**10. BIBLIOGRAPHY**

REFERENCES

[1] J. Bethencourt, D. Song, and B. Water, “New Construction and Practical Applications for Private Streaming Searching,” Proc. IEEE Symp. Security and Privacy, 2006.

[2] J. Bethencourt, D. Song, and B. Water, “New Techniques for Private Stream Searching,” ACM Trans. Information and System Security, vol. 12, no. 3, pp. 1-32, 2009.

[3] D. Boneh, E. Goh, and K. Nissim, “Evaluating 2-DNF Formulas on Ciphertext,” Proc. Second Int’l Conf. Theory of Cryptography, pp. 325- 341, 2005.

[4] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “Fully Homomorphic Encryption without Bootstrapping,” <http://eprint>. iacr.org/2011/277, 2011.

[5] Z. Brakerski and V. Vaikuntanathan, “Efficient Fully Homomorphic Encryption from (Standard) LWE,” <http://eprint>. iacr.org/2011/344, 2011.

[6] I. Damgard and M. Jurik, “A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-Key System,” Proc. Fourth Int’l Workshop Practice and Theory in Public Key Cryptography (PKC ’01), pp. 119-136, 2001.

[7] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully Homomorphic Encryption over the Integers,” Proc. Advances in Cryptology (EUROCRYPT ’10), pp. 24-43, 2010.

[8] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Trans. Information Theory, vol. 31, no. 4, pp. 469-472, July 1985.

[9] C. Gentry, “Fully Homomorphic Encryption Scheme,” PhD thesis, Stanford Univ., http://crypto.stanford.edu/craig, 2009.

[10] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” Proc. 41st Ann. ACM Symp. Theory of Computing (STOC ’09), pp. 169-178, 2009.

[11] C. Gentry, “Computing Arbitrary Functions of Encrypted Data, Comm. ACM, vol. 53, no. 3, pp. 97-105, 2010.

[12] C. Gentry, “Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness,” Proc. Advances in Cryptology (CRYPTO ’10), pp. 116-137, 2010.

[13] C. Gentry and S. Halevi, “Implementing Gentry’s Fully- Homomorphic Encryption Scheme,” Proc. 30th Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT ’11), pp. 129-148, 2011.

[14] D. Harris, D.M. Harris, and S.L. Harris, Digital Design and Computer Architecture. Morgan Kaufmann, 2007.

[15] D.J. Lilja and S.S. Sapatnekar, Designing Digital Computer Systems with Verilog. Cambridge Univ. Press, 2005.

[16] S. Ling and C.P. Xing, Coding Theory: A First Course. Cambridge Press, 2004.

[17] R. Ostrovsky and W. Skeith, “Private Searching on Streaming Data,” Proc. Advances in Cryptology (CRYPTO ’05), pp. 223-240, 2005.

[18] R. Ostrovsky and W. Skeith, “Private Searching on Streaming Data,” J. Cryptology, vol. 20, no. 4, pp. 397-430, 2007.

[19] R. Ostrovsky and W. Skeith, “Algebraic Lower Bounds for Computing on Encrypted Data,” Proc. Electronic Colloquium on Computational Complexity (ECCC ’07), 2007.

[20] P. Paillier, “Public Key Cryptosystems Based on Composite Degree Residue Classes,” Proc. 17th Int’l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT ’99), pp. 223-238, 1999.

[21] B. Parhami, Computer Arithmetic: Algorithms and Hardware Designs, second ed. Oxford Univ. Press, 2010.

[22] N. Smart and F. Vercauteren, “Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes,” Proc. 13th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC ’10), pp. 420-443, 2010.

[23] D. Stehle and R. Steinfeld, “Faster Fully Homomorphic Encryption,” Proc. Advances in Cryptology (ASIACRYPT ’10), pp. 377-394, 2010.

[24] J.F. Wakerly, Digital Design Principles and Practices, third ed. Prentice Hall, 2000.

[25] X. Yi and C.P. Xing, “Private (t, n) Threshold Searching on Streaming Data,” Proc. Int’l Conf. Social Computing Privacy, Security, Risk and Trust (PASSAT ’12), pp. 676-683, 2012.