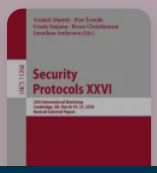
Non-monotonic Security Protocols and Failures in Financial Intermediation

Conference paper | First Online: 24 November 2018

pp 45–54 | Cite this conference paper



Security Protocols XXVI

(Security Protocols 2018)

design failures or wrong assumptions (such as Alice's own misbehavior). Security protocol designers can then focus on preventing or detecting misbehavior (e.g. double spending or double voting).

We argue that general financial intermediation (e.g. Market Exchanges) requires us to consider new form of failures where honest Bob's actions can make honest good standing. Security protocols must be able to deal with *non-monotonic security* and *new types of failures* that stems from rational behavior of honest agents finding themselves on the wrong side.

This has deep implications for the efficient design of security protocols for general financial intermediation, in particular if we need to guarantee a *proportional burden* of computation to the various parties.

- Available as PDF
- Read on any device

- Instant download
- Own it forever

Buy Chapter →

- Available as EPUB and PDF
- Read on any device

- Instant download
- Own it forever

Buy eBook →

Softcover Book

EUR 53.49
Price includes VAT (Poland)

- Compact, lightweight edition
- Dispatched in 3 to 5 business days

- Free shipping worldwide - see info

Notes

1. Obviously the server would have had more load than a client, but this only happens because the server participates to several authentications with several clients at once.

7. The 1229 parties full MPC variant is still out of reach for the foreseable future as experimental papers typically reported MPC with less than 10 parties [5].

8. See Sect. 7 of [14].

9. This does not violate the proportional burden requirement as each trader has the responsibility to prove the solvency if s/he still wants to be in the game.

10. https://tickhistory.thomsonreuters.com.

11. In some cases this fixed order might interfere with the security goal, if the order of actions may leak some information on who started the process.

party and multi-party secure computation. In: ACM Symposium on Theory of Computing, pp. 494–503. ACM (2002)

Google Scholar

5. Damgård, I., Keller, M., Larraia, E., Pastro, V., Scholl, P., Smart, N.P.: Practical covertly secure MPC for dishonest majority – or: breaking the SPDZ limits. In: Crampton, J., Jajodia, S., Mayes, K. (eds.) ESORICS 2013. LNCS, vol. 8134, pp. 1–18. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40203-6_1

Chapter Google Scholar

6. Dierks, T., Allen, C.: The TLS Protocol Version 1.0 (1999)

Google Scholar

11. Kumaresan, R., Moran, T., Bentov, I.: How to use bitcoin to play decentralized poker. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 195–206. ACM (2015)

Google Scholar

12. Kumaresan, R., Vaikuntanathan, V., Vasudevan, P.N.: Improvements to secure computation with penalties. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 406–417, ACM (2016)

Google Scholar

13. Malinova, K., Park, A., Riordan, R.: Do retail traders suffer from high

Heidelberg (1988). https://doi.org/10.1007/3-540-48184-2_32

Chapter Google Scholar

17. Miller, S.P., Neuman, B.C., Schiller, J.I., Saltzer, J.H.: Kerberos authentication and authorization system. In: Project Athena Technical Plan (1987)

Google Scholar

18. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)

Google Scholar

19. Sasson, E.B., et al.: Zerocash: decentralized anonymous payments from bitcoin. In: IEEE Symposium on Security and Privacy, pp. 459–474. IEEE

Fabio Massacci & Chan Nam Ngo

Sapienza University of Rome, Rome, Italy

Daniele Venturi

Durham University Business School, Durham, UK

Julian Williams

Corresponding author

Correspondence to Fabio Massacci .

Editor information

Editors and Affiliations

Masaryk University, Brno, Czech Republic

About this paper

Cite this paper

Massacci, F., Ngo, C.N., Venturi, D., Williams, J. (2018). Non-monotonic Security Protocols and Failures in Financial Intermediation. In: Matyáš, V., Švenda, P., Stajano, F., Christianson, B., Anderson, J. (eds) Security Protocols XXVI. Security Protocols 2018. Lecture Notes in Computer Science(), vol 11286. Springer, Cham. https://doi.org/10.1007/978-3-030-03251-7_5

.RIS .ENW .BIB

DOI	Published	Publisher Name
https://doi.org/10.1007/978-3-030-03251-7_5	24 November 2018	Springer, Cham

Print ISBN	Online ISBN	eBook Packages
978-3-030-03250-0	978-3-030-03251-7	Computer Science

Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 92 **partners**, also use optional cookies and similar technologies for advertising, personalisation of content, usage analysis, and social media.

By accepting optional cookies, you consent to allowing us and our partners to store and access personal data on your device, such as browsing behaviour and unique identifiers. Some third parties are outside of the European Economic Area, with varying standards of data protection. See our **privacy policy** for more information on the use of your personal data. Your consent choices apply to springer.com and applicable subdomains.

You can find further information, and change your preferences via 'Manage preferences'. You can also change your preferences or withdraw consent at any time via 'Your privacy choices', found in the footer of every page.

We use cookies and similar technologies for the following purposes:

Store and/or access information on a device

Personalised advertising and content, advertising and content measurement, audience research and services development

Accept all cookies

Reject optional cookies

Manage preferences