Hong, Jeongdae; **Kim, Jinil**; **Kim, Jihye**; **Franklin, Matthew K.**; **Park, Kunsoo**

Fair threshold decryption with semi-trusted third parties. (English) Zbl 1284.94081

Boyd, Colin (ed.) et al., Information security and privacy. 14th Australasian conference, ACISP 2009, Brisbane, Australia, July 1–3, 2009. Proceedings. Berlin: Springer (ISBN 978-3-642-02619-5/pbk). Lecture Notes in Computer Science 5594, 309-326 (2009).

Summary: A threshold decryption scheme is a multi-party public key cryptosystem that allows any sufficiently large subset of participants to decrypt a ciphertext, but disallows the decryption otherwise. Many threshold cryptographic schemes have been proposed so far, but fairness is not generally considered in this earlier work. In this paper, we present fair threshold decryption schemes, where either all of the participants can decrypt or none of them can. Our solutions employ semi-trusted third parties (STTP) and off-line semi-trusted third parties (OTTP) previously used for fair exchange. We consider a number of variants of our schemes to address realistic alternative trust scenarios. Although we describe our schemes using a simple hashed version of ElGamal encryption, our methods generalize to other threshold decryption schemes and threshold signature schemes as well.

For the entire collection see [Zbl 1165.94302].

MSC:

94A60 Cryptography

Full Text: DOI

References:

[1] Asokan, N., Schunter, M., Waidner, M.: Optimistic protocols for fair exchange. In: ACM Conference on Computer and Communications Security, pp. 7–17 (1997) · doi:10.1145/266420.266426

[2] Asokan, N., Shoup, V., Waidner, M.: Optimistic fair exchange of digital signatures. IEEE J. Selected Areas in Communication˜18(4), 593–610 (2000) · Zbl 0929.68064 · doi:10.1109/49.839935

[3] Bao, F., Deng, R.H., Mao, W.: Efficient and practical fair exchange protocols with off-line TTP. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 77–85 (May 1998)

[4] Ben-Or, M., Goldreich, O., Micali, S., Rivest, R.L.: A fair protocol for signing contracts. IEEE Transactions on Information Theory˜36(1), 40–46 (1990) · doi:10.1109/18.50372

[5] Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: STOC 1988: Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 1–10. ACM, New York (1988) · doi:10.1145/62212.62213

[6] Blum, M.: How to exchange (secret) keys. ACM Trans. Comput. Syst.˜1(2), 175–193 (1983) · doi:10.1145/357360.357368

[7] Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol.˜2656, pp. 416–432. Springer, Heidelberg (2003) · Zbl 1038.94553 · doi:10.1007/3-540-39200-9_26

[8] Boneh, D., Naor, M.: Timed commitments. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol.˜1880, pp. 236–254. Springer, Heidelberg (2000) · Zbl 0989.94517 · doi:10.1007/3-540-44598-6_15

[9] Boudot, F., Schoenmakers, B., Traoré, J.: A fair and efficient solution to the socialist millionaires' problem. Discrete Applied Mathematics˜111(1-2), 23–36 (2001) · Zbl 0978.68062 · doi:10.1016/S0166-218X(00)00342-5

[10] Cachin, C., Camenisch, J.L.: Optimistic fair secure computation. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol.˜1880, pp. 93–111. Springer, Heidelberg (2000) · Zbl 0989.68510 · doi:10.1007/3-540-44598-6_6

[11] Camenisch, J., Shoup, V.: Practical verifiable encryption and decryption of discrete logarithms. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol.˜2729, pp. 126–144. Springer, Heidelberg (2003) · Zbl 1122.94357 · doi:10.1007/978-3-540-45146-4_8

[12] Chaum, D., Crépeau, C., Damgard, I.: Multiparty unconditionally secure protocols. In: STOC 1988: Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 11–19. ACM Press, New York (1988) · doi:10.1145/62212.62214

[13] Cleve, R.: Limits on the security of coin flips when half the processors are faulty (extended abstract). In: STOC, pp. 364–369 (1986)

[14] Cox, B., Tygar, J.D., Sirbu, M.: Netbill security and transaction protocol. In: First USENIX workshop on Electronic Commerce, pp. 77–88 (1995)

[15] Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol.˜435, pp. 307–315.

Springer, Heidelberg (1990) · doi:10.1007/0-387-34805-0_28

[16] Dodis, Y., Lee, P.J., Yum, D.H.: Optimistic fair exchange in a multi-user setting. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol.˜4450, pp. 118–133. Springer, Heidelberg (2007) · Zbl 1127.94345 · doi:10.1007/978-3-540-71677-8_9

[17] Dodis, Y., Reyzin, L.: Breaking and repairing optimistic fair exchange from PODC 2003. In: Digital Rights Management Workshop, pp. 47–54 (2003)

[18] ElGamal, T.: A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory˜31(4), 469–472 (1985) · Zbl 0571.94014 · doi:10.1109/TIT.1985.1057074

[19] Fouque, P., Poupard, G., Stern, J.: Sharing decryption in the context of voting of lotteries. In: Frankel, Y. (ed.) FC 2000. LNCS, vol.˜1962, pp. 90–104. Springer, Heidelberg (2001) · Zbl 0999.94548 · doi:10.1007/3-540-45472-1_7

[20] Franklin, M.K., Reiter, M.K.: Fair exchange with a semi-trusted third party. In: Proceedings of the 4th ACM Conference on Computer and Communications Security (CCS), pp. 1–5 (April 1997) · doi:10.1145/266420.266424

[21] Garay, J.A., MacKenzie, P., Yang, K.: Efficient and secure multi-party computation with faulty majority and complete fairness. Cryptology ePrint Archive, Report 2004/009 (2004), http://eprint.iacr.org/

[22] Garay, J.A., MacKenzie, P.D., Prabhakaran, M., Yang, K.: Resource fairness and composability of cryptographic protocols. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol.˜3876, pp. 404–428. Springer, Heidelberg (2006) · Zbl 1112.94011 · doi:10.1007/11681878_21

[23] Gennaro, R., Halevi, S., Krawczyk, H., Rabin, T.: Threshold RSA for dynamic and ad-hoc groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol.˜4965, pp. 88–107. Springer, Heidelberg (2008) · Zbl 1149.94316 · doi:10.1007/978-3-540-78967-3_6

[24] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Robust and Efficient Sharing of RSA Functions. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol.˜1109, pp. 157–172. Springer, Heidelberg (1996) · Zbl 1329.94060 · doi:10.1007/3-540-68697-5_13

[25] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Robust threshold DSS signatures. Inf. Comput.˜164(1), 54–84 (2001) · Zbl 1021.94527 · doi:10.1006/inco.2000.2881

[26] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Secure distributed key generation for discrete-log based cryptosystems. J. Cryptology˜20(1), 51–83 (2007) · Zbl 1115.68075 · doi:10.1007/s00145-006-0347-3

[27] Gennaro, R., Rabin, T., Jarecki, S., Krawczyk, H.: Robust and efficient sharing of RSA functions. J. Cryptology˜13(2), 273–300 (2000) · Zbl 1059.94022 · doi:10.1007/s001459910011

[28] Goldreich, O.: Secure multi-party computation (working draft, version 1.2) (2000), http://www.wisdom.weizmann.ac.il/oded/pp.html

[29] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: STOC 1987: Proceedings of the nineteenth annual ACM symposium on Theory of computing, pp. 218–229. ACM Press, New York (1987)

[30] Gordon, S.D., Hazay, C., Katz, J., Lindell, Y.: Complete fairness in secure two-party computation. In: STOC, pp. 413–422 (2008) · Zbl 1231.94062 · doi:10.1145/1374376.1374436

[31] Kissner, L., Song, D.: Privacy-preserving set operations. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol.˜3621, pp. 241–257. Springer, Heidelberg (2005) · Zbl 1145.94471 · doi:10.1007/11535218_15

[32] Lepinski, M., Micali, S., Peikert, C., Shelat, A.: Completely fair sfe and coalition-safe cheap talk. In: PODC 2004: Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing, pp. 1–10. ACM, New York (2004) · Zbl 1321.94072 · doi:10.1145/1011767.1011769

[33] Lindell, A.Y.: Legally-enforceable fairness in secure two-party computation. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol.˜4964, pp. 121–137. Springer, Heidelberg (2008) · Zbl 1153.94407 · doi:10.1007/978-3-540-79263-5_8

[34] Luby, M., Micali, S., Rackoff, C.: How to simultaneously exchange a secret bit by flipping a symmetrically-biased coin. In: FOCS, pp. 11–21 (1983) · doi:10.1109/SFCS.1983.25

[35] Pinkas, B.: Fair secure two-party computation. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol.˜2656, pp. 87–105. Springer, Heidelberg (2003) · Zbl 1038.94544 · doi:10.1007/3-540-39200-9_6

[36] Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority. In: STOC 1989: Proceedings of the twenty-first annual ACM symposium on Theory of computing, pp. 73–85. ACM Press, New York (1989) · doi:10.1145/73007.73014

[37] Santis, A.D., Desmedt, Y., Frankel, Y., Yung, M.: How to share a function securely. In: STOC, pp. 522–533 (1994) · Zbl 1345.94094 · doi:10.1145/195058.195405

[38] Shamir, A.: How to share a secret. Commun. ACM˜22(11), 612–613 (1979) · Zbl 0414.94021 · doi:10.1145/359168.359176

[39] Shoup, V.: Practical threshold signatures. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol.˜1807, pp. 207–220. Springer, Heidelberg (2000) · Zbl 1082.94545 · doi:10.1007/3-540-45539-6_15

[40] Zhou, J., Deng, R.H., Bao, F.: Some remarks on a fair exchange protocol. In: Imai, H., Zheng, Y. (eds.) PKC 2000. LNCS, vol.˜1751, pp. 46–57. Springer, Heidelberg (2000) · Zbl 0966.68068 · doi:10.1007/978-3-540-46588-1_4

[41] Zhou, J., Gollmann, D.: An efficient non-repudiation protocol, pp. 126–132. IEEE Computer Society Press, Los Alamitos (1997)