Cryptographe

Acigné · 3 à 5 ans d'expérience · Réf. 2611021026

Ma recherche

Contrat recherché : Tout contrat
Zone : Toute la France
Mobilité : sur toute la france
Rémunération : a étudier
Secteur : Batiment

Formations

12/2020 — Bac +5 — University of Rennes 1, UFR Mathematics
Master de cryptographie
06/2020 — Bac +5 — COSIC, KU Leuven
Thèse de Master sur la Threshold Implementation
12/2018 — Bac +3 — University of Rennes 1, UFR Mathematics
Bachelor of mathematics
12/2016 — Bac — CPGE Alain-René Lesage
MPSI-MP
12/2014 — Bac — Cesson-Sévigné
Baccalauréat S

Expériences professionnelles

10/2025 - 12/2025 — Software Development & Counsel

Quelques missions en CDD pour Dash Core Group, notamment pour déterminer les modernisations requises pour rendre le système post-quantique. En parallèle, je continue à me former en cybersécurité (implémentation de petit logiciel avec la librairie libcrypto d'OpenSSL et setup de PKI basique, apprentissage d'architecture d'ordinateur, veille cryptographique, lecture de manuels de HSMs tel que la gamme Luna de Thalès…). Développement de jeu sur mon temps libre en pseudo-python et .glsl.

01/2022 - 10/2024 — Head of research & Development

Promu à la tête de l'équipe de Recherche et Design, avec une équipe de 2 à 3 personnes. Lancer l'équipe de recherche : création des offres d'emplois, sélection des candidats. Diriger l'équipe : définir la roadmap, distribuer les tâches, créer un backlog de papiers académiques à étudier. Écriture d'articles pour nos utilisateurs sur les features techniques et sur la cryptographie sous-jacente. Point de communication durant une collaboration avec des chercheurs de l'université d'Arizona. Création d'une documentation interne très complète sur la Cryptographie à base de Réseaux dans le contexte du passage au post-quantique. Design des composantes clés de "Dash Platform" (système de preuve GroveDB, système de fees, vote anonyme, découplage par rapport à Dash Core…). Supervision de l'upgrade de la librairie "Core BLS". Design des "randomness beacons". Changement des règles de consensus. Enquête sur des solutions de ZKP et sur la dés-anonymisation de transactions Coinjoin.

01/2021 - 06/2021 — Researcher

Premier cryptographe In-house et designer pour Dash Core Group. Design de nouvelles features à implémenter, guidage des usages cryptographiques. Écriture des spécifications d'implémentation, guidage des développeurs. Articles de vulgarisation pour les utilisateurs. Point de contact pour un audit de sécurité mené par Least Authority. Aide à la documentation. Contributions : 2 documentations internes sur le clustering de transactions Coinjoin, contre-mesure "quorum rotation", revue de la cryptographie des DIPs, "Collaborative MasterNodes", guidage de l'équipe mobile app, détermination de changements pour les connections déterministes P2P intra-Quorum.

Langues

Français (maternelle), Anglais (bilingue), Néerlandais (commerciale)

Atouts

Cryptographie, C, C++, Assembleur, Python, LaTeX, Markdown, Java, Godot, Shader programming, SHA-256, MAC-SHA-256, X25519 implementation, AES (128/192/256) implementation, Kyber512 components, DSA (FIPS 186-3) implementation, Linear equivalence algorithm (Biryukov et al.), GLSL 2D lighting system, Documentation technique, Infrastructure à clés publiques (PKI), Parallel programming (OpenMP, CUDA), Architecture réseau, Lattice-based cryptography, Quantum cryptography, Error-correcting codes, Probability for information theory, Number algorithmic theory for cryptography, General algebra, Commutative algebra & algebraic geometry, Basic algorithmic skills, Video & image editing, Développement logiciel, Cuisine, Dessin, Management d'équipe, Recrutement, Roadmapping, Rédaction de contenu tech, Collaboration recherche, Développement de DApps, Supervision, Zero-Knowledge Proofs (ZKP), Rédaction de spécifications techniques, Vulgarisation technique, Audit de sécurité, Capacité à documenter

Loisirs

Apprentissage de langues, Nature, Video & image editing, Coder, Cuisine, Dessin, art

Fiche anonyme — l'identité et les coordonnées du candidat sont communiquées aux recruteurs qui en font la demande sur pmebtp.com.