Categorical composable cryptography

Anne Broadbent and Martti Karvonen

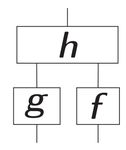
Department of Mathematics and Statistics, University of Ottawa

Big picture

We formalize the real-world ideal-world paradigm using category theory. The end-result is like abstract cryptography with (symmetric monoidal) categories as the algebraic theory of systems:

- General composability theorems: the class of protocols secure against any fixed set of attack models is closed under sequential and parallel composition.
- Can incorporate different attack models (e.g. colluding vs. independent adversaries, classical HBC) and computational security
- String diagrams enable pictorial yet rigorous proofs. For instance, known no-go theorems for two and three parties admit pictorial proofs.

Take home message: the real-world ideal-world paradigm is inherently composable, as long as you believe that pictures such as



can represent connections between computing systems without further specifying the order of drawing.
Full story available at: arXiv:2105.05949

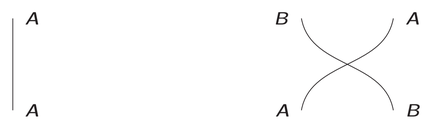
Categories and string diagrams in a nutshell

In a symmetric monoidal category (SMC), the basic notion is that of a morphism $f : A \to B$ going from an object A to the object B, depicted as 

.

Morphisms can be composed sequentially and in parallel:

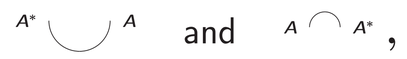
Special morphisms get special pictures



The axioms of an SMC guarantee that the pictures work: for an example, consider the category **Set** whose objects are sets, morphisms are functions, sequential composition is ordinary composition and cartesian products give the parallel composition.

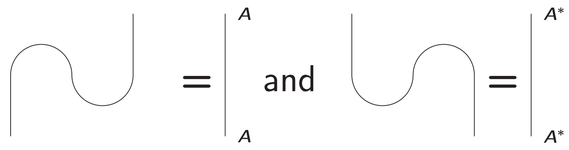
For cryptography, view the boxes as computational systems and the wires as their ports. There can be many ports or none:

In a compact closed category (e.g. sets and relations or f.d. Hilbert spaces) the wires can be bent



,

satisfying



so that "only connectivity matters".

Resource theories

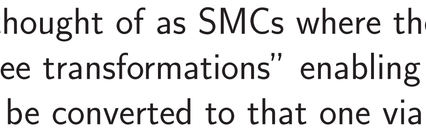
Resource theories can be thought of as SMCs where the objects are resources and the morphisms are "free transformations" enabling conversions between them: e.g. "can this state be converted to that one via LOCC?" or "can this quantum correlation simulate that one?". Cryptography fits this pattern, once security defintions are baked in.

Perfect security

The relevant notion of attack (e.g. this subset of parties is malicious or HBC) is captured by an attack model $\mathcal{A}$, which gives for each protocol f a set $\mathcal{A}(f)$ of potential attacks that could happen instead. Security is then captured like in the simulation paradigm: f securely realizes s from r if for any attack $a \in \mathcal{A}(f)$ on f there is an simulator $b \in \mathcal{A}(\mathrm{id})$ such that $ar = bs$. If $\mathcal{A}$ satisfies some reasonable axioms, this is automatically composable.

Example: multipartite computation

Assume the first k parties are honest and the last $n - k$ parties are dishonest. Then $(f_1, \dots f_k)$ is secure if for any a there is a b such that



It suffices to check this for the initial attack (akin to the"dummy adversary" in UC):

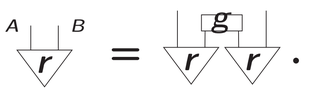
Defining security for any dishonest subset of $\{1, \dots n\}$ (whether colluding or not) is no more difficult.

Computational security

To move to perfect security, one replaces $=$ with an equivalence relation $\approx$ modelling indistinguishability, or works with a pseudometric and protocols secure in the limit or with a security bound ϵ. Composition theorems still go through, and in the last case security bounds compose additively.

Bipartite no-go theorem

For Alice and Bob (one of whom might cheat), if a bipartite functionality r can be securely realized from a communication channel between them, i.e. from $\cup$, then there exists a g such that

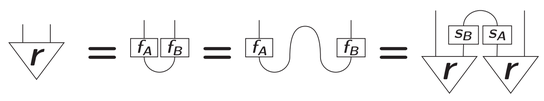


.

Proof sketch

Assume a protocol (f_A, f_B) realizing r securely. Security constraints against each party give us

Which gives



As a corollary, composable bit commitment and oblivious transfer are ruled out. A similar pictorial argument shows that pairwise channels are not enough for (composable) broadcasting in the tripartite case.

For more

Talk at SmP workshop 2021: recording slides
Talk at ACT 2021: recording slides
The preprint at `arXiv:2105.05949`.