Gentry, Craig

Practical identity-based encryption without random oracles. (English) Zbl 1140.94340

Vaudenay, Serge (ed.), Advances in cryptology – EUROCRYPT 2006. 25th annual international conference on the theory and applications of cryptographic techniques, St. Petersburg, Russia, May 28 – June 1, 2006. Proceedings. Berlin: Springer (ISBN 3-540-34546-9/pbk). Lecture Notes in Computer Science 4004, 445-464 (2006).

Summary: We present an Identity Based Encryption (IBE) system that is fully secure in the standard model and has several advantages over previous such systems – namely, computational efficiency, shorter public parameters, and a "tight" security reduction, albeit to a stronger assumption that depends on the number of private key generation queries made by the adversary. Our assumption is a variant of Boneh et al.'s decisional Bilinear Diffie-Hellman Exponent assumption, which has been used to construct efficient hierarchical IBE and broadcast encryption systems. The construction is remarkably simple. It also provides recipient anonymity automatically, providing a second (and more efficient) solution to the problem of achieving anonymous IBE without random oracles. Finally, our proof of CCA2 security, which has more in common with the security proof for the Cramer-Shoup encryption scheme than with security proofs for other IBE systems, may be of independent interest.

For the entire collection see [Zbl 1108.94002].

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:

Identity Based Encryption

Full Text: DOI

References:

[1] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol.˜3621, pp. 205–222. Springer, Heidelberg (2005) · Zbl 1145.94430 · doi:10.1007/11535218_13

[2] Attrapadung, N., Chevallier-Mames, B., Furukawa, J., Gomi, T., Hanaoka, G., Imai, H., Zhang, R.: Efficient Identity Based Encryption with Tight Security Reduction. Cryptology ePrint Archive 2005/320 (2005)

[3] Bellare, M., Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In: Proc. of ACM CCS, pp. 62–73 (1993) · doi:10.1145/168588.168596

[4] Boneh, D., Boyen, X.: Efficient Selective-ID Identity Based Encryption without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol.˜3027, pp. 223–238. Springer, Heidelberg (2004) · Zbl 1122.94355 · doi:10.1007/978-3-540-24676-3_14

[5] Boneh, D., Boyen, X.: Secure Identity Based Encryption without Random Oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol.˜3152, pp. 443–459. Springer, Heidelberg (2004) · Zbl 1104.94019 · doi:10.1007/978-3-540-28628-8_27

[6] Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical Identity Based Encryption with Constant Size Ciphertext. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol.˜3494, pp. 440–456. Springer, Heidelberg (2005) · Zbl 1137.94340 · doi:10.1007/11426639_26

[7] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol.˜3027, pp. 506–522. Springer, Heidelberg (2004) · Zbl 1122.68424 · doi:10.1007/978-3-540-24676-3_30

[8] Boneh, D., Franklin, M.: Identity Based Encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol.˜2139, pp. 213–229. Springer, Heidelberg (2001) · Zbl 1002.94023 · doi:10.1007/3-540-44647-8_13

[9] Boneh, D., Franklin, M.: Identity Based Encryption from the Weil pairing. SIAM Journal of Computing˜32(3), 586–615 (2003) · Zbl 1046.94008 · doi:10.1137/S0097539701398521

[10] Boneh, D., Gentry, C., Waters, B.: Collusion-Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol.˜3621, pp. 258–275. Springer, Heidelberg (2005) · Zbl 1145.94434 · doi:10.1007/11535218_16

[11] Boneh, D., Katz, J.: Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity Based Encryption. In: Menezes,

A. (ed.) CT-RSA 2005. LNCS, vol.˜3376, pp. 87–103. Springer, Heidelberg (2005) · Zbl 1079.94535 · doi:10.1007/978-3-540-30574-3_8

[12] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol.˜2248, pp. 514–532. Springer, Heidelberg (2001) · Zbl 1064.94554 · doi:10.1007/3-540-45682-1_30

[13] Boyen, X., Mei, Q., Waters, B.: Direct Chosen Ciphertext Security from Identity Based Techniques. In: Proc. of ACM CCS, pp. 320–329 (2005) · doi:10.1145/1102120.1102162

[14] Boyen, X., Waters, B.: Anonymous Hierarchical Identity-Based Encryption (without Random Oracles). Cryptology ePrint Archive 2006/085 (2006) · Zbl 1161.94390

[15] Canetti, R., Halevi, S., Katz, J.: A Forward-Secure Public-Key Encryption Scheme. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol.˜2656, pp. 255–271. Springer, Heidelberg (2003) · Zbl 1037.68532 · doi:10.1007/3-540-39200-9_16

[16] Canetti, R., Halevi, S., Katz, J.: Chosen-Ciphertext Security from Identity-Based Encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol.˜3027, pp. 207–222. Springer, Heidelberg (2004) · Zbl 1122.94358 · doi:10.1007/978-3-540-24676-3_13

[17] Cramer, R., Shoup, V.: A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attacks. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol.˜1462, pp. 13–25. Springer, Heidelberg (1998) · Zbl 0931.94018 · doi:10.1007/BFb0055717

[18] Cramer, R., Shoup, V.: Signature Schemes Based on the Strong RSA Assumption. In: Proc. of ACM CCS, pp. 46–51 (1999) · doi:10.1145/319709.319716

[19] Dodis, Y.: Efficient Construction of (Distributed) Verifiable Random Functions. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol.˜2567, pp. 1–17. Springer, Heidelberg (2002) · Zbl 1033.94521

[20] Dodis, Y., Yampolskiy, A.: A Verifiable Random Function with Short Proofs and Keys. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol.˜3386, pp. 416–431. Springer, Heidelberg (2005) · Zbl 1081.94521 · doi:10.1007/978-3-540-30580-4_28

[21] Gentry, C., Silverberg, A.: Hierarchical ID-Based Cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol.˜2501, pp. 548–566. Springer, Heidelberg (2002) · Zbl 1065.94547 · doi:10.1007/3-540-36178-2_34

[22] Horwitz, J., Lynn, B.: Toward Hierarchical Identity-Based Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol.˜2332, pp. 466–481. Springer, Heidelberg (2002) · Zbl 1056.94514 · doi:10.1007/3-540-46035-7_31

[23] Katz, J., Wang, N.: Efficiency Improvements for Signature Schemes with Tight Security Reductions. In: Proc. of ACM CCS, pp. 155–164 (2003) · doi:10.1145/948109.948132

[24] Kurosawa, K., Desmedt, Y.: A New Paradigm of Hybrid Encryption Scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol.˜3152, pp. 426–442. Springer, Heidelberg (2004) · Zbl 1104.94028 · doi:10.1007/978-3-540-28628-8_26

[25] Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol.˜196, pp. 47–53. Springer, Heidelberg (1985) · Zbl 1359.94626 · doi:10.1007/3-540-39568-7_5

[26] Shoup, V.: Lower Bounds for Discrete Logarithms and Related Problems. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol.˜1233, pp. 256–266. Springer, Heidelberg (1997) · doi:10.1007/3-540-69053-0_18

[27] Waters, B.: Efficient Identity-Based Encryption without Random Oracles. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol.˜3494, pp. 114–127. Springer, Heidelberg (2005) · Zbl 1137.94360 · doi:10.1007/11426639_7