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

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. Un 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 calcul [1] 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 fournit 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 organiser 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

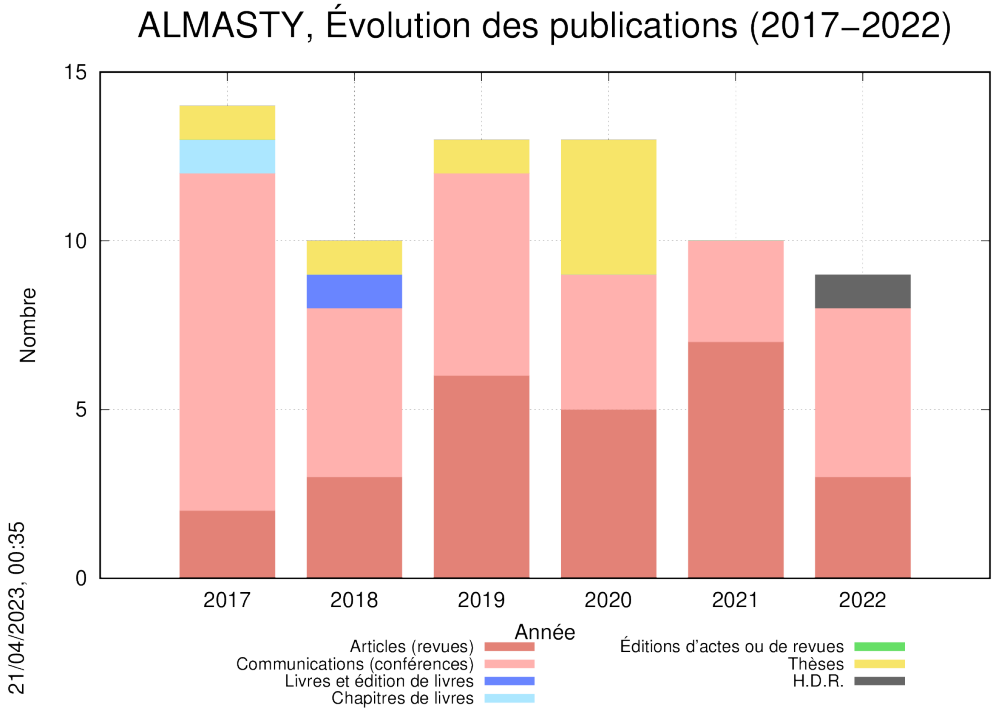


FIGURE 1 – Évolution des publications entre 2017 et 2022

	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 publié des travaux seul 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 référencés 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'un *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 Snekkenes, 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 Thuraisingham, 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.

[Khati and Vergnaud, 2018] Khati, 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

ÉLÉMENT DE PORTFOLIO 01

Publication

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection.

URL de l'élément : `https://eprint.iacr.org/2022/223`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

En 2021, l'équipe ALMASTY a fortement remanié le cours *Cryptologie avancée et appliquée* en deuxième année du parcours **Sécurité, Fiabilité et Performances** (SFPN) du master informatique de Sorbonne Université en intégrant notamment la cryptographie fondée sur les réseaux euclidiens et la géométrie des nombres et les systèmes de preuves à divulgation nulle de connaissance.

Suite à des discussions au sein de l'équipe pédagogique, nous nous sommes intéressés au problème de la *somme (modulaire) de sous-ensembles* qui consiste à trouver, étant donné des entiers $w_1, \ldots, w_n$, t et q, un sous-ensemble des w_i dont la somme est égale à t modulo q, c'est-à-dire à trouver des bits $x_1, \ldots, x_n \in \{0, 1\}$ tels que

$$\sum_{i=1}^{n} x_i w_i = t \bmod q.$$

Ce problème $\mathcal{NP}$-complet (dans sa variante de décision naturelle) est considéré en cryptographie depuis les années 1980 comme une alternative intéressante aux hypothèses algorithmiques fondées sur la théorie des nombres. Il est en particulier censé fournir une sécurité dite *post-quantique*.

Nous nous sommes posés la question de l'existence d'un système à divulgation nulle de connaissance pour ce problème. Nous avons trouvé que plusieurs protocoles avaient été proposés (notamment dans [1, 2, 4, 6]) mais D. Vergnaud a eu une idée pour améliorer leur efficacité en utilisant une variante de la technique *MPC-in-the-head* qu'il venait justement d'étudier pour préparer l'un des cours. Il a présenté cette idée à une audience large lors de la réunion de lancement du projet ANR SANGRIA dont il est le coordinateur. Th. Feneuil (doctorant sous la direction de J.-C. Bajard, A. Joux et M. Rivain, au sein de la société CryptoExperts) était présent à cette réunion et a proposé des améliorations. Nous avons entamé une collaboration avec J. Maire (doctorant qui venait de commencer sa thèse au sein de l'équipe ALMASTY) et M. Rivain qui a abouti en la publication de ce travail à la conférence Asiacrypt 2022 [3].

La genèse de cet article illustre assez bien le fonctionnement de l'équipe ALMASTY avec une interaction importante entre l'enseignement et la recherche, des discussions ouvertes entre les membres (anciens et présents) de l'équipe et des interactions fortes avec le monde académique et le monde industriel.

3 PRÉSENTATION DE CET ÉLÉMENT

Dans ce travail, nous proposons des systèmes d'argument de connaissance à divulgation nulle de connaissance pour le problème de la somme modulaire de sous-ensembles. Les approches combinatoires précédentes, notamment celle due à Shamir, donnaient des arguments avec une complexité de communication cubique (dans le paramètre de sécurité). Des méthodes plus récentes, basées sur la technique *MPC-in-the-head*, produisent également des arguments avec une complexité de communication cubique (et seulement pour des modules q premiers).

Nous améliorons cette approche en utilisant un partage de secret sur de petits entiers (plutôt que modulo q) pour réduire la taille des arguments et supprimer la restriction du module premier. Comme ce partage peut révéler des informations sur le sous-ensemble secret, nous introduisons l'idée de rejet dans le paradigme *MPC-in-the-head*. Un soin particulier doit être apporté pour équilibrer les propriétés de complétude et de solidité et préserver la propriété de divulgation nulle de connaissance. Nous combinons cette idée avec deux techniques pour prouver

que le vecteur secret $(x_1, \ldots, x_n)$ (qui sélectionne le sous-ensemble) est bien constitué de coordonnées binaires. Nos nouvelles techniques ont l'avantage significatif d'aboutir à des arguments de taille indépendante du module q.

Nos nouveaux protocoles pour le problème de la somme modulaire de sous-ensembles réalisent une amélioration asymptotique en produisant des arguments de taille quadratique. Cette amélioration est également pratique : pour un module q de 256 bits la meilleure variante de nos protocoles produit des arguments de 13 Ko, alors que les propositions précédentes donnaient des arguments de 1180 Ko, pour le meilleur protocole général, et de 122 Ko, pour le meilleur protocole limité aux modules premiers. Nos techniques peuvent également être appliquées à des variantes vectorielles du problème de la somme modulaire de sous-ensembles et, en particulier, au problème des solutions entières courtes inhomogènes (*Inhomogeneous Small Integer Solution, ISIS*), pour lequel elles offrent une alternative efficace aux meilleurs protocoles connus lorsque l'anneau sous-jacent n'est pas petit et compatible avec les transformées en nombres entiers (*Number Theoretic Transform, NTT*). Nous montrons également comment adapter notre protocole pour construire des arguments efficaces de connaissance à divulgation nulle de connaissance d'un texte en clair ou de la clé dans le contexte du chiffrement complètement homomorphe. Lorsqu'ils sont appliqués au schéma TFHE, les arguments obtenus sont plus de 20 fois plus petits que ceux obtenus avec les protocoles précédents. Enfin, nous utilisons notre technique pour construire un schéma de signature numérique efficace basé sur une fonction pseudo-aléatoire due à Boneh-Halevi-Howgrave-Graham. La taille des signatures obtenues (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*. Ce protocole a déjà donné lieu à des travaux ultérieurs (notamment un protocole de *mise en gage* disposant d'arguments à divulgation nulle de connaissance [5]).

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Carsten Baum and Ariel Nof. Concretely-efficient zero-knowledge arguments for arithmetic circuits and their application to lattice-based cryptography. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part I*, volume 12110 of *Lecture Notes in Computer Science*, pages 495–526. Springer, 2020.

[2] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Efficient identification schemes using two prover interactive proofs. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 498–506. Springer, 1989.

[3] Thibauld Feneuil, Jules Maire, Matthieu Rivain, and Damien Vergnaud. Zero-knowledge protocols for the subset sum problem from MPC-in-the-head with rejection. In Shweta Agrawal and Dongdai Lin, 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 13792 of *Lecture Notes in Computer Science*, page 371–402. Springer, 2022.

[4] San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings*, volume 7778 of *Lecture Notes in Computer Science*, pages 107–124. Springer, 2013.

[5] Jules Maire and Damien Vergnaud. Commitments with efficient zero-knowledge arguments from subset sum problems. In Mauro Conti and Gene Tsudik, editors, *Computer Security - ESORICS 2023 - 28th European Symposium on Research in Computer Security, The Hague, Netherlands, September 25-29, 2023, Proceedings*, volume to appear of *Lecture Notes in Computer Science*. Springer, 2023.

[6] Adi Shamir. A zero-knowledge proof for knapsacks. presented at a workshop on Probabilistic Algorithms, Marseille, March 1986.

ÉLÉMENT DE PORTFOLIO 02

Autre

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Théorie, pratique, bidouille et supercalculateurs

URL de l'élément :

- `https://doi.org/10.1016/j.parco.2021.102804` ou `https://hal.inria.fr/hal-02306904`
- `https://doi.org/10.13154/tosc.v2020.i3.175-196` ou `https://hal.archives-ouvertes.fr/hal-02700791`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Une partie essentielle des travaux menés au sein de l'équipe ALMASTY concerne la *cryptanalyse*, c'est-à-dire la conception d'attaques qui visent à briser les propriétés de sécurités censées être offertes par les mécanismes cryptographiques. Dans la littérature publiée, beaucoup d'attaques sont "théoriques" seulement : un algorithme est décrit, sa complexité est déterminée dans un modèle calculatoire abstrait, puis il en est conclu qu'il "casse" un mécanisme cryptographique car il s'exécute "trop vite".

La communauté cryptographique est très portée sur les mathématiques et est friande de "théorie". *A contrario*, nous faisons le choix volontariste, militant pourrait-on dire, de ne pas nous confiner à la théorie pure et de chercher à mettre en pratique les algorithmes que nous inventons, à réaliser concrètement les attaques que nous concevons. Nous considérons que cela apporte un autre point de vue, très différent (ce qui est théoriquement supérieur est bien souvent pratiquement inférieur et vice-versa). Cet élément du portfolio présente notre trajectoire intellectuelle à ce propos.

Nous estimons que cette confrontation de point de vue est fructueuse. C'est d'ailleurs l'un des axes essentiels du projet ANR JCJC "GORILLA" porté par l'équipe. Nous nous donnons donc pour objectif d'une part de produire des implantations logicielles de bonne qualité des attaques cryptographiques, et d'autre part de démontrer leur faisabilité en tentant de les exécuter à grande échelle.

L'équipe ALMASTY, depuis sa création, a possédé une expertise significative dans le calcul parallèle et la réalisation de records de calculs.

3 PRÉSENTATION DE CET ÉLÉMENT

3.1 *Computational records with aging hardware : Controlling half the output of SHA-256*

Cette publication est l'aboutissement d'un travail commencé à l'été 2016, qui a donc mis 5 ans à aboutir (c'est de la *slow science*). Tout cela a commencé par une réflexion sur les algorithmes dédiés au problème $3\mathrm{XOR}$: étant donné trois fonctions aléatoires $f, g, h : \{0,1\}^* \to \{0,1\}^n$, trouver un triplet (x, y, z) tel que $f(x) \oplus g(y) \oplus h(z) = 0$ — ici $\oplus$ désigne le XOR des chaînes de n bits. Plusieurs attaques cryptographiques doivent résoudre de tels problèmes [2, 3]. Nous nous sommes notamment posés la question : "*si quelqu'un voulait résoudre une instance du problème en pratique, comment devrait-il faire ?*". Essayer d'y répondre nous a ouvert les yeux sur le fait que toutes les "améliorations" théoriques, qui visent à réduire le nombre total d'opérations, rendaient les algorithmes de moins en moins utilisables en pratique : cela ignore les contraintes d'espace, de parallélisme et de complexité de communication. Pour avancer, nous nous sommes donc donné un défi : calculer un triplet 3XOR sur la fonction de hachage cryptographique $\mathrm{SHA256}$ tronquée à n bits, pour la plus grande valeur possible de n.

Il nous est vite apparu clairement que les "meilleurs" algorithmes plafonnaient à $n \approx 80$ pour cause de manque de mémoire. En 2017, nous parvenions à $n = 96$ avec une méthode naïve sur un petit cluster. En 2018, nous avons publié l'article [1] qui décrivait un nouvel algorithme concrètement plus efficace que l'état de l'art. Pour disposer de plus de puissance de calcul, nous avons acheté sur `leboncoin.fr` une machine à miner des bitcoins de seconde main. Quelques semaines de *hacking* plus tard, nous l'avions convertie en accélérateur de calcul pour la cryptanalyse. Nous l'avons fait fonctionner 8 mois sans interruption. Après cela, en 2019, nous avons soumis

FIGURE 1 – Une machine à miner des bitcoins reprogrammée pour la cryptanalyse, en pleine action (gauche). Les supercalculateurs `turing` (milieu) et `jean-zay` (droite) sur lesquels nous avons mené nos travaux.

un dossier au GENCI pour réaliser 10 millions d'heures de calcul sur la machine `turing` (une IBM Bluegene/Q) de l'IDRIS. Nous avons exécuté une version ultra-optimisée de notre algorithme sur 65536 cœurs simultanément pendant 80 heures pour parvenir à calculer un triplet 3XOR sur $n = 128$ bits. Nous avons donc réussi à "contrôler" la moitié de la sortie de $\mathrm{SHA256}$, ce que personne d'autre n'a fait. En termes de nombre d'opérations, il s'agit du plus "gros" calcul de nature cryptographique jamais réalisé. Il s'agit d'ailleurs du seul et unique résultat de cryptanalyse accéléré par des machines à miner des bitcoins (cf. figure 1).

3.2 *Predicting the PCG Pseudo-Random Number Generator In Practice*

Cette publication décrit une "attaque" pratique sur le générateur pseudo-aléatoire PCG, qui est utilisé par défaut dans la populaire bibliothèque de calcul scientifique `numpy`. L'article décrit une procédure qui permet de calculer la suite du flux pseudo-aléatoire (qui est censé être imprévisible) à partir d'un préfixe de quelques kilo-octets.

Ce travail a été motivé par le site web qui fait la promotion de l'algorithme PCG (cf. fig. 2). Il nous semblait évident que l'algorithme ne peut pas être cryptographiquement sûr, mais l'auteur y affirme de manière ambigüe qu'il pourrait pourtant offrir une certaine sécurité. Pour l'édification de la communauté, nous avons donc entrepris de réfuter cette affirmation.

L'algorithme PCG utilise une combinaison de techniques classiques dans les générateurs pseudo-aléatoires (générateurs linéaires congruentiels tronqués) mais emprunte aussi à la cryptographie symétrique (*data-dependant rotation* comme dans RC5). En venir à bout nécessite tout l'arsenal des techniques de cryptanalyse (réseaux euclidiens, etc.). Après avoir conçu l'attaque, nous avons implanté l'attaque dans un programme C ultra-optimisé. Nous avons demandé à l'auteur de PCG de nous fournir quelques kilo-octets de flux pseudo-aléatoire. Nous avons exécuté notre programme sur 20480 coeurs de `jean-zay` pendant une petite demi-heure et nous lui avons renvoyé la graine utilisée. Ceci a fourni la démonstration irréfutable que l'algorithme est faible.

À notre grande surprise, cette publication a fait l'objet d'une discussion sur le réseau social Reddit [1]. Le code de l'attaque étant fourni, certains se sont amusés à la reproduire. Sur HAL, l'article a par conséquent été téléchargé 3600 fois, alors que nos autres publications plafonnent à quelques centaines de téléchargement.

Bref : justiciers du cyberespace, *buzz* sur les réseaux sociaux, et supercalculateurs pour mettre tout le monde d'accord, voilà qui résume bien l'équipe ALMASTY.

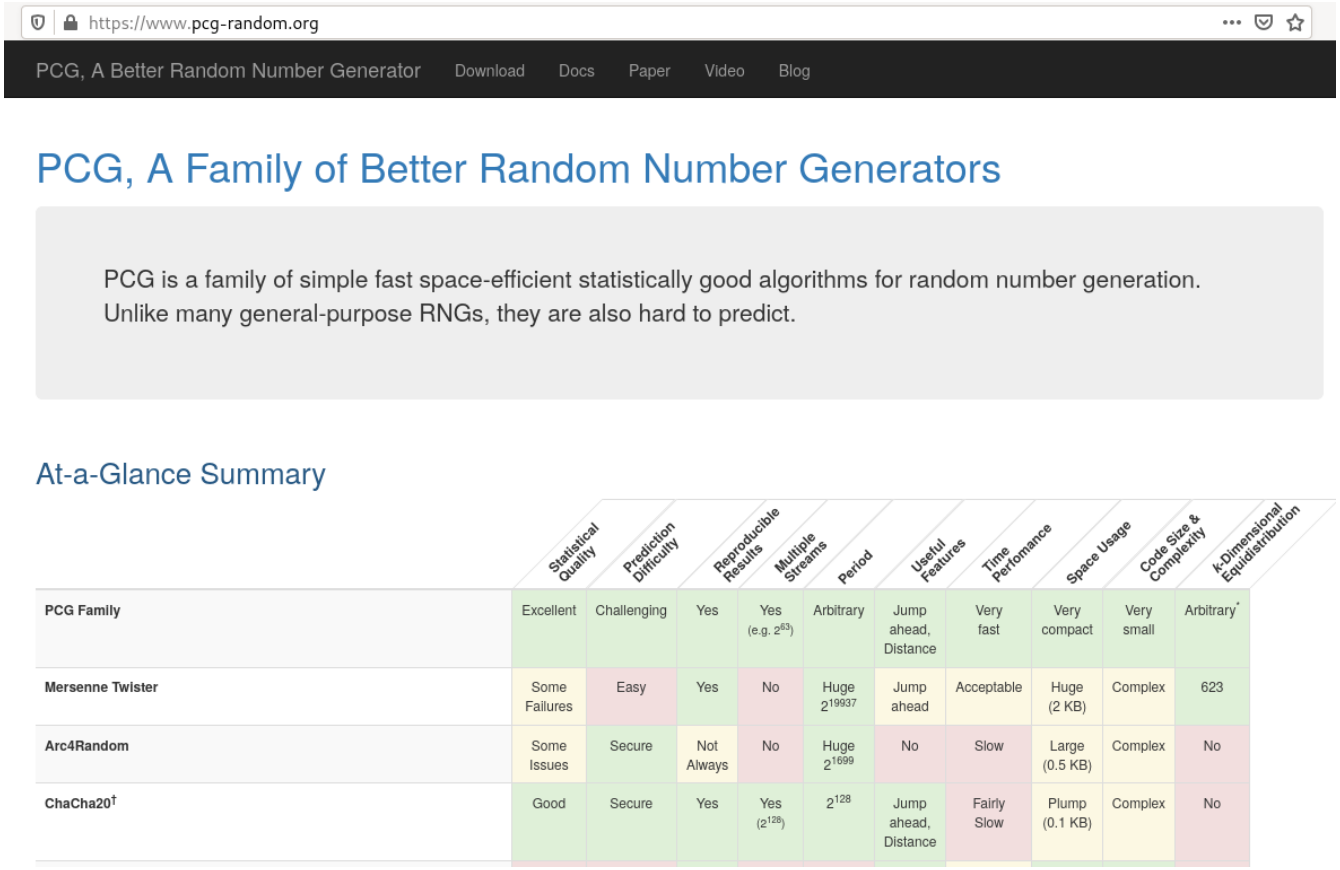
4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Charles Bouillaguet, Claire Delaplace, and Pierre-Alain Fouque. Revisiting and improving algorithms for the 3XOR problem. *IACR Trans. Symmetric Cryptol.*, 2018(1) :254–276, 2018.

[2] Gaëtan Leurent and Ferdinand Sibleyras. Low-memory attacks against two-round even-mansour using the 3-XOR problem. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 210–235. Springer, 2019.

[3] Mridul Nandi. Revisiting Security Claims of XLS and COPA. *IACR Cryptology ePrint Archive*, 2015 :444, 2015.

1. `https://www.reddit.com/r/programming/comments/ja0tji/predicting_the_pcg_pseudorandom_number_generator/`



https://www.pcg-random.org

PCG, A Better Random Number Generator Download Docs Paper Video Blog

PCG, A Family of Better Random Number Generators

PCG is a family of simple fast space-efficient statistically good algorithms for random number generation. Unlike many general-purpose RNGs, they are also hard to predict.

At-a-Glance Summary

	Statistical Quality	Prediction Difficulty	Reproducible Results	Multiple Streams	Period	Useful Features	Time Performance	Space Usage	Code Size & Complexity	k-Dimensional Equidistribution
PCG Family	Excellent	Challenging	Yes	Yes (e.g. 2^{63})	Arbitrary	Jump ahead, Distance	Very fast	Very compact	Very small	Arbitrary*
Mersenne Twister	Some Failures	Easy	Yes	No	Huge 2^{19937}	Jump ahead	Acceptable	Huge (2 KB)	Complex	623
Arc4Random	Some Issues	Secure	Not Always	No	Huge 2^{1699}	No	Slow	Large (0.5 KB)	Complex	No
ChaCha20†	Good	Secure	Yes	Yes (2^{128})	2^{128}	Jump ahead, Distance	Fairly Slow	Plump (0.1 KB)	Complex	No

FIGURE 2 – Le site web faisant une promotion non méritée du générateur pseudo-aléatoire PCG.

ÉLÉMENT DE PORTFOLIO 03

Autre

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Recherche en cryptologie et enseignement de la cryptologie.

URL de l'élément :

- `https://isec.sfpn.net`
- `https://crypta.sfpn.net`
- `https://www.dunod.com/sciences-techniques/exercices-et-problemes-cryptographie-0`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Depuis sa création et pendant toute la période d'évaluation, l'équipe ALMASTY était une équipe universitaire composée uniquement d'enseignants-chercheurs. En principe, la moitié de notre activité concerne l'enseignement, notamment de la cryptologie, du HPC, de la théorie de la complexité, etc. Les membres de l'équipe ont notamment assumé la responsabilité de cours de cryptologie dispensés en première et en deuxième année du parcours **Sécurité, Fiabilité et Performances** (SFPN) du master informatique de Sorbonne Université. Ces cours, ainsi que les projets d'étudiants que nous encadrons, sont la principale source de discussion au sujet de l'enseignement au sein de l'équipe.

Le premier élément du portfolio de l'équipe ALMASTY illustre déjà comment les problèmes que posent la conception de nos enseignements suggèrent des pistes de recherche. Nous discutons ici du flux d'idées inverse, c'est-à-dire des actions menées par l'équipe pour la formation par la recherche et des développements menés par l'équipe pour moderniser l'enseignement de la cryptologie.

3 PRÉSENTATION DE CET ÉLÉMENT

Les enseignants en cryptographie peuvent s'appuyer sur quelques ouvrages de référence ("*textbook*"). Un petit nombre ont été traduits en français, notamment *Cryptographie, Théorie et pratique* de Douglas Stinson, paru en 2003. Cet ouvrage a légèrement vieilli et il est surtout épuisé. Cependant, pour l'animation de séances de travaux dirigés (TDs) ou de travaux pratiques (TPs), les enseignants sont largement livrés au système D.

3.1 Travaux Dirigés

Un membre de l'équipe a publié en 2012 la première édition de l'ouvrage *Exercices et problèmes de cryptographie* [5]. Cet ouvrage comble un manque en proposant une série d'exercices (corrigés) de cryptologie abordant une large palette de thèmes, allant bien au-delà des grands classiques : sécurité sémantique, modes opératoires pour le chiffrement par blocs, attaques sur des versions réduites de l'AES, construction de SHA-3, cryptanalyse linéaire et différentielle, générateurs pseudo-aléatoires, théorie algorithmique des nombres, attaques sur les chiffrements RSA et Elgamal, sur les signatures de Schnorr et Lamport, etc. Une troisième édition est parue pendant la période d'évaluation (octobre 2018) et une quatrième édition est actuellement en cours d'impression (avec une parution prévue pour juin 2023). Cet ouvrage joue toujours un rôle utile une décennie après sa parution ; il permet en effet d'animer des séances de TDs et il est utilisé dans plusieurs autres universités françaises.

3.2 Travaux Pratiques

Du côté des travaux pratiques, la situation n'est pas meilleure. Une rapide recherche sur internet montre que beaucoup de cours de cryptologie contiennent en fait *peu* de TPs, et que ceux qui existent ne sont ni très passionnants ni très en phase avec la pratique moderne de la cryptographie (sans même parler de la recherche dans ce domaine).

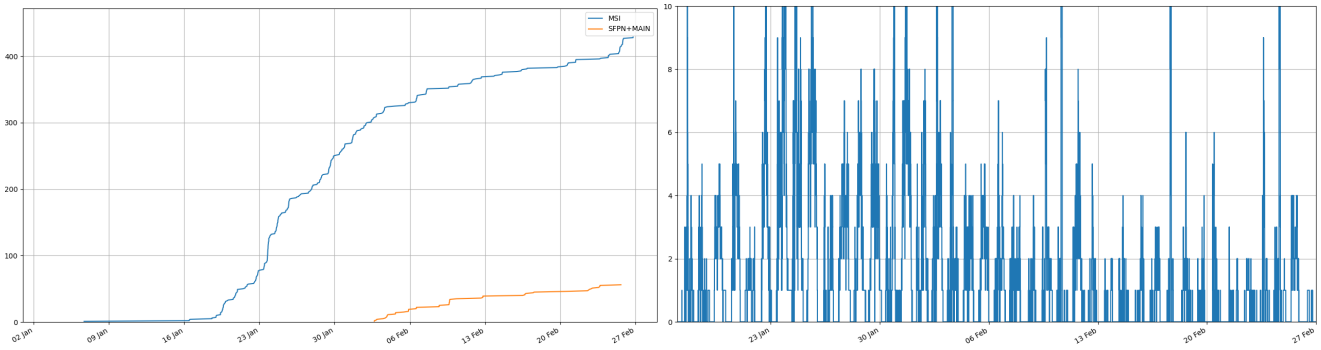


FIGURE 1 – Nombre de tâches réalisés par deux groupes d'étudiants (gauche) et nombre d'étudiants connectés à la plate-forme (droite), en 2023.

Un membre de l'équipe a commencé en 2013-2014 à mettre en place une collection de *web-services* hébergés dans le nuage, avec lesquels les étudiants pouvaient interagir. Non seulement c'est un scénario réaliste d'utilisation de la cryptographie mais cela donne des possibilités pédagogiques inédites :

- Les étudiants peuvent implanter des protocoles cryptographiques (avec le web-service comme « interlocuteur »).
- Les web-services peuvent contenir des secrets cryptographiques. Ceci permet aux étudiants d'implanter des attaques pour tenter de les extraire.

Les étudiants apprécient particulièrement l'aspect interactif : c'est-à-dire que le système leur dit *tout de suite* s'ils ont réussi, et (essaie) de leur expliquer *pourquoi* ils n'ont pas réussi.

Sur le plan de la cryptologie, cela permet de faire accomplir aux étudiants des tâches qui seraient impossibles à mettre en place dans une séance traditionnelle et enrichit considérablement les TPs.

Nous avons choisi de présenter le tout comme un jeu d'aventure rétro en mode texte. Au fur et à mesure que les étudiants résolvent des tâches cryptographiques, ils peuvent explorer une version virtuelle (déserte) de leur campus universitaire et progresser dans le "scénario", qui leur réserve quelques surprises. Il y a même une bande son ! La figure 2 donne une petite idée du résultat.

À très peu d'exceptions près, les étudiants plébiscitent le choix qui consiste à présenter le tout comme une sorte de jeu avec une vague intrigue et une ambiance *geek*. Ils sont nombreux à dire qu'ils apprécient le côté ludique, et « *plus concret* » qu'un TP classique.

Du point de vue des enseignants, il est manifeste que le système capte davantage l'attention des étudiants que des TPs "classiques", comme en témoigne la figure 1. Des étudiants se connectent tous les jours, week-end compris. On voit même des étudiants valider des tâches le samedi à 23h ! Le tout a fait l'objet d'une soumission aux Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) en 2023.

3.3 Formation par la recherche

Cinq des dix doctorants (co-)encadrés par l'équipe sont des étudiants à qui les permanents ont fait cours. C'est une politique, sinon militante, du moins volontariste : nous estimons qu'il est juste que nous prenions en thèse les étudiants que nous formons.

Dans cette optique, nous tenons à ce que nos cours de M2 présentent des résultats récents (nous fixons cette barre à 10 ans). À l'automne 2022, nous avons présenté la spectaculaire cryptanalyse du schéma de signature "post-quantique" Rainbow par W. Beullens qui datait de quelques semaines [1], la signature PICNIC [4] basée sur le "calcul réparti dans la tête" et qui date de 2017, ou encore l'algorithme très simple que nous avons publié l'été dernier pour résoudre des systèmes polynomiaux booléens [2].

Enfin, une de nos publications [3] a débuté par un projet de recherche donné à un binôme d'étudiants de M1. Le binôme a tellement bien réussi que l'une des deux a poursuivi par un stage de recherche au sein de l'équipe, à l'issue duquel la publication a été rédigée. L'étudiante a tourné, pendant un confinement, une vidéo de présentation pour un colloque virtuel, et a fini par rejoindre l'équipe pour préparer son doctorat.

```
[Lower brain functions initialized]

Vous êtes dans un local poubelle.  Il fait tout noir. Il y a des néons au
plafond, mais ils sont éteints.  Seul un éclairage d'urgence de faible
intensité, au niveau du sol, éclaire un peu la pièce.  Le sol et les murs
sont couverts de carrelage, probablement pour faciliter le nettoyage. Une
porte équipée d'une barre anti-panique donne sur une autre pièce.

Ici se trouvent des déchets.
Ici se trouve un conteneur-poubelle.
Ici se trouve une inscription sur le sol.

>>>
```

```
                                                  UGLIX v4.0 beta
                                            (LPNHE Research Terminal)

                  Active user: charles
```

```
*** Process received signal ***
[UGLIX:04968] Signal: Segmentation fault (11)
[UGLIX:04968] Signal code: Address not mapped (1)
[UGLIX:04968] Failing at address: 0xb)

Dumping core...
[Uglix Secure Vault Enclave]

IV = c0696483ca1898e3296b5af242fe13de
```


PTpH9h1JY7wX6S1sexmJahOdyVcLVKiAO4rBSdAeVgRDSMfqtng0B/Z0l2rFa1tN
D53VeMnuiOZhHGylDcU+wIzjuP38968TfNmjdJv0J9F15vGUZ//zSbpJGtCWkEnz
8lqmF7L37gv/BtfWgKUAnS8qdye3mbWKci9nHQiaJUASwXoBHdQUeEOCLoW4pkjz
cuv53CCiCOB2rekxtF2QQI3+1S/EniGh0BHwGBbBcixqZXCug8PIah4zh2KgYJtS
GOqbt4OJBhSwlEHwt+9/aslBMsff8XoUkApxtKTZOuXXgyAgP1bWbxxV32+1LiCr
SL/fXYCTYQi4Jx/vuLJWIM6ggPUemJzkPvSIPbQn+T8MhesL3NRQ6PyEI0IJRUhv
burY9Z/2DMjiF2XdsCK70vdqHjK6WzRACvJ708+FaBShs+OzpeNGNS21B6dFvUvi
GTd0rVxLk/sMFrldm+iAoAOII2N6FVD7+BIamoxvowel6kCwSzkkkafZpKMcNpI/
bZE24LsMfPJ6QAfx8PqEyTpwa/atlKBuQw0bENNndaV2OzzMxd6yQ8OEgVyH97eL
0hYmJ9Pe7GrIrCWIFy8W/TLtzSXsVC6RHffW0E/d+Ld/DQEV73aSLJ3rzur4JMti
634hCmjU6GAAYKVEvZldiMo28Tbw0IOmmP/1IDqkU+DT3xlaxOnDsM6regrTK5In
7cwn3v44ZmjPcbQ50yJvTDAxhmlQy4QNuqsS48eAwNF7WC4AeG+/7oCXMX9cfD6y
yq31YDWLM45fm5Iuo7RY4j0BCHYdRRIu3U1ZAZO0l7a2opK0ap2niJ0/VmjsxT2t
ZcvaSgb10ZMVmKg03kCYSUhVRZu3q+0DC0TR+ZU1ae34gRWj/SLxRN+HsWzBCDRZ
7XGrLaj9ne8g09Vse07u0l+mVuEMsW/myLZ/6QjRAfVswde2VKCJm+cDvI9+RTpl
3DZXEEMXgaHKJQgtaloRfpC9NvEfCLNcq5ShG6B/eKmNWq8J/XFZ/b0Ll+dPy2IG
wQMrsu//Mmx1GoVS/tavk+LhSCQIlcmdi9fxN81bmpq08oImqQGOK09kFhnbO0t8
zy6ELOvYy0EIzTexnUYunqtAtxZrmCD7JavtnG0tSsYq18Vg674jFesfoKAUSYDj
jrcfs4jPWIcBTA1DXaw3XIQfs/NQ+1MXU3XZ8lH1VExc+x5nDfq24mColBsMdfm+
vTWNBrO8q2kOttiXMn94fPeauHbQjeMyyi9wfISzAtQ9IwRDMm38FQH22P6MYERX
goqPHxwG8wLtu/nwNf221lJXxJP0rpf24H4sEclO8NVVyG5nxIbWC2kHRLVJ8B4M
5cMYRCXBkgKmXZp6yGgaGdm0aLZkBHMRgnh5w8NUyLAYR0skPWsD6qtPdvMh1qyX
oREflZMxoNTGtf5nankJKhUzxAyBF4msaQ70i7oBvb//upzHLRjdHulooq6XIutW
JkN4uNzTnURStnCsPq1Rnu5PK+71i/TMy577cJUbcHqxp8aTzib+mjv37rTK/tcI
oxUlCBHHY3JL5yamqP6AQI21JZvCvVqXMQt7vTIgFZQMZg2/goiLF3shgFFGemcZ
OhYY8Rep5XtiqDWt+DelQQ+n2ruOjqQwwPI6Drw9yA1KRBVZ4A7fiJmjz/+EV626
jDWCI3sMubtQRysVqWjZp5i5XGfzTZ30eWvreEEMHY9H1aa5ytkT7ceE7t+Pb1kN
CBg8CRabNgwamuuqC6PMjvjVIk+sfZ4+9xhMPQ4pnjCY/gH2zyc1OCYNAhjpvVqz
musrzQSAXefXe85zrV3V7tc4cjJ6GzeeVraVt7MgmE5/tvAuq5zxS1QvYE0FOGeF
sw2laimMjh5DWp2W7DxC1WInqNbaNSly5UQIFuEA2zZmuNMkDAh1v2WNCVtIZsiA
z6Y3spz6/zZmwWxWVTqbEzEuYDC6RjHCJw4DPVnIrtbriGIRrPuoMDTj5+/TLnuo
Ami1+16OCfaGHgt6n63mfADCvBCHIFkEmnlDw2h5Q1Jbpni5aW1lOSt5ihxtgBBB


```
>>>
```

```
                                        UGLIX v4.0 beta
                                      (Lab Director Proxy)

              Active user: charles

WARNING: - This prototype is INCOMPLETE.
WARNING: - It does not fully implement RSA PKCS#1 v1.5.
WARNING: - Here is what it actually does:
WARNING:   - read the input as a hex-encoded number (big-endian)
WARNING:   - run the IA decision algorithm on the input
WARNING:   - raise it power d modulo N (d is the secret key)
WARNING:   - print the result in hex (big-endian)
WARNING: - This does not produce valid OpenSSL signatures
WARNING:   out of the box because the padding is not applied

YOU HAVE BEEN WARNED

              Data:                 deadbeef

              Checking data ...

              No problem detected

              Signature:
```


8641ada0857569f020f43f44e4dbe6c5bdacb4fd20ac3ec542edfff10969db0fe31bc61968b58f16e1df7b4d03244764a13f6
f57937810380f9daf69d23359363d09f744e98fd7a8e6ae3aa783a7db76e1d1a776174a4497bf7ecb1754f59b378ef07677d66f354523544e983d386b
038f50673b8eebce1064295af9592844a92e03f41b74e840699496adfae04c46fe9a912ed9fdede646f917daf4598f8fe8d88140fe69c8b66cab7ac29
c086e1ba89c9723675924bf9b9a2ca8c0d5ec63b9d51c8


```
[press any key]
```

```
Vous êtes dans le hall du bâtiment, au niveau inférieur.  Les murs et le sol
sont peint en rouge pêtant.  Ca fait presque mal aux yeux.  Une cloison vitrée
vous sépare d'une bibliothèque vide au sud.  En levant le nez, vous voyez tous
les étages de couleurs bariolées, ainsi que l'enchevêtrement d'escaliers qui
y conduit.  À ce propos, celui qui vous permettrait de monter au niveau du
dessus a été retiré.  Au Nord, l'espace de restauration est fermé, mais un
couloir jaune donne sur le coin Nord-Est.  Un couloir turquoise débouche côté
Ouest.

Ici se trouve une clef secrète RSA qui traine dans un coin.

>>>
```

```
                                   UGLIX v4.0 beta
                                 (Service terminal)

Active user: charles
public-key uploaded: YES

                                      PKI menu
                                      --------


0. Query public-key directory
1. Upload public-key
2. Upload signature
3. Tutorial
4. Submit Certificate Signature Request
5. Return to main menu
```

```
Vous êtes dans un petit passage couvert qui sépare deux cours.  Au Sud, une
porte vitrée donne sur le hall d'entrée de la bibliothèque.  En face, au Nord,
une autre porte vitrée, fermée celle-là, donne sur une rotonde qui ceinture
le pied d'une tour peinte en rouge et marquée :

                ,agd"                   "bg,
             ,gdP"                        "Ybg,
           ,dP"                              "Yb,
         ,dP"                                  "Yb,
        ,8"                                      "8,
       ,8'                                        `8,
      ,8'            d8888  .d8888b.               `8,
      d'            d8P888 d88P  Y88b                `b
                   d8P 888       .d88P
                  d8P  888      8888"
                 d88   888       "Y8b.
                 8888888888888     888
                       888 Y88b  d88P
      Y,               888  "Y8888P"                 ,P
      `8,                                           ,8'
       `8,                                         ,8'
        `8a                                       a8'
         `Yba                                   adP'
           "Yba                               adY"
             `"Yba,                       ,adP"'
                `"Y8                    8P"'

>>> sud
Vous êtes dans le hall d'entrée de la bibliothèque des licences.  Vous voyez
l'intérieur à travers les portes vitrées qui vous en séparent : il n'y a personne.
Les portes sont fermées et vous ne pouvez pas entrer.  L'éclairage est tamisé et
les bancs en mousse rouge et mauves sont étonnamment confortables.  Ca vous donne
envie d'y faire une petite sieste, mais le distributeur de friandise à l'Est du
hall fait un bruit désagréable.

Ici se trouve un distributeur de friandises et de gadgets.
Ici se trouve un catalogue électronique.

>>>
```

```
Vous êtes dans la salle de travail de l'équipe des responsable de la sécurité
informatique.  Un vieux carton de pizza traîne dans un coin.  Il n'y a pas de
fenêtres.

Ici se trouve une spécification du journal des évènements de sécurité (partie II).
Ici se trouve un terminal d'administration du security engine.

>>> look spécification
Le MAC qui accompagne chaque entrée du journal des évènements de sécurité
fait 256 bits.  Il se décompose en fait en 4 blocs de 64 bits chacun :
- le premier (octets [0:8]) est obtenu en évaluant un véritable MAC. Celui-ci
                           [--------REDACTED--------]
- les 3 autres blocs contiennent des parts d'un secret partagé avec le
  système de partage de secret de Shamir.
Plus précisément, si on note :
- p : le nombre 2**64 - 59 (qui est premier),
- X : les bits [0:64] du MAC,
- A : les bits [64:128] du MAC,
- B : les bits [128:192] du MAC,
- C : les bits [192:256] du MAC.
Alors A == R(X) mod p, où R est un polynôme de degré 8 inconnu.
Alors B == S(X) mod p, où S est un polynôme de degré 16 inconnu.
Alors C == T(X) mod p, où T est un polynôme de degré 24 inconnu.
Les coefficients constants de R, S et T sont des "firmware update keys", qui
                           [--------REDACTED--------]
Pour reconstituer ces coefficients, qui sont en fait R(0), S(0) et T(0), on
                           [--------REDACTED--------]
                           [--------REDACTED--------]

>>>
```

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Ward Beullens. Breaking rainbow takes a weekend on a laptop. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 464–479. Springer, 2022.

[2] Charles Bouillaguet, Claire Delaplace, and Monika Trimoska. A simple deterministic algorithm for systems of quadratic polynomials over gf(2). In Karl Bringmann and Timothy Chan, editors, *5th Symposium on Simplicity in Algorithms, SOSA@SODA 2022, Virtual Conference, January 10-11, 2022*, pages 285–296. SIAM, 2022.

[3] Charles Bouillaguet, Florette Martinez, and Julia Sauvage. Practical seed-recovery for the PCG pseudo-random number generator. *IACR Trans. Symmetric Cryptol.*, 2020(3) :175–196, 2020.

[4] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Bhavani Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1825–1842. ACM, 2017.

[5] Damien Vergnaud. *Exercices et problèmes de cryptographie — 3ème édition*. Dunod, 2018.