Curriculum Vitae

Antoine JOUX

Né le 12/05/1967 à Amiens (80)
Antoine.Joux@m4x.org

Formation

— *Habilitation à Diriger des Recherches.* Université Denis Diderot, 2000.
— *La réduction de réseaux en cryptographie.* Thèse en Informatique, mention *Très Honorable avec les félicitations du jury*, Ecole Polytechnique, 1993.
— DEA Informatique mathématique et applications, Ecole Polytechnique, 1990.
— Diplome de l'Ecole Polytechnique, 1989. Promotion X86.

Poste actuel (depuis 01/2020)

— Chercheur titulaire au CISPA Helmholtz Center for Information Security, Saarbrucken, Allemagne

Postes précédents

— *Chaire de Cryptologie*, Fondation de Sorbonne Université (anciennement UPMC). 2013–2019.
— *Expert Senior* chez CryptoExperts, Paris. 2012–2015.
— *Professeur associé à temps partiel* (PAST), Université de Versailles–Saint-Quentin. 2004–2013.
— Direction Générale de l'Armement (DGA). 1993–2012.
— *Sous-directeur scientifique*, Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), devenue ANSSI. 1998–2004

Distinctions et récompenses

— Prix Gödel 2013. Co-attribué avec Dan Boneh et Matt Franklin pour l'introduction d'une sous-discipline de la cryptographie à clef publique: *la cryptographie basée sur les couplages bilinéaires.*
— Fellow de l'IACR 2014.
" For contributions to the science of cryptology, the co-invention of Pairing-Based Cryptography, and outstanding work on cryptanalysis of hash functions and discrete logarithms." L'IACR (International Association for Cryptologic Research) est une société savante qui a pour but de promouvoir la recherche internationale en Cryptologie et qui organise, en particulier, les principales conférences du domaine.
— ERC advanced grant, ALMACRYPT. Ce financement européen m'a été accordé en 2015 sur le thème de la cryptographie algorithmique et mathématique.

— Crypto'20, Test of Time award for *Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions.*

— Chevalier de l'Ordre National du Mérite.
— Chevalier dans l'Ordre des Palmes Académiques.

Présentation du domaine de recherche

Depuis ma thèse, mes travaux de recherche portent sur la cryptographie, et principalement la cryptanalyse. Plus concrètement, il s'agit d'étudier des propositions de systèmes cryptologiques (chiffrement, signature, ...) pour détecter des faiblesses susceptibles de remettre en cause leur sécurité.

Le contexte: Cryptographie, Cryptologie, Crypto, ...?

La cryptographie est un concept ancien, que l'on peut faire remonter à l'antiquité. A l'origine, il s'agissait d'établir des conventions d'écriture secrètes, permettant de communiquer des messages d'importance stratégique, sans risquer qu'ils ne soient lus par des tiers. Cette cryptographie historique n'était pas une discipline scientifique, mais plutôt un ensemble de techniques variées et leur maîtrise a pu s'approcher d'une forme d'art. Par

ailleurs, elle souffrait d'une énorme limitation, à savoir la capacité limitée des opérateurs utilisant le système à appliquer les transformations parfois complexes nécessaires pour chiffrer ou déchiffer les messages.

Au début du XXème siècle, la mécanisation puis l'informatisation des systèmes de chiffrement ont permis de complexifier très largement l'éventail des méthodes accessibles. En parallèle, les travaux de Shannon sur la théorie de l'information ont offerts la première analyse scientifique de la question et ont permis de montrer l'existence d'un système de chiffrement, appelé *One-Time pad* ou chiffrement de Vernam, permettant d'offrir une confidentialité absolue sous l'hypothèse [1] que l'émetteur et le destinataire aient préalablement convenu d'un secret commun parfaitement aléatoire et plus long que tous les messages à transmettre.

Dans la plupart des cas pratiques, le résultat de Shannon pose une impossibilité théorique qui ne peut se contourner qu'en s'appuyant sur la théorie de la complexité algorithmique. Ainsi, la cryptographie moderne repose sur l'hypothèse fondamentale qu'il existe des problèmes calculatoires dont la solution est facile à vérifier mais difficile à trouver. En particulier, il est impératif que [2] $P \neq NP$ pour pouvoir construire des systèmes cryptographiques asymptotiquement sûrs.

De façon peut-être paradoxale, ce besoin de recourir à l'existence de problèmes difficiles a permis le développement de la cryptographie, en permettant dans un premier temps l'apparition de la cryptographie à clef publique. Ce concept a été proposé en 1976 par Diffie et Hellman et concrétisé l'année suivante par l'invention du système de Rivest-Shamir-Adleman (RSA) qui repose sur la possibilité de construire rapidement de très grands nombres composés muni de leur factorisation, tout en ayant l'assurance qu'à partir du seul nombre composé, retrouver la factorisation soit absolument impossible en pratique.

Avec l'invention de la cryptographie à clef publique, c'est la cryptologie, c'est-à-dire la science de la cryptographie, qui a fait son apparition. Dans les décennies qui ont suivi, l'explosion de l'informatique a permis à la cryptographie en tant que technique de se développer très rapidement et de devenir un ingrédient essentiel de la sécurité de nos systèmes d'informations actuels. Dans le même temps, le développement de la cryptologie a conduit à l'introduction de nombreuses fonctionnalités avancées autour du calcul distribué sécurisé. A titre d'exemple, citons les cryptomonnaies qui ont connu un énorme développement dans la dernière décennie. À un point tel, que pour certaines personnes le mot *crypto* est devenu synonyme de cryptomonnaie, alors que jusque là, cette abbréviation signifiait plutôt cryptographie. En conséquence, nous éviterons l'usage de ce terme.

La cryptanalyse

Même si cela peut paraître surprenant à première vue, la recherche en cryptanalyse est absolument essentielle pour permettre de disposer de systèmes cryptographiques sûrs. En effet, en recherchant en permanence des failles, on peut éliminer progressivement les systèmes vulnérables pour ne garder que les plus sûrs. En l'absence de tels travaux de cryptanalyse académique, on s'exposerait au risque d'attaque par des adversaires disposant des moyens suffisants pour conduire ces mêmes recherches en secret. Bien sûr, l'existence d'une recherche ouverte en cryptanalyse ne peut pas complètement protéger contre le risque d'attaques secrètes très avancées mais elle en réduit considérablement la probabilité.

Concrètement, en cryptanalyse, on commence par identifier les ressources mobilisables dans une attaque et l'objectif à atteindre pour considérer que l'adversaire a obtenu un avantage contre le cryptosystème. Comme exemple de ressources, on trouve le nombre de messages chiffrés que l'adversaire peut obtenir, souvent en connaissant le clair associé (ou même en le choisissant) et les moyens de calcul qu'il est autorisé à mobiliser pour l'attaque. Dans un scénario plus compliqué, il peut y avoir d'autres types de ressources, comme le nombre de participants que l'adversaire peut corrompre dans un protocole multipartite. Comme but de l'attaque, on choisit souvent quelque chose de minimal, par exemple, demander que l'adversaire soit capable de faire la différence entre un message correctement chiffré et de l'aléa pur. Cela peut sembler biaiser le jeu en sa faveur, mais c'est une excellente méthode pour ne finalement garder que les systèmes les plus sûrs.

Ensuite, on ramène l'attaque du cryptosystème à l'étude et la résolution d'un problème calculatoire, qui devrait être difficile pour que le système soit sûr. Selon les cas, ce problème peut-être soit une construction

1. Irréaliste dans la plupart des contextes envisageables.
2. Ce problème de complexité reste ouvert et constitue même l'un des problèmes de la fondation Clay, cf `https://www.claymath.org/millennium-problems`.

ad'hoc, soit un problème d'origine mathématique bien identifié. Une fois ce problème sous-jacent identifié, il s'agit de développer des méthodes de calcul permettant de le résoudre. Certaines cryptanalyses nécessitent des moyens de calcul plutôt faibles. Pour autant, elles ne sont pas toujours faciles à découvrir et nécessite parfois des années d'analyse. Selon les cas, la difficulté de l'analyse ne se situe pas au même endroit. Elle peut provenir soit de la découverte d'une modélisation astucieuse permettant de ramener la cryptanalyse à un problème facile à résoudre soit de l'étude algorithmique ou mathématique pour résoudre un problème clairement identifié depuis le début.

D'ailleurs, l'objectif de ce que l'on appelle la sécurité prouvable consiste justement à garantir l'équivalence entre la sécurité d'un système cryptographique et un problème de calcul parfaitement spécifié. Il est donc tout à fait légitime de chercher à cryptanalyser des systèmes prouvés sûrs. En premier lieu, le problème sous-jacent peut s'avérer être facile à résoudre. En second lieu, les preuves de sécurité sont complexes et difficiles à vérifier et peuvent parfois être fausses – ce qui justifie le recours à des techniques de vérification formelle de preuves pour éviter de telles erreurs. Enfin, la preuve ne couvre que les scenarii d'attaques imaginés par le concepteur, il est donc possible que certaines approches réalistes ne soient pas couvertes.

Une des spécificités majeures que l'on rencontre également en cryptanalyse est que la définition de la notion d'attaque valide varie fortement selon le contexte. Dans un cadre académique, on considère comme valide toute attaque présentant un avantage calculatoire significatif par rapport au niveau de sécurité annoncé par les concepteurs – le plus souvent, celui-ci est le coût d'une recherche exhaustive, qui consiste simplement à essayer tous les secrets possibles. Comme les tailles de clefs et de paramètres sont choisies pour rendre cette approche totalement infaisable pour les ordinateurs actuels [3] une méthode qui ne bat la sécurité annoncée que d'un facteur 100 par exemple, ne permettra donc pas d'annihiler la sécurité pratique du système. Elle sera pourtant considérée comme une faille importante par le monde académique, ce qui justifiera de plutôt se tourner vers d'autres systèmes qu'un effort de cryptanalyse soutenu n'a pas permis d'affaiblir ainsi. En revanche, une fois les cryptosystèmes déployés dans des applications ou systèmes sécurisé, la définition d'attaque valide a tendance à changer. Ainsi, les industriels et les développeurs considèrent qu'un système devient vulnérable lorsqu'il est susceptible d'être attaqué en pratique (même si cela nécessite des supercalculateurs de très grandes tailles ou des millions de machines en réseau). Cela est logique, car il est coûteux de changer un système déjà en service, alors qu'éliminer un candidat plus faible que les autres en amont ne coutera presque rien.

En conséquence, pour les systèmes déjà déployés, un aspect très important de la cryptanalyse consiste à démontrer les performances pratiques des attaques proposées en réalisant des prototypes effectifs capables d'illustrer les tailles atteignables avec de gros moyens de calcul. Typiquement, dans le cas de problèmes mathématiques comme la factorisation ou le logarithme discret, cette illustration s'exprime par l'obtention de records de calcul pour des nombres de plus en plus gros. Il est ainsi possible pour les développeurs et les utilisateurs de savoir à quel moment le retrait du marché d'un produit obsolète devient indispensable. Pour d'autres systèmes cryptographiques, le principe général reste le même, en revanche, la notion de taille à utiliser pour juger de l'avancée des attaques est un peu plus floue, ce qui conduit parfois à devoir retirer des systèmes devenus trop peu sûrs en urgence.

En résumé, la cryptanalyse est un domaine assez complexe à définir, qui nécessite une bonne compréhension de la cryptographie et de ses objectifs, afin d'identifier des vulnérabilité potentielles et de les traduire en termes de problèmes calculatoires, ainsi qu'une connaissance assez large de méthodes algorithmiques et mathématiques permettant de résoudre les problmes en question. La capacité à programmer efficacement les attaques ainsi obtenues vient en complément et permet de complétement en illustrer l'impact pratique.

Pour terminer, notons que concernant les ressources utilisables, une évolution assez récente est la prise en compte de l'informatique quantique qui introduit une nouvelle dimension dans les attaques possibles. Il s'agit de savoir si l'attaquant est supposé disposer d'ordinateurs quantiques pour mettre en place ses attaques et s'il peut ou non poser des questions quantiques au cryptosystème à attaquer. La prise en compte de ce type d'ordinateur modifie profondément les attaques réalisables et rend obsolète certains problèmes qui deviennent faciles pour un ordinateur quantique. En revanche, l'illustration des attaques quantiques est actuellement beaucoup plus difficiles, puisque les machines nécessaires ne sont pas encore accessibles.

3. Ou même envisageables dans un avenir prévisible pour un adversaire doté de moyens financiers démesurés

Liste de publications

[1] A. Joux and J. Stern. Improving the critical density of the Lagarias-Odlyzko attack against subset sum problems. In *Fundamentals of Computation Theory*, pages 258–264, Berlin, Heidelberg. Springer, 1991.

[2] Y. M. Chee, A. Joux, and J. Stern. The cryptanalysis of a new public-key cryptosystem based on modular knapsacks. In *CRYPTO '91*, pages 204–212, Berlin, Heidelberg. Springer, 1992.

[3] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2(2), 1992.

[4] J. Kowalski, M. Martin, J. Stern, and A. Joux. Encryption and authentication method and circuit for synchronous smart card. Patent FR 9213913A, 1992.

[5] A. Joux. A fast parallel lattice reduction algorithm. In *Proceedings of the Second Gauss Symposium (Munich)*, 1993.

[6] A. Joux and J. Stern. Cryptanalysis of another knapsack cryptosystem. In *ASIACRYPT '91*, pages 470–476, Berlin, Heidelberg. Springer, 1993.

[7] A. Joux and F. Morain. Character sums linked to elliptic-curves with complex multiplication. *Journal of Number Theory*, 55(1):108–128, 1995.

[8] A. Joux and L. Granboulan. A practical attack against knapsack based hash functions. In *EUROCRYPT'94*, pages 58–66, Berlin, Heidelberg. Springer, 1995.

[9] J. Friedman, A. Joux, Y. Roichman, J. Stern, and J. P. Tillich. The action of a few random permutations on r-tuples and an application to cryptography. In *STACS 96*, pages 375–386, Berlin, Heidelberg. Springer, 1996.

[10] F. Chabaud and A. Joux. Differential collisions in SHA-0. In *CRYPTO'98*, 1998.

[11] J. Friedman, A. Joux, Y. Roichman, J. Stern, and J.-P. Tillich. The action of a few permutations on r-tuples is quickly transitive. *Random Structures & Algorithms*, 12(4):335–350, 1998.

[12] A. Joux and J. Stern. Lattice reduction: a toolbox for the cryptanalyst. *J. Cryptology*, 11(3), 1998.

[13] D. Boneh, A. Joux, and P. Q. Nguyen. Why textbook ElGamal and RSA encryption are insecure. In *ASIACRYPT*, 2000.

[14] É. Jaulmes and A. Joux. A chosen-ciphertext attack against NTRU. In *CRYPTO 2000*, pages 20–35. Springer, 2000.

[15] É. Jaulmes and A. Joux. A NICE cryptanalysis. In B. Preneel, editor, *EUROCRYPT 2000*, pages 382–391, Berlin, Heidelberg. Springer, 2000.

[16] A. Joux. A one round protocol for tripartite Diffie–Hellman. In *Algorithmic Number Theory*, pages 385–393. Springer, 2000.

[17] H. Gilbert, H. Handschuh, A. Joux, and S. Vaudenay. A statistical attack on RC6. In *Fast Software Encryption*, pages 64–74, Berlin, Heidelberg. Springer, 2001.

[18] É. Jaulmes and A. Joux. Cryptanalysis of PKP: a new approach. In *Public Key Cryptography*, pages 165–172, Berlin, Heidelberg. Springer, 2001.

[19] A. Joux and R. Lercier. "Chinese & Match", an alternative to Atkin's "Match and Sort" method used in the SEA algorithm. *Mathematics of computation*, 70:827–836, 2001.

[20] P. Chose, A. Joux, and M. Mitton. Fast correlation attacks: an algorithmic point of view. In *EUROCRYPT*. Springer, 2002.

[21] É. Jaulmes, A. Joux, and F. Valette. On the security of randomized CBC-MAC beyond the birthday paradox limit a new construction. In *Fast Software Encryption*, pages 237–251. Springer, 2002.

[22] A. Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. In *Algorithmic Number Theory*, pages 20–32. Springer, 2002.

[23] A. Joux and R. Lercier. The function field sieve is quite special. In *Algorithmic Number Theory*, pages 431–445. Springer, 2002.

[24] A. Joux, G. Martinet, and F. Valette. Blockwise-adaptive attackers revisiting the (in)security of some provably secure encryption modes: CBC, GEM, IACBC. In *CRYPTO 2002*, pages 17–30. Springer, 2002.

[25] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *CRYPTO*. Springer, 2003.

[26] A. Joux. Cryptanalysis of the EMD mode of operation. In *EUROCRYPT 2003*, pages 1–16, Berlin, Heidelberg. Springer, 2003.

[27] A. Joux and R. Lercier. Improvements to the general Number Field Sieve for discrete logarithms in prime fields. a comparison with the Gaussian integer method. *Mathematics of computation*, 72(242), 2003.

[28] A. Joux and F. Muller. Loosening the KNOT. In *Fast Software Encryption*, pages 87–99, Berlin, Heidelberg. Springer, 2003.

[29] A. Joux and K. Nguyen. Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. *J. Cryptology*, 16(4), 2003.

[30] A. Joux, G. Poupard, and J. Stern. New attacks against standardized MACs. In *Fast Software Encryption*, pages 170–181, Berlin, Heidelberg. Springer, 2003.

[31] J.-S. Coron and A. Joux. Cryptanalysis of a provably secure cryptographic hash function. Cryptology ePrint Archive, Report 2004/013, 2004. https://eprint.iacr.org/2004/013.

[32] P.-A. Fouque, A. Joux, G. Martinet, and F. Valette. Authenticated on-line encryption. In *Selected Areas in Cryptography*, pages 145–159, Berlin, Heidelberg. Springer, 2004.

[33] A. Joux. A one round protocol for tripartite Diffie–Hellman. *J. Cryptology*, 17(4), 2004.

[34] A. Joux. Multicollisions in iterated hash functions. Application to cascaded constructions. In *CRYPTO 2004*. Springer, 2004.

[35] A. Joux and F. Muller. A chosen iv attack against Turing. In *Selected Areas in Cryptography*, pages 194–207, Berlin, Heidelberg. Springer, 2004.

[36] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, and W. Jalby. Collisions of SHA-0 and reduced SHA-1. In *EUROCRYPT*. Springer, 2005.

[37] P.-A. Fouque, A. Joux, and G. Poupard. Blockwise adversarial model for on-line ciphers and symmetric encryption schemes. In *Selected Areas in Cryptography*, pages 212–226, Berlin, Heidelberg. Springer, 2005.

[38] A. Joux, S. Kunz-Jacques, F. Muller, and P.-M. Ricordel. Cryptanalysis of the tractable rational map cryptosystem. In *Public Key Cryptography 2005*, pages 258–274, Berlin, Heidelberg. Springer, 2005.

[39] A. Joux and F. Muller. Two attacks against the HBB stream cipher. In *Fast Software Encryption*, pages 330–341, Berlin, Heidelberg. Springer, 2005.

[40] L. Granboulan, A. Joux, and J. Stern. Inverting HFE is quasipolynomial. In *CRYPTO*. Springer, 2006.

[41] A. Joux. Authentication failures in NIST version of GCM. Technical report, NIST Comment, 2006.

[42] A. Joux and P. Delaunay. Galois LFSR, embedded devices and side channel weaknesses. In *INDOCRYPT 2006*, pages 436–451, Berlin, Heidelberg. Springer, 2006.

[43] A. Joux and R. Lercier. Counting points on elliptic curves in medium characteristic. Cryptology ePrint Archive, Report 2006/176, 2006. https://eprint.iacr.org/2006/176.

[44] A. Joux and R. Lercier. The Function Field Sieve in the medium prime case. In *EUROCRYPT*. Springer, 2006.

[45] A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren. The Number Field Sieve in the medium prime case. In *CRYPTO*. Springer, 2006.

[46] A. Joux and F. Muller. Chosen-ciphertext attacks against MOSQUITO. In *Fast Software Encryption*, pages 390–404, Berlin, Heidelberg. Springer, 2006.

[47] A. Bauer and A. Joux. Toward a rigorous variation of Coppersmith's algorithm on three variables. In M. Naor, editor, *EUROCRYPT 2007*, pages 361–378, Berlin, Heidelberg. Springer, 2007.

[48] A. Joux and R. Lercier. Algorithmes pour résoudre le problème du logarithme discret dans les corps finis. In *Nouvelles Méthodes Mathématiques en Cryptographie, Fascicules Journées Annuelles*, pages 23–53. Société Mathématique de France, 2007.

[49] A. Joux, D. Naccache, and E. Thomé. When e-th roots become easier than factoring. In K. Kurosawa, editor, *ASIACRYPT 2007*, pages 13–28, Berlin, Heidelberg. Springer, 2007.

[50] A. Joux and T. Peyrin. Hash functions and the (amplified) boomerang attack. In *CRYPTO*. Springer, 2007.

[51] A. Joux and J.-R. Reinhard. Overtaking VEST. In *Fast Software Encryption*, pages 58–72, Berlin, Heidelberg. Springer, 2007.

[52] P. Delaunay and A. Joux. Yet another attack on vest. In *AFRICACRYPT 2008*, pages 221–235, Berlin, Heidelberg. Springer, 2008.

[53] S. Ionica and A. Joux. Another approach to pairing computation in Edwards coordinates. In *INDOCRYPT*. Springer, 2008.

[54] C. Berbain, H. Gilbert, and A. Joux. Algebraic and correlation attacks against linearly filtered non linear feedback shift registers. In *Selected Areas in Cryptography*, pages 184–198, Berlin, Heidelberg. Springer, 2009.

[55] G. Castagnos, A. Joux, F. Laguillaumie, and P. Q. Nguyen. Factoring pq2 with quadratic forms: nice cryptanalyses. In *ASIACRYPT 2009*, pages 469–486, Berlin, Heidelberg. Springer, 2009.

[56] J.-S. Coron, A. Joux, I. Kizhvatov, D. Naccache, and P. Paillier. Fault attacks on RSA signatures with partially unknown messages. In *Cryptographic Hardware and Embedded Systems - CHES 2009*, pages 444–456, Berlin, Heidelberg. Springer, 2009.

[57] A. Joux, editor. *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, 2009. Springer.

[58] A. Joux. *Algorithmic cryptanalysis*. Chapman and Hall/CRC, 2009.

[59] A. Joux. Introduction to identity-based cryptography. In M. Joye and G. Neven, editors, *Identity-Based Cryptography*. Volume 2, Cryptology and Information Security Series, chapter 1. IOS Press, 2009.

[60] A. Joux, R. Lercier, D. Naccache, and E. Thomé. Oracle-assisted static Diffie-Hellman is easier than discrete logarithms. In M. G. Parker, editor, *Cryptography and Coding*, pages 351–367, Berlin, Heidelberg. Springer, 2009.

[61] A. Joux and S. Lucks. Improved generic algorithms for 3-collisions. In *ASIACRYPT 2009*. Springer, 2009.

[62] J.-C. Faugère, A. Joux, L. Perret, and J. Treger. Cryptanalysis of the hidden matrix cryptosystem. In *LATINCRYPT 2010*, pages 241–254, Berlin, Heidelberg. Springer, 2010.

[63] N. Howgrave-Graham and A. Joux. New generic algorithms for hard knapsacks. In *EUROCRYPT*. Springer, 2010.

[64] S. Ionica and A. Joux. Pairing computation on elliptic curves with efficiently computable endomorphism and small embedding degree. In *Pairing-Based Cryptography 2010*, pages 435–449, Berlin, Heidelberg. Springer, 2010.

[65] S. Ionica and A. Joux. Pairing the volcano. In *Algorithmic Number Theory*, pages 201–218, Berlin, Heidelberg. Springer, 2010.

[66] A. Joux. On the security of blockwise secure modes of operation beyond the birthday bound. *IEEE Transactions on Information Theory*, 56(3):1239–1246, 2010.

[67] A. Becker, J. Coron, and A. Joux. Improved generic algorithms for hard knapsacks. In *EUROCRYPT*. Springer, 2011.

[68] J.-S. Coron, A. Joux, A. Mandal, D. Naccache, and M. Tibouchi. Cryptanalysis of the RSA subgroup assumption from tcc 2005. In *Public Key Cryptography 2011*, pages 147–155. Springer, 2011.

[69] A. Joux, editor. *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, 2011. Springer.

[70] A. Joux and R. Lercier. *Encyclopedia of cryptography and security*. In Springer, 2011. Chapter Number Field Sieve for DLP, pages 867–873.

[71] A. Joux and V. Vitse. A variant of the F4 algorithm. In *Topics in Cryptology – CT-RSA 2011*, pages 356–375. Springer, 2011.

[72] A. Becker, A. Joux, A. May, and A. Meurer. Decoding random binary linear codes in $2^{n/20}$: how $1+1=0$ improves information set decoding. In *EUROCRYPT*. Springer, 2012.

[73] C. Bouillaguet, P.-A. Fouque, A. Joux, and J. Treger. A family of weak keys in HFE and the corresponding practical key-recovery. *Journal of Mathematical Cryptology*, 5(3-4):247–275, 2012.

[74] A. Joux. A tutorial on high performance computing applied to cryptanalysis. In *EUROCRYPT 2012*, pages 1–7. Springer, 2012.

[75] A. Joux and V. Vitse. Cover and decomposition index calculus on elliptic curves made practical — Application to a previously unreachable curve over $\mathbb{F}_{p^6}$. In *EUROCRYPT*. Springer, 2012.

[76] M. Medwed, F.-X. Standaert, and A. Joux. Towards super-exponential side-channel security with efficient leakage-resilient PRFs. In *Cryptographic Hardware and Embedded Systems 2012*, pages 193–212. Springer, 2012.

[77] P.-A. Fouque, A. Joux, and C. Mavromati. Multi-user collisions: applications to discrete logs, Even-Mansour and Prince. *IACR Cryptology ePrint Archive*, 2013:761, 2013. Accepted at Asiacrypt'14.

[78] P.-A. Fouque, A. Joux, and M. Tibouchi. Injective encodings to elliptic curves. In *Information Security and Privacy*, pages 203–218, Berlin, Heidelberg. Springer, 2013.

[79] A. Joux. A new index calculus algorithm with complexity $L(1/4+o(1))$ in small characteristic. In *Selected Areas in Cryptography*. Springer, 2013.

[80] A. Joux. Faster index calculus for the medium prime case, Application to 1175-bit and 1425-bit fields. In *EUROCRYPT*. Springer, 2013.

[81] A. Joux and C. Pierrot. The special number field sieve in $\mathbb{F}_{p^n}$ – application to pairing-friendly constructions. In *Pairing-Based Cryptography*. Springer, 2013.

[82] A. Joux and V. Vitse. Elliptic curve discrete logarithm problem over small degree extension fields. application to the static Diffie–Hellman problem. *Journal of Cryptology*, 26:119–143, 2013.

[83] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *EUROCRYPT*. Springer, 2014.

[84] A. Becker, N. Gama, and A. Joux. A sieve algorithm based on overlattices. *LMS Journal of Computation and Mathematics*, 17, Special Issue A, Jan. 2014.

[85] J.-C. Faugère, L. Huot, A. Joux, G. Renault, and V. Vitse. Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus. In *EUROCRYPT*. Springer, 2014.

[86] J. Gutierrez, A. Ibeas, and A. Joux. Recovering a sum of two squares decomposition. *Journal of Symbolic Computation*, 64:16–21, 2014. Mathematical and computer algebra techniques in cryptology.

[87] A. Joux, A. Odlyzko, and C. Pierrot. *The past, evolving present, and future of the discrete logarithm*. In *Open Problems in Mathematics and Computational Science*. Springer, 2014, pages 5–36.

[88] A. Joux and C. Pierrot. Improving the polynomial time precomputation of Frobenius representation discrete logarithm algorithms – Simplified setting for small characteristic finite fields. In *ASIACRYPT*. Springer, 2014.

[89] E. Biham, R. Chen, and A. Joux. Cryptanalysis of SHA-0 and reduced SHA-1. *J. Cryptology*, 28(1):110–160, 2015.

[90] A. Joux and C. Pierrot. Discrétion assurée ? *Gazette des mathématiciens*, 144, 2015. Société Mathématique de France.

[91] A. Joux and A. Rojat. Security ranking among assumptions within the uber assumption framework. In *Information Security*, pages 391–406. Springer, 2015.

[92] A. Gélin and A. Joux. Reducing number field defining polynomials: an application to class group computations. *LMS Journal of Computation and Mathematics*, 19(A):315–331, 2016.

[93] A. Joux and C. Pierrot. Technical history of discrete logarithms in small characteristic finite fields - the road from subexponential to quasi-polynomial complexity. *Des. Codes Cryptogr.*, 78(1), 2016.

[94] A. Joux. Discrete logarithms in small characteristic finite fields: a survey of recent advances (invited talk). In *STACS*, 2017.

[95] A. Joux and V. Vitse. A crossbred algorithm for solving boolean polynomial systems. In *NuTMiC*, 2017.

[96] D. Aggarwal, A. Joux, A. Prakash, and M. Santha. A new public-key cryptosystem via Mersenne numbers. In *CRYPTO*. Springer, 2018.

[97] U. Chabaud, E. Diamanti, D. Markham, E. Kashefi, and A. Joux. Optimal quantum-programmable projective measurement with linear optics. *Phys. Rev. A*, 98:062318, 6, 2018.

[98] D. Goudarzi, A. Joux, and M. Rivain. How to securely compute with noisy leakage in quasilinear complexity. In T. Peyrin and S. Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 547–574, Cham. Springer International Publishing, 2018. ISBN: 978-3-030-03329-3.

[99] A. Joux, A. Nitaj, and T. Rachidi, editors. *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*, volume 10831 of *Lecture Notes in Computer Science*, 2018. Springer.

[100] F. Göloglu and A. Joux. A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms. *Math. Comput.*, 88(319), 2019.

[101] A. Joux and A. K. Narayanan. Drinfeld modules are not for isogeny based cryptography. Cryptology ePrint Archive, Report 2019/1329, 2019. `https://eprint.iacr.org/2019/1329`.

[102] A. Joux and C. Pierrot. Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms. Cryptology ePrint Archive, Report 2019/782, 2019. `https://eprint.iacr.org/2019/782`.

[103] T. Espitau and A. Joux. Certified lattice reduction. *Advances in Mathematics of Communications*, 14(1):137–159, 2020.

[104] T. Espitau, A. Joux, and N. Kharchenko. On a hybrid approach to solve small secret LWE. Cryptology ePrint Archive, Report 2020/515, 2020. `https://eprint.iacr.org/2020/515`.

[105] R. Granger and A. Joux. Computing discrete logarithms. In J. Bos and M. Stam, editors, *Computational Cryptography — Algorithmic Aspects of Cryptology*. London Math. Society, 2021.

[106] A. Joux and C. Pierrot. *Nearly sparse linear algebra and application to discrete logarithms computations*. In *Contemporary Developments in Finite Fields and Applications*, pages 119–144.