Citation Record of Publication of Sung-Ming Yen

Total citation count until June 2, 2000: 103

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

A. Journal papers

1. M. Joye and S.M. Yen, "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. S.M. Yen and M. Joye, "Checking Before Output May Not Be Enough Against Fault-Based Cryptanalysis," *IEEE Trans. on Computers*, (to appear in 2000).
   - Comments received from Paul Kocher (the inventor of timing attack and differential power attack) as: "*The idea of detecting whether faults cause output errors is intriguing.*"
3. S.M. Yen, 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.
   - Cited in the famous textbook by Prof. Israel Koren, "Computer Arithmetic Algorithms (after the 2nd Edition)", published by Prentice-Hall, pp.26–27, (1st Edition in 1993).
   - Cited in D.S. Phatak and I. Koren's paper "Hybrid Signed-digit Number Systems: A Unified Framework for Redundant Number Representations with Bounded Carry Propagation Chains," *IEEE Tran. on Computers*, Vol.43, No.8, pp.880-891, Aug. 1994.
   - On Sep. 3, 1998:
     It was told by Chung-Tao Chang, a Logic Designer of a start-up company in US, that the technique may be able to improve their design.
     `chunchan@3dsp.com` or `chunchan@scf.usc.edu`.
   - Cited in Hong-Yi Huang's Ph.D. thesis of Institute of Electronics, National Chiao-Tung University, June 1994.
4. S.M. Yen, C.S. Laih and A.K. Lenstra, "Multi-Exponentiation," *IEE Proceedings Part-E: Computers and Digital Techniques*, Vol.141, No.6, Nov. 1994. (NSC81-0408-E-006-02)
   - Cited **as the performance benchmark** 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.
   - Cited **as the performance benchmark** in V.S. Dimitrov, G.A. Jullien, and W.C. Miller's important paper "Algorithms for Multi-exponentiation Based on Complex Arithmetic," *Proc. of IEEE International Conference on Computer Arithmetic '97*, pp.208-215, 1997.
   - Employed in "LIP" package (a software for multi-precision integer arithmetic) developed by BELL Communications Research, Inc.
   - Employed in an implementation of NIST's DSA developed by BELL Communications Research, Inc.
   - Cited in P. de Rooij's paper "Efficient Exponentiation Using Precomputation and Vector Addition Chains," *Advances in Cryptology - Eurocrypt'94*, Springer-Verlag, 1994.

- Cited in H. Petersen and G. Poupard's paper "Efficient Scalable Fair Cash with Off-line Extortion Prevention ," *Proc. ICICS'97*, Beijing 1997. (Also as a Technical Report of Ecole Normale Sup'erieure, Paris, May 1997.)
- Cited in P. Horster, M. Michels and H. Petersen's report "Blind Multisignature schemes and Their Relevance to Electronic Voting," Technical Report **TR-95-16-F**, Dept. of Computer Science, University of Technology Chemnitz-Zwickau, Germany, Aug. 1995.
- On August 15, 1995, requested by:
  Leida Perea
  Instituto Superior Politecnico Jose Antonio Echeverria
  Centro de Informacion Cientifico-Tecnica
  Calle 127 s/n, Cujae, Marianao CP 19390
  Ciudad de la Habana, CUBA
- Cited in the book by C.S. Laih, L. Harn, and C.C. Chang, "Contemporary Cryptography and Its Applications", published by UNALIS Book Company, Sept. 1995.
- Cited in C.S. Laih and W.C. Kuo's paper "Speeding Up the Computations of Elliptic Cryptoschemes," *Proc. of ISC '96*, pp.1-9, May 1996.

5. S.M. Yen 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. (NSC84-2213-E-006-004)
   - Cited in Marc Joye's Ph.D. thesis "Security Analysis of RSA-type Cryptosystems", UCL Crypto Group, University Catholique de Louvain, Belgium, October 1997.
   - 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.
   - Cited in M. Joye and J.J. Quisquater's paper "Efficient Computation of Full Lucas Sequences," *Electronics Letters*, Vol.32, No.6, March 1996.
   - Cited in P. Horster, M. Michels and H. Petersen's paper "Digital Signature Schemes Based on Lucas Functions," *Proc. of Comm. and Multimedia Security*, Sept. 20-21, 1995.
   - Cited in J.R. Chen and C.Y. Hwang's paper "Digital Signature Based on Lucas Function," *Proc. of ISC '96*, pp.44-47, May 1996.
   - On July 19, 1997, requested by:
     Mikdam A-J.T. ALsalami
     P.O. Box 463
     Dept. of Computer Science
     College of Science, Basrah University
     Basrah 42001, IRAQ

6. S.M. Yen and C.S. Laih, "Improved Digital Signature Suitable for Batch Verification," *IEEE Trans. on Computers*, Vol.44, No.7, July 1995. (NSC82-0408-E-006-030)
   - 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.
   - Cited in the book by Birgit Pfitzmann "Digital Signature Schemes – General Framework and Fail-Stop Signatures", published by Springer-Verlag, p.29, 1996.
   - Cited in V.S. Dimitrov, G.A. Jullien, and W.C. Miller's paper "Complexity and Fast Algorithms for Multi-exponentiations," *IEEE Trans. Computers*, Vol.49, No.2, pp.141-147, Feb. 2000.
   - On July 1998, requested by:
     Prof. Mihir Bellare

Department of Computer Science & Engineering
University of California at San Diego
9500 Gilman Drive, La Jolla, CA 92093-0114
U.S.A.

- In the final version of the following paper (which can be obtained from Bellare's homepage):
M. Bellare, J. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," Extended abstract in Advances in Cryptology- Eurocrypt 98 Proceedings, Lecture Notes in Computer Science Vol. 1403, K. Nyberg ed, Springer-Verlag, 1998.
- Cited in C.J. Pavlovski and C. Boyd's paper "Efficient Batch Signature Generation Using Tree Structures," *Proc. of CrypTec '99*, Hong Kong, pp.70-77, 5-8 July, 1999.
- On September 22, 1995, requested by:
Ming Chi
Institute of Cryptology
Chi-An University of Electronic Technology
Chi-An 710071, China

7. S.M. Yen and C.S. Laih, "Improved Digital Signature Algorithm," *IEEE Trans. on Computers*, Vol.44, No.5, May 1995. (NSC82-0408-E-006-030)
   - Cited in the book by Bruce Schneier "Applied Cryptography (2nd Edition)", published by John Wiley & Sons, p.494 and p.497, 1996.
   - Requested by: Panomporn Suvannapattanan
   Department of Computer Science, Mahidol University, Thailand
   With whom a **Correction** of the original paper has been published.
   - On August 25, 1995, requested by:
   Viena Garcia
   Centro de Ingenieria Genetica y Biotecnologia
   Apartado 6162, CP 10600
   Habana, CUBA
   - On September 22, 1995, requested by:
   Ming Chi
   Institute of Cryptology
   Chi-An University of Electronic Technology
   Chi-An 710071, China
   - Cited in the book by C.S. Laih, L. Harn, and C.C. Chang, "Contemporary Cryptography and Its Applications", published by UNALIS Book Company, Sept. 1995.
   - On Feb. 16, 1996, requested by:
   Shin-Young Lim and Chang-Ryul Yoo
   Korea Research Environment Open Network
   Systems Engineering Research Institute
   Korea Institute of Science & Technology
   - Cited in J.R. Chen and C.Y. Hwang's paper "Digital Signature Based on Lucas Function," *Proc. of ISC '96*, pp.44-47, May 1996.
   - Cited in J.R. Chen and P.T. Sun's paper "A Multi-signature Scheme Based on Discrete Logarithm Problem," *Proc. of ISC '96*, pp.61-69, May 1996.

8. S.M. Yen and C.S. Laih, "New Digital Signature Scheme Based On Discrete Logarithm," *Electronics Letters*, Vol.29, No.12, pp.1120-1121, June 1993. (NSC82-0408-E-006-030)

- Cited in the book by Bruce Schneier "Applied Cryptography (2nd Edition)", published by John Wiley & Sons, 1996.
- Cited in the book by A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone "Handbook of Applied Cryptography", published by CRC Press, 1997.
- On May 1999, suggested by Beni Arazi:
  The scheme was proposed for possible inclusion in the IEEE P1363 standard.
- Cited in K. Nyberg and A. Rueppel's paper "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Advances in Cryptology, *Proc. of Eurocrypt '94*, vol.950, Springer-Verlag, pp.182-193, 1994.
- Cited in a series of technical reports and published papers (about 5 reports/papers) by P. Horster, M. Michels and H. Petersen at Dept. of Computer Science, University of Technology Chemnitz-Zwickau, Germany.
- Cited in the book by C.S. Laih, L. Harn, and C.C. Chang, "Contemporary Cryptography and Its Applications", published by UNALIS Book Company, Sept. 1995.
- On April 20, 1994, requested by:
  Lic. Raul Gramatges Triana
  Facultad de Matematica y Computacion
  Universidad de la Habana, C. Habana, CUBA
- Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.
- Cited in J.R. Chen and C.Y. Hwang's paper "Digital Signature Based on Lucas Function," *Proc. of ISC '96*, pp.44-47, May 1996.
- Cited in J.R. Chen and P.T. Sun's paper "A Multi-signature Scheme Based on Discrete Logarithm Problem," *Proc. of ISC '96*, pp.61-69, May 1996.

9. S.M. Yen and C.S. Laih, "Server-Aided Honest Computation for Cryptographic Applications," *Computer Mathematics with Applications*, Vol.26, No.12, pp.61-64, June 1993. (NSC82-0408-E-006-030)
   - Cited in C.H. Lim and P.J. Lee's paper "Server(Prover/Signer)-Aided Verification of Identity Proofs and Signatures," *Advances in Cryptology - Eurocrypt'95*, Springer-Verlag, pp.64-78, 1995.
   - On Oct. 31 1994, requested by:
     Ing Gerardo LLizo Gonzalesnico Jose Antonio Echeverria
     Apartado Postal 8011, Altahabana
     Ciudad de la Habana, CUBA
   - Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.
10. S.M. Yen and C.S. Laih, "More About the Active Attack on the Server-Aided Secret Computation Protocol," *Electronics Letters*, Vol.28, No.24, p.2250, 1992.
    - Cited in P. Beguin and J.J. Quisquater's paper "Secure Acceleration of DSS Signatures Using Insecure Server," *Proc. of Asiacrypt'94*, pp.208-218, 1994.
    - Cited in an Usenet News article of newsgroup "sci.crypt" posted by Manuel Cerecedo. on June 17, 1993.
    - Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.
11. S.M. Yen and C.S. Laih, "Common-Multiplicand Multiplication and Its Applications to Public Key Cryptography," *IEE Electronics Letters*, Vol.29, No.17, pp.1583-1584, Aug. 1993.
    - Cited in Jean-Francois Dhem's Ph.D. thesis "Design of An Efficient Public-key Cryptographic Library for RISC-based Smart Cards", Laboratory of Micro Electronics, University Catholique de Louvain, Belgium, May 1998.

- Cited in Marc Joye's Ph.D. thesis "Security Analysis of RSA-type Cryptosystems", UCL Crypto Group, University Catholique de Louvain, Belgium, October 1997.
- Cited in C.K. Koc and S. Johnson's paper "Multiplication of Signed-digit Numbers," *Electronics Letters*, Vol.30, No.11, pp.840-841, May 1994.
- Cited in T.C. Wu and Y.S. Chang's paper "Improved Generalization Common-Multiplicand Multiplication Algorithm of Yen and Laih," *Electronics Letters*, Vol.31, No.20, pp.1738-1739, 1995.
- Cited in D.C. Lou and C.C. Chang's paper "Fast Exponentiation Method Obtained by Folding the Exponent in Half," *Electronics Letters*, Vol.32, No.11, pp.984-985, 1996.
- Cited in S.M. Yen's paper "Improved Common-Multiplicand Multiplication and Fast Exponentiation by Exponent Decomposition," *IEICE Trans. on Fundamentals* Vol.E80-A, No.6, pp.1160-1163, June 1997.

12. S.M. Yen and C.S. Laih, "Analysis and Improvement of an Access Control Scheme with User Authentication," *IEE Proceedings: Computers and Digital Techniques*, Vol.141, No.5, pp.271-273, Sept. 1994.
    - Cited in J.K. Jan and Y.M. Tseng's paper "Two Integrated Schemes of User Authentication and Access Control in a Distributed Computer Network," *IEE Proceedings Part-E: Computers and Digital Techniques*, Vol.145, No.6, pp.419-424, Nov. 1998.

13. S.M. Yen and C.S. Laih, "On the Design of Dynamic Access Control Scheme with User Authentication," *Computer Mathematics with Applications*, Vol.25, No.7, pp.27-32, Apr. 1993.
    - Cited in J.K. Jan and Y.M. Tseng's paper "Two Integrated Schemes of User Authentication and Access Control in a Distributed Computer Network," *IEE Proceedings Part-E: Computers and Digital Techniques*, Vol.145, No.6, pp.419-424, Nov. 1998.
    - On Nov. 25 1993, requested by:
Raisa Giraldez Dominguez
Universidad de Matanzas "Camilo Cienfuegos"
Dir. Inform. Cientifica
Carr. Varadero KM 3 1/2
Matanzas, CUBA
    - On Mar. 23 1994, requested by:
Instituto Superior Politecnico Jose Antonio Echeverria
Centro de Informacion Cientifico-Tecnica
Calle 127 s/n, Cujae, Marianao ZP 15
Ciudad de la Habana, CUBA

14. S.M. Yen, "Cryptanalysis and Repair of the Multi-Verifier Signature with Verifier Specification," *Computers and Security*, Vol.15, No.6, pp.537-544, 1996. (NSC86-2213-E-212-001)
    - On Jan. 18, 1997, requested by:
Dr. Hoi-Kwong Lo
BRIMS, Hewlett-Packard Labs
Filton Road, Stoke Gifford
Bristol, BS12 6QZ, United Kingdom

15. S.M. Yen, "Cryptanalysis of Secure Addition Chain for SASC Applications," *Electronics Letters*, Vol.31, No.3, pp.175-176, Feb. 1995.
    - Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.

16. S.M. Yen and K.H. Liao, "Shared Authentication Token Secure Against Replay and Weak Key Attacks," *Information Processing Letters*, Vol.62, No.2, pp.77-80, April 1997. (NSC86-2213-E-212-001)

- On July 6, 1997, requested by:
  XiaoDong Lin
  P.O.Box 145, Dept. of Information Eng.
  Beijing University of Posts and Telecommunications
  Beijing 100088, P.R.China

17. C.S. Laih and S.M. Yen, "Secure Addition Sequence and its Applications on the Server-Aided Secret Computation Protocols," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E77-A, No.1, pp.81-88, Jan. 1994. (NSC81-0408-E-006-02)
    - Cited in S.M. Yen's paper "Cryptanalysis of the Secure Addition Chain for the SASC Applications," *Electronics Letters*, Vol.31, No.3, pp.175-176, Feb. 1995.

B. Conference papers

1. S.M. Yen, L.T. Ho and C.Y. Huang, "Internet Micropayment Based on Unbalanced One-way Binary Tree," In *Proc. of International Workshop on Cryptographic Techniques and E-Commerce, CrypTEC '99*, Hong Kong, pp.155-162, 5-8 July 1999.
    - Received great interest from Prof. Rivest when the paper was presented in CrypTEC '99. Some further ideas were shared after the presentation.
    - Comments received from Michael Peirce (one author of the book *Electronic Payment Systems* published by Artech House, INC., 1997) at the Dept. of Computer Science, Trinity College, Univ. of Dublin, Ireland as: "*... I had considered the idea of using multiple hash chains, committed to with a single digital signature as with the UOBT – however, I had never thought of a way to generate all these hash chains from a single value – and as you say, this could be really useful. ... UOBT increases the efficiency by having the base of each of the m chains as another hash chain itself. It makes so much sense when you see it written down, just like when I first saw PayWord.*"
    - On July 1999, requested by:
      Matthew Prebble
      Department of Computer Science
      University of Bristol
      United Kingdom
2. S.M. Yen, J.M. Lee, and J.G. Lee, "PayFair: A Prepaid Internet Micropayment Scheme Promising Customer Fairness," In *Proc. of International Workshop on Cryptographic Techniques and E-Commerce, CrypTEC '99*, Hong Kong, pp.213-221, 5-8 July 1999.
    - Comments received from Michael Peirce (one author of the book *Electronic Payment Systems* published by Artech House, INC., 1997) at the Dept. of Computer Science, Trinity College, Univ. of Dublin, Ireland as: "*I think this is a useful secret-sharing protocol, and it is good that the customer-merchant secret of Millicent has been removed. Also, there is no global bank secret like SVP.*"
    - On July 1999, requested by:
      Matthew Prebble
      Department of Computer Science
      University of Bristol
      United Kingdom
3. S.M. Yen and P.Y. Kuo, "Improved Micro-payment System," *Proc. of the 8th National Conference on Information Security*, May 1998.

- On July 1999, requested by:
Matthew Prebble
Department of Computer Science
University of Bristol
United Kingdom

4. M. Joye and S.M. Yen, "Generation and Release of Secrets Using One-way Cross-trees," (**receives a paper award**) *Proc. of the 1998 International Computer Symposium, Workshop and Cryptography and Information Security*, Tainan, Taiwan, R.O.C., 17-19th December 1998, pp. 23-28.
   - On July 1999, requested by:
   Matthew Prebble
   Department of Computer Science
   University of Bristol
   United Kingdom

5. S.M. Yen and C.S. Laih, "The Fast Cascade Exponentiation Algorithm and its Applications on Cryptography," *Proc. of the AUSCRYPT'92* and in the **Lecture Notes in Computer Science by Springer-Verlag**.
   - Cited in V.S. Dimitrov, G.A. Jullien, and W.C. Miller's paper "Complexity and Fast Algorithms for Multi-exponentiations," *IEEE Trans. Computers*, Vol.49, No.2, pp.141-147, Feb. 2000.
   - Cited in P. de Rooij's paper "Efficient Exponentiation Using Precomputation and Vector Addition Chains," *Advances in Cryptology - Eurocrypt'94*, Springer-Verlag, 1994.
   - Cited in M. Michels, D. Naccache and H. Petersen's report "GOST 34.10 – A Brief Overview of Russia's DSA," Technical Report **TR-95-14-D**, Dept. of Computer Science, University of Technology Chemnitz-Zwickau, Germany, Aug. 1995.
   - Cited in Y. Ding and H. Petersen's report "A New Approach for Delegation Using Hierarchical Delegation Tokens," Technical Report **TR-95-5-E**, Dept. of Computer Science, University of Technology Chemnitz-Zwickau, Germany, Apr. 1995.
   - Cited in the book by C.S. Laih, L. Harn, and C.C. Chang, "Contemporary Cryptography and Its Applications", published by UNALIS Book Company, Sept. 1995.
   - Cited in C.C. Chang, W.J. Horng, and D.J. Buehrer's paper "A Cascade Exponentiation Evaluation Scheme Based on the Lempel-Ziv-Welch Compression Algorithm," *Journal of Information Science and Engineering*, 1995.
   - Cited in C.C. Chang, W.J. Horng, and S.J. Hwang's paper "A New Evaluating Scheme for Cascade Exponentiation," *Proc. of the 5th National Conference on Information Security*, pp.165-175, May 1995.

6. C.S. Laih, S.M. Yen and L. Harn, "Two Efficient Server-Aided Secret Computation Protocols Based on the Addition Sequence," *Proc. of the ASIACRYPT'91* and in the **Lecture Notes in Computer Science by Springer-Verlag**.
   - Cited in an Usenet News article of newsgroup "sci.crypt" posted by Manuel Cerecedo. on June 17, 1993.
   - Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.

7. T. Matsumoto, H. Imai and C.S. Laih, S.M. Yen (a combined paper), "On Verifiable Implicit Asking Protocols for RSA Computation," *Proc. of the AUSCRYPT'92* and in the **Lecture Notes in Computer Science by Springer-Verlag**.
   - Cited in P. Beguin and J.J. Quisquater's paper "Secure Acceleration of DSS Signatures Using Insecure Server," *Proc. of Asiacrypt'94*, pp.208-218, 1994.
   - Cited in C.H. Lim and P.J. Lee's paper "Server(Prover/Signer)-Aided Verification of Identity Proofs and Signatures," *Advances in Cryptology - Eurocrypt'95*, Springer-Verlag, pp.64-78, 1995.

- Cited in an Usenet News article of newsgroup "sci.crypt" posted by Manuel Cerecedo. on June 17, 1993.

8. C.S. Laih and S.M. Yen, "Secure Addition Sequence and its Applications on the Server-Aided Secret Computation Protocols," *Proc. of the AUSCRYPT'92* and in the **Lecture Notes in Computer Science by Springer-Verlag**.
   - Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.

D. Technical reports and other publication

1. S.M. Yen, "Design and Computation of Public Key Cryptosystems," Ph.D. thesis of Department of Electrical Engineering, National Cheng Kung University, Apr. 1994.
   - Cited in the book by Bruce Schneier "Applied Cryptography (2nd Edition)", published by John Wiley & Sons, 1996.
   - On Mar. 8 1995, requested by:
     William Stallings (author of "Network and Internetwork Security")
   - On Jan. 26 1995, requested by:
     Prof. Lam Kwok-Yan
     Department of Information Systems and Computer Science
     University of Singapore
     Kent Ridge
     Singapore 0511, REPUBLIC OF SINGAPORE
   - On May 25, 1999, requested by:
     Olivier Chevassut
     Information and Computing Sciences Divisions
     Ernest Orlando Lawrence Berkeley National Laboratory
     One Cyclotron Road, 50B-2239
     Berkeley, CA 94720, USA
   - Cited in S.J. Hwang's Ph.D. thesis "The Design and Server-Aided Secret Computation of Digital Signatures", Institute of Computer and Information Science, National Chiao-Tung University, May 1996.
   - Cited in K.C. Chang and J.H. Fea's paper "An ID-based Cryptosystem Using Lucas Function for Authentication and Conference Key Broadcasting Scheme," *Proc. of ISC '96*, pp.215-223, May 1996.
2. S.M. Yen, "The Study of Fast Exponentiation Based on Addition Sequence and Signed Digit Arithmetic," Master thesis of Department of Electrical Engineering, National Cheng Kung University, June 1991.
   - On Jan. 26 1995, requested by:
     Prof. Lam Kwok-Yan
     (a member of the committee of 3rd ACM Conference on Security)
     Department of Information Systems and Computer Science
     Kent Ridge
     Singapore 0511, REPUBLIC OF SINGAPORE
   - On September 7, 1995, requested by:
     Yong-Fei Han
     Department of Computer Science
     Royal Holloway
     University of London
     Egham, Surrey TW20 0EX
     United Kingdom

3. S.M. Yen, "Vulnerability of the SVP Micropayment Scheme," *LCIS Tech. Report TR-99-2*, January 1999.

   - On July 1999, requested by:
     Matthew Prebble
     Department of Computer Science
     University of Bristol
     United Kingdom

4. S.M. Yen, "Comparisons of PayWord and Millicent Micropayment Systems," *LCIS Tech. Report TR-98-13*, July 1998.

   - On July 1999, requested by:
     Matthew Prebble
     Department of Computer Science
     University of Bristol
     United Kingdom

5. S.M. Yen, "Overview of Integer Factorization – Key Length Requirement of Public Key Cryptosystem," *Information Security Newsletter*, Vol.1, No.3, pp.7-10, March 1995.

   - Cited in the book by C.S. Laih, L. Harn, and C.C. Chang, "Contemporary Cryptography and Its Applications", published by UNALIS Book Company, Sept. 1995.

6. S.M. Yen, "Investigation and Suggestion of NII Security Technique and Architecture," Technical Report of project G4-85012-20, (supported by the Industrial Technology Research Institute, Computer & Communication Research Laboratories), June 1996.

   - On Dec. 1996, requested by:
     Dr. Kwo-Jean Farn
     CCL/ITRI
     Taiwan, R.O.C.

7. S.M. Yen, "Study on the Privacy Enhanced Mail and Its Related Cryptographic Techniques," Technical Report of project NSC-85-2213-E-212-007, (supported by the National Science Council), July 1996.

   - On Dec. 1996, requested by:
     Prof. Chi-Sung Laih
     Dept. of Electrical Engineering
     National Cheng Kung University
     Taiwan, R.O.C.