Publications

Laurent Imbert

http://www.lirmm.fr/~imbert

July 1, 2016

Preprints

[1] S. Lindner, L. Imbert, and M. J. Jacobson Jr. "Improved Explicit Formulas of Genus 2 Hyperelliptic Curves in Weierstrass Form". (submitted). 2016.

[2] E. Guerrini, L. Imbert, and T. Winterhalter. *Randomizing Scalar Multiplication Using Exact Covering Systems of Congruences*. Cryptology ePrint Archive, Report 2015/475. http://eprint.iacr.org/. 2015.

International journals with editorial board

[3] G. Perin, L. Imbert, P. Maurine, and L. Torres. "Vertical and Horizontal Correlation Attacks on RNS-Based Exponentiations". In: *Journal of Cryptographic Engineering* 5.3 (2015), pp. 171–185. DOI: 10.1007/s13389-015-0095-0.

[4] F. Disanto, L. Imbert, and F. Philippe. "On the maximal weight of (p, q)-ary chains with bounded parts". In: *INTEGERS, Electronic Journal of Combinatorial Number Theory* 14 (2014), #A37. URL: http://www.integers-ejcnt.org/vol14.html.

[5] L. Imbert and M. J. Jacobson Jr. "Empirical optimization of divisor arithmetic on hyperelliptic curves over $\mathbb{F}_{2^m}$". In: *Advances in Mathematics of Communication* 7.4 (2013), pp. 485–502. DOI: doi:10.3934/amc.2013.7.485.

[6] J. Adikari, V. Dimitrov, and L. Imbert. "Hybrid binary-ternary number system for elliptic curve cryptosystems". In: *IEEE Transactions on Computers* 60.2 (2011), pp. 254–265. DOI: 10.1109/TC.2010.138.

[7] L. Imbert, M. J. Jacobson Jr., and A. Schmidt. "Fast ideal cubing in quadratic number and function fields". In: *Advances in Mathematics of Communications* 4.2 (2010), pp. 237–260. DOI: 10.3934/amc.2010.4.237.

[8] L. Imbert and F. Philippe. "Strictly chained (p, q)-ary partitions". In: *Contributions to Discrete Mathematics* 5.2 (2010), pp. 119–136. arXiv: 1212.0048 [Math.NT]. URL: http://hdl.handle.net/10515/sy5hx1653.

[9] V. Berthé and L. Imbert. "Diophantine approximation, Ostrowski numeration and the double-base number system". In: *Discrete Mathematics & Theoretical Computer Science* 11.1 (2009), pp. 153–172. URL: http://www.dmtcs.org/dmtcs-ojs/index.php/dmtcs/article/view/1011/0.

[10] V. Dimitrov, L. Imbert, and P. K. Mishra. "The Double-Base Number System and its Application to Elliptic Curve Cryptography". In: *Mathematics of Computation* 77.262 (Apr. 2008), pp. 1075–1104. DOI: 10.1090/S0025-5718-07-02048-0.

[11] R. Glabb, L. Imbert, G. A. Jullien, A. Tisserand, and N. Veyrat-Charvillon. "Multi-mode Operator for SHA-2 Hash Functions". In: *Journal of Systems Architecture, Special Issue on Embedded Hardware for Cryptosystems* 53.2-3 (Feb. 2007), pp. 127–138. DOI: 10.1016/j.sysarc.2006.09.006.

[12] J.-C. Bajard, L. Imbert, and C. Negre. "Arithmetic Operations in Finite Fields of Medium Prime Characteristic using the Lagrange Representation". In: *IEEE Transactions on Computers* 55.9 (Sept. 2006), pp. 1167–1177. DOI: 10.1109/TC.2006.136.

[13] J.-C. Bajard and L. Imbert. "A Full RNS Implementation of RSA". In: *IEEE Transactions on Computers* 53.6 (June 2004), pp. 769–774. DOI: 10.1109/TC.2004.2.

[14] L. Imbert, V. Dimitrov, and G. A. Jullien. "Fault-Tolerant Computations over Replicated Finite Rings". In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 50.7 (July 2003), pp. 858–864. DOI: 10.1109/TCSI.2003.814085.

[15] J.-C. Bajard, L. Imbert, and F. Rico. "Évaluation des fonctions élémentaires en multiprécision". In: *Technique et Science Informatiques* 20.1 (2001), pp. 91–110.

[16] L. Imbert and G. A. Jullien. "Fault-Tolerant Computation of Large Inner-Products". In: *IEE Electronics Letters* 37.9 (Apr. 2001), pp. 551–552. DOI: 10.1049/el:20010378.

[17] M. D. Ercegovac, L. Imbert, D. W. Matula, J.-M. Muller, and G. Wei. "Improving Goldschmidt Division, Square Root and Square Root Reciprocal". In: *IEEE Transactions on Computers* 49.7 (July 2000), pp. 759–763. DOI: 10.1109/12.863046.

[18] L. Imbert, J.-M. Muller, and F. Rico. "A Radix-10 BKM Algorithm for Computing Transcendentals on Pocket Computers". In: *Journal of VLSI Signal Processing* 25.2 (June 2000), pp. 179–186. DOI: 10.1023/A:1008127208220.

Invited Talk in Conferences and Workshops

[19] L. Imbert. "Randomizing Scalar Multiplication Using Exact Covering Systems of Congruences". Invited Talk. Kick-Workshop on Explicit Methods for Abelian Varieties. May 2015.

[20] L. Imbert. "Strictly chained (p, q)-ary partitions". Invited Talk. Alberta Number Theory Day, Calgary, Canada. Apr. 2009.

[21] L. Imbert. "Quelques pistes pour accélérer les calculs sur les courbes elliptiques". Invited Talk. Journées Codage et Cryptographie, Carcans, France. Mar. 2008.

Miscelaneous

[56] C. Bouvier, P. Gaudry, L. Imbert, H. Jeljeli, and E. Thomé. *Discrete logarithms in $GF(p)$ – 180 digits*. NMBRTHRY Archives. https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1406&L=NMBRTHRY&F=&S=&P=3161. June 2014.

Proceedings of International Conferences with Program Committees

[22] G. Perin, L. Imbert, L. Torres, and P. Maurine. "Attacking Randomized Exponentiation using Unsupervised Learning". In: *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014. Revised Selected Papers*. Vol. 8622. Lecture Notes in Computer Science. Springer, 2014, pp. 144–160. DOI: 10.1007/978-3-319-10175-0_11.

[23] G. Perin, L. Imbert, L. Torres, and P. Maurine. "Practical Analysis of RSA Countermeasures Against Side-Channel Electromagnetic Attacks". In: *Smart Card Research and Advanced Applications, 12th International Conference, CARDIS 2013. Revised selected papers*. Vol. 8419. Lecture Notes in Computer Science. Springer, 2014, pp. 200–215.

[24] P. Giorgi, L. Imbert, and T. Izard. "Parallel modular multiplication on multi-core processors". In: *Proceedings of the 21st IEEE Symposium on Computer Arithmetic, ARITH21*. IEEE Computer Society, 2013, pp. 135–142.

[25] G. Perin, L. Imbert, L. Torres, and P. Maurine. "Electromagnetic Analysis on RSA Algorithm Based on RNS". In: *Proceedings of 16th Euromicro Conference on Digital System Design, DSD 2013*. IEEE, 2013, pp. 345–352.

[26] J. Adikari, V. Dimitrov, and L. Imbert. "Hybrid Binary-Ternary Joint Sparse Form and its Application in Elliptic Curve Cryptography". In: *Proceedings of the 19th IEEE Symposium on Computer Arithmetic, ARITH19*. IEEE Computer Society, 2009, pp. 76–82. DOI: 10.1109/ARITH.2009.10.

[27] P. Ferraro, P. Hanna, L. Imbert, and T. Izard. "Accelerating Query-by-Humming on GPU". In: *Proceedings of the 10th International Society for Music Information Retrieval Conference, ISMIR 2009*. 2009, pp. 279–284. URL: http://ismir2009.ismir.net/proceedings/PS2-15.pdf.

[28] P. Giorgi, L. Imbert, and T. Izard. "Optimizing elliptic curve scalar multiplication for small scalars". In: *Mathematics for Signal and Information Processing*. Vol. 7444. Proceedings of SPIE. SPIE Ed., 2009, 74440N. DOI: 10.1117/12.827689.

[29] C. Doche and L. Imbert. "The Double-Base Number System in Elliptic Curve Cryptography". In: *Conference Records of the 42nd Asilomar Conference on Signals, Systems and Computers*. IEEE, 2008, pp. 777–780. DOI: 10.1109/ACSSC.2008.5074514.

[30] V. Dimitrov, L. Imbert, and A. Zakaluzny. "Multiplication by a Constant is Sublinear". In: *Proceedings of the 18th IEEE Symposium on Computer Arithmetic, ARITH18*. IEEE Computer Society, 2007, pp. 261–268. DOI: 10.1109/ARITH.2007.24.

[31] L. Imbert, A. Pereira, and A. Tisserand. "A Library for Prototyping the Computer Arithmetic Level in Elliptic Curve Cryptography". In: *Advanced Signal Processing Algorithms, Architectures, and Implementations XVII*. Vol. 6697. Proceedings of SPIE. SPIE Ed., 2007, 66970N. DOI: 10.1117/12.733652.

[32] V. Dimitrov, L. Imbert, and A. Zakaluzny. "Sublinear Constant Multiplication Algorithms". In: *Advanced Signal Processing Algorithms, Architectures and Implementations XVI*. Vol. 6313. Proceedings of SPIE. SPIE, 2006, p. 631305. DOI: 10.1117/12.680289.

[33] C. Doche and L. Imbert. "Extended Double-Base Number System with Applications to Elliptic Curve Cryptography". In: *Progress in Cryptology, INDOCRYPT'06*. Vol. 4329. Lecture Notes in Computer Science. Springer, 2006, pp. 335–348. DOI: 10.1007/11941378_24.

[34] R. Glabb, L. Imbert, G. A. Jullien, A. Tisserand, and N. Veyrat-Charvillon. "Multi-mode Operator for SHA-2 Hash Functions". In: *Proceedings of 2006 International Conference on Engineering of Reconfigurable Systems and Algorithms, ERSA'06*. June 2006, pp. 207–210.

[35] J.-C. Bajard, L. Imbert, and G. A. Jullien. "Parallel Montgomery Multiplication in GF(2^k) using Trinomial Residue Arithmetic". In: *Proceedings of the 17th IEEE Symposium on Computer Arithmetic, ARITH17*. IEEE Computer Society, 2005, pp. 164–171. DOI: 10.1109/ARITH.2005.34.

[36] J.-C. Bajard, L. Imbert, G. A. Jullien, and H. C. Williams. "A CRT-Based Montgomery Multiplication for Finite Fields of Small Characteristic". In: *Proceedings 17th IMACS World Congress, Scientific Computation, Applied Mathematics and Simulation*. 2005, pp. 101–107.

[37] J.-C. Bajard, L. Imbert, and T. Plantard. "Arithmetic Operations in the Polynomial Modular Number System". In: *Proceedings of the 17th IEEE Symposium on Computer Arithmetic, ARITH17*. IEEE Computer Society, 2005, pp. 206–213. DOI: 10.1109/ARITH.2005.11.

[38] J.-C. Bajard, L. Imbert, and T. Plantard. "Modular Number Systems: Beyond the Mersenne Family". In: *Proceedings of the 11th International Workshop on Selected Areas in Cryptography, SAC'04*. Vol. 3357. Lecture Notes in Computer Science. Springer, 2005, pp. 159–169. DOI: 10.1007/978-3-540-30564-4_11.

[39] V. Dimitrov, L. Imbert, and P. K. Mishra. "Efficient and Secure Elliptic Curve Point Multiplication using Double-Base Chains". In: *Advances in Cryptology, ASIACRYPT'05*. Vol. 3788. Lecture Notes in Computer Science. Springer, 2005, pp. 59–78. DOI: 10.1007/11593447_4.

[40] I. Steiner, P. Chan, L. Imbert, G. A. Jullien, V. Dimitrov, and G. H. McGibney. "A Fault-Tolerant Modulus Replication Complex FIR Filter". In: *Proceedings 16th IEEE International Conference on Application-Specific Systems, Architecture Processors, ASAP'05*. 2005, pp. 387–392. DOI: 10.1109/ASAP.2005.6.

[41] J.-C. Bajard, L. Imbert, P.-Y. Liardet, and Y. Teglia. "Leak Resistant Arithmetic". In: *Cryptographic Hardware and Embedded Systems, CHES'04*. Vol. 3156. Lecture Notes in Computer Science. Springer, 2004, pp. 62–75. DOI: 10.1007/978-3-540-28632-5_5.

[42] V. Berthé and L. Imbert. "On Converting Numbers to the Double-Base Number System". In: *Advanced Signal Processing Algorithms, Architecture and Implementations XIV*. Vol. 5559. Proceedings of SPIE. SPIE, 2004, pp. 70–78. DOI: 10.1117/12.558895.

[43] P. Chan, G. A. Jullien, L. Imbert, V. Dimitrov, and G. H. McGibney. "Fault-Tolerant Computations within Complex FIR Filters". In: *2004 IEEE Workshop on Signal Processing Systems, Design and Implementation, SIPS'04*. IEEE, 2004, pp. 316–320. DOI: 10.1109/SIPS.2004.1363069.

[44] J.-C. Bajard, L. Imbert, C. Negre, and T. Plantard. "Multiplication in GF(p^k) for Elliptic Curve Cryptography". In: *Proceedings of the 16th IEEE Symposium on Computer Arithmetic, ARITH16*. IEEE Computer Society, 2003, pp. 181–187. DOI: 10.1109/ARITH.2003.1207677.

[45] J.-C. Bajard, L. Imbert, and T. Plantard. "Improving Euclidean Division and Modular Reduction for some Classes of Divisors". In: *Conference Records of The Thirty-Seventh Asilomar Conference on Signals, Systems, and Computers*. Vol. 2. IEEE, Nov. 2003, pp. 2218–2221. DOI: 10.1109/ACSSC.2003.1292374.

[46] J.-L. Beuchat, L. Imbert, and A. Tisserand. "Comparison of modular multipliers on FPGAs". In: *Advanced Signal Processing Algorithms, Architectures and Implementations XIII*. Vol. 5205. Proceedings of SPIE. SPIE, 2003, pp. 490–498. DOI: 10.1117/12.508121.

[47] J.-C. Bajard, L. Imbert, and C. Negre. "Modular Multiplication in GF(p^k) using Lagrange Representation". In: *Progress in Cryptology, INDOCRYPT'02*. Lecture Notes in Computer Science 2551. Springer, 2002, pp. 275–284. DOI: 10.1007/3-540-36231-2_22.

[48] V. Dimitrov, J. Eskritt, L. Imbert, G. A. Jullien, and W. C. Miller. "The use of the multi-dimensional logarithmic number system in DSP applications". In: *Proceedings of the 15th IEEE Symposium on Computer Arithmetic, ARITH15*. IEEE Computer Society, 2001, pp. 247–254. DOI: 10.1109/ARITH.2001.930126.

[49] L. Imbert and G. A. Jullien. "Efficient fault-tolerant arithmetic using a symmetrical modulus replication RNS". In: *2001 IEEE Workshop on Signal Processing Systems, Design and Implementation, SIPS'01*. IEEE, 2001, pp. 93–100. DOI: 10.1109/SIPS.2001.957334.

[50] L. Imbert, G. A. Jullien, V. Dimitrov, and A. Garg. "Fault Tolerant Complex FIR Filter Architectures Using a Redundant MRRNS". In: *Conference Records of The Thirty-Fifth Asilomar Conference on Signals, Systems, and Computers*. Vol. 2. IEEE, 2001, pp. 1222–1226. DOI: 10.1109/ACSSC.2001.987685.

[51] J.-C. Bajard, M. D. Ercegovac, L. Imbert, and F. Rico. "Fast evaluation of elementary functions with combined shift-and-add and polynomial methods". In: *Real Numbers and Computers*. 2000, pp. 75–87.

[52] L. Imbert, C. Moreau, and F. Rico. "Comparison of different techniques to compute the complex exponential for hundred bit precision". In: *Proceedings of SCAN 2000, the 9th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics*. 2000, pp. 124–125.

[53] J.-C. Bajard and L. Imbert. "Evaluation of complex elementary functions: a new version of BKM". In: *Advanced Signal Processing Algorithms, Architectures and Implementations IX*. Vol. 3807. Proceedings of SPIE. SPIE Ed., 1999, pp. 2–9. DOI: 10.1117/12.367631.

[54] J.-C. Bajard, L. Imbert, and F. Rico. “Évaluation de l’exponentielle du sinus et du cosinus à base d’additions de décalages et de polynômes”. In: *Actes de la conférence SympA’5, 5^{ieme} symposium en architectures nouvelles de machines*. 1999, pp. 19–26.

Books and Book Chapters

[55] L. Imbert. “Calcul et arithmétique des ordinateurs”. In: Traité IC2, série Informatique et Systèmes d’Information. Hermes science publications, 2004. Chap. 5, Arithmétique multiprécision, pp. 155–179.