References

[1] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in *In Crypto 97*, Springer-Verlag, 1996, pp. 90–104.

[2] D. Markus and F. D. Mandell, "Deniable encryption with negligible detection probability: an interactive construction," in *Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, ser. EUROCRYPT'11, Berlin, Heidelberg: Springer-Verlag, 2011, pp. 610–626.

[3] B. M. David and A. C. A. Nascimento, "Deniable encryption from the mceliece assumptions," *IACR Cryptology ePrint Archive*, 2011, http://eprint.iacr.org/2011/144.

[4] O. Adam, P. Chris, and W. Brent, "Bi-deniable public-key encryption," in *Proceedings of the 31st Annual Conference on Advances in Cryptology*, ser. CRYPTO'11, Berlin, Heidelberg: Springer-Verlag, 2011, pp. 525–542.

[5] M. H. Ibrahim, "A method for obtaining deniable public-key encryption," in *International Journal of Network Security (IJNS)*, 2009, pp. 159–164.

[6] M. H. Ibrahim, "Receiver-deniable public-key encryption," in *International Journal of Network Security (IJNS)*, 2009, p. 165.

[7] B. Dan, D. Xuhua, T. Gene, and W. C. Ming, "A method for fast revocation of public key certificates and security capabilities," in *Proceedings of the 10th Conference on USENIX Security Symposium*, ser. SSYM'01, vol. 10, Berkeley, CA, USA: USENIX Association, 2001, pp. 297–308.

[8] H. M. Sun, Y. Chen, and J. S. Chou, *An efficient secure oblivious transfer*, Cryptology ePrint Archive, http://eprint.iacr.org/2009/521, 2009.

[9] A. Sahai and B. Waters, "How to use indistinguishability obfuscation: deniable encryption, and more," 2013, http://eprint.iacr.org/.

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

[11] K. P. Klonowski Marek and K. Miroslaw, "Practical deniable encryption," in *SOFSEM 2008: Theory and Practice of Computer Science*, vol. 4910, ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2008, pp. 599–609.

[12] A. Czeskis, D. J. S. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, and B. Schneier, "Defeating encrypted and deniable file systems: truecrypt v5.1a and the case of the tattling os and applications," in *Proceedings of the 3rd Conference on Hot Topics in Security*, ser. HOTSEC'08, Berkeley, CA, USA: USENIX Association, 2008, 7:1–7:7.

[13] K. John, S. Bruce, W. David, and H. Chris, "Side channel cryptanalysis of product ciphers," *J. Comput. Secur.*, vol. 8, no. 2,3, pp. 141–158, Aug. 2000.

[14] B. Rikke, N. J. Buus, N. P. Sebastian, and O. Claudio, "Lower and upper bounds for deniable public-key encryption," in *Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security*, ser. ASIACRYPT'11, Berlin, Heidelberg: Springer-Verlag, 2011, pp. 125–142.

[15] R. Canetti, U. Feige, O. Goldreich, and M. Naor, "Adaptively secure multi-party computation," in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, New York, NY, USA: ACM, 1996, pp. 639–648.

[16] H. Jaydeep, N. Vivek, and M. A. K. Basu Saikat, "Uncoercibility in e-voting and auctioning mechanisms using deniable encryption," vol. 3, p. 97, 2011.

[17] A. Skillen and M. Mannan, "Deniable storage encryptionfor mobile devices," *Dependable and Secure Computing, IEEE Transactions on*, vol. 11, no. 3, pp. 224–237, 2014.

[18] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*, ser. WPES '10, New York, NY, USA: ACM, 2010, pp. 31–42.

[19] O. Goldreich, L. A. Levin, and N. Nisan, "On constructing 1-1 one-way functions," in *Studies in Complexity and Cryptography*, 2011, pp. 13–25.

[20] I. B. Demgȧrd and J. B. Nielsen, "Improved non-committing encryption schemes based on a general complexity assumption," in *Advances in Cryptology CRYPTO 2000*, M. Bellare, Ed., vol. 1880, ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2000, pp. 432–450.

[21] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang, "On the (im)possibility of obfuscating programs," in *Lecture Notes in Computer Science*, Springer-Verlag, 2001, pp. 1–18.

[22] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, K. Yang, and S. Vadhan, "On the (im)possibility of obfuscating programs," 2012, vol. 59, New York, NY, USA: ACM, May 2012.

[23] G. Sanjam, G. Craig, H. Shai, R. Mariana, S. Amit, and W. Brent, "Candidate indistinguishability obfuscation and functional encryption for all circuits," in *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, ser. FOCS '13, Washington, DC, USA: IEEE Computer Society, 2013, pp. 40–49.

[24] S. Dreyfus, *The idiot savant's guide of rubberhose*, http://web.archive.org, 2012.

[25] M. Bo and W. JiangQing, "An efficient receiver deniable encryption scheme and its applications.," *JNW*, vol. 5, no. 6, pp. 683–690, 2010.

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

[27] A. Irwinp and R. Hunt, *Forensic methods for detection of deniable encryption in mobile networks in Communications*. 2009, pp. 169–174.

[28] G. Juan, W. Daniel, and Z. H. Sheng, “Somewhat non-committing encryption and efficient adaptively secure oblivious transfer,” in *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO ’09, Berlin, Heidelberg: Springer-Verlag, 2009, pp. 505–523.

[29] S. Choi, D. Dachman-Soled, T. Malkin, and H. Wee, “Improved non-committing encryption with applications to adaptively secure protocols,” in *Advances in Cryptology - ASIACRYPT 2009*, M. Matsui, Ed., vol. 5912, ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 287–302.

[30] K. Sako and J. Kilian, “Receipt-free mix-type voting scheme: a practical solution to the implementation of a voting booth,” in *Proceedings of the 14th Annual International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT’95, Berlin, Heidelberg: Springer-Verlag, 1995, pp. 393–403.

[31] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” *DSN progress report*, vol. 42, no. 44, pp. 114–116, 1978.

[32] N. Ryo, I. Hideki, K. Kazukuni, and M. Kirill, “Semantic security for the mceliece cryptosystem without random oracles,” *Des. Codes Cryptography*, vol. 49, no. 1-3, pp. 289–305, 2008.

[33] P. Christof and P. Jan, *Understanding Cryptography: A Textbook for Students and Practitioners*, 1st. Springer Publishing Company, Incorporated, 2009.

[34] B. Schneier, *Applied Cryptography : Protocols, Algorithms, and Source Code in C*, 2nd. John Wiley & Sons, Inc., 1996.

msc.bib