Dossier de Qualification aux fonctions de maître de conférences

Section 27

Léo Robert

Léo Robert

Post-Doctorant au sein du XLIM, Université de Limoges, France

56 rue Bonnabaud
63000 Clermont-Ferrand
+33 6 83 49 90 78

leor38120@gmail.com
`https://perso.limos.fr/~leorober/`

1 Résumé

Je suis actuellement post-doctorant au sein du laboratoire XLIM de l'Université de Limoges sous la supervision de Cristina ONETE. J'ai soutenu ma thèse de doctorat le 22 septembre 2022 avec le sujet :
"*Conceptions et Analyses de Protocoles en Sécurité Prouvable : Applications aux messageries et à l'attestation*".

Thème de recherche

Mon axe de recherche principal porte sur la construction de protocoles cryptographiques, avec une spécialisation dans l'établissement de canal sécurisé par échange de clés pour un chiffrement de bout-en-bout. Les preuves de sécurité de ces protocoles sont dans le modèle calculatoire.

Mots-clés : techniques asymétriques (clés publiques), sécurité de protocoles, modèle calculatoire, messagerie sécurisée, Signal, guérison, chiffrement de bout-en-bout, protocoles de messageries asynchrones, réseau 5G, attestation en profondeur, liage par couche.

Publications

12 publications en conférences internationales (1 **A***, 6 **B**, 3 **C** et 2 **Non Notés**).

4 publications en revues internationales (3 **Q2** et 1 **Q3**).

4 autres publications (conférences nationales, rapport de master, manuscrit de thèse).

12 Présentations et Séminaires.

Enseignements

J'effectue 86 heures d'équivalents TD en tant que vacataire pour l'année 2022/2023, 192 heures en tant que doctorant pour les trois années scolaires 2019/2020-2020/2021-2021/2022. De plus, j'ai eu le CAPES de mathématiques en 2015 où j'ai enseigné en lycée pendant l'année scolaire 2015/2016 et une partie de l'année 2016/2017 en collège. J'ai aussi effectué un stage de professionnalisation (Emploi Avenir Professeur) en collège de 2014 à 2016. J'ai pris en charge un monitorat de mathématiques à l'université au cours de l'année 2013/2014. Enfin, j'ai donné des cours particulier de mathématiques de 2011 à 2016.

- Professeur de Mathématiques - Lycée climatique Jean Prévost, VILLARD-DE-LANS (2015/2016) et collège Le Vergeron MOIRANS (de septembre à décembre 2016). Chaque année comporte un enseignement de 9 heures de cours par semaine (sans compter les préparations).
- Doctorant contractuel à l'Université Clermont Auvergne :
  - 3×12h TD/TP: "Security System Information" (Master 2; ≈ 25 étudiants)
  - 3×12h TD : "Security Models" (Master 2; ≈ 10 étudiants)
  - 10h CM : Introduction à la sécurité (Licence 3; 39 étudiants)
  - 21h : TP de sécurité (IUT2 Réseaux et Télécoms; 12 étudiants)
  - 2×20h TD : Analyse de Fourier (IUT1 Réseaux et Télécoms; 22 étudiants)
  - 2×20h TD : Statistiques (IUT2 Réseaux et Télécoms; 24 étudiants)
- Vacataire à l'Université Clermont Auvergne :
  - 68h TD/TP : Introduction à la base de données (BUT1 Informatique; 27 étudiants)
  - 18h TP : Technologies de l'Internet (BUT2 informatique)

2 Curriculum Vitae

Identité

NOM	ROBERT
Prénom	Léo
Nationalité	Française
Âge	31 ans
Email	leor38120@gmail.com
Téléphone	+33683499078
Website	`https://perso.limos.fr/~leorober/`
Situation familiale	Pacsé, 1 enfant

Les pièces complémentaires optionnelles (feuille de CM/TD/TP, rapports, implémentation, diaporamas, vidéos, ...) sont disponibles sur mon site web : `https://perso.limos.fr/~leorober/`.

Parcours universitaire

Doctorat **2022**

Université Clermont Auvergne

Débuté le 01 octobre 2019 et soutenu le 22 septembre 2022 avec le sujet :
"Conceptions et Analyses de Protocoles en Sécurité Prouvable : Applications aux messageries et à l'attestation"

Président	M. David POINTCHEVAL	Professeur des universités ENS, INRIA, PSL, Paris
Rapporteur	M. Benjamin NGUYEN	Professeur des universités LIFO, INSA Centre Val de Loire
Rapporteur	Mme Melek ÖNEN	Maître de conférences Eurecom, Sophia Antipolis
Examinateur	M. Karthikeyan BHARGAVAN	Directeur de Recherche INRIA, Paris
Examinateur	M. Jean-Guillaume DUMAS	Professeur des universités LJK, Université Grenobles Alpes
Examinateur	M. Olivier SANDERS	Ingénieur de recherche Orange Labs, Cesson-Sévigné
Co-Directeur de thèse	M. Pascal LAFOURCADE	Maître de conférences LIMOS, Université Clermont Auvergne
Co-Directrice de thèse	Mme. Cristina ONETE	Maître de conférences XLIM, Université de Limoges

Master 2 **2019**

Université Grenoble Alpes

Cybersecurity - Mémoire de master "Design of a multi-party non-interactive protocol using homomorphic encryption Case study of organ transplant" réalisé au sein du LJK (UGA).

Master 1 **2018**

Université Grenoble Alpes

Science in Industrial and Applied Mathematics - Stage au sein de l'Institut Laue Langevin "Modélisation des profils de diffusion des nanoclusters"

CAPES Mathématiques **2015**

Université Grenoble Alpes

CAPES obtenu pendant le master MEEF.

Licence Mathématiques **2014**

Université Joseph Fourier

Expériences professionnelles

Post-Doctorant (CDD) — **01/10/2022 – 31/03/2024**

XLIM, Université de Limoges

Travaux de recherche supervisés par Cristina ONETE pour le projet ANR MobiS5.

Doctorant (CDD) — **2019–2022**

LIMOS, Université Clermont Auvergne

Débuté le 01 octobre 2019 et soutenu le 22 septembre 2022 avec le sujet "Conceptions et Analyses de Protocoles en Sécurité Prouvable : Applications aux messageries et à l'attestation".

Stagiaire M2 (CDD) — **02/2019 – 06/2019**

LJK, Université Grenoble Alpes

Travail de recherche sur le sujet "Design of a multi-party non-interactive protocol using homomorphic encryption Case study of organ transplant" sous la supervision de Jean-Guillaume Dumas.

Stagiaire M1 (CDD) — **06/2018 – 08/2018**

Institut Laue Langevin

Stage de Master 1 pour sujet "Modélisation des profils de diffusion des nanoclusters". Le but était d'écrire un programme en C^{++} permettant de simuler différents phénomènes d'agrégations en 3D, sous la supervision de Sylvain Prevost (ILL) et Sergei Grudinin (INRIA).

3 Activités d'enseignements

Enseignements actuels

Lors de cette année scolaire 2022/2023, j'ai la responsabilité de 2 modules ainsi qu'un encadrement de projet de stage. Ces enseignements sont efféctués au sein de l'Université Clermont Auvergne en tant que vacataire. Le total d'heures d'enseignement équivaut à 86 heures et l'encadrement est un suivi de 1 heure par semaine environ (pour une durée de 4 mois). Tous ces enseignements sont donnés en français.

- Introduction à la base de données (TD/TP) : **BUT1 Informatique** [68 heures] [27 étudiants]

  Ce module est déstiné aux premières années de BUT informatique. Toutes les notions de base pour la gestion de bases de données sont introduites (modèle conceptuel, modèle logique, requêtes SQL basiques et avancées, formes normales). Ce module se déroule sur un semestre avec 1 heure de TD et 2 de TP par semaine pour chaque groupe (j'ai la responsabilité de deux groupes). La plupart de TD/TP sont déjà mis en forme, j'en ai repris quelqu'uns. L'évaluation se fait à l'aide de deux évaluations (préparées en équipe) et une Saé sous forme de rapport et d'oral (par groupe de 3 4).

- Technologies de l'Internet (TP) : **BUT2 informatique** [18 heures] [? étudiants]

  Cet enseignement est prévu pour le second semestre. Il consistera à mettre en place des TP de réseaux.

Enseignement en tant que doctorant contractuel

J'ai pu effectuer un total de 192 heures d'enseignements au cours de mon doctorat (en tant que contractuel) ce qui correspond à 64 heures annuelles. A cela se rajoute des encadrements lors de ces trois années. Les enseignements ont concernés des étudiants allant de première année d'IUT (ex BUT) à master 2. Il y a des modules de mathématiques (statistiques et transformée de Fourier), de cryptographie (informatique et mathématiques) et de réseaux.

Je regroupe les modules suivants ces trois années de doctorat.

- Security System Information (TD/TP) : **Master 2** [3×12 heures] [≈ 25 étudiants]

  J'ai eu la responsabilité de ce module pour la partie pratique (je n'ai pas donné de CM) pendant mes trois années de doctorat (2019-2020, 2020-2021 et 2021-2022). Le but de ce module est d'introduire la sécurité pour des systèmes d'informations. Il y avait une partie théorique (cryptographie symétrique, asymétrique) et aussi pratique (PGP, PKI). J'ai participé à l'élaboration des planches de TD/TP et à l'évaluation finale ainsi que sa correction.

- Security Models (TD) : **Master 2** [3×12 heures] [≈ 10 étudiants]

  J'ai eu la responsabilité de ce module pour la partie pratique (je n'ai pas donné de CM) pendant mes trois années de doctorat (2019-2020, 2020-2021 et 2021-2022). Ce module est déstiné à introduire la sécurité prouvable de schémas/protocoles dans deux modèles (calculatoire et symbolique). J'ai participé à l'élaboration des planches de TD/TP et à l'évaluation finale ainsi que sa correction.

- Introduction à la sécurité (CM) : **L3 alternants** [10 heures] [39 étudiants]

  J'ai eu la responsabilité de ce module lors de l'année 2021-2022. J'ai personnellement réalisé le contenu du cours qui visait à introduire la cryptographie. J'ai aussi écrit et corrigé l'évaluation finale de ce module.

- TP de sécurité : **IUT2** [21 heures] [12 étudiants]

  J'ai pris en charge les TP de ce module lors de l'année 2021-2022. Le but était de faire manipuler les étudiants à différents processus réseaux liés à la sécurité (VLAN, IPtables, SSL, firewall).

- Analyse de Fourier (TD) : **IUT1** [2×20 heures] [22 étudiants]

  J'ai eu la responsabilité de ce module pour la partie exercice (je n'ai pas donné de CM) pendant mes deux premières années de doctorat (2019-2020 et 2020-2021). Ce module vise à introduire les transformées de Fourier afin d'être plus à l'aise sur le domaine du traitement du signal.

- Statistiques (TD) : **IUT2** [2×20 heures] [24 étudiants]

  J'ai eu la responsabilité de ce module pour la partie exercice (je n'ai pas donné de CM) pendant mes deux premières années de doctorat (2019-2020 et 2020-2021). Ce module reprend les notions élémentaires de statistiques et aussi de probabilités.

Autres enseignements

J'ai eu plusieurs expériences d'enseignement avant mon doctorat. J'ai eu le CAPES de mathématiques en 2015 grâce auquel j'ai été stagiaire dans un lycée et un collège. J'ai aussi eu la chance de pouvoir expérimenter le travail d'enseignant à travers le dispositif Emploi Avenir Professeur qui permettait de suivre un enseignant en classe (observation et pratique) durant deux années scolaires. J'ai pu aussi découvrir l'enseignement grâce à du tutorat de mathématiques (sur les équations différentielles) lorsque j'étais étudiant.

Mediation

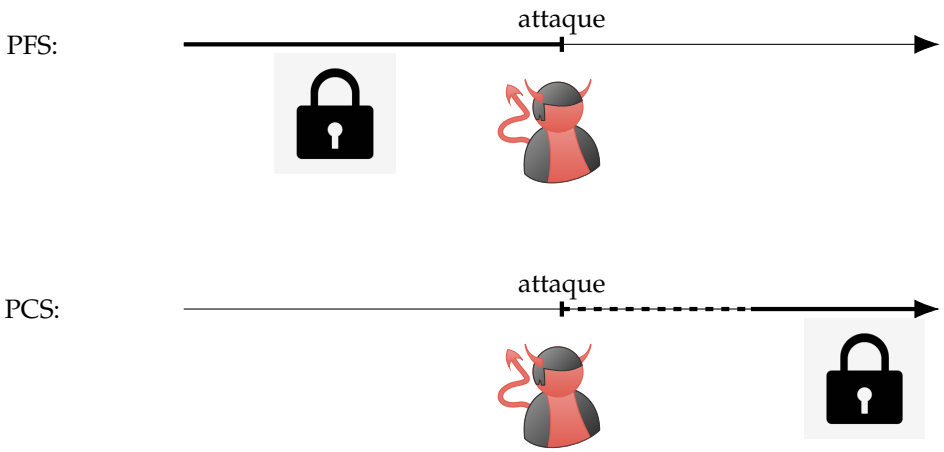
- 07/11/2020 : Participation aux Rendez-vous des Jeunes Mathematiciennes (distanciel). Le but était de proposer des énigmes sur la cryptographie à des élèves de premières pendant un atelier durant 1h30.
- Du 05/03/2020 au 07/03/2020 : Animations pour le festival Math en Scène à Castanet-Tolosan. Les deux premières journées étaient consacrées aux scolaires (du primaire au lycée) et la dernière journée était tout publique. Les animations sont issues du groupe Informatique Sans Ordinateur (ISO) de l'IREM de Clermont.
- 18/12/2019 : Animation de la "Journée Activités Debranchées" à Bordeaux (INRIA). Nous avons présentés (avec Pascal LAFOURCADE) des activités pouvant être réutilisés en cours à des enseignants du secondaire et universitaires.

4 Activités de recherche

Pouvoir communiquer avec n'importe qui est devenu nécessaire dans notre société actuelle. Le besoin de sécurité à travers les outils permettant l'échange d'information est un besoin exprimé par de nombreux citoyens [1], notamment depuis les révélations d'Edward Snowden. Celui-ci a rendu publique une surveillance de masse opérée par des gouvernements et visant une large part de la population. Depuis ces révélations, de nombreux travaux (de recherches, mais aussi industriels) ont émergé pour assurer au mieux la sécurité des services de communication ainsi que de la vie privée des utilisateurs. L'un de ces services, appelé Signal, a connue un succès important lors de sa sortie notamment grâce à sa robustesse mais aussi pour sa facilité d'utilisation (d'autres outils existaient mais sans réussir à susciter l'intérêt des citoyens; par exemple PGP). La robustesse de Signal peut être exprimée à travers ses propriétés de sécurité:

- Asynchronicité : les communications entre participants peuvent se faire alors qu'un des deux participants ne soit en ligne. Ceci implique qu'Alice doit pouvoir envoyer un message à Bob à tout moment et Bob sera capable de lire ce message quand il reviendra en ligne;
- Authenticité : les participants sont sûrs de parler à la bonne personne. Autrement dit, si Alice pense parler à Bob alors Bob est effectivement son partenaire de communication (et vice-versa);
- Sécurité Parfaite en Amont (*Perfect Forward Secrecy* – PFS) : si un adversaire réussit à compromettre à un moment donné la communication, alors tous les messages échangés *avant* l'attaque de l'adveraire restent sécurisés.
- Sécurité Après Compromission (*Post-Compromise Security* – PCS) : cette propriété est l'inverse de la PFS, autrement dit les messages échangés *après* l'attaque doivent pouvoir être à nouveau sécurisés, au bout d'un certain temps.

Ces deux dernières propriétés peuvent être illustrées de la manière suivante:



L'utilisation de Signal est prévue pour des communications à long terme; si Alice et Bob ont débuté une communication, elle doit pouvoir continuer sans avoir besoin de recalculer la mise en place d'une session. La propriété PCS devient donc cruciale dans ce contexte : si un attaquant réussit à compromettre un des participants (et donc à faire perdre la confidentialité de la communication) alors le PCS assure qu'au bout d'un moment, la communication "guérit" et annule tout dégât causé par l'attaque précédente. En pratique, il est préférable d'avoir une guérison rapide afin d'avoir le moins de messages possibles découvert par l'adversaire.

Mon premier axe de recherche se focalise sur cette notion de PCS. Dans un premier temps, nous proposons deux variantes de Signal qui améliorent la notion de PCS. Ensuite, nous proposons un modèle permettant d'évaluer ce temps de guérison quel que soit le protocole envisagé (possédant la notion de PCS). Le but est de pouvoir comparer des protocoles (qui a priori ne sont pas comparables) sous cette propriété de PCS afin de répérer le meilleur protocole (*i.e.*, celui avec la guérison la plus courte).

Nous supposons que l'application Signal, installée dans un composant dédié (ordinateur, smartphone, tablette, etc) pour Alice et Bob, se comporte de la manière attendue. Cependant, notre description haut-niveau (dans le sens où nous avons abstraits des briques de base) ne prend pas en compte toute la chaîne de production pour arriver jusqu'à l'application qu'utilisent Alice et Bob. Une description correcte (avec des preuves de sécurité, calculatoires ou formelles) est indispensable [2] mais des failles peuvent survenir à chaque point intermédiaire jusqu'à l'utilisation finale de l'application. Par exemple :

[1] Un exemple de ce changement de mentalité peut être illustré par un évènement survenu en 2021 avec WhatsApp; cette entreprise a vu un nombre important de désinscriptions de ses utilisateurs suite à une modification des conditions d'utilisation rendant un niveau de vie privée amoindri.

[2] Une illustration intéressante de ce fait est une remarque de Michel Raynal concernant les algorithmes (discutés de manière générale) : ce ne sont pas les algorithmes qui font voler un avion mais si les algorithmes utilisés ne sont pas corrects alors l'avion ne volera pas (ou pas longtemps en tout cas).

- Le protocole doit être implémenté dans un langage de programmation. Il existe des bibliothèques cryptographiques pour que les briques de base soient bien utilisées mais certains choix de paramètres peuvent poser problèmes, le langage lui-même peut être source de failles.
- La partie logiciel de l'application vit dans un système (l'OS du composant *i.e.*, Windows, Linux, etc) comportant lui aussi des failles.
- Les composants physiques (la partie "hardware") sont eux aussi sources de failles avec notamment les attaques par canaux auxiliaires. Ces attaques prennent en compte les fuites d'information par des phénomènes physiques (*i.e.*, la consommation d'énergie, la production d'ondes électromagnétiques, les variations de température, etc).
- L'utilisation même du service par les utilisateurs. Par exemple, Alice pourrait laisser son smartphone ouvert, laissant la possibilité à un attaquant d'utiliser toutes sortes de moyens pour arriver à ses fins (simplement regarder, installer des applications, etc).

Il existe de nombreuses étapes, indépendantes des spécifications haut-niveau du protocole, pouvant amener à des attaques. Cependant, il existe aussi des solutions permettant d'avoir certaines assurances concernant la fiabilité des services voulus. L'une d'elles, appelée *attestation*, permet la verification d'une propriété pour une composante (réseau, machine virtuelle, IoT, etc). Les propriétés pouvant être évaluées sont nombreuses et dépendent de l'infrastructure analysée; ces propriétés peuvent être la géolocalisation, le contrôle d'accès à des ressources, l'intégrité de code.

L'attestation en profondeur. Dans un autre axe de recherche, nous nous concentrons sur une variante du processus d'attestation appelée *Deep Attestation*. Le but est de proposer le premier modèle de sécurité (pour de la sécurité prouvable) permettant d'évaluer la sécurité d'une solution que nous proposons pour le Deep Attestation. Cette solution, accompagnée d'une preuve de concept permettant d'évaluer sa faisabilité dans un contexte pratique, vise à améliorer l'équilibre entre la sécurité et la performance des solutions existantes (et standardisées).

Les protocoles ZKP basés sur des cartes à jouer. Prouver que l'on détient un secret sans le révéler est très utile en cryptographie. De nombreuses applications requièrent ce processus comme le vote électronique, l'accès à des données sur un serveur, la gestion de mots de passe, la blockchain... Pour cela, des protocoles de preuves à divulgation nulle de connaissance sont utilisés (ou ZKP pour Zero Knowledge Proof). Cependant, ces protocoles sont souvent difficiles à concevoir surtout pour des publics ayant peu de bases en cryptographie (comme des étudiants par exemple). Nous prenons donc le parti de transformer les hypothèses de compléxité algorithmiques en hypothèses physiques, afin de rendre ces protocoles plus simples et directs à comprendre. Ainsi, nous proposons des protocoles utilisant des objets de la vie courante (notamment des cartes à jouer) pour prouver la détention d'un secret sans le révéler. Les applications de tels protocoles concernent des puzzles de type Sudoku; l'idée est de mettre en place un protocole où un joueur qui prétend avoir la solution, parvient à convaincre à une autre personne qu'il a la solution sans révéler la moindre information sur cette solution. L'existence de ces protocoles sont assurées par un résultat théorique qui énonce qu'un problème NP-complet possède toujours un protocole ZKP associé. Cependant, ce résultat ne permet pas d'obtenir des protocoles efficaces (inutilisable en pratique) donc chaque protocole doit être construit spécifiquement pour un jeu donné.

Principales Contributions

B Olivier Blazy, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Cristina Onete, and Léo Robert. MARSHAL: Messaging with Asynchronous Ratchets and Signatures for faster HeALing. In *SAC 2022 - 37th ACM/SIGAPP Symposium On Applied Computing*, pages 1–8, Virtual, Czech Republic, April 2022. ACM

Résumé : La notion de PCS permet de garantir un niveau de sécurité après une compromission de clés. Suivant les clés révélées, un attaquant peut avoir accès à une partie de la communication jusqu'à un certain point où le protocole *guérit*. En ajoutant de l'aléa, l'attaquant n'a plus les informations nécessaires pour continuer à accéder à la communication et est éjecté du protocole.

Le protocole Signal peut être rapidement décrit en 4 étapes:

- Un échange de clé intial : le protocole X3DH est utilisé avec l'aide d'un serveur;
- Un ratchet symétrique : dérivation d'une clé de message par une fonction de dérivation de clé (KDF) par un même participant sans attendre la réponse du destinataire; c'est cette étape qui assure la PFS.
- Un ratchet asymétrique : lorsque les rôles d'envoyeur/destinataire sont échangés, une nouvelle valeur Diffie-Hellman est insérée dans la dérivation de clé; c'est cette étape qui assure la PCS.
- Chiffrement authentifié : chaque message est chiffré avec une nouvelle clé (qu'on appelle *clé de message*); il faut associer à chaque envoi de message, des données auxiliaires via AEAD.

Les garanties de PCS pour Signal sont limitées par deux facteurs :

- le manque d'authentification persistante : les clés sont modifiées mais cette évolution doit venir du bon participant.
- la fréquence d'utilisation du ratchet asymétrique : plus le ratchet asymétrique est utilisé souvent et plus le protocole guérit rapidement.

Notre but est de développer un protocole, appelé MARSHAL (Messaging with Asynchronous Ratchets and Signatures for faster HeALing) qui améliore la PCS tout en restant le plus proche possible de Signal. Nous restons proche de Signal en gardant la même structure, ce qui nous permet d'avoir une implémentation plus directe et aussi une comparaison claire de ces protocoles.

Ces propriétés ajoutées ont un coût. La principale raison de ce surcoût résulte du temps de calcul nécessaire pour calculer deux nouvelles opérations : une nouvelle valeur Diffie-Hellman et une signature pour chaque donnée auxiliaire supplémentaire.

A* How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment. In *32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA, August 2023. USENIX Association

Disponible sur `https://www.usenix.org/conference/usenixsecurity23/presentation/blazy`

Résumé : De nombreux protocoles de messagerie ont vu le jour depuis ces dernières années. Chacun dispose de propriétés de sécurité spécifiques mais certaines sont reconnues comme étant indispensables. Par exemple, la confidentialité des messages doit être assurée, mais aussi l'authenticité ou bien l'intégrité. Parmi ces propriétés se trouve la *Post-Compromise Security* (PCS) dont nous avons proposé une amélioration pour le protocole Signal appelé MARSHAL. Le protocole Signal n'est cependant pas le seul à proposer la PCS; il y a aussi OTR, Matrix, et Wire. Une comparaison directe de ces protocoles en termes de PCS est impossible car chacun d'eux évolue dans un système donné. Par exemple, Signal possède un serveur semi-honnête (on lui fait seulement confiance dans le fait de stocker, sans modification, les clés d'utilisateurs) alors que SAID, une autre variante de Signal, basée sur l'identité, possède un centre de distribution de clés (KDC) qui connait tous les secrets associés aux utilisateurs.

Nous proposons un modèle permettant de quantifier le temps de guérison pour des protocoles possèdant la PCS. Pour définir formellement ce modèle, chaque protocole est modélisé en schéma SCEKE (Secure-Channel Establishment schemes with Key-Evolution, *i.e.*, Schémas avec Evolution de Clé pour un Etablissement de Canal Sécurisé). Le but d'un adversaire contre ce genre de protocole est d'apprendre le plus de messages possibles (qui sont chacun chiffrés avec une clé de message différente) après une attaque donnée. Toutes les attaques ne sont pas équivalentes, certaines peuvent donner lieu à des attaques actives, révéler plus ou moins de messages au cours de la communication. En plus de définir un modèle générique, nous proposons aussi une taxonomie exhaustive sur le type d'attaquant possible. Notre métrique mesure le nombre de messages "perdus" (*i.e.*, accessibles à l'adversaire) jusqu'au point où les messages sont à nouveaux hors d'atteinte de l'attaquant. Par exemple, la guérison optimale dans notre métrique vaut $(1, 0)$ alors que la pire vaut (∞, ∞) *i.e.*, le protocole ne guérit jamais. Ces cas sont évidents à traiter, mais notre métrique devient intéressante pour les cas se trouvant entre ces deux extrêmes.

Afin de montrer l'expressivité de notre modèle, nous comparons 4 schémas a priori très difficiles à comparer autrement :

- Signal, basé sur une infrastructure à clé publique;
- SAID, une variante de Signal basée sur l'identité;
- enfin, des procédures de relais (*handover*) pour le réseau 5G. Ces procédures n'ont encore jamais été étudiées pour la PCS, c'est donc la première fois qu'une telle analyse est faite. De plus, nous proposons une variante visant l'amélioration de la PCS.

B Ghada Arfaoui, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Adina Nedelcu, Cristina Onete, and Léo Robert. A cryptographic view of deep-attestation, or how to do provably-secure layer-linking. In Giuseppe Ateniese and Daniele Venturi, editors, *Applied Cryptography and Network Security - 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, Proceedings*, volume 13269 of *Lecture Notes in Computer Science*, pages 399–418. Springer, 2022

Résumé : Notre monde est de plus en plus interconnecté, avec un besoin de réseaux flexibles et dynamiques toujours plus grandissants. Dans un environnement comme le cloud ou le réseau 5G, la technologie de virtualisation permet une mise à l'echelle facile et spécifique à la demande des utilisateurs. En effet, les machines virtuelles peuvent être facilement mises en place, mises à l'échelle ou bien déplacées sur n'importe quel type d'infrastructure physique permettant ainsi de meilleures performances et une plus grande sécurité. Cependant, de nouveaux besoins ont vu le jour; par exemple dans le domaine de la santé numérique (e-santé) où la géolocalisation est primordiale. Un outil permet de vérifier si ces infrastructures ont un état de fonctionnement valide, c'est *l'attestation*.

Le processus d'attestation permet à une entité indépendante de la platerforme de vérifier si cette plateforme a un comportement attendu, si son état n'a pas été modifié de manière inattendue. Le but est de vérifier que certaines propriétés de sécurité sont vérifiées. Par exemple, un serveur pourrait vérifier que le code source d'une machine virtuelle est bien valide (*i.e.*, aucun code malicieux n'a été inséré). Nous nous intéressons à ce cas, où des machines virtuelles sont gérées par un hyperviseur qui lui-même interagit avec un composant physique nommé "racine de confiance" (*root of trust*).

Il existe actuellement deux solutions pour l'attestation en profondeur :

- L'attestation via un seul canal : chaque VM est attestée en même temps que l'hyperviseur qui la gère. Cette solution est sûre dans le sens où une VM est liée à son hyperviseur mais la mise à l'échelle est très coûteuse, l'hyperviseur est attesté à chaque fois qu'une VM l'est.
- L'attestation par canal multiple : cette solution atteste l'hyperviseur et les machines virtuelles indépendamment. Cette fois la mise à l'échelle est efficace (une seule attestation pour l'hyperviseur) mais la sécurité n'est plus garantie, les VM ne sont plus liées à l'hyperviseur.

Nous prenons le meilleur des deux solutions standardisées (unique/multiple canal) pour l'attestation en profondeur pour obtenir un outil liant des machines virtuelles et des hyperviseurs avec une efficacité raisonnable (dans le sens où les performances se rapprochent de celles des deux solutions). Notre solution est simple, mais élégante, et utilisant des standards cryptographiques pour assurer qu'une attestation d'un hyperviseur est bien liée aux machines virtuelles dont il a la charge. Les contributions sont sur 3 points:

(a) **Un schéma cryptographique :** Notre schéma assure la sécurité et l'efficacité pour l'attestation en profondeur. Pour cela, chaque hyperviseur et chaque machine virtuelle ne s'atteste qu'une seule fois. Chaque VM possède une paire de clés dont la partie publique fait partie de l'attestation même de l'hyperviseur qui la gère (qui lui-même est attesté par la racine de confiance physique). Afin d'authentifier ces clés, elles sont incluses dans un nonce, et transmises par le serveur de vérification. Si l'attestation de l'hyperviseur réussit, alors le serveur de vérification peut lier cet hyperviseur avec des VM qui s'attesteraient ultérieurement. Si l'attestation de l'hyperviseur échoue, alors l'ensemble des clés publiques ne peuvent pas être de confiance.

(b) **Prouver la sécurité d'une attestation liante en étant autorisé** Un avantage clair de notre approche est d'avoir complètement formalisé et prouvé les garanties de sécurité. Nous utilisons une approche par série de jeux, permettant la construction de primitives de plus en plus fortes basées sur des plus faibles. Notre but est d'obtenir une primitive d'attestation liante et autorisante (ALA) : chaque composant s'atteste individuellement à une entité autorisée à vérifier pour avoir leurs attestations liées. Nous réglons ainsi le problème où des VM pourraient ne pas appartenir à un hyperviseur car chaque attestation de VM est maintenant liée à un hyperviseur (et casser cette hypothèse reviendrait à résoudre un problème reconnu difficile).

ALA a trois propriétés :

- l'autorisation : seulement un serveur dédié peut effectuer une attestation;
- l'indistinguabilité : aucun attaquant au milieu ne pourrait deviner qu'un seul bit d'information durant la communication entre des participants honnêtes;
- le liage : un serveur peut détecter si deux composants sont liés ou pas.

Nous formalisons une série de primitives dont la dernière est un échange de clé authentifiée. Chaque primitive est d'interêt indépendant et possède une sécurité de plus en plus forte. Cette approche a deux avantages : elle permet d'utiliser des primitives plus faibles en boîte noire pour former des primitives plus fortes; et elle permet aussi d'avoir des preuves plus directes et plus simples.

Nous commençons notre construction par un schéma basique d'attestation retournant simplement un résultat binaire (oui/non). Nous supposons donc une sécurité par définition. Sa fonctionnalité est simple : si le résultat de l'attestation retourne "non" alors le composant est malicieux mais retournera "oui" si le composant est honnête. Basés sur cette hypothèse, nous construisons une série de mécanismes cryptographiques pour ajouter des propriétés de sécurité afin de resister à des adversaires ayant plus de pouvoir. La première étape est de rajouter de l'authentification, ce qui assure qu'un composant pourra toujours s'attester avant une corruption mais pas après. Ensuite nous ajoutons la propriété de liage qui permet de lier certains composants entre eux (les VM avec l'hyperviseur qui les gère).

(c) **Implémentation :** Nous avons effectué une preuve de concept pour assurer que notre solution a bien les performances attendues, et est capable d'être appliquée dans un contexte pratique. L'architecture est composée d'un hyperviseur et de plusieurs VM (jusqu'à 55). Cela montre que notre solution est plus performante que la solution à canal unique et ajoute un petit surplus (un calcul de fonction de hashage) comparé à la solution de canal multiple.

Ce travail est le premier à formaliser, en utilisant des outils cryptographiques, l'attestation en profondeur. Ce traitement est plus difficile que la conception en soi de la solution car l'attestation est un processus générique présentant de nombreuses classes d'algorithmes qui ont chacun des buts différents. Ainsi, nous ne faisons qu'effleurer le problème mais espérons – à part pour le côté pratique de nos constructions – que le traitement cryptographique, primitives, et preuves sont indépendamment intéressantes pour cet axe de recherche.

Conférences Internationales

C Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Card-based ZKP protocol for Nurimisaki. In Stéphane Devismes, Franck Petit, Karine Altisen, Giuseppe Antonio Di Luna, and Antonio Fernández Anta, editors, *Stabilization, Safety, and Security of Distributed Systems - 24th International Symposium, SSS 2022, Clermont-Ferrand, France, November 15-17, 2022, Proceedings*, volume 13751 of *Lecture Notes in Computer Science*, pages 285–298. Springer, 2022

B Daiki Miyahara, Léo Robert, Pascal Lafourcade, So Takeshige, Takaaki Mizuki, Kazumasa Shinagawa, Atsuki Nagao, and Hideaki Sone. Card-Based ZKP Protocols for Takuzu and Juosan. In Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara, editors, *10th International Conference on Fun with Algorithms (FUN 2021)*, volume 157 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:21, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik

C Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Physical Zero-Knowledge Proof for Suguru Puzzle. In *22nd International Symposium on Stabilization, Safety, and Security of Distributed Systems SSS 2020*, Austin, United States, November 2020

C Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Interactive Physical ZKP for Connectivity: Applications to Nurikabe and Hitori. In *CiE*, à distance, Belgium, July 2021

NN Xavier Bultel, Pascal Lafourcade, Charles Olivier-Anclin, and Léo Robert. Generic Construction for Identity-based Proxy Blind Signature. *Lecture Notes in Computer Science*, June 2022

B Pascal Lafourcade, Léo Robert, and Demba Sow. Linear Generalized ElGamal Encryption Scheme. In *International Conference on Security and Cryptography (SECRYPT)*, Paris, France, July 2020

B Pascal Lafourcade, Léo Robert, and Demba Sow. Fast Short and Fast Linear Cramer-Shoup. In *Foundations and Practice of Security - 13th International Symposium, FPS*, Montreal, France, December 2020

B Pascal Lafourcade, Léo Robert, and Demba Sow. Fast Cramer-Shoup Cryptosystem. In *18th International Conference on Security and Cryptography, SECRYPT 2021*, Online, France, July 2021

NN Matthieu Journault, Pascal Lafourcade, Malika More, Rémy Poulain, and Léo Robert. How to Teach the Undecidability of Malware Detection Problem and Halting Problem. In *WISE13: The 13th World Conference on Information Security Education*, Maribor, Slovenia, May 2020

Revues Internationales

Q2 Léo Robert, Daiki Miyahara, Pascal Lafourcade, Luc Libralesso, and Takaaki Mizuki. Physical zero-knowledge proof and np-completeness proof of suguru puzzle. *Information and Computation*, page 104858, 2021

Q2 Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone. How to construct physical zero-knowledge proofs for puzzles with a "single loop" condition. *Theoretical Computer Science*, 888:41 – 55, 2021

Q2 Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, and Léo Robert. Optimal Threshold Padlock Systems. *Journal of Computer Security*, pages 1–34, 2021

Q3 Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Card-based ZKP for connectivity: Applications to Nurikabe, Hitori, and Heyawake. *New Gener. Comput.*, 40(1):149–171, 2022

Visibilité

Présentations d'articles accéptés en conférences:

- 17/11/2022 : SSS 2022 (présentiel).
- 06/2022 : ACNS 2022 (présentiel).
- 04/2022 : SAC 2022 (vidéo).

- Autres présentations en distanciel : SSS 2020; SECRYPT 2020 et 2021; FPS 2021 et 2021.
- 05/2022 : présentation d'un poster à RESSI 2022.
- 18/12/2020 : vidéo présentant une activité pédagogique à RESSI 2020.

Séminaire :

- 13/09/2022 : Séminaire au XLIM (Limoges) concernant mes travaux.
- 04/05/2022 : Présentation de mes travaux de thèse au CIRM (Marseille).
- 24/02/2022 : Séminaire à l'INSA Bourges sur l'attestation en profondeur.
- 25/01/2022 : Séminaire des doctorants au LIMOS (Clermont) concernant les protocoles ZKP basés sur des cartes.
- 06/2021 : Journées des doctorants au LIMOS (Clermont), présentation à l'aide d'un poster.
- Séminaire du LIMOS : 08/09/2020 (Deep Attestation); 18/05/2021 (Protocole ZKP physique); 08/02/2022 (Metrique sur la PCS).

Visites et écoles d'été :

- Du 17/08/2022 au 26/08/2022 : visite à l'université de Surrey (Guildford – Angleterre) en collaboration avec Ioana Boureanu.
- Du 01/08/2022 au 05/08/2022 : école d'été sur la cryptographie post-quantique à Budapest.
- Du 04/07/2022 au 08/07/2022 : école d'été sur les méthodes formelles à Nancy (Cyber In Nancy).

Membre de comité de relecture :

- ACNS 2022 (sous-relecteur).
- FPS 2022 (sous-relecteur).
- WISE15.
- WISE14.
- New Generation Computer (revue).

Enadrements

- 2022-2023 : **"Etude des monoïdes plaxique pour une application cryptographique"** [1h/semaine] [2 étudiants]

  J'ai déposé un sujet de projet pour des étudiants de Master 1 (2A d'école d'ingénieur). Le but de ce projet est de comprendre un objet mathématique (les monoïdes plaxiques) pour une éventuelle application en cryptographie. Il y a d'abord un état de l'art sur ce sujet, puis une analyse mathématiques et de la compléxité des algorithmes associés puis une implémentation (en RUST) des différents algorithmes. Selon les résultats obtenus, il est possible de les appliquer à des schémas d'échange de clés ou des schémas de signature électronique.

- 2021-2022 : **"Implementation of MARSHAL and SAMURAI"** [1h/semaine] [2 étudiants]

  Ce projet prévue pour deux étudiants de Master 2 (3A d'école d'ingénieur ISIMA) avait pour but d'implémenter deux variantes du protocole Signal. Les deux étudiants devaient dans un premier temps mettre en place un état de l'art sur la propriété de sécurité PCS ainsi que sur les protocoles de messageries multi-parties. Le développement des deux protocoles s'est fait en Java avec une évalution du temps d'exécution et de la mémoire.

- 2021-2022 : **"Analysis of SET (the game)"** [1h/semaine] [2 étudiants]

  L'étude mathématiques des jeux de société est un domaine de recherche dynamique. Ce projet avait pour but d'analyser les configurations maximums (et maximales) du jeu SET. Il y avait une analyse théorique et aussi expérimentale (implémenter en Python). Deux étudiantes de Master 1 (2A d'école d'ingénieur) se sont portées volontaires pour ce projet.

- 2020-2021 : **"Implementation of MARSHAL"** [1h/semaine] [2 étudiants]

  Ce projet consistait à implémenter une variante du protocole Signal, par deux étudiantes de Master 1 (2A d'école d'ingénieur).

- 2019-2020 : **"On the implementation of Signal"** [1h/semaine] [2 étudiants]

  Le but de ce stage était de comprendre l'implémentation de Signal (qui est open-source) afin de répérer les morceaux de code susceptible d'être modifié. Ce projet a eu lieu durant le premier confinement.

5 Activités Administratives

SSS 2022	Participation à l'organisation de la conférence.
RESSI 2022	Participation à l'organisation de la conférence.
SST	Certification de Sauveteur Secouriste du Travail (24/06/2021).
ISO	Participation au groupe Informatique Sans Ordinateur de l'IREM Clermont.

6 Liste des pièces complémentaires

- Les deux rapports des rapporteurs de thèse [2 documents séparés].
- Pièce d'identité [1 document].
- Attestations d'enseignement et recommendations (David COURSIMAULT, Gérard CHALHOUB, Cédric BOUHOURS, Joël TOUSSAINT, Pascal LAFOURCADE) [5 documents dans 1 fichier].

References

[AFJ+22] Ghada Arfaoui, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Adina Nedelcu, Cristina Onete, and Léo Robert. A cryptographic view of deep-attestation, or how to do provably-secure layer-linking. In Giuseppe Ateniese and Daniele Venturi, editors, *Applied Cryptography and Network Security - 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, Proceedings*, volume 13269 of *Lecture Notes in Computer Science*, pages 399–418. Springer, 2022.

[BFJ+22] Olivier Blazy, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Cristina Onete, and Léo Robert. MARSHAL: Messaging with Asynchronous Ratchets and Signatures for faster HeALing. In *SAC 2022 - 37th ACM/SIGAPP Symposium On Applied Computing*, pages 1–8, Virtual, Czech Republic, April 2022. ACM.

[bla23] How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment. In *32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA, August 2023. USENIX Association.

[BLOAR22] Xavier Bultel, Pascal Lafourcade, Charles Olivier-Anclin, and Léo Robert. Generic Construction for Identity-based Proxy Blind Signature. *Lecture Notes in Computer Science*, June 2022.

[DDLR21] Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, and Léo Robert. Optimal Threshold Padlock Systems. *Journal of Computer Security*, pages 1–34, 2021.

[JLM+20] Matthieu Journault, Pascal Lafourcade, Malika More, Rémy Poulain, and Léo Robert. How to Teach the Undecidability of Malware Detection Problem and Halting Problem. In *WISE13: The 13th World Conference on Information Security Education*, Maribor, Slovenia, May 2020.

[LMM+21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone. How to construct physical zero-knowledge proofs for puzzles with a "single loop" condition. *Theoretical Computer Science*, 888:41 – 55, 2021.

[LRS20a] Pascal Lafourcade, Léo Robert, and Demba Sow. Fast Short and Fast Linear Cramer-Shoup. In *Foundations and Practice of Security - 13th International Symposium, FPS*, Montreal, France, December 2020.

[LRS20b] Pascal Lafourcade, Léo Robert, and Demba Sow. Linear Generalized ElGamal Encryption Scheme. In *International Conference on Security and Cryptography (SECRYPT)*, Paris, France, July 2020.

[LRS21] Pascal Lafourcade, Léo Robert, and Demba Sow. Fast Cramer-Shoup Cryptosystem. In *18th International Conference on Security and Cryptography, SECRYPT 2021*, Online, France, July 2021.

[MRL+20] Daiki Miyahara, Léo Robert, Pascal Lafourcade, So Takeshige, Takaaki Mizuki, Kazumasa Shinagawa, Atsuki Nagao, and Hideaki Sone. Card-Based ZKP Protocols for Takuzu and Juosan. In Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara, editors, *10th International Conference on Fun with Algorithms (FUN 2021)*, volume 157 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:21, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[RML+21] Léo Robert, Daiki Miyahara, Pascal Lafourcade, Luc Libralesso, and Takaaki Mizuki. Physical zero-knowledge proof and np-completeness proof of suguru puzzle. *Information and Computation*, page 104858, 2021.

[RMLM20] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Physical Zero-Knowledge Proof for Suguru Puzzle. In *22nd International Symposium on Stabilization, Safety, and Security of Distributed Systems SSS 2020*, Austin, United States, November 2020.

[RMLM21] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Interactive Physical ZKP for Connectivity: Applications to Nurikabe and Hitori. In *CiE*, à distance, Belgium, July 2021.

[RMLM22a] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Card-based ZKP for connectivity: Applications to Nurikabe, Hitori, and Heyawake. *New Gener. Comput.*, 40(1):149–171, 2022.

[RMLM22b] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Card-based ZKP protocol for Nurimisaki. In Stéphane Devismes, Franck Petit, Karine Altisen, Giuseppe Antonio Di Luna, and Antonio Fernández Anta, editors, *Stabilization, Safety, and Security of Distributed Systems - 24th International Symposium, SSS 2022, Clermont-Ferrand, France, November 15-17, 2022, Proceedings*, volume 13751 of *Lecture Notes in Computer Science*, pages 285–298. Springer, 2022.