Renaud DUBOIS

(+33) 6.XX.XX.XX.XX
Paris, France
prenom.nom@monentreprise.fr

Senior Cryptographer
Innovation Leader

github.com/rdubois-crypto
linkedin.com/in/renaud-dubois-63a62411

Enthusiast, Energic, I have been bringing Cryptography to real-world applications in the design of military-grade applications for sixteen years. I'm currently working on enhancing privacy by integrating Advanced Cryptographic features (ZKP, Anonymous Credentials) to SSI and blockchain frameworks.

Skills

Languages	Python, LaTeX, C, assembly (ARM, Intel), VHDL
Tools	Magma, Sagemath, Git, SVN
Quantitative Research	Advanced Cryptography (ZKP, Pairing-based), Mathematical Modeling, Machine Learning
Communication	French (native), English (fluent), Spanish (fluent), Portuguese (reading and writing)
Presentations	I love to be under the spotlights and pitch

Technical Experience

Senior Cryptographer / Ledger Innovation Team **04/2022 — Aujourd'hui**
Ledger *Paris, France*

- Veille technologique: ZKP, Decentralized Identity, Attribute-Based crypto
- Développement de PoC au sein de l'équipe innovation
- Soutien à l'intégration du framework Starknet

Expert Cryptologue / Laboratoire Chiffre **2019 —**
Thales *Gennevilliers, France*

Le périmètre de mon poste au sein du Laboratoire chiffre de THALES s'est enrichi graduellement avec deux promotions au sein de la filière expertise. La séparation des tâches est plus intriquée que comme restitutée par commodité ici.

- **Référent crypto sur plusieurs projets Défense.** Ce terme propre à THALES de "référent crypto" consiste en un mélange d'expertise technique (correspondant identifié vis-à-vis du client sur les aspects expertise crypto) et managementde projet transverse. Pour les projets type "réalisation de composants", cela signifie s'assurer de la conformité de la réalisation de services cryptographiques rendus par un composant conformément aux spécifications de besoins, en compatibilité avec des règles et normes (règles FIPS pour des composants exports, règles RGS issues de l'ANSSI pour les composants souverains). Management transverse de cryptologues juniors (respect des coûts délais et coaching). Pour les projets type "intégration de service crypto dans des systèmes satellitaires ou radio", assurer la coordination entre l'ingénierie système, les équipes de développement et les experts clients DGA/ESA
- **Rôle officieux de Responsable innovation du Laboratoire.**

Spécialiste Cryptologue / Laboratoire Chiffre **01/2011 — 01/2019**
Thales Communications *Gennevilliers, France*

- **Responsable chargé d'affaire et coordinateur technique du projet de recherche BEST (Broad-cast Encryption for Secure Telecommunications).** Encadrement industriel d'une thèse et de stagiaires. Le but de ce projet de 4 ans était de concevoir un protocole de broadcast encryption adapté à une faible bande passante pour beaucoup d'utilisateurs. Le projet réunissait un consortium de 2 industriels (THALES, NAGRA) une PME (CE) et des académiques (ENS Ulm, Paris VIII). Mon rôle en externe THALES était d'assurer la coordination technique du consortium sur tout le projet, transmettre les jalons en respectant les délais à l'ANR. En interne THALES j'assurais le suivi des coûts, encadrais en moyenne deux personnes sur le sujet et contribuais techniquement aux activités de R&D. J'ai contribué à des optimisations algorithmiques (Publication 4.) et la rédaction d'un document de référence (cf Publication 5.) dans une approche similaire aux documents normatifs type ANSIX9.62 (document de description des algorithmes qu'appellent les PKCS).
- **Tuteur, partenaire académique.** Encadrement industriel d'une thèse en MPC. Tuteur d'une douzaine de stages de fin de master. Je place la recherche académique en très haute estime et considère qu'une entreprise doit s'appuyer sur ses publications scientifiques plutôt que sa marque pour revendiquer une légitimité.

Ingénieur Cryptologue / Laboratoire Chiffre **03/2005 — 01/2011**
Thales Communications *Colombes, France*

- **Ingénierie Système.** Spécification de composants et systèmes développés dans le domaine civil, militaire et export. THALES réalise des systèmes radios et satellitaires. J'ai contribué à spécifier dans des trames (systèmes CONTACT, GALILEO) la réalisation de service cryptographiques (chiffrement, intégrité, authentification) tout en respectant des contraintes (bande passante, latence, menaces identi
fiées).

Renaud DUBOIS

(+33) 6.XX.XX.XX.XX
Paris, France
prenom.nom@monentreprise.fr

Senior Cryptographer
Innovation Leader

github.com/rdubois-crypto
linkedin.com/in/renaud-dubois-63a62411

- **Soutien à l'intégration d'algorithmes et de mécanismes cryptographiques.** Développement en C et assembleur d'algorithmes cryptographiques (chiffrerement, signature, authentification). J'ai eu l'opportunité de développer les algorithmes suivants pour le civil : RC4, AES,ECDSA, ECKCDSA, SHA, RSA, MIKKEY-SAKKE (protocole à base de cou- plage sur courbe elliptique), modes opératoires (ECB, OFB, CBC, GCM, CTR). Tous ces algorithmes trouvent leur équivalent (et plus) dans le monde Défense, j'en ai implémenté une vingtaine pour des modèles de référence comme pour du code opérationnel. Les implémentations doivent répondre à des contraintes d'espace et de débit.
- **Recherche.** Publications internationales et dépôts de brevets
- Enseignement. Enseignement d'un module de cryptographie à l'université Paris XIII en 2008 et 2009.

Stagiaire Cryptologue / Laboratoire Chiffre **04/2004 — 10/2004**
Thales Communications *Colombes, France*

- Étude des protocoles de broadcast encryption
- Analyse de la faisabilité : simulations des meilleurs protocoles en C++
- Dépôt d'un brevet à l'issue du stage

Education

Master 2 cryptographie et codes(Mention Assez Bien). *Université Bordeaux I & Science* 2003
Maîtrise d'Ingénierie Mathématiques (Mention Très Bien, major), *Université Paris VI (UPMC)* 1998-2003

Activities

Sport: Plongée (N3), Apnée (A2), Natation, Squash, Kitesurf
Personal Tastes: For obvious reasons, my favorite beers are DDH and i prefer RHUM over the standard model.
Loisirs: Voyages, Piano

Brevets (extract)

https://www.patentguru.com/inventor/dubois-renaud
The final name of the patent may differ from the original technical text once chewed by the IP teams. Last sentences give the real patent aim.

1. Renaud Dubois, David Lefranc, Matthieu Walle, MKD-Procédé de chiffrement hybride multi-contenus et multi-destinataires. Utilisation de tables de hachages et de Merkleisation pour optimiser des maj logicielles.
2. Renaud Dubois, Eric Garrido, Olivier Bernard, Alexandre Anzala, Anne-Rose Gratadour, Solution d'intégrité au niveau trame pour un système de diffusion possiblement sans voie de retour.
3. Renaud Dubois, Olivier Bernard EC4 - Procédé de génération des paramètres caractérisant un protocole cryptographique. 2016. (dépôt N1601067). Génération transparente de paramètres elliptiques.
4. Renaud Dubois, Aurélien Dupin, Julien Prat, Thomas Ricosset. METHOD FOR SECURING THE BALANCE OF AN ELECTRONIC ACCOUNT.https://www.patentguru.com/EP3843324A1. Décrit comment réaliser un bitcoin post quantique et une méthode de transition via commitment d'une chain à l'autre.
5. Renaud Dubois, Aurore Guillevic, Damien Vergnaud. Method for generating session key from secret key and public parameter by cryptography unit, involves deducing session key from value received from calculating unit, where value is value of binary function applied to data from tokens. 2018. Technique de délégation de calcul de couplage sur courbes.
6. METHOD OF IDENTIFYING A PROTOCOL GIVING RISE TO A DATA FLOW. Techniques de machine learning appliquées à la détection d'intrusion.

Publications

https://dblp.org/pid/26/211.html

1. Abdessamad Fazzat, Rida Khatoun, Houda Labiod, Renaud Dubois: A comparative performance study of cryptographic algorithms for connected vehicles. 2020.
2. Olivier Bernard, Renaud Dubois, Simon Masson: Efficient four-dimensional GLV curve with high security.
3. Renaud Dubois: Trapping ECC with Invalid Curve Bug Attacks.
4. Renaud Dubois, Margaux Dugardin, Aurore Guillevic: Golden Sequence for the PPSS Broadcast Encryption Scheme with an Asymmetric Pairing.

Renaud DUBOIS

(+33) 6.XX.XX.XX.XX
Paris, France
prenom.nom@monentreprise.fr

Senior Cryptographer
Innovation Leader

github.com/rdubois-crypto
linkedin.com/in/renaud-dubois-63a62411

5. Renaud Dubois, Aurore Guillevic, Marine Sengelin Le Breton: Improved Broadcast Encryption Scheme with Constant-Size Ciphertext. Pairing 2012.

6. Fabien Allard, Mathieu Morel, Renaud Dubois et Paul Gompel. CASTAFIOR : Tunneling activities detection using machine learning techniques. JTIT2010, Journal of Telecommunications and Information Technology.

7. Guillaume Fumaroli, Emmanuel Mayer, Renaud Dubois: First-Order Differential Power Analysis on the Duplication Method. INDOCRYPT 2007.