 16 -29 2014).
- **On the use of Random Redundancy In Codes based PKC:** 4^{th} Annual Workshop on Cryptography, Algebra and geometry (**CRAG-4**), University of Dschang-Cameroon (July 21-25 2014).
- **Version Dyadique du Cryptosystème de McElièce:** 2^{nd} Annual Workshop on Cryptography, Algebra and geometry (**CRAG-2**), University of Ngaoundere-Cameroon (December 04th 2012).