Basic Graphical Cryptography

Lucas C. Meier
lucas@cronokirby.com

2025-06-08

Abstract

Ahoy

1 Introduction

2 Abstract Graphical Language

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & \mathrm{im}(f) \\
G/\ker(f) \arrow[ur, dashed, hook, "\tilde{f}"] &
\end{tikzcd}$$

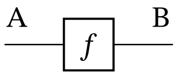
State our goal of defining “systems”

Show some final diagrams we aim to have

2.1 String Diagrams

We start with basic systems that have only a single input and output. These are sometimes called *functions*, but we avoid this term, as it suggests that these systems are mere mathematical functions, which is not the case. The jargon here, instead, is that of a *morphism*. In our case of cryptography, such morphisms may have effects, such as randomness. In general, these morphisms may not even be functions at all, for more abstract categories.

We depict a morphism $f : A \to B$ as a box, with one input wire, and one output wire:



The input and output wires are labelled with the type of object on that wire. We often omit these labels, when the object is clear from other context.

2.2 Copying and Deleting

2.3 Backwards Arrows

3 Some Cryptography Exercises

4 Concrete Semantics

5 State Separable Proofs

6 Past and Future

7 Conclusion