Bibliographie

Guides de bonnes pratiques

• *Guide des mécanismes cryptographiques*, guide technique
En savoir plus

• *Recommandations pour une configuration sécurisée d'un pare-feu Stormshield Network Security (SNS) en version 3.7.17,* guide technique
En savoir plus

• *Recommandations pour la mise en œuvre d'un site web : maîtriser les standards de sécurité côté navigateur,* guide technique
En savoir plus

• *Recommandations relatives à l'administration sécurisée des systèmes d'information,* guide technique
En savoir plus

• *Recommandations relatives à la sécurité des (systèmes d') objets connectés,* guide technique
En savoir plus

• *Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte,* guide technique
En savoir plus

• *Recommandations relatives à l'authentification multifacteur et aux mots de passe,* guide technique
En savoir plus

Partenariats

• ANSSI-DGE, *La cybersécurité pour les TPE/PME en 12 questions,* février 2021.
En savoir plus

• ANSSI-AFPA, *Les profils de la cybersécurité, enquête 2021,* octobre 2021.
En savoir plus

• ANSSI-CDSE, *Crise cyber, les clés d'une gestion opérationnelle et stratégique,* décembre 2021.
En savoir plus

• ANSSI-Cap'Com, *Anticiper sa communication de crise cyber,* décembre 2021.
En savoir plus

Publications scientifiques

Laboratoire architecture matérielle et logicielle (LAM)

From CVEs to proof: Make your USB device stack great again, Symposium sur la sécurité des technologies de l'information et des communications (SSTIC), **R. Benadjila**, C. Debergé, **P. Mouy, P. Thierry,** Rennes, France, juin 2021.

Laboratoire cryptologie (LCR)

"The Deoxys AEAD Family", *Journal of Cryptology* 34 (3): 31, **J. Jean**, I. Nikolic, T. Peyrin, **Y. Seurin**, 2021.

QCB: Efficient Quantum-secure Authenticated Encryption, Asiacrytpt 2021, R. Bhaumik, X. Bonnetain, A. Chailloux, G. Leurent, M. Naya-Plasencia, A. Schrottenloher, **Y. Seurin**, décembre 2021.

The Key-Dependent Message Security of Key-Alternating Feistel Ciphers, P. Farshim, **L. Khati**, **Y. Seurin**, D. Vergnaud, CT-RSA 2021, San Francisco, mai 2021.

MuSig2: Simple Two-Round Schnorr Multisignatures, J. Nick, T. Ruffing, **Y. Seurin**, Crypto 2021, août 2021.

Zalcon: An Alternative FPA-free NTRU Sampler for Falcon, P.A. Fouque, F. Gérard, **M. Rossi**, Y. Yu, Proceedings of Third NIST PQC Standardization Conference, juin 2021.

"On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry", S. Ballet, J. Pieltant, M. Rambaud, **H. Randriambololona**, R. Rolland, and J. Chaumine, *Russian Math. Surveys 76* (2021).

"Algebraic geometry codes and some applications", *A concise encyclopedia of coding theory,* A. Couvreur, **H. Randriambololona**, CRC Press, 2021.

Laboratoire exploration et recherche en détection (LED)

Dynamically Heterogeneous High-Order Interactions for Malicious Behavior Detection in Event Logs, S. Clémençon, **C. Larroche, J. Mazel**, mars 2021.

Anomalous Cluster Detection in Large Networks with Diffusion-Percolation Testing, S. Clémençon, **C. Larroche, J. Mazel**, Symposium on Intelligent Data Analysis, ESANN, octobre 2021.

Laboratoire sécurité réseau, protocole (LRP)

Inter-CESTI: Methodological and Technical Feedbacks on Hardware Devices Evaluations, **R. Benadjila**, SSTIC, Rennes, juin 2020.

U2F2: Prévenir la menace fantôme sur FIDO/U2F, **R. Benadjila, P. Thierry**, SSTIC, Rennes, France, juin 2021.

Laboratoire sécurité des composants (LSC)

Exploitation du graphe de dépendance d'AOSP à des fins de sécurité, A. Challande, R. David, **G. Renault**, SSTIC, Rennes, France, juin 2021.

"Electromagnetic fault injection against a complex CPU, toward new micro-architectural fault models", **G. Bouffard,** S. K. Bukasa, M. Escouteloup, R. Lashermes, **T. Trouchkine**, *Journal of Cryptographic Engineering* 11 (4), 2021.

EM Fault Model Characterization on SoCs: From Different Architectures to the Same Fault Model, **G. Bouffard**, J. Clédière, **T. Trouchkine**, FDTC 2021.

On using RSA/ECC Coprocessor for Ideal Lattice-Based Key Exchange, A. Greuet, S. Montoya, **G. Renault**, COSADE 2021.

Safe-Error Analysis of Post-Quantum Cryptography Mechanisms, L. Bettale, S. Montoya, **G. Renault**, FDTC 2021.

PhiAttack: Rewriting the Java Card Class Hierarchy, **G. Bouffard**, J. Dubreuil, CARDIS 2021.

Laboratoire de la sécurité des technologies sans-fil (LSF)

BlueMirror: Defeating Bluetooth Authentification Protocols, **T. Claverie, J. Lopes Esteves**, Hardware.io, La Haye, Pays-Bas, octobre 2021.

Interférences intentionnelles et attaques en faute : différentes similarités, **J. Lopes Esteves**, Journée thématique sur les attaques par injection de fautes (JAIF), Paris, France, septembre 2021.

BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols, **T. Claverie, J. Lopes Esteves,** 15th USENIX Workshop on Offensive Technologies (WOOT), mai 2021.

Analyse des propriétés de sécurité dans les implementations du Bluetooth Low Energy, **T. Claverie**, N. Docq, **J. Lopes Esteves**, SSTIC, Rennes, France, juin 2021.

Un pare-feu pour le FDMI, **J. Lopes Esteves**, P.M. Ricordel, SSTIC, Rennes, France, juin 2021.

Caractérisation d'antennes pour l'injection de fautes sur composants électroniques, **G. Bouffard, V. Houchouas, J. Lopes Esteves, T. Trouchkine,** Conférence plénière du GDR Ondes, Lille, France, novembre 2021.

"100 Years of URSI: The Past, Present and Future of Commission E", **J. Lopes Esteves,** *100 Years of the International Union of Radio Science,* URSI Press, 2021.

Laboratoire Sécurité du logiciel (LSL)

From CVEs to proof: Make your USB Device Stack great again, SSTIC, **R. Benadjila**, C. Debergé, **P. Mouy, P. Thierry**, Rennes, France, juin 2021.

Rapport sur les incidents et menaces

• *État de la menace rançongiciel à l'encontre des entreprises et des institutions*, 5 février 2021.
En savoir plus

• *Infrastructure d'attaque du groupe cybercriminel TA505*, 10 février 2021.
En savoir plus

• *The Malware-as-a-Service Emotet,* 12 février 2021.
En savoir plus

• *Campagne d'attaque du mode opératoire Sandworm ciblant des serveurs Centreon,* 15 février 2021. (EN)
En savoir plus

• *The Ryuk Ransomware*, 26 février 2021.
En savoir plus

• *The Egregor Ransomware,* 2 mars 2021.
En savoir plus

• *Identification d'un nouveau groupe cybercriminel : Lockean*, 3 novembre 2021. (EN)
En savoir plus

• *Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,* 6 décembre 2021. (EN)
En savoir plus

• *Campagne d'attaque du mode opératoire APT31 : description, contre-mesures et code,* 15 décembre 2021. (EN)
En savoir plus

Autre publication

• *Papiers numériques*, la revue annuelle de l'ANSSI, septembre 2021.
En savoir plus

Légende

(EN) : également disponible en anglais

Noms en gras : personnes rattachées à l'ANSSI au moment de la soumission ou de la publication de l'article scientifique.