Categories for Cryptographic Composability

Riley Shahar

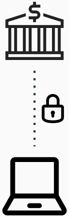
Advised by Angélica Osorno (Math) and Adam Groce (CS)

Cryptography

Cryptography is *the mathematical study of secure computation.*

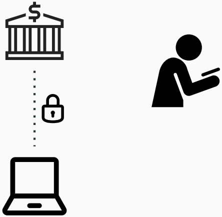
Cryptography

Cryptography is *the mathematical study of secure computation.*



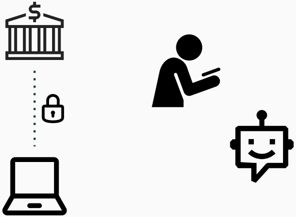
Cryptography

Cryptography is *the mathematical study of secure computation.*



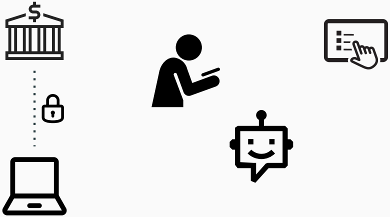
Cryptography

Cryptography is *the mathematical study of secure computation.*



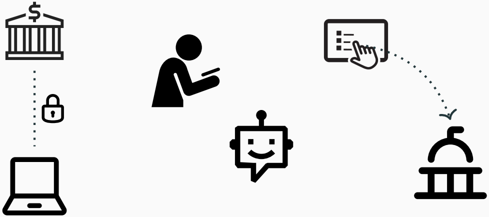
Cryptography

Cryptography is *the mathematical study of secure computation.*



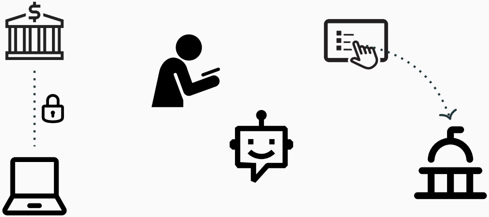
Cryptography

Cryptography is *the mathematical study of secure computation.*



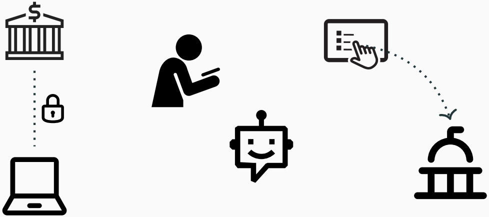
Cryptography

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



Cryptography

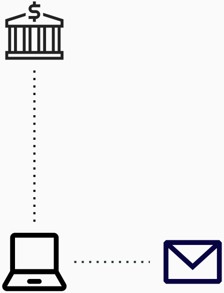
Cryptography is *the **mathematical** study of secure computation.*



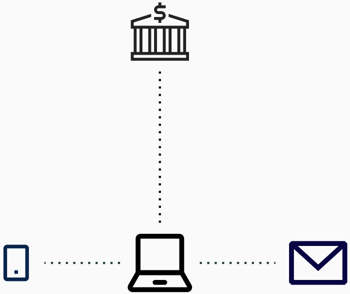
We want *proofs* that these things are secure.

Cryptographic Composability

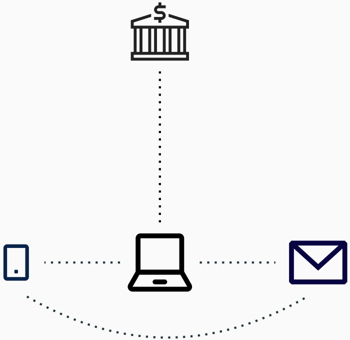
Cryptographic Composability



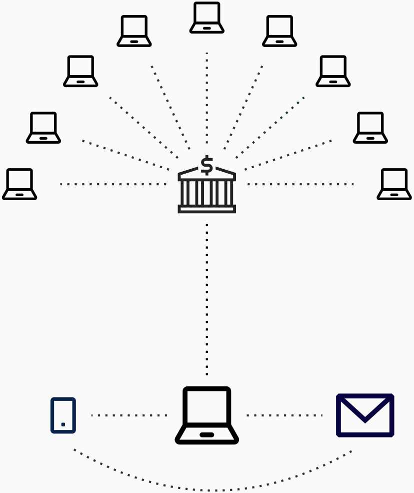
Cryptographic Composability



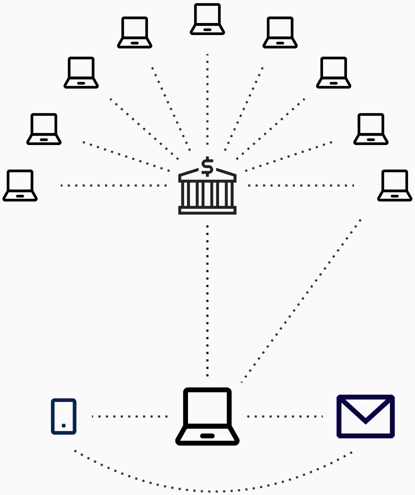
Cryptographic Composability



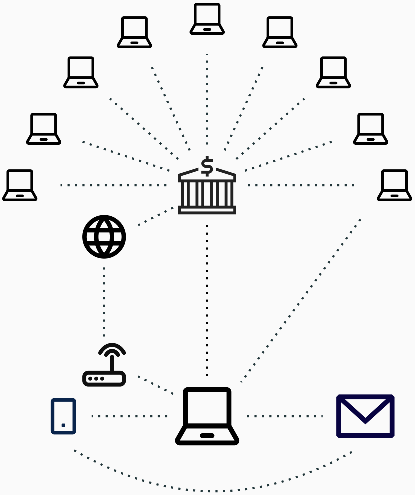
Cryptographic Composability



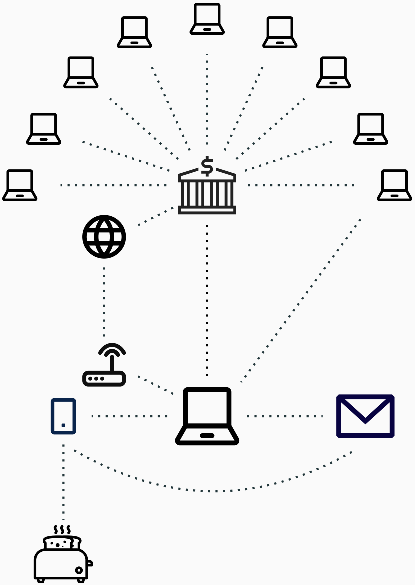
Cryptographic Composability



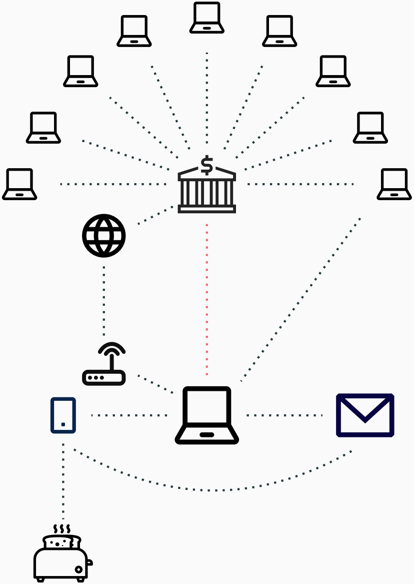
Cryptographic Composability



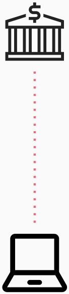
Cryptographic Composability



Cryptographic Composability

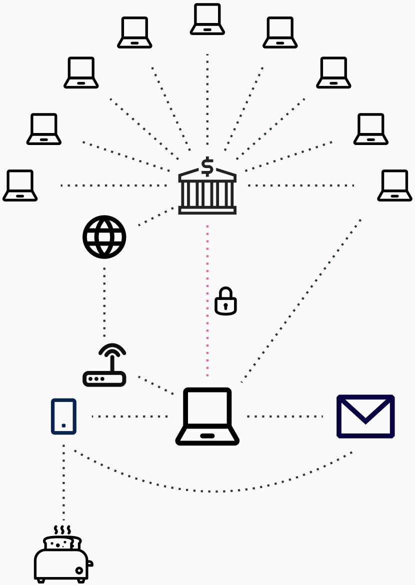


Cryptographic Composability

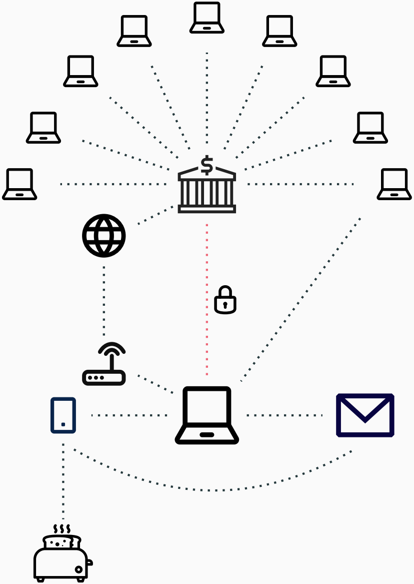


Cryptographic Composability

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

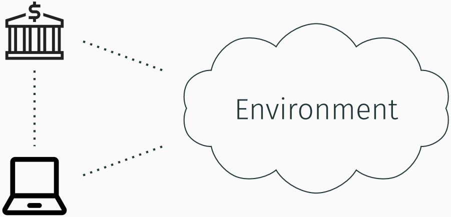
Due to Ran Canetti (2000).

Universal Composability

Due to Ran Canetti (2000).

Universal Composability

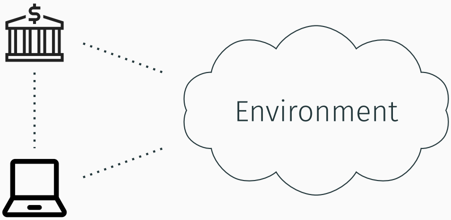
Due to Ran Canetti (2000).



Universal Composability

Due to Ran Canetti (2000).

Exactly what we want!

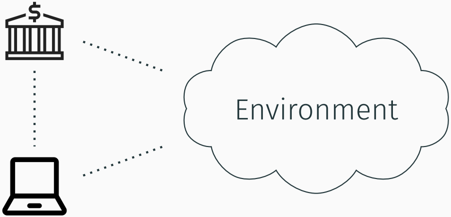


Universal Composability

Due to Ran Canetti (2000).

Exactly what we want!

Informal survey of CRYPTO* 2023:



*Cryptography, not cryptocurrency!

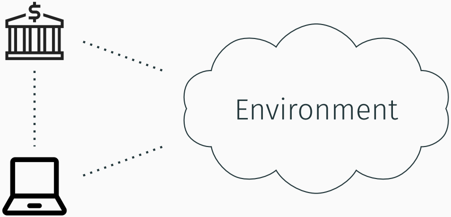
Universal Composability

Due to Ran Canetti (2000).

Exactly what we want!

Informal survey of CRYPTO* 2023:

- 124 papers



*Cryptography, not cryptocurrency!

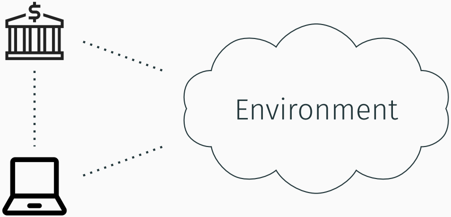
Universal Composability

Due to Ran Canetti (2000).

Exactly what we want!

Informal survey of CRYPTO* 2023:

- 124 papers
- 9 address general composition of their work



*Cryptography, not cryptocurrency!

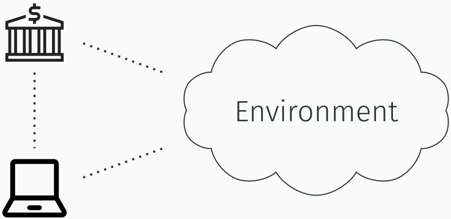
Universal Composability

Due to Ran 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 concurrent 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 and carefully arguing their security.*
>
> –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.”

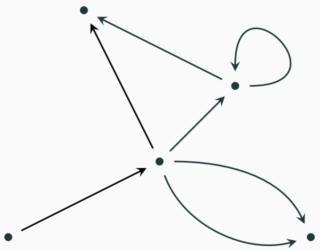
Categories are to composition as calculus is to change.

Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

Categories are to composition as calculus is to change.

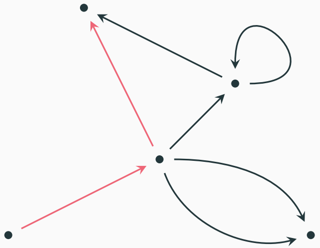


Category Theory

Lovingly called “abstract nonsense.”

The “mathematics of mathematics.”

Categories are to composition as calculus is to change.

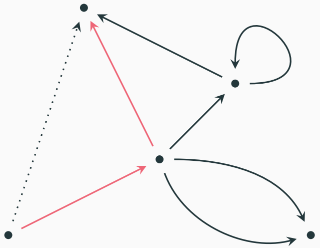


Category Theory

Lovingly called "abstract nonsense."

The "mathematics of mathematics."

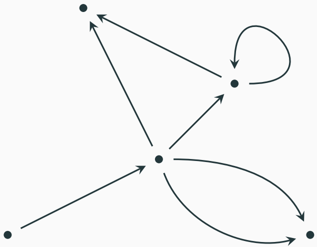
Categories are to composition as calculus is to change.



Categories and Cryptography

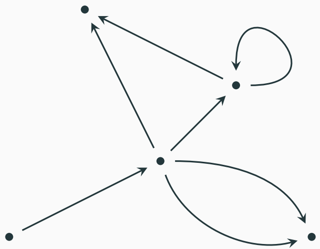
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



[Largely following Broadbent and Karvonen (2022)]

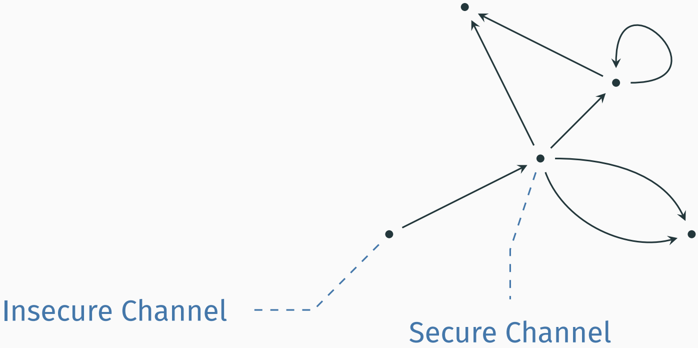
Categories and Cryptography



Insecure Channel

[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography

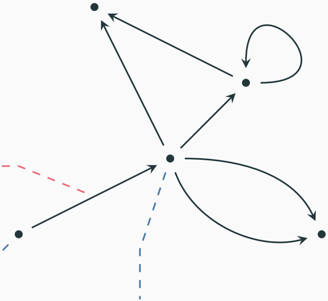


Insecure Channel

Secure Channel

[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



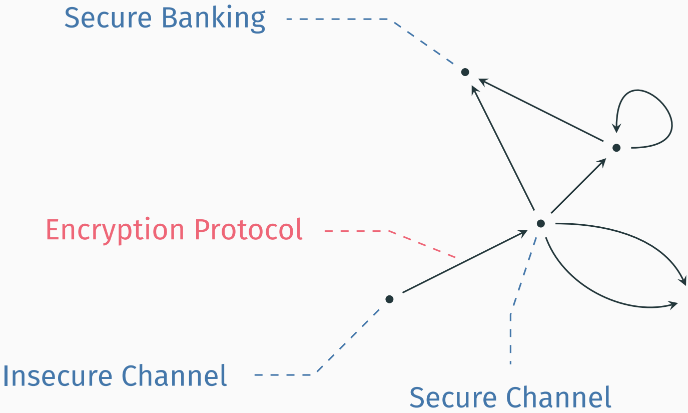
Encryption Protocol

Insecure Channel

Secure Channel

[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



Secure Banking

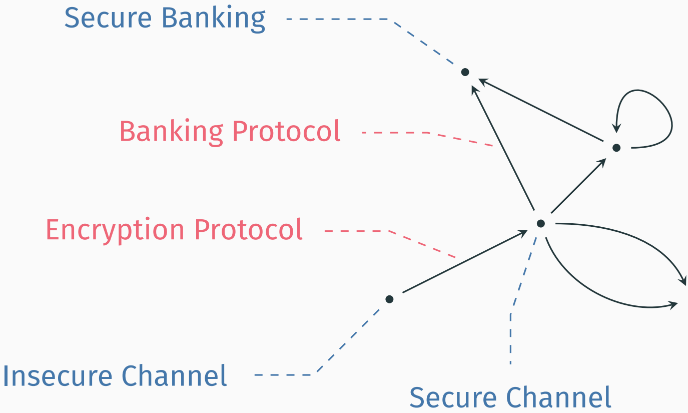
Encryption Protocol

Insecure Channel

Secure Channel

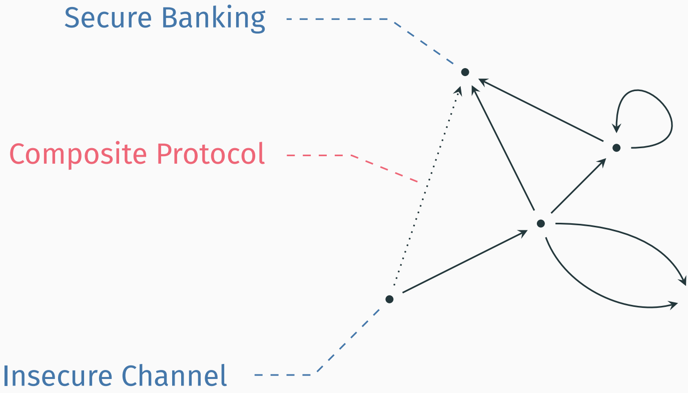
[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



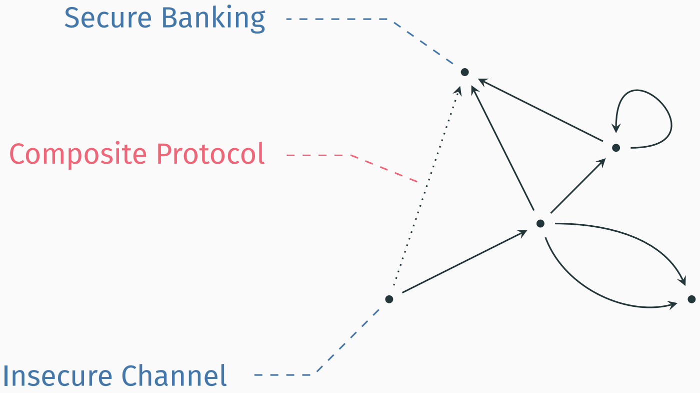
Secure Banking

Composite Protocol

Insecure Channel

[Largely following Broadbent and Karvonen (2022)]

Categories and Cryptography



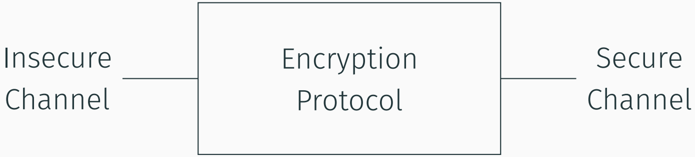
Secure Banking

Composite Protocol

Insecure Channel

The challenge is to encode cryptographic objects as a category.

Security is Approximate

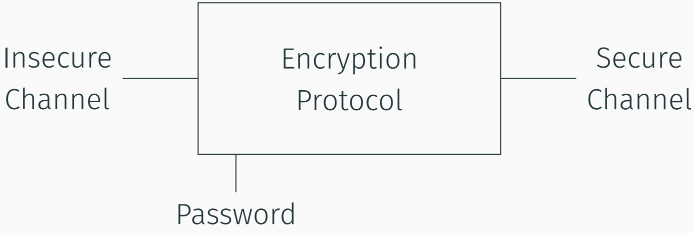


Insecure Channel

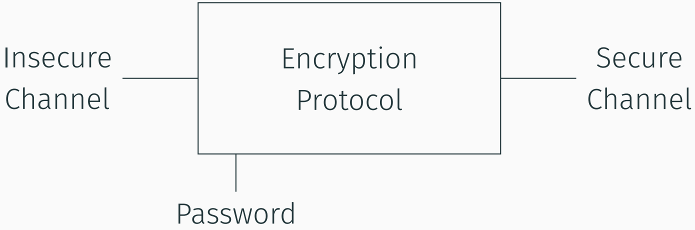
Encryption Protocol

Secure Channel

Security is Approximate



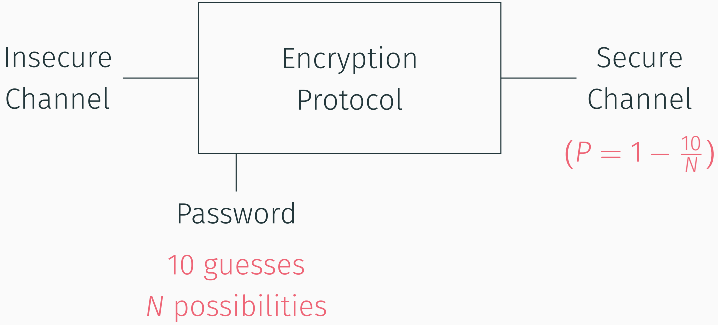
Security is Approximate



10 guesses

N possibilities

Security is Approximate



Insecure Channel

Encryption Protocol

Secure Channel

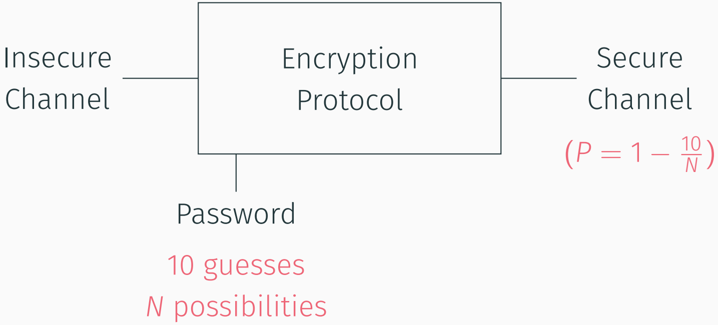
$(P = 1 - \frac{10}{N})$

Password

10 guesses

N possibilities

Security is Approximate


Insecure Channel

Encryption Protocol

Secure Channel

$(P = 1 - \frac{10}{N})$

Password

10 guesses

N possibilities

Cryptographers are very good at dealing with this.

Approximate Composition

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[rr, bend right, dotted] & \bullet \arrow[r] & \bullet
\end{tikzcd}$$

Approximate Composition

$$\begin{tikzcd}
\bullet \arrow[r, "P = 1 - \epsilon"] \arrow[rr, bend right, dotted] & \bullet \arrow[r] & \bullet
\end{tikzcd}$$

Approximate Composition

$$\begin{tikzcd}
\bullet \arrow[r, "P = 1 - \epsilon"] \arrow[rr, bend right, dotted] & \bullet \arrow[r, "P = 1 - \epsilon'"] & \bullet
\end{tikzcd}$$

Approximate Composition

$$\begin{tikzcd}
\bullet \arrow[r, "P = 1 - \epsilon"] \arrow[rr, dotted, bend right, "P = 1 - \epsilon - \epsilon'"'] & \bullet \arrow[r, "P = 1 - \epsilon'"] & \bullet
\end{tikzcd}$$

Approximate Composition

$$\begin{tikzcd}
\bullet \arrow[r, "P = 1 - \epsilon"] \arrow[rr, bend right, dotted, "P = 1 - \epsilon - \epsilon'"'] & \bullet \arrow[r, "P = 1 - \epsilon'"] & \bullet
\end{tikzcd}$$

Small probabilities compound under composition.

Approximate Composition

$$\begin{tikzcd}
\bullet \arrow[r, "P = 1 - \epsilon"] \arrow[rr, bend right, dotted, "P = 1 - \epsilon - \epsilon'"'] & \bullet \arrow[r, "P = 1 - \epsilon'"] & \bullet
\end{tikzcd}$$

Small probabilities compound under composition.

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

Approximate Composition

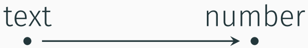
$$\begin{tikzcd} \bullet \arrow[r, "P = 1 - \epsilon"] \arrow[rr, bend right, dotted, "P = 1 - \epsilon - \epsilon'"'] & \bullet \arrow[r, "P = 1 - \epsilon'"] \arrow[d, phantom, "\Downarrow"] & \bullet \\ & {} & \end{tikzcd}$$

Small probabilities compound under composition.

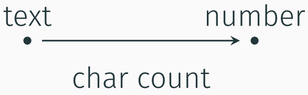
Our idea is to work in *monoidal categories enriched over symmetric monoidal bicategories*.

Breaking the Type System

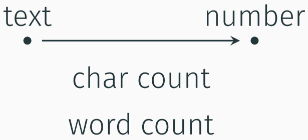
Breaking the Type System



Breaking the Type System



Breaking the Type System



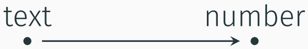
text

number

char count

word count

Breaking the Type System

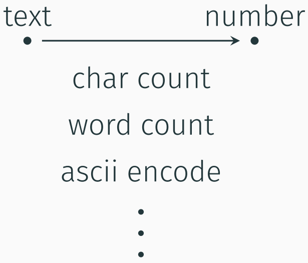


char count

word count

ascii encode

Breaking the Type System



text

number

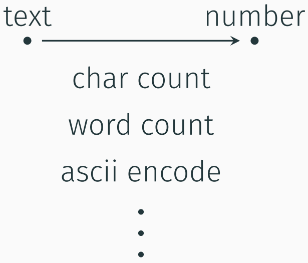
char count

word count

ascii encode

⋮

Breaking the Type System



text

number

char count

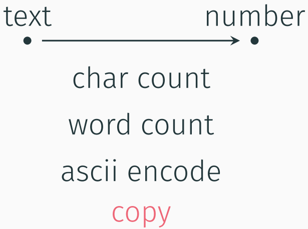
word count

ascii encode

⋮

In a category, we *have* to get a number at the end.

Breaking the Type System



text

number

char count

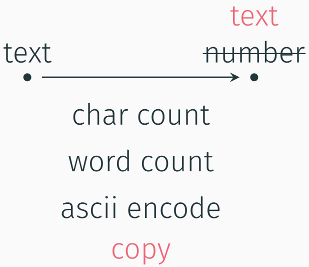
word count

ascii encode

copy

In a category, we *have* to get a number at the end.

Breaking the Type System



text

~~number~~

text

char count

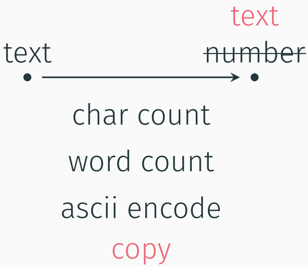
word count

ascii encode

copy

In a category, we *have* to get a number at the end.

Breaking the Type System



text

text

~~number~~

char count

word count

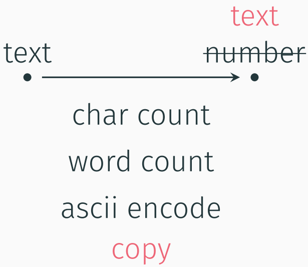
ascii encode

copy

In a category, we *have* to get a number at the end.

In cryptography, this isn't always true.

Breaking the Type System



text

text ~~number~~

char count

word count

ascii encode

copy

In a category, we *have* to get a number at the end.

In cryptography, this isn't always true.

B&K propose a workaround, but it's somewhat artificial.

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, potentially unresolvable.

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, potentially unresolvable.

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`. URL: `https://doi.org/10.1007/978-3-030-99253-8_9`.
- 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. `https://eprint.iacr.org/2023/843`. URL: `https://eprint.iacr.org/2023/843`.
- Khelifi, Adel et al. (2013). **“Enhancing protection techniques of e-banking security services using open source cryptographic algorithms”.** In: *2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*. IEEE, pp. 89–95.
- Sharma, Neha and Brahmdutt Bohra (2017). **“Enhancing online banking authentication using hybrid cryptographic method”.** In: *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*. IEEE, pp. 1–8.
- Shazmeen, Syeda Farha and Shyam Prasad (2012). **“A practical approach for secure internet banking based on cryptography”.** In: *International Journal of Scientific and Research Publications* 2.12, pp. 1–6.
- Yang, Yi-Jen (1997). **“The security of electronic banking”.** In: *Proc. Nat. I International Systems Security Conference*, pp. 41–52.