Publications du projet PROUVÉ

September 12, 2008

Ce document contient la liste complète de toutes les publications des membres du projet PROUVÉ qui ont été produites dans le contexte du projet. Nous nous limitons ici aux publications parues dans des livres, journaux, conférences ou ateliers internationales ou nationales. Les rapports techniques sont omis, ainsi que les thèses. La liste des thèses soutenues est donné dans le rapport final.

References

[1] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. The AVISPA Tool for the automated validation of internet security protocols and applications. In K. Etessami and S. Rajamani, editors, *17th International Conference on Computer Aided Verification, CAV'2005*, volume 3576 of *Lecture Notes in Computer Science*, pages 281–285, Edinburgh, Scotland, 2005. Springer.

[2] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Combining algorithms for deciding knowledge in security protocols. In Franck Wolter, editor, *Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)*, volume 4720 of *Lecture Notes in Artificial Intelligence*, pages 103–117, Liverpool, UK, September 2007. Springer.

[3] Mathieu Baudet. Random polynomial-time attacks and Dolev-Yao models. In Siva Anantharaman, editor, *Proceedings of the Workshop on Security of Systems: Formalism and Tools (SASYFT'04)*, Orléans, France, June 2004.

[4] Mathieu Baudet. Deciding security of protocols against off-line guessing attacks. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25, Alexandria, Virginia, USA, November 2005. ACM Press.

[5] Mathieu Baudet. Random polynomial-time attacks and Dolev-Yao models. *Journal of Automata, Languages and Combinatorics*, 11(1):7–21, 2006.

[6] Mathieu Baudet, Véronique Cortier, and Steve Kremer. Computationally sound implementations of equational theories against passive adversaries. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *Lecture Notes in Computer Science*, pages 652–663, Lisboa, Portugal, July 2005. Springer.

[7] Vincent Bernat. *Théories de l'intrus pour la vérification des protocoles cryptographiques.* Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2006.

[8] Vincent Bernat and Hubert Comon-Lundh. Normal proofs in intruder theories. In Mitsu Okada and Ichiro Satoh, editors, *Revised Selected Papers of the 11th Asian Computing Science Conference (ASIAN'06)*, volume 4435 of *Lecture Notes in Computer Science*, pages 151–166, Tokyo, Japan, January 2008. Springer.

[9] Y. Boichut, N. Kosmatov, and L. Vigneron. Validation of Prouve protocols using the automatic tool TA4SP. In *Proceedings of 3rd Taiwanese-French Conference on Information Technology (TFIT)*, pages 467–480, Nancy, France, March 2006.

[10] M. S. Bouassida, N. Chridi, I. Chrisment, O. Festor, and L. Vigneron. Automatic Verification of a Key Management Architecture for Hierarchical Group Protocols. In F. Cuppens and H. Debar, editors, *Proceedings of 5th Conference on Security and Network Architectures (SAR)*, pages 381–397, Seignosse, France, June 2006.

[11] L. Bozga, Y. Lakhnech, and M. Périn. Abstract interpretation for secrecy using patterns. In H. Garavel and J. Hatcliff, editors, *Proceedings of TACAS'03 - 9th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Warsaw, Poland*, volume 2619 of *LNCS*. Springer, April 2003.

[12] L. Bozga, Y. Lakhnech, and M. Périn. Hermes: An automatic tool for verification of secrecy in security protocols. In Jr. W. A. Hunt and F. Somenzi, editors, *Proceedings of CAV'03 - 15th International Conference on Computer Aided Verification, Boulder, Colorado*, volume 2725 of *LNCS*. Springer-Verlag, July 2003.

[13] Liana Bozga, Cristian Ene, Romain Janvier, Yassine Lakhnech, Laurent Mazaré, and Michaël Périn. Automatic verification of security properties based on abstractions. In Clarke et al. [29], pages 23–53.

[14] Liana Bozga, Cristian Ene, and Yassine Lakhnech. On the existence of an effective and complete inference system for cryptographic protocols. In Walukiewicz [71], pages 42–57.

[15] Liana Bozga, Cristian Ene, and Yassine Lakhnech. A symbolic decision procedure for cryptographic protocols with time stamps (extended abstract). In Gardner and Yoshida [50], pages 177–192.

[16] Liana Bozga, Cristian Ene, and Yassine Lakhnech. A symbolic decision procedure for cryptographic protocols with time stamps. *J. Log. Algebr. Program.*, 65(1):1–35, 2005.

[17] Liana Bozga, Yassine Lakhnech, and Michaël Périn. Pattern-based abstraction for verifying secrecy in protocols. *STTT*, 8(1):57–76, 2006.

[18] Emmanuel Bresson, Yassine Lakhnech, Laurent Mazaré, and Bogdan Warinschi. A generalization of ddh with applications to protocol analysis and computational soundness. In Menezes [64], pages 482–499.

[19] Jeremy W. Bryans, Maciej Koutny, Laurent Mazare, and Peter Y.A. Ryan. Opacity generalised to transition systems. Technical Report TR-2004-25, Verimag, Centre Équation, 38610 Gières, December 2004.

[20] Sergiu Bursuc, Hubert Comon-Lundh, and Stéphanie Delaune. Associative-commutative deducibility constraints. In Wolfgang Thomas and Pascal Weil, editors, *Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07)*, volume 4393 of *Lecture Notes in Computer Science*, pages 634–645, Aachen, Germany, February 2007. Springer.

[21] Sergiu Bursuc, Hubert Comon-Lundh, and Stéphanie Delaune. Deducibility constraints, equational theory and electronic money. In Hubert Comon-Lundh, Claude Kirchner, and Hélène Kirchner, editors, *Rewriting, Computation and Proof — Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday*, volume 4600 of *Lecture Notes in Computer Science*, pages 196–212, Cachan, France, June 2007. Springer.

[22] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. In *Proceedings of the Logic In Computer Science Conference LICS'03*, pages 261–270, June 2003. Long version available as Technical Report RR-4697, INRIA, France.

[23] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents. In *Proceedings of the Foundations of Software Technology and Theoretical Computer Science, FSTTCS'03*, Lecture Notes in Computer Science. Springer, December 2003. Long version available as Christian-Albrecht Universität IFI-Report 0305, Kiel (Germany).

[24] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. *Theoretical Computer Science*, 338(1-3):247–274, June 2005.

[25] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with commuting public key encryption. In *Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA'2004*, volume 125:1 of *Electronic Notes in Theoretical Computer Science - ENTCS*, pages 55–66, Cork, Ireland, 2005.

[26] Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, and L. Vigneron. Extending the Dolev-Yao Intruder for Analyzing an Unbounded Number of Sessions. In M. Baaz, editor, *Computer Science Logic (CSL 03) and 8th Kurt Gödel Colloquium (8th KCG)*, volume 2803 of *Lecture Notes in Computer Science*, Vienna, Austria, August 2003. Springer.

[27] Y. Chevalier and L. Vigneron. Automated Unbounded Verification of Security Protocols. In Ed Brinksma and Kim Guldstrand Larsen, editors, *14th International Conference on Computer Aided Verification, CAV'2002*, volume 2404 of *Lecture Notes in Computer Science*, pages 324–337, Copenhagen (Denmark), July 2002. Springer.

[28] N. Chridi and L. Vigneron. Modélisation des propriétés de sécurité de protocoles de groupe. In *Actes du 1er Colloque sur les Risques et la Sécurité d'Internet et des Systèmes, CRiSIS*, pages 119–132, Bourges, France, October 2005. Élu meilleur papier de la conférence.

[29] Edmund M. Clarke, Marius Minea, and Ferucio Laurentiu Tiplea, editors. *Verification of Infinite-State Systems with Applications to Security, Proceedings of the NATO Advanced Research Workshop "Verification of Infinite State Systems with Applications to Security VISSAS 2005", Timisoara, Romania, March 17-22, 2005*, volume 1 of *NATO Security through Science Series D: Information and Communication Security*. IOS Press, 2006.

[30] Hubert Comon-Lundh. Intruder theories (ongoing work). In Igor Walukiewicz, editor, *Proceedings of the 7th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'04)*, volume 2987 of *Lecture Notes in Computer Science*, pages 1–4, Barcelona, Spain, March 2004. Springer. Invited talk.

[31] Hubert Comon-Lundh and Stéphanie Delaune. The finite variant property: How to get rid of some algebraic properties. In Jürgen Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307, Nara, Japan, April 2005. Springer.

[32] Hubert Comon-Lundh and Ralf Treinen. Easy intruder deductions. In Nachum Dershowitz, editor, *Verification: Theory and Practice, Essays Dedicated to Zohar Manna on the Occasion of His 64th Birthday*, volume 2772 of *Lecture Notes in Computer Science*, pages 225–242. Springer, February 2003. Invited paper.

[33] Véronique Cortier and Stéphanie Delaune. Deciding knowledge in security protocols for monoidal equational theories. In Nachum Dershowitz and Andrei Voronkov, editors, *Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)*, volume 4790 of *Lecture Notes in Artificial Intelligence*, pages 196–210, Yerevan, Armenia, October 2007. Springer.

[34] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.

[35] M. Daubignard, Romain Janvier, Yassine Lakhnech, and Laurent Mazaré. Game-based criterion partition applied to computational soundness of adaptive security. In Dimitrakos et al. [49], pages 47–64.

[36] Stéphanie Delaune. Intruder deduction problem in presence of guessing attacks. In Michaël Rusinowitch, editor, *Proceedings of the Workshop on Security Protocols Verification (SPV'03)*, pages 26–30, Marseilles, France, September 2003.

[37] Stéphanie Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, March 2006.

[38] Stéphanie Delaune. An undecidability result for AGh. *Theoretical Computer Science*, 368(1-2):161–167, December 2006.

[39] Stéphanie Delaune and Florent Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick McDaniel, editors, *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, Washington, D.C., USA, October 2004. ACM Press.

[40] Stéphanie Delaune and Florent Jacquemard. Narrowing-based constraint solving for the verification of security protocols. In Michael Kohlhase, editor, *Proceedings of the 18th International Workshop on Unification (UNIF'04)*, Cork, Ireland, July 2004.

[41] Stéphanie Delaune and Florent Jacquemard. A theory of dictionary attacks and its complexity. In *Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW'04)*, pages 2–15, Asilomar, Pacific Grove, California, USA, June 2004. IEEE Computer Society Press.

[42] Stéphanie Delaune and Florent Jacquemard. Decision procedures for the security of protocols with probabilistic encryption against offline dictionary attacks. *Journal of Automated Reasoning*, 36(1-2):85–124, January 2006.

[43] Stéphanie Delaune and Francis Klay. Vérification automatique appliquée à un protocole de commerce électronique. In *Actes des 6èmes Journées Doctorales Informatique et Réseau (JDIR'04)*, pages 260–269, Lannion, France, November 2004.

[44] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Receipt-freeness: Formal definition and fault attacks (extended abstract). In *Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005)*, Milan, Italy, September 2005.

[45] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, pages 28–39, Venice, Italy, July 2006. IEEE Computer Society Press.

[46] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying properties of electronic voting protocols. In *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE'06)*, pages 45–52, Cambridge, UK, June 2006.

[47] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In Michele Buglesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II*, volume 4052 of *Lecture Notes in Computer Science*, pages 132–143, Venice, Italy, July 2006. Springer.

[48] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis for monoidal equational theories. *Information and Computation*, 206(2-4):312–351, February-April 2008.

[49] Theodosis Dimitrakos, Fabio Martinelli, Peter Y. A. Ryan, and Steve A. Schneider, editors. *Formal Aspects in Security and Trust, Fourth International Workshop, FAST 2006, Hamilton, Ontario, Canada, August 26-27, 2006, Revised Selected Papers*, volume 4691 of *Lecture Notes in Computer Science*. Springer, 2007.

[50] Philippa Gardner and Nobuko Yoshida, editors. *CONCUR 2004 - Concurrency Theory, 15th International Conference, London, UK, August 31 - September 3, 2004, Proceedings*, volume 3170 of *Lecture Notes in Computer Science*. Springer, 2004.

[51] Jean Goubault-Larrecq. Deciding $\mathcal{H}_1$ by resolution. *Information Processing Letters*, 95(3):401–408, August 2005.

[52] Jean Goubault-Larrecq, Muriel Roger, and Kumar N. Verma. Abstraction and resolution modulo AC: How to verify Diffie-Hellman-like protocols automatically. *Journal of Logic and Algebraic Programming*, 64(2):219–251, August 2005.

[53] F. Jacquemard, M. Rusinowitch, and L. Vigneron. Tree Automata with Equality Constraints Modulo Equational Theories. In U. Furbach and N. Shankar, editors, *Proceedings of 3rd International Joint Conference on Automated Reasoning, IJCAR*, volume 4130 of *Lecture Notes in Artificial Intelligence*, pages 557–571, Seattle (WA), August 2006. Springer.

[54] R. Janvier, Y. Lakhnech, and L. Mazare. Completing the picture: Soundness of formal encryption in the presence of active adversaries. In *Proceedings of the 14th European Symposium on Programming (ESOP'05)*, LNCS. Springer-Verlag, 2005.

[55] Romain Janvier, Yassine Lakhnech, and Laurent Mazaré. Computational soundness of symbolic analysis for protocols using hash functions. *Electr. Notes Theor. Comput. Sci.*, 186:121–139, 2007.

[56] Steve Kremer and Mark D. Ryan. Analysis of an electronic voting protocol in the applied pi-calculus. In Mooly Sagiv, editor, *Programming Languages and Systems — Proceedings of the 14th European Symposium on Programming (ESOP'05)*, volume 3444 of *Lecture Notes in Computer Science*, pages 186–200, Edinburgh, U.K., April 2005. Springer.

[57] Pascal Lafourcade. Intruder deduction for the equational theory of *exclusive-or* with commutative and distributive encryption. In Maribel Fernández and Claude Kirchner, editors, *Proceedings of the 1st International Workshop on Security and Rewriting Techniques (SecReT'06)*, volume 171 of *Electronic Notes in Theoretical Computer Science*, pages 37–57, Venice, Italy, July 2007. Elsevier Science Publishers.

[58] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In Jürgen Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 308–322, Nara, Japan, April 2005. Springer.

[59] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. ACUNh: Unification and disunification using automata theory. In Jordi Levy, editor, *Proceedings of the 20th International Workshop on Unification (UNIF'06)*, pages 6–20, Seattle, Washington, USA, August 2006.

[60] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for the equational theory of Abelian groups with distributive encryption. *Information and Computation*, 205(4):581–623, April 2007.

[61] L. Mazaré. Decidability of opacity with non-atomic keys. In *Proc. of the second international Workshop on Formal Aspects in Security and Trust (FAST2004), Toulouse, France*, 2004.

[62] L. Mazaré. Satisfiability of Dolev-Yao constraints. In *Proc. of Automated Reasoning for Security Protocol Analysis(ARSPA'04)*, 2004.

[63] L. Mazaré. Using unification for opacity properties. In *Proc. of the Workshop on Issues in the Theory of Security (WITS'04)*, 2004.

[64] Alfred Menezes, editor. *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*. Springer, 2007.

[65] M. Rusinowitch and M. Turuani. Protocol Insecurity with Finite Number of Sessions and Composed Keys is NP-complete. *Theoretical Computer Science*, 299:451–475, April 2003.

[66] J. Santiago and L. Vigneron. Study for Automatically Analysing Non-repudiation. In *Actes du 1er Colloque sur les Risques et la Sécurité d'Internet et des Systèmes, CRiSIS*, pages 157–171, Bourges, France, October 2005.

[67] J. Santiago and L. Vigneron. Automatically Analysing Non-repudiation with Authentication. In *Proceedings of 3rd Taiwanese-French Conference on Information Technology (TFIT)*, pages 541–554, Nancy, France, March 2006.

[68] Mathieu Turuani. The CL-Atse Protocol Analyser. In *Term Rewriting and Applications - Proc. of RTA*, volume 4098 of *Lecture Notes in Computer Science*, pages 277–286, Seattle, WA, USA, 2006.

[69] Kumar N. Verma and Jean Goubault-Larrecq. Alternating two-way AC-tree automata. *Information and Computation*, 205(6):817–869, June 2007.

[70] Laurent Vigneron. A Tool helping to Design Cryptographic Protocols (tutorial). In 4th Conference on Security and Network Architectures (SAR'05), Batz sur Mer, France, June 2005.

[71] Igor Walukiewicz, editor. *Foundations of Software Science and Computation Structures, 7th International Conference, FOSSACS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 - April 2, 2004, Proceedings*, volume 2987 of *Lecture Notes in Computer Science*. Springer, 2004.