

CURRICULUM VITAE

Joonsang Baek

Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
Email: jsbaek@gmail.com
Tel: +65 6874 6674 Fax: +65 6774 4990

1 Education

- PhD, Faculty of Information Technology, Monash University, Australia, April 2004
 - Thesis title: Construction and Formal Security Analysis of Cryptographic Schemes in the Public Key Setting
- MS in Computer Science, School of Engineering, Information and Communications University (ICU), Korea, August 2000
 - Thesis title: A Study on Provable Security of Public-Key Encryption Schemes and Key Agreement Protocols
- BS in Mathematics, Department of Mathematics, Pohang University of Science and Technology (POSTECH), Korea, February 1998

2 Employment History (Full-time Only)

- Research Fellow, Institute for Infocomm Research, 21 March 2006 – present
- Associate Research Fellow, School of Information Technology and Computer Science, University of Wollongong, 1 April 2004 – 15 March 2006 ”
- Research Staff, SECUi.COM Corp., Korea, 26 August 2000 - 20 February 2001
- Researcher, Basic Science Research Institute, Department of Mathematics, POSTECH, Korea, 19 February 1998 – 18 August 1998

3 Professional Activities

- Program Committee Member
 - International Conference on Information Security and Cryptology 2008 (ICISC 2008), Seoul, Korea
 - The International Conference on Cryptology and Network Security 2008 (CANS 2008), Hong Kong, PR China
 - International Conference on Provable Security 2008 (ProvSec 2008), Shanghai, PR China
 - International Conference on Emerging Security Information, Systems and Technologies 2008 (SECURWARE 2008), Cap Esterel, France
 - International Conference on Security and Cryptography 2008 (SECRYPT 2008), Porto, Portugal
 - Information Security Practice and Experience Conference 2008 (ISPEC 2008), Wollongong, Australia
 - International Conference on Emerging Security Information, Systems and Technologies 2007 (SECURWARE 2007), Valencia, Spain
 - International Conference on Information Security and Cryptology 2007 (ICISC 2007), Seoul, Korea
 - The International Workshop on Interactive Multimedia & Intelligent Services in Mobile and Ubiquitous Computing 2007 (IMIS-07), Seoul, Korea
 - The International Workshop on Service, Security and its Data management for Ubiquitous Computing (SSDU-07) 2007, Nanjing, PR China
 - International Conference on Security and Cryptography 2007 (SECRYPT 2007), Barcelona, Spain
 - International Conference on Provable Security 2007 (ProvSec 2007), Wollongong, Australia
 - Information Security Practice and Experience Conference 2007 (ISPEC 2007), Hong Kong, PR China
 - International Conference on Information Security and Cryptology 2006 (ICISC 2006), Busan, Korea
 - Applied Cryptography and Information Security 2006 (ACIS 2006), Edinburgh, UK
 - International Workshop on Security in Ubiquitous Computing System 2006 (SECUBIQ 2006), Seoul, Korea
- External referee for ICISC 2001, ACISP 2001, ACISP 2002, Asiacrypt 2002, CT-RSA 2002, CT-RSA 2003, PKC 2003, PKC 2004, Asiacrypt 2004, PKC 2005, IEEE-Security & Privacy 2005, ISPEC 2005, ISC 2005, ACM-CCS 2005, Asiacrypt 2005, ACM-DRM

2005, ICICS 2005, ISPEC 2006, ACM-ASIA-CCS 2006, ACNS 2006, Crypto 2006, ISCIS 2006, WISA 2006, IWSEC 2006, VietCrypt 2006, Asiacrypt 2006, ACNS 2007, ACISP 2007, ACM-CCS 2007, ESORICS 2007, INSCRYPT 2007, ACNS 2008

4 Successful Grant Applications

- Australia Research Council (ARC) Discovery Project Grant (with W. Susilo and Y. Mu), *Secure and Practical Anonymous Electronic Payment and Applications*, 2008 – 2010
- Microsoft Asia Research Grant (with R. Safavi-Naini, Y. Mu, J. Horton, W. Susilo and W. Li), *Trusted Computing*, 2006

5 Teaching Experience

- University of Wollongong
 - Procedural Programming (CSCI114), Assistant Subject Coordinator, July 2005 – February 2006
 - Algorithms and Problem Solving (CSCI103), Tutor, July 2005 – November 2005
 - Procedural Programming (CSCI114), Tutor, February 2005 - June 2005
- Monash University
 - Object-Oriented Programming in Java (CPE1001), Tutor, 2002 - 2003
 - System Modeling and Simulation (CPE1005), Tutor, 2002
 - Information and Network Security (CPE3001), Lecturer/Tutor, 2001 - 2002
 - Object Oriented Design and Programming (CPE1004), Tutor, 2001
- Information and Communications University
 - Concrete Mathematics (ICE615), Tutor, 2000

6 Students Supervision

- S. Shahandashti, PhD student, University of Wollongong, January 2006 – March 2006
- L. Luo, Master of Science by Research student, University of Wollongong, May 2004 – March 2006

7 Awards

- International Postgraduate Research Scholarship (IPRS), Department of Education, Science and Training Youth Affairs (DEST), Australian Government, 2001 - 2003
- Monash Graduate Scholarship (MGS), Monash University, 2001 - 2003.
- Distinction Scholarship, Information and Communications University (ICU), Korea, 1999
- Brain Korea 21 Scholarship, Ministry of Information and Communications (MIC), Korean Government, 1999-2000

8 Publications

- Book Chapters
 1. J. Baek, W. Susilo and J. Zhou, *Fuzzy Identity-based Encryption: New and Efficient Schemes* Chapter ?? of "Coding and Cryptology", ISBN ??, World Scientific Press, 2008, to appear.
 2. J. Baek, E. Foo, H. Tan and J. Zhou, *Securing Wireless Sensor Networks - Threats and Countermeasures*, Security and Privacy in Wireless and Mobile Computing, ISBN 978-1905886-906, Troubador Publishing, 2008.
 3. J. Baek and R. Steinfeld, *Security for Signcryption: The Multi-User Model*, Practical Signcryption, A. Dent and Y. Zheng (eds.), Springer Verlag, 2007, to appear.
- Refereed Journal Papers
 1. J. Baek, R. Steinfeld and Y. Zheng, *Formal Proofs for the Security of Signcryption*, Journal of Cryptology, Vol. 20, No. 2, April, pp 203-235, Springer-Verlag, 2007.
 2. J. Baek and Y. Zheng, *Zheng and Seberry's Public Key Encryption Scheme Revisited*, International Journal of Information Security (IJIS), Springer-Verlag, Vol. 2, No. 1, November, pp. 37-44, 2003.
 3. J. Baek, B. Lee and K. Kim, *Provably Secure Length-Saving Public-Key Encryption Scheme under the Computational Diffie-Hellman Assumption*, ETRI Journal Vol. 22, No.4, December, pp. 25-31, 2000.
 4. J. Baek and K. Kim, *Remarks on the Unknown Key-Share Attacks*, IEICE (Institute of Electronics, Information and Communications Engineers) Transactions on Fundamentals of Electronics, Vol. E83-A, No.12, December, pp. 2766-2769, 2000.
- Refereed Conference Papers

1. J. Baek, D. Galindo, W. Susilo and J. Zhou, Constructing Strong KEM from Weak KEM (or How to Revive the KEM/DEM Framework), Proc. of the 6th Conference on Security and Cryptography for Networks (SCN 2008), Lecture Notes in Computer Science, 2008, to appear.
2. J. K. Liu, J. Baek, W. Susilo and J. Zhou, Certificate Based Signature Schemes without Pairings or Random Oracles , Proc. of the 11th Information Security Conference (ISC'08), Lecture Notes in Computer Science, Springer Verlag, 2008, to appear.
3. J. Baek, H. Tan, J. Zhou and J. Wong, *Realizing Stateful Public Key Encryption in Wireless Sensor Network*, Proc. of the 23rd International Information Security Conference (IFIP-SEC 2008), Lecture Notes in Computer Science, 2008, to appear.
4. J. Baek, J. Zhou and F. Bao, *Generic Constructions of Stateful Public Key Encryption and Their Applications*, Proc. of the 6th International Conference on Applied Cryptography and Network Security (ACNS 2008), Lecture Notes in Computer Science 5037, pp. 75–93, Springer-Verlag, 2008.
5. Y. Sun, F. Zhang and J. Baek, *Strongly Secure Certificateless Public Key Encryption without Pairing*, Proc. of the 6th International Conference on Cryptology and Network Security (CANS 2007), Lecture Notes in Computer Science 4856, pp. 194–208, Springer-Verlag, 2007.
6. G. Wang, J. Baek, D. S. Wong and F. Bao. *On the Generic and Efficient Constructions of Secure Designated Confirmer Signatures*, Proc. of International Workshop on Public Key Cryptography 2007 (PKC 2007), Lecture Notes in Computer Science 4450, pp. 43 – 60, Springer-Verlag, 2007.
7. J. Baek, W. Susilo and J. Zhou, *New Constructions of Fuzzy Identity-Based Encryption*, Proc. of ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007), pp. 368–370, ACM Press, 2007.
8. S. Shahandashti, R. Safavi-Naini and J. Baek, *Concurrently-Secure Credential Ownership Proofs*, Proc. of ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007), pp. 161–172, ACM Press, 2007.
9. J. Baek, R. Safavi-Naini and W. Susilo, *On the Integration of Public Key Data Encryption and Public Key Encryption with Keyword Search*, Proc. of Information Security Conference 2006 (ISC 2006), Lecture Notes in Computer Science 4176, pp. 217 - 232, Springer-Verlag, 2006.
10. J. Baek, R. Safavi-Naini and W. Susilo, *Public Key Encryption with Keyword Search Revisited*, Proc. of Applied Cryptography and Information Security 2006 (ACIS 2006), Lecture Notes in Computer Science, Springer-Verlag, 2006, to appear.
11. L. Luo, R. Safavi-Naini, J. Baek and W. Susilo, *Self-Organised Group Key Management for Ad-hoc Networks*, Proc. of the 1st ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS 2006), pp. 138- 147, ACM Press, 2006.

12. J. Baek, R. Safavi-Naini and W. Susilo, *Universal Designated Signature Proof (or How to Efficiently Prove the Knowledge of a Signature)*, Advances in Cryptology -Proc. of Asiacrypt 2005, Lecture Notes in Computer Science 3788, pp. 644-661, Springer-Verlag, 2006.
13. Y Chen, R. Safavi-Naini and J. Baek, *Server-Aided RSA Key Generation against Collusion Attack*, Proc. of Secure Mobile Ad-hoc Networks and Sensors 2005 (MADNES 2005), Lecture Notes in Computer Science 4074, pp. 27-37, Springer-Verlag, 2006.
14. J. Baek, R. Safavi-Naini and W. Susilo, *Certificateless Public Key Encryption without Pairing*, Proc. of Information Security Conference 2005 (ISC 2005), Lecture Notes in Computer Science 3650, pp. 134-148, Springer-Verlag, 2005.
15. J. Baek, R. Safavi-Naini and W. Susilo, *Token-Controlled Public Key Encryption*, Proc. of Information Security Practice and Experience Conference 2005 (ISPEC 2005), Lecture Notes in Computer Science 3439, pp. 386 - 397, Springer-Verlag, 2005.
16. J. Baek, R. Safavi-Naini and W. Susilo, *Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption*, Proc. of International Workshop on Public Key Cryptography 2005 (PKC 2005), Lecture Notes in Computer Science 3386, pp. 380 - 397, Springer-Verlag, 2005.
17. J. Baek, J. Newmarch, R. Safavi-Naini and W. Susilo, *A Survey of Identity-Based Cryptography*, Proc. of Australian Unix Users Group Annual Conference 2004 (AUUG 2004), pp. 95-102, 2004.
18. J. Baek and Y. Zheng, *Identity-Based Threshold Signature Scheme from the Bilinear Pairing*, Proc. of the Information Assurance and Security (IAS) track of International Conference on Information Technology, Coding and Computing 2004 (ITCC 2004), pp. 124-128, IEEE Computer Society, 2004.
19. J. Baek and Y. Zheng, *Identity-Based Threshold Decryption*, Proc. of International Workshop on Public Key Cryptography 2004 (PKC 2004), Lecture Notes in Computer Science 2947, pp. 262-276, Springer-Verlag, 2004.
20. J. Baek and Y. Zheng, *Simple and Efficient Threshold Cryptosystem from the Gap Diffie-Hellman Group*, Proc. of IEEE Global Communications Conference 2003 (GLOBECOM 2003), Communication Security Track, pp. 1491-1495, IEEE Press, 2003.
21. R. Steinfeld, J. Baek and Y. Zheng, *On the Necessity of Strong Assumptions for the Security of a Class of Asymmetric Encryption Schemes*, Proc. of Australasian Conference on Information Security and Privacy 2002 (ACISP 2002), Lecture Notes in Computer Science 2384, pp. 241-256, Springer-Verlag, 2002.
22. J. Baek, R. Steinfeld and Y. Zheng, *Formal Proofs for the Security of Signcryption*, Proc. of International Workshop on Public Key Cryptography 2002 (PKC 2002), Lecture Notes in Computer Science 2274, pp. 80-98, Springer-Verlag, 2002.

23. H. Kim, J. Baek, B. Lee and K. Kim, *Computing with Secrets for Mobile Agent using One-Time Proxy Signature*, Proc. of Symposium on Cryptography and Information Security 2001 (SCIS 2001), Vol.2/2, pp.845-850, 2001.
24. H. Kim, J. Baek, G. Ahn, J. Kim, H. Park, B. Song, M. Lee, J. Park, J. Go, B. Lee and K. Kim, *Design and Implementation of Revocable Electronic Cash System based on Elliptic Curve Discrete Logarithm Problem*, Proc. of Workshop on Information Security Application 2000 (WISA 2000), pp. 85-102, 2000.
25. J. Baek, B. Lee and K. Kim, *Secure Length-saving ElGamal Encryption under the Computational Diffie-Hellman Assumption*, Proc. of Australasian Conference on Information Security and Privacy 2000 (ACISP 2000), Lecture Notes in Computer Science 1841, pp.49-58, Springer-Verlag, 2000.
26. J. Baek, K. Kim and T. Matsumoto, *On the Significance of Unknown Key-Share Attacks: How to Cope with Them?*, Proc. of Symposium on Cryptography and Information Security (SCIS 2000), C29, 2000.
27. K. Kim, S. Park and J. Baek, *Improving Fairness and Privacy of Zhou-Gollmann's Fair Non-Repudiation Protocol*, Proc. of International Workshop on Security '99 (IWSEC '99), pp.140-145, IEEE Computer Society, 1999.

9 Invited Talks

- *Efficient Public Key Broadcast Encryption*, Centre for Advanced Computing, Algorithms and Cryptography, Macquarie University, Sydney, 14 January 2005
- *State of the Art of Identity-Based Cryptography*, Mathematics of Communications Security, Australian Mathematical Science Institute (AMSI), University of Melbourne, Melbourne, 20 November 2003
- *Identity-Based Threshold Decryption*, Victorian Communications and Security Research Seminar, Royal Melbourne Institute of Technology (RMIT), Melbourne, 11 June 2003
- *Zheng and Seberry's Encryption Scheme Revisited*, Victorian Communications and Security Research Seminar, Royal Melbourne Institute of Technology (RMIT), Melbourne, Australia, 11 June 2003. Melbourne, 13 November 2002