Sujets de PER 2017-2018

1 Sujets proposés par Emmanuel Fleury

Contact : emmanuel.fleury@u-bordeaux.fr

1.1 Isomorphisme de graphes en temps quasi-polynomial

Le problème de trouver un isomorphisme de graphes est un problème que l'on peut rencontrer dans de nombreux cas d'applications pour identifier les similitudes entre deux programmes. Récemment (2015), László Babai a proposé un algorithme qui propose une solution en temps quasi-polynomial. La preuve de cet algorithme a nécessité encore un certain nombre d'allers et retours avant que la communauté scientifique soit vraiment convaincue de sa véracité. Néanmoins, le but de ce projet est de tester les différentes méthodes connues pour construire un isomorphisme de graphes (total ou partiel) et de tester (si possible) l'algorithme proposé par Babai. À minima, nous espérons essayer d'avancer un peu sur la compréhension du problème et de l'algorithme qui a été proposé.

Références :

- Graph Isomorphism in Quasipolynomial Time László Babai, 2015. `https://arxiv.org/abs/1512.03547`

1.2 Heap-overflow Exploitation in 2017

Valentin BAPST, Maxime BINEAU, Pierre CUBERO-CASTAN Daniel Henry MANTILLA

Le but de ce projet est de dresser un panorama des failles touchant la Heap et des techniques d'exploitations qui marchent encore en 2017. Le groupe devra étudier les articles de référence et tester les différentes failles en les exploitants sur des systèmes Linux relativement récents (Debian/Ubuntu/...). Le but de ce projet est d'arriver à une synthèse des techniques qui marchent encore et une compréhension du fonctionnement du malloc d'une libc6 récente.

Références :

- Malloc Des-Maleficarum blackngel, 2009 `http://www.phrack.org/issues/66/10.html`
- Yet another free() exploitation technique huku, 2009 `http://www.phrack.org/issues/66/6.html`
- The House Of Lore : Reloaded (ptmalloc v2,v3 : Analysis & Corruption) blackngel, 2009 `http://www.phrack.org/issues/67/8.html`
- Advanced Doug lea's malloc exploits jp, 2003 `http://www.phrack.org/issues/61/6.html`
- Vudo - An object superstitiously believed to embody magical powers Michel "MaXX" Kaempf, 2001 `http://www.phrack.org/issues/57/8.html`
- Once upon a free() anonymous, 2001 `http://www.phrack.org/issues/57/9.html`
- Heap overflow using Malloc Maleficarum sploitF-U-N, 2015. `https://sploitfun.wordpress.com/2015/03/04/heap-overflow-using-malloc-maleficarum/`
- how2heap, shellphish, 2017. `https://github.com/shellphish/how2heap`

1.3 Rootkit noyau pour Android

Hadrien AMROUCHE, Nicolas GRELLETY, Bowen LIU, Roland MOUNIER

Le but de ce projet est de réaliser un Kernel Rootkit pour Android et de comprendre les différences par rapport à un noyau "classique" (Desktop et x86). Il serait intéressant de réaliser une preuve de concept complète avec différentes fonctionnalités. Attention, notez que l'assembleur utilisé ici sera du ARM !

Références :

- Android platform based linux kernel rootkit dong-hoon you, 2011 `http://phrack.org/issues/68/6.html`

1.4 Plongée dans la mémoire noyau

Le but du projet sera de comprendre en détail les différents mécanismes de la mémoire dynamique du noyau (SLAB, SLOB, SLUB) et les techniques mises en œuvre pour y détecter les corruptions mémoire (et, éventuellement, comment déjouer cette surveillance). Une preuve de concept pourra être réalisée si le temps imparti le permet.

Références :

- Linux Kernel Heap Tampering Detection Larry H., 2009. `http://www.phrack.org/issues/66/15.html`
- The Linux kernel memory allocators from an exploitation perspective argp, 2012. `https://argp.github.io/2012/01/03/linux-kernel-heap-exploitation/`

2 Sujets proposés par Jean-Marc Couveignes

Contact : Jean-Marc.Couveignes@math.u-bordeaux.fr

2.1 Arithmétique rapide pour les polynômes et les séries.

Étant donnés deux polynômes, ou deux séries, $f(x)$ et $g(x)$ on souhaite calculer rapidement le produit, le quotient et la composée $f(g(x))$ losqu'elle est définie. Les algorithmes rapides pour ces problèmes sont des briques de bases utiles pour la factorisation de polynômes, la recherche de polynômes irréductibles, etc.

On propose d'étudier, d'implémenter et de comparer les algorithmes les plus efficaces connus pour ces problèmes. Si le temps le permet, on pourra examiner les récents algorithmes optimaux mais apparemment impraticables pour la composition.

Références :

- Donald E. Knuth : The Art of Computer Programming, Volume II : Seminumerical Algorithms, 2nd Edition Addison-Wesley 1981
- R. Brent and H.T. Kung, O((nlogn)3=2) Algorithms for composition and reversion of power series, Analytic Computational Complexity, Academic Press, New York, 1975, pp. 217-225.
- Algorithmes en calcul formel et automatique Frédéric Chyzak, Marc Giusti, François Ollivier, Bruno Salvy, Éric Schost `http://algo.inria.fr/salvy/mpri/poly.pdf`
- Fast construction of irreducible polynomials over finite fields, Journal of Symbolic Computation 17 :371-391, 1994 ; extended abstract in Proc. 4th Annual Symposium on Discrete Algorithms, pp. 484-492, 1993. `http://shoup.net/papers/fastirred.pdf`
- A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic, in Proc. 1991 International Symposium on Symbolic and Algebraic Computation, pp. 14-21, 1991. `http://shoup.net/papers/quadfactor.pdf`
- Kiran S. Kedlaya, Christopher Umans Fast Modular Composition in any Characteristic. FOCS 2008 : 146-155

2.2 Arithmétique rapide, multiplication des matrices.

On sait depuis 1969 (Strassen) que la méthode standard pour multiplier deux matrices n'est pas la meilleure et qu'il existe des méthodes théoriquement plus rapides. Cependant, on ignore s'il existe des algorithmes optimaux : multiplier deux matrices est aujourd'hui bien plus lent que de recopier le résultat. Ce problème peut se reformuler en terme de rang d'un certain tenseur de multiplication. Cohn, Kleinberg, Umans et Szegedy on récemment reformulé cette question en termes combinatoire (puzzles).

Références :

- Henry Cohn, Robert D. Kleinberg, Balázs Szegedy, Christopher Umans : Group-theoretic Algorithms for Matrix Multiplication. FOCS 2005 : 379-388
- P. Buergisser, M. Clausen, and A. Shokrollahi. Algebraic Complexity Theory. Grundlehren der mathematischen Wissenschaften. Springer Verlag, Heidelberg, 1996.

2.3 Algorithmes pour la primalité.

Il existe toutes sortes d'algorithmes pour la primalité. On les distingue selon leur caractère déterministe ou probabiliste (Las Vegas ou Monte Carlo). On les distingue aussi selon les outils mathématiques mobilisés (congruences, anneaux, courbes elliptiques). Ce projet consistera en un tour d'horizon des algorithmes pour la primalité. On cherchera à en implémenter un au moins de façons efficace.

Références :

- Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. Ann. of Math. (2), 160(2) :781–793, 2004.
- R. Schoof. Four primality testing algorithms. MSRI Publications, pages 101–126, 2008.
- Atkin, A. O. L. and Morain, F. Elliptic curves and primality proving Mathematics of Computation, 61, 1993.

2.4 Factorisation des entiers

Les algorithmes de crible pour la factorisation des entiers mobilisent un nombre considérable de techniques algorithmiques élémentaires ou sophistiquées. Par exemple, la méthode de factorisation ECM est maintenant incorporée dans ces cribles. On présentera les principes de ces algorithmes et on tachera d'approfondir l'un de leurs aspects critiques, notamment à travers une implémentation.

Références :

- T. Kleinjung et al. GGNFS, 2005. Software available at `https://github.com/radii/ggnfs`
- T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, et al. Factorization of a 768–bit RSA modulus. In Advances in Cryptology–CRYPTO 2010, volume 6223 of Lecture Notes in Comput. Sci. pages 333–350. Springer, 2010.
- P. L. Montgomery. An FFT extension of the elliptic curve method of factorization. PhD thesis, Univers. of California Los Angeles, 1992.
- P. Zimmermann and B. Dodson. 20 years of ECM. In Algorithmic Number Theory–ANTS VII, volume 4076 of Lecture Notes in Comput. Sci., pages 525–542. Springer, 2006.

3 Sujets proposés par Abdou Guermouche

Contact : abdou.guermouche@labri.fr

Étudier les articles suivants (certains sont susceptibles de nécessiter du code) :

3.1 Evil-AP - Mobile Man-in-the-Middle Threat

Anthony Boens, Thibault Krafft, Mickael Mestouri, Quentin Rouves
https://link.springer.com/chapter/10.1007/978-3-319-59105-6_53

3.2 TrustBase : An Architecture to Repair and Strengthen Certificate-based Authentication

https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-oneill.pdf
Adel Guessoum, Clément Lauga

3.3 A Longitudinal, End-to-End View of the DNSSEC Ecosystem

https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-chung.pdf

3.4 The Loopix Anonymity System

Yann Razafimahefa, Ambre Toulemonde
https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-piotrowska.pdf

4 Sujet proposé par Damien Robert

Rémi Clarisse, Antton Domercq
Contact : damien.robert@inria.fr

Le NIST a lancé un appel à projet pour concevoir de nouveaux protocoles résistants aux ordinateurs quantiques : https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Une des soumissions *Supersingular Isogeny Key Encapsulation* repose sur un échange de clé sur le graphe d'isogénies de courbes elliptiques supersingulières (SIDH) https://ecc2017.cs.ru.nl/slides/ecc2017-costello.pdf.

Le projet consiste à étudier et si possible implémenter le protocole SIDH optimisé décrit dans *Efficient algorithms for supersingular isogeny Diffie-Hellman* https://eprint.iacr.org/2016/413

Références :

- C. Costello, P. Longa et M. Naehrig. « Efficient algorithms for supersingular isogeny Diffie-Hellman ». In : Advances in Cryptology. Springer. 2016. https://ecc2017.cs.ru.nl/slides/ecc2017-costello.pdf (cf. p. 1).
- L. De Feo. « Mathematics of Isogeny Based Cryptography ». In : arXiv preprint arXiv :1711.04062 (2017). https://arxiv.org/abs/1711.04062
- L. De Feo, D. Jao et J. Plût. « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies ». In : Journal of Mathematical Cryptology 8.3 (2014), p. 209–247.

5 Sujets proposés par Guilhem Castagnos

Contact : guilhem.castagnos@math.u-bordeaux.fr

5.1 Attaques à base de réduction de réseaux euclidiens sur RSA

Pour accélérer la signature RSA, on peut être tenté d'utiliser un petit exposant privé d. Cependant, Wiener a montré en 1990, que si on utilise un exposant $d < N^{0.25}$, où N est le module public, alors le système RSA peut être cassé. Par la suite, Boneh et Durfee ont montré par des attaques utilisant l'algorithme de réduction de réseaux LLL que le système n'est pas sûr dès que $d < N^{0.292}$.

Il s'agira d'étudier et d'expérimenter de telles attaques. On pourra en particulier implanter l'attaque de Boneh Durfee en utilisant des méthodes de constructions de réseaux pour la cryptanalyse récemment proposée par May et Hermann.

Références :

- D. Boneh, G. Durfee, Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$, `http://crypto.stanford.edu/~dabo/papers/lowRSAexp.ps`
- M. Herrmann, A. May, Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA, `http://www.cits.rub.de/imperia/md/content/may/paper/pkc10_rsa_unraveled.pdf`

5.2 Chiffrement homomorphe

Sarah Bordage, Sylvain Cottanceau, Clément Hec

On dit qu'un système de chiffrement à clef publique est homomorphe si l'espace des messages clairs $\mathscr{M}$ et un groupe $(\mathscr{M}, +)$ et si étant donné deux chiffrés de deux messages m_1 et m_2, il est possible, sans connaître la clef secrète de produire un chiffré de $m_1 + m_2$. Diverses méthodes sont connues pour construire de tels systèmes (chiffrement Elgamal ou de Paillier par exemple). Si $\mathscr{M}$ est maintenant un anneau $(\mathscr{M}, +, \times)$, le problème de construire un système homomorphe à la fois pour $+$ et $\times$ n'a été résolu par Gentry qu'en 2009 en utilisant des réseaux euclidiens. Depuis la proposition de Gentry plusieurs générations plus efficaces de systèmes homomorphes ont été proposées, notamment par Gentry Sahai et Waters (2013) basé sur le problème LWE introduit par Regev en 2005.

Il s'agira d'étudier et d'implanter ce dernier système et de l'appliquer pour évaluer des circuits simples. On pourra également s'appuyer sur une implantation récente.

Références :

- Gentry, Sahai and Waters, Homomorphic Encryption from Learning with Errors : Conceptually-Simpler, Asymptotically Faster, Attribute-Based, `https://eprint.iacr.org/2013/340.pdf`
- I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. TFHE : Fast fully homo- morphic encryption library. `https://tfhe.github.io/tfhe/`, August 2016.

5.3 Chiffrement basé sur les attributs

Le chiffrement basé sur les attributs (ABE), introduit en 2005 par Sahai et Waters, permet de définir une politique d'accès au déchiffrement. Qui peut déchiffrer un chiffré donné est décidé par des attributs et une politique d'accès. Les constructions de tels systèmes utilisent généralement des couplages sur des courbes elliptiques.

Il s'agira d'étudier des constructions de tels protocoles et les notions de sécurités associées et de voir leur comportement lorsque la politique d'accès est peu complexe.

Il est fortement recommandé d'avoir suivi l'UE de cryptologie avancée pour faire ce projet.

Références :

- Amit Sahai and Brent Waters. Fuzzy identity-based encryption, `http://eprint.iacr.org/2004/086.pdf`
- Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, `https://eprint.iacr.org/2006/309.pdf`

5.4 Cryptanalyse de KASUMI

Julien Armentia, Pierre-Arnaud Laporte, Marie Salviac

KASUMI est un chiffrement par bloc utilisé pour les générations récentes de téléphonie mobile. Plusieurs attaques ont été proposées sur ce chiffrement. La plus avancée date de 2010 : Dunkleman, Keller et Shamir donnent une attaque réalisable en pratique sur un PC classique en utilisant des clefs reliées. L'objectif du projet sera d'implanter KASUMI et cette attaque.

Références :

- Le chiffrement KASUMI, http://en.wikipedia.org/wiki/KASUMI
- Orr Dunkelman, Nathan Keller, Adi Shamir, A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, http://eprint.iacr.org/2010/013.pdf

5.5 Cryptographie Post Quantique

Maïa Alexandre, Laura-Graziella Bourrec, Paul Hermouet

Il y a un an, le NIST a lancé un appel à projet pour standardiser de nouveaux protocoles résistants aux ordinateurs quantiques : https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. Les candidats avaient jusqu'au 30 novembre denier pour soumettre leurs propositions. La liste officielle des candidats n'est pas encore connue, mais quelques informations sont disponibles (voir https://twitter.com/hashtag/nistpqc, https://post-quantum.ch et aussi le sujet de Damien Robert). Le projet consistera a étudier une ou plusieurs soumissions basées sur les codes et les réseaux euclidiens.

Références :

- CAKE : Code-based Algorithm for Key Encapsulation, Barreto, Gueron, Gueneysu, Misoczki, Persichetti, Sendrier, Tillich, https://eprint.iacr.org/2017/757.pdf
- CRYSTALS – Kyber : a CCA-secure module-lattice-based KEM, Bos, Ducas, Kiltz, Lepoint, Lyubashevsky, Schanck, Schwabe, Stehlé, https://eprint.iacr.org/2017/634.pdf