Kimmo Järvinen

List of publications

Updated: September 12, 2016

This list of publications follows the guidelines from Publication Type Classification Manual, Ministry of Education of Finland (2010).

A1. Articles in refereed scientific journals

[A1.1] Zhe Liu, Johann Großschädl, Zhi Hu, Kimmo Järvinen, Husen Wang, and Ingrid Verbauwhede. "Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things". In: *IEEE Transactions on Computers* (to appear).

[A1.2] Reza Azarderakhsh, Mehran Mozaffari Kermani, and Kimmo Järvinen. "Secure and Efficient Architectures for Single Exponentiation in Finite Field Suitable for High-Performance Cryptographic Applications". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34.3 (Mar. 2015), pp. 332–340. URL: http://dx.doi.org/10.1109/TCAD.2014.2387866.

[A1.3] Kimmo Järvinen, Vassil Dimitrov, and Reza Azarderakhsh. "A Generalization of Addition Chains and Fast Inversions in Binary Fields". In: *IEEE Transactions on Computers* 64.9 (Sept. 2015), pp. 2421–2432. URL: http://dx.doi.org/10.1109/TC.2014.2375182.

[A1.4] Reza Azarderakhsh, Kimmo Järvinen, and Vassil Dimitrov. "Fast Inversion in $GF(2^m)$ with Normal Basis Using Hybrid-Double Multipliers". In: *IEEE Transactions on Computers* 63.4 (2014), pp. 1041–1047. URL: http://dx.doi.org/10.1109/TC.2012.265.

[A1.5] Reza Azarderakhsh, Kimmo U. Järvinen, and Mehran Mozaffari-Kermani. "Efficient Algorithm and Architecture for Elliptic Curve Cryptography for Extremely Constrained Secure Applications". In: *IEEE Transactions on Circuits and Systems I—Regular Papers* 61.4 (2014), pp. 1144–1155. URL: http://dx.doi.org/10.1109/TCSI.2013.2283691.

[A1.6] Jithra Adikari, Vassil Dimitrov, and Kimmo Järvinen. "A Fast Hardware Architecture for Integer to τNAF Conversion for Koblitz Curves". In: *IEEE Transactions on Computers* 61.5 (May 2012), pp. 732–737. URL: http://dx.doi.org/10.1109/TC.2011.87.

[A1.7] Philipp Grabher, Johann Großschädl, Simon Hoerder, Kimmo Järvinen, Dan Page, Stefan Tillich, and Marcin Wójcik. "An exploration of mechanisms for dynamic cryptographic instruction set extension". In: *Journal of Cryptographic Engineering* 2.1 (May 2012), pp. 1–18. URL: http://dx.doi.org/10.1007/s13389-011-0025-8.

[A1.8] Vassil S. Dimitrov, Kimmo U. Järvinen, and Jithra Adikari. "Area-Efficient Multipliers Based on Multiple-Radix Representations". In: *IEEE Transactions on Computers* 60.2 (Feb. 2011), pp. 189–201. URL: http://dx.doi.org/10.1109/TC.2010.200.

[A1.9] Kimmo Järvinen. "Optimized FPGA-based Elliptic Curve Cryptography Processor for High-Speed Applications". In: *Integration, the VLSI Journal* 44.4 (2011), pp. 270–279. URL: http://dx.doi.org/10.1016/j.vlsi.2010.08.001.

[A1.10] Billy Bob Brumley and Kimmo U. Järvinen. "Conversion Algorithms and Implementations for Koblitz Curve Cryptography". In: *IEEE Transactions on Computers* 59.1 (Jan. 2010), pp. 81–92. URL: http://dx.doi.org/10.1109/TC.2009.132.

[A1.11] Kimmo Järvinen and Jorma Skyttä. "Fast Point Multiplication on Koblitz Curves: Parallelization Method and Implementations". In: *Microprocessors and Microsystems* 33.2 (Mar. 2009), pp. 106–116. URL: http://dx.doi.org/10.1016/j.micpro.2008.08.002.

[A1.12] Vassil S. Dimitrov, Kimmo U. Järvinen, Michael J. Jacobson, Jr., Wai Fong Chan, and Zhun Huang. "Provably Sublinear Point Multiplication on Koblitz Curves and Its Hardware Implementation". In: *IEEE Transactions on Computers* 57.11 (Nov. 2008), pp. 1469–1481. URL: http://dx.doi.org/10.1109/TC.2008.65.

[A1.13] Kimmo Järvinen and Jorma Skyttä. “On Parallelization of High-Speed Processors for Elliptic Curve Cryptography”. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 16.9 (Sept. 2008), pp. 1162–1175. URL: http://dx.doi.org/10.1109/TVLSI.2008.2000728.

[A1.14] Kimmo Järvinen, Matti Tommiska, and Jorma Skyttä. “Comparative Survey of High-Performance Cryptographic Algorithm Implementations on FPGAs”. In: *IEE Proceedings—Information Security* 152.1 (Oct. 2005), pp. 3–12. URL: http://dx.doi.org/10.1049/ip-ifs:20055004.

A3. Book sections, chapters in research books

[A3.1] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. “Efficient Secure Two-Party Computation with Untrusted Hardware Tokens”. In: *Towards Hardware-Intrinsic Security*. Ed. by Ahmad-Reza Sadeghi and David Naccache. Springer, 2010, pp. 367–386. URL: http://dx.doi.org/10.1007/978-3-642-14452-3_17.

A4. Articles in refereed scientific conference proceedings

[A4.1] Kimmo Järvinen and Josep Balasch. “Single-Trace Side-Channel Attacks on Scalar Multiplications with Precomputations”. In: *Proceedings of the 15th Smart Card Research and Advanced Application Conference, CARDIS 2016*. to appear.

[A4.2] Kimmo Järvinen, Andrea Miele, Reza Azarderakhsh, and Patrick Longa. “Four$\mathbb{Q}$ on FPGA: New Hardware Speed Records for Elliptic Curve Cryptography over Large Prime Characteristic Fields”. In: *Proceedings of the IACR Conference on Cryptographic Hardware and Embedded Systems, CHES 2016*. Vol. 9813. Lecture Notes in Computer Science. Springer, 2016, pp. 517–537. URL: http://dx.doi.org/10.1007/978-3-662-53140-2_25.

[A4.3] Jeroen Bosmans, Sujoy Sinha Roy, Kimmo Järvinen, and Ingrid Verbauwhede. “A Tiny Coprocessor for Elliptic Curve Cryptography over the 256-bit NIST Prime Field”. In: *Proceedings of the 29th International Conference on VLSI Design*. IEEE, 2016, pp. 523–528. URL: http://dx.doi.org/10.1109/VLSID.2016.82.

[A4.4] Burak Gövem, Kimmo Järvinen, Kris Aerts, Ingrid Verbauwhede, and Nele Mentens. “A Fast and Compact FPGA Implementation of Elliptic Curve Cryptography Using Lambda Coordinates”. In: *Progress in Cryptology (AFRICACRYPT 2016)*. Vol. 9646. Lecture Notes in Computer Science. Springer, 2016, pp. 63–68. URL: http://dx.doi.org/10.1007/978-3-319-31517-1_4.

[A4.5] Sujoy Sinha Roy, Kimmo Järvinen, and Ingrid Verbauwhede. “Lightweight Coprocessor for Koblitz Curves: 283-bit ECC Including Scalar Conversion with only 4300 Gates”. In: *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2015)*. Vol. 9293. Lecture Notes in Computer Science. Springer, 2015, pp. 102–122. URL: http://dx.doi.org/10.1007/978-3-662-48324-4_6.

[A4.6] Sujoy Sinha Roy, Kimmo Järvinen, Frederik Vercauteren, Vassil Dimitrov, and Ingrid Verbauwhede. “Modular Hardware Architecture for Somewhat Homomorphic Function Evaluation”. In: *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2015)*. Vol. 9293. Lecture Notes in Computer Science. Springer, 2015, pp. 164–184. URL: http://dx.doi.org/10.1007/978-3-662-48324-4_9.

[A4.7] Josep Balasch, Benedikt Gierlichs, Kimmo Järvinen, and Ingrid Verbauwhede. “Hardware/Software Co-Design Flavors of Elliptic Curve Scalar Multiplication”. In: *Proceedings of the 2014 IEEE International Symposium on Electromagnetic Compatibility (EMC 2014)*. IEEE, 2014, pp. 758–763. URL: http://dx.doi.org/10.1109/ISEMC.2014.6899070.

[A4.8] Kimmo Järvinen and Ingrid Verbauwhede. “How to Use Koblitz Curves on Small Devices?” In: *Proceedings of the 13th Smart Card Research and Advanced Application Conference (CARDIS 2014), Revised Selected Papers*. Vol. 8968. Lecture Notes in Computer Science. Springer, 2014, pp. 154–170. URL: http://dx.doi.org/10.1007/978-3-319-16763-3_10.

[A4.9] Vassil Dimitrov and Kimmo Järvinen. “Another Look at Inversions over Binary Fields”. In: *Proceedings of the 21st IEEE International Symposium on Computer Arithmetic, ARITH 21*. IEEE Computer Society, 2013, pp. 211–218. URL: http://dx.doi.org/10.1109/ARITH.2013.25.

[A4.10] Simon Hoerder, Kimmo Järvinen, and Dan Page. "On Secure Embedded Token Design – Quasi-Looped Yao Circuits and Bounded Leakage". In: *Proceedings of the 7th Workshop on Information Security Theory and Practice (WISTP 2013)*. Vol. 7886. Lecture Notes in Computer Science. Springer, 2013, pp. 112–128. URL: http://dx.doi.org/10.1007/978-3-642-38530-8_8.

[A4.11] Kimmo Järvinen, Céline Blondeau, Dan Page, and Michael Tunstall. "Harnessing Biased Faults in Attacks on ECC-based Signature Schemes". In: *Proceedings of the 9th Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2012*. IEEE Computer Society, 2012, pp. 72–82. URL: http://dx.doi.org/10.1109/FDTC.2012.13.

[A4.12] Philipp Grabher, Johann Großschädl, Simon Hoerder, Kimmo Järvinen, Dan Page, Stefan Tillich, and Marcin Wójcik. "An exploration of mechanisms for dynamic cryptographic instruction set extension". In: *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems 2011, CHES 2011*. Vol. 6917. Lecture Notes in Computer Science. Springer-Verlag, 2011, pp. 1–16. URL: http://dx.doi.org/10.1007/978-3-642-23951-9_1.

[A4.13] Kimmo Järvinen. "Elliptic curve cryptography on FPGAs: How fast can we go with a single chip? (Invited talk)". In: *Proceedings of the 2011 International Conference on Engineering of Reconfigurable Systems and Algorithms, ERSA 2011*. 2011, pp. 118–127.

[A4.14] Kimmo Järvinen. "Sharing Resources Between AES and the SHA-3 Second Round Candidates Fugue and Grøstl". In: *The Second SHA-3 Candidate Conference*. 2010. URL: http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/papers/Jarvinen_paper_20100709.pdf.

[A4.15] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. "Embedded SFE: Offloading Server and Network using Hardware Tokens". In: *Proceedings of the 14th International Conference on Financial Cryptography and Data Security, FC'10*. Vol. 6052. Lecture Notes in Computer Science. Springer-Verlag, 2010, pp. 207–221. URL: http://dx.doi.org/10.1007/978-3-642-14577-3_17.

[A4.16] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. "Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs". In: *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems 2010, CHES 2010*. Vol. 6225. Lecture Notes in Computer Science. Springer-Verlag, 2010, pp. 383–397. URL: http://dx.doi.org/10.1007/978-3-642-15031-9_26.

[A4.17] Kimmo U. Järvinen. "On repeated squarings in binary fields". In: *Proceedings of the 16th International Workshop on Selected Areas in Cryptography, SAC 2009*. Vol. 5867. Lecture Notes in Computer Science. Springer-Verlag, 2009, pp. 331–349. URL: http://dx.doi.org/10.1007/978-3-642-05445-7_21.

[A4.18] Billy Bob Brumley and Kimmo U. Järvinen. "Fast Point Decompression for Standard Elliptic Curves". In: *Proceedings of the 5th European PKI Workshop, EuroPKI 2008*. Vol. 5057. Lecture Notes in Computer Science. Springer-Verlag, 2008, pp. 134–149. URL: http://dx.doi.org/10.1007/978-3-540-69485-4_10.

[A4.19] Kimmo U. Järvinen and Jorma O. Skyttä. "High-Speed Elliptic Curve Cryptography Accelerator for Koblitz Curves". In: *Proceedings of the 16th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, FCCM 2008*. IEEE Computer Society, 2008, pp. 109–118. URL: http://dx.doi.org/10.1109/FCCM.2008.30.

[A4.20] Billy Bob Brumley and Kimmo Järvinen. "Koblitz Curves and Integer Equivalents of Frobenius Expansions". In: *Revised Selected Papers of the 14th International Workshop on Selected Areas in Cryptography, SAC 2007*. Vol. 4876. Lecture Notes in Computer Science. Springer-Verlag, 2007, pp. 126–137. URL: http://dx.doi.org/10.1007/978-3-540-77360-3_9.

[A4.21] Kimmo Järvinen, Juha Forsten, and Jorma Skyttä. "FPGA Design of Self-certified Signature Verification on Koblitz Curves". In: *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES 2007*. Vol. 4727. Lecture Notes in Computer Science. Springer-Verlag, 2007, pp. 256–271. URL: http://dx.doi.org/10.1007/978-3-540-74735-2_18.

[A4.22] Vassil S. Dimitrov, Kimmo U. Järvinen, Michael J. Jacobson, jr., Wai Fong Chan, and Zhun Huang. "FPGA Implementation of Point Multiplication on Koblitz Curves Using Kleinian Integers". In: *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES 2006*. Vol. 4249. Lecture Notes in Computer Science. Springer-Verlag, 2006, pp. 445–459. URL: http://dx.doi.org/10.1007/11894063_35.

[A4.23] Kimmo Järvinen, Juha Forsten, and Jorma Skyttä. "Efficient Circuitry for Computing τ-adic Non-Adjacent Form". In: *Proceedings of the 13th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2006*. IEEE, 2006, pp. 232–235. URL: http://dx.doi.org/10.1109/ICECS.2006.379768.

[A4.24] Kimmo Järvinen, Matti Tommiska, and Jorma Skyttä. "Hardware Implementation Analysis of the MD5 Hash Algorithm". In: *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, HICSS-38*. Abstract. Full paper available at the IEEE Xplore. IEEE, 2005, p. 298. URL: http://dx.doi.org/10.1109/HICSS.2005.291.

[A4.25] Kimmo U. Järvinen, Matti T. Tommiska, and Jorma O. Skyttä. "A Compact MD5 and SHA-1 Co-Implementation Utilizing Algorithm Similarities". In: *Proceedings of the 2005 International Conference on Engineering of Reconfigurable Systems and Algorithms, ERSA 2005*. CSREA Press, 2005, pp. 48–54.

[A4.26] Kimmo Järvinen, Matti Tommiska, and Jorma Skyttä. "A Scalable Architecture for Elliptic Curve Point Multiplication". In: *Proceedings of the 2004 IEEE International Conference on Field-Programmable Technology, FPT 2004*. IEEE, 2004, pp. 303–306. URL: http://dx.doi.org/10.1109/FPT.2004.1393285.

[A4.27] Kimmo Järvinen, Matti Tommiska, and Jorma Skyttä. "A VHDL Generator for Elliptic Curve Cryptography". In: *Proceedings of the 14th International Conference on Field Programmable Logic and Applications, FPL 2004*. Vol. 3203. Lecture Notes in Computer Science. Springer-Verlag, 2004, pp. 1098–1100. URL: http://dx.doi.org/10.1007/b99787.

[A4.28] Kimmo U. Järvinen, Matti T. Tommiska, and Jorma O. Skyttä. "A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor". In: *Proceedings of the 11th ACM International Symposium on Field-Programmable Gate Arrays, FPGA 2003*. ACM Press, 2003, pp. 207–215. URL: http://dx.doi.org/10.1145/611817.611848.

B1. Articles in non-refereed journal articles

[B1.1] Kimmo Järvinen. "Elliptisten käyrien salausmenetelmät ja niiden laskenta ohjelmoitavalla logiikalla". fin. In: *Tietojenkäsittelytiede* 32 (2011), pp. 34–47. URL: http://www.cse.tkk.fi/fi/tkt-lehti/a32/jarvinen.pdf.

B3. Articles in non-refereed conference proceedings

[B3.1] Kimmo Järvinen. "Elliptic Curve Cryptography Processor for High-Speed Applications — Extended Abstract". In: *Tietojenkäsittelytieteen päivät 2010: Computer Science Days 2010*. Publications of the University of Eastern Finland, Reports and Books in Forestry and Natural Sciences. 2010, pp. 10–11. URL: http://urn.fi/URN:ISBN:978-952-61-0130-9.

C2. Edited books, conference proceedings or special issues

[C2.1] Tuomas Aura, Kimmo Järvinen, and Kaisa Nyberg, eds. *Information Security Technology for Applications, 15th Nordic Conference on Secure IT Systems, NordSec 2010, Aalto University, Finland, October 27-29, 2010, Revised Selected Papers*. Vol. 7127. Lecture Notes in Computer Science. Heidelberg, Berlin: Springer, 2012, p. 289. URL: http://dx.doi.org/10.1007/978-3-642-27937-9.

D4. Published development or research reports or studies

[D4.1] Kimmo Järvinen, Andrea Miele, Reza Azarderakhsh, and Patrick Longa. *Four$\mathbb{Q}$ on FPGA: New Hardware Speed Records for Elliptic Curve Cryptography over Large Prime Characteristic Fields*. Cryptology ePrint Archive, Report 2016/569. 2016. URL: http://eprint.iacr.org/2016/569.

[D4.2] Sujoy Sinha Roy, Kimmo Järvinen, and Ingrid Verbauwhede. *Lightweight Coprocessor for Koblitz Curves: 283-bit ECC Including Scalar Conversion with only 4300 Gates*. Cryptology ePrint Archive, Report 2015/556. 2015. URL: http://eprint.iacr.org/2015/556.

[D4.3] Sujoy Sinha Roy, Kimmo Järvinen, Frederik Vercauteren, Vassil Dimitrov, and Ingrid Verbauwhede. *Modular Hardware Architecture for Somewhat Homomorphic Function Evaluation*. Cryptology ePrint Archive, Report 2015/337. 2015. URL: http://eprint.iacr.org/2015/337.

[D4.4] Simon Hoerder, Kimmo Järvinen, and Dan Page. *On secure embedded token design (Long Version) – Quasi-looped Yao circuits and bounded leakage*. Cryptology ePrint Archive, Report 2013/168. Extended version of the paper appearing in WISTP 2013. Mar. 2013. URL: http://eprint.iacr.org/2013/168.

[D4.5] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. *Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs*. Cryptology ePrint Archive, Report 2010/276. Extended version of the paper appearing in CHES'10. May 2010. URL: http://eprint.iacr.org/2010/276.

[D4.6] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. *Embedded SFE: Offloading Server and Network using Hardware Tokens*. Cryptology ePrint Archive, Report 2009/591. Extended version of the paper appearing in FC'10. Dec. 2009. URL: http://eprint.iacr.org/2009/591.

[D4.7] Vassil S. Dimitrov, Kimmo U. Järvinen, Michael J. Jacobson, jr., Wai Fong Chan, and Zhun Huang. *Provably Sublinear Point Multiplication on Koblitz Curves and its Hardware Implementation*. Cryptology ePrint Archive, Report 2006/305. Extended version of the paper from CHES'06. Sept. 2006. URL: http://eprint.iacr.org/2006/305.

G2. Master's thesis

[G2.1] Kimmo Järvinen. "Hardware Description Language Generator for Elliptic Curve Point Multiplication". Master's Thesis. Helsinki University of Technology, Signal Processing Laboratory, Nov. 2003.

G5. Doctoral dissertation (article)

[G5.1] Kimmo Järvinen. "Studies on High-Speed Hardware Implementation of Cryptographic Algorithms". Department of Signal Processing and Acoustics Report Series, Report 5. Doctoral dissertation. Helsinki University of Technology, Nov. 2008. URL: http://lib.tkk.fi/Diss/2008/isbn9789512295906/.