Bibliography

[1] K. G. Paterson, J. C. N. Schuldt, M. Stam, and S. Thomson, "On the joint security of encryption and signature, revisited," in *ASIACRYPT: 17th Int. Conf. on Theory and Applicat. Of Cryptology and Inform. Security*, ser. Lecture Notes in Computer Science, vol. 7073, Springer, 2011, pp. 161–178.

[2] T. Acar, M. Belenkiy, M. Bellare, and D. Cash, "Cryptographic agility and its relation to circular encryption," in *EUROCRYPT: 29thAnnu. Int. Conf. on the Theory and Applicat. of Cryptographic Techniques*, ser. Lecture Notes in Computer Science, vol. 6110, Heidelberg: Springer, 2010, pp. 403–422.

[3] S. Haber and B. Pinkas, "Securely combining public-key cryptosystems," in *Proc. ACM Conf. on Comput. And Commun. Security*, ACM, Ed., 2001, pp. 215–224.

[4] M. I. G. Vasco, F. Hess, and R. Steinwandt, "Combined (identity-based) public key schemes," in *CryptologyePrintArchiveReport 2008/466*, 2008.

[5] J. H. An, Y. Dodis, and T.Rabin, "On the security of joint signature and encryption," in *EUROCRYPT*, 2002, pp. 83–107.

[6] Y. Komano and K. Ohta, "Efficient universal padding techniques for multiplicative trapdoor one-way permutation.," in *Proc. CRYPTO 2003, 23rd Annu. Int. Cryptology Conf.*, 2003, pp. 366–382.

[7] B. C. Mames, D. H. Phan, and D. Pointcheval, "Optimal asymmetric encryption and signature paddings," in *Proc. of Applied Cryptography and Network Security*, ser. Lecture Notes in Computer Science, vol. 3531, Springer-Verlag, 2005, pp. 254–268.

[8] J. S. Coron, M. Joye, D. Naccache, and P. Paillier, "Universal padding schemes for rsa," in *Proc. of CRYPTO*, ser. Lecture Notes in Computer Science, vol. 2442, Springer-Verlag, 2002, pp. 226–241.

[9] A. Menezes, P. V.Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[10] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes.," in *Advances in Cryptology - CRYPTO '98, 18th Annu. Int. Cryptology Conf., Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, 1998, pp. 26–45.

[11] D. P. Eiichiro Fujisaki Tatsuaki Okamoto and J. Stern, "Rsa-oaep is secure under the rsa assumption," in *Proc. of CRYPTO' 2001*, ser. Lecture Notes in Computer Science, vol. 2139, Springer-Verlag, 2001, pp. 260–274.

[12] "Pkcs #1: rsa encryption standard," *RSA Data Security*, 1991.

[13] W. M. S. M. D. Johnson A. Lee and J. Wilkins, "Hybrid key distribution scheme giving key record recovery," *IBM Technical Disclosure Bulletin*, 1994.

[14] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM conference on Computer and communications security*, ACM, 1993, pp. 62–73.

[15] M. Bellare and P. Rogaway, "Optimal asymmetric encryption - how to encrypt with rsa," in *Proc. of Eurocrypt*, ser. Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1994, pp. 92–111.

[16] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*, New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 10–18.

[17] Y. Tsiounis and M. Yung, "On the security of elgamal based encryption," in *Public Key Cryptography*, H. Imai and Y. Zheng, Eds., vol. 1431, ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1998, pp. 117–134.

[18] E. Fujisaki and T. Okamoto, *Secure integration of asymmetric and symmetric encryption schemes*, 1999.

[19] K. K. Joonsang Baek Byoungcheon Lee, *Provably secure length-saving public-key encryption scheme under the computational diffie-hellman assumption*, 2000.

[20] D. Boneh, “The decision diffie-hellman problem,” Springer-Verlag, 1998, pp. 48–63.

[21] M. Bellare and P. Rogaway, “The exact security of digital signatures: how to sign with rsa and rabin.”

[22] D. Stinson, *Cryptography: Theory and Practice*, econd Edition. Chapman & Hall, CRC, London, UK: CRC press, 2002.

[23] D. Pointcheval and J. Stern, “Security proofs for signature schemes,” in *Adv. in Cryptology Ű Proc. of EUROCRYPT 1996*, ser. Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 387–398.

[24] R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack,” in *CRYPTO*.

[25] M. Naor and M. Yung, “Public-key cryptosystems provably secure against chosen ciphertext attacks,” in *In Proc. of the 22nd STOC*, ACM Press, 1995, pp. 427–437.

[26] D. Dolev, C. Dwork, and M. Naor, “Non-malleable cryptography,” in *SIAM J. on Computing*, 2000, pp. 542–552.

[27] V. Shoup, “Oaep reconsidered,” in *J. of Cryptology*, Springer-Verlag, 2000, pp. 239–259.

[28] R. Cramer and V. Shoup, “Signature schemes based on the strong rsa assumption,” in *ACM TRANSACTIONS ON INFORMATION AND SYSTEM SECURITY*, ACM press, 1998, pp. 46–51.

[29] R. Gennaro, S. Halevi, and T. Rabin, “Secure hash-and-sign signatures without the random oracle,” in *Adv. in Cryptology Ű Proc. of Eurocrypt Š99*, Springer-Verlag, 1999, pp. 123–139.

[30] C. P. Schnorr, “Efficient signature generation by smart cards.,” *J. Cryptology*, vol. 4, pp. 161–174, 1991.

[31] D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” *J. OF CRYPTOLOGY*, vol. 13, pp. 361–396, 2000.

[32] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. of Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[33] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proceeding of SAC 2002*, ser. Lecture Notes in Computer Science, vol. 2595.

[34] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," Springer-Verlag, 2004, pp. 207–222.

[35] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," *J. Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[36] T. Matsuda, K. Matsuura, and J. C. N. Schuldt, "Efficient constructions of signcryption schemes and signcryption composability," in *Lecture Notes in Computer Science*, INDOCRYPT: 10th Int. Conf. on Cryptology in India, vol. 5922, Heidelberg: Springer, 2009, pp. 321–342.

[37] J. Sébastien and Coron, *Optimal security proofs for pss and other signature schemes*.