Chanathip Namprempre

Department of Electrical and Computer Engineering
nchanath@engr.tu.ac.th
http://chanathip.ece.engr.tu.ac.th

Faculty of Engineering, Thammasat University
Rangsit Campus, Klong Luang
Pathumthani, Thailand 12120

Research Interests

CRYPTOGRAPHY:	encryption, message authentication, digital signatures, identification, authenticated encryption, forward security, threshold cryptography.
ELECTRONIC COMMERCE:	secure protocols, blind signatures, electronic payments.
COMPUTER SECURITY:	intrusion detection.
DISTRIBUTED SYSTEMS:	optimistic execution, causal logging.

Education

University of California, San Diego, La Jolla, California.
PH.D. Computer Science, September 2002.
AREA: Cryptography, computer system security, distributed systems.
THESIS: Simultaneously Ensuring Privacy and Authenticity in Digital Communication

Massachusetts Institute of Technology, Cambridge, Massachusetts.
M.ENG. Electrical Engineering and Computer Science, June 1997.
THESIS: *Electrocardiography in DICOM*
B.S. Computer Science and Engineering, June 1996.
AREA: Information retrieval, content routing system.

Professional Experience

October 2002 – Present. Associate Professor.
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING, THAMMASAT UNIVERSITY.
Perform research and teach undergraduate and graduate courses (both in the standard and the international programs). Courses include discrete mathematics, computer programming, and introduction to computer security and cryptography. International program instruction is in English.

August 2002 – September 2002. Security Consultant.
IMAGINEER SOFTWARE, INC.
Reviewed and improved the company's security protocols and system infrastructure.

June 1999 – September 2002. Graduate Student Researcher with Dr. Mihir Bellare.
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, UCSD.
Performed research on cryptography, including encryption, authentication, and identification protocols, as well as protocols for electronic commerce such as blind signature schemes.

May 2001 – August 2001. Senior Engineer.

CYBERDOG COMMUNICATION, INC.
Designed secure protocols and system infrastructure.

March 1998 – May 1999. Graduate Student Researcher with Dr. Keith Marzullo.
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, UCSD.
Performed research on fault-tolerant distributed systems with focus on optimistic execution and intrusion detection in a CORBA environment.

June 1998 – September 1998. Engineering Intern.
QUALCOMM, INCORPORATED.
Performed research on frameworks for building fault-tolerant systems.

June 1996 – June 1997. Graduate Student Researcher with Dr. C. Forbes Dewey.
THE INTERNATIONAL CONSORTIUM FOR MEDICAL IMAGING TECHNOLOGY, MIT
Performed research on providing support for Electrocardiogram data in the Digital Imaging and Communications in Medicine (DICOM) standard.

June 1995 – December 1996. Undergraduate Researcher with Dr. David Gifford.
LABORATORY FOR COMPUTER SCIENCE, MIT.
Performed research on document clustering algorithms for information retrieval.

Publications

[1] C. Namprempre, P. Rogaway, and T. Shrimpton Reconsidering Generic Composition. In P. Nguyen and E. Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 257–274. Springer-Verlag, Berlin Germany, May 2014.

[2] M. Bellare, A. Boldyreva, and C. Namprempre. On-line Ciphers and the Hash-CBC Constructions *Journal of Cryptology*, 25(4): 640–6679, Oct 2012. Impact Factor 2.265.

[3] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of Cryptology*, 21(4):469–491, Oct 2008. Impact Factor 2.265.

[4] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 22(1):1–61, Jan 2009. Impact Factor 2.265.

[5] M. Abdalla, J. H. An, M. Bellare, and C. Namprempre. From identification to signatures via the Fiat-Shamir transform: Necessary and sufficient conditions for security and forward-security. *IEEE Transactions on Information Theory*, 54(8):3631–3646, Aug 2008. Impact Factor 3.793.

[6] M. Bellare, C. Namprempre, and G. Neven. Unrestricted aggregate signatures. *International Colloquium on Automata, Languages and Programming – ICALP 2007*, volume 4596 of *Lecture Notes in Computer Science*, pages 411–422. Springer-Verlag, Berlin Germany, Aug 2007.

[7] C. Namprempre and M. Dailey. Mitigating dictionary attacks with a text-graphics character CAPTCHA. *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences*, E90-A(1):179–186, Jan 2007. Impact Factor 0.437.

[8] C. Namprempre, G. Neven, and M. Abdalla. A study of blind message authentication codes. *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences*, E90-A(1):75–82, Jan 2007. Impact Factor 0.437.

[9] M. Abdalla, C. Namprempre, and G. Neven. On the (im)possibility of blind message authentication codes. In D. Pointcheval, editor, *Topics in Cryptology – CT-RSA 2006*, volume 3860 of *Lecture Notes in Computer Science*, pages 262–279. Springer-Verlag, Berlin Germany, February 2006.

[10] M. Dailey and C. Namprempre. A text-graphics character CAPTCHA for password authentication. IEEE TENCON 2004, pages B045–B048, November 2004.

[11] M. Bellare, T. Kohno, and C. Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm. *ACM Transactions on Information and System Security (TISSEC)*, 7(2):206–241, May 2004.

[12] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer-Verlag, Berlin Germany, May 2004.

[13] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *Journal of Cryptology*, 16(3): 185–215, June 2003. Impact Factor 2.265.

[14] C. Namprempre. Secure channels based on authenticated encryption schemes: A simple characterization. In Y. Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 515–532. Springer-Verlag, Berlin Germany, 2002.

[15] M. Bellare, T. Kohno, and C. Namprempre. Provably fixing the SSH binary packet protocol. In R. Sandhu, editor, *Proceedings of the 9th Conference on Computer and Communications Security*, pages 1–11. ACM Press, November 2002.

[16] M. Abdalla, J. H. An, M. Bellare, and C. Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In L. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 418–433. Springer-Verlag, Berlin Germany, April 2002.

[17] M. Bellare, A. Boldyreva, L. Knudsen, and C. Namprempre. On-line ciphers and the hash-CBC construction. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 292–309. Springer-Verlag, Berlin Germany, August 2001.

[18] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The power of RSA inversion oracles and the security of chaum's RSA-based blind signature scheme. In P. Syverson, editor, *Financial Cryptography 2001*, volume 2339 of *Lecture Notes in Computer Science*, pages 319–338. Springer-Verlag, Berlin Germany, February 2001.

[19] M. Abdalla, S. Miner, and C. Namprempre. Forward secure threshold signature schemes. In D. Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 441–456. Springer-Verlag, Berlin Germany, April 2001.

[20] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In T. Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer-Verlag, Berlin Germany, December 2000.

[21] C. Namprempre, J. Sussman, and K. Marzullo. Implementing causal logging using OrbixWeb interception. In *Proceedings of the 5th USENIX Conference on Object-Oriented Technologies and Systems — COOTS 1999*, pages 57–67, San Diego, California, May 1999.

[22] R. Weiss, B. Velez, M. Sheldon, C. Namprempre, P. Szilagyi, and D. Gifford. Hypursuit: A hierarchical network search engine that exploits content-link hypertext clustering. In *Proceedings of the 7th ACM Conference on Hypertext — Hypertext 1996*, pages 180–193, March 1996.

Invited Presentations

[1] Cloud Computing and Security. *Pathumthani University*, Pathumthani, Thailand, Nov 2014.

[2] Cryptography: A Necessary, but Not Sufficient, Component in Electronic Payment Systems. *World Bitcoin, Digital Money & Payment Systems Conference*, Bangkok, Thailand, Nov 2014.

[3] Encryption Standards. *Thailand Open Source Software Festival 2014*, Bangkok, Thailand, Oct 2014.

[4] A Whirlwind Tour of Modern Cryptography. *Asian Institute of Technology*, Patumtani, Thailand, May 2006.

[5] Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *Thammasat University*, Patumtani, Thailand, Dec 2000.

[6] Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *Chulalongkorn University*, Bangkok, Thailand, Dec 2000.

[7] Electrocardiography in DICOM. *Imperial College*, London, England, Dec 1997.

Conference Presentations

[8] A Text-Graphics Character CAPTCHA for Password Authentication. *IEEE TENCON 2004.* Chiangmai, Thailand, November 2004.

[9] Secure channels based on authenticated encryption schemes: A simple characterization. *ASIACRYPT 2002.* Queenstown, New Zealand, December 2002.

[10] The Power of RSA Inversion Oracles and the Security of Chaum's RSA-Based Blind Signature Scheme. *Financial Cryptography 2001.* Grand Cayman, BWI, February 2001.

[11] Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *ASIACRYPT 2000.* Kyoto, Japan, December 2000.

Professional Activities

Program commitee member:

- ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2008
- International Conference on Provable Security (ProvSec) 2007
- Progress in Cryptology – VietCrypt 2006
- Theory of Cryptography (TCC) 2006
- ACM Conference on Computer and Communications Security (CCS) 2004
- Applied Cryptography and Network Security (ACNS) 2004
- International Conference on Information Security and Cryptology (ICISC) 2003

Reviewer:

- Information Processing Letters
- Journal of Systems and Software
- IEEE Transactions on Wireless Communications
- Information and Computation
- Institute of Electronics, Information, and Communication Engineers
- Advances in Cryptology – Eurocrypt 2004

Member:

- International Association for Cryptologic Research (IACR)

Skills

Computer: Ruby, Rails, Unix, Windows, Java, CORBA, PHP, Mysql, HTML
Languages: English, Thai

References

PROFESSOR MIHIR BELLARE
Department of Computer Science & Engineering UCSD, 9500 Gilman Drive,
La Jolla, CA 92093-0114. Phone: (858) 534-4544 E-Mail: mihir@cs.ucsd.edu

Others available upon request.