Important <u>Industrial Oriented</u> Citation Record of <u>Sung-Ming Yen</u>

NATIONAL CENTRAL UNIVERSITY
Dept of Computer Science and Information Engineering
LCIS · Laboratory of Cryptography and Information Security
`http://www.csie.ncu.edu.tw/~yensm/lcis.html`

May 15, 2000

Abstract

The following list reports the techniques or systems developed by Sun-Ming Yen which were employed or considered by some institutes, companies, or standard organizations.

1. M. Joye and <u>S.M. Yen</u>, "Optimal Left-to-right Binary Signed-Digit Recoding," *IEEE Trans. on Computers – Special issue on Computer Arithmetic*, Vol.49, No.7, July 2000. (accepted as a full paper).
   - Patent application filed with Gemplus Card International (the largest smart card/IC card manufacturer in the world). This was requested by David Naccache – chief scientist of Gemplus, Crypto Team.
2. <u>S.M. Yen</u>, C.S. Laih, C.H. Chen and J.Y. Lee, "An Efficient Redundant-Binary Number to Binary Number Converter," *IEEE Journal of Solid State Circuits*, Vol.27, No.1, pp.109-112, Jan. 1992.
   - On Sep. 3, 1998:
     It was told by Chung-Tao Chang, a Logic Designer of a start-up company in USA, that the technique may be able to improve their design.
     `chunchan@3dsp.com` or `chunchan@scf.usc.edu`.
3. <u>S.M. Yen</u>, C.S. Laih and A.K. Lenstra, "Multi-Exponentiation," *IEE Proceedings Part-E: Computers and Digital Techniques*, Vol.141, No.6, Nov. 1994.
   - Employed in "LIP" package (a software for multi-precision integer arithmetic) developed by BELL Communications Research, Inc. USA.
   - Cited **<u>as the performance benchmark</u>** in V.S. Dimitrov, G.A. Jullien, and W.C. Miller's important paper "Complexity and Fast Algorithms for Multi-exponentiations," *IEEE Trans. Computers*, Vol.49, No.2, pp.141-147, Feb. 2000.
4. <u>S.M. Yen</u> and C.S. Laih, "Fast Algorithms for the LUC Digital Signature Computation," *IEE Proceedings Part-E: Computers and Digital Techniques*, Vol.142, No.2, pp.165-169, March 1995.
   - Employed in the implementation of LUC in "Sifr" (it is a cipher & authentication software) developed by Christopher T. Skinner at Cybanim Pty Ltd, Australia.
     It was told by C.T. Skinner that the computation of LUC is reduced to about 66% of their previous implementation.
5. <u>S.M. Yen</u> and C.S. Laih, "Improved Digital Signature Suitable for Batch Verification," *IEEE Trans. on Computers*, Vol.44, No.7, July 1995.
   - Requested by David Naccache at Gemplus Card International, Crypto Team, 95200 Sarcelles, France (the largest smart card/IC card manufacturer in the world). Gemplus has also developed a similar scheme based on NIST's DSA signature scheme and applied for a patent.
6. <u>S.M. Yen</u> and C.S. Laih, "New Digital Signature Scheme Based On Discrete Logarithm," *Electronics Letters*, Vol.29, No.12, pp.1120-1121, June 1993.
   - On May 1999, suggested by Beni Arazi:
     Arazi suggested that the signature scheme can be considered for inclusion in the IEEE P1363 standard.