# **SPRINGER NATURE** Link

**∃** Menu

**Search** 

<u>Home</u> > <u>Security Protocols XXVI</u> > Conference paper

# 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)

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Cart

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.

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences



## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences

# Notes

- 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.
- 2. The largest claimed example is the Danish sugar beet auction where 1229 Danish farmers auctioned their production [3]. However, an actual technical reading of the paper reveals that there were only three servers performing MPC over the secret shares generated by the 1200 bidders. As we will illustrate in Sect. 3 it is actually a good example of a monotonic security protocol.

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies	
Reject optional cookies	
Manage preferences	

- 10. <u>https://tickhistory.thomsonreuters.com</u>.
- 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.

# References

1. Abadi, M., Needham, R.: Prudent engineering practice for cryptographic protocols. IEEE Trans. Software Eng. **22**(1), 6–15 (1996)

#### Article Google Scholar

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies	
Reject optional cookies	
Manage preferences	

1-18. Springer, Heidelberg (2013). <u>https://doi.org/10.1007/978-3-642-40203-</u> 6\_1

Chapter Google Scholar

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

#### **Google Scholar**

7. Gong, L.: Fail-Stop Protocols: An Approach To Designing Secure Protocols (1994)

**Google Scholar** 

#### 8 Harkins, D., Carrel, D.: The internet key exchange (IKE). Technical report

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences

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 frequency traders (2013). SSRN 2183806

#### **Google Scholar**

14. Massacci, F., Ngo, C.N., Nie, J., Venturi, D., Williams, J.: FuturesMEX: secure, distributed futures market exchange. In: IEEE Symposium on Security and Privacy, pp. 453–471. IEEE (2018)

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences

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 (2014)

#### **Google Scholar**

20. Spulber, D.F.: Market microstructure and intermediation. J. Econ. Perspect.
 10(3), 135–152 (1996)

Article Google Scholar

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences

# **Editor information**

# **Editors and Affiliations**

## Masaryk University, Brno, Czech Republic

Vashek Matyáš

## Masaryk University, Brno, Czech Republic

Petr Švenda

## University of Cambridge, Cambridge, UK

Frank Stajano

## University of Hertfordshire, Hatfield, UK

Bruce Christianson

## Memorial University of Newfoundland, St. John's, NL, Canada

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies	
Reject optional cookies	
Manage preferences	

DOI	Published	Publisher Name
https://doi.org/10.1007/978-3- 030-03251-7_5	24 November 2018	Springer, Cham
Print ISBN 978-3-030-03250-0	Online ISBN 978-3-030-03251-7	eBook Packages <u>Computer Science</u> <u>Computer Science (R0)</u>

# **Publish with us**

Policies and ethics

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences

## Your privacy, your choice

We use essential cookies to make sure the site can function. We, and our 96 **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

Accept all cookies
Reject optional cookies
Manage preferences