Projets 2015

Décembre 2014

Sujets proposés par *Emmanuel Fleury.*

1. **Analyse de programmes binaires par exécutions concrètes et symboliques**
   Salwan, Saudel

   Le but de ce projet sera de dresser un état de l'art des différentes techniques de reconstruction du CFG d'un programme à partir de son seul binaire. Nous étudierons les différents algorithmes et les techniques utilisant des SMT-Solveurs (Z3, YCES, MathSAT) et différents outils d'analyse dynamique tels que Pintool ou autres.

   La finalité de ce projet est de produire un outils permettant l'extraction d'un CFG, même partiel, du binaire étudié.

2. **Hacking Week 2015**
   El Jaouhari, Nonguierma, Jabari

   Le but de ce projet sera de constituer une base de challenges qui serviront à la HackingWeek 2015 de cette année (voir : `http://hackingweek.fr/`).

   Cette année, chaque catégories devra regrouper 4 challenges de complexité croissante (de "facile" à "très dure). Les catégories seront (probablement), les suivantes :
   - Cryptologie
   - Exploitation
   - Forensic
   - Réseau
   - Rétro-ingénierie

   Un coup de main sur la réalisation du site ne sera pas de refus.

Sujets proposés par *Abdou Guermouche*

1. **Beast et Crime : Comment peut-on encore faire des attaques en man-in-the-middle visant SSL/TLS**
   Laforgue, Suivant

   SSL/TLS est un des standards les plus répandus pour la sécurisation des communications sur internet. Bien que le protocole soit assez simple et robuste, de nombreuses

attaques ont été mises au point pour récupérer le contenu en clair des communications. Une première étape de ce projet consistera donc à faire un inventaire des differentes techniques existantes visant à attaquer SSL/TLS. Puis dans un second temps, on s'intéressera aux dernières en date, à savoir les timing attacks basées sur de la compression (TIME, BREACH, ...). Ces attaques permettent d'attaquer une communication http sécurisée via SSL/TLS (https) pour récupérer des informations sensibles en clair (en l'occurrence les cookies d'authentification). L'objectif sera d'étudier ces attaques de manière assez fine et de les mettre en œuvre et de se rapprocher le plus possible d'une implémentation réaliste. (dans la mesure

2. **Mécanismes de Single Packet Authorization : étude et implémentation**
   Ceola, Monin
   Le mécanisme de Single Packet Authorization (SPA) est une approche permettant de modifier dynamiquement le comportement d'un firewall. L'idée est de ne permettre la connexion aux ressources d'une machine qu'aux clients qui se sont authentifiés à l'aide de SPA. Pour ce faire, le client, lorsqu'il veut accéder à un service, va construire un paquet contenant des informations (contenant par exemple la liste des services auxquels il veut accéder) et le chiffrer avec une clé partagée avec le serveur. À la réception de ce message, le serveur vérifie que le message est valide puis ouvre l'accès aux ressources demandées pendant un certain temps. Bien entendu, lors de la vérification, le serveur doit s'assurer que le paquet n'est pas issu d'un rejeu et qu'il est bien issu d'un client légitime. Le but de ce projet est dans un premier temps d'étudier des mécanismes de SPA (tels que fwknop (`http://cipherdyne.org/fwknop/`) ou knocknock (`http://www.thoughtcrime.org/software/knockknock/`)) pour en voir les limites etc ... Puis d'implémenter dans un deuxième temps un couple client/serveur implémentant SPA dont le fonctionnement devra être validé.

Sujets proposés par *Guilhem Castagnos*

Quatre ou cinq parmi :

1. **Cryptanalyse de KASUMI**
   Abdelhamid Boumaraf, Xun Gong et Irène Morel
   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.

   Liens :
   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`

2. **Attaques par fautes sur des clefs publiques**
   Berkane, Brelurut, Chaux
   Il s'agira d'étudier et d'expérimenter par simulation des attaques par fautes sur cartes à puces consistant à perturber la clef publique d'un algorithme de signature. On s'intéressera en particulier à des attaques sur des implantations de signature RSA, proposées par Berzati, Canovas et autres, et Brier, Chevallier-Mames et autres.

   Liens :
   Berzati, Canovas, Goubin, Perturbating RSA Public Keys : an Improved Attack, http://www.iacr.org/archive/ches2008/51540376/51540376.pdf
   Berzati, Canovas, Dumas, Goubin, Fault Attacks on RSA Public Keys : Left-To-Right Implementations are also Vulnerable, https://hal.inria.fr/file/index/docid/560931/filename/rsa_laser.pdf
   Brier, Chevallier-Mames, Ciet, Clavier, Why One Should Also Secure RSA Public Key Elements, http://bcm.crypto.free.fr/pdf/BCCC06.pdf

3. **Attaques à base de réduction de réseaux euclidiens sur RSA**
   Wong
   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.

   Liens :
   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

4. **Applications multilinéaires pour la cryptographie**
   Ekwa Langa, Querol
   L'utilisation des applications bilinéaires issues des couplages des courbes elliptiques en cryptographie il y a une dizaines d'années a donnée lieu à une multitude d'applications. L'extension de ces applications bilinéaires à des applications multilinéaires est

restée un problème ouvert jusqu'à très récemment. De telles applications $n-$linéaires permettraient par exemple de généraliser l'échange de clefs Diffie-Hellman à $n+1$ utilisateurs et auraient de nombreuses autres applications, notamment pour la diffusion chiffrée. Garg, Gentry et Halevi ont proposé en 2013 une construction basé sur des réseaux euclidiens en utilisant des outils issus des systèmes de chiffrement homomorphes. Il s'agira d'étudier et d'implanter cette construction, en s'appuyant sur des variantes et des implantations récemment proposées.

Liens :

Sanjam Garg and Craig Gentry and Shai Halevi, Candidate Multilinear Maps from Ideal Lattices, http://eprint.iacr.org/2012/610.pdf

Langlois, Stehlé, Steinfeld, GGHLite : More Efficient Multilinear Maps from Ideal Lattices, http://eprint.iacr.org/2014/487.pdf

Albrecht, Cocis, Laguillaumie, Langlois, Improved Parameters and an Implementation of Graded Encoding Schemes from Ideal Lattices, http://eprint.iacr.org/2014/928.pdf

5. **Chiffrement homomorphe**

   Bardeau, Lopez

   On dit qu'un système de chiffrement à clef publique est homomorphe si l'espace des messages clairs $\mathcal{M}$ et un groupe $(\mathcal{M}, +)$ 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 $\mathcal{M}$ est maintenant un anneau $(\mathcal{M}, +, \times)$, 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 une deuxième génération plus efficace de systèmes homomorphes a été proposée, notamment par Brakerski.

   Il s'agira d'étudier et d'implanter ce dernier système. On pourra s'appuyer sur une implantation récente.

   Liens :

   Craig Gentry, A Fully Homomorphic Encryption Scheme, http://crypto.stanford.edu/craig/craig-thesis.pdf

   Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. Fully homomorphic encryption without bootstrapping, http://eprint.iacr.org/2011/277.pdf

   Halevi, Shoup, Algorithms in HElib, http://eprint.iacr.org/2014/106.pdf

6. **HIBE et ABE**

   Le chiffrement basé sur l'identité hiérarchique (HIBE) a été introduit par Horwitz and Lynn en 2002. Comme dans un chiffrement basé sur l'identité tout utilisateur peut

envoyer un message chiffré en utilisant l'identité du destinataire comme clef publique. On a de plus une notion de hiérarchie : tout utilisateur au niveau k va pouvoir déchiffrer les chiffrés qui lui sont destinés mais également les chiffrés destinés aux niveaux inférieurs. De même, 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.

Liens :

J. Horwitz and B. Lynn, Toward hierarchical identity-based encryption, http://theory.stanford.edu/~horwitz/pubs/hibe.pdf

C. Gentry and A. Silverberg, Hierarchical id-based cryptography, http://eprint.iacr.org/2002/056.pdf

Amit Sahai and Brent Waters. Fuzzy identity-based encryption, http://eprint.iacr.org/2004/086.pdf

7. **NIKE**

   Le protocole de Diffie Hellman est l'exemple canonique d'échange de clef non interactif (NIKE) : Alice a une clef publique g^x, une clef privée x et Bob a une clef publique g^y et une clef privée y. Sans échanger de messages, ils peuvent tous les deux calculer la valeur g^{xy}. Depuis la contribution de Diffie et Hellman en 1976, ce type de primitive a été peu étudiée. Depuis peu, on constate un intérêt renouvelé pour cette primitive, notamment motivé par les applications embarquées qui nécessitent des protocoles peu gourmands en énergie.

   Il s'agira d'étudier des constructions de tels protocoles, les notions de sécurités associées, et les relations avec d'autres primitives telle que le chiffrement.

   Liens :

   Cash, Kiltz and Shoup, The Twin Diffie-Hellman Problem and Applications, https://www.iacr.org/archive/eurocrypt2008/49650126/49650126.pdf

   Freire, Hofheinz, Kiltz, Paterson, Non-Interactive Key Exchange, https://eprint.iacr.org/2012/732.pdf

(Jusqu'à trois) Sujets proposés par *Jean-Marc Couveignes*.

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.

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. **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).

   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.

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.

   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.

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.

   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.

Sujet proposé par *Karim Belabas*.

Multiplication scalaire sur les courbes elliptiques

Benejean

Le sujet consiste à étudier / implanter différentes représentations possibles pour une courbe elliptique et sa loi de groupe, au delà de la forme de Weierstrass vue en cours.

On peut partir de la base de données de Dan Bernstein et Tanja Lange

`http://hyperelliptic.org/EFD/`

et étudier un certain nombre de courbes (les plus intéressantes pour des critères à déterminer). Un bon point de départ :

`http://www.hyperelliptic.org/EFD/precomp.pdf`

et sa bibliographie, en particulier [12]. Ce preprint contient un nombre conséquent d'idées agorithmiques intéressantes pour optimiser des algorithmes arithmétiques.

Sujets proposés par *Sorina Ionica*

1. **Implémentation des couplages** Les couplages sont utilisés en cryptographie pour mener des attaques contre le logarithme discret sur certaines courbes elliptiques, ainsi que pour la construction des schémas cryptographiques, comme les signatures courtes

ou le schéma de chiffrement à base d'identité. L'objectif de ce projet sera de réaliser une implémentation du couplage pour un niveau de sécurité donné, de préference 192 bits. Une extension possible sera de regarder plusieurs courbes existantes dans la littérature du domaine, afin de déterminer le meilleur choix en terme de performance au niveau de sécurité 192.

2. **Logarithme discret et attaques par canaux cachés**

   Carré, Canto-Torres

   La sécurité des protocoles à base de courbes repose sur le problème du logarithme discret. L'objectif de ce projet est d'évaluer comment une information extérieure, connue à un attaquant qui dispose des outils supplémentaires (typiquement les attaques par canaux auxiliares), permet d'améliorer significativement la complexité des algorithmes pour la résolution du probléme du logarithme discret. Ainsi, suite à des mesures physiques, on supposera qu un certain nombre de bits (de la clé secrète par exemple) sont connus. Il faudra réaliser une implémentation de l'algorithme du kangoroo, qui permet de récupérer les b bits inconnus en temps $2^{b/2}$.

   [1]Tanja Lange, Christine van Vredendaal and Marnix Wakker, Kangoroos in Side-Channel Attacks, http://eprint.iacr.org/2014/565.pdf

3. **Multiplication scalaire sur une courbe elliptique et attaques par canaux auxiliaires**

   Deroo

   La multiplication scalaire est l'opération de base pour la plus part des protocoles cryptographiques utilisant des courbes elliptiques. Étant donné un entier λ et un point P sur la courbe, il faut calculer λP, ce qui se fait de manière efficace par un algorithme classique de type "square-and-multiply". L'algorithme GLV est un algorithme de type "square-and-multiply" plus performant, qui fait usage de la arithmétique de la courbe. On implémentera cet algorithme et on étudiera la résistance aux attaques par canaux cachés.

   [1] A. Faz-Hernandez and P. Longa and A. Sanchez, Efficient and Secure Algorithms for GLV-Based Scalar Multiplication and their Implementation on GLV-GLS Curves, http://eprint.iacr.org/2013/158.pdf

4. **Marche aléatoire dans un groupe et l'algorithme rho de Pollard** La sécurité des protocoles à base de courbes repose sur le problème du logarithme discret, qu'on résout sur une courbe générique en utilisant l'algorithme rho de Pollard. La performance de cet algorithme dépend de manière critique de comment on simule une marche aléatoire dans le groupe. On implémentera cet algorithme et on étudiera ses performances avec la marche aléatoire proposée par Pollard et les marches aléatoires additives proposées par Teske.

   [1] Edlyn Teske, On random walks for Pollard's rho method, Mathematics of Computation, vol 734, number 734, 2000.

5. **Blind signatures à base de couplages**

Reynaud

Une signature aveugle est une signature effectuée sur un document qui a été masqué avant d'être signé, afin que le signataire ne puisse prendre connaissance de son contenu. De telles signatures sont donc employées lorsque le signataire et l'auteur du document ne sont pas la même personne, comme par exemple dans les protocoles de vote electronique. On s'intéressera à la mise en place d'un tel système, les points clé étant d'implémenter les opération primitives sur la courbe, comme la multiplication scalaire et le couplage sur la courbe.

[1] ID-based blind signatures and ring signature from pairings F. Zhang and K. Kim, Asiacrypt 2002.

6. **Comptage de points d'une courbe elliptique et cryptographie** L'objectif de ce projet est de générer des courbes elliptiques qu'on pourra utiliser pour le chiffrement au niveau de sécurité 128. On cherchera des courbes dont le groupe associé est d'ordre un grand nombre premier. On implémentera l'algorithme Schoof-Elkies-Atkin pour le comptage de points et on l'utilisera pour la recherche des courbes. La maîtrise des prerequis vus en cours "Courbes elliptiques" est nécessaire.

Sujet proposé par *Christine Bachoc*.

Attaques sur des cryptosystèmes basés sur les codes linéaires, exploitant le produit de codes.

Doz, Michel, Zirri

Si $C \subset \mathbb{F}_q^n$ et $C' \subset \mathbb{F}_q^n$ sont des codes linéaires, on note $C * C'$ le code linéaire engendré par l'ensemble des $(a_1b_1, \ldots, a_nb_n)$ où $a = (a_1, \ldots, a_n) \in C$ et $b = (b_1, \ldots, b_n) \in C'$. On note $C^2 = C * C$ et, plus généralement, $C^k = C^{k-1} * C$. Des attaques récentes sur certains cryptosystèmes basés sur des codes de Reed Solomon généralisés, et plus généralement sur certaines familles de codes de Goppa, exploitent le fait que le produit de codes ne se comporte pas sur ces instances comme il se comporte sur un code aléatoire. On propose dans ce sujet d'étudier ces attaques à partir des articles cités ci-dessous (accessibles sur la page web de Alain Couvreur). Le projet comprendra une partie de programmation, qui pourra concerner l'algorithme de reconstruction des codes de Reed-Solomon généralisés proposé dans [1], ou tout ou partie de l'une des attaques décrites.

[1] A. Couvreur, P. Gaborit, V. Gauthier-Umana, A. Otmani and J.-P. Tillich, Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes. Des. Codes Cryptogr. 73(2), 641-666, 2014

[2] A. Couvreur, A. Otmani and J.-P. Tillich, Polynomial Time Attack on Wild McEliece Over Quadratic Extensions. To Appear EUROCRYPT 2014. Copenhagen (Denmark).

Sujet proposé par *Gilles Zémor*.

Étude et mise en œuvre de l'attaque de Bleichenbacher sur le procédé de padding PKCS# 1.

il s'agit d'une attaque maintenant célèbre, à chiffré choisi, où la réponse de l'oracle (ou en pratique du serveur) est 0 ou 1 (en pratique : message d'erreur ou absence de message d'erreur). L'attaque adaptative à chiffré choisi permet à terme de décrypter un cryptogramme cible.

Référence principale :

http://archiv.infsec.ethz.ch/education/fs08/secsem/Bleichenbacher98.pdf