CURRICULUM VITAE

Joonsang Baek

1 Contact Information

- Mailing address:
  Khalifa University of Science, Technology and Research (KUSTAR)
  P.O. Box 127788
  Abu Dhabi, UAE
- Contact emails:
  joon.baek@kustar.ac.ae, jsbaek@gmail.com
- Telephone numbers:
  Tel (Office): +971 2 501 8587
  Tel (Mobile): +971 56 611 2546
  Fax:+971 2 4472 442

2 Education

- PhD in Computer Science, 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 Engineering, School of Engineering, KAIST (Former Information and Communication University), 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.

3 Employment History (Full-Time Only)

- Assistant Professor, Khalifa University of Science, Technology and Research (KUSTAR), 25 March 2011 – Present.
- Research Scientist, Institute for Infocomm Research, 21 March 2006 – 22 March 2011.
- Postdoctoral Research Fellow, School of Information Technology and Computer Science, University of Wollongong, 1 April 2004 – 15 March 2006.
- Research Staff, Samsung 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.

4 Professional Activities

- Program Committee Member
  - Year 2015: ACISP, ICPAD, SocialSec, 3PGCIC (Security Track Chair)
  - Year 2014: ACISP, NSS, ICISC, ISPEC
  - Year 2013: ACISP, ARES, NSS, ICISC
  - Year 2012: AINA (Also served as Program Vice Chair), ACISP, ARES, InCos, NSS, ICISC
  - Year 2011: ACISP ICTC, ICICS, ISC, ProvSec, WISA, ICISC
  - Year 2009: WISA, SECRYPT, ICISC, ProvSec
  - Year 2008: ICISC, CANS, ProvSec, SECURWARE, SECRYPT, ISPEC
  - Year 2007: ICISC, SECRYPT, ProvSec, ISPEC, ICISC
  - Year 2006: ACIS
  - 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, ACNS 2009.
- Reviewer for Journals
  - The Computer Journal, Designs, Codes and Cryptography, IEEE Transactions on Information Forensics & Security, Information Processing Letters, Security and Communication Networks, IEEE Transactions on Computers, International Journal of Computer Mathematics, International Journal of Information Security, IET security, Aerospace Science & Technology

5 Successful Grant Applications

- Khaliafa University Internal Research Fund (KUIRF) (with Q. Vu and A. Jones), *A Flexible, Scalable, and Secured Resource Management Framework for Smart Grid*, 2012–2013
- 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

6 Teaching Experience

- Khalifa University
  - Advanced Internet and Computing Paradigms (ECCE631), 2015 January – Present.
  - Stochastic Processes and Random Variables (MATH603), Lecturer, September 2013 - September 2014.
  - Complex Variables and Transforms (MATH312), Lecturer, September 2013 - September 2014.
  - Introduction to Cryptography (ISEC602), Lecturer, March 2013 – Present.
  - Mathematics for Information Security (ISEC614), Lecturer, March 2013 – Present.
  - Fundamentals of Engineering Mathematics I, (ISEC501), Lecturer, September 2012 – February 2013.

- Principles of Computer Programming (CMPE111), Lecturer, September 2011 – June 2012.
- Cryptographic Algorithm Design (E618), Lecturer, March 2011 – June 2011.

- 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.

7 Students Supervision

- Ahmed AlShemeili, MSc Student at KUSTAR, September 2013 - December 2014.
- Eman Hableel, MSc Student at KUSTAR, September 2013 - September 2014.
- Nour Al Ebri, MSc Student at KUSTAR, September 2011 - September 2012.
- Hajer Al Housani, MSc Student at KUSTAR, September 2011 - September 2012.
- Jangseung Kim, PhD student at Information and Communications University, Korea, I^2R Post-graduate Attachment Program, November 2008 – February 2009.
- Siamak Shahandashti, PhD student, University of Wollongong, January 2006 – March 2006.
- Ling Luo, Master of Science by Research student,University of Wollongong, May 2004 – March 2006.

8 Publications

- Edited Book
  1. J. Baek, F. Bao, K. Chen and X. Lai, *Provable Security, Second International Conference, ProvSec 2008*, Shanghai, China, October 30 - November 1, 2008. Proceedings Springer 2008.

- Book Chapters
  2. J. Baek, W. Susilo and J. Zhou, *Fuzzy Identity-based Encryption: New and Efficient Schemes*, Series on Coding Theory and Cryptology Vol. 4, ISBN 978-981-283-223-8, World Scientific Press, pp. 1-14, 2008.
  3. 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.

4. J. Baek and R. Steinfeld, *Security for Signcryption: The Multi-User Model*, Practical Signcryption, A. Dent and Y. Zheng (eds.), Springer Verlag, 2009, to appear.

- Refereed Journal Papers

5. J. Baek, Y. Byon, E. Hableel and M. Al-Qutayri, *Making Air Traffic Surveillance More Reliable: A New Authentication Framework for Automatic Dependent Surveillance-Broadcast (ADS-B) Based on Online/Offline Identity-Based Signature*, Security and Communication Networks 8(5): 740–750, 2015.
6. L. Xu, J. Li, S. Tang and J. Baek, J. *Server-Aided Verification Signature with Privacy for Mobile Computing*, Mobile Information Systems, Online Published Vol. 2015, Article ID 626415, 11 pages, 2015. doi:10.1155/2015/626415, 2015.
7. J. Baek, Q. Vu, J. Liu, X. Huang and Y. Xiang, *A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid*, IEEE Transactions on Cloud Computing, 3(2): 233-244, 2015.
8. J. Baek, Q. Vu, A. Shoufan, A. Jones, and D. S. Wong, *Stateful Public-Key Encryption Schemes Forward-Secure Against State Exposure*. The Computer Journal, 56(4): 497–507, Oxford Press, 2013.
9. N. Al Ebri, J. Baek, A. Shoufan, Q. Vu, *Forward-Secure Identity-Based Signature: New Generic Constructions and Their Applications*, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 4(1): 32-54, 2013.
10. J. Kim, J. Baek and T. Shon, *An Efficient and Secure Service Discovery Protocol for Ubiquitous Computing Environments*, IEICE Transactions on Fundamentals of Electronics, IEICE Transactions 95-D(1): 117-125, 2012.
11. J. Kim, J. Baek and T. Shon, *An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network* IEEE Transaction on Consumer Electronics, pp. 516–522, IEEE Press, 2011.
12. J. K. Liu, J. Baek, J. Zhou, Y. Yang and J. Wong, *Efficient online/offline Identity-Based Signature for Wireless Sensor Network*, International Journal of Information Security (IJIS), 9(4): 287–296, Springer-Verlag, 2010.
13. 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.
14. 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.
15. 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.
16. 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

17. E. Hableel, J. Baek, Y. Byon and D. S. Wong, *How to Protect ADS-B: Confidentiality Framework for Future Air Traffic Communication* IEEE Infocom Workshop on Mobility Management in the Networks of the Future World, April 2015, To appear.
18. H. AlNoon, A. Shoufan and J. Baek, *On the Power Consumption of Cryptographic Processors in Civil Microdrones*, International Conference on Information Systems Security and Privacy (ICISSP), 2015.

19. E. Hableel, C. Yeun and J. Baek, *Emerging Trend of Cybercrime in the UAE*, The 6th FTRA International Symposium on Advances in Computing, Communications, Security, and Applications (ACSA-14), 2014.
20. E. Al-Alkeem, C. Yeun and J. Baek, *Secure NFC Authentication Protocol Based on LTE Network*, Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering Volume 280, 2014, pp 363-371.
21. Y. Byon, Y. Jeong, S. Essa and J. Baek, *Feasibility Analysis of Transportation Applications Based on APIs of Social Network Services*, IEEE ICIST 2013, pp 59–64.
22. E. Hableel, J. Baek and Y. Byon, *Public Key Infrastructure for UAE: A Case Study*, SIN 2013, pp. 336–340.
23. J. Baek, Y. Byon, E. Hableel and M. Al-Qutayri, *An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature*, The Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet 3PGCIC 2013: pp. 358–363, IEEE Computer Society.
24. J. Baek, Q. Vu, A. Jones, S. Al-Mulla, C. Yeun, *Smart-Frame: A Flexible, Scalable, and Secure Information Management Framework for Smart Grids.* ICITST 2012: pp. 668–673, IEEE, 2012.
25. N. Al Ebri, J. Baek, A. Shoufan, Q. Vu, *Efficient Generic Construction of Forward-Secure Identity-Based Signature*, Conference on Availability, Reliability and Security (ARES 2012), pp. 55–64, IEEE Computer Society.
26. J. Baek and J. Zhou, *Compact Identity-Based Encryption without Strong Symmetric Cipher*, Proc. of ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011), pp. 61–70, 2011.
27. W. Susilo and J. Baek, *On the Security of the Identity-based Encryption based on DHIES from ASIACCS 2010*, Proc. of ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011), pp. 376-380, 2011.
28. J. Baek, C. Chu and J. Zhou, *On Shortening Ciphertexts: New Constructions for Compact Public Key and Stateful Encryption Schemes* , The Cryptographers' Track at the RSA Conference 2011 (CT-RSA 2011) Lecture Notes in Computer Science 6558, pp. 302–318, Springer-Verlag, 2011.
29. J. Baek, W. Susilo, J. K. Liu and J. Zhou, *A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack* , Proc. of the 7th International Conference on Applied Cryptography and Network Security (ACNS 2009), Lecture Notes in Computer Science 5536, pp. 143–155, Springer-Verlag, 2009.
30. J. K. Liu, J. Baek and J. Zhou, *Certificate-Based Sequential Aggregate Signature*, Proc. of the 2nd ACM Conference on Wireless Network Security (Wisec 2009), pp.21–28, ACM, 2009.
31. 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 5229, pp. 358–374, Springer-Verlag, 2008.
32. 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 5222, pp. 285–297, Springer-Verlag, 2008.
33. 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), pp. 95–107, Springer, 2008.
34. 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.

35. J. Baek, R. Safavi-Naini and W. Susilo, *Public Key Encryption with Keyword Search Revisited*, Proc. of ICCSA 2008, Lecture Notes in Computer Science 5072, pp. 1249–1259, Springer-Verlag, 2008.
36. 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.
37. 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.
38. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.
45. 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.
46. J. Baek, R. Safavi-Naini and W. Susilo, *Efficient Multi-Reciever 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.
47. 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.
48. 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.
49. 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.
50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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 Personal Information

- Date of Birth: 5 Dec 1973
- Nationality: Citizen of Republic of Korea (South Korean)