CATEGORICAL COMPOSABLE CRYPTOGRAPHY *

ANNE BROADBENT AND MARTTI KARVONEN

Department of Mathematics and Statistics, University of Ottawa, Canada
e-mail address: abroadbe@uottawa.ca

Department of Mathematics and Statistics, University of Ottawa, Canada
e-mail address: martti.karvonen@uottawa.ca

Abstract. We formalize the simulation paradigm of cryptography in terms of category theory and show that protocols secure against abstract attacks form a symmetric monoidal category, thus giving an abstract model of composable security definitions in cryptography. Our model is able to incorporate computational security, set-up assumptions and various attack models such as colluding or independently acting subsets of adversaries in a modular, flexible fashion. We conclude by using string diagrams to rederive the security of the one-time pad and no-go results concerning the limits of bipartite and tripartite cryptography, ruling out e.g., composable commitments and broadcasting. On the way, we exhibit two categorical constructions of resource theories that might be of independent interest: one capturing resources shared among multiple parties and one capturing resource conversions that succeed asymptotically.

1. Introduction

Modern cryptographic protocols are complicated algorithmic entities, and their security analyses are often no simpler than the protocols themselves. Given this complexity, it would be highly desirable to be able to design protocols and reason about them compositionally, i.e., by breaking them down into smaller constituent parts. In particular, one would hope that combining protocols proven secure results in a secure protocol without need for further security proofs. However, this is not the case for stand-alone security notions that are common in cryptography. To illustrate such failures of composability, let us consider the history of quantum key distribution (QKD), as recounted in [PR14]: QKD was originally proposed in the 80s [BB84]. The first security proofs against unbounded adversaries followed a decade later [May96, BBB$^+$00, SP00, May01]. However, since composability was originally not a concern, it was later realized that the original security definitions did not provide a good enough level of security [KRBM07]—they didn't guarantee security if the keys were to be actually used, since even a partial leak of the key would compromise the rest. The story

Key words and phrases: Cryptography, composable security, category theory.
* This is an extended version of a FoSSaCS 2022 conference paper [BK22] with the same title. This work was supported by the Air Force Office of Scientific Research under award number FA9550-20-1-0375, Canada's NFRF and NSERC, an Ontario ERA, and the University of Ottawa's Research Chairs program.

Preprint submitted to
Logical Methods in Computer Science

ends on a positive note, as eventually a new security criterion was proposed, together with stronger proofs [Ren05, BOHL+05].

In this work we initiate a categorical study of composable security definitions in cryptography. In the viewpoint developed here one thinks of cryptography as a resource theory: cryptographic functionalities (e.g. secure communication channels) are viewed as resources and cryptographic protocols let one transform some starting resources to others. For instance, one can view the one-time-pad as a protocol that transforms an authenticated channel and a shared secret key into a secure channel. For a given protocol, one can then study whether it is secure against some (set of) attack model(s), and protocols secure against a fixed set of models can always be composed sequentially and in parallel.

This is in fact the viewpoint taken in constructive cryptography [Mau11], which also develops the one-time-pad example above in more detail. However [Mau11] does not make a formal connection to resource theories as usually understood, whether as in quantum physics [HO13, CG19], or more generally as defined in order theoretic [Fri15] or categorical [CFS16] terms. Instead, constructive cryptography is usually combined with abstract cryptography [MR11] which is formalized in terms of a novel algebraic theory of systems [MMP+18].

Our work can be seen as a particular formalization of the ideas behind constructive cryptography, or alternatively as giving a categorical account of the real-world-ideal-world paradigm (also known as the simulation paradigm [GM84]), which underlies more concrete frameworks for composable security, such as universally composable cryptography [Can01] and others [PW00, BPW04, BPW07, MT13, HS15, LHM19, KTR20]. We will discuss these approaches and abstract and constructive cryptography in more detail in Section 1.1

Our long-term goal is to enable cryptographers to reason about composable security at the same level of formality as stand-alone security, *without having to fix all the details of a machine model nor having to master category theory.* Indeed, our current results already let one define multipartite protocols and security against arbitrary subsets of malicious adversaries *in any symmetric monoidal category* $\mathbf{C}$. Thus, as long as one's model of interactive computation results in a symmetric monoidal category, or more informally, one is willing to use pictures such as Figure 1d to depict connections between computational processes without further specifying the order in which the picture was drawn, one can use the simulation paradigm to reason about multipartite security against malicious participants composably—and specifying finer details of the computational model is only needed to the extent that it affects the validity of one's argument. Moreover, as our attack models and composition theorems are fairly general, we hope that more refined models of adversaries can be incorporated.

We now highlight our contributions to cryptography:

- We show how to adapt resource theories as categorically formulated [CFS16] in order to reason abstractly about *secure* transformations between resources. This is done in Section 4 by formalizing the simulation paradigm in terms of an abstract attack model (Definition 4.1), designed to be general enough to capture standard attack models of interest (and more) while still structured enough to guarantee composability. This section culminates in Corollary 4.5, which shows that for any fixed set of attack models, the class of protocols secure against each of them results in a symmetric monoidal category. In Theorem 4.8 we observe that under suitable conditions, images of secure protocols under monoidal functors remain secure, which gives an abstract variant of the lifting theorem [Unr10, Theorem 15] that states that perfectly UC-secure protocols are quantum UC-secure.

- We adapt this framework to model *computational security* in section 5.2 in two ways: either by replacing equations with an equivalence relation, abstracting the idea of computational indistinguishability, or by working with a notion of distance. In the case of a distance, one can then either explicitly bound the distance between desired and actually achieved behavior, or work with sequences of protocols that converge to the target in the limit: the former models working in the finite-key regimen [TLGR12] and the latter models the kinds of asymptotic security and complexity statements that are common in cryptography. In the former case we show that errors compose additively in Lemma 5.5, and in Theorem 5.6 and in Corollary 5.7 we show that protocols that are correct in the limit can be composed at will.
- We then apply the framework developed to study bipartite and tripartite cryptography. We begin by giving *purely pictorial* proof of the security of the one-time pad in Section 6, valid for any Hopf algebra in any symmetric monoidal category. In Section 7, we reprove the no-go-theorems of [PR08, MR11, MMP$^+$18] concerning two-party commitments (resp. three-party broadcasting) in our setting, and reinterpret them as limits on what can be achieved securely in any compact closed category (resp. symmetric monoidal category). The key steps of the proof are done graphically, thus opening the door for cryptographers to use such pictorial representations as rigorous tools rather than merely as illustrations.
- We conclude by discussing choice of a model in Section 8 and further questions in Section 9.

Moreover, we discuss some categorical constructions capturing aspects of resource theories appearing in the physics literature. These contributions may be relevant for further categorical studies on resource theories, independently of their usage here.

- In [CFS16] it is observed that many resource theories arise from an inclusion $\mathbf{C}_F \hookrightarrow \mathbf{C}$ of free transformations into a larger monoidal category, by taking the resource theory of states. We observe that this amounts to applying the monoidal Grothendieck construction [MV20] to the functor $\mathbf{C}_F \to \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$. This suggests applying this construction more generally to the composite of monoidal functors $F\colon \mathbf{D} \to \mathbf{C}$ and $R\colon \mathbf{C} \to \mathbf{Set}$.
- In Example 3.1 we note that choosing F to be the n-fold monoidal product $\mathbf{C}^n \to \mathbf{C}$ captures resources shared by n parties and n-partite transformations between them.
- In Section 5.1 we model categorically situations where there is a notion of distance between resources, and instead of exact resource conversions one either studies approximate transformations or sequences of transformations that succeed in the limit.
- In Section 5.3 we discuss a variant of a construction on monoidal categories, used in special cases in [FST19] and discussed in more detail in [CGG$^+$21, Gav19], that allows one to declare some resources free and thus enlarge the set of possible resource conversions.

1.1. **Related work.** We have already mentioned that cryptographers have developed a plethora of frameworks for composable security, such as universally composable cryptography [Can01], reactive simulatability [PW00, BPW04, BPW07] and others [MT13, HS15, LHM19, KTR20]. Moreover, some of these frameworks have been adapted to the quantum setting [BOM04, Unr10, MQR09]. One might hence be tempted to think that the problem of composability in cryptography has been solved. However, it is fair to say that most mainstream cryptography is not formulated composably and that composable cryptography has yet to realize its full potential. Moreover, this proliferation of frameworks should be taken as evidence of the continued importance of the issue, and is in fact reflected by the existence of a recent Dagstuhl seminar on this matter [CKLS19]. Indeed, the aforementioned frameworks mostly consist of setting up fairly detailed models of interacting machines, which as an approach suffers from two drawbacks:

- In order to be more realistic, the detailed models are often complicated, both to reason in terms of and to define, thus making practicing cryptographers less willing to use them. Perhaps more importantly it is not always clear whether the results proven in a particular model apply more generally for other kinds of machines, whether those of a competing framework or those in the real world. It is true that the choice of a concrete machine model does affect what can be securely achieved—for instance, quantum cryptography differs from classical cryptography and similarly classical cryptography behaves differently in synchronous and asynchronous settings [BOCG93, KMTZ13]. Nevertheless, one might hope that composable cryptography could be done at a similar level of formality as complexity theory, where one rarely worries about the number of tapes in a Turing machine or of other low-level details of machine models.
- Changing the model slightly (to e.g. model different kinds of adversaries or to incorporate a different notion of efficiency) often requires reproving "composition theorems" of the framework or at least checking that the existing proof is not broken by the modification.

In contrast to frameworks based on detailed machine models, there are two closely related top-down approaches to cryptography: constructive cryptography [Mau11] and its cousin abstract cryptography [MR11]. We are indebted to both of these approaches, and indeed our framework could be seen as formalizing the key idea of constructive cryptography—namely, cryptography as a resource theory—and thus occupying a similar space as abstract cryptography. A key difference is that constructive cryptography is usually instantiated in terms of abstract cryptography [MR11], which in turn is based on a novel algebraic theory of systems [MMP$^+$18]. However, our work is not merely a translation from this theory to categorical language, as there are important differences and benefits that stem from formalizing cryptography in terms of a well-established and well-studied algebraic theory of systems—that of (symmetric) monoidal categories:

- The fact that cryptographers wish to compose their protocols *sequentially and in parallel* strongly suggests using *monoidal categories*, that have these composition operations as primitives. In our framework, protocols secure against a fixed set of attack models results in a symmetric monoidal category. In contrast, the algebraic theory of systems [MMP$^+$18] on which abstract cryptography is based takes parallel composition and internal wiring as its primitives. This design choice results in some technical kinks and tangles that are natural with any novel theory but have already been smoothed out in the case of category theory. For instance, in the algebraic theory of systems of [MMP$^+$18] the parallel composition is a partial operation and in particular the parallel composite of a system with itself is never defined[1] and the set of wires coming out of a system is fixed once and for all[2]. In contrast, in a monoidal category parallel composition is a total operation and whether one draws a box with n output wires of types $A_1, \dots A_n$ or single output wire of

[1]While the suggested fix is to assume that one has "copies" of the same system with disjoint wire labels, it is unclear how one recognizes or even defines *in terms of the system algebra* that two distinct systems are copies of each other.

[2]Indeed, while [PMM$^+$17] manages to bundle and unbundle ports along isomorphism when convenient, it seems like the chosen technical foundation makes this more of a struggle than it should be.

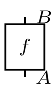
type $\bigotimes_{i=1}^{n} A_i$ is a matter of convenience. Technical differences such as these make a direct formal comparison or translation between the frameworks difficult, even if informally and superficially there are similarities.
- We do not abstract away from an attacker model, but rather make it an explicit part of the formalism that can be modified without worrying about composability. This makes it possible to consider and combine very easily different security properties, and in particular paves the way to model attackers with limited powers such as honest-but-curious adversaries. In our framework, one can first fix a protocol transforming some resource to another one, and then discuss whether this transformation is secure against different attack models. In contrast, in abstract cryptography a cryptographic resource is a tuple of functionalities, one for each set of dishonest parties, and thus has no prior existence before fixing the attack model. This makes the question "what attack models is this protocol secure against?" difficult to formalize.
- As category theory is de facto the lingua franca between several subfields of mathematics and computer science, elucidating the categorical structures present in cryptography opens up the door to further connections between cryptography and other fields. For instance, game semantics readily gives models of interactive, asynchronous and probabilistic (or quantum) computation [Win13, CDVW19b, CdVW19a] in which our theory can be instantiated, and thus further paves the way for programming language theory to inform cryptographic models of concurrency.
- Category theory comes with existing theory, results and tools that can readily be applied to questions of cryptographic interest. In particular the graphical calculi of symmetric monoidal and compact closed categories [Sel10] enables one to rederive impossibility results shown in [PR08, MR11, MMP^{+}18] purely pictorially. In fact, such pictures were already often used as heuristic devices that illuminate the official proofs, and viewing these pictures categorically lets us promote them from mere illustrations to rigorous yet intuitive proofs. Indeed, in [MR11, Footnote 27] the authors suggest moving from a 1-dimensional symbolic presentation to a 2-dimensional one, and this is exactly what the graphical calculus already achieves.

The approaches above result in a framework where security is defined so as to guarantee composability. In contrast, approaches based on various protocol logics [DMP01, DMP03, DDMP03b, DDMP03a, DDMP05, DDMR07] aim to characterize situations where composition can be done securely, even if one does not use composable security definitions throughout. As these approaches are based on process calculi, they are categorical under the hood [Pav97, MMP95] even if not overtly so. There is also earlier work explicitly discussing category theory in the context of cryptography [BMR19, CWW^{+}11, SHW20, BKM18, Heu08, Hil11, CP12, KTW17, SV13, Pav14, Hin20, Pav12], but they concern stand-alone security of particular (kinds of) cryptographic protocols, rather than categorical aspects of composable security definitions.

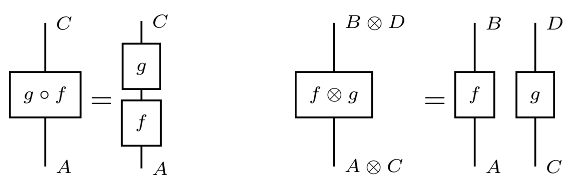
2. Background on monoidal categories and string diagrams

We assume that the reader is familiar with category theory in general and with monoidal and compact closed categories in particular, so we will recall the main concepts very briefly, mostly to explain the notation and string diagrams used. General references for category theory include [Mac71, Awo10, Bor94a, Bor94b, Rie17, Lei14] and string diagrams are surveyed in [Sel10]. However, a working cryptographer might find it easier to consult texts which are written with some applications in mind and introduce string diagrams concurrently with categories, such as [CP10, FS19, HV19].

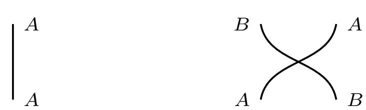
Let $\mathbf{C}$ be a symmetric monoidal category (SMC). Roughly speaking, this means that we have a class of objects $A, B, C, \ldots$, and a class of morphisms $f, g, h, \ldots$. We also have functions dom and cod that give us the domain and codomain of morphisms, and we write $f\colon A \to B$ to express that $A = \mathrm{dom}(f)$ and $B = \mathrm{cod}(f)$. Morphisms can be composed sequentially, i.e., whenever $f\colon A \to B$ and $g\colon B \to C$ there is a morphism $g \circ f = gf\colon A \to C$. In addition, there is a monoidal product $\otimes$ on objects and morphisms, that sends $f\colon A \to B$ and $g\colon C \to D$ to $f \otimes g\colon A \otimes C \to B \otimes D$. For each object there should be an identity morphism $\mathrm{id}_A\colon A \to A$, and there should be a special object I called the tensor unit. This data is subject to some constraints: composition should be (strictly) associative and unital, and the monoidal product should be associative, commutative and unital *up to coherent isomorphisms*, see [Bor94b, Section 6.1] for the precise details. Moreover, $\circ$ and $\otimes$ should cooperate in that the equations $(g \circ f) \otimes (j \circ h) = (g \otimes j) \circ (f \otimes h)$ and $\mathrm{id}_{A\otimes B} = \mathrm{id}_A \otimes \mathrm{id}_B$ hold. We will assume throughout that the variables $\mathbf{C}$ and $\mathbf{D}$ denote strict SMCs, meaning that associativity and unitality of $\otimes$ holds up to equality. This is mainly for notational convenience—first, any SMC is equivalent to a strict one and second, the theory we put forward could be developed without assuming strictness at the cost of some notational overhead. As an example of a (non-strict) SMC the reader could think e.g. of the category $\mathbf{Set}$ of sets and functions between them, with the monoidal structure given by cartesian product, or the category $\mathbf{Vect}_{\mathbb{R}}$ of real vector spaces and linear maps between them, with the monoidal structure given by tensor product.

The tersely sketched structure of an SMC is naturally internalized in the *graphical calculus* we use, which provides a sound and complete method for reasoning about them. Thus the reader less familiar with SMCs is invited to trust their visual intuition as it is unlikely to lead them astray. In this graphical calculus, we will denote a morphism $f\colon A \to B$ as 

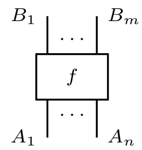
, and composition and monoidal product as



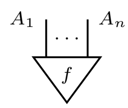
Special morphisms get special pictures: identities and symmetries are depicted as



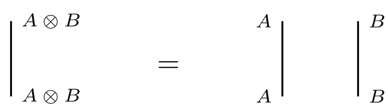
whereas the identity on the tensor unit is denoted by the empty picture. In general, a morphism might have multiple input/output wires



In particular a morphism $I \to A_1 \otimes \cdots \otimes A_n$ will have no incoming wires. We will call such morphisms *states* on $A_1 \otimes \cdots \otimes A_n$ and depict them as triangles instead of boxes:

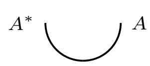


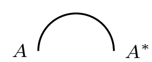
Note that the property $\mathrm{id}_{A\otimes B} = \mathrm{id}_A \otimes \mathrm{id}_B$ becomes



so that whether multiple wires are packaged into one or not is largely a matter of convenience. We will often omit labeling wires with the name of the object unless necessary, and at times the label will only give partial information.

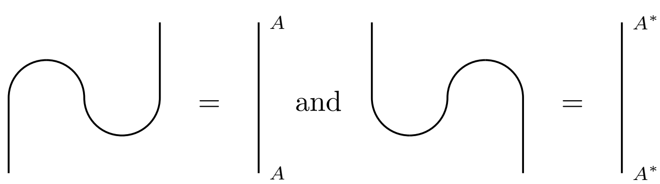
For Theorem 7.1 we will assume that our ambient category $\mathbf{C}$ is in fact a *compact closed category.* This means that $\mathbf{C}$ is an SMC, and we are also given for every object A an object A^* and morphisms



and


,

called cups and caps respectively, satisfying



Informally, this somewhat blurs the distinction between input and output wires, as one expects to happen if the boxes represent interactive and open computational processes. In particular, morphisms $A \to B$ correspond bijectively to states on $A^* \otimes B$, where the bijection is given by bending and unbending wires, and this correspondence should be seen as the categorical counterpart to the Choi–Jamiołkowski isomorphism from quantum information.

We will briefly conclude this section by discussing functors between SMCs. A lax monoidal functor $\mathbf{C} \to \mathbf{D}$ between monoidal categories is a functor $F\colon \mathbf{C} \to \mathbf{D}$ equipped with natural maps $F(A) \otimes F(B) \to F(A \otimes B)$ and a morphism $I_{\mathbf{D}} \to F(I_{\mathbf{C}})$ subject to certain coherence equations that roughly say that it cooperates with the monoidal structures on $\mathbf{C}, \mathbf{D}$ in a well-behaved manner. A strong monoidal functor is a lax monoidal one for which the structure maps $F(A) \otimes F(B) \to F(A \otimes B)$ and $I_{\mathbf{D}} \to F(I_{\mathbf{C}})$ are isomorphisms. A monoidal functor (in either sense) is symmetric if it additionally cooperates with the symmetries. We will use graphical calculus of strong monoidal functors in the proof of

Theorem 4.8, but otherwise do not refer to the detailed definitions nor use this graphical language, and hence we do not go into more detail here. Full definitions can be found e.g. at [Lei04, Section I.1.2] or at [Bor94b, Section 6.4], and a graphical calculus for them is discussed in [Mel06]. For us, all functors will be symmetric and either strong or lax monoidal, and we will specify which we mean whenever it makes a difference.

3. Resource theories

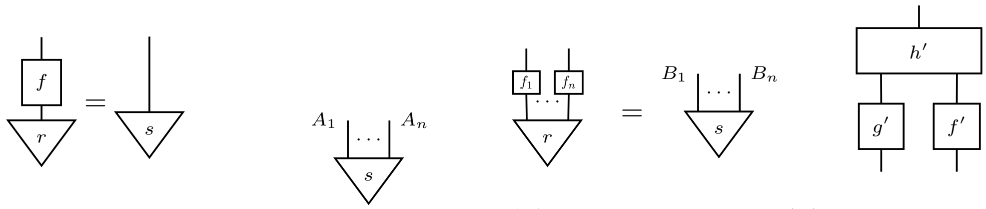
We briefly review the categorical viewpoint on resource theories of [CFS16]. Roughly speaking, a resource theory can be seen as an SMC but the change in terminology corresponds to a change in viewpoint: usually in category theory one studies global properties of a category, such as the existence of (co)limits, relationships to other categories, etc. In contrast, when one views a particular SMC $\mathbf{C}$ as resource theory, one is interested in local questions. One thinks of objects of $\mathbf{C}$ as resources, and morphisms as processes that transform a resource to another. From this point of view, one mostly wishes to understand whether $\hom_{\mathbf{C}}(X, Y)$ is empty or not for resources X and Y of interest. Thus from the resource-theoretic point of view, most of the interesting information in $\mathbf{C}$ is already present in its preorder collapse. As concrete examples of resource-theoretic questions, one might wonder if

- some noisy channels can simulate a (almost) noiseless channel [CFS16, Example 3.13.]
- there is a protocol that uses only local quantum operations and classical communication and transforms a particular quantum state to another one [CLM$^+$14]
- some non-classical statistical behavior can be used to simulate other such behavior [ABKM19]

In [CFS16] the authors show how many familiar resource theories arise in a uniform fashion: starting from an SMC $\mathbf{C}$ of processes equipped with a wide sub-SMC $\mathbf{C}_F$, the morphisms of which correspond to "free" processes, they build several resource theories (=SMCs). Perhaps the most important of these constructions is the resource theory of states: given $\mathbf{C}_F \hookrightarrow \mathbf{C}$, the corresponding resource theory of states can be explicitly constructed by taking the objects of this resource theory to be states of $\mathbf{C}$, i.e., maps $r \colon I \to A$ for some A, and maps $r \to s$ are maps $f \colon A \to B$ in $\mathbf{C}_F$ that transform r to s as in Figure 1a.

We now turn our attention towards cryptography. As contemporary cryptography is both broad and complex in scope, any faithful model of it is likely to be complicated as well. A benefit of the categorical idiom is that we can build up to more complicated models in stages, which is what we will do in the sequel. We phrase our constructions in terms of an arbitrary SMC $\mathbf{C}$, but in order to model actual cryptographic protocols, the morphisms of $\mathbf{C}$ should represent interactive computational machines with open "ports", with composition then amounting to connecting such machines together. Different choices of $\mathbf{C}$ set the background for different kinds of cryptography, so that quantum cryptographers want $\mathbf{C}$ to include quantum systems whereas in classical cryptography it is sufficient that these computational machines are probabilistic. Constructing such categories $\mathbf{C}$ in detail is not trivial but is outside our scope—we will discuss this in more detail in section 9.

Our first observation is that there is no reason to restrict to inclusions $\mathbf{C}_F \hookrightarrow \mathbf{C}$ in order to construct a resource theory of states. Indeed, while it is straightforward to verify explicitly that the resource theory of states is a symmetric monoidal category, it is instructive to understand more abstractly why this is so: in effect, the constructed category is the category of elements of the composite functor $\mathbf{C}_F \to \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$. As this composite is a (lax) symmetric monoidal functor, the resulting category is automatically symmetric monoidal as



(A) A map in the resource theory of states (B) An n-partite state (C) An n-partite transformation (D) Factorization of an attack on $f \otimes g$

FIGURE 1. Some resource transformations

observed in [MV20]. Thus this construction goes through for any symmetric (lax) monoidal functors $\mathbf{D} \xrightarrow{F} \mathbf{C} \xrightarrow{R} \mathbf{Set}$. Here we may think of F as interpreting free processes into an ambient category of all processes, and $R\colon \mathbf{C} \to \mathbf{Set}$ as an operation that gives for each object A of $\mathbf{C}$ the set $R(A)$ of resources of type A.

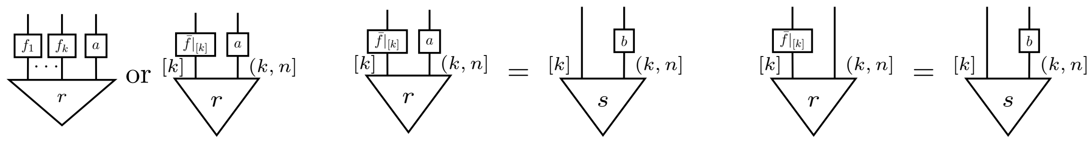
Explicitly, given symmetric monoidal functors $\mathbf{D} \xrightarrow{F} \mathbf{C} \xrightarrow{R} \mathbf{Set}$, the category of elements $\int RF$ has as its objects pairs (r, A) where A is an object of $\mathbf{D}$ and $r \in RF(A)$, the intuition being that r is a resource of type $F(A)$. A morphism $(r, A) \to (s, B)$ is given by a morphism $f\colon A \to B$ in $\mathbf{D}$ that takes r to s, i.e., satisfies $RF(f)(r) = s$. The symmetric monoidal structure comes from the symmetric monoidal structures of $\mathbf{D}, \mathbf{Set}$ and RF. Somewhat more explicitly, $(r, A) \otimes (s, B)$ is defined by $(r \otimes s, A \otimes B)$ where $r \otimes s$ is the image of (r, s) under the function $RF(A) \times RF(B) \to RF(A \otimes B)$ that is part of the monoidal structure on RF, and on morphisms of $\int RF$ the monoidal product is defined from that of $\mathbf{D}$.

From now on we will assume that F is strong monoidal, and while $R = \hom(I, -)$ captures our main examples of interest, we will phrase our results for an arbitrary lax monoidal R. This relaxation allows us to capture the n-partite structure often used when studying cryptography, as shown next.

Example 3.1. Consider the resource theory induced by $\mathbf{C}^n \xrightarrow{\otimes} \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$, where we write $\bigotimes$ for the n-fold monoidal product[3]. The resulting resource theory has a natural interpretation in terms of n agents trying to transform resources to others: an object of this resource theory corresponds to a pair $((A_i)_{i=1}^n, r\colon I \to \bigotimes A_i)$, and can be thought of as an n-partite state, depicted in Figure 1b, where the ith agent has access to a port of type A_i. A morphism $\bar{f} = (f_1, \dots f_n)\colon ((A_i)_{i=1}^n, r) \to ((B_i)_{i=1}^n, s)$ between such resources then amounts to a protocol that prescribes, for each agent i a process f_i that they should perform so that r gets transformed to s as in Figure 1c.

In this resource theory, all of the agents are equally powerful and can perform all processes allowed by $\mathbf{C}$, and this might be unrealistic: first of all, $\mathbf{C}$ might include computational processes that are too powerful/expensive for us to use in our cryptographic protocols. Moreover, having agents with different computational powers is important to model e.g. blind quantum computing [BFK09] where a client with access only to limited, if any, quantum computation tries to securely delegate computations to a server with a powerful quantum computer. This limitation is easily remedied: we could take the ith agent to be able to implement computations in some sub-SMC $\mathbf{C}_i$ of $\mathbf{C}$, and then consider $\prod_{i=1}^n \mathbf{C}_i \to \mathbf{C}$.

[3]As $\mathbf{C}$ is symmetric, the functor $\bigotimes$ is strong monoidal.



(A) Attack by the parties $k+1,\dots,n$ (B) Security against the parties $k+1,\dots,n$ (C) Security against the initial attack

FIGURE 2. Attacks and security constraints

A more serious limitation is that such transformations have no security guarantees—they only work if each agent performs f_i as prescribed by the protocol. We fix this next.

4. Cryptography as a resource theory

In order for a protocol $\bar{f} = (f_1,\dots,f_n)\colon ((A_i)_{i=1}^n, r) \to ((B_i)_{i=1}^n, s)$ to be secure, we should have some guarantees about what happens if, as a result of *an attack* on the protocol, something else than $(f_1,\dots,f_n)$ happens. For instance, some subset of the parties might deviate from the protocol and do something else instead. In the simulation paradigm [GM84], security is then defined by saying that, anything that could happen when running the real protocol, i.e., $\bar{f}$ with r, could also happen in the ideal world, i.e., with s. A given protocol might be secure against some kinds of attacks and insecure against others, so we define security against an abstract attack model. This abstract notion of an attack model is one of the main definitions of our paper. It isolates conditions needed for the composition theorem (Theorem 4.4). It also captures our key examples that we use to illustrate the definition after giving it.

Definition 4.1. 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 $h' \in \mathcal{A}(\mathrm{id}_{B\otimes D})$.

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 $b \in \mathcal{A}(\mathrm{id}_{F(B)})$ with $\mathrm{dom}(b) = F(B)$ such that $R(f')r = R(b)s$.

The above definition of security asks for perfect equality and corresponds to information-theoretic security in cryptography. This is often too much to hope for, and we will relax this requirement in Section 5.2.

The intuition is that $\mathcal{A}$ gives, for each process in $\mathbf{C}$, the set of behaviors that the attackers could force to happen instead of honest behavior. In particular, $\mathcal{A}(\mathrm{id}_B)$ give the set of behaviors that is available to attackers given access to a system of type B. Then property (i) amounts to the assumption that the adversaries could behave honestly. The first halves of properties (ii) and (iii) say that, given an attack on g and one on f, both attacks could happen when composing g and f sequentially or in parallel. The second parts of these say that attacks on composite processes can be understood as composites of attacks. However, note that (iii) does not say that an attack on a product has to be a product of attacks: the factorization says that any $h \in \mathcal{A}(g \otimes f)$ factorizes as in Figure 1d with $g' \in \mathcal{A}(g)$, $f' \in \mathcal{A}(f)$ and $h' \in \mathcal{A}(\mathrm{id}_{B\otimes D})$. The intuition is that an attacker does not have to attack two parallel protocols independently of each other, but might play the protocols against each other in complicated ways. This intuition also explains why we do not require that all morphisms in $\mathcal{A}(f)$ have $F(A)$ as their domain, despite the definition of $\mathcal{A}$-security quantifying only against those: when factoring $h \in \mathcal{A}(g \circ f)$ as $g' \circ f'$ with $g' \in \mathcal{A}(g)$ and $f' \in \mathcal{A}(f)$, we can no longer guarantee that $F(B)$ is the domain of g'—perhaps the attackers take us elsewhere when they perform f'.

If one thinks of $F\colon \mathbf{D} \to \mathbf{C}$ as representing the inclusion of free processes into general processes, one also gets an explanation why we do not insist that free processes and attacks live in the same category, i.e., that $F = \mathrm{id}_{\mathbf{C}}$. This is simply because we might wish to prove that some protocols are secure against attackers that can use more resources than we wish or can use in the protocols.

Example 4.2. For any SMC $\mathbf{C}$ there are two trivial attack models: the minimal one defined by $\mathcal{A}(f) = \{f\}$ and the maximal one sending f to the class of all morphisms of $\mathbf{C}$. We interpret the minimal attack model as representing honest behavior, and the maximal one as representing arbitrary malicious behavior.

Proposition 4.3. *If $\mathcal{A}_1, \dots, \mathcal{A}_n$ are attack models on SMCs $\mathbf{C}_1, \dots, \mathbf{C}_n$ respectively, then there is a product $\prod_{i=1}^n \mathcal{A}_i$ attack model on $\prod_{i=1}^n \mathbf{C}_i$ defined by $(\prod_{i=1}^n \mathcal{A}_i)(f_1, \dots, f_n) = \prod_{i=1}^n \mathcal{A}_i(f_i)$.*

Proof. The required properties of $\prod_{i=1}^n \mathcal{A}_i$ follow from those of each $\mathcal{A}_i$ and the fact that operations in $\prod_{i=1}^n \mathbf{C}_i$ are defined pointwise. □

This proposition, together with the minimal and maximal attack models, is already expressive enough to model multi-party computation where some subset of the parties might do arbitrary malicious behavior. Indeed, consider the n-partite resource theory induced by $\mathbf{C}^n \xrightarrow{\otimes} \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$. Let us first model a situation where the first $n-1$ participants are honest and the last participant is dishonest. In this case we can set $\mathcal{A} = \prod_{i=1}^n \mathcal{A}_i$ where each of $\mathcal{A}_1, \dots, \mathcal{A}_{n-1}$ is the minimal attack model on $\mathbf{C}$ and $\mathcal{A}_n$ is the maximal attack model. Then, an attack on $\bar{f} = (f_1, \dots f_n)\colon ((A_i)_{i=1}^n, r) \to ((B_i)_{i=1}^n, s)$ can be represented by the first $n-1$ parties obeying the protocol and the n-th party doing an arbitrary computation a, as depicted in the two pictures of Figure 2a, where $[n] := \{1, \dots, n\}$, $(k, n] := \{k+1, \dots n\}$, $\bar{f}|_{[k]} := \bigotimes_{i=1}^k f_i$, and here $k = n-1$. The latter representation will be used when we do not need to emphasize pictorially the fact that the honest parties are each performing their own individual computations.

If instead of just one attacker, there are several *independently* acting adversaries, we can take $\mathcal{A} = \prod_{i=1}^n \mathcal{A}_i$ where $\mathcal{A}_i$ is the minimal or maximal attack structure depending on whether the ith participant is honest or not. If the set of dishonest parties can collude and communicate arbitrarily during the process, we need the flexibility given in Definition 4.1 and have the attack structure live in a different category than where our protocols live. For simplicity of notation, assume that the first k agents are honest but the remaining parties are malicious and might do arbitrary (joint) processes in $\mathbf{C}$. In particular, the action done by the dishonest parties $k+1,\dots,n$ need not be describable as a product $\bigotimes_{i=k+1}^{n}(a_i)$ of individual actions. In that case we define $\mathcal{A}$ as follows: we first consider our resource theory as arising from $\mathbf{C}^n \xrightarrow{\mathrm{id}^k\times\otimes} \mathbf{C}^k\times\mathbf{C} \xrightarrow{\otimes} \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$, and define $\mathcal{A}$ on $\mathbf{C}^k\times\mathbf{C}$ as the product of the minimal attack model on $\mathbf{C}^k$ and the maximal one on $\mathbf{C}$. Concretely, this means that the first k agents always obey the protocol, but the remaining agents can choose to perform arbitrary joint behaviors in $\mathbf{C}$. Then a generic attack on a protocol $\bar{f}$ can be represented exactly as before in Figure 2a, except we no longer insist that $k=n-1$. Now a protocol $\bar{f}$ is $\mathcal{A}$-secure if for any a with $\mathrm{dom}(a)=(A_i)_{i=k+1}^{n}$ there is a b with $\mathrm{dom}(b)=(B_i)_{i=k+1}^{n}$ satisfying the equation of Figure 2b.

If one is willing to draw more wire crossings, one can easily depict and define security against an arbitrary subset of the parties behaving maliciously, and henceforward this is the attack model we have in mind when we say that some n-partite protocol is secure against some subset of the parties. Moreover, for any subset J of dishonest agents, one could consider more limited kinds of attacks: for instance, the agents might have limited computational power or limited abilities to perform joint computations—as long as the attack model satisfies the conditions of Definition 4.1 one automatically gets a composable notion of secure protocols by Theorem 4.4 below.

Theorem 4.4. *Given symmetric monoidal functors $F\colon\mathbf{D}\to\mathbf{C}$, $R\colon\mathbf{C}\to\mathbf{Set}$ with F strong monoidal and R lax monoidal, and an attack model $\mathcal{A}$ on $\mathbf{C}$, the class of $\mathcal{A}$-secure maps forms a wide sub-SMC of the resource theory $\int RF$ induced by RF.*

Proof. We first prove the claim when $F=\mathrm{id}_{\mathbf{C}}$. As the class of $\mathcal{A}$-secure maps is a subclass of maps inside an SMC, it suffices to show it contains all coherence isomorphisms (and thus all identities) and is closed under $\circ$ and $\otimes$.

For coherence isomorphisms we prove a stronger claim and show that all isomorphisms are $\mathcal{A}$-secure. Let $f\colon(A,r)\to(B,s)$ be an isomorphism so that f is an isomorphism $A\to B$ in $\mathbf{C}$, and consider $f'\in\mathcal{A}(f)$ with $\mathrm{dom}(f')=A$. Then $R(f')r=R(f')R(f^{-1})R(f)r=R(f')R(f^{-1})s$, so it suffices to show that $f'f^{-1}\in\mathcal{A}(\mathrm{id}_B)$. Property (i) of $\mathcal{A}$ implies that $(f^{-1})\in\mathcal{A}(f^{-1})$ so that property *(ii)* gives us $f'f^{-1}\in\mathcal{A}(ff^{-1})=\mathcal{A}(\mathrm{id}_B)$, as desired.

Assume now that $f\colon(A,r)\to(B,s)$ and $g\colon(B,s)\to(C,t)$ are $\mathcal{A}$-secure. Given $h\in\mathcal{A}(g\circ f)$ with domain A, factorize it as $g'\circ f'$ as guaranteed by (ii). As f is $\mathcal{A}$-secure, there is some $b\in\mathcal{A}(\mathrm{id}_B)$ with $R(f')r=R(b)s$ and by (ii) $g'b\in\mathcal{A}(g)$, so that security of g implies the existence of $c\in\mathcal{A}(\mathrm{id}_B)$ such that $R(g'b)(s)=R(c)t$. Thus $R(g'f')t=R(g')R(b)s=R(c)t$ showing that $g\circ f$ is $\mathcal{A}$-secure.

To show that secure maps are closed under $\otimes$, let $f\colon(A,r)\to(B,s)$ and $g\colon(C,t)\to(D,u)$ be $\mathcal{A}$-secure. Given $h\in\mathcal{A}(f\otimes g)$ with domain $A\otimes C$, factorize it as $h'\circ(f'\otimes g')$ as guaranteed by (iii). Then security of f and g gives us $b\in\mathcal{A}(\mathrm{id}_B)$ and $d\in\mathcal{A}(\mathrm{id}_D)$ so that $R(f')r=R(b)s$ and $R(g')t=R(d)u$. This implies that $R(h)(r\otimes t)=R(h')\circ(R(b)\otimes R(d))(s\otimes u)$, so $h'\circ(b\otimes d)\in\mathcal{A}(\mathrm{id}_B\otimes\mathrm{id}_D)$ witnesses that $f\otimes g$ is $\mathcal{A}$-secure.

To prove the claim for an arbitrary strong monoidal F, observe first that $f\colon(A,r)\to(B,s)$ is $\mathcal{A}$-secure in $\int RF$ if, and only if $F(f)\colon(F(A),r)\to(F(B),s)$ is $\mathcal{A}$-secure in $\int R$. The claim can now be deduced from the existence and description of pullbacks in the category of SMCs, but we give an explicit proof: the class of $\mathcal{A}$-secure maps in $\int RF$ contains all isomorphisms and is closed under composition because it is so in $\int R$. As F is strong monoidal, the square

$$\begin{array}{ccc} F(A\otimes C) & \xrightarrow{F(f\otimes g)} & F(B\otimes D) \\ \cong\downarrow & & \uparrow\cong \\ F(A)\otimes F(C) & \xrightarrow[F(f)\otimes F(g)]{} & F(B)\otimes F(D) \end{array}$$

commutes in $\mathbf{C}$. If $f\colon (A,r)\to(B,s)$ and $g\colon (C,t)\to(D,u)$ are $\mathcal{A}$-secure in $\int RF$, then $F(f)$ and $F(g)$ are $\mathcal{A}$-secure in $\int R$. The case $F=\mathrm{id}_{\mathbf{C}}$ implies that $F(f)\otimes F(g)$ is $\mathcal{A}$-secure so that $F(f\otimes g)$ is $\mathcal{A}$-secure as a composite of secure maps, which means that $f\otimes g$ is $\mathcal{A}$-secure in $\int RF$ as desired. □

So far we have discussed security only against a single, fixed subset of dishonest parties, while in multi-party computation it is common to consider security against any subset containing e.g. at most $n/3$ or $n/2$ of the parties. However, as monoidal subcategories are closed under intersection, we immediately obtain composability against multiple attack models.

Corollary 4.5. *Given a non-empty family of functors* $(\mathbf{D}\xrightarrow{F_i}\mathbf{C_i}\xrightarrow{R_i}\mathbf{Set})_{i\in I}$ *with* $R_iF_i=R_jF_j=:R$ *for all* $i,j\in I$ *and attack models* $\mathcal{A}_i$ *on* $\mathbf{C}_i$ *for each* i*, the class of maps in* $\int R$ *that is secure against each* $\mathcal{A}_i$ *is a sub-SMC of* $\int R$*.*

Using Corollary 4.5 one readily obtains composability of protocols that are simultaneously secure against different attack models $\mathcal{A}_i$. Thus one could, in principle, consider composable cryptography in an n-party setting where some subsets are honest-but-curious, some might be outright malicious but have limited computational power, and some subsets might be outright malicious but not willing or able to coordinate with each other, without reproving any composition theorems.

While the security definition of f quantifies over $\mathcal{A}(f)$, which may be infinite, under suitable conditions it is sufficient to check security only on a subset of $\mathcal{A}(f)$, so that whether f is $\mathcal{A}$-secure often reduces to finitely many equations.

Definition 4.6. Given $f\colon A\to B$, 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 $b\in\mathcal{A}(\mathrm{id}_B)$.

Theorem 4.7. *Let* $f\colon (A,r)\to(B,s)$ *define a morphism in the resource theory induced by* $F\colon\mathbf{D}\to\mathbf{C}$ *and* $R\colon\mathbf{C}\to\mathbf{Set}$ *and let* $\mathcal{A}$ *be an attack model on* $\mathbf{C}$*. If* $X\subset\mathcal{A}(F(f))$ *is initial, then* f *is* $\mathcal{A}$*-secure if, and only if the security condition holds against attacks in* X*, i.e., if for any* $f'\in X$ *with* $\mathrm{dom}(f')=F(A)$ *there is* $b\in\mathcal{A}(\mathrm{id}_{F(B)})$ *such that* $R(f')r=R(b)s$*.*

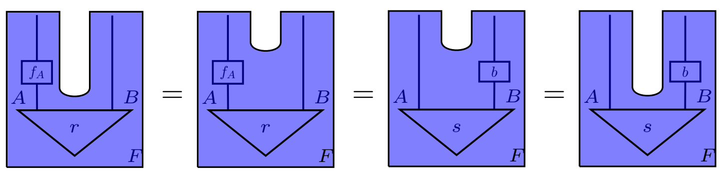
Proof. Let $f'\in\mathcal{A}(F(f))$ be an attack satisfying $\mathrm{dom}(f')=F(A)$. As X is initial, we can factorize f' as $b\circ a$ with $a\in X$ and $b\in\mathcal{A}(\mathrm{id}_{F(B)})$. As f is secure against attacks in X and $a\in X$, there is a $c\in\mathcal{A}(\mathrm{id}_{F(B)})$ such that $R(a)r=R(c)s$. Then $R(f')r=R(b)R(a)r=R(b)R(c)s=R(b\circ c)s$ sothat $b\circ a\mathcal{A}(\mathrm{id}_{F(B)})$ witnesses security against f'. □

Let us return to the example of $\mathbf{C}^n\to\mathbf{C}$ with the first k agents being honest and the final $n-k$ dishonest and collaborating. Then we can take a singleton as our initial subset of attacks on $\bar{f}$, and this is given by $\bar{f}|_{[k]}\otimes(\bigotimes_{i=k+1}^n\mathrm{id})$. Intuitively, this represents a situation where the dishonest parties $k+1,\ldots,n$ merely stand by and forward messages between the environment and the functionality, so that initiality can be seen as explaining "completeness of the dummy adversary" [Can01, Claim 11] in UC-security. In this case the security condition can be equivalently phrased by saying that there exists $b \in \mathcal{A}([\mathrm{id}_b])$ satisfying the equation of Figure 2c, which reproduces the pictures of [MT13]. Similarly, for classical honest-but-curious adversaries one usually only considers the initial such adversary, who follows the protocol otherwise except that they keep track of the protocol transcript.

Theorem 4.8. *In the resource theory of n-partite states, if $(f_1, \dots f_n)$ is secure against some subset J of $[n]$ and F is a strong monoidal, then $(Ff_1, \dots, Ff_n)$ is secure against J as well.*

Proof. Let us first spell out explicitly how the domain and codomain of $(Ff_1, \dots, Ff_n)$ depends on those of $\bar{f}$: if $\bar{f}\colon ((A_i)_{i=1}^n, r) \to ((B_i)_{i=1}^n, s)$, then $Fr\colon F(I_{\mathbf{C}}) \to F(\bigotimes_{i=1}^n A_i)$ induces a state on $\bigotimes_{i=1}^n F(A_i)$ by precomposing with the isomorphism $I_{\mathbf{D}} \to F(I_{\mathbf{C}})$ and postcomposing with the isomorphism $F(\bigotimes_{i=1}^n A_i) \cong \bigotimes_{i=1}^n F(A_i)$ stemming from the strong monoidal structure of F. This is the state that $(Ff_1, \dots, Ff_n)$ transforms to the one induced by $F(s)$. Let us now show that this transformation is secure provided that $\bar{f}$ is.

The heart of the argument is already apparent in the case of $n = 2$, so let us first show that if (f_A, f_B) is secure against a malicious Bob, so is (Ff_A, Ff_B). For this attack model, there is an initial attack, and the corresponding security constraint is depicted in Figure 2c. Then security of (Ff_A, Ff_B) can be shown graphically using the functorial boxes of [Mel06] by considering the equations



where the second equation is security of the original protocol and the other two equations rely on F being strong monoidal. The case of an arbitrary n can be shown similarly by drawing a similar picture with $n - 1$ dips in the box. □

For instance, if the inclusion of classical interactive computations into quantum ones is strong monoidal, i.e., respects sequential and parallel composition (up to isomorphism), then unconditionally secure classical protocols are also secure in the quantum setting, as shown in the context of UC-security in [Unr10, Theorem 15]. More generally, this result implies that the construction of the category of n-partite transformations secure against any fixed subset of $[n]$ is functorial in $\mathbf{C}$, and this is in fact also true for any family of subsets of $[n]$ by Corollary 4.5.

5. Further extensions of the framework

5.1. **Approximately correct transformations.** The discussion above has been focused on perfect security, so that the equations defining security hold exactly. This is often too high a standard for security to hope for, and consequently cryptographers routinely work with computational or approximate security. We model this in two ways. The first approach replaces equations with an equivalence relation abstracting from the idea that the end results are "computationally indistinguishable" rather than strictly equal. The latter approach amounts to working in terms of a (pseudo)metric, that quantifies how close we are to the ideal resource, so that one can discuss approximately correct transformations or sequences of transformations that succeed in the limit. The first approach is mathematically straightforward and we discuss it next, while the second approach takes the rest of this section. The second approach, while mathematically more involved, is needed to model protocols that are "close enough" to being computationally indistinguishable from the ideal, and thus to model statements in finite-key cryptography [TLGR12].

Replacing strict equations with equivalence relations is easy to describe on an abstract level as an instance of the theory so far: one just assumes that $\mathbf{C}$ has a monoidal congruence $\approx$ and then works with the resource theory induced by $\mathbf{C}^n \to \mathbf{C}/{\approx} \xrightarrow{\hom(I,-)} \mathbf{Set}$ with similar attack models as above. More explicitly, as long as each hom-set of $\mathbf{C}$ is equipped with an equivalence relation $\approx$ that respects $\otimes$ and $\circ$ in that $f \approx f'$ and $g \approx g'$ imply $gf \approx g'f'$ (whenever defined) and $g \otimes f \approx g' \otimes f'$, then working with $\mathbf{C}^n \to \mathbf{C}/{\approx} \xrightarrow{\hom(I,-)} \mathbf{Set}$ results in security conditions that replace $=$ in $\mathbf{C}$ with $\approx$ throughout. If $\mathbf{C}$ describes (interactive) computational processes and $\approx$ represents computational indistinguishability (inability for any "efficient" process to distinguish between the two), one might need to replace $\mathbf{C}$ (and consequently functionalities, protocols and attacks on them) with the subcategory of $\mathbf{C}$ of efficient processes so that $\approx$ indeed results in a congruence.

We now move to the metric case. If for each A the set of resources $R(A)$ associated to it is not just a set but has the structure of a metric space, using this additional structure enables one to construct other resource theories where instead of transforming $r \in R(A)$ to $s \in R(B)$ exactly we are happy to be able to get (arbitrarily) close. While such approximate (or asymptotic) conversions are readily studied in the physics literature (see e.g. [CG19, V.A and V.B]), as far as we are aware this has not been formalized in the categorical context, so we first describe the situation without security constraints. As many interesting measures of distance in cryptography are in fact pseudometrics (non-equal functionalities might have distance 0), we work in a more general setting.

Definition 5.1. An *extended pseudometric space* is a pair (X, d) where X is a set and $d\colon X \times X \to [0, \infty]$ is a function satisfying (i) $d(x, x) = 0$, (ii) $d(x, y) = d(y, x)$ and (iii) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x, y, z \in X$. A *short map* $(X, d) \to (Y, e)$ is a function $f\colon X \to Y$ satisfying $d(x, y) \geq e(f(x), f(y))$. We will denote the category of extended pseudometric spaces and short maps simply by $\mathbf{Met}$. We equip $\mathbf{Met}$ with a monoidal structure where $(X, d) \otimes (Y, e)$ is given by equipping $X \times Y$ with ℓ^1-distance, i.e., the distance between (x, y) and (x', y') is given by $d(x, x') + e(y, y')$.

Let $R\colon \mathbf{C} \to \mathbf{Met}$ be a symmetric monoidal functor. Given $r \in R(A)$, $s \in R(B)$ and $\epsilon > 0$, a morphism $f\colon A \to B$ is an *ϵ-correct transformation* $(A, r) \to (B, s)$ if $d(R(f)r, s) < \epsilon$. The resource theory $\int^{\mathbf{Met}} R$ of *asymptotically correct conversions* is defined as follows: an object is given by a pair (A, r) where A is an object of $\mathbf{C}$ and $r \in R(A)$. A morphism $(A, r) \to (B, s)$ is given by a sequence $(f_n)_{n \in \mathbb{N}}$ of maps $A \to B$ in $\mathbf{C}$ that is eventually ϵ-correct for any $\epsilon > 0$, i.e., for which $R(f_n)r \to s$ as $n \to \infty$.

In some resource theories, the relevant asymptotic transformations are allowed to use more and more copies of the resource, so that instead of a sequence of maps $A \to B$ we have a sequence $(f_n)_{n \in \mathbb{N}}$ of maps $A^{\otimes n} \to B$ taking $r^{\otimes n}$ to s in the limit. The theory developed here adapts easily to this variant as well, with essentially the same proofs.

Lemma 5.2. *Let $R\colon \mathbf{C} \to \mathbf{Met}$ be symmetric monoidal. The composite or tensor product of an ϵ-correct map with an ϵ'-correct map is $\epsilon + \epsilon'$-correct.*

Proof. Assume that f is an ϵ-correct transformation $(A,r) \to (B,s)$ and that g is an ϵ'-correct transformation $(B,s) \to (C,t)$. As $R(g)$ is a short map, this gives $d(R(gf)r, s) \leq d(R(gf)r, R(g)s) + d(R(g)s, t) < \epsilon + \epsilon'$.

Assume now that $f : (A,r) \to (B,s)$ is ϵ-correct and that $g\colon (C,t) \to (D,u)$ is ϵ'-correct. Then $d(R(f \otimes g)r \otimes t, s \otimes u) \leq d((R(f)s, R(g)t), (s,u)) = d(R(f)r, s) + d(R(g)t, u) < \epsilon + \epsilon'$. □

Theorem 5.3. *The resource theory* $\int^{\mathbf{Met}} R$ *of asymptotically correct conversions induced by* $R\colon \mathbf{C} \to \mathbf{Met}$ *is a symmetric monoidal category.*

Proof. The coherence isomorphisms are given by constant sequences of coherence isomorphisms of the resource theory induced by $\mathbf{C} \xrightarrow{R} \mathbf{Met} \to \mathbf{Set}$, and this implies that they satisfy the required equations of an SMC. Moreover, as they are exact resource conversions, they are also asymptotically correct. Thus it suffices to check that asymptotically correct conversions are closed under $\circ$ and $\otimes$. But this follows from Lemma 5.2: given two asymptotically correct transformations and $\epsilon > 0$, the two transformations are eventually $\epsilon/2$-correct after which their composite (whether $\circ$ or $\otimes$) is ϵ-correct. □

In particular, if $\mathbf{C}$ is $\mathbf{Met}$-enriched, the functor $\hom(I, -)$ lands in $\mathbf{Met}$ so that one can discuss asymptotic transformations between states.

While in resource theories one first tries to understand whether a given transformation is possible at all, once some resource conversion has been shown to be possible one might ask for more. In particular, in the asymptotic setting one might want the sequence $(f_n)_{n\in\mathbb{N}}$ to be efficient (and in particular computable) in n, and to converge to the target fast in terms of some measure of cost of implementing f_n. One might even want to be able to give an explicit bound on the distance between $R(f_n)r$ and s, as is done for instance in finite-key cryptography [TLGR12]. However, such considerations are best addressed when working inside a specific resource theory rather than being hardwired into the definitions at the abstract level. Conversely, if one can show that a given asymptotic transformation is impossible even for such a permissive notion of transformation, the resulting no-go theorem is stronger than if one worked with "efficient" sequences.

5.2. **Computational security.** We now show that one can reason composably about computational security in such a metric setting. The proofs follow rather straightforwardly from the definitions we have by using the structure at hand: most importantly, from the triangle inequality of any metric space and the fact that our maps between metric spaces are contractive. For concrete models of cryptography, one might need to do nontrivial work to show that one has all this structure, after which our theorems apply.

Definition 5.4. Consider $F\colon \mathbf{D} \to \mathbf{C}$ and $R\colon \mathbf{C} \to \mathbf{Met}$ and an attack model $\mathcal{A}$ on $\mathbf{C}$. For an $\epsilon > 0$ and an ϵ-correct map $(A,r) \to (B,s)$, we say that f is an *ϵ-secure transformation* $(A,r) \to (B,s)$ against $\mathcal{A}$ 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 $d(R(f')r, R(b)s) < \epsilon$.

Let $(f_n)_{n\in\mathbb{N}}\colon (A,r) \to (B,s)$ now define an asymptotically correct conversion in $\int^{\mathbf{Met}} RF$. We say that $(f)_{n\in\mathbb{N}}$ is *asymptotically secure* against $\mathcal{A}$ (or asymptotically $\mathcal{A}$-secure) if it is eventually ϵ-secure for any $\epsilon > 0$. Explicitly, $(f_n)_{n\in\mathbb{N}}\colon (A,r) \to (B,s)$ is asymptotically secure if for any $\epsilon > 0$ there is a threshold $k \in \mathbb{N}$ such that for any $n > k$ and any $f' \in \mathcal{A}(F(f_n))$ with $\mathrm{dom}(f') = F(A)$ there is $b \in \mathcal{A}(\mathrm{id}_{F(B)})$ such that $d(R(f')r, R(b)s) < \epsilon$.

We now show that bounds on security compose additively.

Lemma 5.5. *Let $R\colon \mathbf{C} \to \mathbf{Met}$ be lax monoidal and $\mathcal{A}$ an attack model on $\mathbf{C}$. The composite or tensor product of an ϵ-secure map with an ϵ'-secure map is $\epsilon + \epsilon'$-secure.*

Proof. We have already seen that ϵ-correctness behaves as desired in Lemma 5.2. Assume that f is an ϵ-secure transformation $(A, r) \to (B, t)$ and that g is an ϵ'-secure transformation $(B, s) \to (C, t)$ against $\mathcal{A}$. Given $h \in \mathcal{A}(g \circ f)$ with domain A, factorize it as $g' \circ f'$ as guaranteed by (ii). As f is $\mathcal{A}$-secure there is some $s \in \mathcal{A}(\mathrm{id}_B)$ with $d(R(f')r, R(b)s) < \epsilon$. Now $g'b \in \mathcal{A}(g)$ by (ii) so that security of g implies the existence of $c \in \mathcal{A}(\mathrm{id}_B)$ such that $d(R(g'b)(s), R(c)t) < \epsilon'$. Thus

$$d(R(g'f')t, R(c)t) \leq d(R(g'f')t, R(g')R(b)s) + d(R(g')R(b)s, R(c)t) < \epsilon + \epsilon'$$

as desired.

Assume now that f is ϵ-secure transformation $(A, r) \to (B, t)$ against $\mathcal{A}$ and that g is ϵ'-secure transformation $(C, t) \to (D, u)$ against $\mathcal{A}$. Given $h \in \mathcal{A}(f \otimes g)$ with domain $A \otimes C$ factorize it as $h' \circ (f' \circ g')$ as guaranteed by (iii). Then ϵ-security of f (ϵ'-security of g) gives us $b \in \mathcal{A}(\mathrm{id}_B)$ so that $d(R(f')r, R(b)s) < \epsilon$ ($d \in \mathcal{A}(\mathrm{id}_D)$ so that $d(R(g')t, R(d)u) < \epsilon'$). Now

$$\begin{aligned} &d(R(h') \circ R(f' \otimes g')(r \otimes t), R(h') \circ (R(b) \otimes R(d))(s \otimes u)) \\ &\quad \leq d(R(f' \otimes g')(r \otimes t), (R(b) \otimes R(d))(s \otimes u)) \\ &\quad = d(R(f')r, R(b)s) + d(R(g')t, R(d)u) < \epsilon + \epsilon' \end{aligned}$$

as desired. □

We now give a composition theorem for asymptotically secure protocols.

Theorem 5.6. *Given symmetric monoidal functors $F\colon \mathbf{D} \to \mathbf{C}$, $R\colon \mathbf{C} \to \mathbf{Set}$ with F strong monoidal and R lax monoidal, and an attack model $\mathcal{A}$ on $\mathbf{C}$, the class of asymptotically $\mathcal{A}$-secure maps forms a wide sub-SMC of the asymptotic resource theory $\int^{\mathbf{Met}} RF$ induced by F and R.*

Proof. As with Theorem 4.4, it suffices to show that asymptotically secure maps contain all coherence isomorphisms and are closed under $\circ$ and $\otimes$. Moreover, the reduction from the general case to $F = \mathrm{id}$ is the same, so we assume that $F = \mathrm{id}$. It is easy to see that whenever f is $\mathcal{A}$-secure in the resource theory induced by $\mathbf{C} \xrightarrow{R} \mathbf{Met} \to \mathbf{Set}$, the constant sequence $(f)_{n\in\mathbb{N}}$ is asymptotically $\mathcal{A}$-secure. Thus security of coherence isomorphisms implies their asymptotic security.

Assume now that $(f_n)_{n\in\mathbb{N}}\colon (A, r) \to (B, s)$ and $(g_n)_{n\in\mathbb{N}}\colon (B, s) \to (C, t)$ are asymptotically $\mathcal{A}$-secure. Given $\epsilon > 0$, for sufficiently large n both f_n and g_n are $\epsilon/2$-secure so that their composite is ϵ-secure by Lemma 5.5. The case for $\otimes$ follows similarly from Lemma 5.5. □

Corollary 5.7. *Given a non-empty family of functors $(\mathbf{D} \xrightarrow{F_i} \mathbf{C_i} \xrightarrow{R_i} \mathbf{Met})_{i\in I}$ with $R := R_iF_i = R_jF_j$ for all $i, j \in I$ and attack models $\mathcal{A}_i$ on $\mathbf{C}_i$ for each i, the class of maps in $\int^{\mathbf{Met}} R$ that is asymptotically secure against each $\mathcal{A}_i$ is a sub-SMC of $\int^{\mathbf{Met}} R$.*

To make these abstract results closer to cryptographic practice, one would work within some explicit $\mathbf{C}$ and with (pseudo)metrics relevant for cryptographers. A paradigmatic case is given by metrics induced by distinguisher advantage, where one defines the distance between two behaviors by first taking the supremum over all (efficient) distinguishers d of the probability of d distinguishing the two behaviors and then normalizing this value from $[1/2, 1]$

to $[0,1]$. If our starting category $\mathbf{C}$ contains processes that are not (efficiently) computable, such distinguisher metrics might not be contractive as composing two distinct behaviors with a very powerful behavior might help a distinguisher trying to tell them apart. However, as long as one restricts $\mathbf{C}$ (and consequently the behaviors available as resources, protocols and attacks) to behaviors that the relevant class of distinguishers can freely implement, this readily results in a **Met**-enrichment, as composing two morphisms with a fixed morphism available to the distinguishers cannot increase distinguisher advantage. For instance, if the metric is induced by distinguisher advantage of polynomial-time distinguishers, one should get a **Met**-enrichment on the subcategory of $\mathbf{C}$ corresponding to polynomial-time behaviors. Once one has specified a concrete $\mathbf{C}$ and a **Met**-enrichment on it, for any asymptotically secure protocol one can then discuss its speed of convergence, and in principle discuss which actual value of the security parameter is sufficiently secure for the task at hand.

We now wish to prove a variant of Theorem 4.8 in the approximate setting, abstracting from [Unr10, Theorem 18]. Again, we specialize to the n-partite resource theory of states, where our attack models consist of some subset $J \subset \{1, \ldots, n\}$ behaving maliciously. In this case, we assume our base categories to be **Met**-enriched, so that $\hom(I, -)$ lands in **Met**. In such a setting, a protocol is a sequence $(\bar{f}_i)_{i\in\mathbb{N}}$ where each $\bar{f}_i := (f_{i,1}, \ldots f_{i,n})$ is an n-tuple of morphisms.

Theorem 5.8. *Let* $\mathbf{C}$ *and* $\mathbf{D}$ *be* **Met***-enriched SMCs, and let* $F\colon \mathbf{C} \to \mathbf{D}$ *be a strong monoidal* **Met***-enriched functor. If* $(\bar{f}_i)_{i\in\mathbb{N}}$ *is an asymptotic transformation between two states of* $\mathbf{C}$ *that is asymptotically secure against* $J \subset \{1, \ldots, n\}$*, so is* $(F\bar{f}_i)_{i\in\mathbb{N}}$.

Proof. Again, it suffices to prove security against initial attacks. Now, the proof of Theorem 4.8 implies that if the desired equation in $\mathbf{C}$ holds up to $\epsilon > 0$, so does the equation in $\mathbf{D}$, so the claim follows. □

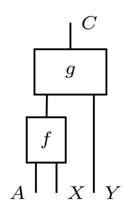
As discussed in [Unr10], the computational version above is not as strong as the result in the case of perfect security, as the assumptions of Theorem 5.8 are rather strong. For instance, if a protocol is secure against polynomial-time classical adversaries, it does not follow that it is secure against polynomial-time quantum adversaries. Correspondingly, if we use the metric induced by "polynomial-time distinguishers", the inclusion of classical computations into quantum computations is not **Met**-enriched, as the distances might increase. However, if on the quantum side we use polynomial-time distinguishers, but on the classical side we use distinguishers that are able to simulate quantum polynomial-time machines, then protocols that are classically secure remain secure when thought of as quantum computations.

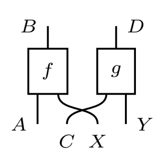
5.3. **Setup assumptions and freely usable resources.** Cryptographers often prove results saying that a given functionality is impossible to realize in the *plain* model but is possible with some *setup*. For instance, in [CF01] they show that bit commitment (BC) is impossible in the plain UC-framework but it is possible assuming a common reference string (CRS)—a functionality that gives all parties the same string drawn from some fixed distribution. In our viewpoint, claims such as these can be interpreted in the categories we have already built: for instance, impossibility of commitments amounts to non-existence of a secure map $I \to BC$ that builds bit commitments out of a trivial resource I, and possibility of bit commitments given a common reference string amounts to the existence of a secure protocol $CRS \to BC$.

A related, but distinct matter is that sometimes cryptographers wish to make some (possibly shared) functionalities freely available to all parties without having to explicitly mention them being used as a resource. For instance, so far in our framework all communication between the honest parties has been mediated by the functionality r that they start from. However, one might want to model situations where e.g. pairwise communication between parties is freely available (as is standard in multi-party computation) and does not need to be provided explicitly by the functionality one starts from. Put more abstractly, one might wish to declare some set $\mathcal{X}$ of functionalities "free" and think of secure protocols that build s from r and some functionalities from $\mathcal{X}$ just as maps $r \to s$, without having to explicitly keep track of how many copies of which $x \in \mathcal{X}$ was used. This is in fact something that happens quite often in resource theories even before any security conditions arise, as it could happen that the free processes $\mathbf{C}_F$ are not quite expressive enough for the resource theory at hand. While one could try to define a larger category of free processes directly, it might be technically more convenient to obtain a larger class of free processes by allowing resource transformations to consume a resource from some class that is considered free. This can be achieved via a general construction on SMCs, a special case used in [FST19] when constructing the category of learners. A special case also appears in the resource theory of contextuality as defined in [ABKM19], where one first defines deterministic free processes, and probabilistic (but classical) transformations $d \to e$ are then defined as transformations $d \otimes c \to e$ where c is a non-contextual (and thus free) resource. This construction is discussed more generally in [Gav19, CGG$^+$21], but we modify it slightly by allowing one to choose a class of objects as "parameters" instead of taking that class to consist of all objects: this modification is important for resource theories as it lets one control which resources are made freely available.

Proposition 5.9. *Let $\mathbf{C}$ be an SMC and $\mathcal{X}$ a class of objects that contains I and is closed under $\otimes$. Then there is an SMC whose objects are those of $\mathbf{C}$, and whose morphisms $A \to B$ are given by equivalence classes of morphisms $A \otimes X \to B$ in $\mathbf{C}$ with $X \in \mathcal{X}$, where $f \colon A \otimes X \to B, f' \colon A \otimes X' \to B$ are equivalent if there is an isomorphism $g \colon X \to X'$ such that $f = f' \circ (\mathrm{id}_A \otimes g)$*

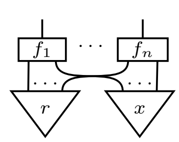
Sketch. The composites $g \circ f$ and $g \otimes f$ are depicted by





It is easy to show graphically that these are well-defined and that this results in an SMC. □

Using Proposition 5.9 we can easily model protocols that have free access to some cryptographic functionalities: one just declares a class $\mathcal{X}$ of functionalities (e.g. pairwise communication channels) that is closed under $\otimes$ to be free. In that case a protocol acting on $(A_{i=1}^n, r)$ can be depicted by



(A) The copy map (B) Alice's copy map (C) Alice broadcasting to Bob and Eve (D) Random shared key

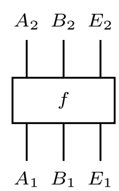
FIGURE 3. Variants of the copy map

where $x \in \mathcal{X}$ is a free resource.

6. THE ONE-TIME PAD

We will now explore how the one-time pad (OTP) fits into our framework, paralleling the discussion of OTP in [Mau11]. We will start from the category **FinStoch** of finite sets and stochastic maps between them, with $\otimes$ given by cartesian product of sets. This is sufficient for OTP, even if more complicated and interactive cryptographic protocols will need a different starting category. However, the actual category **C** we work in is built from **FinStoch**, essentially by a tripartite variant of the "resource theory of universally-combinable processes" of [CFS16, Section 3.4]. We will defer the detailed construction of **C** and work in it more heuristically, allowing us to focus first on the OTP itself.

Roughly speaking, a "basic object" of **C** consists of finite sets A_i,B_i, E_i for $i = 1, 2$, and of a map $f\colon A_1 \otimes B_1 \otimes E_1 \to A_2 \otimes B_2 \otimes E_2$ in **FinStoch**, depicted by

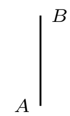


The intuition is that $\langle (A_i, B_i, E_i)_{i\in\{1,2\}}, f\rangle$ represents a box shared by Alice, Bob and Eve, with Alice's inputs and outputs ranging over A_1 and A_2 respectively, and similarly for Bob and Eve. We will often label the ports just by the party who accesses it, and omit labeling trivial ports. For example, if Figure 3a depicts the copy map $X \to X \otimes X$ for some set X in **FinStoch**, then Figure 3b denotes an object of **C** representing Alice copying data in X privately, whereas Figure 3c denotes an object **C** that sends Alice's input unchanged to Bob and to Eve—which we view as an insecure (but authenticated) channel from Alice to Bob.

A general object of **C** then consists of a list of such basic objects, representing a list of such resources shared between Alice, Bob and Eve. A morphism of **C** is roughly speaking a way of using the starting resources and local computation by the three parties to produce the target resources: we will give a more formal definition after we conclude the example. In our attack model Alice and Bob are honest but Eve is dishonest, so she might do arbitrary local computation instead of whatever our protocols might prescribe.

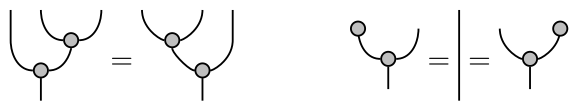
In the version of the one-time pad we discuss, our starting resources consist of an insecure but authenticated channel[4] from Alice to Bob as in Figure 3c and of a random key

[4]If the insecure channel allows Eve to tamper with the message, the analysis changes, as the resulting channel still lets Eve flip bits in the sent message, even if she cannot read the message. Consequently, one can study the OTP with a different domain and codomain than chosen here, corresponding.

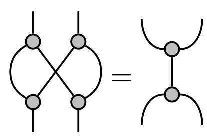
over the same message space, shared by Alice and Bob, depicted in Figure 3d. Here Alice and Bob having access to both of these resources is modelled by them sharing the monoidal product of these resources. The goal is to build a secure channel  from Alice to Bob from these.

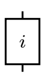
We will next describe the local ingredients needed for OTP. First of all, Alice and Bob must agree on a group structure on the message space: this consists of a multiplication  with unit  that is associative and unital, i.e., satisfies the equations

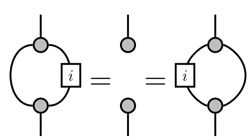
Note that copying and deleting satisfy similar equations



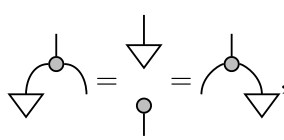
In addition, multiplication and copying interact:



and the map  giving inverses[5] satisfies



That the key is uniformly random is captured by

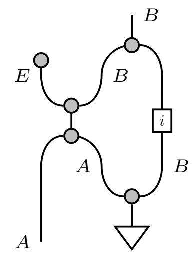


which amounts to saying that "adding uniform noise to a channel results in uniform noise".

Taken together, the equations describe a known as a Hopf algebra with an integral [Swe69] in a symmetric monoidal category. Any finite group gives rise to such a structure in **FinStoch**, with the integral given by the uniform distribution. Concretely, this means that Alice and Bob must agree on a group structure on the message space, and the fact that this multiplication forms a group and that the key is random can be captured by these equations.

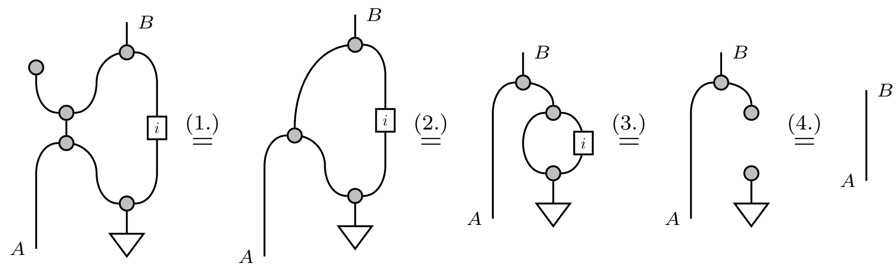
[5]usually in OTP, one works over a power of $\mathbb{Z}_2$ so that i is given by the identity map

The OTP protocol is then depicted as follows:



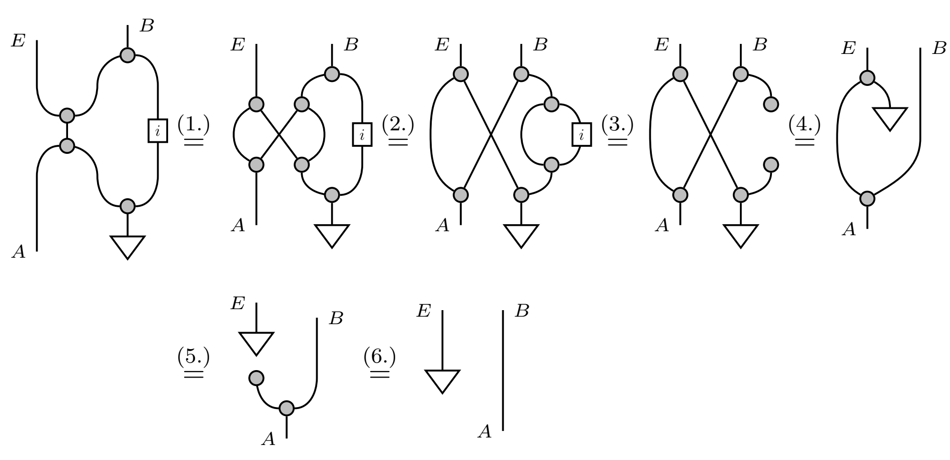
i.e., Alice adds the key to her message, broadcasts it to Eve and Bob. Eve deletes her part and Bob adds the inverse of the key to the ciphertext to recover the message.

That the protocol is correct (i.e., works when everyone follows it) can be proven as follows:



Here the first equation uses the counit law, the second one uses associativity, the third one uses inverses and the final one follows form unitality.

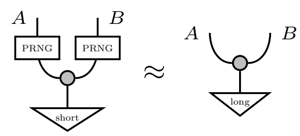
However, we also need to show that the protocol is secure. In this case, Eve has an initial attack given by just reading the ciphertext. We can now prove security pictorially as follows:



The first equation is the interaction between multiplication and copying, the second uses (co)associativity, the third one properties of inverses, the fourth and last one use unitality, and the fifth one follows from the key being random. Taken together, these show that Eve's initial attack is equal to her just producing a random message herself when Alice and Bob share the target resource.

Thus OTP represents a map shared key $\otimes$ authenticated channel $\to$ secure channel in $\mathbf{C}$, that is secure against Eve.

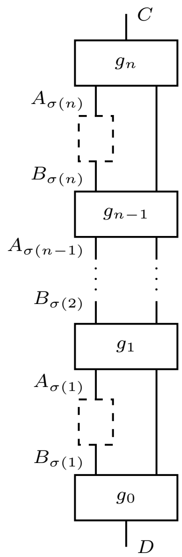
We now use this example to illustrate the use of the composition theorems as in [Mau11]. A major drawback of OTP, despite its perfect security, is the fact that one needs a key that is as long as the message. In practice, Alice and Bob might only share a short key and wish to promote it a long key. If they agree on a pseudo-random number generator (PRNG) with their key as the seed, they can map the short key to a longer key. If the PRNG is computationally secure, then the end-result is (computationally) indistinguishable from a long key, depicted by



where $\approx$ stands for computational indistinguishability. We envision the computational security of the chosen PRNG to be proven "the usual way" (starting from complexity-theoretic assumptions e.g., as in), and not graphically—after all, we believe that our framework is there to supplement ordinary cryptographic reasoning and not to replace it. Alternatively, one simply assumes the existence of a computationally secure PRNG. Either way, the PRNG then results in a (computationally) secure way of promoting a short shared key into a long shared key, and then the composition theorems guarantee that these protocols can be composed, resulting in the security of the stream cipher.

We now explain how the category we described informally when discussing OTP fits our framework. We begin with a simpler case lacking the tripartite structure. We will also see how the "resource theory of universally-combinable processes" of [CFS16, Section 3.4] arises as a Grothendieck construction.

Definition 6.1. Given an SMC $\mathbf{C}$, the category n-comb($\mathbf{C}$) is defined as follows: objects of n-comb($\mathbf{C}$) are lists $(A_i, B_i)_{i=1}^n$ of pairs of objects of $\mathbf{C}$. Morphisms are defined in two stages: A morphism $(A_i, B_i)_{i=1}^n \to (C, D)$ is given by permutation $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ and an n-comb[6]



in $\mathbf{C}$. A morphism $(A_i, B_i)_{i=1}^n \to (C_j, D_j)_{j=1}^m$ is given by a function $f\colon \{1, \dots, n\} \to \{1, \dots, m\}$ and a morphism $(A_i, B_i)_{i \in f^{-1}(j)} \to (C_j, D_j)$ for each j. Composition is defined by plugging circuits in to circuits, and the monoidal product is given by concatenation of lists.

The tensor unit of n-comb($\mathbf{C}$) is given by the empty sequence, and a state of type (A, B) is just a morphism $A \to B$ in $\mathbf{C}$. Thus a state of type $(A_i, B_i)_{i=1}^n$ consists of a list of morphisms $(f_i\colon A_i \to B_i)_{i=1}^n$ in $\mathbf{C}$. The resource theory induced by n-comb($\mathbf{C}$) $\xrightarrow{\hom(I,-)}$ $\mathbf{Set}$ is the "resource theory of universally-combinable processes" of [CFS16, Section 3.4] and is almost the one we were working in, except that it lacks the tripartite structure on resources and on protocols. The tripartite structure is then obtained by noticing that the trifold tensor product $\mathbf{C}^3 \to \mathbf{C}$ of $\mathbf{C}$ induces a monoidal functor n-comb($\mathbf{C}^3$) $\to$ n-comb($\mathbf{C}$). We obtain the category described informally in the above, by setting $\mathbf{C} = \mathbf{FinStoch}$ and then taking the resource theory induced by n-comb($\mathbf{C}^3$) $\to$ n-comb($\mathbf{C}$) $\xrightarrow{\hom(I,-)}$ $\mathbf{Set}$. One readily verifies that the attack model on $\mathbf{C}^3$ given by honest Alice and Bob and malicious Eve induces an attack model on n-comb($\mathbf{C}^3$).

7. No-go results

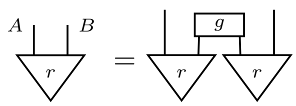
Composable security is a stronger constraint than stand-alone security, and indeed many cryptographic functionalities are known to be impossible to achieve "in the plain model", i.e., without set-up assumptions. A case in point is bit commitment, which was shown to be impossible in the UC-framework in [CF01]. This result was later generalized in [PR08] to show that any two-party functionality that can be realized in the plain UC-framework is "splittable". While the authors of [PR08] remark that their result applies more generally than

[6]For other purposes it might be preferable to work with equivalence classes of such n-combs, but it does not affect questions of resource convertibility so we ignore the issue here.

just to the UC-framework, this wasn't made precise until [MR11][7]. We present a categorical proof of this result in our framework, which promotes the pictures "illustrating the proof" in [PR08] into a full proof—the main difference is that in [PR08] the pictures explicitly keep track of an environment trying to distinguish between different functionalities, whereas we prove our result in the case of perfect security and then deduce the asymptotic claim.

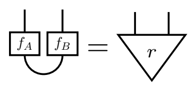
We now assume that $\mathbf{C}$, our ambient category of interactive computations is compact closed[8]. As we are in the 2-party setting, we take our free computations to be given by $\mathbf{C}^2$, and we consider two attack models: one where Alice cheats and Bob is honest, and one where Bob cheats and Alice is honest. We think of $\cup$ as representing a two-way communication channel, but this interpretation is not needed for the formal result.

Theorem 7.1. *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 is a g such that*

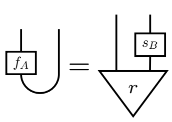


(∗)

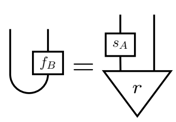
Proof. A secure protocol transforming $\cup$ to r consists of maps f_A, f_B satisfying



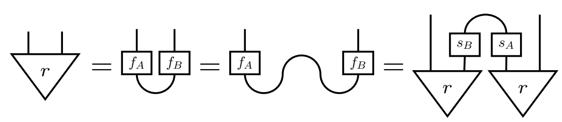
and the security constraints against attacks by Alice or Bob. In particular, security against Alice's and Bob's initial attacks give us s_A and s_B such that



and



so that



∎

We now wish to use this result to rule out functionalities that do not satisfy this equation for any g. Notable examples of this include bit commitment, which lets Alice commit to a bit that will be revealed to Bob later, and oblivious transfer, which lets Alice choose two bits, of which Bob can choose to learn exactly one, with Alice not learning Bob's choice.

Corollary 7.2. *Given a compact closed $\mathbf{C}$ modeling computation in which wires model communication channels, (composable) bit commitment and oblivious transfer are impossible in that model without setup, even asymptotically in terms of distinguisher advantage.*

Proof. If r represents bit commitment from Alice to Bob, it does not satisfy the equation required by Theorem 7.1 for any g, and the two sides of $(*)$ can be distinguished efficiently with at least probability $1/2$. Indeed, take any f and let us compare the two sides of $(*)$: if the distinguisher commits to a random bit b, then Bob gets a notification of this on the left hand-side, so that f has to commit to a bit on the right side of $(*)$ to avoid being

[7] Except that in their framework the 2-party case seems to require security constraints also when both parties cheat.

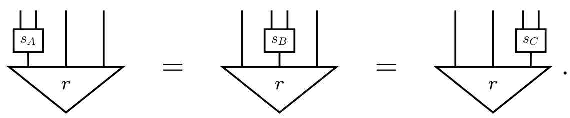
[8] We do not view this as overtly restrictive, as many theoretical models of concurrent interactive (probabilistic/quantum) computation are compact closed [Win13, CDVW19b, CdVW19a].

distinguished from the left side. But this bit coincides with b with probability at most $1/2$, so that the difference becomes apparent at the reveal stage. The case of OT is similar. □

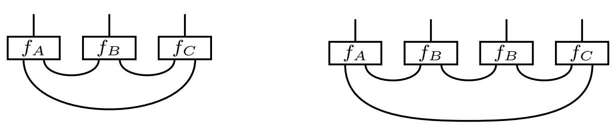
We now discuss a similar result in the tripartite case, which rules out building a broadcasting channel from pairwise channels securely against any single party cheating. In [MMP+18] comparable pictures are used to illustrate the official, symbolically rather involved, proof, whereas in our framework the pictures are the proof. Another key difference is that [MMP+18] rules out broadcasting directly, whereas we show that any tripartite functionality realizable from pairwise channels satisfies some equations, and then use these equations to rule out broadcasting.

Formally, we are working with the resource theory given by $\mathbf{C}^3 \xrightarrow{\otimes} \mathbf{C} \xrightarrow{\hom(I,-)} \mathbf{Set}$ where $\mathbf{C}$ is an SMC, and reason about protocols that are secure against three kinds of attacks: one for each party behaving dishonestly while the rest obey the protocol. Note that we do not need to assume compact closure for this result, and the result goes through for any state on $A \otimes A$ shared between each pair of parties: we will denote such a state by $\cup$ by convention.

Theorem 7.3. *If a tripartite functionality r can be realized from each pair of parties sharing a state $\cup$, securely against any single party, then there are simulators s_A, s_B, s_C such that*



Proof. Any tripartite protocol building on top of each pair of parties sharing $\cup$ can be drawn as in the left side of



Consider now the morphism in $\mathbf{C}$ depicted on the right: it can be seen as the result of three different attacks on the protocol (f_A, f_B, f_C) in $\mathbf{C}^3$: one where Alice cheats and performs f_A and f_B (and the wire connecting them), one where Bob performs f_B twice, and one where Charlie performs f_B and f_C. The security of (f_A, f_B, f_C) against each of these gives the required simulators. □

Corollary 7.4. *Given an SMC $\mathbf{C}$ modeling interactive computation, and a state $\cup$ on $A \otimes A$ modeling pairwise communication, it is impossible to build broadcasting channels securely (even asymptotically in terms of distinguisher advantage) from pairwise channels.*

Proof. We show that a channel r that enables Bob to broadcast an input bit to Alice and Charlie never satisfies the required equations for any s_A, s_B, s_C. Indeed, assume otherwise and let the environment plug "broadcast 0" and "broadcast 1" to the two wires in the middle. The leftmost picture then says that Charlie receives 1, the rightmost picture implies that Alice gets 0 and the middle picture that Alice and Bob get the same output (if anything at all)—a contradiction. Indeed, one cannot satisfy all of these simultaneously with high probability, which rules out an asymptotic transformation. □

8. On the choice of a model

In this section we will discuss the choice of a base category **C** in which to work in. As we believe that one of the advantages of the current framework is how it allows one to separate the concern for composability from the choice of a model of computation, we do not think that choosing or building suitable models **C** is central to the work at hand. Moreover, we do not believe that there is a single model suitable for all cryptographic purposes, as some assumptions that simplify the model mathematically might be justified for some tasks but not for others. Consequently, we will refer to the existing literature to explain where to find some models that are expressive enough for cryptography and result in an SMC, even when the original works are not expressed in categorical terms.

Let us first explain why choosing (let alone building) a starting category is not trivial. In general, the following desiderata pull in opposite directions

- The computational model should be mathematically tractable.
- the computational model should be sufficiently expressive. One should be able to model both cryptographic protocols and realistic attacks in the model. In particular, any adversarial behavior simply assumed away creates room for side-channel attacks.

To elaborate on the required expressiveness, cryptographically reasonable models of computation should have most of the following features:

- computation should be probabilistic (or quantum) as there's no security without randomness.
- in general, concurrent computation should be asynchronous: after all cryptography behaves differently in synchronous and asynchronous settings [BOCG93, KMTZ13] and we cannot assume synchronicity throughout
- cryptographic protocols need not have a fixed number of communication rounds, and might instead be repeated until a success condition occurs.

In particular, the requirement of asynchronous probabilistic computation causes some difficulties for modelling cryptography, as discussed in [MT13]. To paraphrase, the issue is that traditionally concurrency in asynchronous systems is modelled by nondeterminism, so that a system describes the set of all possible behaviors. Unfortunately, this does not work too well for cryptography, where one wants to bound the probability of a successful attack. Cryptographers often solve this by letting an adversary be responsible for scheduling. This is not always a reasonable assumption, and makes the resulting models inherently less compositional. However, one can still achieve categorical models that achieve most of these features, even if many existing models are not phrased categorically. Indeed, the aforementioned [MT13] builds a model of interactive, asynchronous probabilistic computation, where composition of computations is associative (resulting in a category), with the cartesian product of sets inducing a parallel composition operation (resulting in an SMC). The resulting framework is rich enough to study many cryptographic protocols such as broadcasting and secret sharing.

Another possible source of a model stems from cryptHOL [BLS20], an approach to formally verified cryptographic protocols using higher-order-logic. While [BLS20] does not give an explicit category of probabilistic and stateful computations, we expect it to induce one despite not having verified this in detail. We base our optimism on the fact that the monadic and coalgebraic techniques used in [BLS20] are inherently categorical. Moreover cryptHOL has also been used to formalize constructive cryptography [LSBM19], and as a consequence one would expect that the same model could be phrased in categorical terms. We leave verifying this for future work as it is outside the scope of this paper.

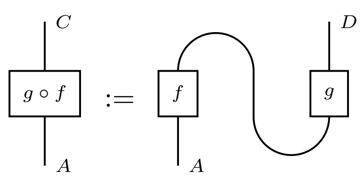
Additional models can be found in the literature on programming language theory, and particularly from game semantics [Win13]. While these models are more often expressed categorically, and even result in compact closed categories so that Theorem 7.1 applies directly, they run the risk of being too involved mathematically, at least in order to gain mainstream traction among cryptographers.

We now turn our attention to modelling quantum cryptography. Again, one can use models coming from game semantics [CDVW19b, CdVW19a] with the aforementioned caveats. Another model, this time built by and for quantum cryptographers, can be obtained from [PMM+17]. The model is rather general, as it is intended to be also suitable for relativistic quantum protocols, and indeed it has been used for such purposes in [VPDR19]. As the constructions are rather involved, we restrict ourselves to giving a high-level description. As [PMM+17] is not expressed in categorical words, we will explain why their model can equally well be interpreted as a category.

In this work, the authors work over a countable but otherwise arbitrary partial order T, and then define for each (finite-dimensional) Hilbert space A a new Hilbert-space $F(A)$ modelling a wire with A-messages being sent/received at times given by $t \in T$. They then define causal maps $A \to B$ as certain families of CPTP-maps $\{F(A) \to F(B)_C\}$ where C ranges over downward-closed subsets of T—the intuition being that for a causal map the output at time $t \in T$ depends only on the past of t with some delay. The authors then define two ways of combining causal boxes:

- parallel composition, which we will denote by $\otimes$, which takes causal boxes $A \to B$ and $C \to D$ and produces a causal box $A \otimes C \to B \otimes D$.
- An internal wiring operation, which takes as input a causal box $A \otimes B \to B \otimes C$, and produces a causal box $A \otimes C$. The intuition is that the resulting causal box is obtained by wiring the output B-wire into the the input B-wire.

Moreover, the authors prove that these composition operations satisfy "composition order invariance", so that adding loops commutes with parallel composition, and the order in which loops was added does not affect the end result. While the authors phrase their constructions in terms of the algebraic theory of systems of [MMP+18], the parallel composition operation they define is in fact a total operation, whereas in a system algebra $f \otimes f$ is never defined[MMP+18, Definition 3.1]. This allows us to extract a category from [PMM+17]. The objects of this category are given by (finite-dimensional) message spaces $A, B, C, \ldots$, and morphisms $A \to B$ are given by T-causal maps $A \to B$. The composite of $f\colon A \to B$ and $g\colon B \to C$ is given internally wiring the B-ports together in $g \otimes f$, pictorially represented by



Now, composition order invariance implies that this composition operation is associative. As identity-maps are *not* causal (informally this is because they're delay-free), this results only in a semicategory—i.e., a category-like structure without identities. However, we can formally add identities, resulting in a symmetric monoidal category.[9] Moreover, the authors equip these causal boxes with an explicit pseudometric. This pseudometric is a cryptographically well-motivated one, as the distance between f and g is defined in terms of the ability of an environment to guess whether it interacts with f or g. Consequently one can also apply the asymptotic definitions of Sections 5.1 and 5.2 in this category.

9. Outlook

We have presented a categorical framework providing a general, flexible and mathematically robust way of reasoning about composability in cryptography. Besides contributing a further approach to composable cryptography and potentially helping with cross-talk and comparisons between existing approaches [CKLS19], we believe that the current work opens the door for several further questions.

First, due to the generality of our approach we hope that one can, besides honest and malicious participants, reason about more refined kinds of adversaries composably. Indeed, we expect that Definition 4.1 is general enough to capture e.g. honest-but-curious adversaries[10]. It would also be interesting to see if this captures even more general attacks, e.g. situations where the sets of participants and dishonest parties can change during the protocol. This might require understanding our axiomatization of attack models more structurally and perhaps generalizing it. Does this structure (or a variant thereof) already arise in category theory? While we define an attack model on a category, perhaps one could define an attack model on a (strong) monoidal functor F, the current definition being recovered when $F = \mathrm{id}$.

Second, we expect that rephrasing cryptographic questions categorically would enable more cross-talk between cryptography and other fields already using category theory as an organizing principle. For instance, many existing approaches to composable cryptography develop their own models of concurrent, asynchronous, probabilistic and interactive computations. As categorical models of such computation exist in the context of game semantics [Win13, CDVW19b, CdVW19a], one is left wondering whether the models of the semanticists' could be used to study and answer cryptographic questions, or conversely if the models developed by cryptographers contain valuable insights for programming language semantics.

Besides working inside concrete models—which ultimately blends into "just doing composable cryptography"—one could study axiomatically how properties of a category relate to cryptographic properties in it. As a specific conjecture in this direction, if one has an environment structure [CP12], i.e., coherent families of maps $\dot{\top}_A$ for each A that axiomatize the idea of deleting a system, one might be able to talk about honest-but-curious adversaries at an abstract level. Similarly, having agents purify their actions is an important tool in quantum

[9] One might be tempted to guess that *any* model of abstract cryptography yields a category in an analogous manner. We make the more reserved but less precise guess that this holds for those models of abstract cryptography that are "reasonable" or arise "naturally". However, we don't think there exists a simple construction of an SMC directly from any (composition-order-invariant) system algebra in the sense of [MMP+18]: for one, in a system algebra $f \otimes f$ is never defined, whereas in a monoidal category $f \otimes f$ is always defined. Rather, we believe that natural sources of system algebras are also natural sources of SMCs.

[10] Heuristically speaking this is the case: an honest-but-curious attack on $g \circ f$ should be factorizable as one on g and one on f, and similarly an honest-but-curious attack on $g \otimes f$ should be factorizable into ones on g and f that then forward their transcripts to an attack on $\mathrm{id} \otimes \mathrm{id}$.

cryptography [LC97]—can categorical accounts of purification [CDP10, CH17, CP12] be used to elucidate this?

Finally, we hope to get more mileage out of the tools brought in with the categorical viewpoint. For instance, can one prove further no-go results pictorially? More specifically, given the impossibility results for two and three parties, one wonders if the "only topology matters" approach of string diagrams can be used to derive general impossibility results for n parties sharing pairwise channels. Similarly, while diagrammatic languages have been used to reason about positive cryptographic results in the stand-alone setting [KTW17, BMR19, BKM18], can one push such approaches further now that composable security definitions have a clear categorical meaning? Besides the graphical methods, thinking of cryptography as a resource theory suggests using resource-theoretic tools such as monotones. While monotones have already been applied in cryptography [WW08], a full understanding of cryptographically relevant monotones is still lacking.

References

[ABKM19] Samson Abramsky, Rui Soares Barbosa, Martti Karvonen, and Shane Mansfield. A comonadic view of simulation and quantum resources. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 2019. doi:10.1109/LICS.2019.8785677.

[Awo10] S. Awodey. *Category theory*. Oxford University Press, 2010.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BBB$^+$00] Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, and Vwani Roychowdhury. A proof of the security of quantum key distribution (extended abstract). In *32nd Annual ACM Symposium on Theory of Computing—STOC 2000*, pages 715 – 724, 2000. doi:10.1145/335305.335406.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *50th Annual Symposium on Foundations of Computer Science—FOCS 2009*, pages 517–526, 2009. doi:10.1109/FOCS.2009.36.

[BK22] Anne Broadbent and Martti Karvonen. Categorical composable cryptography. In *Foundations of Software Science and Computation Structures (FoSSaCS)*, volume 13242 of *Lecture Notes in Computer Science*, pages 161–183. Springer, 2022. doi:10.1007/978-3-030-99253-8_9.

[BKM18] Spencer Breiner, Amir Kalev, and Carl A. Miller. Parallel self-testing of the GHZ state with a proof by diagrams. In *Proceedings of QPL 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 43–66, 2018. doi:10.4204/eptcs.287.3.

[BLS20] David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar. CryptHOL: Game-Based Proofs in Higher-Order Logic. *Journal of Cryptology*, 33(2):494–566, January 2020. doi:10.1007/s00145-019-09341-z.

[BMR19] Spencer Breiner, Carl A. Miller, and Neil J. Ross. Graphical methods in device-independent quantum cryptography. *Quantum*, 3:146, 2019. doi:10.22331/q-2019-05-27-146.

[BOCG93] Michael Ben-Or, Ran Canetti, and Oded Goldreich. Asynchronous secure computation. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 52–61, 1993. doi:10.1145/167088.167109.

[BOHL$^+$05] Michael Ben-Or, Michał Horodecki, Debbie W Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *2nd Theory of Cryptography Conference—TCC 2005*, pages 386–406, 2005. doi:10.1007/978-3-540-30576-7_21.

[BOM04] Michael Ben-Or and Dominic Mayers. General security definition and composability for quantum & classical protocols, 2004. URL: https://arxiv.org/abs/quant-ph/0409062, arXiv:quant-ph/0409062.

[Bor94a] F. Borceux. *Handbook of Categorical Algebra 1: Basic Category Theory*. Cambridge University Press, 1994. doi:10.1017/cbo9780511525858.

[Bor94b] F. Borceux. *Handbook of Categorical Algebra 2: Categories and Structures*. Cambridge University Press, 1994. doi:10.1017/CBO9780511525865.

[BPW04] Michael Backes, Birgit Pfitzmann, and Michael Waidner. A general composition theorem for secure reactive systems. In *1st Theory of Cryptography Conference—TCC 2004*, pages 336–354, 2004. doi:10.1007/978-3-540-24638-1_19.

[BPW07] Michael Backes, Birgit Pfitzmann, and Michael Waidner. The reactive simulatability (RSIM) framework for asynchronous systems. *Information and Computation*, 205(12):1685–1720, 2007. doi:10.1016/j.ic.2007.05.002.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science—FOCS 2001*, pages 136–145, 2001. doi:10.1109/SFCS.2001.959888.

[CDP10] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Probabilistic theories with purification. *Physical Review A*, 81(6), June 2010. doi:10.1103/physreva.81.062348.

[CdVW19a] Pierre Clairambault, Marc de Visme, and Glynn Winskel. Concurrent quantum strategies. In *International Conference on Reversible Computation*, pages 3–19. Springer, 2019. doi:10.1007/978-3-030-21500-2_1.

[CDVW19b] Pierre Clairambault, Marc De Visme, and Glynn Winskel. Game semantics for quantum programming. *Proceedings of the ACM on Programming Languages*, 3(POPL):1–29, 2019. doi:10.1145/3290345.

[CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In *Advances in cryptology—CRYPTO 2001*, pages 19–40. Springer, 2001. doi:10.1007/3-540-44647-8_2.

[CFS16] Bob Coecke, Tobias Fritz, and Robert W Spekkens. A mathematical theory of resources. *Information and Computation*, 250:59–86, 2016. doi:10.1016/j.ic.2016.02.008.

[CG19] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2):025001, 2019. doi:10.1103/revmodphys.91.025001.

[CGG+21] GSH Cruttwell, Bruno Gavranović, Neil Ghani, Paul Wilson, and Fabio Zanasi. Categorical foundations of gradient-based learning, 2021. URL: https://arxiv.org/abs/2103.01931, arXiv:2103.01931.

[CH17] Oscar Cunningham and Chris Heunen. Purity through factorisation. In *Proceedings of QPL 2017*, volume 266 of *Electronic Proceedings in Theoretical Computer Science*, pages 315–328, 2017. doi:10.4204/EPTCS.266.20.

[CKLS19] Jan Camenisch, Ralf Küsters, Anna Lysyanskaya, and Alessandra Scafuro. Practical Yet Composably Secure Cryptographic Protocols (Dagstuhl Seminar 19042). *Dagstuhl Reports*, 9(1):88–103, 2019. doi:10.4230/DagRep.9.1.88.

[CLM+14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014. doi:10.1007/s00220-014-1953-9.

[CP10] Bob Coecke and Eric Oliver Paquette. Categories for the practising physicist. In *New Structures for Physics*, pages 173–286. Springer, 2010. doi:10.1007/978-3-642-12821-9_3.

[CP12] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. *Logical Methods in Computer Science*, Volume 8, Issue 4, 2012. doi:10.2168/LMCS-8(4:14)2012.

[CWW+11] Bob Coecke, Quanlong Wang, Baoshan Wang, Yongjun Wang, and Qiye Zhang. Graphical calculus for quantum key distribution (extended abstract). *Electronic Notes in Theoretical Computer Science*, 270(2):231–249, 2011. doi:10.1016/j.entcs.2011.01.034.

[DDMP03a] Anupam Datta, Ante Derek, John C Mitchell, and Dusko Pavlovic. A derivation system for security protocols and its logical formalization. In *16th IEEE Computer Security Foundations Workshop, 2003. Proceedings.*, pages 109–125. IEEE, 2003. doi:10.1109/csfw.2003.1212708.

[DDMP03b] Anupam Datta, Ante Derek, John C Mitchell, and Dusko Pavlovic. Secure protocol composition. *Electronic Notes in Theoretical Computer Science*, 83:201–226, 2003. doi:10.1016/s1571-0661(03)50011-1.

[DDMP05] Anupam Datta, Ante Derek, John C. Mitchell, and Dusko Pavlovic. A derivation system and compositional logic for security protocols. *Journal of Computer Security*, 13(3):423–482, August 2005. doi:10.3233/JCS-2005-13304.

[DDMR07] Anupam Datta, Ante Derek, John C. Mitchell, and Arnab Roy. Protocol composition logic (PCL). *Electronic Notes in Theoretical Computer Science*, 172:311–358, April 2007. doi:10.1016/j.entcs.2007.02.012.

[DMP01] N. Durgin, J. Mitchell, and D. Pavlovic. A compositional logic for protocol correctness. In *Proceedings. 14th IEEE Computer Security Foundations Workshop, 2001*. IEEE, 2001. doi:10.1109/csfw.2001.930150.

[DMP03] Nancy Durgin, John Mitchell, and Dusko Pavlovic. A compositional logic for proving security properties of protocols. *Journal of Computer Security*, 11(4):677–721, October 2003. doi:10.3233/JCS-2003-11407.

[Fri15] Tobias Fritz. Resource convertibility and ordered commutative monoids. *Mathematical Structures in Computer Science*, 27(6):850–938, 2015. doi:10.1017/s0960129515000444.

[FS19] Brendan Fong and David I. Spivak. *An Invitation to Applied Category Theory: Seven Sketches in Compositionality*. Cambridge University Press, 2019. doi:10.1017/9781108668804.

[FST19] Brendan Fong, David Spivak, and Remy Tuyeras. Backprop as functor: A compositional perspective on supervised learning. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2019. doi:10.1109/lics.2019.8785665.

[Gav19] Bruno Gavranović. Compositional deep learning, 2019. URL: https://arxiv.org/abs/1907.08292, arXiv:1907.08292.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. doi:10.1016/0022-0000(84)90070-9.

[Heu08] Chris Heunen. Compactly accessible categories and quantum key distribution. *Logical Methods in Computer Science*, 4(4), 2008. doi:10.2168/lmcs-4(4:9)2008.

[Hil11] Anne Hillebrand. Superdense coding with GHZ and quantum key distribution with W in the ZX-calculus. In *Proceedings of QPL 2011*, volume 95 of *Electronic Proceedings in Theoretical Computer Science*, pages 103–121, 2011. doi:10.4204/EPTCS.95.10.

[Hin20] Peter M. Hines. A diagrammatic approach to information flow in encrypted communication, 2020. doi:10.1007/978-3-030-62230-5_9.

[HO13] Michal Horodecki and Jonathan Oppenheim. (Quantumness in the context of) Resource Theories. *International Journal of Modern Physics B*, 27(01n03):1345019, 2013. doi:10.1142/s0217979213450197.

[HS15] Dennis Hofheinz and Victor Shoup. GNUC: A new universal composability framework. *Journal of Cryptology*, 28(3):423–508, 2015. doi:10.1007/s00145-013-9160-y.

[HV19] Chris Heunen and Jamie Vicary. *Categories for Quantum Theory: an introduction*. Oxford University Press, USA, 2019.

[KMTZ13] Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Universally composable synchronous computation. In *Theory of Cryptography*, pages 477–498. Springer, 2013. doi:10.1007/978-3-642-36594-2_27.

[KRBM07] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14):140502, 2007. doi:10.1103/PhysRevLett.98.140502.

[KTR20] Ralf Küsters, Max Tuengerthal, and Daniel Rausch. The IITM model: a simple and expressive model for universal composability. *Journal of Cryptology*, 33(4):1461–1584, 2020. doi:10.1007/s00145-020-09352-1.

[KTW17] Aleks Kissinger, Sean Tull, and Bas Westerbaan. Picture-perfect quantum key distribution, 2017. URL: https://arxiv.org/abs/1704.08668, arXiv:1704.08668.

[LC97] Hoi-Kwong Lo and H .F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. arXiv:9711040, doi:10.1103/PhysRevLett.78.3410.

[Lei04] Tom Leinster. *Higher Operads, Higher Categories*. Cambridge University Press, 2004. doi:10.1017/cbo9780511525896.

[Lei14] Tom Leinster. *Basic category theory*, volume 143. Cambridge University Press, 2014. doi:/10.1017/CBO9781107360068.

[LHM19] Kevin Liao, Matthew A. Hammer, and Andrew Miller. ILC: a calculus for composable, computational cryptography. In *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation*, pages 640–654. ACM, June 2019. doi:10.1145/3314221.3314607.

[LSBM19] Andreas Lochbihler, S. Reza Sefidgar, David Basin, and Ueli Maurer. Formalizing Constructive Cryptography using CryptHOL. In *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*. IEEE, June 2019. doi:10.1109/csf.2019.00018.

[Mac71] S. Mac Lane. *Categories for the Working Mathematician*. Springer, 2nd edition, 1971.

[Mau11] Ueli Maurer. Constructive cryptography–a new paradigm for security definitions and proofs. In *Joint Workshop on Theory of Security and Applications—TOSCA 2011*, pages 33–56, 2011. doi:10.1007/978-3-642-27375-9_3.

[May96] Dominic Mayers. The trouble with quantum bit commitment, 1996. URL: http://arxiv.org/abs/quant-ph/9603015, arXiv:9603015.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, 2001. doi:10.1145/382780.382781.

[Mel06] Paul-André Melliès. Functorial boxes in string diagrams. In *Computer Science Logic*, Lecture Notes in Computer Science, pages 1–30. Springer, 2006. doi:10.1007/11874683_1.

[MMP95] A. Mifsud, R. Milner, and J. Power. Control structures. In *Proceedings of Tenth Annual IEEE Symposium on Logic in Computer Science*, pages 188–198. IEEE, 1995. doi:10.1109/lics.1995.523256.

[MMP+18] Christian Matt, Ueli Maurer, Christopher Portmann, Renato Renner, and Björn Tackmann. Toward an algebraic theory of systems. *Theoretical Computer Science*, 747:1–25, 2018. doi:10.1016/j.tcs.2018.06.001.

[MQR09] Jörn Müller-Quade and Renato Renner. Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006, 2009. doi:10.1088/1367-2630/11/8/085006.

[MR11] Ueli Maurer and Renato Renner. Abstract cryptography. In *Innovations in Computer Science—ICS 2011*, 2011.

[MT13] Daniele Micciancio and Stefano Tessaro. An equational approach to secure multi-party computation. In *4th Conference on Innovations in Theoretical Computer Science—ITCS 2013*, pages 355–372, 2013. doi:10.1145/2422436.2422478.

[MV20] Joe Moeller and Christina Vasilakopoulou. Monoidal Grothendieck construction. *Theory and Applications of Categories*, 35(31):1159–1207, 2020.

[Pav97] Dusko Pavlovic. Categorical logic of names and abstraction in action calculi. *Mathematical Structures in Computer Science*, 7(6):619–637, 1997. doi:10.1017/S0960129597002296.

[Pav12] Dusko Pavlovic. Tracing the man in the middle in monoidal categories. In *Coalgebraic Methods in Computer Science*, pages 191–217. Springer, 2012. doi:10.1007/978-3-642-32784-1_11.

[Pav14] Dusko Pavlovic. Chasing diagrams in cryptography. In Claudia Casadio, Bob Coecke, Michael Moortgat, and Philip Scott, editors, *Categories and Types in Logic, Language, and Physics: Essays Dedicated to Jim Lambek on the Occasion of His 90th Birthday*, pages 353–367. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. doi:10.1007/978-3-642-54789-8_19.

[PMM+17] Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner, and Björn Tackmann. Causal boxes: quantum information-processing systems closed under composition. *IEEE Transactions on Information Theory*, 63(5):3277–3305, 2017. doi:10.1109/TIT.2017.2676805.

[PR08] Manoj Prabhakaran and Mike Rosulek. Cryptographic complexity of multi-party computation problems: Classifications and separations. In *Advances in Cryptology—CRYPTO 2008*, pages 262–279, 2008. doi:10.1007/978-3-540-85174-5_15.

[PR14] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution, 2014. URL: https://arxiv.org/abs/1409.3525, arXiv:1409.3525.

[PW00] Birgit Pfitzmann and Michael Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *2001 IEEE Symposium on Security and Privacy—S&P 2001*, pages 184–200, 2000. doi:10.1109/SECPRI.2001.924298.

[Ren05] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 06(01):1–127, 2005. arXiv:0512258v2, doi:10.1142/S0219749908003256.

[Rie17] Emily Riehl. *Category theory in context*. Courier Dover Publications, 2017.

[Sel10] Peter Selinger. A survey of graphical languages for monoidal categories. In *New structures for physics*, pages 289–355. Springer, 2010. doi:10.1007/978-3-642-12821-9_4.

[SHW20] Xin Sun, Feifei He, and Quanlong Wang. Impossibility of quantum bit commitment, a categorical perspective. *Axioms*, 9(1):28, 2020. doi:10.3390/axioms9010028.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000. doi:10.1103/physrevlett.85.441.

[SV13] Mike Stay and Jamie Vicary. Bicategorical semantics for nondeterministic computation. In *Proceedings of the Twenty-ninth Conference on the Mathematical Foundations of Programming*

Semantics, MFPS XXIX, volume 298 of *Electronic Notes in Theoretical Computer Science*, pages 367 – 382, 2013. doi:10.1016/j.entcs.2013.09.022.

[Swe69] Moss Eisenberg Sweedler. Integrals for hopf algebras. *Annals of Mathematics*, 89(2):323–335, 1969. doi:10.2307/1970672.

[TLGR12] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, 2012. doi:10.1038/ncomms1631.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology—EUROCRYPT 2010*, pages 486–505, 2010. doi:10.1007/978-3-642-13190-5_25.

[VPDR19] Venkatesh Vilasini, Christopher Portmann, and Lídia Del Rio. Composable security in relativistic quantum cryptography. *New Journal of Physics*, 21(4):043057, 2019. doi:10.1088/1367-2630/ab0e3b.

[Win13] Glynn Winskel. Distributed probabilistic and quantum strategies. *Electronic Notes in Theoretical Computer Science*, 298:403–425, 2013. doi:10.1016/j.entcs.2013.09.024.

[WW08] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. *IEEE Transactions on Information Theory*, 54(6):2792–2797, 2008. doi:10.1109/tit.2008.921674.