Publications

Laurent Imbert

Laurent.Imbert@lirmm.fr

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

March 5, 2012

Refereed Journal Papers

[1] J. Adikari, V. Dimitrov, and L. Imbert. Hybrid binary-ternary number system for elliptic curve cryptosystems. *IEEE Transactions on Computers*, 60(2):254–265, 2011.

[2] L. Imbert and F. Philippe. Strictly chained (p, q)-ary partitions. *Contributions to Discrete Mathematics*, 5(2):119–136, 2010.

[3] L. Imbert, M. J. Jacobson Jr., and Schmidt A. Fast ideal cubing in quadratic number and function fields. *Advances in Mathematics of Communications*, 4(2):237–260, May 2010.

[4] V. Berthé and L. Imbert. Diophantine approximation, Ostrowski numeration and the double-base number system. *Discrete Mathematics & Theoretical Computer Science*, 11(1):153–172, 2009.

[5] V. Dimitrov, L. Imbert, and P. K. Mishra. The double-base number system and its application to elliptic curve cryptography. *Mathematics of Computation*, 77(262):1075–1104, April 2008.

[6] R. Glabb, L. Imbert, G. A. Jullien, A. Tisserand, and N. Veyrat-Charvillon. Multi-mode operator for SHA-2 hash functions. *Journal of Systems Architecture, Special Issue on Embedded Hardware for Cryptosystems*, 53(2-3):127–138, February 2007.

[7] J.-C. Bajard, L. Imbert, and C. Negre. Arithmetic operations in finite fields of medium prime characteristic using the Lagrange representation. *IEEE Transactions on Computers*, 55(9):1167–1177, September 2006.

[8] J.-C. Bajard and L. Imbert. A full RNS implementation of RSA. *IEEE Transactions on Computers*, 53(6):769–774, June 2004.

[9] L. Imbert, V. Dimitrov, and G. A. Jullien. Fault-tolerant computations over replicated finite rings. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 50(7):858–864, July 2003.

[10] L. Imbert and G. A. Jullien. Fault-tolerant computation of large inner-products. *IEE Electronics Letters*, 37(9):551–552, April 2001.

[11] J.-C. Bajard, L. Imbert, and F. Rico. Évaluation des fonctions élémentaires en multiprécision. *Technique et Science Informatiques*, 20(1):91–110, 2001.

[12] M. D. Ercegovac, L. Imbert, D. W. Matula, J.-M. Muller, and G. Wei. Improving Goldschmidt division, square root and square root reciprocal. *IEEE Transactions on Computers*, 49(7):759–763, July 2000.

[13] L. Imbert, J.-M. Muller, and F. Rico. A radix-10 BKM algorithm for computing transcendentals on pocket computers. *Journal of VLSI Signal Processing*, 25(2):179–186, June 2000.

Books and Book Chapters

[14] L. Imbert. *Calcul et arithmétique des ordinateurs*, chapter 5, Arithmétique multi-précision, pages 155–179. Traité IC2, série Informatique et Systèmes d'Information. Hermes science publications, 2004.

Invited Talks

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

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

Refereed Papers in International Conference Proceedings

[17] 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*, pages 279–284, 2009.

[18] P. Giorgi, L. Imbert, and T. Izard. Optimizing elliptic curve scalar multiplication for small scalars. In *Mathematics for Signal and Information Processing*, volume 7444 of *Proceedings of SPIE*, page 74440N. SPIE Ed., 2009.

[19] 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*, pages 76–82. IEEE Computer Society, 2009.

[20] 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*, pages 777–780. IEEE, 2008.

[21] 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*, volume 6697 of *Proceedings of SPIE*, page 66970N. SPIE Ed., 2007.

[22] V. Dimitrov, L. Imbert, and A. Zakaluzny. Multiplication by a constant is sublinear. In *Proceedings of the 18th IEEE Symposium on Computer Arithmetic, ARITH18*, pages 261–268. IEEE Computer Society, 2007.

[23] C. Doche and L. Imbert. Extended double-base number system with applications to elliptic curve cryptography. In *Progress in Cryptology, INDOCRYPT'06*, volume 4329 of *Lecture Notes in Computer Science*, pages 335–348. Springer, 2006.

[24] V. Dimitrov, L. Imbert, and A. Zakaluzny. Sublinear constant multiplication algorithms. In *Advanced Signal Processing Algorithms, Architectures and Implementations XVI*, volume 6313 of *Proceedings of SPIE*, page 631305. SPIE, 2006.

[25] R. Glabb, L. Imbert, G. A. Jullien, A. Tisserand, and N. Veyrat-Charvillon. Multimode operator for SHA-2 hash functions. In *Proceedings of 2006 International Conference on Engineering of Reconfigurable Systems and Algorithms, ERSA'06*, pages 207–210, June 2006.

[26] 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*, volume 3788 of *Lecture Notes in Computer Science*, pages 59–78. Springer, 2005.

[27] 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*, pages 387–392, 2005.

[28] 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*, pages 101–107, 2005.

[29] 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*, pages 164–171. IEEE Computer Society, 2005.

[30] 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*, pages 206–213. IEEE Computer Society, 2005.

[31] 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*, volume 3357 of *Lecture Notes in Computer Science*, pages 159–169. Springer, 2005.

[32] 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*, pages 316–320. IEEE, 2004.

[33] V. Berthé and L. Imbert. On converting numbers to the double-base number system. In *Advanced Signal Processing Algorithms, Architecture and Implementations XIV*, volume 5559 of *Proceedings of SPIE*, pages 70–78. SPIE, 2004.

[34] J.-C. Bajard, L. Imbert, P.-Y. Liardet, and Y. Teglia. Leak resistant arithmetic. In *Cryptographic Hardware and Embedded Systems, CHES'04*, volume 3156 of *Lecture Notes in Computer Science*, pages 62–75. Springer, 2004.

[35] 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*, volume 2, pages 2218–2221. IEEE, November 2003.

[36] J.-L. Beuchat, L. Imbert, and A. Tisserand. Comparison of modular multipliers on FPGAs. In *Advanced Signal Processing Algorithms, Architectures and Implementations XIII*, volume 5205 of *Proceedings of SPIE*, pages 490–498. SPIE, 2003.

[37] 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*, pages 181–187. IEEE Computer Society, 2003.

[38] J.-C. Bajard, L. Imbert, and C. Negre. Modular multiplication in GF(p^k) using Lagrange representation. In *Progress in Cryptology, INDOCRYPT'02*, number 2551 in Lecture Notes in Computer Science, pages 275–284. Springer, 2002.

[39] 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*, volume 2, pages 1222–1226. IEEE, 2001.

[40] 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*, pages 93–100. IEEE, 2001.

[41] 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*, pages 247–254. IEEE Computer Society, 2001.

[42] 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*, pages 124–125, 2000.

[43] 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*, pages 75–87, 2000.

[44] 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*, volume 3807, pages 2–9, 1999.

Refereed Papers in National Conference Proceedings

[45] 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*, pages 19–26, 1999.

Thesis

[46] L. Imbert. Arithmexotiques. Habilitation à Diriger les Recherches, Université Montpellier 2, Montpellier, France, April 2008.

[47] L. Imbert. *Évaluation des fonctions élémentaires – Algorithmes et Implémentations.* PhD thesis, Université de Provence, Marseille, France, May 2000.