AUGUSTIN BARIANT

Doctorant en cryptographie symétrique à l'Inria de Paris.

@ augustin.bariant@inria.fr +33 6 88 26 26 71 0000-0003-0415-6785

ÉDUCATION

Inria de Paris

Thèse en cryptographie symétrique

Mars 2021 - Ajd Paris, France

- Sous la supervision de Gaëtan Leurent.
- Mission d'enseignement à Sorbonne Université (128h).
- Spécialisation dans l'utilisation du MILP pour la cryptanalyse et dans les attaques algébriques sur les algorithmes orientés arithmétisation.

KTH - Institut Royal de Technologie

Master en sécurité et confidentialité

Août 2019 - Février 2021 Stockholm, Suède

- Cours de cryptographie théorique et appliquée, de programmation et de sécurité de logiciels à grande échelle.

École Polytechnique

Diplôme d'ingénieur

Août 2016 - Août 2019 Palaiseau, France

- Cours d'algorithmie, de complexité, de théorie de l'information et d'informatique théorique.
- Spécialisation en cybersécurité en troisième année.

ÉXPERIENCE

Nanyang Technological University - Équipe SYLLAB

Stage de recherche

Février - Juin 2023 Singapour

- Design de primitives symmétriques à bas coût, sous la supervision de Thomas Peyrin.

Quarkslab

Stage en cybersécurité

Sep. - Fév. 2020/21 Paris, France

- Bitslicing de S-boîtes pour de la cryptographie en boîte blanche.

Inria de Paris - Équipe COSMIQ

Stage de recherche

Avril - Août 2019 Paris, France

- Cryptanalyse des forkciphers, sous la supervision de Gaëtan Leurent .

PUBLICATIONS

Truncated Boomerang Attacks and Application to AES-Based Ciphers

A. Bariant et G. Leurent,
***EUROCRYPT 2023*.**

- Nouvelles attaques boomerang sur 6 tours d'AES.
- Modélisation MILP sur Deoxys-BC.
- Amélioration des meilleures attaques sur Deoxys-BC, Kiasu-BC et TNT-AES.

Algebraic Attacks against Some Arithmetization-Oriented Primitives

A. Bariant, C. Bouvier, G. Leurent et L. Perrin,
IACR Transactions on Symmetric Cryptology 2022

- Implémentation d'attaques algébriques sur des versions réduites d'algorithmes orientés arithmétisation.
- Nouvelle attaque algébrique sur Ciminion.

Cryptanalysis of Forkciphers

A. Bariant, N. David et G. Leurent,
IACR Transactions on Symmetric Cryptology 2020

- Attaque sur la version complète de ForkAES.
- Amélioration des attaques sur ForkSkinny.

PRÉSENTATIONS

- **Algebraic Attacks against Some Arithmetization-Oriented Hash Functions**, Inria Junior Seminar, 2022.
- **Generating Bitslice Implementations of Arbitrary S-Boxes**, Journées C2, 2022.
- **Cryptanalysis of Forkciphers** (first part), Fast Software Encryption (FSE), 2020.

CAPTURE THE FLAG (CTF)

Pseudonyme: **graniter**
Some CTF Write-ups: Github.

- **Aviation ISAC Collegiate CTF 2020**: 2ème en équipe.
- **French CyberSecurity Challenge 2022**: 2ème senior (<25 ans) dans la catégorie cryptographie.
- **CryptoCTF 2022**: 10ème en équipe.
- **French CyberSecurity Challenge 2023**: 3ème dans la catégorie cryptographie.
- **Cryptohack**.