Ferradi, Houda; **Géraud, Rémi**; **Maimut, Diana**; **Naccache, David**; **Pointcheval, David**
Legally fair contract signing without keystones. (English) Zbl 1346.94142
Manulis, Mark (ed.) et al., Applied cryptography and network security. 14th international conference, ACNS 2016, Guildford, UK, June 19–22, 2016. Proceedings. Cham: Springer (ISBN 978-3-319-39554-8/pbk; 978-3-319-39555-5/ebook). Lecture Notes in Computer Science 9696, 175-190 (2016).

Summary: In two-party computation, achieving both fairness and guaranteed output delivery is well known to be impossible. Despite this limitation, many approaches provide solutions of practical interest by weakening somewhat the fairness requirement. Such approaches fall roughly in three categories: "gradual release" schemes assume that the aggrieved party can eventually reconstruct the missing information; "optimistic schemes" assume a trusted third party arbitrator that can restore fairness in case of litigation; and "concurrent" or "legally fair" schemes in which a breach of fairness is compensated by the aggrieved party having a digitally signed cheque from the other party (called the keystone).

In this paper we describe and analyse a new contract signing paradigm that doesn't require keystones to achieve legal fairness, and give a concrete construction based on Schnorr signatures which is compatible with standard Schnorr signatures and provably secure.

For the entire collection see [Zbl 1337.94004].

MSC:

94A62 Authentication, digital signatures and secret sharing

Full Text: DOI

References:

[1] Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n signatures from a variety of keys. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 415–432. Springer, Heidelberg (2002) · Zbl 1065.94560 · doi:10.1007/3-540-36178-2_26

[2] Asokan, N., Schunter, M., Waidner, M.: Optimistic protocols for fair exchange. In: ACM CCS 1997: 4th Conference on Computer and Communications Security, pp. 7–17. ACM Press, Zurich 1–4 April 1997 · doi:10.1145/266420.266426

[3] Baum-Waidner, B., Waidner, M.: Round-optimal and abuse-free optimistic multi-party contract signing. In: Welzl, E., Montanari, U., Rolim, J.D.P. (eds.) ICALP 2000. LNCS, vol. 1853, pp. 524–535. Springer, Heidelberg (2000) · Zbl 0973.94540 · doi:10.1007/3-540-45022-X_44

[4] Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: 20th Annual ACM Symposium on Theory of Computing, pp. 1–10. ACM Press, Chicago 2–4 May 1988

[5] 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

[6] Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: 20th Annual ACM Symposium on Theory of Computing, pp. 11–19. ACM Press, Chicago 2–4 May 1988

[7] Chen, L., Kudla, C., Paterson, K.G.: Concurrent signatures. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 287–305. Springer, Heidelberg (2004) · Zbl 1122.94412 · doi:10.1007/978-3-540-24676-3_18

[8] Cleve, R.: Limits on the security of coin flips when half the processors are faulty (extended abstract). In: Hartmanis, J. (ed.) Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28–30, Berkeley, California, USA, pp. 364–369. ACM (1986)

[9] El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985) · Zbl 1359.94590 · doi:10.1007/3-540-39568-7_2

[10] Garay, J.A., Jakobsson, M., MacKenzie, P.D.: Abuse-free optimistic contract signing. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 449–466. Springer, Heidelberg (1999) · Zbl 0942.94027 · doi:10.1007/3-540-48405-1_29

[11] 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

[12] Girault, M., Poupard, G., Stern, J.: On the fly authentication and signature schemes based on groups of unknown order. J. Cryptology 19(4), 463–487 (2006) · Zbl 1133.94345 · doi:10.1007/s00145-006-0224-0

[13] Goldreich, O.: A simple protocol for signing contracts. In: Chaum, D. (ed.) CRYPTO 1983, pp. 133–136. Plenum Press, New

York (1983)

[14] Goldreich, O.: Foundations of Cryptography: Basic Applications, vol. 2. Cambridge University Press, Cambridge (2004) · Zbl 1068.94011 · doi:10.1017/CBO9780511721656

[15] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th Annual ACM Symposium on Theory of Computing, pp. 218–229. ACM Press, New York 25–27 May 1987

[16] Goldwasser, S., Levin, L.A.: Fair computation of general functions in presence of immoral majority. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 77–93. Springer, Heidelberg (1991) · Zbl 0800.68459 · doi:10.1007/3-540-38424-3_6

[17] Gordon, S.D., Hazay, C., Katz, J., Lindell, Y.: Complete fairness in secure two-party computation. In: Ladner, R.E., Dwork, C. (eds.) 40th Annual ACM Symposium on Theory of Computing, pp. 413–422. ACM Press, Victoria 17–20 May 2008 · Zbl 1231.94062 · doi:10.1145/1374376.1374436

[18] Horster, P., Petersen, H., Michels, M.: Meta-El-Gamal signature schemes. In: ACM CCS 94: 2nd Conference on Computer and Communications Security, pp. 96–107. ACM Press, Fairfax (1994)

[19] Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 143–154. Springer, Heidelberg (1996) · Zbl 1304.94065 · doi:10.1007/3-540-68339-9_13

[20] Lindell, A.Y.: Legally-enforceable fairness in secure two-party computation. In: Malkin, T. (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

[21] Micali, S.: Simple and fast optimistic protocols for fair electronic exchange. In: Borowsky, E., Rajsbaum, S. (eds.) 22nd ACM Symposium Annual on Principles of Distributed Computing, pp. 12–19. Association for Computing Machinery, Boston 13–16 July 2003 · Zbl 06478713 · doi:10.1145/872035.872038

[22] 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

[23] Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001) · Zbl 1064.94558 · doi:10.1007/3-540-45682-1_32

[24] Yao, A.C.C.: How to generate and exchange secrets (extended abstract). In: 27th Annual Symposium on Foundations of Computer Science, pp. 162–167. IEEE Computer Society Press, Toronto 27–29 October 1986