Categorical composable cryptography

Martti Karvonen (joint work with Anne Broadbent)

ACT
16.7.2021

Composability in cryptography

One would expect that if you wire together “provably secure” protocols you end up with a secure protocol.

- This is false in general! Standard game-based security notions don’t necessarily guarantee composability. In fact, many“secure” protocols might not be secure anymore if several copies are run concurrently.

- QKD and 20(ish) years between first security proofs and composable ones.

- Several frameworks for composability and plenty of work within them, but none have convinced the whole community.

Real-world ideal-world paradigm

AKA simulation paradigm.

Usual definition: a real protocol P securely realizes the ideal functionality F from the resource R if for any attack A on $P \circ R$ there is a simulator S on F such that $(A, P) \circ R$ is indistuingishable from $S \circ F$ by any (efficient) environment.

"Any bad thing that could happen during the protocol could also happen in the ideal world."

Usual ways of making this precise:

- Fixing a concrete low-level formalism for interactive computation (e.g. UC-security)
- Abstract cryptography and constructive cryptography — close to our work in spirit but technically different

Cryptography as a resource theory

The key idea is that cryptography is a resource theory: the resources are various functionalities (e.g. keys, channels etc) and transformations are given by protocols that build the target resource *securely* from the starting resources.

E.g. the one-time pad is a protocol *key* $\otimes$ *insecure channel* $\rightarrow$ *secure channel* and its security corresponds to the fact that an eavesdropper might as well produce a random ciphertext for themselves.

This example is discussed in more detail in

'*Constructive Cryptography – A New Paradigm for Security Definitions and Proofs*'
Maurer, U., TOSCA 2011.

and I presented a string diagrammatic security proof (valid for any Hopf algebra with an integral in a monoidal cat) at the Structure Meets Power workshop on June 28th.

N+1th approach

In our work we formalize the simulation paradigm over an arbitrary category (and a model of attacks). The main result is that protocols secure against a fixed attack model can be composed sequentially and in parallel. The resulting model is flexible:

- simulation-based security definitions are inherently composable, whether the model of computation is synchronous or not, classical or quantum etc. To model multiparty computation, need only a symmetric monoidal category.
- abstract attack models pave way for other kinds of attackers than malicious ones
- different notions of security (computational, finite-key regimen etc) fit in
- CT and the tools and connections it brings

N+1th approach

Moreover, our approach lets one see existing results from a new viewpoint:

- Under some assumptions, monoidal functors preserve security vs. Unruh's lifting theorem
- existence of initial attacks vs. Canetti's "completeness of the dummy adversary"
- purely pictorial derivations of existing no-go results for two and three parties. Moreover, the pictures were already there to "illustrate" the proofs

Resource theories

Roughly: An SMC where you mostly care whether a hom-set is empty or not.
Examples:

- Can these noisy channels be used to simulate a (almost) noiseless channel?
- Is there a LOCC-protocol that transforms this quantum state to that one?
- Any preordered commutative monoid.

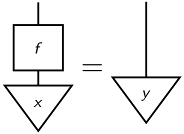
Many resource theories arise by taking the Grothendieck construction of $\mathbf{D} \xrightarrow{F} \mathbf{C} \xrightarrow{R} \mathbf{Set}$ where F interprets "free operations" in $\mathbf{C}$ and R gives for each $A \in \mathbf{C}$ the set $R(A)$ of resources of type $\mathbf{C}$.
Whenever RF is lax symmetric monoidal, $\int RF$ is a symmetric monoidal category, see

'*Monoidal Grothendieck construction*'

Moeller & Vasilakopoulou, TAC 2020.

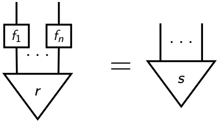
Example resource theories

Resource theory of states: apply $\int$ to $\mathbf{C}_F \hookrightarrow \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$.
Objects are states of $\mathbf{C}$, and maps $x \to y$ are maps f in $\mathbf{C}_F$ such that



.

n-partite version: apply $\int$ to $\mathbf{C}_F^n \xrightarrow{\otimes} \mathbf{C} \to \mathbf{Set}$. Objects are of the form $((A_i)_{i=1}^n, r\colon I \to \bigotimes A_i)$. A map $(((A_i)_{i=1}^n, r) \to (((B_i)_{i=1}^n, s)$ is then a tuple $(f_i)_{i=1}^n$ that transforms r to s:



We think of this as a resource theory with n-parties who try to agree on actions $f_1, \ldots f_n$ to transform some resource to another one.

Towards security

Such a protocol is not necessarily secure—what if some subset of the parties does something else instead?

If a subset J of $[n] := \{1, \ldots n\}$ is malicious, they can replace f_js for $j \in J$ with anything. The simulation paradigm says that the protocol is secure $r \to s$ if for any such attack on $(f_1 \ldots f_n)$ the subset could've attacked s with the same end-result

We abstract from here:

- an abstract attack model $\mathcal{A}$ that gives for each protocol f a collection $\mathcal{A}(f)$ of attacks on it
- security against $\mathcal{A}$: for each attack on the protocol there is an attack on the target with similar end-results

Abstract attacks

Definition

An *attack model* $\mathcal{A}$ on an SMC $\mathbf{C}$ consists of giving for each morphism f of $\mathbf{C}$ a class $\mathcal{A}(f)$ of morphisms of $\mathbf{C}$ such that

1. $f \in \mathcal{A}(f)$ for every f.
2. For any $f \colon A \to B$ and $g \colon B \to C$ and composable $g' \in \mathcal{A}(g), f' \in \mathcal{A}(f)$ we have $g' \circ f' \in \mathcal{A}(g \circ f)$. Moreover, any $h \in \mathcal{A}(g \circ f)$ factorizes as $g' \circ f'$ with $g' \in \mathcal{A}(g)$ and $f' \in \mathcal{A}(f)$.
3. For any $f \colon A \to B$, $g \colon C \to D$ in $\mathbf{C}$ and $f' \in \mathcal{A}(f), g' \in \mathcal{A}(g)$ we have $f' \otimes g' \in \mathcal{A}(f \otimes g)$. Moreover, any $h \in \mathcal{A}(f \otimes g)$ factorizes as $h' \circ (f' \otimes g')$ with $f' \in \mathcal{A}(f)$, $g' \in \mathcal{A}(g)$ and $h' \in \mathcal{A}(\mathrm{id}_{B \otimes D})$.

Examples

- $\mathcal{A}_{\mathrm{min}}(f) := \{f\}$ — represents honest behavior
- $\mathcal{A}_{\mathrm{max}}(f) := Mor(\mathbf{C})$ — represents arbitrary malicious behavior
- If $\mathcal{A}_i$ is an attack model on $\mathbf{C}_i$, then $\prod \mathcal{A}_i$ is an attack model on $\prod_i \mathbf{C}_i$. For instance, $\mathcal{A}_{\mathrm{min}} \times \mathcal{A}_{\mathrm{max}}$ represents two parties, Alice and Bob, with Alice honest and Bob malicious.
- In a concrete model of probabilistic interacting computation, can set $\mathcal{A}(f) := \{$ honest-but-curious variants of $f\}$

Abstract security

Definition

Let $f\colon (A,r) \to (B,s)$ define a morphism in the resource theory $\int RF$ induced by $F\colon \mathbf{D} \to \mathbf{C}$ and $R\colon \mathbf{C} \to \mathbf{Set}$. We say that f is *secure* against an attack model $\mathcal{A}$ on $\mathbf{C}$ (or $\mathcal{A}$-secure) if for any $f' \in \mathcal{A}(F(f))$ with $\mathrm{dom}(f') = F(A)$ there is $b \in \mathcal{A}(\mathrm{id}_{F(B)})$ such that $R(f')r = R(b)s$.

A subset X of $\mathcal{A}(f)$ is said to be *initial* if any $f' \in \mathcal{A}(f)$ with $\mathrm{dom}(f') = A$ can be factorized as $b \circ a$ with $a \in X$ and $b \in \mathcal{A}(\mathrm{id}_B)$.

Proposition

It suffices to check security against initial sets of attacks.

Composability

Theorem

Secure protocols form an SMC

Corollary

Protocols secure against $\mathcal{A}_1, \dots \mathcal{A}_k$ form a symmetric monoidal category

Proof.

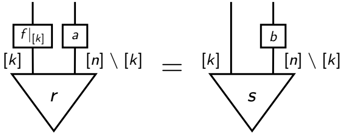
Symmetric monoidal subcategories are closed under intersection $\square$

Example

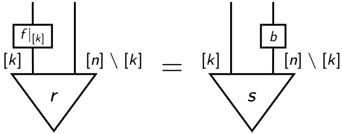
Fix a family of subsets of n parties: protocols secure against each of these subsets behaving maliciously form an SMC. For instance, in MPC one often studies protocols secure against at most $n/2$ or $n/3$ malicious participants.

Examples

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 $\bigotimes_{k+1}^{n} \mathrm{id}$:



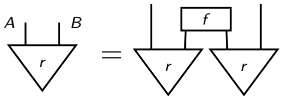
Initial honest-but-curious: follows the protocol and retains a transcript of it. Security: an identical (indistinguishable) protocol transcript can be simulated from the target functionality.

A no-go theorem for two parties

Let **C** now be a compact closed category, with $\cup$ modelling a shared communication channel.

Theorem

For Alice and Bob (one of whom might cheat), if a bipartite functionality r can be realized from a communication channel between them, i.e. from $\cup$ by a simple protocol, then r satisfies

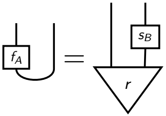


For some f.

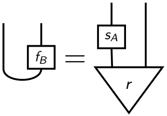
A no-go theorem for two parties

Proof.

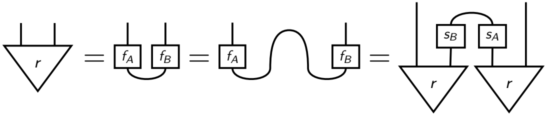
Assume a protocol $f_A \otimes f_B$ achieving this. Security constraints against each party give us



and



Which gives

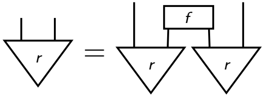


□

A no-go theorem for two parties

Theorem

For Alice and Bob (one of whom might cheat), if a bipartite functionality r can be realized from a communication channel between them, i.e. from $\cup$ *by a simple protocol, then r satisfies*



for some f.

Corollary

In the same bipartite setting, (composable) bit commitment and oblivious transfer are impossible without setup.

Extensions of the simple model

The above captures a very particular cryptographic situation:
There is no set-up, i.e. the parties have no free cryptographic primitives or communication not given by the starting functionality.

- This can be fixed by fixing a class $\mathcal{X}$ of free resources and defining general protocols $r \to s$ as those of the form $r \otimes x \to s$ — a variant of the Para-construction.

Security is perfect (i.e. information theoretic) instead of computational. This can be fixed in two ways:

- replace $=$ with an equivalence relation $\approx$ modelling computational indistinguishability
- Enrich in **Met**, and work with protocols that are secure in the limit

Summary

We have a categorical framework where

- composability is guaranteed (also for computational security)

- attack models are general enough to cover various kinds of adversarial behavior (e.g. colluding vs independent attackers)

- string diagrams can be used to make existing (or new) pictures into rigorous proofs

Questions...

?

Broadbent A., MK, “Categorical composable cryptography” (2021),arXiv:2105.05949

See also my talk at the Structure meets Power workshop on June 28th.