

Haut Conseil de l'Évaluation de la Recherche et
de l'Enseignement Supérieur



DOCUMENT D'AUTOÉVALUATION

Équipe ALMASTY



Campagne d'évaluation 2023-2024 — Vague D

Table des matières

1	INFORMATIONS GÉNÉRALES SUR L'ÉQUIPE ALMASTY	3
1.1	Les thématiques scientifiques et leurs enjeux	3
	Avancées scientifiques majeures dans la période	4
	Animation scientifique de l'équipe	5
2	INTRODUCTION DU PORTFOLIO	6
3	AUTOÉVALUATION DU BILAN	7
3.1	Autoévaluation de l'équipe	7
	Domaine 2. Attractivité	7
	Domaine 3. Production scientifique	8
	Domaine 4. Inscription des activités de recherche dans la société	9
4	RÉFÉRENCES BIBLIOGRAPHIQUES SIGNIFICATIVES DE ALMASTY	10
A	ANNEXE — MEMBRES PERMANENTS AU 31/12/2022	12

1 INFORMATIONS GÉNÉRALES SUR L'ÉQUIPE ALMASTY

Nom de l'équipe : Algorithmes pour la sécurité des communications (ALMASTY)

Responsable de l'équipe : Damien Vergnaud

	2017	2018	2019	2020	2021	2022
PR	2	2	2	1	1	1
MCF HDR	0	0	0	0	0	1
MCF	0	0	0	0	1	0
DR	0	0	0	0	0	0
CR HDR	0	0	0	0	0	0
CR	0	0	0	0	0	0
Total permanents	2	2	2	1	2	2
Émérites	0	0	0	0	0	0
Doctorants	8	6	5	3	2	5
Ingénieurs CDD ou hors tutelles	0	0	0	0	0	0
Post-doc, ATER, etc.	1	2	1	1	0	0
Stagiaires	0	1	4	2	4	1
Total non permanents	9	9	10	6	6	6
Total avec émérites	11	11	12	7	8	8
Equivalent temps plein recherche	1.0	1.0	1.0	0.5	1.0	1.0

TABLE 1 – Personnels ALMASTY sur la période 2017-2022 (au 1er juillet de chaque année)

Note. L'équipe a recruté un CR CNRS au concours 2022 qui a pris ses fonctions en février 2023.

1.1 Les thématiques scientifiques et leurs enjeux

L'équipe est principalement orientée vers l'utilisation de techniques algorithmiques et mathématiques efficaces pour proposer et améliorer des cryptosystèmes et évaluer leurs niveaux de sécurité. Dans ce but, elle utilise de nombreux outils mathématiques et développe des algorithmes pour améliorer l'efficacité des calculs au-delà de ce qui est possible avec les méthodes de référence. Ses activités de recherche portent sur les sujets suivants : sécurité réductionniste, conception et analyse de protocoles et primitives, cryptographie (post-)quantique, (pseudo-)aléa en cryptographie, implantations efficaces de cryptosystèmes, attaques par canaux auxiliaires, cryptanalyse algorithmique, cryptanalyse par réseaux euclidiens, calcul haute performance, développement logiciel ...

Construction de protocoles et primitives cryptographiques – Sécurité réductionniste. Fournir des fondations solides pour l'étude des systèmes cryptographiques est une des directions majeures de recherche en cryptographie depuis 40 ans. La *sécurité réductionniste* est une approche formelle, empruntant ses méthodes à la théorie de la complexité, qui propose des preuves relatives qui réduisent la sécurité d'un système cryptographique à la difficulté supposée d'un problème algorithmique classique. Un axe des activités de recherche de l'équipe ALMASTY est consacré à la *construction de protocoles et primitives cryptographiques*.

Les travaux de l'équipe sont notamment consacrés aux systèmes de chiffrement asymétrique [Blazy et al., 2021], aux protocoles de signature numérique [Beunardeau et al., 2017], aux schémas symétriques de chiffrement et d'authentification de message [Khati and Vergnaud, 2018], aux systèmes de preuve à divulgation nulle de connaissance [Towa and Vergnaud, 2020] [Feneuil et al., 2022] et aux protocoles de calcul réparti distribué [Kushilevitz et al., 2021] [Chevalier et al., 2021]. Ces cryptosystèmes reposent soit sur la difficulté d'hypothèses de théorie des nombres bien étudiées (comme la factorisation des entiers ou le problème du logarithme discret) ou sur des techniques plus récentes dont l'objectif est notamment d'assurer une sécurité dite *post-quantique* (c'est-à-dire résistante aux attaques d'ordinateurs quantiques de grande envergure).

En plus de ces aspects, l'équipe a débuté en 2021, en collaboration avec l'équipe QI, une activité de recherche en cryptographie *quantique* (c'est-à-dire qui utilise les propriétés de la physique quantique pour assurer la sécurité de la communication). L'utilisation d'*aléa en cryptographie* est un élément fondamental qui est nécessaire non seulement pour générer des clés mais également dans l'exécution d'algorithmes cryptographiques. Dans ce domaine, un objectif de l'équipe ALMASTY est d'obtenir une meilleure compréhension de l'interaction entre l'aléa et la cryptographie [Kushilevitz et al., 2021].

Implantations efficaces et sécurisées de systèmes cryptographiques. L'équipe ALMASTY est également très investie dans la conception et l'analyse des implantations matérielles et logicielles de la cryptographie. Un premier aspect de ses activités de recherche est consacré à la conception d'*implantations efficaces* à travers différentes approches algorithmiques et arithmétiques. Pendant la période d'évaluation, des travaux ont été consacrés aux systèmes cryptographiques classiques [Courtois et al., 2019] et dits post-quantiques [Martins et al., 2017].

Les **attaques par canaux auxiliaires** sont les techniques de cryptanalyse qui exploitent des fuites d'information d'un algorithme de cryptographie lors de son implantation logicielle ou matérielle. Un autre axe des activités de recherche de l'équipe ALMASTY vise à proposer et étudier des implantations cryptographiques sécurisées pour des primitives cryptographiques dites post-quantiques [Bootle et al., 2018], [Barthe et al., 2018a], [Barthe et al., 2019a] ou pour des circuits booléens génériques (d'intérêt important notamment en cryptographie symétrique) [Belaïd et al., 2022], [Belaïd et al., 2021b], [Belaïd et al., 2021a].

Cryptanalyse. La **cryptanalyse algorithmique** est une branche de la cryptanalyse qui consiste à améliorer des algorithmes servant à résoudre des problèmes calculatoires (supposés) difficiles liés à la cryptographie et dont la difficulté sert à garantir la sécurité de certains cryptosystèmes. Il s'agit de mieux comprendre le coût de la résolution de ces problèmes algorithmiques, et donc le niveau de sécurité offert par les mécanismes cryptographiques liés. Dans l'équipe, des travaux de recherche ont été menés pour analyser la difficulté de problèmes comme la factorisation des grands entiers [Gélin et al., 2017], le calcul de logarithme discret [Joux, 2017], et la résolution de systèmes polynomiaux. [Joux and Vitse, 2017], [Bouillaguet et al., 2022b].

L'algorithmique des réseaux euclidiens a de nombreuses applications en cryptographie et en cryptanalyse. Une partie des activités de recherche de l'équipe ALMASTY se structure autour des techniques de **cryptanalyse fondée sur les réseaux euclidiens** pour analyser des cryptosystèmes à clé publique lorsque l'attaquant dispose d'informations sur les clés (obtenues par exemple par des attaques par canaux auxiliaires). L'équipe a ainsi attaqué des protocoles de délégation de calcul cryptographique [Bouillaguet et al., 2022c], [Chevalier et al., 2021] et des générateurs pseudo-aléatoires [Bouillaguet et al., 2020], [Martinez, 2022a]. Plus généralement, des travaux ont également été consacrés à l'étude du célèbre algorithme LLL [Espitau and Joux, 2020].

En cryptographie, l'identification des failles de sécurité dans les systèmes cryptographiques plutôt que dans les problèmes difficiles sous-jacents est également une voie de recherche importante. Au cours de la période d'évaluation l'équipe a également publié plusieurs contributions de ce type (p. ex. [Khati and Vergnaud, 2018]).

Production logicielle. ALMASTY se propose de produire des logiciels libres, de bonne qualité, implantant les algorithmes mentionnés ci-dessus, afin de les rendre accessibles à notre communauté de recherche. Elle propose de valider algorithmes et implantations en les exécutant sur des supercalculateurs, pour obtenir des records de calcul. Ceci permet à la communauté comme au grand public de suivre les progrès de la cryptanalyse.

Avancées scientifiques majeures dans la période

Résolution de systèmes polynomiaux booléens. L'équipe a acquis en 2017 la position de référence mondiale pour la résolution de systèmes polynomiaux booléens grâce à la conception d'un nouvel algorithme [Joux and Vitse, 2017]. Celui-ci est le premier qui a « battu la force brute » *en pratique*, et pas seulement sur le plan théorique. L'algorithme s'est avéré plus efficace sur une implantation réelle qu'une recherche exhaustive correctement implantée et a permis en 2017 la réalisation de records de calcul¹ qui n'ont pas été égalés depuis. L'équipe s'est employée à maintenir cette position en continuant à travailler sur l'aspect algorithmique [Bouillaguet et al., 2022b] du problème et en entreprenant la réalisation d'un logiciel libre encore plus performant.

Sécurité dans le modèle par sondage aléatoire. Pour contrer les attaques par canaux auxiliaires, le masquage est l'une des approches les plus utilisées en pratique : l'idée est de répartir l'information secrète entre plusieurs variables lors d'un calcul cryptographique sur un circuit (généralement booléen). Un attaquant doit alors collecter et agréger les informations de toutes ces variables pour récupérer les données sensibles. Dans le modèle par sondage aléatoire, un attaquant apprend la valeur portée sur chaque fil d'un circuit avec une probabilité $p > 0$ fixée et il faut montrer que les informations obtenues ne sont pas suffisantes pour reconstruire une information secrète (avec très forte probabilité). Dans la série de travaux [Belaïd et al., 2022], [Belaïd et al., 2021b], [Belaïd et al., 2021a], l'équipe a présenté des techniques qui améliorent la sécurité des constructions existantes dans le modèle de sondage aléatoire. Comme la vérification manuelle de la sécurité de ces constructions est fastidieuse, elle a présenté des techniques algorithmiques pour valider rapidement et efficacement la sécurité des petits circuits.

Arguments à divulgation nulle de connaissance. Dans [Towa and Vergnaud, 2020], ALMASTY a fourni le premier argument succinct à divulgation nulle de connaissance face à un vérifieur honnête pour la satisfiabilité des équations diophantiennes avec une complexité de communication logarithmique en la taille de l'équation polynomiale. Dans [Feneuil et al., 2022], l'équipe a proposé des systèmes d'argument de connaissance à divulgation nulle de connaissance pour le problème \mathcal{NP} -complet de la somme modulaire de sous-ensembles. Il s'agit d'un travail qui apporte une amélioration théorique importante (avec complexité en communication quadratique au lieu de cubique pour tous les travaux depuis 1986) et des applications pratiques inattendues.

1. <https://www.mqchallenge.org/>

Implantations sécurisées en cryptographie dite post-quantique. Le *National Institute of Standards and Technology* (NIST) a initié en 2016 un processus de normalisation de nouveaux algorithmes cryptographiques à clé publique dits post-quantique. Pour la première fois, l'accent était également mis sur la sécurité contre les attaques par canaux auxiliaires. En 2022, le NIST a sélectionné notamment trois cryptosystèmes reposant sur les réseaux euclidiens. Dès 2017, l'équipe ALMASTY a étudié la sécurité de constructions cryptographiques fondées sur les réseaux euclidiens face à des attaques par canaux auxiliaires [Espitau et al., 2017], [Bootle et al., 2018], [Barthe et al., 2018a], [Barthe et al., 2019a]. L'équipe a notamment présenté des techniques d'implémentation qui permettent de décrire une implémentation du protocole de signature BLISS avec une protection complète contre les attaques par mesure de temps, atteignant le même niveau d'efficacité que le code original non protégé, sans avoir recours à l'arithmétique en virgule flottante ou à des optimisations spécifiques.

Animation scientifique de l'équipe

L'équipe organise un séminaire régulier. Elle est également impliquée dans le *séminaire parisien de cryptographie* qui regroupe les équipes académiques parisiennes de recherche en cryptographie. Un membre de l'équipe était membre du comité scientifique du séminaire national "Codage et Cryptographie" pendant la période d'évaluations. Avec les journées d'étude des différents projets de recherche et les groupes de travail informels, les membres de l'équipe se réunissent au moins une fois par semaine pour des discussions scientifiques.

En 2020 et 2021, avec les difficultés dues à la crise sanitaire, l'équipe a mené ses travaux de recherche à distance en utilisant des outils de communication en ligne pour se coordonner et collaborer. Nous avons organisé des réunions régulières en ligne pour discuter de l'avancement des travaux en cours, partager des idées et discuter de nouvelles perspectives. Cette période "ALMASTY chez nous" nous a donné l'opportunité de donner et suivre des formations en ligne pour améliorer nos compétences dans des domaines spécifiques.

ALMASTY organise des activités sociales et des événements de renforcement d'équipe (*team building*) très fréquemment pour encourager la communication et renforcer les liens entre les membres de l'équipe. Ces activités permettent aux doctorants et post-doctorants de se sentir intégrés à l'équipe. Ces activités pour ALMASTY prennent notamment la forme de jeux, de repas d'équipe, de sorties de groupe ou d'une retraite résidentielle.

2 INTRODUCTION DU PORTFOLIO

- ▶ **Élément 1 (Publication)** : *Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection*. [Feneuil et al., 2022].

Dans ce travail, nous proposons des systèmes d'argument de connaissance à divulgation nulle de connaissance pour le problème \mathcal{NP} -complet de la somme modulaire de sous-ensembles. Il s'agit d'un travail dont l'inspiration est venue de nos activités en enseignement et qui apporte une amélioration théorique importante (avec complexité en communication quadratique au lieu de cubique pour tous les travaux depuis 1986) et des applications pratiques inattendues (notamment des signatures numériques dites post-quantiques dont la taille – environ 5 Ko pour un niveau de sécurité de 128 bits – est la plus courte parmi toutes les autres signatures basées sur le paradigme “MPC-in-the-Head”).

- ▶ **Élément 2 (Autre)** : Théorie, pratique, bidouille et supercalculateurs.

L'équipe ALMASTY possède depuis sa création une expérience dans la réalisation pratique d'attaques cryptographiques et/ou de “gros calculs” autour et alentour de la cryptographie. Nous cherchons de manière volontariste à ne pas faire que de la théorie, et de nous confronter au monde réel, aux vrais ordinateurs, etc. En particulier, plusieurs de nos travaux récents ont fait appels aux machines de l'IDRIS, le centre national de calcul du CNRS. Cet aspect significatif de notre approche de la recherche est notamment illustré par deux publications. Les résultats présentés dans ces travaux ont nécessité des ressources calculatoires importantes.

- ▶ **Élément 3 (Autre)** : Recherche en cryptologie et enseignement de la cryptologie.

L'équipe ALMASTY est une équipe universitaire composée d'enseignants-chercheurs. En principe, la moitié de notre activité concerne l'enseignement, en particulier de la cryptologie. L'équipe ALMASTY contribue de manière notoire à un renouvellement de l'enseignement de la cryptographie dans l'hexagone à travers la rédaction d'ouvrages pédagogiques (*Exercices et problèmes de cryptographie*, éd. Dunod), ainsi que par la création de plate-formes pédagogiques en-ligne innovantes pour la réalisation de travaux pratiques. Les étudiants sont confrontés à un *MMORPG* (Massively Multiplayer Online Role-Playing Game) truffé de tâches cryptographiques à accomplir.

3 AUTOÉVALUATION DU BILAN

3.1 Autoévaluation de l'équipe

Domaine 2. Attractivité

Référence 1. L'unité est attractive par son rayonnement scientifique et s'insère dans l'espace européen de la recherche.

Les membres de ALMASTY ont été invités pour des séjours dans des institutions académiques à l'étranger (p. ex. Lisbonne (PO), Singapore (SG), Wollongong (AU)) et pour des exposés pléniers dans des congrès internationaux (p. ex. STACS). Ils ont organisés plusieurs conférences nationales et internationales. Ils ont participé à plus de 25 comités de programme de conférences internationales (dont Eurocrypt 2018, Eurocrypt 2020 et Asiacrypt 2021) et au comité éditorial de deux revues (*Journal of Cryptographic Engineering* et *IEEE Trans. on Inf. Forensics and Security*). Un membre de l'équipe est responsable éditorial pour le thème « Cryptographie, sécurité des données » du projet d'encyclopédie SCIENCES de l'éditeur ISTE (2019-2024).

Les membres de l'équipe ont participé à différentes instances d'expertise scientifique (p. ex. le *College of Expert Reviewers* de l'*European Science Foundation*, le *comité d'évaluation scientifique 48* de l'ANR et des analogues de l'ANR aux Pays-Bas ou en République Tchèque). Ils ont également pris part à diverses instances de pilotage de la recherche (p. ex. le groupe de travail "Codage et Cryptographie" ou le bureau du GDR Sécurité Informatique). Les résultats scientifiques de l'équipe ont été reconnus par différents prix (p. ex. nomination à l'*Institut Universitaire de France* ou *Test of Time Award*).

Référence 2. L'unité est attractive par la qualité de sa politique d'accompagnement des personnels.

ALMASTY, malgré sa petite taille, compte des chercheurs aux sujets d'intérêt très variés. Cette diversité permet une perspective large sur les problématiques de recherche en cryptographie, favorisant l'identification d'approches innovantes pour résoudre des problèmes complexes et développer de nouvelles idées. Les doctorants et post-doctorants ont la possibilité de recevoir un financement pour leur recherche (généralement sur les fonds propres de l'équipe). Ils peuvent collaborer avec des chercheurs de renom, participer à des conférences internationales et effectuer des séjours de recherche à l'étranger pour développer leurs compétences et leur autonomie scientifique.

Référence 3. L'unité est attractive par la reconnaissance de ses succès à des appels à projets compétitifs.

Projets européens et internationaux. L'équipe a reçu une bourse **ERC Advanced** : l'**ERC ALMACRYPT** pour *Algorithmic and Mathematical Cryptology* (2016-2021) et a participé au projet européen **ICT HEAT** pour *Homomorphic Encryption Applications and Technology* porté par la KU Leuven (BE) (2015-2017). Elle a également porté le projet **PHC PESSOA PUNCTual**, pour *Post qUantum Cryptography TooLbox* avec l'Universidade de Lisboa (PO) (2018-2019). Elle a également coordonné le projet **PICS LEARAC**, pour *Leak Resistant Arithmetics for Cryptography* avec l'University of Wollongong (AU) (2016-2018).

Projets nationaux. L'équipe a porté quatre **projets ANR** pendant la période d'évaluation : l'**ANR ARRAND**, *ARithmétiques RANDomisées*, PRC (2016-2020), l'**ANR ALAMBIC**, *AppLicAtions of MalleaBility in Cryptography*, PRC (2016-2022), l'**ANR GORILLA**, *alGORithmic CryptanaLysis wIth actual impleMentAtions*, JCJC (2021 - présent) et l'**ANR SANGRIA**, *Secure distributed computAtioN - cryptoGRaphy, combinatorIcs and computer Algebra*, PRC (2021-2025). Elle a également participé à deux autres projets ANR portés par d'autres partenaires académiques : l'**ANR POSTCRYPTUM**, *Algebraic cryptanalysis for post-quantum cryptography* (Université de Picardie Jules Verne, 2021-2023) et l'**ANR KLEPTOMANIAC**, *Key Length Estimates - Practical and Theoretical Optimizations and Modern Approaches on NFS Instances for Accurate Costs* (LORIA, 2022-2026).

Référence 4. L'unité est attractive par la qualité de ses équipements et de ses compétences techniques.

Cette référence ne s'applique pas à l'équipe ALMASTY.

Domaine 3. Production scientifique

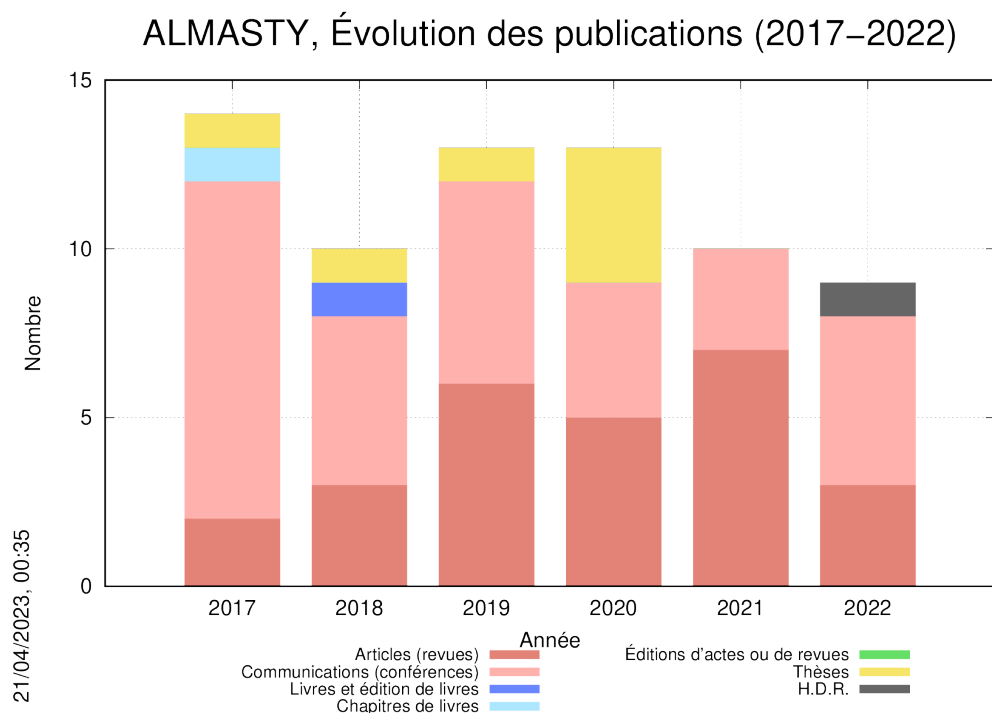


FIGURE 1 – Évolution des publications entre 2017 et 2022

	2017	2018	2019	2020	2021	2022
Articles (revues)	2.00	3.00	6.00	10.00	7.00	3.00
Communications (conférences)	10.00	5.00	6.00	8.00	3.00	5.00

TABLE 2 – Publications par ETPR par an entre 2017 et 2022

Référence 1. La production scientifique de l'unité satisfait à des critères de qualité.

L'HCÉRES, le CNRS et SU sont signataires de la déclaration de San-Francisco sur l'évaluation de la recherche qui rappelle que l'évaluation de la qualité d'une recherche scientifique doit être basée sur une évaluation rigoureuse de la pertinence et de la qualité des résultats, plutôt que sur des mesures quantitatives simplistes et arbitraires. ALMASTY soutient également fortement ce principe (et a notamment publié en collaboration avec Camille Noûs). L'équipe vise à publier ses travaux de recherche dans des conférences internationales choisies en raison de leur processus de sélection rigoureux et de leur réputation en cryptographie et en sécurité informatique :

- ▶ les conférences généralistes Asiacrypt, Crypto et Eurocrypt et les conférences spécialisées CHES, FSE, PKC et TCC organisées par l'IACR (*International Association for Cryptologic Research*) ;
- ▶ les conférences de sécurité informatique ACM CCS, ESORICS, IEEE S&P ...

En plus de ces conférences, la diversité des travaux menés dans l'équipe ALMASTY aboutit parfois à des publications dans des conférences généralistes reconnues (p. ex. ICALP, STACS ou SODA) ou des conférences d'autres domaines de plus petite audience, mais ayant une bonne réputation (p. ex. ARITH, ISSAC, ESOP ou SOSA).

En cryptographie, les publications dans les journaux sont le plus souvent des versions longues des articles publiés lors des conférences. L'équipe vise la publication de ses travaux dans des journaux ayant une bonne réputation en informatique théorique (p. ex. Algorithmica, IEEE Trans. {Inf. Theory, Computers}, SIAM J. on Discret. Math., ...).

L'équipe ALMASTY considère la production de logiciels comme un travail de recherche à part entière, même si ce point de vue est encore marginal dans la communauté de recherche à laquelle nous appartenons. Outre des articles scientifiques, l'équipe se fixe comme but de mettre à la disposition du public des logiciels performants et de bonne qualité pour réaliser certains types de calculs qui interviennent notamment en cryptanalyse.

Référence 2. La production scientifique de l'unité est proportionnée à son potentiel de recherche et correctement répartie entre ses personnels.

L'HCÉRES soutient le manifeste de Leiden qui indique que le nombre de publications n'est pas une mesure fiable de la contribution d'un chercheur dans son domaine. En effet, il ne prend pas en compte la qualité des travaux publiés, le type de publication, les co-auteurs et la diversité des domaines de recherche. Les membres de l'équipe ALMASTY sont tous actifs en recherche et disposent d'un budget suffisant pour participer aux événements scientifiques de leur choix (la pratique de l'équipe est de mutualiser les différents financements obtenus). Le travail de recherche est très exigeant et il est bien sûr possible qu'un chercheur diminue ses activités de recherche. L'équipe est attentive et en cas d'une diminution (non voulue) des activités de recherche de l'un de ses membres, nous pourrions identifier rapidement les causes et proposer des solutions pour relancer une dynamique de recherche.

Dans l'équipe, une place importante est accordée aux jeunes chercheurs pour assurer leur développement professionnel et leur succès dans le domaine de la recherche. Ils sont impliqués dans les projets de recherche de l'équipe et peuvent contribuer de manière significative aux travaux scientifiques. Un objectif de l'équipe est de développer leur autonomie et ils sont fortement encouragés à publier des travaux seuls ou avec d'autres co-auteurs que leur encadrant. En cas d'invitation à présenter les résultats de la recherche de l'équipe ALMASTY, une préférence est donnée aux jeunes chercheurs pour les aider à établir des relations et à développer leur réseau professionnel.

Référence 3. La production scientifique de l'unité respecte les principes de l'intégrité scientifique, de l'éthique et de la science ouverte. Elle est conforme aux directives applicables dans ce domaine.

Les publications scientifiques de l'équipe ALMASTY sont toutes disponibles en accès libre (*open access*) via notamment un lien direct fourni sur le site de l'équipe. Cette politique de publication présente plusieurs avantages pour la communauté scientifique et pour la société en général. L'approche de l'équipe est de refuser les publications avec APC (*Article Processing Charges*) en raison de leurs coûts élevés, des problèmes éthiques liés aux revues prédatrices et de l'existence de modèles alternatifs. Des revues *Diamond Open Access* ont été créées par des collègues, à l'instar de *Mathematical Cryptology*. Elles sont jeunes, parfois mal référencées et "peu rentables" en termes d'indicateurs bibliométriques. Nous choisissons, volontairement, d'y publier parfois nos travaux dans le but exprès de les faire vivre et de leur permettre de prendre de l'importance. Dans la même perspective, plusieurs publications de l'équipe remercient Alexandra Assanovna Elbakyan pour le rôle positif qu'elle joue pour le monde de la recherche. Enfin, sur le terrain des logiciels produits par l'équipe, leur code source est publié, ou bien mis dans le domaine public ou bien attaché à une licence "*open source*" telle que la GPL.

Domaine 4. Inscription des activités de recherche dans la société

Référence 1. L'unité se distingue par la qualité et la quantité de ses interactions avec le monde non-académique.

ALMASTY entretient des collaborations avec des entreprises par le co-encadrement de thèses CIFRE avec les sociétés Quarkslab, CryptoExperts et Thales. En plus de ces co-encadrements, l'équipe a également des collaborations informelles avec plusieurs entreprises qui ont donné lieu à des publications communes (p. ex. IBM Research – Zurich (CH), CryptoExperts – Paris (FR), NTT Corporation – Tokyo (JP), PQShield – Oxford (UK)). ALMASTY a obtenu l'attribution d'une *Research Grant* de la société Oracle de \$80k en 2022. L'équipe a également des collaborations avec plusieurs partenaires institutionnels : l'ANSSI (encadrement de thèse et publications communes), le CEA (co-encadrement de thèse) et la DGA (publications communes).

Référence 2. L'unité développe des produits à destination du monde culturel, économique et social.

Cette référence ne s'applique pas à l'équipe ALMASTY.

Référence 3. L'unité partage ses connaissances avec le grand public et intervient dans des débats de société.

L'équipe a une implication importante en vulgarisation et en médiation scientifique. Elle a notamment accueilli au laboratoire des collégiens lauréats du *concours Alkindi*. Un membre de l'équipe a rédigé un article de vulgarisation pour *La Recherche* dans le cadre d'un nombre spécial sur "Le hasard". ALMASTY a proposé lors de la *Fête de la science* en 2018 et 2019 des activités autour de la cryptographie moderne ; en 2021 et 2022, l'équipe a utilisé l'outil pédagogique "Turing Tumble®" pour présenter sous forme ludique les concepts de base de l'informatique.

4 RÉFÉRENCES BIBLIOGRAPHIQUES SIGNIFICATIVES DE ALMASTY

- [Barthe et al., 2018a] Barthe, G., Belaïd, S., Espitau, T., Fouque, P., Grégoire, B., Rossi, M., and Tibouchi, M. (2018a). Masking the GLP lattice-based signature scheme at any order. In Nielsen, J. B. and Rijmen, V., editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 354–384. Springer.
- [Barthe et al., 2019a] Barthe, G., Belaïd, S., Espitau, T., Fouque, P., Rossi, M., and Tibouchi, M. (2019a). GALACTICS : gaussian sampling for lattice-based constant- time implementation of cryptographic signatures, revisited. In Cavallaro, L., Kinder, J., Wang, X., and Katz, J., editors, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, pages 2147–2164. ACM.
- [Belaïd et al., 2021a] Belaïd, S., Rivain, M., and Taleb, A. R. (2021a). On the power of expansion : More efficient constructions in the random probing model. In Canteaut, A. and Standaert, F., editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 313–343. Springer.
- [Belaïd et al., 2022] Belaïd, S., Rivain, M., and Taleb, A. R. (2022). Ironmask : Versatile verification of masking security. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, 22-26 May 2022*, volume to appear. IEEE.
- [Belaïd et al., 2021b] Belaïd, S., Rivain, M., Taleb, A. R., and Vergnaud, D. (2021b). Dynamic random probing expansion with quasi linear asymptotic complexity. In Tibouchi, M. and Wang, H., editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part II*, volume 13091 of *Lecture Notes in Computer Science*, pages 157–188. Springer.
- [Beunardeau et al., 2017] Beunardeau, M., Connolly, A., Ferradi, H., Géraud, R., Naccache, D., and Vergnaud, D. (2017). Reusing nonces in Schnorr signatures - (and keeping it secure...). In Foley, S. N., Gollmann, D., and Snekenes, E., editors, *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I*, volume 10492 of *Lecture Notes in Computer Science*, pages 224–241. Springer.
- [Blazy et al., 2021] Blazy, O., Brouilhet, L., Chevalier, C., Towa, P., Tucker, I., and Vergnaud, D. (2021). Hardware security without secure hardware : How to decrypt with a password and a server. *Theor. Comput. Sci.*, 895 :178–211.
- [Bootle et al., 2018] Bootle, J., Delaplace, C., Espitau, T., Fouque, P., and Tibouchi, M. (2018). LWE without modular reduction and improved side-channel attacks against BLISS. In Peyrin, T. and Galbraith, S. D., editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 494–524. Springer.
- [Bouillaguet et al., 2022b] Bouillaguet, C., Delaplace, C., and Trimoska, M. (2022b). A simple deterministic algorithm for systems of quadratic polynomials over \mathbb{F}_2 . In Bringmann, K. and Chan, T., editors, *5th Symposium on Simplicity in Algorithms, SOSA@SODA 2022, Virtual Conference, January 10-11, 2022*, pages 285–296. SIAM.
- [Bouillaguet et al., 2020] Bouillaguet, C., Martinez, F., and Sauvage, J. (2020). Practical seed-recovery for the PCG pseudo-random number generator. *IACR Trans. Symmetric Cryptol.*, 2020(3) :175–196.
- [Bouillaguet et al., 2022c] Bouillaguet, C., Martinez, F., and Vergnaud, D. (2022c). Cryptanalysis of modular exponentiation outsourcing protocols. *Comput. J.*, 65(9) :2299–2314.
- [Chevalier et al., 2021] Chevalier, C., Laguillaumie, F., and Vergnaud, D. (2021). Privately outsourcing exponentiation to a single server : Cryptanalysis and optimal constructions. *Algorithmica*, 83(1) :72–115.
- [Courtois et al., 2019] Courtois, J., Abbas-Turki, L. A., and Bajard, J. (2019). Resilience of randomized RNS arithmetic with respect to side-channel leaks of cryptographic computation. *IEEE Trans. Computers*, 68(12) :1720–1730.
- [Espitau et al., 2017] Espitau, T., Fouque, P., Gérard, B., and Tibouchi, M. (2017). Side-channel attacks on BLISS lattice-based signatures : Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In Thuraishingham, B. M., Evans, D., Malkin, T., and Xu, D., editors, *Proceedings of the 2017 ACM*

- SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1857–1874. ACM.
- [Espitau and Joux, 2020] Espitau, T. and Joux, A. (2020). Certified lattice reduction. *Adv. in Math. of Comm.*, 14(1) :137–159.
- [Feneuil et al., 2022] Feneuil, T., Maire, J., Rivain, M., and Vergnaud, D. (2022). Zero-knowledge protocols for the subset sum problem from MPC-in-the-head with rejection. In Agrawal, S. and Lin, D., editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings*, volume to appear of *Lecture Notes in Computer Science*. Springer.
- [Gélin et al., 2017] Gélin, A., Kleinjung, T., and Lenstra, A. K. (2017). Parametrizations for families of ECM-friendly curves. In Burr, M. A., Yap, C. K., and Din, M. S. E., editors, *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017*, pages 165–171. ACM.
- [Joux, 2017] Joux, A. (2017). Discrete logarithms in small characteristic finite fields : a survey of recent advances (invited talk). In Vollmer, H. and Vallée, B., editors, *34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany*, volume 66 of *LIPIcs*, pages 3 :1–3 :1. Schloss Dagstuhl - Leibniz-Zentrum für Informatik.
- [Joux and Vitse, 2017] Joux, A. and Vitse, V. (2017). A crossbred algorithm for solving boolean polynomial systems. In Kaczorowski, J., Pieprzyk, J., and Pomykala, J., editors, *Number-Theoretic Methods in Cryptology - First International Conference, NuTMiC 2017, Warsaw, Poland, September 11-13, 2017, Revised Selected Papers*, volume 10737 of *Lecture Notes in Computer Science*, pages 3–21. Springer.
- [Khatai and Vergnaud, 2018] Khatai, L. and Vergnaud, D. (2018). Analysis and improvement of an authentication scheme in incremental cryptography. In Cid, C. and Jr., M. J. J., editors, *Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers*, volume 11349 of *Lecture Notes in Computer Science*, pages 50–70. Springer.
- [Kushilevitz et al., 2021] Kushilevitz, E., Ostrovsky, R., Prouff, E., Rosén, A., Thillard, A., and Vergnaud, D. (2021). Lower and upper bounds on the randomness complexity of private computations of AND. *SIAM J. Discret. Math.*, 35(1) :465–484.
- [Martinez, 2022a] Martinez, F. (2022a). Attacks on pseudo random number generators hiding a linear structure. In Galbraith, S. D., editor, *Topics in Cryptology - CT-RSA 2022 - Cryptographers' Track at the RSA Conference 2022, Virtual Event, March 1-2, 2022, Proceedings*, volume 13161 of *Lecture Notes in Computer Science*, pages 145–168. Springer.
- [Martins et al., 2017] Martins, P., Eynard, J., Bajard, J., and Sousa, L. (2017). Arithmetical improvement of the round-off for cryptosystems in high-dimensional lattices. *IEEE Trans. Computers*, 66(12) :2005–2018.
- [Towa and Vergnaud, 2020] Towa, P. and Vergnaud, D. (2020). Succinct diophantine-satisfiability arguments. In Moriai, S. and Wang, H., editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part III*, volume 12493 of *Lecture Notes in Computer Science*, pages 774–804. Springer.

A ANNEXE — MEMBRES PERMANENTS AU 31/12/2022

La table ci dessous liste les membres permanents de l'équipe ALMASTY.

NOM	Prénom	Corps	Employeur
BOUILLAGUET	Charles	MCF (HDR)	Sorbonne Université
VERGNAUD	Damien	PR	Sorbonne Université