Categories for Cryptographic Composability

Riley Shahar
Advised by Angélica Osorno (Math) and Adam Groce (CS)

Cryptography

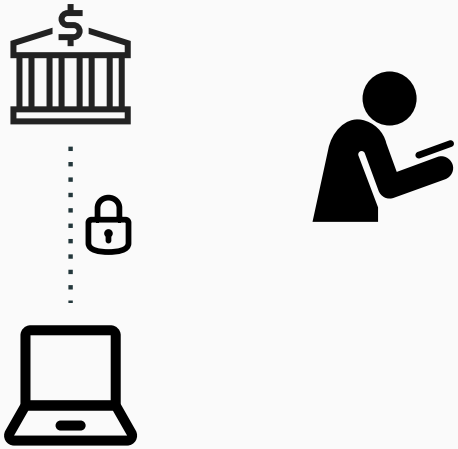
Cryptography is *the mathematical study of secure computation.*

Cryptography

Cryptography is *the mathematical study of secure computation.*

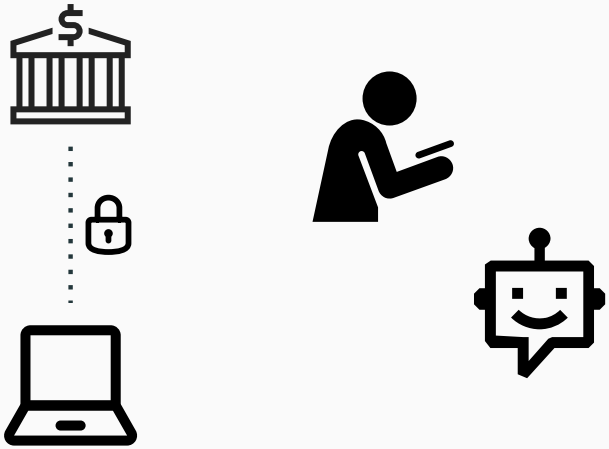
Cryptography

Cryptography is *the mathematical study of secure computation.*



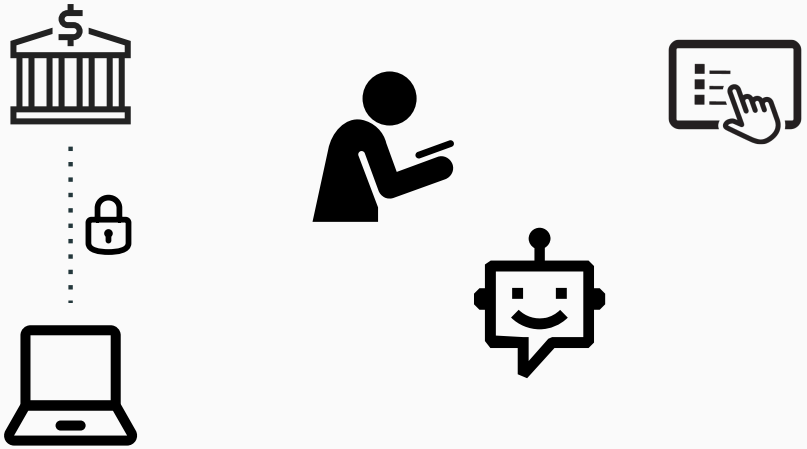
Cryptography

Cryptography is *the mathematical study of secure computation.*



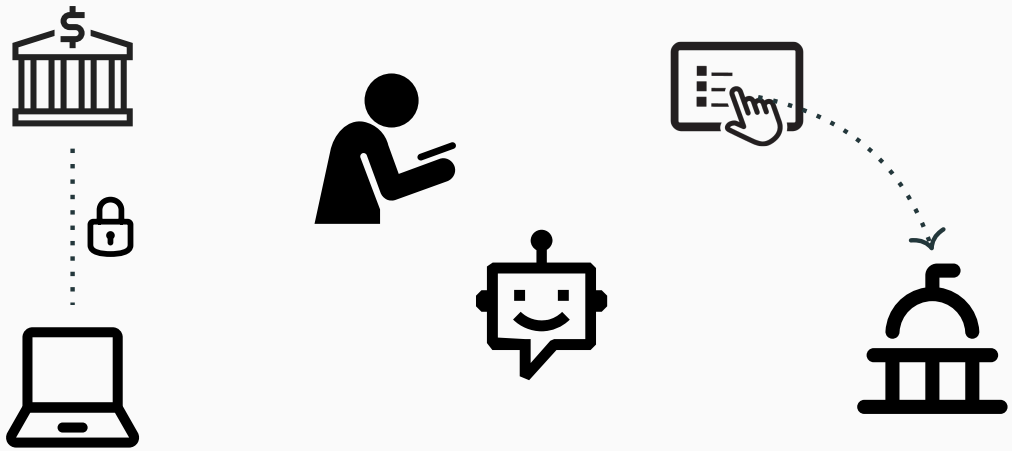
Cryptography

Cryptography is *the mathematical study of secure computation.*



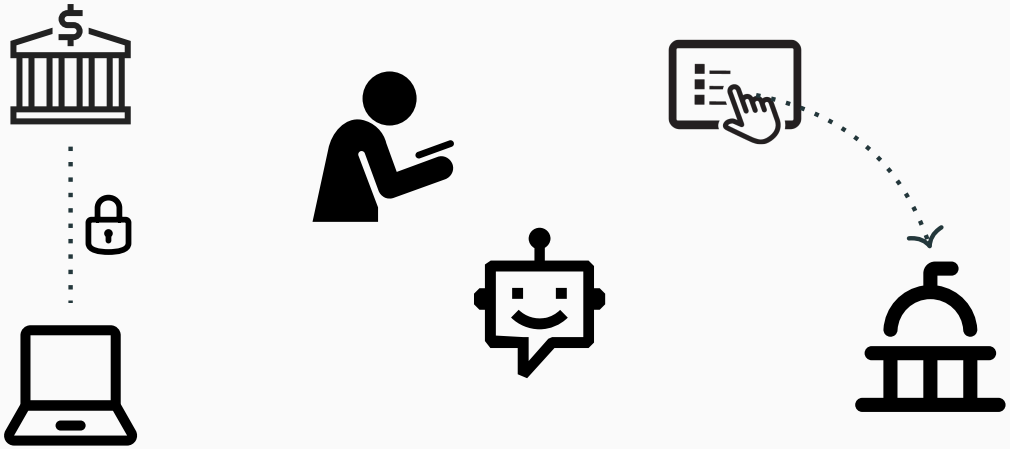
Cryptography

Cryptography is *the mathematical study of secure computation.*



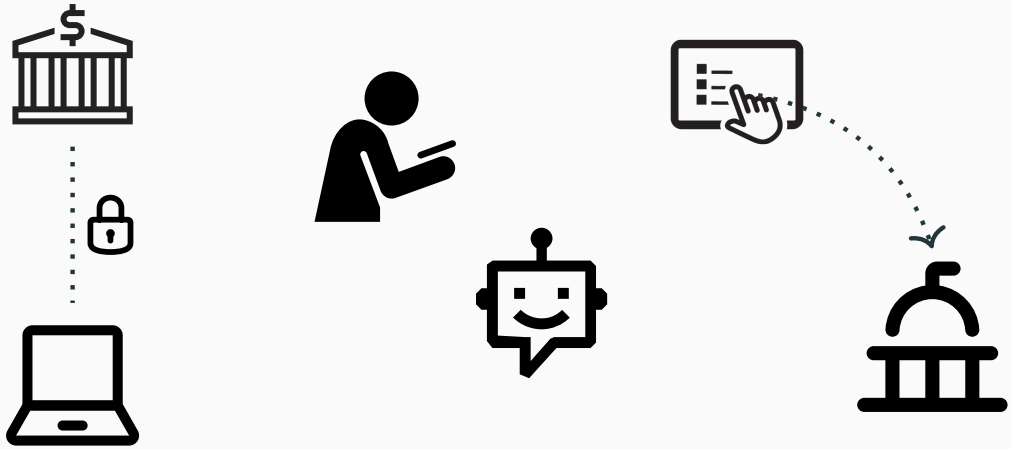
Cryptography

Cryptography is *the* ***mathematical*** *study of secure computation.*



Cryptography

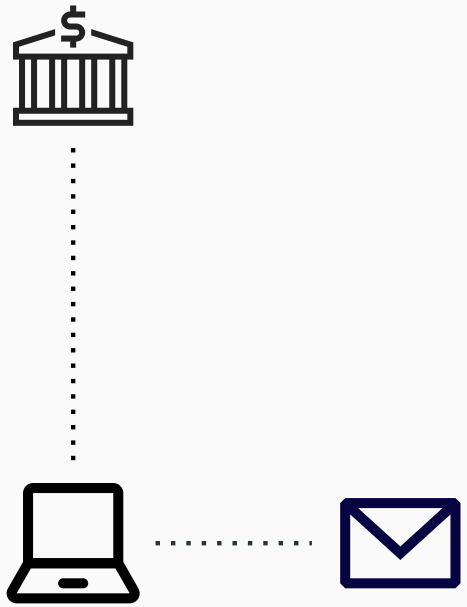
Cryptography is *the* ***mathematical*** *study of secure computation.*



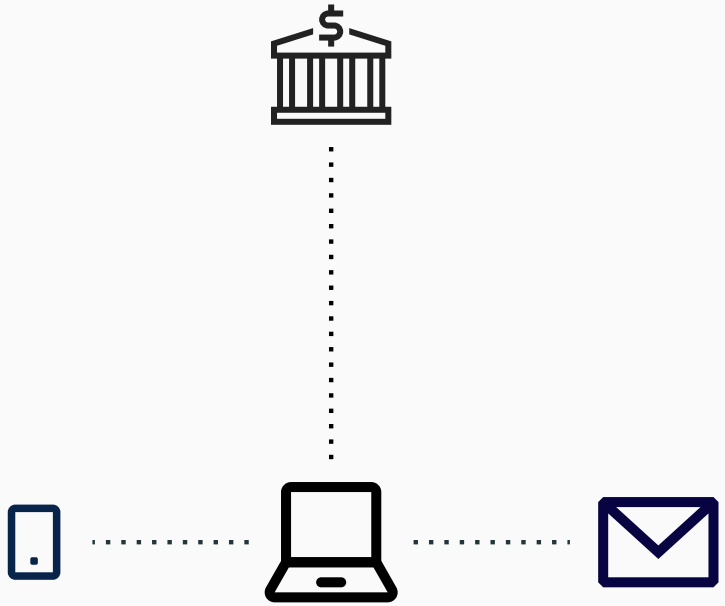
We want *proofs* that these things are secure.

Cryptographic Composability

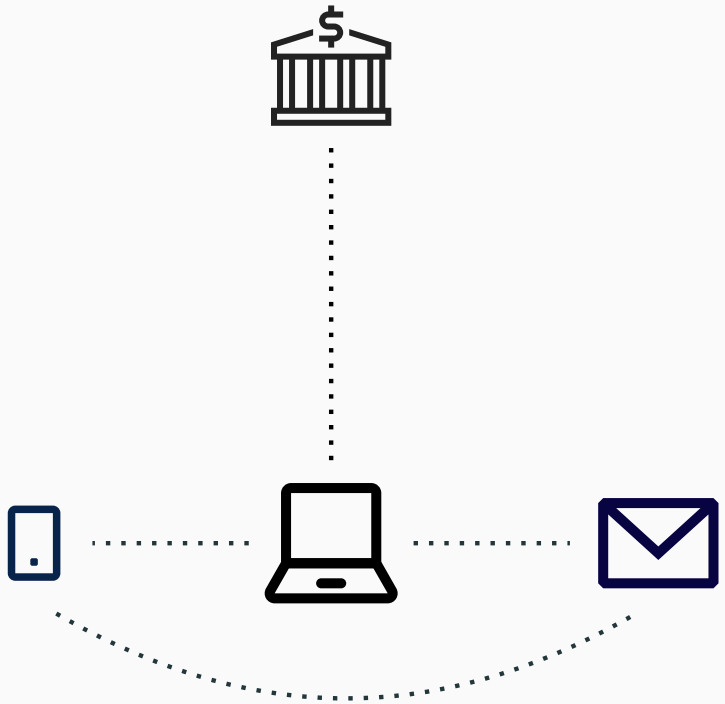
Cryptographic Composability



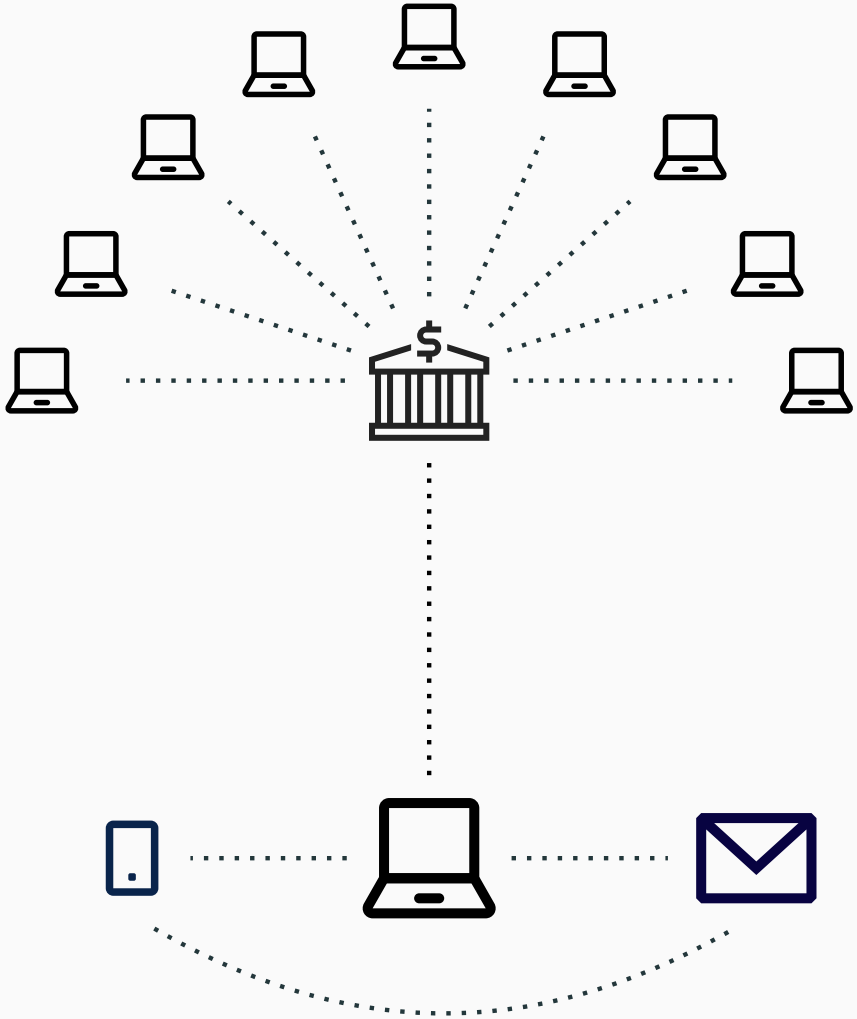
Cryptographic Composability



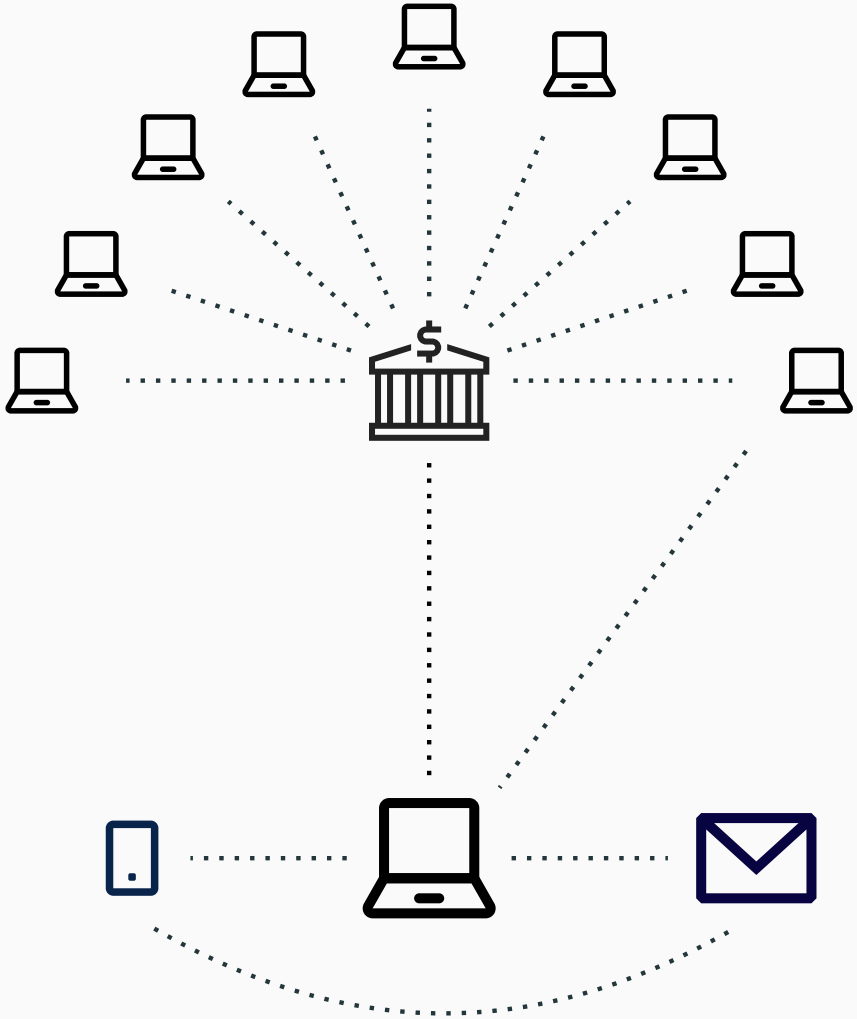
Cryptographic Composability



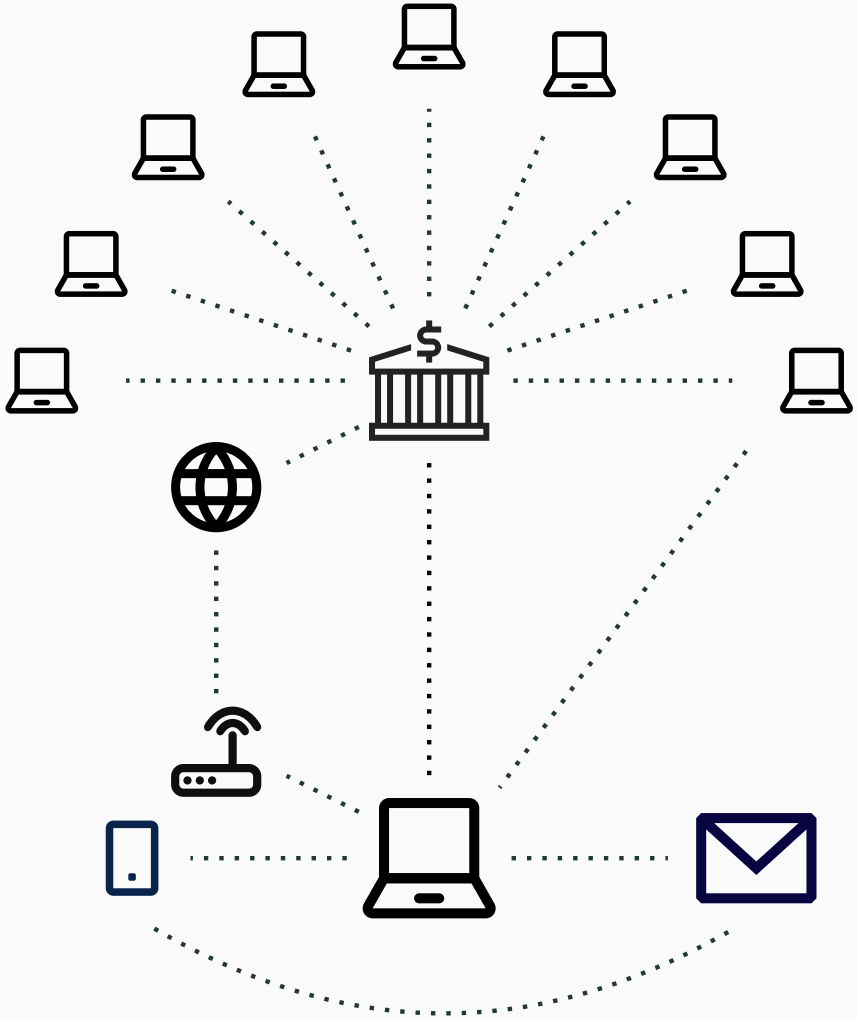
Cryptographic Composability



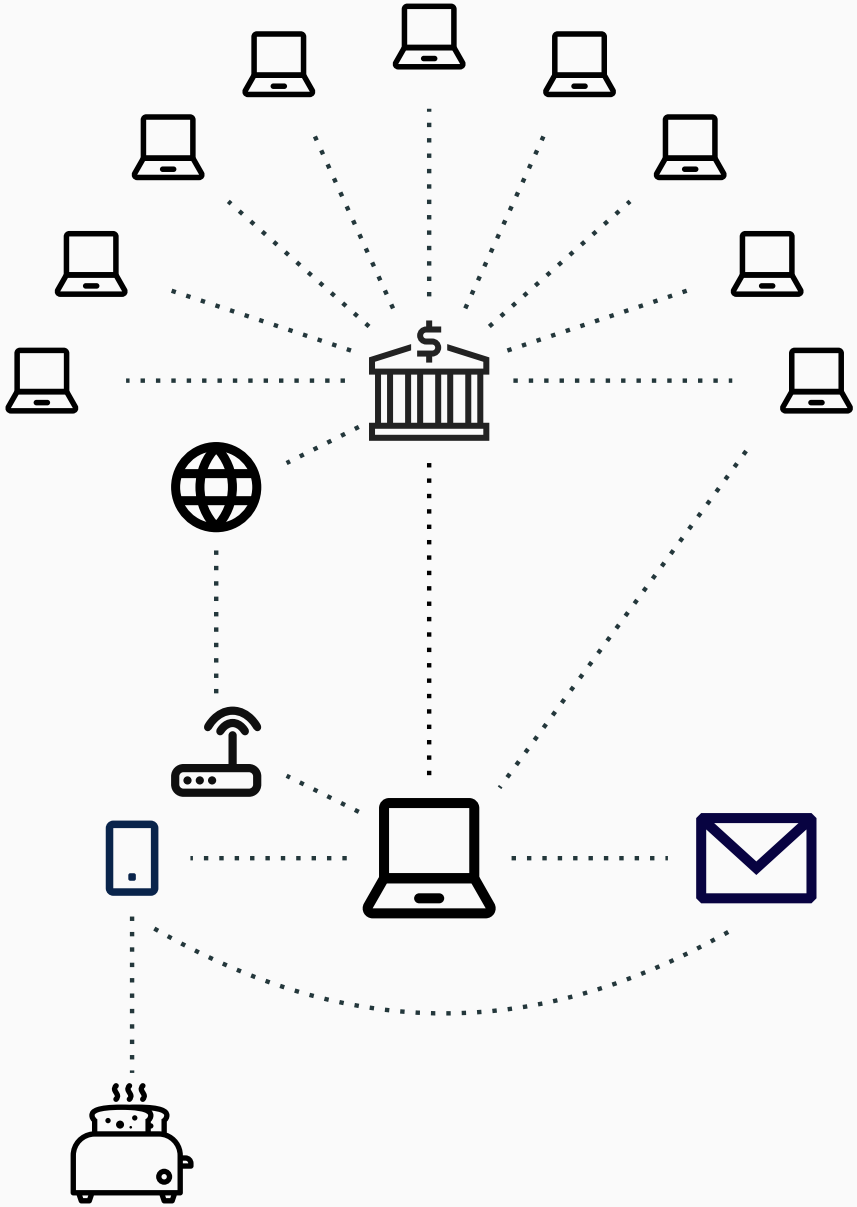
Cryptographic Composability



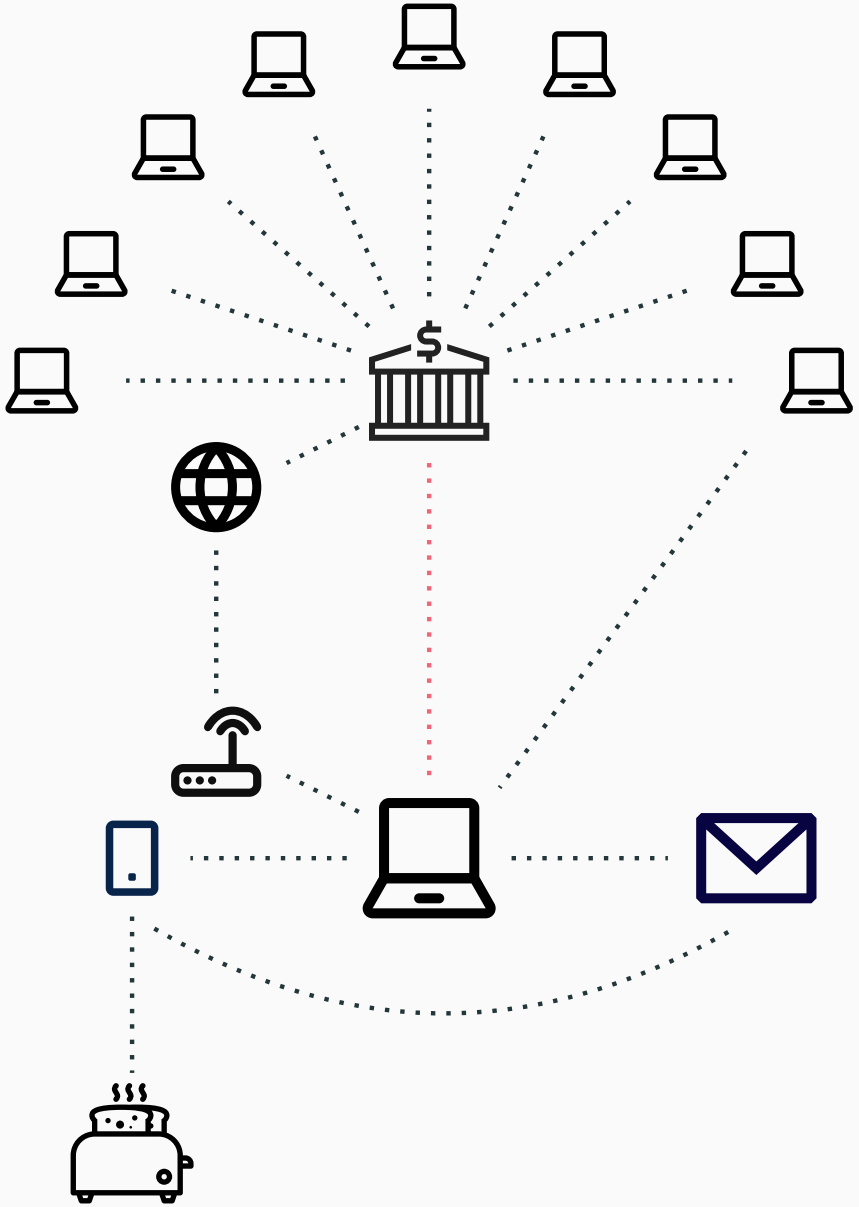
Cryptographic Composability



Cryptographic Composability



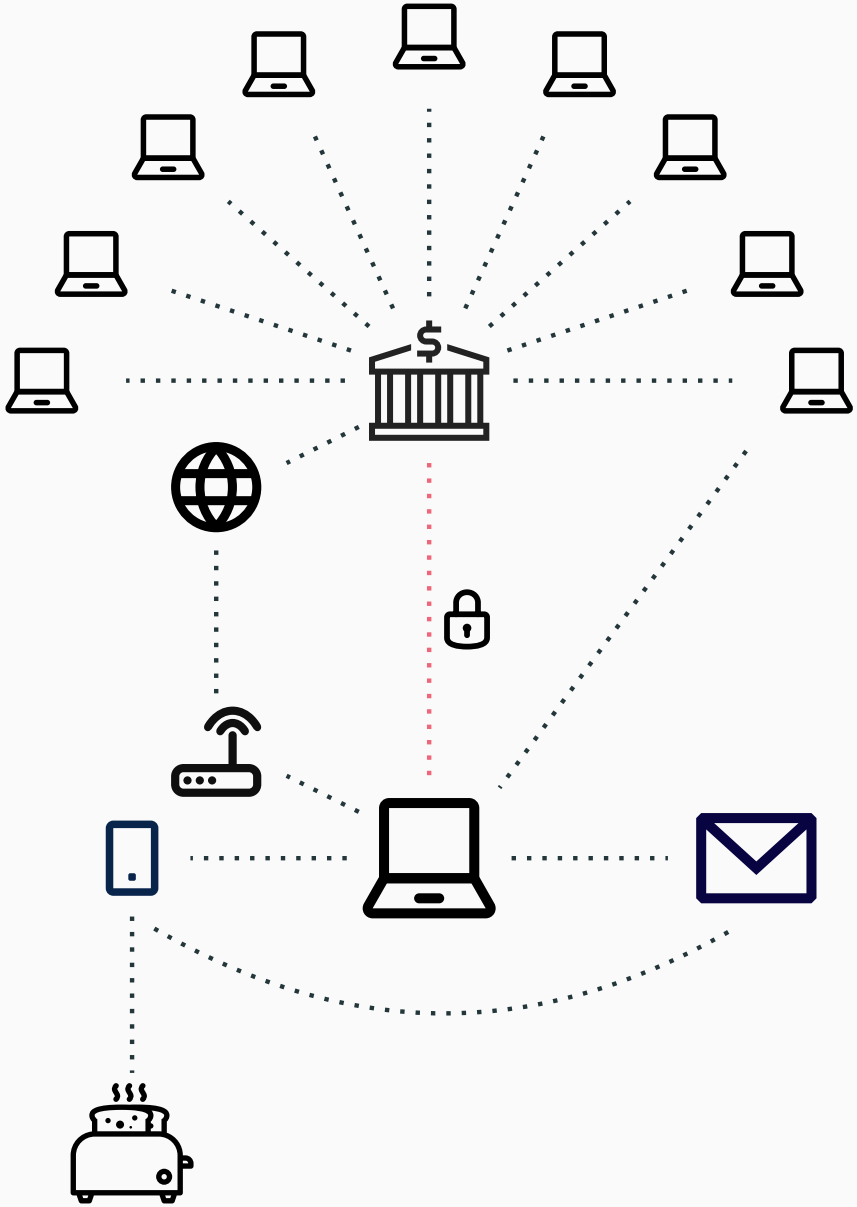
Cryptographic Composability



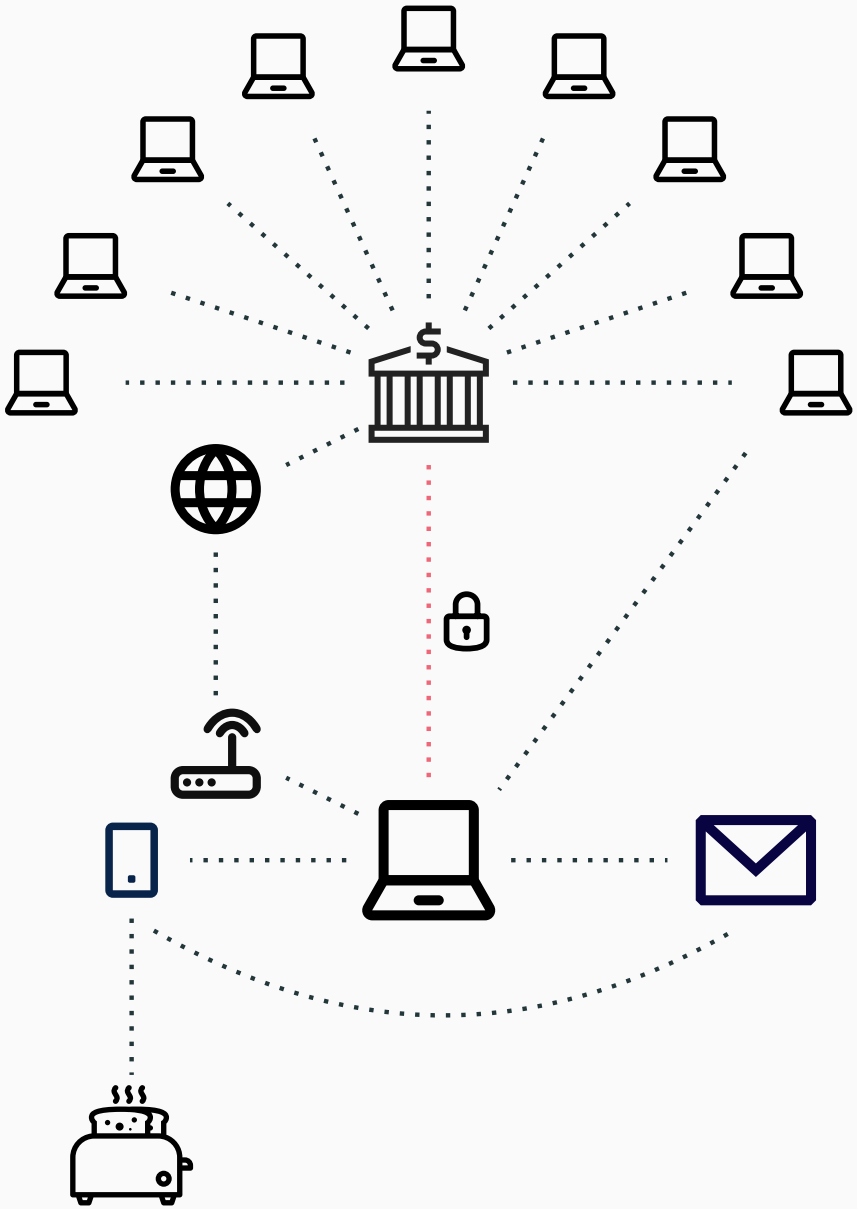
Cryptographic Composability

Cryptographic Composability

Cryptographic Composability



Cryptographic Composability



What do we need to prove about a computation in a vacuum so that it's still secure no matter what else is going on?

Universal Composability

Universal Composability

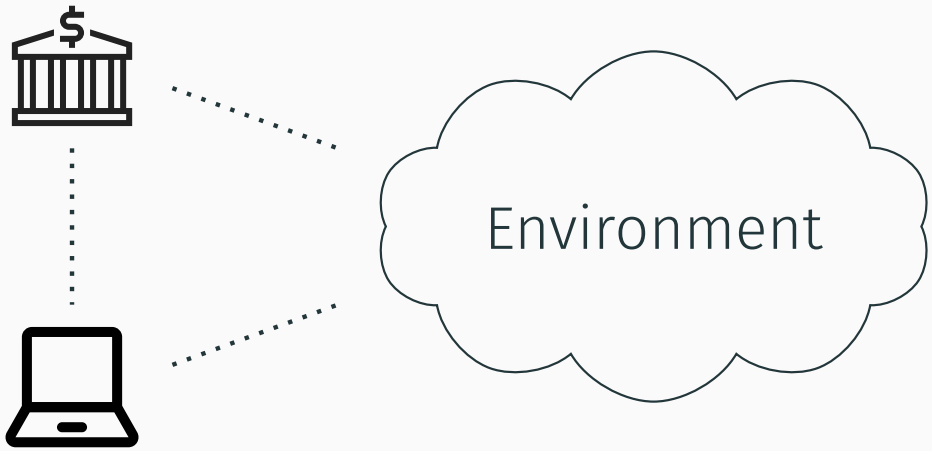
Due to Canetti 2000.

Universal Composability

Due to Canetti 2000.

Universal Composability

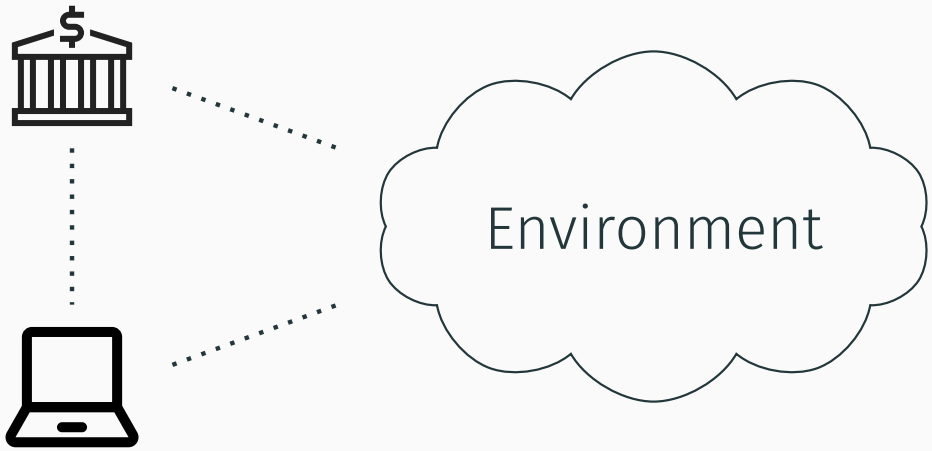
Due to Canetti 2000.



Universal Composability

Due to Canetti 2000.

Exactly what we want!

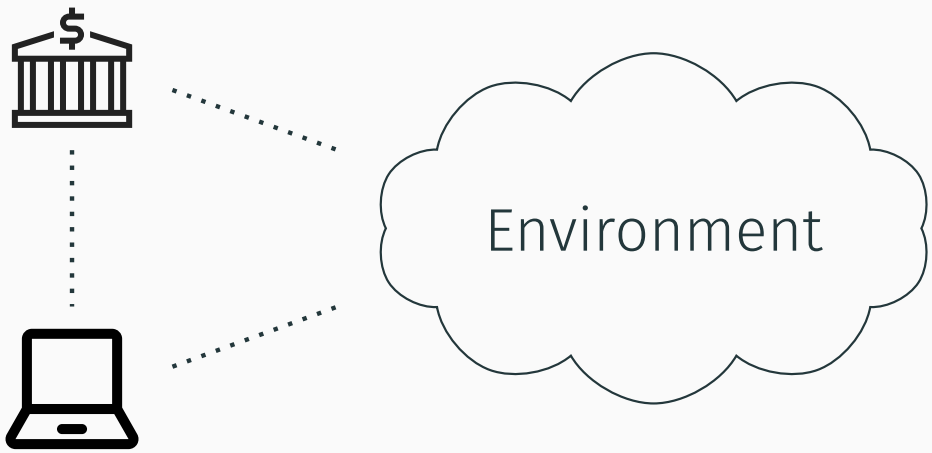


Universal Composability

Due to Canetti 2000.

Exactly what we want!

Informal survey of CRYPTO* 2023:



*Cryptography, not cryptocurrency!

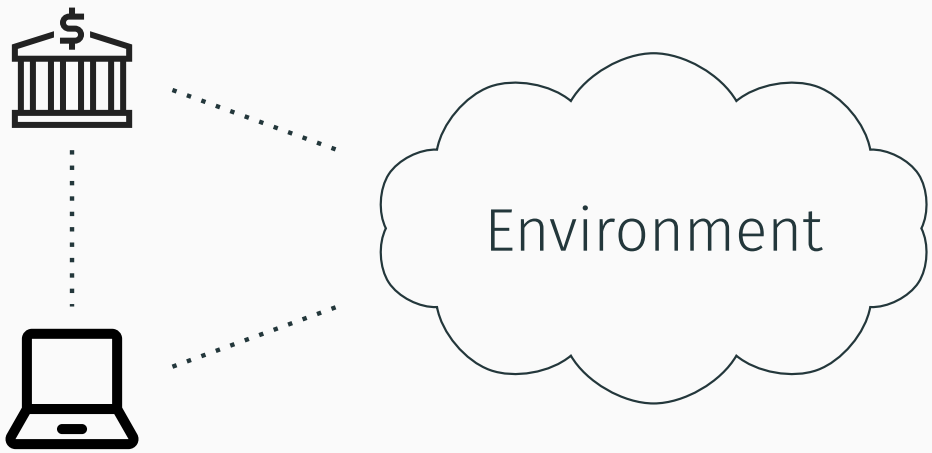
Universal Composability

Due to Canetti 2000.

Exactly what we want!

Informal survey of CRYPTO* 2023:

- 124 papers



*Cryptography, not cryptocurrency!

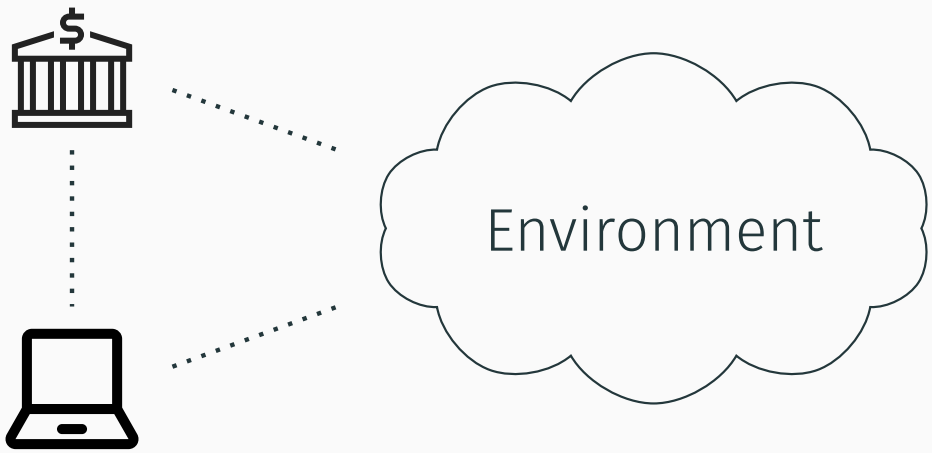
Universal Composability

Due to Canetti 2000.

Exactly what we want!

Informal survey of CRYPTO* 2023:

- 124 papers
- 9 address general composition of their work



*Cryptography, not cryptocurrency!

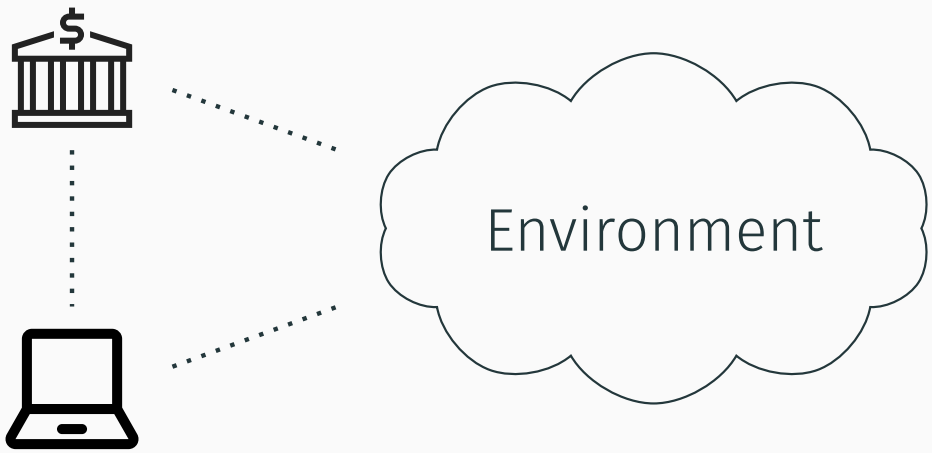
Universal Composability

Due to Canetti 2000.

Exactly what we want!

Informal survey of CRYPTO* 2023:

- 124 papers
- 9 address general composition of their work
- 1 uses UC (Davies et al. 2023)



*Cryptography, not cryptocurrency!

Universal Composability

It is necessary that execution preserve security guarantees under composition. We refrain from proving UC security ... since such an analysis will be cumbersome. Instead, we prove the security of our protocols by constructing simulators.

–David et al. 2023

Cryptography is in need of an elegant mathematical theory abstracting composability of computational processes...

Cryptography is in need of an elegant mathematical theory abstracting composability of computational processes...

...**category theory** is an excellent candidate for such a theory.

Category Theory

Category Theory

Lovingly called “abstract nonsense.”

Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

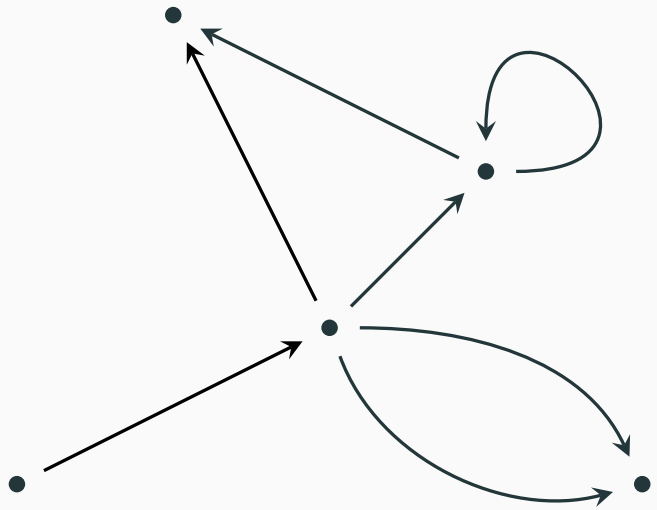
Categories are to composition as calculus is to change.

Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

Categories are to composition as calculus is to change.

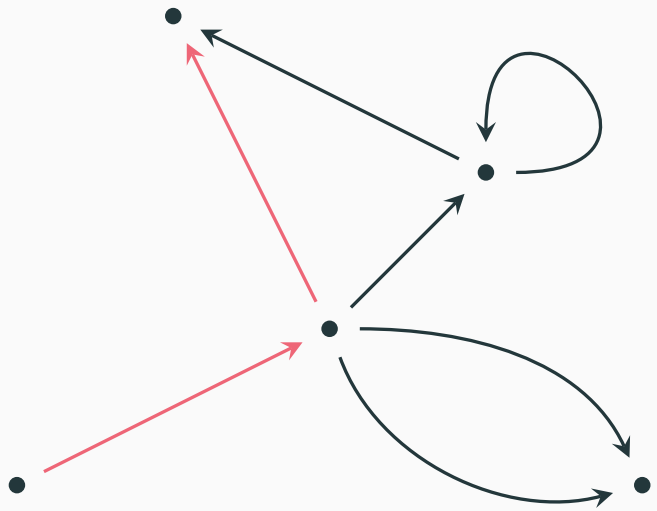


Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

Categories are to composition as calculus is to change.

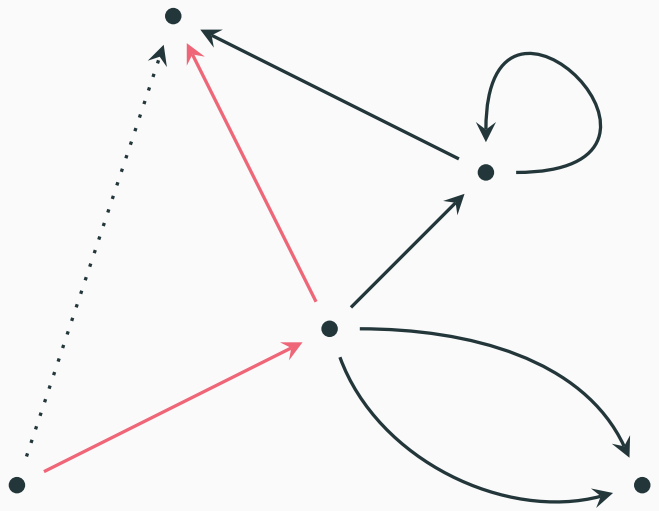


Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

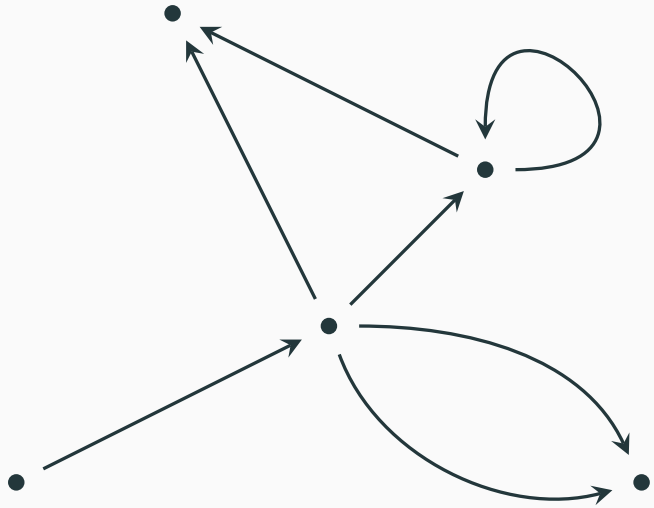
Categories are to composition as calculus is to change.



Categories and Cryptography

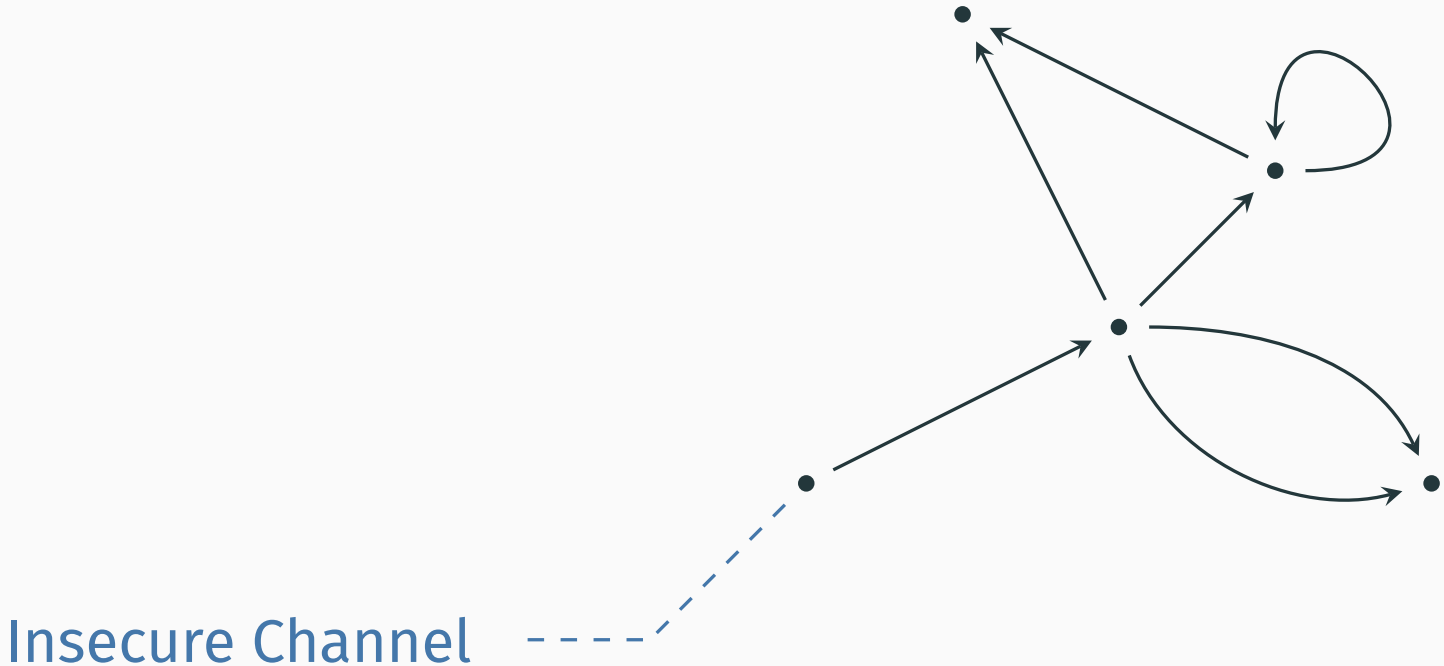
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



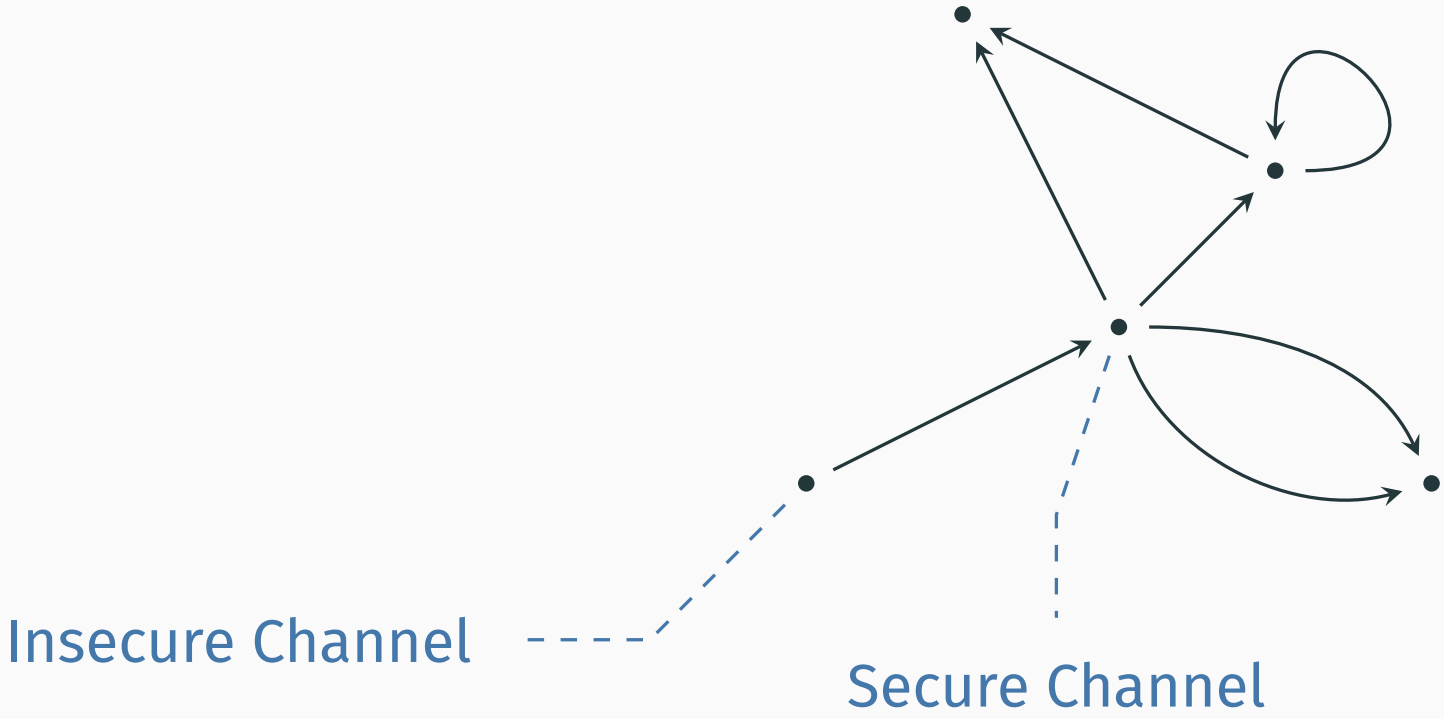
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



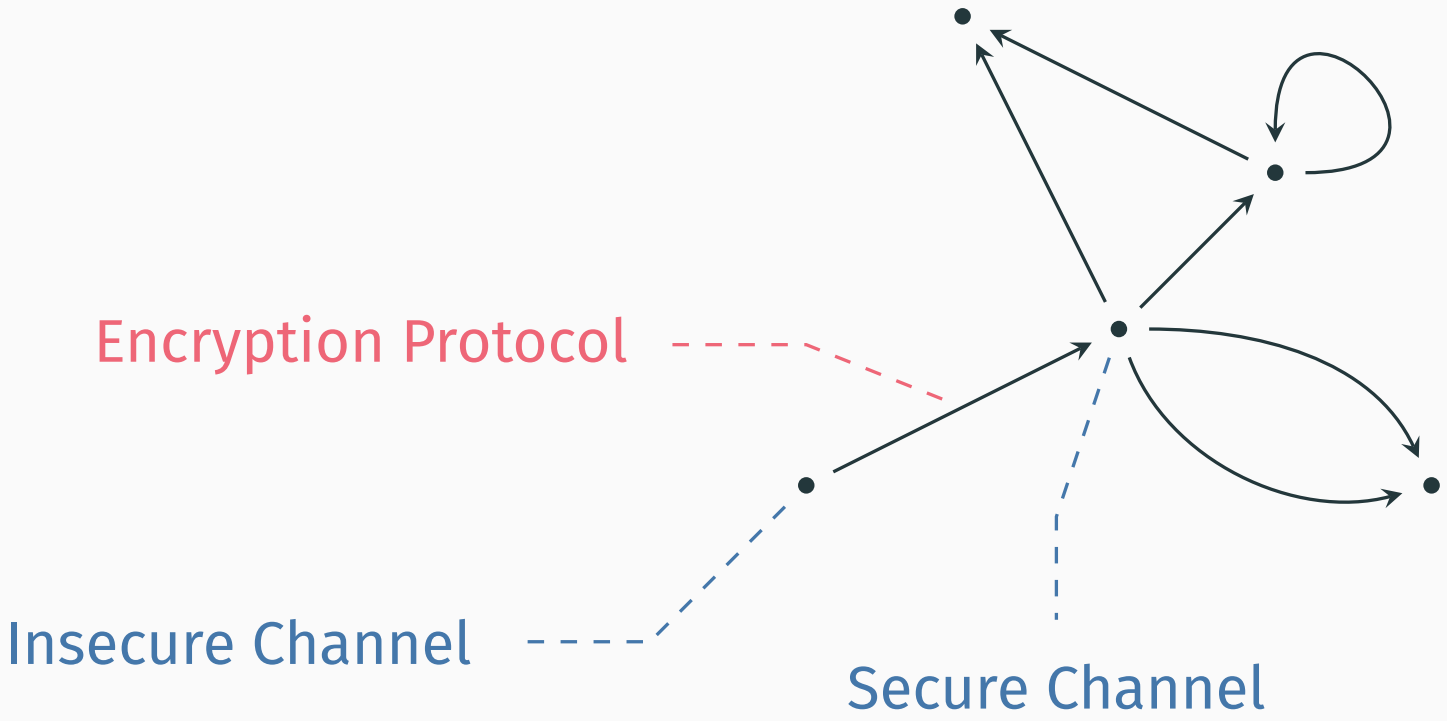
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



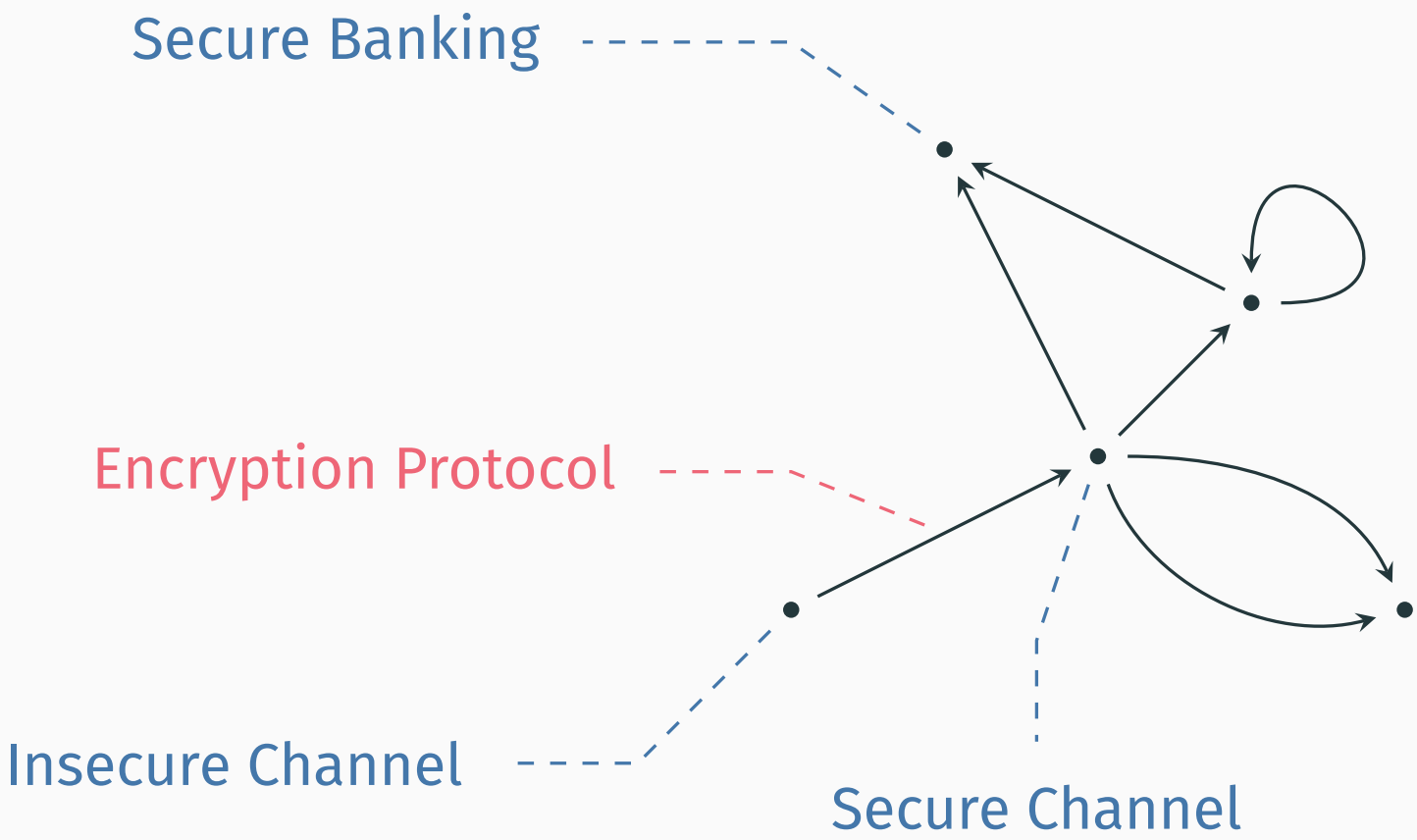
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



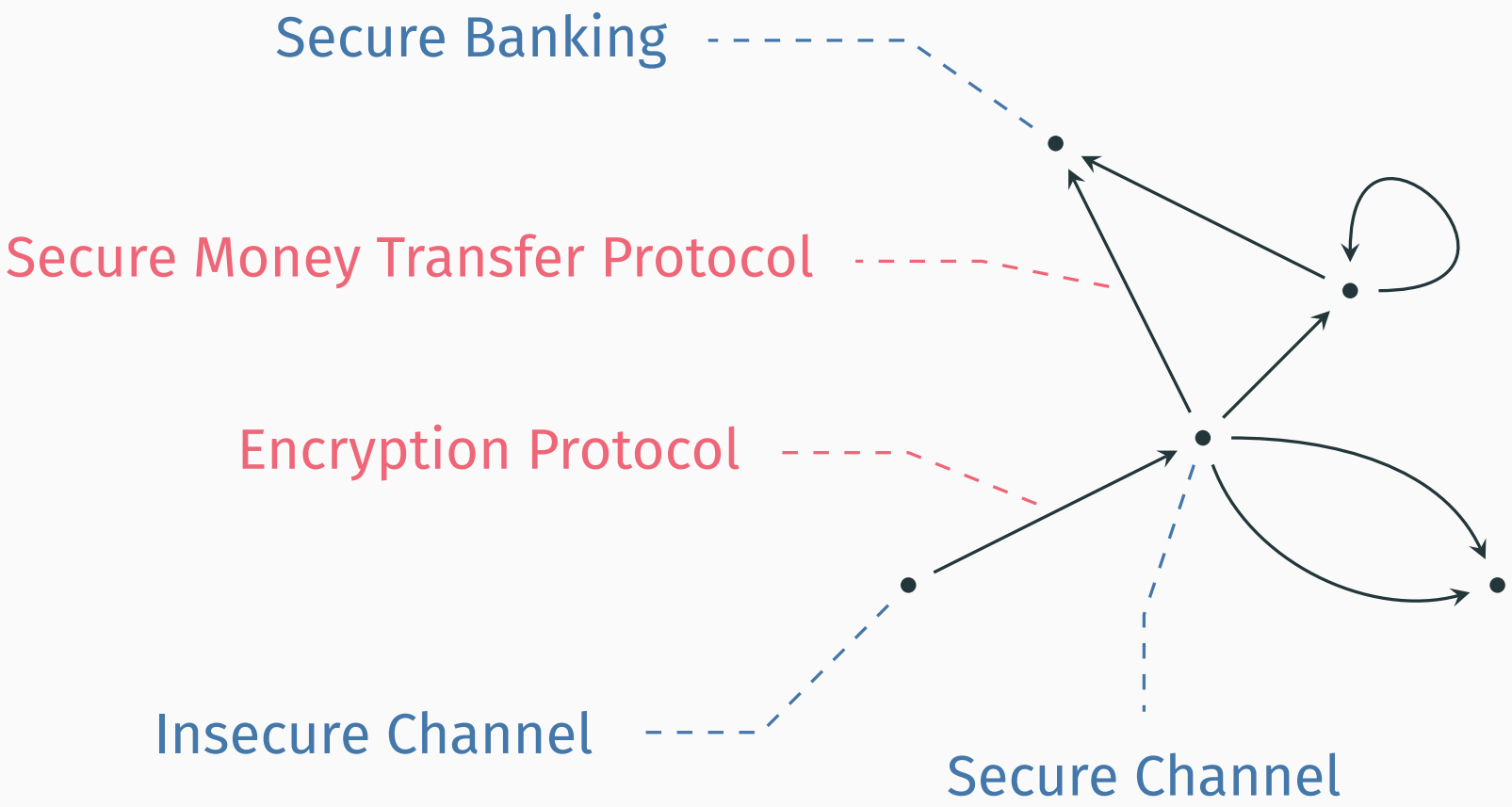
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



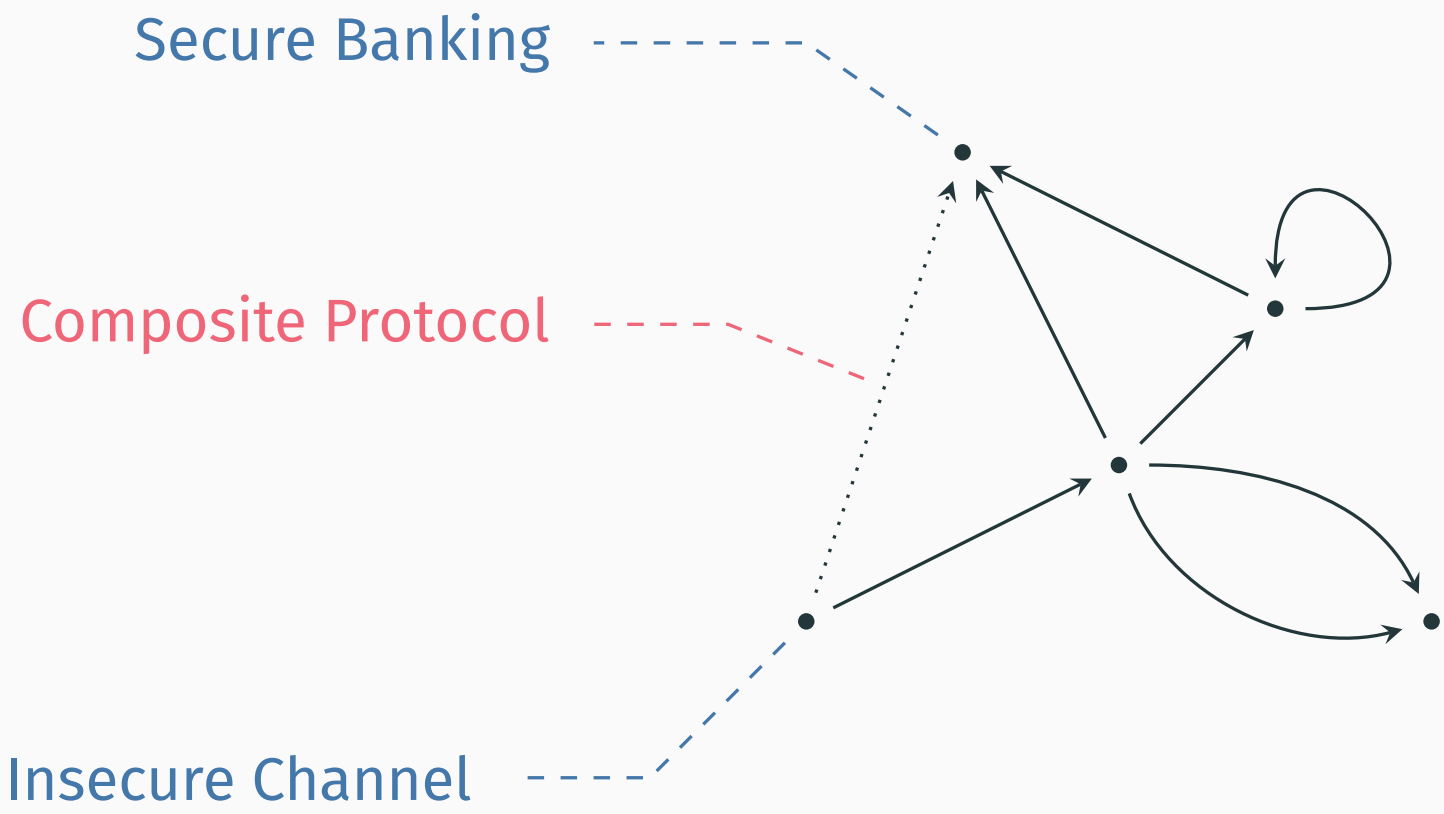
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



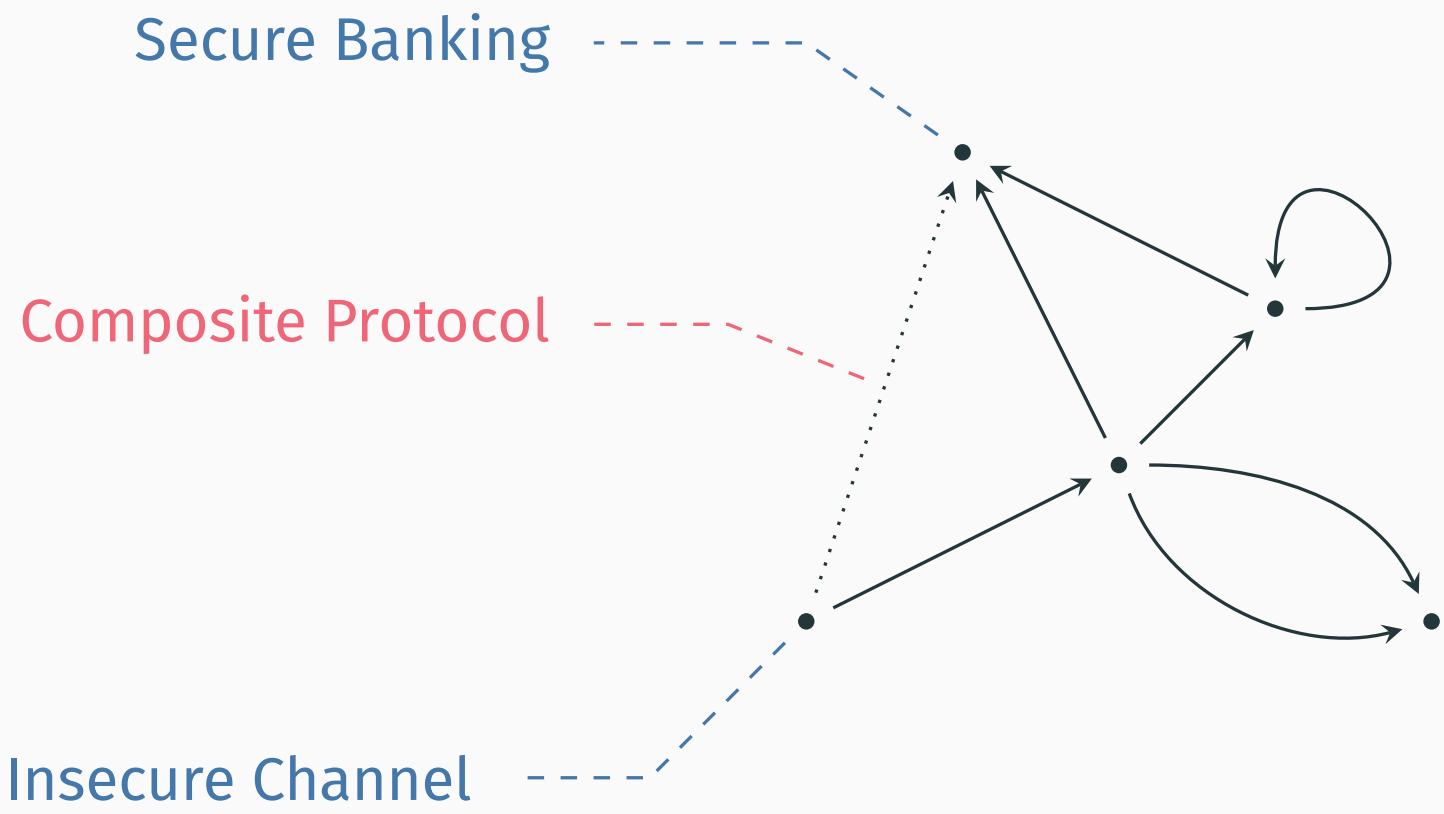
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



[Largely following Broadbent and Karvonen (2022)]

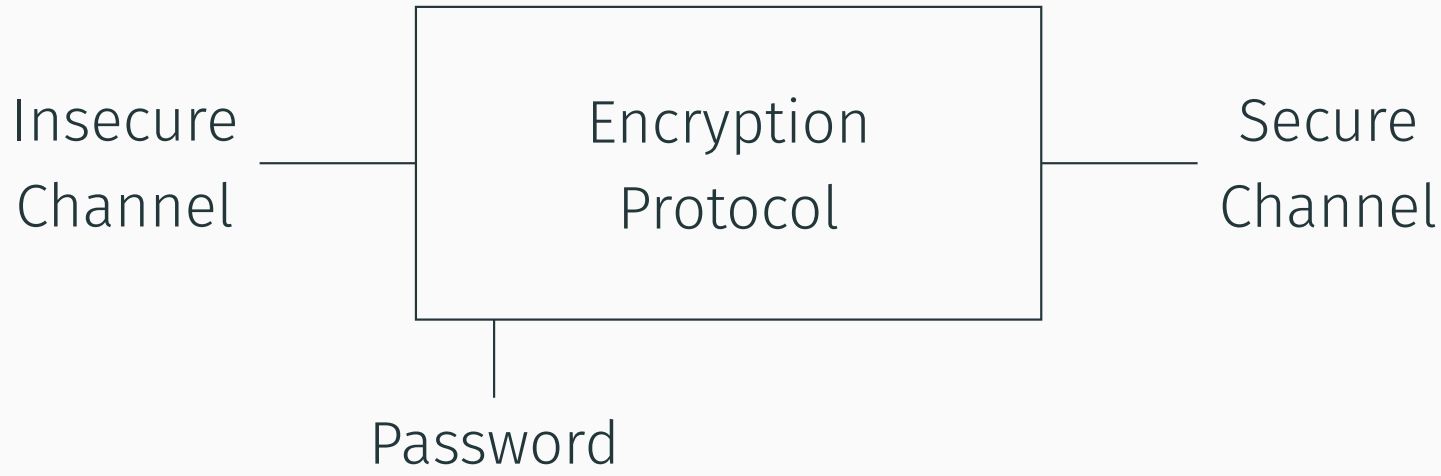
Categories and Cryptography



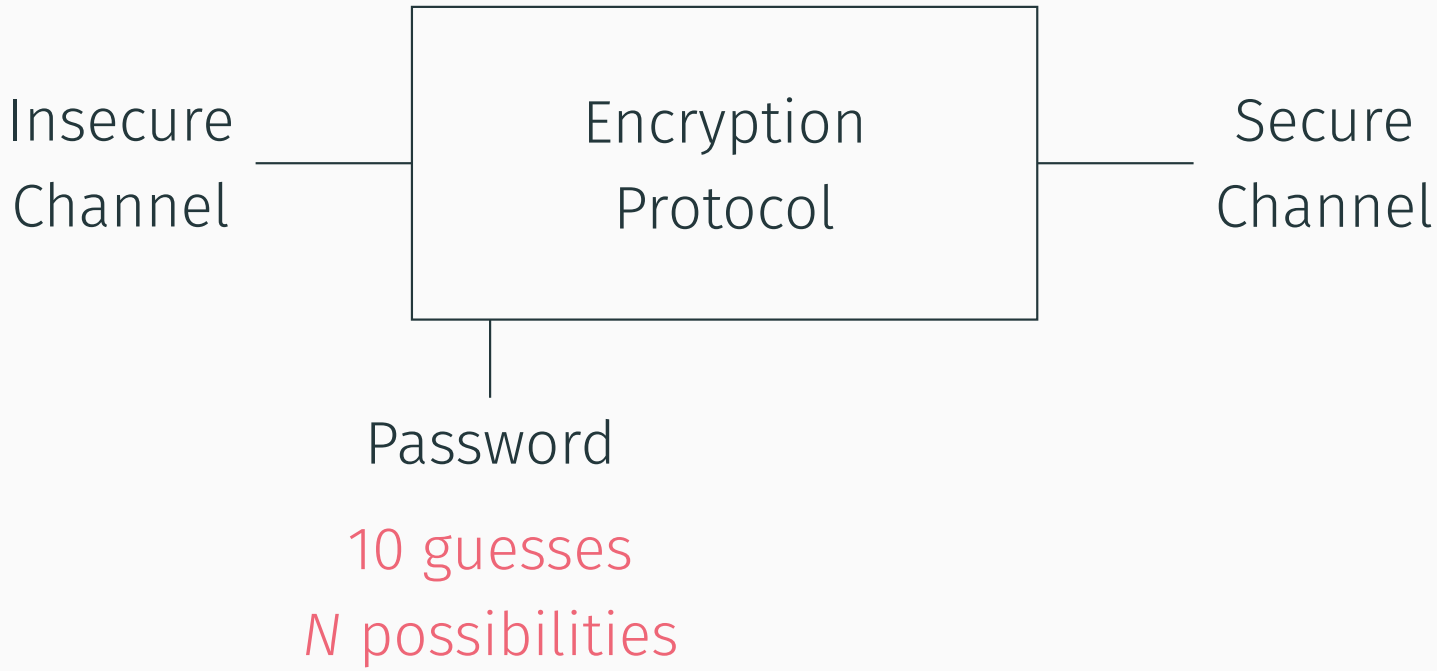
The challenge is to encode cryptographic objects as a category.

Security is Approximate

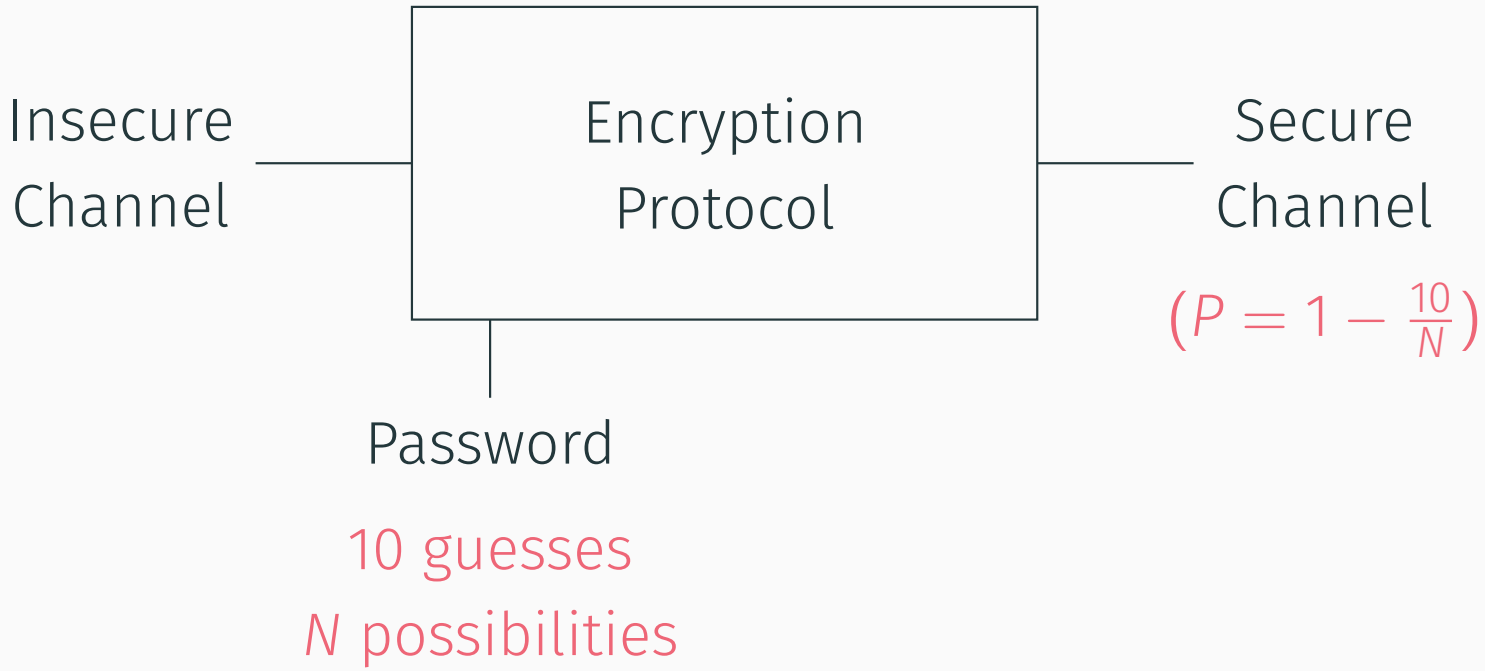
Security is Approximate



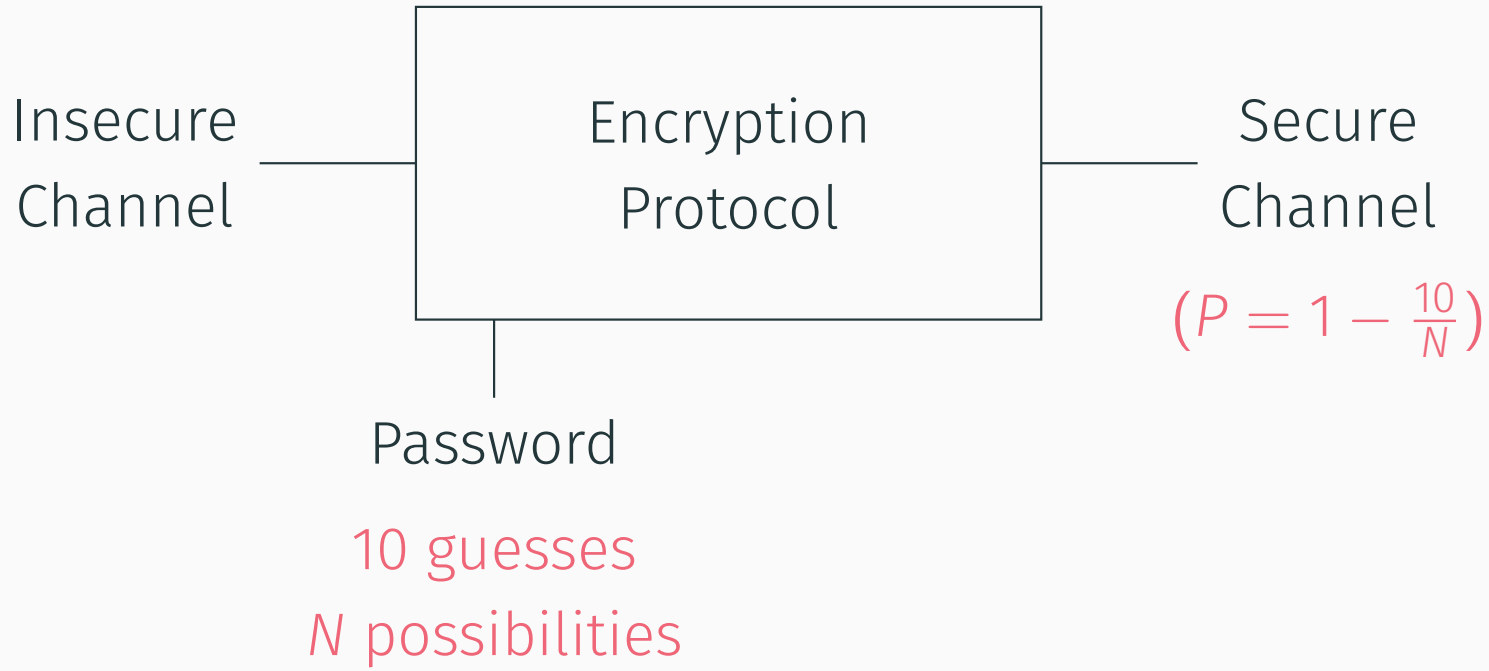
Security is Approximate



Security is Approximate

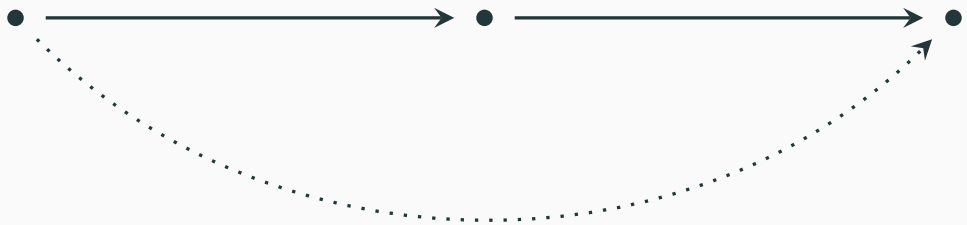


Security is Approximate

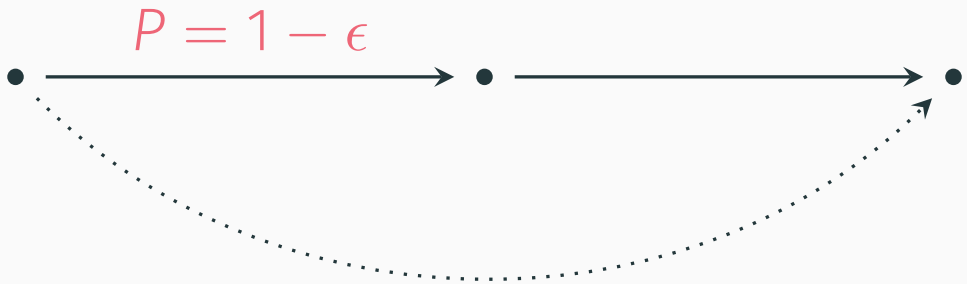


Cryptographers are very good at dealing with this.

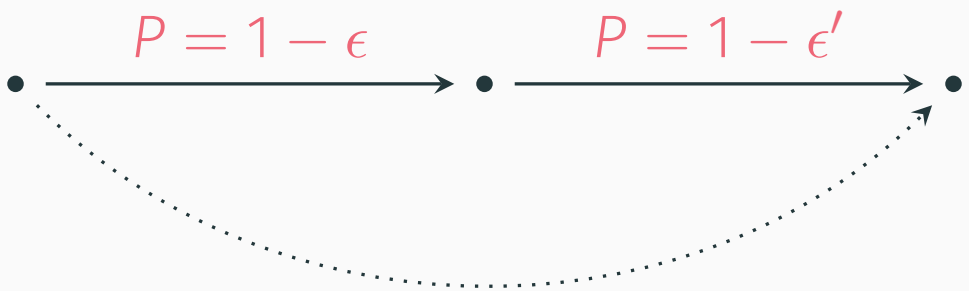
Approximate Composition



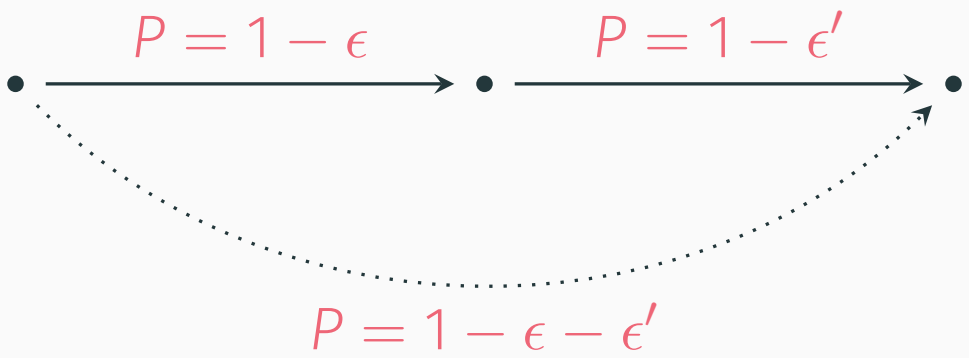
Approximate Composition



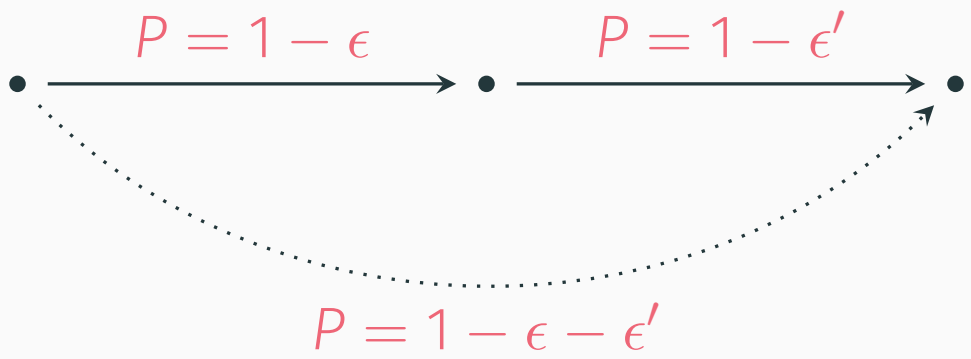
Approximate Composition



Approximate Composition

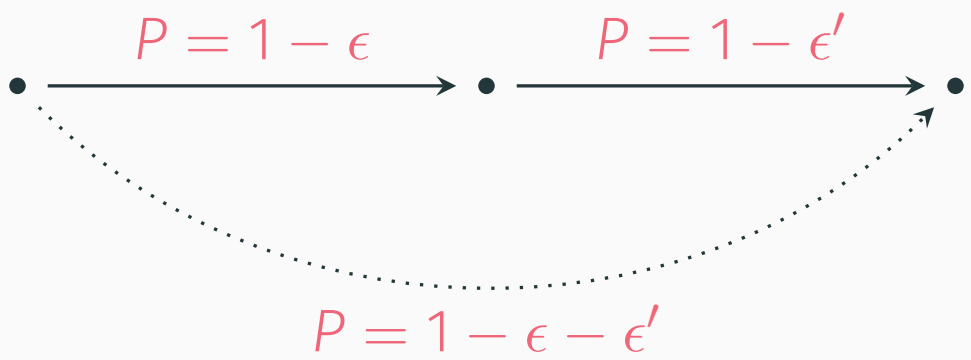


Approximate Composition



Small probabilities compound under composition.

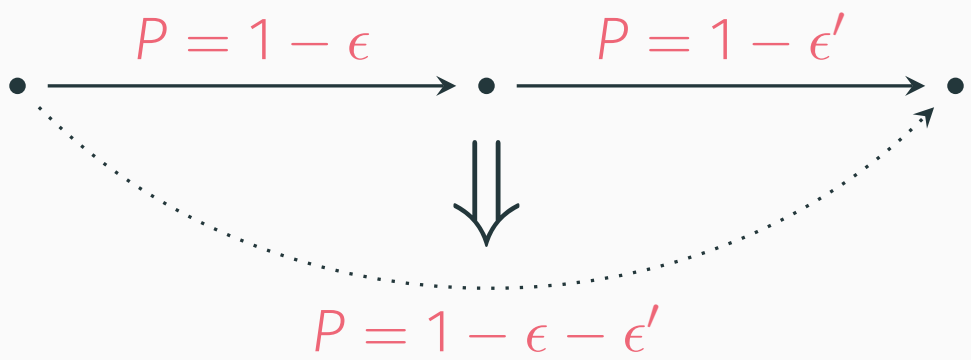
Approximate Composition



Small probabilities compound under composition.

Our idea is to work in *monoidal categories enriched over symmetric monoidal bicategories*.

Approximate Composition



Small probabilities compound under composition.

Our idea is to work in *monoidal categories enriched over symmetric monoidal bicategories*.

Outlook

Outlook

There are good reasons to want a categorical theory of cryptographic composability.

Outlook

There are good reasons to want a categorical theory of cryptographic composability.

We've made meaningful progress towards this goal.

Outlook

There are good reasons to want a categorical theory of cryptographic composability.

We've made meaningful progress towards this goal.

There are major outstanding issues.

Outlook

There are good reasons to want a categorical theory of cryptographic composability.

We've made meaningful progress towards this goal.

There are major outstanding issues.

Thanks for your time!

References

Broadbent, Anne and Martti Karvonen (2022). **“Categorical composable cryptography”.** In: *Foundations of software science and computation structures*. Vol. 13242. Lecture Notes in Comput. Sci. Springer, Cham, pp. 161–183. ISBN: 9783030992538. DOI: 10.1007/978-3-030-99253-8_9.

Canetti, Ran (2000). ***Universally Composable Security: A New Paradigm for Cryptographic Protocols.*** Cryptology ePrint Archive, Paper 2000/067. URL: https://eprint.iacr.org/2000/067.

David, Bernardo et al. (2023). **“Perfect MPC over Layered Graphs”.** In: *Advances in Cryptology – CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. Cham: Springer Nature Switzerland, pp. 360–392. ISBN: 978-3-031-38557-5.

Davies, Gareth T. et al. (2023). ***Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol.*** Cryptology ePrint Archive, Paper 2023/843. URL: https://eprint.iacr.org/2023/843.