How to Incentivize Data-Driven Collaboration Among Competing Parties

Pablo Daniel Azar[1], Shafi Goldwasser[2], and Sunoo Park[1]

[1]MIT
[2]MIT and the Weizmann Institute of Science

Abstract

The availability of vast amounts of data is changing how we can make medical discoveries, predict global market trends, save energy, and develop new educational strategies. In certain settings such as Genome Wide Association Studies or deep learning, the sheer size of data (patient files or labeled examples) seems critical to making discoveries. When data is held distributedly by many parties, as often is the case, they must share it to reap its full benefits.

One obstacle to this revolution is the lack of willingness of different entities to share their data, due to reasons such as possible loss of privacy or competitive edge. Whereas cryptographic works over the last 30 years address the privacy aspects, they shed no light on individual parties' losses and gains that may influence their decision to collaborate. This is the question we model and study in this paper. The *order* in which collaborators receive the outputs of a collaboration will be a crucial aspect. Our contributions are:

- We formalize a model of n-party collaboration for computing functions over private inputs, in which the participants receives their outputs in order (i.e. player i receives his output in position $\pi(i)$, where π is a permutation over n elements) and where each output "improves" on all previous outputs. Both π and the outputs received depend on all players' input data. The model includes a reward function that captures the utility of collaboration for player i depending on his input, his output, other players' outputs, and $\pi(i)$.
- We design mechanisms to compute a distribution of outputs and an ordering of output delivery, based on the n participants' private inputs. We say that a collaboration outcome is a *collaborative equilibrium* if it guarantees a higher reward for all participants when joining a collaboration compared to not joining it. We show that while in general computing a collaborative equilibrium is NP-complete, we can design polynomial-time algorithms for computing it for a range of natural model settings.
- We show how to extend the theory of multi-party computation (MPC) to impose an ordering on the delivery of outputs to different players. This extension, named *ordered MPC*, can be used to implement our mechanisms without a centralized trusted party and in the presence of a subset of colluding players who may deviate from the protocol in an arbitrary fashion, under cryptographic assumptions. Since the delivery schedule depends on players private inputs, it may leak information. Hence, we enhance the MPC privacy requirement to require each player to learn nothing more than his output and his own position in the output ordering. We also adapt the notions of guaranteed output delivery and fairness to require instead *ordered output delivery* and *prefix-fairness*.
- We introduce *timed-delay MPC*, where explicit time delays are introduced into the output delivery schedule. We use the classical time-lock primitive, to obtain protocols for timed-delay MPCs. Finally, we introduce a new concept called *time-line puzzles*, which are a natural extension of classical time-lock puzzles, in which multiple data items can be locked so that their eventual openings can be "serialized" in time.

1 Introduction

The availability of vast amounts of data is changing how we can make medical discoveries, predict global market trends, save energy, improve our infrastructures, and develop new educational strategies. Indeed, it is is becoming clearer that *sample size* may be the most important factor in making surprising new discoveries in a number of areas such as *genome-wide association studies*[1] (GWAS) and *machine learning* (ML), as witnessed by the striking success of GWAS studies with large samples for schizophrenia[2] [BP12; PGC14; For11] and the success of deep learning in ML.

When large data is required, often parts of the data are held by different entities. Such entities need to share their data, or at least engage in a collaborative computation where each entity manages its own private data, in order for society to reap the benefit of large sample sizes. Referring back to the GWAS example, success was explicitly attributed to such collaboration: "The schizophrenia study was made possible due to unusually large scale collaborations among many institutes... This level of cooperation between institutions is absolutely essential... If we are to continue elucidating the biology of psychiatric disease through genomic research, we must continue to work together." [Ins14]

Unfortunately, the above example is the exception rather than the rule. A major obstacle to the big-data revolution is the lack of willingness of different entities to share data in collaborations with each other: so-called "data hoarding". One obstacle is privacy concerns, where parties refuse to collaborate, in order to protect the privacy of their data. Privacy, however, is not the only obstacle.

An equally important obstacle is competition between entities holding data. When access to data carries tangible rewards, say, if the entities are companies competing for a share of the same market or research laboratories competing for scientific credit, it is unclear whether an individual collaborator is better off, even if it is clear that better overall conclusions can be drawn from collaboration. Stated in more game-theoretic terms, the entities face the following dilemma: *whereas the overall societal benefit of collaboration is clear, the utility for an individual collaborator may be negative, so why collaborate?* Addressing this question is the topic of this paper.

In this paper, we present a formal model for collaboration in which this question can be analyzed, as well as design mechanisms to enable collaboration where all collaborators are provably "better off", when possible. The *order* in which collaborators receive the outputs of a collaboration will be a crucial aspect of our model and mechanisms. We believe that timing is an important and primarily unaddressed issue in data-based collaborations. For example, in the scientific research community, data sharing can translate to losing a prior publication date. In financial enterprises, the timing of investments and stock trading can translate to large financial gains or losses.

The collaboration mechanisms we develop assume a central trusted party; however, we will show that this assumption is not necessary under standard cryptographic assumptions. We show in Section 3 how the mechanisms can be implemented in a decentralized way by n distrustful parties by using new extensions of classical secure multiparty computation that give formal guarantees on the *order and timing* of output delivery as well as the standard requirements of privacy and correctness.

[1] A genome-wide association study is an investigation of common genetic variants in a population, in order to identify genetic variants that are associated with a given trait.

[2] "Dramatic increase in patient data size enabled the discovery of more than 100 gene loci associated with the disease up from a handful loci seen with small sets of patients. This was made possible due to an unusually large scale collaborations among many institutes."

1.1 Summary of our contributions

1.1.1 A model of collaboration

We propose a model for collaboration which enables the determination of whether the utility obtained by a collaborator outweighs the utility he may obtain without collaboration. The ultimate desired outcome of a collaboration is to learn the output y^* of a function f evaluated on participants' input data $x_1, \ldots, x_n$. In our model, the outcome of a collaboration is a pair $(\pi, \mathbf{z})$ where π is a permutation of player identities and $\mathbf{z} = (z_1, , \ldots, z_n)$ is a vector of "public outputs" where $z_{\pi(i)}$ is the output of player i. For example, in the setting of scientific collaboration, the public output could be an academic publication. Our model setup assumes an underlying distance metric d in which any two outputs can be compared. The quality of a player's output z_i will be higher when the distance $d(z_i, y^*)$ to the "true output" y^* is lower.

The model includes a *reward function* R_t which characterizes the gain in utility for any given party i in a collaboration. The reward that a party i gets depends on how much his $z_{\pi(i)}$ *improves on* the previous state of the art $z_{\pi(i)-1}$, and on $\pi(i)$, namely, *when* the party makes his public output. Specifically, the reward function includes a multiplicative *discount factor* β^t where $\beta \in [0, 1]$ and t is the time of publication, meaning that the reward from a publication is "discounted" more as time goes on.

$$R_t(\pi, \mathbf{z}) = \beta^t \cdot (d(z_{\pi(t-1)}, y^*) - d(z_{\pi(t)}, y^*))$$

To determine whether the utility of collaboration outweighs the utility of working on one's own, our model uses "outside payoff" values α_i which are the utility that party i would obtain *without collaborating*.[3] These values may be provided by the relevant party i or, in some scenarios (as discussed in the examples given in the next subsection), α_i can be computed directly from the input x_i of party i.

Our results hold for general distance metrics; however, it is illustrative to discuss concrete instantiations, as we do in the next subsection.

1.1.2 Mechanisms and collaborative equilibrium

We define a notion of *collaborative equilibrium* in which all parties are guaranteed a non-negative reward, and develop *mechanisms* for collaboration that compute such equilibria (when they exist). When an equilibrium exists, our mechanism delivers a sequence of progressively improving approximations of y^* to the collaborating parties. More specifically, the mechanism will take as input the data of all parties, and output a pair $(\pi, \mathbf{y})$ where π is a permutation of player identities and $\mathbf{y} = (y_1, , \ldots, y_n)$ specifies the outcomes to be delivered to the players: each $y_{\pi(i)}$ is the approximation to y^* that is given to player i at time-step $\pi(i)$, such that the quality of outputs is increasing with time. That is, $d(y_{\pi(1)}, y^*) > \cdots > d(y_{\pi(n)}, y^*)$. We emphasize that both the order π and the outcomes y_i are computed based on the inputs of all players.

When player i receives an output $y_{\pi(i)}$ from the central mechanism, she may combine $y_{\pi(i)}$ with the information that she learned from prior public outputs and her own input x_i, to generate a public output $z_{\pi(i)}$. We first prove that the ability of the players to learn from others' publications, in general, will make the problem of deciding whether there exists an equilibrium is NP-complete (see Theorem 2.8).

[3] Our model is flexible enough that we could have $\alpha_i' = \alpha_i + c_i$ where α_i is the utility to player i from not collaborating and c_i is some overhead cost of collaboration. Alternatively, we could have $\alpha_i' = \alpha_i \cdot c_i$, so that agent i will collaborate only if her reward from doing so is greater than c_i times her reward for not collaborating. (Indeed, α_i' could be any function of α_i.) All our results would follow through by replacing α_i with the corresponding α_i'.

Next, we show that there is a polynomial-time mechanism that can output an equilibrium whenever one exists (or output `NONE` if one does not exist) for a variety of model settings and parameters which we characterize (see Theorem 2.6). An example of a setting when a polynomial-time mechanism is possible is when

- an upper bound μ_j can be set on the amount of information that any player can learn from a given player j's publication, and
- it is possible to efficiently compute, for any y^* and $\delta > 0$, an "approximation" y' such that $d(y', y^*) = \delta$.

In a nutshell, the bounds μ_j can be used to define a weighted graph in which the weight of the minimum-weight perfect matching determines the existence of a collaborative equilibrium. In general, our mechanism takes the bounds μ_j as input. However, similarly to the outside payoffs α_i, it is often possible to compute bounds μ_j directly based on the input datasets $x_1, \ldots, x_n$ of the parties, as detailed in the examples which follow.

We now illustrate our model and mechanism with some concrete instantiations.

Example 1: Outputs as real-valued statistics. One instantiation of our model is where the set of collaboration outputs is the set of real random variables with finite mean and variance, with the distance $d(a, b) = \sqrt{\mathbb{E}[(a-b)^2]}$. This model captures a reasonable class of common data analysis functions f where each player i's data consists of a random variable x_i and we want to compute a statistic $y^* = f(x_1, ..., x_n)$ such as the mean $\frac{1}{n}\sum_{i=1}^n x_i$ or variance $\frac{1}{n}\sum_{j=1}^n (\frac{1}{n}\sum_{i=1}^n x_i - x_j)^2$. The quality of an answer $\hat{y}$ is measured by the expected square error $d(\hat{y}, y^*) = \mathbb{E}[(\hat{y} - y^*)^2]$.

In this case, the "outside option" value α_i is the expected square error of agent i's best prediction of y given only the information contained in her data x_i. Note that the best possible output that player i can produce on her own is $\hat{y}_i = \min_z \mathbb{E}[(z - y^*)^2 | x_i]$. Our mechanism for this type of setting will consist of slowly revealing closer and closer approximations to y.

Example 2: Machine learning classifiers. Another example is where each dataset x_i is a set of labeled observations $x_i = ((x_{i,1}, c_{i,1}), \ldots, (x_{i,n_i}, c_{i,n_i}))$ where each $x_{i,j}$ is an attribute vector in some large set X and $c_{i,j}$ is a classification label. Let $\mathcal{C}(x_{ij}, \theta)$ be a classifier that takes a parameter vector θ and an input vector x_{ij} and outputs c_{ij}. We may not be able to learn this classifier perfectly just with access to the finite datasets $x_1, \ldots, x_n$, but we may be able to learn a good approximation $\theta^* = f(x_1, ..., x_n)$ to the parameter vector θ. In this case, f is a learning algorithm which takes the players' data as input and outputs the classifier parameter vector θ^*. The "loss" from using θ^* instead of θ is the expected square classification error $d(\theta, \theta^*) = \sum_{x \in X} (\mathcal{C}(x_{ij}, \theta^* - \mathcal{C}(x_{ij}, \theta))^2$. In this case, α_i represents the best reward that agent i can obtain using only her data. That is, she can learn a parameter vector $\hat{\theta}_i$ from her own dataset $x_i = ((x_{i,1}, c_{i,1}), \ldots, (x_{i,n}, c_{i,n}))$ and $\alpha_i = d(\hat{\theta}_i, \theta)$. Since more data improves the accuracy of the learning algorithm, we will always have that $d(\theta^*, \theta) < d(\hat{\theta}_i, \theta)$.

Example 3: Outputs as sets of findings. An instantiation of a different flavor is when the output of the collaboration is not real-valued, but instead is a *set* of findings. An important use case is genomics research seeking to identify sets of gene loci that are correlated with a particular disease. An interesting difference of this example from the previous ones is that the output set is discrete. While the analysis of the real-valued case does not translate directly to the discrete setting, we show that under certain additional assumptions on model parameters, our mechanism can address the discrete case too. Details are given in Section 2.7 and Appendix A.

Computing μ_j. In all our cases, the upper bound μ_j on how much any player can learn from player j's publication is harder to pin down and depends more explicitly on the function being learned and the inference algorithm that each player i uses to combine his data and player j's publication. We give a more formal discussion on section 2.3 showing how to define learning bounds for our first example where inputs are random variables (the machine learning example is analogous). As we shall see, our learning bounds will be very high dimensional objects which depend on the order in which players make their publications. We will argue in section 2.3 on how we reduce the dimensionality of these learning bounds to obtain the n-dimensional vector $\{\mu_j\}_{j=1}^n$. An useful intuition is that, when the number of players is large and the output does not depend too much on any single player's data, both μ_j and α_i should be small numbers. There is not much that can be learned from one player's individual data, but aggregating all the players' data leads to important insights.

1.1.3 Cryptographic protocols to implement the mechanisms

We develop cryptographic protocols for implementing the mechanisms without a centralized trusted party and in the presence of a subset of colluding players who may deviate from the protocol in an arbitrary fashion, under cryptographic assumptions. The protocols compute the collaboration outcome $(\pi, \mathbf{y})$ via multi-party secure computation on players' private inputs. Since a crucial aspect of the mechanism's ability to yield non-negative reward to all players is the delivery of outputs in order, we need to extend the classical notion of MPC to incorporate guarantees on the order and timing of output delivery. These extensions may be of interest independent of the application of mechanisms for incentivizing collaborations.

We define *ordered MPC* as follows. Let f be an arbitrary n-ary function and p be an n-ary function that outputs permutation $[n] \to [n]$. An ordered MPC protocol is executed by n parties, where each party $i \in [n]$ has a private input $x_i \in \{0,1\}^*$, who wish to securely compute $f(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ where y_i is the output of party i. Moreover, the parties are to receive their outputs in a particular *ordering* dictated by $p(x_1, \ldots, x_n) = \pi$ where π is a permutation of the player identities. Since the choice of π depends on private inputs, it may leak information: hence, we formulate an enhanced *privacy* requirement for ordered MPC that each player should learn his output and his *own* position in the output ordering, and nothing more (see Definition 3.1).

We show a simple transformation from classical MPC protocols for general functionalities f to ordered MPC protocols for general functionalities f and permutation functions p that achieve enhanced privacy, even when a minority of the n players may be colluding to sabotage the protocol (see Theorem 3.4). The assumptions necessary are the same as for the classical MPC constructions (e.g. [GMW87]). When the colluding players are in majority, it is well known that output delivery to all honest parties cannot be guaranteed [Cle86].

Next, we define *timed-delay MPC*, where explicit time delays are introduced into the output delivery schedule. Time delays between the outputs may be crucial to enable parties to reap the benefits of their position in the order. We give two constructions of timed-delay MPC in the honest majority setting[4]. First, we give a conceptually simple protocol which runs "dummy rounds" of communication in between issuing outputs to different players, in order to measure time-delays. The simple protocol has the flaw that all (honest) players must continue to interact until the last party receives his output (that is, they must stay online until all the time-delays have elapsed). To address this issue, we present a second protocol assuming the existence of time-lock puzzles [RSW96] in addition to the classical MPC [GMW87] assumptions (see Theorem 4.6). Informally, a

[4]We cannot hope to achieve timed-delay MPC in the case of dishonest majority since, as mentioned in the preceding paragraph, even output delivery cannot be guaranteed in this setting.

time-lock puzzle is a primitive which allows "locking" of data, such that it will be released after a pre-specified time delay, and no earlier. Our second timed-delay MPC protocol, instead of issuing outputs to players in the clear, gives to each party his output *locked* into a time-lock puzzle; and in order to enforce the desired ordering, the delays required to unlock the puzzles are set to be an increasing sequence. An issue that arises when giving out time-lock puzzles to many parties is that different parties may have different computing power, and hence solve their puzzles at different speeds: for example, it is clear that we cannot guarantee that players learn their outputs in the desired ordering if some players compute arbitrarily faster than others. Still, we show that our protocol is secure and achieves ordered output delivery in the case that the difference between any two players' computing power is known to be bounded by a logarithmic factor. If the assumption about computing power does not hold, then the protocol still achieves security (i.e. correctness and privacy), but the ordering of outputs is not guaranteed.

The definition of ordered and timed-delay MPC inspire new notions unrelated to the central topic of this paper. In particular:

- **Time-lines.** Inspired by the application of time-lock puzzles to time-delayed MPC, we propose the new concept of a *time-line*, where multiple data items can be locked so that their unlocking must be serialized in (future) time. See Section 4.4 for details.

- **Prefix-fairness.** In the traditional MPC landscape, fairness is the one notion that addresses the idea that either all parties participating in an MPC should benefit, or none should. Fairness requires that either all players receive their output, or none do. However, it is well-known that fairness is achievable when a majority of the players are honest, but it is *not* achievable for general functionalities when a majority of players are faulty [Cle86]. We propose a refinement of the classical notion of fairness in the setting of ordered MPC, called *prefix-fairness*, where players are to receive their outputs one after the other according to a given ordering π, and the guarantee is that *either* no players receive an output *or* those who do strictly belong to a prefix of the mandated order π (see Definition 3.3). Prefix-fairness can be achieved for general functionalities and *any number* of faulty players, under the same assumptions as classical MPC [GMW87] (see Theorem 3.5).

1.2 Discussion and interpretation of our work

Slowing down scientific discovery? Intuitively, the mechanisms we develop always take the following form: the mechanism computes the "ideal outcome" y^* based on all inputs of the potential collaborators, and then hands out a sequence of successively more accurate (according to the distance metric) outcomes, where the final party receives y^*.

One may ask: why slow down scientific progress and hand out inferior results when better ones are available? We argue that progress will in fact be *enhanced*, not slowed down, by this methodology, as it will be a decisive factor in parties' willingness to collaborate in the first place. This bears great similarity to the original philosophy of *differential privacy* and privacy-preserving data analysis more generally. In these fields, accuracy (so-called utility) of answers to aggregate queries over items in database is partially sacrificed in order to preserve privacy of individual data items, as a way to encourage individuals to contribute their data items to the database. In an analogous way, in order to get results based on the large data sets held by potential collaborators, we sacrifice the *speed* of discovery of the "ultimate" collaboration outcome: we are willing to pay this price to incentivize parties to collaborate and contribute their data. In contrast to differential privacy, we do not sacrifice ultimate accuracy. The last collaborator to receive an output, receives the ideal outcome y^*. Namely, $y_n = y^*$.

The Fort Lauderdale example: the importance of time A recurring idea in this work is the importance of time and ordering of research discoveries, which is inspired in part by the following striking example from the field of genomics. In the 2003 Fort Lauderdale meeting on large-scale biological research [Wel03], the gathering of leading researchers in the field recognized that "pre-publication data release can promote the best interests of [the field of genomics]" but "might conflict with a fundamental scientific incentive – publishing the first analysis of one's own data". Researchers at the meeting agreed to adopt a set of principles by which although data is shared upon discovery, researchers hold off publication until the original holder of the data has published a first analysis. Being a close-knit community in which reputation is key, this was a viable agreement which has led to great productivity and advancement of the field. However, more generally, their report states that "incentives should be developed by the scientific community to support the voluntary release of [all sorts of] data prior to publication". This example teaches us to focus on three key aspects of collaboration: the incentive to collaborate has to be clear to all collaborators; there must be a way to ensure adherence to the rules of collaboration; and timing is of the essence.

Privacy implies increased utility Although the goal of our work is to design mechanisms *to incentivize collaboration* by increasing the utility of collaborations rather than focusing on the privacy of individual entities' input data, MPC protocols prove to be an important technical tool to implement the mechanisms which guarantee increased utility. As a by-product, the use of MPC provides our mechanisms with the additional guarantee of privacy.

Future directions When collaboration is feasible, each party i in our model is guaranteed a reward from collaborating that is greater than the reward α_i that they could get on their own. However, there are many settings where "the sum is greater than the parts", and the contribution that player i's data x_i makes to the collaboration output $y^* = f(x_1, ..., x_n)$ is much larger than the value α_i of just knowing x_i in isolation. Furthermore, the contributions of the players' data to the computation of the final output y^* may be asymmetric: some special player i^* may have some data that helps solve the "puzzle", but this player i^* may not be known a priori before the participants decide to collaborate[5] An interesting future direction would be to develop mechanisms where, even if we do not know a priori which players have higher quality data, we can still allocate more credit after the collaboration is done to the players whose contribution turned out to be the most valuable.

Another future direction of interest to design *truthful* mechanisms so that collaborating parties will be provably incentivized to submit their true and accurate data as input. In our work, we assume that, while we can incentivize the players to collaborate or not, once they decide to collaborate they are truthful about the value of their dataset x_i. From the point of view of scientific publications, this assumption is reasonable if we believe that the experiments that generate this data can be verified or replicated, and that a failure to replicate would hurt a scientific group's reputation. However, there are many settings, such as businesses pooling their data together to generate larger profits, where the parties may be incentivized to lie about their output x_i. Since we are already assuming that parties are rational, a future direction would be to develop mechanisms where, even when parties can lie about x_i (because x_i cannot be verified by others), they are still incentivized to report it truthfully. One possible direction is where x_i is the output of some long $\#P$ computation (for example, a Markov Chain Monte-Carlo simulation), where (a) replicating the computation would take a very long time and delay publication for everyone in the group and (b) player i cannot prove

[5] An example in the same vein is the following. In the medical setting, a hospital with a larger patient population will clearly have more patient data than a small facility, and yet access to data of small but homogeneous or rare communities can at times be more valuable than access to larger heterogeneous sets of data.

in a classical way that their output x_i is correct. Even in this case, player i can be incentivized to give the right answer via a rational proof [AM12; AM13; GHRV14].

1.3 Other related work

The problem of how to make progress in a scientific community has been studied in other contexts. Banerjee, Goel and Krishnaswamy [BGK14] consider the problem of partial progress sharing, where a scientific task is modeled as a directed acyclic graph of subtasks. Their goal is to minimize the time for all tasks to be completed by selfish agents who may not wish to share partial progress.

Kleinberg and Oren [KO11] study a model where researchers have different projects to choose from, and can work on at most one. Each researcher i has a certain probability of being able to solve a problem j, and she gets a reward w_j if she is the only person to solve it. If multiple researchers solve the problem, they study how to split the reward in a socially optimal way. They show that assigning credit asymmetrically can be socially optimal when researchers seek to maximize individual reward, and they suggest implementing a "Matthew Effect", where researchers who are already credit-rich should be allocated more credit than in an even-split system. Interestingly, this is coherent with the results of our paper, where it is socially optimal to obfuscate data so that researchers who are already "ahead" (in terms of data), end up "ahead" in terms of credit.

Cai, Daskalakis and Papadimitriou [CDP14] study the problem of incentivizing n players to share data, in order to compute a statistical estimator. Their goal is to minimize the sum of rewards made to the players, as well as the statistical error of their estimator. In contrast, our goal is to give a decentralized mechanism through which players can pool their data, and distribute partial information to themselves in order so as to increase the utility of every collaborating player.

Boneh and Naor [BN00] construct timed commitments that can be "forced open" after a certain time delay, and discuss applications of their timed commitments to achieve fair two-party contract signing (and coin-flipping) under certain timing assumptions including bounded network delay and the [RSW96] assumption about sequentiality of modular exponentiation.

Roadmap Section 2 covers the scientific collaboration model, mechanisms, and feasibility theorems. Section 3 covers the definitions and constructions of ordered MPC, and Section 4 covers definitions and constructions of timed-delay MPC, and associated primitives such as time-line puzzles.

2 Scientific collaboration model

In this section, we present and analyze mechanisms for scientific collaboration in our model. In our exposition, we focus primarily on the setting of scientific collaboration and publication. However, we want to highlight that our results apply to more broad collaboration and discovery in general, in which case a "publication" should be thought of as any kind of public output.

Notation Throughout this section, we denote by $[n]$ the set $\{1, ..., n\}$ of integers between 1 and n, and by $[n] \to [n]$ the set of all permutations of $[n]$.

2.1 Finding feasible orders for scientific collaboration

We present a model of scientific collaboration, addressing *whether* it is beneficial for parties to collaborate, and if so, *how*: in particular, since the order of research publication matters, we examine the problem of finding a feasible collaboration order.

We propose a model of collaboration between n research groups which captures the following features. Groups may pool their data, but each group will publish their own results. Moreover, only results that improve on the "state of the art" may be published. That is, a new result must improve on prior publications. However, more credit may be given to earlier publications. Finally, a group will learn not only from pooling their data with other groups, but also from other groups' publications.

2.2 The model

To formalize the intuitions outlined above, we specify a model as follows.

- There is a set $[n]$ of players.
- For each $i \in [n]$, there is a set X_i of possible datasets, and a dataset $x_i \in X_i$ that the player knows. Let X denote $X_1 \times \cdots \times X_n$.
- A metric space Y with distance function $d : Y \times Y \to \mathbb{R}_+$.
- A function $f : X \to Y$, whose output $y^* \stackrel{\text{def}}{=} f(x_1, \ldots, x_n)$ the players wish to learn.
- All players commonly know an "initial result" $y_0 \in Y$.
- For each player i, we denote by $\alpha_i \geq 0$ their reward from not collaborating. This models the best "outside payoff" that they could receive from publishing on their own. We denote by $A = \mathbb{R}_+^n$ the set of all outside option vectors.
- A *collaboration outcome* is given by a permutation $\pi : [n] \to [n]$ and a vector of outputs $(z_{\pi(1)}, \ldots, z_{\pi(n)}) \in Y^n$ such that $d(y_0, y^*) > d(z_{\pi(1)}, y^*) > \cdots > d(z_{\pi(n)}, y^*)$.

  The intuition behind this condition is that, at time t, player $\pi(t)$ will publish result $z_{\pi(t)}$. This result is a distance $d(z_{\pi(t)}, y^*)$ away from the true answer y^*. A result $z_{\pi(t)}$ is of higher quality when it is closer to the the true answer y^*. Since only results that improve on the "state of the art" can be published, we must have that $d(z_{\pi(t)}, y^*)$ decreases with the time of publication t.
- If $\omega = (\pi, \mathbf{z})$ is a collaboration outcome, the player who publishes at time t obtains a reward

$$R_t(\pi, \mathbf{z}) = \beta^t \cdot (d(z_{\pi(t-1)}, y^*) - d(z_{\pi(t)}, y^*))$$

  where $\beta \in (0, 1]$ is a *discount factor* which penalizes later publications, and $d(z_{\pi(t-1)}, y^*) - d(z_{\pi(t)}, y^*)$.[6]
- Players may learn information not only from their own data, but also from the prior publications of others. A *learning bound vector* $\{\lambda_{\pi,i}\}_{\pi \in ([n] \to [n]), i \in [n]}$ characterizes, for any publication order π, the maximum amount that each player i can learn from prior publications. This notion is defined formally in Section 2.3.

2.3 Data-sharing mechanisms

We seek to design a data-sharing mechanism that takes as input the data of all the parties, and outputs some information y_i to each player i. Moreover, the mechanism will output the y_i values to players sequentially, in a particular order. Upon receiving y_i, player i will produce a public output (i.e a publication in the research collaboration example) which we denote by z_i.

We note that the public output of player i will not necessarily be the same as what was delivered by the data-sharing mechanism. Since player i wants to maximize her reward, she will publish a z_i that will maximize her reward, conditional on the information she has at the time of publication. This information includes, in addition to the output y_i which she receives from the mechanism, also

[6] This is motivated by market scoring rules [Han12], where different experts only receive a reward equal to how much they improve existing predictions.

her own dataset x_i, and all the outputs that came before her. Recall that a *collaboration outcome* $(\pi, \mathbf{z})$ is given by a permutation $\pi : [n] \to [n]$ and a vector of outputs $(z_{\pi(1)}, \ldots, z_{\pi(n)}) \in Y^n$ such that $d(y_0, y^*) > d(z_{\pi(1)}, y^*) > \cdots > d(z_{\pi(n)}, y^*)$. We now define a *proposed collaboration outcome* $(\pi, \mathbf{y})$ as a permutation $\pi : [n] \to [n]$ together with a vector of *proposed* outputs $(y_{\pi(1)}, \ldots, y_{\pi(n)}) \in Y^n$ generated by a data-sharing mechanism, such that $d(y_0, y^*) > d(y_{\pi(1)}, y^*) > \cdots > d(y_{\pi(n)}, y^*)$.

Recall that we need to bound how much player i can learn from previous publications (and from her own dataset). We formally capture this with the notion of *learning bound vectors* $\lambda_{\pi,i}$ – an upper bound on the amount that player i learns from all previous publications when the order of publication is determined by permutation π.

Definition 2.1. *A* learning bound vector $\lambda = \{\lambda_{\pi,i}\}_{\pi \in ([n] \to [n]), i \in [n]}$ *is a non-negative vector such that, if* $(\pi, (y_1, \ldots, y_n))$ *is a collaboration outcome proposed by a data-sharing mechanism, and* z_i *is the best result that player* i *knows at time* $\pi^{-1}(i)$*, then* $d(z_i, y^*) \geq d(y_i, y^*) - \lambda_{\pi,i}$*. We denote by* $\Lambda = \mathbb{R}_+^{n! \times n}$ *the set of all learning bound vectors.*

The set of inferred outputs *derived from* $(\pi, \mathbf{y})$ *is the set*

$$\mathcal{I}(\pi, \mathbf{y}) = \{(z_1, \ldots, z_n) : \forall t \in [n],\ d(y_{\pi(t)}, y^*) - \lambda_{\pi,\pi(t)} \leq d(z_\pi(t), y^*) \leq d(y_{\pi(t)}, y^*)\}.$$

The intuition behind the above definition is that the amount of information that player $\pi(t)$ (namely, the player who publishes at time t) can learn from prior outputs is measured by how much she can reduce the distance of her prediction to the true output y^*. This reduction in distance is bounded by $\lambda_{\pi,\pi(t)}$. Thus, her eventual output will be some $z_{\pi(t)}$ with distance between $d(y_{\pi(t)}, y^*) - \lambda_{\pi,\pi(t)}$ and $d(y_{\pi(t)}, y^*)$.

For example, when outputs are random variables and the distance is the expected squared error to the true answer, we have that the best possible inferred output for player $\pi(t)$ is $z_{\pi(t)} = \min_z \mathbb{E}[(z - y^*)^2 | x_{\pi(t)}, y_{\pi(t)}, z_{\pi(t-1)}, \ldots, z_{\pi(1)}, y_0]$. In this case, $\lambda_{\pi,\pi(t)} = d(y_{\pi(t)}, y^*) - d(z_{\pi(t)}, y^*)$.

Remark. In our example above, $\lambda_{\pi,\pi(t)}$ measures exactly the amount of information that player $\pi(t)$ can learn from her data. However, in our definition $\lambda_{\pi,\pi(t)}$ is an upper bound, and we emphasize that it may be a loose upper bound on the amount of information $\pi(t)$ can learn. We put the emphasis on a bound for two reasons.

- In general, the vector $\lambda \in \mathbb{R}^{n! \times n}$ has very high dimension, and finding such a vector is infeasible. We may want to approximate this vector via a low-dimensional encoding (as we will do below, where we encode learning bounds using n-dimensional vectors). Since this low-dimensional encoding will lose information, we will not be able to represent $\lambda_{\pi,\pi(t)}$ exactly, but may get a reasonable upper bound on its value.
- For some other settings, we may not be able to derive a precise expression for $\lambda_{\pi,\pi(t)}$ in terms of expectations, but we may still be able to derive an upper bound on the amount of information that player $\pi(t)$ learns. An example of such a setting is detailed in Section 2.7.

Now that we have established a formal definition of learning bound vectors, we proceed to formally define a data-sharing mechanism.

Definition 2.2. *Given a function* $f : X \to Y$*, a* data sharing mechanism *is a function*

$$M_f : X \times A \times \Lambda \to ([n] \to [n]) \times Y^n$$

which takes as inputs a vector $(x_1, \ldots, x_n)$ *of datasets, a vector* $(\alpha_1, \ldots, \alpha_n)$ *of outside options, and* $\{\lambda_{\pi,i}\}_{\pi \in ([n] \to [n]), i \in [n]}$ *a learning bound vector. The outputs from such a mechanism are an ordering* π *of the players, and a vector of outputs* $(y_1, \ldots, y_n)$*.*

Remark. In the definition, for the sake of generality, we assume that the α_i and λ values are given as input to the mechanism. We remark that in certain settings, these values can be computed directly from the inputs x_i of the parties, as discussed in the examples of Section 1.1.2. In this case, one may think of the mechanism $M_f : X \to ([n] \to [n]) \times Y^n$ as having input domain X only.

2.4 Collaborative equilibria

In our model, each research group $\pi(t)$ will collaborate only if the credit they obtain from doing so is greater than the "outside option" reward $\alpha_{\pi(t)}$. We want to design a mechanism that guarantees collaboration whenever possible.

Given the above definition, we can define the following equilibrium concept.

Definition 2.3. *Let $(\mathbf{x}, \alpha, \lambda) \in X \times A \times \Lambda$ and $(\pi, \mathbf{y}) = M_f(\mathbf{x}, \alpha, \lambda)$. Let $\mathcal{I}(\pi, \mathbf{y})$ be the set of inferred outputs from $(\pi, \mathbf{y})$. We say that $(\pi, \mathbf{y})$ is a* collaborative equilibrium *if $\forall \mathbf{z} \in \mathcal{I}(\pi, \mathbf{y})$ we have $R_t(\pi, \mathbf{z}) \geq \alpha_{\pi(t)}$ where R_t is the reward function as defined in Section 2.1.*

Our goal is to find data-sharing mechanisms M_f for which collaboration is an equilibrium. Intuitively, since we are searching for a feasible permutation over a very high-dimensional space ($n!$-dimensions), the problem will be NP-complete (see Theorem 2.8). However, there is a very natural condition on the learning vectors for which we can reduce the dimension of the search space and efficiently find a collaborative equilibrium, if one exists. The feasible case corresponds to the case where, for any player j, there is a bound on the amount of information that player j could *teach* any other players. We denote this bound by μ_j. Analogously, we could define μ_j to be a bound on the amount that player j can *learn* from any other player. For this write-up, we describe only the first case, when μ_j represents a bound on how much information player j can teach other players. The other case is analogous.

Formally, we define a learning bound vector to be *n-dimensional* if it satisfies the following property.

Definition 2.4. *We say that a learning vector $\lambda \in \Lambda$ is n-dimensional if there exists a non-negative vector $\{\mu_j\}_{j=1}^n$ such that $\lambda_{\pi,\pi(t)} = \sum_{\tau=1}^{t-1} \mu_{\pi(\tau)}$. We denote by $\Lambda_1 \subset \Lambda$ the set of all n-dimensional learning vectors.*

When λ is an *n-dimensional* learning vector, the total amount that player $\pi(t)$ learns from all prior outputs is $\sum_{\tau=1}^{t-1} \mu_{\pi(\tau)}$. We show below that in this case, we can give necessary and sufficient conditions for an equilibrium to exist.

Note that since the output y^* is real-valued, it is possible to add noise to this value y^* to obtain less accurate approximations $y_i = y^* + Normal(0, \delta_i)$. More precisely, the following "divisibility" condition is satisfied, which is important for the following analysis.

Output Divisibility Condition. For any $y \in Y$ and any real $\delta > 0$, it is possible to find in constant time (independent of n) a $y' \in Y$ such that $d(y, y') = \delta$.

Theorem 2.5. *Suppose that the Output Divisibility Condition holds. Let $\mathbf{x}$ be a vector of inputs, α be a vector of outside options and λ be an n-dimensional learning bound vector λ such that $\lambda_{\pi,\pi(t)} = \sum_{\tau=1}^{t-1} \mu_{\pi(\tau)}$. Then for $(\pi, \mathbf{y})$ to be a collaborative equilibrium it is necessary and sufficient that*

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} (n-t)\mu_{\pi(t)} \leq d(y_0, y^*).$$

Proof. **Necessity.** Let $(\pi, \mathbf{y})$ be a proposed collaborative equilibrium, and let $\mathbf{z} \in \mathcal{I}(\pi, \mathbf{y})$ be a possible vector of inferred outputs. For every t, we must have that

$$\beta^t(d(z_{\pi(t-1)}, y^*) - d(z_{\pi(t)}, y^*)) \geq \alpha_{\pi(t)}$$

$$d(z_{\pi(t-1)}, y^*) - d(z_{\pi(t)}, y^*) \geq \frac{\alpha_{\pi(t)}}{\beta^t}.$$

The worst case for player $\pi(t)$ is when player $\pi(t-1)$ learns as much as possible from prior publications and player $\pi(t)$ learns as little as possible. That is

$$d(z_{\pi(t-1)}, y^*) = d(y_{\pi(t-1)}, y^*) - \mu_{\pi(1)} - \cdots - \mu_{\pi(t-2)}$$

$$d(z_{\pi(t)}, y^*) = d(y_{\pi(t)}, y^*)$$

In this case, the equilibrium condition becomes $d(y_{\pi(t-1)}, y^*) - \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)} - d(y_{\pi(t)}, y^*) \geq \frac{\alpha_{\pi(t)}}{\beta^t}$. Letting $\delta_{\pi(t)} = d(y_{\pi(t)}, y^*)$, we have $\delta_{\pi(t)} - \delta_{\pi(t-1)} \leq -\frac{\alpha_{\pi(t)}}{\beta^t} - \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$.

Summing over all t yields $\delta_{\pi(n)} - \delta_{\pi(0)} \leq -\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} - \sum_{t=1}^{n}(n-t)\mu_{\pi(t)}$, where $\delta_{\pi(0)} = d(y_0, y^*)$ is the distance of the prior knowledge to the true answer (and can be interpreted as the "size of the pie" of credit to be allocated). Flipping the signs in the inequality, the existence of a collaborative equilibrium implies

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n}(n-t)\mu_{\pi(t)} \leq d(y_0, y^*) - \delta_{\pi(n)} \leq d(y_0, y^*).$$

Sufficiency. To prove the condition is sufficient, we need to construct $(y_1, \ldots, y_n)$ such that $(\pi, \mathbf{y})$ is a collaborative equilibrium. We construct $\mathbf{y}$ inductively as follows: let $\delta_{\pi(n)} = 0$, and for any t such that $2 \leq t \leq n$, let $\delta_{\pi(t-1)} = \delta_{\pi(t)} + \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$. Note that defining $\{\delta_{\pi(t)}\}_{t=1}^{n}$ in this way, if we set $y_{\pi(t)}$ such that $d(y_{\pi(t)}, y^*) = \delta_{\pi(t)}$ then for all $t \geq 2$ we have

$$d(y_{\pi(t-1)}, y^*) - d(y_{\pi(t)}, y^*) = \delta_{\pi(t-1)} - \delta_{\pi(t)} = \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$$

$$\beta^t((d(y_{\pi(t-1)}, y^*) - \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}) - d(y_{\pi(t)}, y^*)) = \alpha_{\pi(t)}$$

Since for any inferred outcome $z_{\pi(t-1)}$ we have $d(z_{\pi(t-1)}, y^*) \geq d(y_{\pi(t-1)}, y^*) - \lambda_{\pi,\pi(t-1)} = d(y_{\pi(t-1)}, y^*) - \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$ and $d(z_{\pi(t)}, y^*) \leq d(y_{\pi(t)}, y^*)$ we conclude that

$$\beta^t(d(z_{\pi(t-1)}, y^*) - d(z_{\pi(t)}, y^*)) \geq \alpha_{\pi(t)}$$

for all $t \geq 2$.

Finally, we need to check that player $\pi(1)$ is incentivized to collaborate. Define $\delta_{\pi(0)} = d(y_0, y^*)$. Note that player $\pi(1)$ publishes first, so she cannot learn anything from previous publications. She will be incentivized to publish if

$$\beta(d(y_0, y^*) - \delta_{\pi(1)}) \geq \alpha_{\pi(1)}.$$

This condition holds when

$$d(y_0, y^*) \geq \frac{\alpha_{\pi(1)}}{\beta} + \delta_{\pi(1)}.$$

Replacing $\delta_{\pi(t-1)} = \delta_{\pi(t)} + \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$ iteratively, we get that player $\pi(1)$ is incentivized to collaborate if and if

$$d(y_0, y^*) \geq \sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} (n-t)\mu_{\pi(t)}$$

which is guaranteed by assumption. □

2.5 The polynomial-time mechanism

We show a polynomial-time mechanism when learning bounds are given by a *n-dimensional* vector.

Theorem 2.6. *If the sufficient conditions for existence of equilibria are satisfied (as specified in Theorem 2.5), then there exists a polynomial-time mechanism* SHARE-DATA $: X \times A \times \Lambda_1$ *that, given inputs* $(\mathbf{x}, \alpha, \mu)$*, outputs a collaborative equilibrium* $(\pi, \mathbf{y})$ *if such an equilibrium exists.*

SHARE-DATA$(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_n, \mu_1, \ldots, \mu_n)$

- Let $y = f(x_1 \ldots, x_n)$ and $\delta_0 = d(y_0, y^*)$.
- Construct a complete weighted bipartite graph $G = (L, R, E)$ where $L = [n], R = [n], E = L \times R$. For each edge (i, t), assign a weight $w(i, t) = \frac{\alpha_i}{\beta^t} + (n-t)\mu_i$
- Let M be the minimum-weight perfect matching on G. For each node $t \in R$, let $\pi(t) \in L$ be the node that it is matched with. If the weight of M is larger than δ_0, output `NONE`. Else, define $\delta_{\pi(n)} = 0$, $y_{\pi(n)} = y^*$.
- For t from n to 2:
  - Let $\delta_{\pi(t-1)} = \delta_{\pi(t)} + \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$.
  - Let $y_{\pi(t-1)}$ be such that $d(y_{\pi(t-1)}, y^*) - d(y_{\pi(t)}, y^*) = \delta_{\pi(t-1)} - \delta_{\pi(t)}$.
- Output $\omega = (\pi, (y_{\pi(1)}, \ldots, y_{\pi(n)}))$.

Proof. The fact that the algorithm runs in polynomial time is immediate, since additions, comparisons, and finding minimum weight matchings in a graph [Edm65] can all be done in (randomized) polynomial time. Finding $y_{\pi(t-1)}$ such that $d(y_{\pi(t-1)}, y^*) = \delta_{\pi(t-1)}$ can be done in constant time, by assumption.

By Theorem 2.5, a collaborative equilibrium exists if and only if there exists a permutation π such that

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} (n-t)\mu_{\pi(t)} \leq d(y_0, y^*).$$

Note that our algorithm constructs a complete bipartite graph $G = (L \cup R, E)$ where the weight on every edge is $w(i, t) = \frac{\alpha_i}{\beta^t} + (n-t)\mu_i$. A matching M on this graph induces a permutation π where, for every $t \in R$, we have $\pi(t) = i$ such that $(i, t) \in M$. The weight of such a matching is

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} (n-t)\mu_{\pi(t)}.$$

Thus, there exists a collaborative equilibrium if and only if the maximum-weight matching in G has weight less than or equal to $d(y_0, y^*)$. Note that when the weight of the maximum-matching is greater than $d(y_0, y^*)$, our algorithm outputs `NONE`, indicating such an equilibrium does not exist.

Finally, when the weight of the maximum matching is less than or equal to $d(y_0, y^*)$, the algorithm outputs $(\pi, \mathbf{y})$ where $d(y_{\pi(t-1)}, y^*) - d(y_{\pi(t)}, y^*) = \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$, so the sufficient conditions for $(\pi, \mathbf{y})$ to be an equilibrium are satisfied. □

2.6 General NP-completeness

One may wonder if we can get an efficient mechanism for learning vectors which are not *n-dimensional*. We show that this is unlikely, since finding a collaborative equilibrium is NP-complete even under a weak generalization of *n-dimensional* learning vectors.

Definition 2.7. *We say that a learning vector $\lambda \in \Lambda$ is n^2-dimensional if there exists a non-negative matrix $\{\mu_{ij}\}_{i,j=1}^n$ such that $\lambda_{\pi,\pi(t)} = \sum_{\tau=1}^{t-1} \mu_{\pi(t),\pi(\tau)}$. We denote by $\Lambda_2 \subset \Lambda$ the set of all n^2-dimensional learning vectors.*

When λ is an n^2-*dimensional* learning vector, the amount that player $\pi(t)$ learns from $\pi(\tau)$'s output is bounded above by $\mu_{\pi(t),\pi(\tau)}$. Thus, the total amount that player $\pi(t)$ learns from all prior outputs is $\sum_{\tau=1}^{t-1} \mu_{\pi(t),\pi(\tau)}$. The corresponding necessary condition for a collaborative equilibrium is that there is a permutation π such that

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} \sum_{s>t} \mu_{\pi(s),\pi(t)} \leq d(y_0, y^*).$$

We show that even checking whether this condition holds is NP-complete.

Theorem 2.8. *Given inputs y_0,α and $\{\mu_{ij}\}_{i,j=1}^n$, it is NP-complete to decide whether there exists π such that*

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} \sum_{s>t} \mu_{\pi(s),\pi(t)} \leq d(y_0, y^*).$$

Proof. It is clear that the problem is in NP, since we can always guess a permutation π and check in polynomial time whether the condition holds.

To show that the problem is NP-hard, we reduce it to the *minimum weighted feedback arc set problem*. The unweighted version of this problem was shown to be NP-complete by Karp [Kar72], and the weighted version is also NP-complete [ENSS95].

> Minimum-Weight-Feedback-Arc-Set
>
> INPUTS: A graph $G = (V, E)$ and a weight function $w : E \to \mathbb{R}_{\geq 0}$, a threshold $\gamma \in \mathbb{R}_{\geq 0}$.
>
> OUTPUT: Whether or not there exists a set $S \subset E$ of edges which intersects every cycle of G and has weight less than γ.

All that we need to show is that, given a graph G, a set S of edges is a feedback arc set if and only if there exists a permutation π of the vertices of V such that $S = \{(\pi(t), \pi(s)) \in E : s < t\}$.

To see this, note that if π is a permutation and $S = \{(\pi(t), \pi(s)) \in E : s < t\}$ then the set S intersects every cycle of G. This is because, if $C = \{(\pi(i_1), \pi(i_2)), (\pi(i_2), \pi(i_3), \ldots, (\pi(i_k), \pi(i_1))\}$ is a cycle in G, then there must exist s, t such that $s < t$ and $(\pi(t), \pi(s)) \in C$, so S intersects C. Thus, S is a feedback arc set.

Conversely, if S is a feedback arc set, then $G' = (V, E - S)$ is a directed acyclic graph, and we can induce an ordering π on V following topological sort. Any edge $(\pi(t), \pi(s)) \in E - S$ must satisfy $t < s$. Thus, any edge $(\pi(t), \pi(s))$ where $s < t$ must be in S. Thus, given π from the topological sort, we must have $S \supset \{(\pi(t), \pi(s)) \in E : s < t\}$. Since weights are non-negative, the minimal feedback arc set S^* will correspond to a permutation π^* such that $S^* = \{(\pi^*(t), \pi^*(s)) \in E : s < t\}$.

We show how to reduce Minimum-Weight-Feedback-Arc-Set to our problem. Given $G = (V, E)$, $w : E \to \mathbb{R}_{\geq 0}$ and $t \in \mathbb{R}_{\geq 0}$, let $d(y_0, y^*) = \gamma$, $\alpha = 0$, and $\mu_{ij} = w(i, j)$ if $(i, j) \in E$ and $\mu_{ij} = 0$ otherwise.

Suppose there exists a permutation π such that

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} \sum_{s>t} \mu_{\pi(s),\pi(t)} \leq d(y_0, y^*).$$

Plugging in our choices of $\alpha, \mu_{ij}, d(y_0, y^*)$, this becomes

$$\sum_{(\pi(s),\pi(t)) \in E : s>t} w(\pi(s), \pi(t)) \leq \gamma.$$

Since the set $S = \{(\pi(s), \pi(t)) \in E : s > t\}$ is a feedback arc set, we have that there exists a feedback arc set with weight less than γ.

Conversely, assume no such permutation π exists. That is,

$$\sum_{(\pi(s),\pi(t)) : s>t} \mu_{\pi(s),\pi(t)} > d(y_0, y^*)$$

for all permutations π. Note that whether s comes before t or vice-versa does not matter, since this inequality holds for all permutations. Thus, we can also write $\sum_{(\pi(s),\pi(t)) : s<t} \mu_{\pi(s),\pi(t)} > d(y_0, y^*)$ for all permutations π. From the argument above, the minimum weight feedback arc set S^* induces a permutation π^* such that $S^* = \{(\pi^*(t), \pi^*(s)) \in E : s < t\}$. The weight of S^* is

$$\sum_{(\pi^*(s),\pi^*(t)) \in E : s<t} w(\pi^*(s), \pi^*(t)) = \sum_{(\pi^*(s),\pi^*(t)) : s<t} \mu_{\pi^*(s),\pi^*(t)} > d(y_0, y^*) = \gamma.$$

Thus, there does not exist a feedback arc set with weight less than or equal to γ.

We conclude that if we can efficiently check whether

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} \sum_{s>t} \mu_{\pi(s),\pi(t)} \leq d(y_0, y^*),$$

then we can efficiently check whether there exists a feedback arc set S with weight less than γ. Thus, the feedback arc set problem reduces to ours, and our problem is NP-complete. □

We have shown that in our model of scientific collaboration, it can indeed be very beneficial to *all parties involved* to collaborate under certain ordering functions, and such beneficial collaboration outcomes can be efficiently computed under certain realistic conditions (but probably not in the general case).

2.7 The discrete case: outputs as sets of facts

In our model as described so far, the distance metric d is real-valued, which makes the Output Divisibility Condition easy to satisfy. We remark that many of our results will also apply when distances can be discrete. One important category of data-driven collaboration with discrete distances is the case where outputs are *sets* of findings: for example, in medical research, they could be sets of gene loci that are correlated with a given disease. More concretely, let Ψ be a finite set of possible findings. Let $Y^* = f(x_1, ..., x_n)$ be the set of all findings that are obtained with the given data $x_1, \ldots, x_n$. The set of outputs is the set $\Psi(Y^*)$ of all possible subsets of Y^* (note that this set of outputs depends on Y^*). For any possible output set $S \subset Y^*$, we define the distance from S to Y^* as $d(S, Y^*) = |Y^* - S|$.

Observe, however, that the Output Divisibility Condition does not hold here. Namely, it is not necessarily possible to efficiently compute $y_{\pi(t-1)}$ such that $d(y_{\pi(t-1)}, y^*) - d(y_{\pi(t)}, y^*) = \delta$ for arbitrary real δ, as required by the mechanism SHARE-DATA. Therefore, our earlier results cannot be applied directly. Nonetheless, under certain conditions outlined below, our mechanism can address the discrete setting too.

In the discrete model, the extra reward from a new publication is always an integer because it is the cardinality of a set of findings. It is thus natural to assume that α_i, μ_i are integers, since they are, respectively, the number of findings that player i can discover and publish on her own (without collaborating), and the number of extra findings that players can learn from player i's publication, given their own information.[7] In this case, if we restrict β to be of the form $\beta = \frac{1}{k}$ for some integer $k \geq 1$, then we have that

$$\delta_{\pi(t-1)} - \delta_{\pi(t)} = \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{\tau=1}^{t-1} \mu_{\pi(\tau)}$$

is an integer, and we can find (if an equilibrium exists), a $y_{\pi(t-1)}$ such that $d(y_{\pi(t-1)}, y^*) - d(y_{\pi(t)}, y^*) = \delta_{\pi(t-1)} - \delta_{\pi(t)}$. The analysis of our mechanism in this setting is very similar to the analysis given in Sections 2.3-2.6; full details are given in Appendix A.

3 Ordered MPC

We introduce formal definitions of ordered MPC and associated notions of fairness and ordered output delivery, and give protocols that realize these notions. Our definitions build upon the standard security notion[8] for traditional MPC, which is described formally in Appendix B.

Notation. For a finite set A, we will write $a \leftarrow A$ to denote that a is drawn uniformly at random from A. For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, 2, \ldots, n\}$. The operation $\oplus$ stands for exclusive-or. The relation $\overset{c}{\approx}$ denotes computational indistinguishability. $\mathsf{negl}(n)$ denotes a negligible function in n, and $\mathsf{poly}(n)$ denotes a polynomial in n. An *efficient* algorithm is one which runs in probabilistic polynomial time (PPT). $\circ$ denotes function composition, and for a function f, we write f^t to denote $\underbrace{f \circ f \circ \cdots \circ f}_{t}$.

Throughout this work, we consider computationally bounded (rushing) adversaries in a synchronous complete network, and we assume the players are honest-but-curious, since any protocol secure in the presence of honest-but-curious players can be transformed into a protocol secure against malicious players [GMW87].

3.1 Definitions

Let f be an arbitrary n-ary function and p be an n-ary function that outputs permutation $[n] \to [n]$. An ordered MPC protocol is executed by n parties, where each party $i \in [n]$ has a private input $x_i \in \{0,1\}^*$, who wish to securely compute $f(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \in (\{0,1\}^*)^n$ where y_i is the output of party i. Moreover, the parties are to receive their outputs in a particular *ordering* dictated by $p(x_1, \ldots, x_n) = \pi \in ([n] \to [n])$. That is, for all $i < j$, party $\pi(i)$ must receive his output

[7] Of course, if we assume they are integers, we are blocking the possibility that the players have uncertainty over how many gene loci they can publish on their own or how much they can learn from others, which could lead to expected values of α_i and μ_i which are not integers.

[8] Note that throughout this work, we use "stand-alone" security notions rather than "universally composable" ones.

before party $\pi(j)$ receives her output. Note that the output ordering π is *data-dependent*, as p is a function of the parties' inputs.

Following [GMW87], the security of ordered MPC with respect to a functionality f and permutation function p is defined by comparing the execution of a protocol to an ideal process $\mathcal{F}_{\text{Ordered-MPC}}$ where the outputs and ordering are computed by a trusted party who sees all the inputs. An ordered MPC protocol F is considered to be secure if for any real-world adversary $\mathcal{A}$ attacking the real protocol F, there exists an ideal adversary $\mathcal{S}$ in the ideal process whose outputs (views) are indistinguishable from those of $\mathcal{A}$. Note that this implies that no player learns more information about the other players' inputs than can be learned from his own input and output, *and his own position in the output delivery order*. The latter condition is important because the output ordering depends on parties' private inputs, and thus we require that the protocol reveals as little information as possible about the ordering.

Many rather than one view In the ordered MPC setting, the ideal adversary $\mathcal{S}$ and the real-world adversary $\mathcal{A}$ each output a view after each output phase. This is in contrast to standard MPC, where the adversaries simply output one view at the end of the protocol execution.

IDEAL FUNCTIONALITY $\mathcal{F}_{\text{Ordered-MPC}}$

In the ideal model, a trusted third party T is given the inputs, computes the functions f, p on the inputs, and outputs to each player i his output y_i in the order prescribed by the ordering function. In addition, we model an ideal process adversary $\mathcal{S}$ who attacks the protocol by corrupting players in the ideal setting.

Public parameters. $\kappa \in \mathbb{N}$, the security parameter; $n \in \mathbb{N}$, the number of parties; $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$, the function to be computed; and $p : (\{0,1\}^*)^n \to ([n] \to [n])$, the ordering function.

Private parameters. Each player $i \in [n]$ holds a private input $x_i \in \{0,1\}^*$.

1. INPUT. Each player i sends his input x_i to T.
2. COMPUTATION. T computes $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ and $\pi = p(x_1, \ldots, x_n)$.
3. OUTPUT. The output proceeds in n sequential output rounds. At the start of the j^{th} round, T sends the output value $\mathsf{out}_{i,j}$ to each party i, where $\mathsf{out}_{j,j} = y_{\pi(j)}$ and $\mathsf{out}_{i,j} = \perp$ for all $i \neq j$. When party $\pi(j)$ receives his output, he responds to T with the message ack. (The players who receive $\perp$ are not expected to respond.) Upon receipt of the ack, T proceeds to the $(j+1)^{th}$ round – or, if $j = n$, then the protocol terminates.
4. OUTPUT OF VIEWS. At each output round, after receiving his message from T, each party produces an output, as follows. Each uncorrupted party i outputs y_i if he has already received his output, or $\perp$ if he has not. Each corrupted party outputs $\perp$. Additionally, the adversary $\mathcal{S}$ outputs an arbitrary function of the information that he has learned during the execution of the ideal protocol.

   Let the output of party i in the j^{th} round be denoted by $\mathscr{V}_{i,j}$, and let the view outputted by $\mathcal{S}$ in the j^{th} round be denoted by $\mathscr{V}_{\mathcal{S},j}$. Let $\mathscr{V}^{\mathsf{ideal}}_{\text{Ordered-MPC}}$ denote the collection of all views for all output rounds:

$$\mathscr{V}^{\mathsf{ideal}}_{\text{Ordered-MPC}} = ((\mathscr{V}_{\mathcal{S},1}, \mathscr{V}_{1,1}, \ldots, \mathscr{V}_{n,1}), \ldots, (\mathscr{V}_{\mathcal{S},n}, \mathscr{V}_{1,n}, \ldots, \mathscr{V}_{n,n}))\,.$$

   (If the protocol is terminated early, then views for rounds which have not yet been started are taken to be $\perp$.)

Definition 3.1 (Security)**.** *A multi-party protocol F is said to securely realize $\mathcal{F}_{\text{Ordered-MPC}}$, if the following conditions hold.*

1. *The protocol description specifies n check-points $C_1, \ldots, C_n$ corresponding to events during the execution of the protocol.*

2. *Take any* PPT *adversary $\mathcal{A}$ who corrupts a subset of players $S \subset [n]$, and let $V_{\mathcal{A},j}$ be the result of an arbitrary function A applies to his view after each check-point C_j. Let*

$$V_{\mathcal{A}}^{\mathsf{real}} = ((V_{\mathcal{A},1}, V_{1,1}, \ldots, V_{n,1}), \ldots, (V_{\mathcal{A},n}, V_{1,n}, \ldots, V_{n,n}))$$

be the tuple consisting of the adversary $\mathcal{A}$'s outputted views along with the outputs of the real-world parties as specified in the ideal functionality description. Then there is a PPT *ideal adversary $\mathcal{S}$ which, attacking $\mathcal{F}_{\text{Ordered-MPC}}$ by corrupting the same subset S of players, can output views $\mathcal{V}_{\mathcal{S},j}$ such that for each $j \in [n]$, it holds that $\mathcal{V}_{\mathcal{S},j} \overset{c}{\approx} V_{\mathcal{A},j}$.*

In the context of ordered MPC, the standard guaranteed output delivery notion is insufficient. Instead, we define *ordered output delivery*, which requires in addition that all parties receive their outputs in the order prescribed by p.

Definition 3.2 (Ordered output delivery)**.** *An ordered MPC protocol satisfies* ordered output delivery *if for any inputs $x_1, \ldots, x_n$, functionality f, and ordering function p, it holds that all parties receive their outputs before protocol termination, and moreover, if $\pi(i) < \pi(j)$, then party i receives his output before party j receives hers, where $\pi = p(x_1, \ldots, x_n)$.*

We also define a natural relaxation of the fairness requirement for ordered MPC, called *prefix-fairness*. Although it is known that fairness is impossible for general functionalities in the presence of a dishonest majority, we show in the next subsection that prefix-fairness can be achieved even when a majority of parties are corrupt. We emphasize that this notion relaxes *only* the fairness requirement: that is, prefix-fair protocols satisfy full privacy (and correctness) guarantees.

Definition 3.3 (Prefix-fairness)**.** *An ordered MPC protocol is* prefix-fair *if for any inputs $x_1, \ldots, x_n$, it holds that the set of parties who have received their outputs at the time of protocol termination (or abortion) is a prefix of $(\pi(1), \ldots, \pi(n))$, where $\pi = p(x_1, \ldots, x_n)$ is the permutation induced by the inputs.*

Prefix-fairness can be useful, for example, in settings where it is more important for one party to receive the output than the other; or where there is some prior knowledge about the trustworthiness of each party (so that more trustworthy parties may receive their outputs first).

3.2 Construction

Ordered MPC is achievable by using standard protocols for general MPC, as described in Protocol 1 below. The protocol has n sequential output phases, so that the n outputs can be issued in order. A subtle point is that because the ordering is a function of the input data, knowledge of the ordering may reveal information about the input data. Thus, we have to "mask" the output values such that each party only learns the minimal possible amount of information about the ordering: namely, his own position in the ordering.

PROTOCOL 1: ORDERED MPC

Public parameters. $\kappa \in \mathbb{N}$, the security parameter; $n \in \mathbb{N}$, the number of parties; $k \in \mathbb{N}$, an upper bound on the number of corrupt parties; $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$, the function to be computed; and $p : (\{0,1\})^* \to ([n] \to [n])$, the ordering function.

1. **Computing shares of $(\pi, \mathbf{y})$:** Using any general secure MPC protocol (such as [GMW87]) on inputs $x_1, \ldots, x_n$, jointly compute a k-out-of-n secret-sharing[9]of $(\pi, \mathbf{y})$ where $\mathbf{y} = (y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ and $\pi = p(x_1, \ldots, x_n)$ is a permutation of $[n]$. At the end of this step, each player possesses a share of the outputs $\mathbf{y} = (y_1, \ldots, y_n)$ and of the permutation π.

2. **Outputting $y_1, \ldots, y_n$ in n phases:** In the i^{th} output phase, player $\pi^{-1}(i)$ will learn his output. In phase i the parties run a new instance of a general secure MPC protocol such that:

   - Player j's inputs to the protocol are: the shares of $\mathbf{y}$ and π that he got in step 1, and a random string $r_{i,j}$.
   - The functionality computed is:

     `for` j `from 1 to` n`:` `if` $\pi(j) = i$ `then` $z_{i,j} := y_j \oplus r_{i,j}$ `else` $z_{i,j} = \perp \oplus r_{i,j}$.
     `output` $z_i = (z_{i,1}, \ldots, z_{i,n})$.

     where $\perp$ is a special string that lies outside the output domain.
   - To recover his output, each player j computes $y'_{i,j} = z_{i,j} \oplus r_{i,j}$ for all i. By construction, there is exactly one $i \in [n]$ for which $y'_{i,j} \neq \perp$, and that is equal to the output value y_j for player j.

Check-points. There are n check-points. For $i \in [n]$, the check-point C_i is at the end of the i^{th} output phase, when z_i is learned by all players.

In case of abort. When running the protocol for the honest majority setting, the honest players continue until the end of the protocol regardless of other players' behavior. When running the protocol for dishonest majority, if any party aborts in an output phase[10], then the honest players do not continue to the next phase.

In proving the security of Protocol 1, we refer to the security of modular composition of general protocols shown by [Can00], Theorem 5.

Theorem 3.4. *Protocol 1 securely realizes $\mathcal{F}_{\text{Ordered-MPC}}$.*

Proof. Let ρ_0 denote the general MPC protocol execution in step 1, and let ρ_i be the general MPC protocol execution in phase i of step 2, for $i \in [n]$. For $j \in [n]$, let the protocol π_j be the concatenation of the protocols $\rho_0, \ldots, \rho_j$. To prove security at each check-point, it is sufficient to prove that π_j satisfies security for all $j \in [n]$: in other words, that the view outputted by any

[9]The standard definition of a secret-sharing scheme can be found in Appendix C.

[10]Each output phase consists of an execution of the underlying general MPC protocol. If a party aborts at any time during (and before the end of) the execution of the underlying general MPC protocol, this fact will be detected by all honest parties by the end of the phase.

adversary in the real protocol execution at check-point j can be simulated in the ideal execution. Finally, for all $j \in [n]$, the security of π_j follows directly from the security of modular composition of general protocols ([Can00], Theorem 5). □

Theorem 3.5. *In the case of honest majority, Protocol 1 achieves fairness. In the dishonest majority setting, prefix-fairness is achieved.*

Proof. Fairness holds in the honest majority case, since the honest players complete all output phases, and the shares that the honest players hold are sufficient to reconstruct each output y_i (recall that the secret-sharing threshold k is $\lceil n/2 \rceil$ in the honest majority case). In the dishonest majority setting, prefix-fairness holds since for all $i \in [n]$, *all* n shares are required in order to reconstruct the output $y_{\pi(i)}$ in output phase i, and

- if the corrupt parties do not abort during the i^{th} output phase, then by the security of Protocol 1, the output $y_{\pi(i)}$ associated with the i^{th} output phase is delivered correctly to party i;
- if the corrupt parties abort during the i^{th} output phase, then no outputs $y_{\pi(j)}$ for $j > i$ will be learned by any player, since the honest parties will not execute subsequent output phases. □

4 Timed-delay MPC

In this section, we implementing *time delays* between different players receiving their outputs. The model is exactly as before, with n players wishing to compute a function $f(x_1, \ldots, x_n)$ in an ordering prescribed by $p(x_1, \ldots, x_n)$ – except that now, there is an additional requirement of a delay after each player receives his output and before the next player receives her output. To realize the timed-delay MPC functionality, we make use of time-lock and time-line puzzles, which are introduced in section 4.4.

4.1 Ideal functionality with time delays

We measure time delay in units of computation, rather than seconds of a clock: that is, rather than making any assumption about global clocks (or synchrony of local clocks)[11], we measure time by the *evaluations of a particular function* (on random inputs), which we call the *clock function*.

IDEAL FUNCTIONALITY $\mathcal{F}_{\text{Timed-Delay-MPC}}$

In the ideal model, a trusted third party T is given the inputs, computes the functions f, p on the inputs, and outputs to each player i his output y_i in the order prescribed by the ordering function. Moreover, T imposes delays between the issuance of one party's output and the next. In addition, we model an ideal process adversary $\mathcal{S}$ who attacks the protocol by corrupting players in the ideal setting.

[11] A particular issue that arises when considering a clock-based definition is that it is not clear that we can reasonably assume or prove that clocks are in synchrony between the real and ideal world – but this seems necessary in order to prove security by simulation in the ideal functionality.

We remark that if one is happy to assume the existence of a global clock (or synchrony of local clocks), then there are other ways to implement timed-delay MPC which sidestep many of the issues inherent in the arguably more realistic model where clocks may not be perfectly synchronized between different (adversarial) parties. One example is the "Bitcoin model" where the assumption is that the Bitcoin block-chain can serve as a global clock: in this model, existing protocols such as [BK14] implement some time-delays in MPC, and it seems likely that such protocols can be adapted to achieve our notion of timed-delay MPC.

Public parameters. $\kappa \in \mathbb{N}$, the security parameter; $n \in \mathbb{N}$, the number of parties; $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$, the function to be computed; $p : (\{0,1\}^*)^n \to ([n] \to [n])$, the ordering function; and $G = G(\kappa) \in \mathbb{N}$, the number of time-steps between the issuance of one party's output and the next.

Private parameters. Each player $i \in [n]$ holds a private input $x_i \in \{0,1\}^*$.

1. INPUT. Each player i sends his input x_i to T. If, instead of sending his input, any player sends the message quit, then the computation is aborted.
2. COMPUTATION. T computes $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ and $\pi = p(x_1, \ldots, x_n)$.
3. OUTPUT. The output proceeds in n sequential output phases. At each phase j, T waits for G time-steps, then sends the j^{th} output, $y_{\pi(j)}$, to party $\pi(j)$.
4. OUTPUT OF VIEWS. At the end of each output phase, each party produces an output as follows. Each uncorrupted party i outputs y_i as his view if he has already received his output, or $\perp$ if he has not. Each corrupted party outputs $\perp$. Additionally, the adversary $\mathcal{S}$ outputs an arbitrary function of the information that he has learned during the execution of the ideal protocol, after each check-point.

   Let the output of party i in the j^{th} round be denoted by $\mathscr{V}_{i,j}$, and let the view outputted by $\mathcal{S}$ in the j^{th} round be denoted by $\mathscr{V}_{\mathcal{S},j}$. Let $\mathscr{V}^{\mathsf{ideal}}_{\text{Timed-Delay-MPC}}$ denote the collection of all views for all output phases:

$$\mathscr{V}^{\mathsf{ideal}}_{\text{Timed-Delay-MPC}} = ((\mathscr{V}_{\mathcal{S},1}, \mathscr{V}_{1,1}, \ldots, \mathscr{V}_{n,1}), \ldots, (\mathscr{V}_{\mathcal{S},n}, \mathscr{V}_{1,n}, \ldots, \mathscr{V}_{n,n}))\,.$$

For an algorithm $\mathcal{A}$, let the run-time[12] of $\mathcal{A}$ on input inp be denoted by $\mathsf{time}_{\mathcal{A}}(\mathsf{inp})$. If $\mathcal{A}$ is probabilistic, the run-time will be a distribution over the random coins of $\mathcal{A}$. Note that the exact run-time of an algorithm will depend on the underlying computational model in which the algorithm is run. In this work, all algorithms are assumed to be running in the same underlying computational model, and our definitions and results hold regardless of the specific computational model employed.

Definition 4.1 (Security)**.** *A multi-party protocol F (with parameters κ, n, f, p, G) is said to securely realize $\mathcal{F}_{\text{Timed-Delay-MPC}}$, if the following conditions hold.*

1. *The protocol description specifies n check-points $C_1, \ldots, C_n$ corresponding to events during the execution of the protocol.*
2. *There exists a "clock function" g such that between any two consecutive checkpoints C_i, C_{i+1} during an execution of F, any one of the parties (in the real world) must be able to locally run $\Omega(G)$ sequential evaluations of g on random inputs. g may also be a* protocol *(involving $n' \leq n$ parties) rather than a function, in which case we instead require that any subset consisting of n' parties must be able to run $\Omega(G)$ sequential executions of g (on random inputs) over the communication network being used for the main multi-party protocol F. Then, we say that F is "clocked by g".*
3. *Take any* PPT *adversary $\mathcal{A}$ attacking the protocol F by corrupting a subset of players $S \subset [n]$, which outputs an arbitrary function $V_{\mathcal{A},j}$ of the information that it has learned in the protocol*

[11] The use of checkpoints is introduced to capture the views of players and the adversary at intermediate points in protocol execution.

[12] Run-time is, naturally, measured in "CPU time" (i.e. the number of instructions executed in the underlying computational model) as opposed to real-world "clock time".

execution after each check-point C_j. Let

$$V_{\mathcal{A}}^{\mathsf{real}} = ((V_{\mathcal{A},1}, V_{1,1}, \ldots, V_{n,1}), \ldots, (V_{\mathcal{A},n}, V_{1,n}, \ldots, V_{n,n}))$$

be the tuple consisting of the adversary $\mathcal{A}$'s outputted views along with the views of the real-world parties as specified in the ideal functionality description. Then there is a PPT *ideal adversary $\mathcal{S}$ which, attacking $\mathcal{F}_{\text{Timed-Delay-MPC}}$ by corrupting the same subset S of players, can output views $\mathscr{V}_{\mathcal{S},1}, \ldots, \mathscr{V}_{\mathcal{S},n}$ (at check-points $C_1, \ldots, C_n$ respectively) such that for each $j \in [n]$, it holds that*

$$|\Pr[D(\mathscr{V}_{\mathcal{S},j}, \mathscr{V}_{1,j}, \ldots, \mathscr{V}_{n,j}) = 1] - \Pr[D(V_{\mathcal{A},j}, V_{1,j}, \ldots, V_{n,j}) = 1]| \leq \mathsf{negl}(\kappa),$$

for any distinguisher D such that

$$\Pr_{\vec{v} \leftarrow \mathcal{V}}[\mathsf{time}_D(\vec{v}) \leq j \cdot \mathsf{time}_{\mathcal{G}}()] = 1/\mathsf{poly}(\kappa),$$

when $\mathcal{V}$ is the distribution of views outputted by $\mathcal{A}$ or $\mathcal{S}$ (that is, for $\mathcal{V} \in \{(\mathscr{V}_{\mathcal{S},j}, \mathscr{V}_{1,j}, \ldots, \mathscr{V}_{n,j}), (V_{\mathcal{A},j}, V_{1,j}, \ldots, V_{n,j})\}$), and $\mathcal{G}$ is the algorithm that computes the function g sequentially on G random inputs.

4.2 Realizing timed-delay MPC with dummy rounds

A simple protocol for securely realizing timed-delay MPC is to implement delays by running G "dummy rounds" of communication in between issuing outputs to different players.

PROTOCOL 2: TIMED-DELAY MPC WITH DUMMY ROUNDS

Public parameters. $\kappa \in \mathbb{N}$, the security parameter; $n \in \mathbb{N}$, the number of parties; $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$, the function to be computed; $p : (\{0,1\})^* \to ([n] \to [n])$, the ordering function; and $G = \mathsf{poly}(\kappa)$, the number of time-steps between the issuance of one party's output and the next.

1. **Computing shares of $(\pi, \mathbf{y})$:** Using any general secure MPC protocol (such as [GMW87]), jointly compute an k-out-of-n secret-sharing[13]of $(\pi, \mathbf{y})$ where $\mathbf{y} = (y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ and permutation $\pi = p(x_1, \ldots, x_n)$ on the players' inputs. At the end of this step, each player possesses a share of the outputs $\mathbf{y} = (y_1, \ldots, y_n)$ and of the permutation π.

2. **Outputting $y_1, \ldots, y_n$ in n phases:** The outputs will occur in n phases: in the i^{th} phase, player $\pi^{-1}(i)$ will learn his output. In each phase, the players first run G "dummy rounds" of communication. A dummy round is a "mini-protocol" defined as follows (let this mini-protocol be denoted by g_{dum}):

   - each player initially sends the message challenge to every other player;
   - each player responds to each challenge he receives with a message response.

   In each phase, after the dummy rounds have been completed, the parties will run a new instance of a general secure MPC protocol. In phase i:

- Player j's inputs to the protocol are: the shares of $\mathbf{y}$ and π that he got in step 1, and a fresh random string $r_{i,j}$.
- The functionality computed in each phase $i \in [n]$ is:

  `for` j `from 1 to` n`:` `if` $\pi(j) = i$ `then` $z_{i,j} := y_j \oplus r_{i,j}$ `else` $z_{i,j} = \perp \oplus r_{i,j}$.
  `output` $z_i = (z_{i,1}, \ldots, z_{i,n})$.

  where $\perp$ is a special string that lies outside the output domain.
- To recover his output, each player j computes $y'_{i,j} = z_{i,j} \oplus r_{i,j}$ for all i. By construction, there is exactly one $i \in [n]$ for which $y'_{i,j} \neq \perp$, and that is equal to the output value y_j for player j.

Check-points. There are n check-points. For $i \in [n]$, the check-point C_i is at the end of the i^{th} output phase, when z_i is learned by all players.

In case of abort. When running the protocol for the honest majority setting, the honest players continue until the end of the protocol regardless of other players' behavior. When running the protocol for dishonest majority, if any party aborts in an output phase[14], then the honest players do not continue to the next phase.

Theorem 4.2. *In the presence of honest majority, Protocol 2 securely realizes* $\mathcal{F}_{\text{Timed-Delay-MPC}}$ *clocked by* g_{dum}.

Proof. Let $\mathcal{A}$ be any PPT adversary attacking Protocol 2 by corrupting a subset of players $S \subset [n]$, and let

$$V_{\mathcal{A}}^{\mathsf{real}} = ((V_{\mathcal{A},1}, V_{1,1}, \ldots, V_{n,1}), \ldots, (V_{\mathcal{A},n}, V_{1,n}, \ldots, V_{n,n}))$$

be the tuple consisting of the adversary $\mathcal{A}$'s outputted views along with the views of the real-world parties (as specified in the description of $\mathcal{F}_{\text{Timed-Delay-MPC}}$). In order to show that condition 3 of the security definition (Definition 4.1) holds, we need to show that there is a PPT ideal adversary $\mathcal{S}$ which, given access to $\mathcal{F}_{\text{Timed-Delay-MPC}}$ and corrupting the same subset S of players, can output views $\mathscr{V}_{\mathcal{S},j}$ such that $V_{\mathcal{A}}^{\mathsf{real}} \overset{c}{\approx} \mathscr{V}_{\text{Timed-Delay-MPC}}^{\mathsf{ideal}}$.

Recall that the adversary's view can be any function of the inputs of the corrupt parties and the messages that the corrupt parties see during the protocol execution. In particular, it is sufficient to show that there is an ideal adversary $\mathcal{S}$ which can output views $\mathscr{V}_{\mathcal{S},j}$ which are indistinguishable from the transcript of all the messages that the corrupt parties see during the real protocol execution.

Protocol 2 consists of sequential executions of the underlying general MPC protocol and the mini-protocol g_{dum}. When the mini-protocol executions are removed from Protocol 2, the resulting protocol is identical to Protocol 1. Hence, by Theorem 3.4, there is an ideal adversary $\mathcal{S}'$ which, given access to $\mathcal{F}_{\text{Timed-Delay-MPC}}$ and corrupting the same subset S of players, can output views $\mathscr{V}_{\mathcal{S}',j}$ such that which are indistinguishable from the transcript of all the messages that the corrupt parties see *during the* $n+1$ *executions of the underlying general MPC protocol* within Protocol 2. The only

[13] For the honest majority setting, we set $k = \lceil n/2 \rceil$. For the dishonest majority setting, $k = n$.

[14] Each output phase consists of an execution of the underlying general MPC protocol preceded by G dummy rounds. If a party aborts before the completion of the G dummy rounds, this fact will be detected by all parties in the dummy round in which the abort happens, because every party is supposed to communicate with every other party in each dummy round. If a party aborts at any time during (and before the end of) the execution of the underlying general MPC protocol, this fact will be detected by all honest parties by the end of the phase.

other messages that are sent in Protocol 2 are the "dummy" messages challenge and response, which are fixed messages that do not depend on the players' inputs. In fact, the transcript of an execution of g_{dum} is a deterministic sequence of challenge and response. It follows that there exists an ideal adversary $\mathcal{S}$ which, by calling $\mathcal{S}'$ and adding the deterministic transcript corresponding to each execution of g_{dum}, can output views $\mathscr{V}_{\mathcal{S},j}$ which are indistinguishable from the transcript of all the messages that the corrupt parties see during the real execution of Protocol 2.

Finally, it remains to show that condition 2 of the security definition (Definition 4.1) is satisfied. The players are literally running g over the MPC network G times in between issuing outputs, so it is clear that condition 2 holds. □

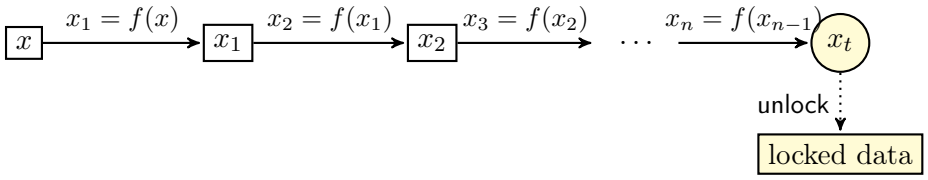
One downside of the simple solution above is that it requires all (honest) parties to be online and communicating until the last player receives his output. To address this, in Section 4.3 we propose an alternative solution based on *timed-release cryptography*, at the cost of an additional assumption that all players have comparable computing speed (within a logarithmic factor).

4.3 Realizing timed-delay MPC with time-lock puzzles

Informally, a time-lock puzzle is a primitive which allows "locking" of data, such that it will be released after a pre-specified time delay, and no earlier. Our next protocol, instead of issuing outputs to players in the clear, gives to each party his output *locked* into a time-lock puzzle; and in order to enforce the desired ordering, the delays required to unlock the puzzles are set to be an increasing sequence. We first give the definition of time-lock puzzles (in Section 4.4) then describe and prove security of our time-lock-based protocol (in Section 4.3.2).

4.3.1 Time-lock puzzles

The delayed release of data in MPC protocols can be closely linked to the problem of "timed-release crypto" in general, which was introduced by [May93] and constructed first by [RSW96] with their proposal of *time-lock puzzles*. We assume time-lock puzzles with a particular structure (that is present in all known implementations): namely, the passage of "time" will be measured by sequential evaluations of a function (TimeStep). Unlocking a t-step time-lock puzzle can be considered analogous to following a chain of t pointers, at the end of which there is a special value x_t (e.g. a decryption key) that allows retrieval of the locked data.



Definition 4.3 (Time-lock puzzle scheme)**.** *A* time-lock puzzle scheme *is a tuple of* PPT *algorithms* $T = (\mathsf{Lock}, \mathsf{TimeStep}, \mathsf{Unlock})$ *as follows:*

- $\mathsf{Lock}(1^\kappa, d, t)$ *takes parameters* $\kappa \in \mathbb{N}$ *the security parameter,* $d \in \{0,1\}^\ell$ *the data to be locked, and* $t \in \mathbb{N}$ *the number of steps needed to unlock the puzzle, and outputs a time-lock puzzle* $P = (x, t, b, a) \in \{0,1\}^n \times \mathbb{N} \times \{0,1\}^{n''} \times \{0,1\}^{n'}$ *where* $\ell, n, n', n'' = \mathsf{poly}(\kappa)$.
- $\mathsf{TimeStep}(1^\kappa, x', a')$ *takes parameters* $\kappa \in \mathbb{N}$ *the security parameter, a bit-string* $x' \in \{0,1\}^n$*, and auxiliary information* a'*, and outputs a bit-string* $x'' \in \{0,1\}^n$.

- $\mathsf{Unlock}(1^\kappa, x', b')$ *takes parameters* $\kappa \in \mathbb{N}$ *the security parameter, a bit-string* $x' \in \{0,1\}^n$*, and auxiliary information* $b' \in \{0,1\}^{n'}$*, and outputs some data* $d' \in \{0,1\}^\ell$*.*

To unclutter notation, we will sometimes omit the initial security parameter of these functions (writing e.g. simply $\mathsf{Lock}(d,t)$). We now define some auxiliary functions. For a time-lock puzzle scheme $T = (\mathsf{Lock}, \mathsf{TimeStep}, \mathsf{Unlock})$ and $i \in \mathbb{N}$, let $\mathsf{IterateTimeStep}_i^T$ denote the following function:

$$\mathsf{IterateTimeStep}^T(i,x,a) = \underbrace{\mathsf{TimeStep}(\mathsf{TimeStep}(\dots(\mathsf{TimeStep}(x,a),a)\dots),a)}_{i}.$$

Define $\mathsf{CompleteUnlock}^T$ to be the following function:

$$\mathsf{CompleteUnlock}^T((x,t,b,a)) = \mathsf{Unlock}(\mathsf{IterateTimeStep}^T(t,x,a),b),$$

that is, the function that should be used to unlock a time-lock puzzle outputted by Lock.

The following definitions formalize correctness and security for time-lock puzzle schemes.

Definition 4.4 (Correctness)**.** *A time-lock puzzle scheme* $T = (\mathsf{Lock}, \mathsf{TimeStep}, \mathsf{Unlock})$ *is* correct *if the following holds (where* κ *is the security parameter):*

$$\Pr_{(x,t,b,a)\leftarrow\mathsf{Lock}(d,t)}\left[\mathsf{CompleteUnlock}^T((x,t,b,a)) \neq d\right] \leq \mathsf{negl}(\kappa).$$

Definition 4.5 (Security)**.** *Let* $T = (\mathsf{Lock}, \mathsf{TimeStep}, \mathsf{Unlock})$ *be a time-lock puzzle scheme.* T *is* secure *if it holds that: for all* $d, d' \in \{0,1\}^\ell, t = \mathsf{poly}(\kappa)$*, if there exists an adversary* $\mathcal{A}$ *that solves the time-lock puzzle* $\mathsf{Lock}(d,t)$*, that is,*

$$\Pr_{P\leftarrow\mathsf{Lock}(d,t)}[\mathcal{A}(P) = d] = \varepsilon \text{ for some non-negligible } \varepsilon,$$

then for each $j \in [t]$*, there exists an adversary* $\mathcal{A}_j$ *such that*

$$\Pr_{P'\leftarrow\mathsf{Lock}(d',j)}\left[\mathcal{A}_j(P') = d'\right] \geq 1 - \mathsf{negl}(\kappa), \text{ and}$$

$$\Pr_{\substack{P\leftarrow\mathsf{Lock}(d,t),\\ P'\leftarrow\mathsf{Lock}(d',j)}}\left[\mathsf{time}_{\mathcal{A}}(P) \geq (t/j)\cdot\mathsf{time}_{\mathcal{A}_j}(P') \mid \mathcal{A}(P) = d\right] \geq 1 - \mathsf{negl}(\kappa).$$

4.3.2 Protocol based on time-lock puzzles

Because of the use of time-lock puzzles by different parties in the protocol that follows, we require an additional assumption that all players have comparable computing power (within a logarithmic factor).

Relative-Delay Assumption. The difference in speed of performing computations between any two parties $i, j \in [n]$ is at most a factor of $B = O(\log(\kappa))$.

PROTOCOL 3: TIMED-DELAY MPC WITH TIME-LOCK PUZZLES

Public parameters. $\kappa \in \mathbb{N}$, the security parameter; $n \in \mathbb{N}$, the number of parties; $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$, the function to be computed; $p : (\{0,1\})^* \to ([n] \to [n])$, the ordering function; $B = O(\log(\kappa))$, the maximum factor of difference between any two parties' computing power; $G = \mathsf{poly}(\kappa)$, the number of time-steps between the issuance of one party's output and the next; and $T = \{\mathsf{Lock}, \mathsf{TimeStep}, \mathsf{Unlock}\}$ a time-lock puzzle scheme.

INPUTS. Each party i has input x_i.

PROTOCOL STEPS. Let $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ and $\pi = p(x_1, \ldots, x_n)$. Define $t_1 = 1$ and $t_{i+1} = (B \cdot G + 1) \cdot t_i$ for $i \in [n-1]$. Compute $(P_1, \ldots, P_n)$, where each $P_i = (x_i, t_{\pi(i)}, a_i, b_i)$ is a time-lock puzzle computed as

$$P_i = \mathsf{Lock}(y_i \oplus r_i, t_{\pi(i)}),$$

where each r_i is a random string provided as input randomness by party i.

OUTPUTS. For each $i \in [n]$, the puzzle P_i is outputted to party i. The players all receive their respective outputs at the same time, then recovers his output y_i by solving his time-lock puzzle, and finally "unmasking" the result by XORing with his random input r_i.

Check-points. There are n check-points. For $i \in [n]$, the check-point C_i is the event of party $\pi(i)$ learning his eventual output $y_{\pi(i)}$ (i.e. when he finishes solving his time-lock puzzle).

For the following theorem, we assume that each player i uses the optimal algorithm to solve his puzzle P_i that outputs the correct answer. Without this assumption, any further protocol analysis would not make sense: there can always be a "lazy" player who willfully uses a very slow algorithm to solve his puzzle, who will as a result learn his eventual output much later in the order than he could otherwise have done. The property that we aim to achieve is that every player *could* learn his output at his assigned position in the ordering π, with appropriate delays before and after he learns his output.

Theorem 4.6. *Suppose that the Relative-Delay Assumption holds, and each player i uses the optimal algorithm to solve his puzzle P_i that outputs (with overwhelming probability) the correct answer. Then, Protocol 3 securely realizes $\mathcal{F}_{\text{Timed-Delay-MPC}}$ when there is an honest majority.*

Proof. First, we prove that condition 2 of the security definition (Definition 4.1) is satisfied. Let $\mathcal{A}_i$ denote the algorithm that party i uses to solve his time-lock puzzle, and let the time at which party i learns his answer y_i be denoted by $\tau_i = \mathsf{time}_{\mathcal{A}_i}(P_i)$. By the security of the time-lock puzzles, there exists an algorithm $\mathcal{A}'_i$ that player i could use to solve the puzzle $\mathsf{Lock}(0^\ell, 1)$ in time τ_i / t_i. Moreover, by the Relative-Delay Assumption, it holds that no player can solve the puzzle $\mathsf{Lock}(0^\ell, 1)$ more than B times faster than another player: that is, $\max_i(\tau_i/t_i) \leq B \cdot \min_i(\tau_i/t_i)$. It follows that even the slowest player (call him i^*) would be able to run t_i/B executions of $\mathcal{A}'_{i^*}$ within time τ_i, for any i.

Without loss of generality, assume that the ordering function p is the identity function. Consider any consecutive pair of checkpoints C_i, C_{i+1}. These checkpoints occur at times τ_i and τ_{i+1}, by definition. We have established that in time τ_i, player i^* can run t_i/B executions of $\mathcal{A}'_{i^*}$, and in time τ_{i+1}, he can run t_{i+1}/B executions of $\mathcal{A}'_{i^*}$. It follows that in between the two checkpoints (i.e. in time $\tau_{i+1} - \tau_i$), he can run $(t_{i+1} - t_i)/B$ executions of $\mathcal{A}'_{i^*}$. Substituting in the equation $t_{i+1} = (B \cdot G + 1) \cdot t_i$ from the protocol definition, we get that player i^* can run $G \cdot t_i$ executions of

$\mathcal{A}'_{i^*}$ between checkpoints C_i and C_{i+1}. Since $t_i \geq 1$ for all i, this means that i^* can run at least G executions of $\mathcal{A}'_{i^*}$ between *any* consecutive pair of checkpoints. Hence, condition 2 holds.

We now prove condition 3. Let $\mathcal{G}$ be the algorithm that evaluates $\mathcal{A}'_{i^*}$ sequentially G times on random inputs. It is sufficient to show that for any adversary $\mathcal{A}$ attacking the protocol by corrupting a subset $S \subset [n]$ of players, which outputs a view $V_{\mathcal{A},j}$ at each checkpoint j which is the *transcript of all messages that it has seen so far*, there is an ideal adversary $\mathcal{S}$ which outputs views $\mathscr{V}_{\mathcal{S},1}, \ldots, \mathscr{V}_{\mathcal{S},n}$ such that for any $j \in [n]$, for any distinguisher D whose run-time satisfies the conditions in Definition 4.1, item 3,

$$|\Pr[D(\mathscr{V}_{\mathcal{S},j}, \mathscr{V}_{1,j}, \ldots, \mathscr{V}_{n,j}) = 1] - \Pr[D(V_{\mathcal{A},j}, V_{1,j}, \ldots, V_{n,j}) = 1]| \leq \mathsf{negl}(\kappa).$$

Recall that there are n sequential output stages in the ideal functionality $\mathcal{F}_{\text{Timed-Delay-MPC}}$. Consider an ideal adversary $\mathcal{S}$ attacking $\mathcal{F}_{\text{Timed-Delay-MPC}}$ by corrupt a set of parties $S \subset [n]$. Let $\vec{inp}$ denote the vector of inputs and input randomness of the corrupt parties (note that these are known to $\mathcal{S}$). Take any $i \in [n]$. In the ideal protocol execution, $\mathcal{S}$ learns the following in the $\pi(i)^{th}$ output stage:

- nothing, if $i \notin S$; or
- the input value x_i, the input randomness r_i, and the eventual output y_i if $i \in S$.

Note that as a result, $\mathcal{S}$ learns $\pi(i)$ at output stage $\pi(i)$, for each $i \in S$. The delay values $t_1, \ldots, t_n$ are a fixed sequence of values independent of the parties' inputs, so they are known to $\mathcal{S}$. Thus, at each check-point $j \in [n]$, the ideal adversary $\mathcal{S}$ can compute n time-lock puzzles

$$\hat{P}_{j,i} = \begin{cases} \mathsf{Lock}(y_i \oplus r_i, t_{\pi(i)}) & \text{if } 1 \leq i \leq j \\ \mathsf{Lock}(r_i, t_{\pi(i)}) & \text{if } j < i \leq n \end{cases}.$$

Let the ideal adversary $\mathcal{S}$ output the following view at each check-point j:

$$\mathscr{V}_{\mathcal{S},j} = \mathcal{S}_j(\vec{inp}, (\hat{P}_{j,1}, \ldots, \hat{P}_{j,n})),$$

where $\mathcal{S}_j$ is the ideal adversary (for the underlying general MPC protocol) that simulates the adversary's j^{th} view $V_{\mathcal{A},j}$.

We now analyze the distribution of the puzzles $\hat{P}_{j,i}$. For the range $1 \leq i \leq j$, the puzzle $\hat{P}_{j,i}$ is by definition identically distributed to the puzzle that is outputted to player i in the real execution of Protocol 3. Now take any $j \in [n]$, and let D be any distinguisher whose run-time satisfies the conditions in Definition 4.1, item 3. Recall that the players are assumed to solve the time-lock puzzles using the optimal algorithm. Hence, it follows from the security of the underlying time-lock puzzle scheme that for any i in the range $j < i \leq n$,

$$\left|\Pr\left[D(P_{j,i}) = 1\right] - \Pr\left[D(\hat{P}_{j,i}) = 1\right]\right| \leq \mathsf{negl}(\kappa).$$

Since we defined the outputs of $\mathcal{S}$ to be $\mathscr{V}_{\mathcal{S},j} = \mathcal{S}_j(\vec{inp}, (\hat{P}_{j,1}, \ldots, \hat{P}_{j,n}))$ for $j \in [n]$, it follows that

$$|\Pr[D(\mathscr{V}_{\mathcal{S},j}, \mathscr{V}_{1,j}, \ldots, \mathscr{V}_{n,j}) = 1] - \Pr[D(V_{\mathcal{A},j}, V_{1,j}, \ldots, V_{n,j}) = 1]| \leq \mathsf{negl}(\kappa)$$

as required. We conclude that Protocol 3 securely realizes $\mathcal{F}_{\text{Timed-Delay-MPC}}$ clocked by $\mathcal{A}'_{i^*}$. □

A few remarks are in order. In Protocol 3, all the parties can stop interacting as soon as all the puzzles are outputted. When the locking algorithm $\mathsf{Lock}(d, t)$ has run-time that is independent of the delay t, the run-time of Protocol 3 is also independent of the delay parameters. (This is achievable using the [RSW96] time-lock construction, for example.) Alternatively, using a single time-line puzzle in place of the time-lock puzzles in Protocol 3 can improve efficiency, since the time required to generate a time-line puzzle is dependent only on the longest delay t_n, whereas the time required to generate n separate time-lock puzzles depends on the sum of all the delays, $t_1 + \cdots + t_n$.

4.4 Time-line puzzles

We now introduce the more general, novel definition of *time-line* puzzles, which can be useful for locking together many data items with different delays for a single recipient, or for locking data for a group of people. In the latter case, it becomes a concern that computation speed will vary between parties: indeed, the scheme will be unworkable if some parties have orders of magnitude more computing power than others, so some assumption is required on the similarity of computing power among parties, such as the Relative-Delay Assumption of Section 4.3.2. When a time-line puzzle is given to a single recipient, then no additional assumptions are required.

We remark that time-line puzzles could be used (instead of a set of time-lock puzzles) to realize Protocol 3. More generally, we present this new notion because we believe that time-line puzzles may be of independent interest as a timed-release primitive.

In some ways, a time-line puzzle can be thought of as a primitive that packages a sequence of time-lock puzzles together into a unified system about which we can reason and give security guarantees. However, time-line puzzles can also provide concrete advantages over a collection of time-lock puzzles. For example, when issuing many time-lock puzzles to one recipient, the recipient has to run the computation for all of the puzzles in parallel: that is, he does $O(m \cdot t)$ computation where m is the number of data items and t is the time-delay. If instead he gets a time-line puzzle, he only has to run one puzzle's worth of computation in order to unlock all the data items: that is, he does only $O(t)$ computation, just like for a single time-lock puzzle.

Definition 4.7 (Time-line puzzles)**.** *A* time-line puzzle scheme *is a family of* PPT *algorithms* $\mathcal{T} = \{(\mathsf{Lock}_m, \mathsf{TimeStep}_m, \mathsf{Unlock}_m)\}_{m \in \mathbb{N}}$ *as follows:*

- $\mathsf{Lock}_m(1^\kappa, (d_1, \ldots, d_m), (t_1, \ldots, t_m))$ *takes parameters* $\kappa \in \mathbb{N}$ *the security parameter,* $(d_1, \ldots, d_m) \in (\{0,1\}^\ell)^m$ *the data items to be locked, and* $(t_1, \ldots, t_m) \in \mathbb{N}^m$ *the number of steps needed to unlock each data item (respectively), and outputs a puzzle*

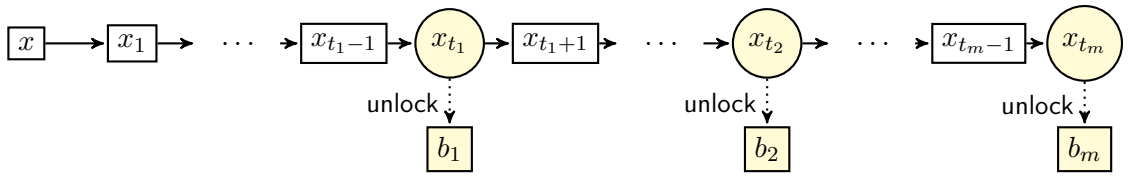
$$P = (x, (t_1, \ldots, t_m), (b_1, \ldots, b_m), a) \in \{0,1\}^n \times \mathbb{N} \times (\{0,1\}^{n''})^m \times \{0,1\}^{n'}$$

  where $n, n', n'' = \mathsf{poly}(\kappa)$*, and* a *can be thought of as auxiliary information.*

- $\mathsf{TimeStep}_m(1^\kappa, x', a')$ *takes parameters* $\kappa \in \mathbb{N}$ *the security parameter, a bit-string* $x' \in \{0,1\}^n$*, and auxiliary information* a'*, and outputs a bit-string* $x'' \in \{0,1\}^n$*.*

- $\mathsf{Unlock}_m(1^\kappa, x', b')$ *takes parameters* $\kappa \in \mathbb{N}$ *the security parameter, a bit-string* $x' \in \{0,1\}^n$*, and auxiliary information* $b' \in \{0,1\}^{n'}$*, and outputs some data* $d' \in \{0,1\}^\ell$*.*

In terms of the "pointer chain" analogy above, solving a time-line puzzle may be thought of as following a pointer chain where not one but many keys are placed along the chain, at different locations $t_1, \ldots, t_m$. Each key x_{t_i} in the pointer chain depicted below enables the "unlocking" of the locked data b_i: for example, b_i could be the encryption of the i^{th} data item d_i under the key x_{t_i}.



Using similar notation to that defined for time-lock puzzles: for a time-line puzzle scheme $\mathcal{T}$, let $\mathsf{IterateTimeStep}_m^{\mathcal{T}}$ denote the following function:

$$\mathsf{IterateTimeStep}_m^{\mathcal{T}}(i,x,a) = \underbrace{\mathsf{TimeStep}_m(\mathsf{TimeStep}_m(\ldots(\mathsf{TimeStep}_m(x,a),a)\ldots),a)}_{i}.$$

Define $\mathsf{CompleteUnlock}_{m,i}^{\mathcal{T}}$ to be the following function:

$$\mathsf{CompleteUnlock}_{m,i}^{\mathcal{T}}((x,t_i,b_i,a)) = \mathsf{Unlock}_m(\mathsf{IterateTimeStep}_m^{\mathcal{T}}(t_i,x,a),b_i),$$

that is, the function that should be used to unlock the i^{th} piece of data locked by a time-line puzzle which was generated by Lock_m. We now define correctness and security for time-line puzzle schemes.

Definition 4.8 (Correctness)**.** *A time-line puzzle scheme $\mathcal{T}$ is* correct *if for all $m = \mathsf{poly}(\kappa)$ and for all $i \in [m]$, it holds that*

$$\Pr_{(x,\vec{t},\vec{b},a)\leftarrow\mathsf{Lock}_m(\vec{d},\vec{t})}\left[\mathsf{CompleteUnlock}_i^{\mathcal{T}}((x,t_i,b_i,a)) \neq d_i\right] \leq \mathsf{negl}(\kappa),$$

where κ is the security parameter, $\vec{d} = (d_1,\ldots,d_m)$, and $\vec{t} = (t_1,\ldots,t_m)$.

Security for time-line puzzles involves more stringent requirements than security for time-lock puzzles. We define security in terms of two properties which must be satisfied: *timing* and *hiding*. The timing property is very similar to the security requirement for time-lock puzzles, and gives a guarantee about the relative amounts of time required to solve different time-lock puzzles. The hiding property ensures (informally speaking) that the ability to unlock any given data item that is locked in a time-line puzzle does not imply the ability to unlock any others. The security definition (Definition 4.9, below) refers to the following security experiment.

The experiment $\mathsf{HidingExp}_{\mathcal{A},\mathcal{T}}(\kappa)$

1. $\mathcal{A}$ outputs $m = \mathsf{poly}(\kappa)$ and data vectors $\vec{d}_0, \vec{d}_1 \in (\{0,1\}^\ell)^m$ and a time-delay vector $\vec{t} \in \mathbb{N}^m$.
2. The challenger samples $(\beta_1,\ldots,\beta_m) \leftarrow \{0,1\}^m$, computes the time-line puzzle $(x,\vec{t},\vec{b},a) = \mathsf{Lock}_m(1^\kappa,((d_{\beta_1})_1,\ldots,(d_{\beta_m})_m),\vec{t})$, and sends (x,a) to $\mathcal{A}$.
3. $\mathcal{A}$ sends a query $i \in [m]$ to the challenger. The challenger responds by sending b_i to $\mathcal{A}$. This step may be repeated up to $m-1$ times. Let I denote the set of queries made by $\mathcal{A}$.
4. $\mathcal{A}$ outputs $i' \in [m]$ and $\beta' \in \{0,1\}$.
5. The output of the experiment is 1 if $i' \notin I$ and $\beta' = \beta_{i'}$. Otherwise, the output is 0.

Definition 4.9 (Security)**.** *Let $\mathcal{T} = \{(\mathsf{Lock}_m, \mathsf{TimeStep}_m, \mathsf{Unlock}_m)\}_{m\in\mathbb{N}}$ be a time-line puzzle scheme. T is* secure *if it satisfies the following two properties.*

- TIMING: *For all* $m = \mathsf{poly}(\kappa)$ *and* $\vec{d}, \vec{d'} \in (\{0,1\}^\ell)^m$ *and* $\vec{t} = (t_1, \ldots, t_m)$*, if there exists an adversary* $\mathcal{A}$ *that solves any one of the puzzles defined by the time-line, that is,*

$$\Pr_{P \leftarrow \mathsf{Lock}_m(\vec{d},\vec{t})}[\mathcal{A}(P) = d_i] = \varepsilon \text{ for some non-negligible } \varepsilon \text{ and some } i \in [m],$$

then for all $j \in [t_i]$ *and all* $\vec{t'} \in [t_m]^m$*, there exists an adversary* $\mathcal{A}_{j,\vec{t'}}$ *such that*

$$\Pr_{P' \leftarrow \mathsf{Lock}_m(\vec{d'},\vec{t'})}[\mathcal{A}_{j,\vec{t'}}(P') = d_j] \geq 1 - \mathsf{negl}(\kappa), \text{ and}$$

$$\Pr_{\substack{P \leftarrow \mathsf{Lock}_m(\vec{d},\vec{t}) \\ P' \leftarrow \mathsf{Lock}_m(\vec{d'},\vec{t'})}}[\mathsf{time}_{\mathcal{A}}(P) \geq (t'_j/t_i) \cdot \mathsf{time}_{\mathcal{A}_{j,\vec{t'}}}(P') \mid \mathcal{A}(\mathsf{Lock}_m(\vec{d},\vec{t})) = d_i] \geq 1 - \mathsf{negl}(\kappa).$$

- HIDING: *For all* PPT *adversaries* $\mathcal{A}$*, it holds that*

$$\Pr[\mathsf{HidingExp}_{\mathcal{A},\mathcal{T}}(\kappa) = 1] \leq 1/2 + \mathsf{negl}(\kappa).$$

In Appendix D, we describe and prove the security of two constructions of time-line puzzle schemes. One of these schemes is based on a concrete assumption (specifically, on the sequentiality of modular exponentiation, like the time-lock puzzles of [RSW96]), whereas the other is based on the existence of a "black-box" inherently-sequential hash function.

Acknowledgements

We would like to thank Yehuda Lindell for an interesting discussion on the nature of fairness in multiparty computation, and we are grateful to Juan Garay, Björn Tackmann, and Vassilis Zikas for an illuminating discussion about measures of partial fairness in MPC.

The first author acknowledges research support by the Robert Solow Fellowship 3310100. The second and third authors acknowledge research supported by NSF Eager CNS-1347364, NSF Frontier CNS-1413920, the Simons Foundation (agreement dated June 5, 2012), Air Force Laboratory FA8750-11-2-0225, and Lincoln Lab PO7000261954. This work was done in part while these authors were visiting the Simons Institute for the Theory of Computing, supported by the Simons Foundation and by the DIMACS/Simons Collaboration in Cryptography through NSF grant CNS-1523467.

References

[AM12] Pablo Daniel Azar and Silvio Micali. "Rational proofs". In: *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*. ACM. 2012, pp. 1017–1028.

[AM13] Pablo Daniel Azar and Silvio Micali. "Super-efficient rational proofs". In: *Proceedings of the fourteenth ACM conference on Electronic commerce*. ACM. 2013, pp. 29–30.

[BGK14] Siddhartha Banerjee, Ashish Goel, and Anilesh Kollagunta Krishnaswamy. "Re-incentivizing discovery: mechanisms for partial-progress sharing in research". In: *ACM Conference on Economics and Computation, EC '14, Stanford , CA, USA, June 8-12, 2014*. Ed. by Moshe Babaioff, Vincent Conitzer, and David Easley. ACM, 2014, pp. 149–166. ISBN: 978-1-4503-2565-3. DOI: 10.1145/2600057.2602888. URL: http://doi.acm.org/10.1145/2600057.2602888.

[BK14] Iddo Bentov and Ranjit Kumaresan. "How to Use Bitcoin to Design Fair Protocols". In: *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*. Ed. by Juan A. Garay and Rosario Gennaro. Vol. 8617. Lecture Notes in Computer Science. Springer, 2014, pp. 421–439. ISBN: 978-3-662-44380-4. DOI: 10.1007/978-3-662-44381-1_24. URL: http://dx.doi.org/10.1007/978-3-662-44381-1_24.

[BP12] Sarah E. Bergen and Tracey L. Petryshen. "Genome-wide association studies (GWAS) of schizophrenia: does bigger lead to better results?" In: *Current opinion in psychiatry* 25.2 (Mar. 2012), pp. 76–82.

[BN00] Dan Boneh and Moni Naor. "Timed Commitments". In: *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*. Ed. by Mihir Bellare. Vol. 1880. Lecture Notes in Computer Science. Springer, 2000, pp. 236–254. ISBN: 3-540-67907-3. DOI: 10.1007/3-540-44598-6_15. URL: http://dx.doi.org/10.1007/3-540-44598-6_15.

[CDP14] Yang Cai, Constantinos Daskalakis, and Christos Papadimitriou. "Optimum Statistical Estimation with Strategic Data Sources". In: *ArXiv e-prints* (2014). arXiv: 1408.2539 [stat.ML].

[Can00] Ran Canetti. "Security and Composition of Multiparty Cryptographic Protocols". In: *J. Cryptology* 13.1 (2000), pp. 143–202. DOI: 10.1007/s001459910006. URL: http://dx.doi.org/10.1007/s001459910006.

[Cle86] Richard Cleve. "Limits on the Security of Coin Flips when Half the Processors Are Faulty (Extended Abstract)". In: *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*. Ed. by Juris Hartmanis. ACM, 1986, pp. 364–369. ISBN: 0-89791-193-8. DOI: 10.1145/12130.12168. URL: http://doi.acm.org/10.1145/12130.12168.

[Edm65] Jack Edmonds. "Paths, trees, and flowers". In: *Canadian Journal of mathematics* 17.3 (1965), pp. 449–467.

[ENSS95] Guy Even, Joseph(Seffi) Naor, Baruch Schieber, and Madhu Sudan. "Approximating minimum feedback sets and multi-cuts in directed graphs". English. In: *Integer Programming and Combinatorial Optimization*. Ed. by Egon Balas and Jens Clausen. Vol. 920. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1995, pp. 14–28. ISBN: 978-3-540-59408-6. DOI: 10.1007/3-540-59408-6_38. URL: http://dx.doi.org/10.1007/3-540-59408-6_38.

[For11] Schizophrenia Research Forum. *GWAS Goes Bigger: Large Sample Sizes Uncover New Risk Loci, Additional Overlap in Schizophrenia and Bipolar Disorder*. Sept. 2011. URL: http://www.schizophreniaforum.org/new/detail.asp?id=1692.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority". In: *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*. Ed. by Alfred V. Aho. ACM, 1987, pp. 218–229. ISBN: 0-89791-221-7. DOI: 10.1145/28395.28420. URL: http://doi.acm.org/10.1145/28395.28420.

[GHRV14] Siyao Guo, Pavel Hubáček, Alon Rosen, and Margarita Vald. "Rational arguments: single round delegation with sublinear verification". In: *Proceedings of the 5th conference on Innovations in theoretical computer science*. ACM. 2014, pp. 523–540.

[Han12] Robin Hanson. "Logarithmic Market Scoring Rules For Modular Combinatorial Information Aggregation". In: *The Journal of Prediction Markets* 1.1 (2012), pp. 3–15.

[Ins14] Broad Institute. *International team sheds new light on biology underlying schizophrenia.* July 2014. URL: https://www.broadinstitute.org/news/5895.

[Kar72] Richard M Karp. *Reducibility among combinatorial problems.* Springer, 1972.

[KO11] Jon M. Kleinberg and Sigal Oren. "Mechanisms for (mis)allocating scientific credit". In: *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011.* Ed. by Lance Fortnow and Salil P. Vadhan. ACM, 2011, pp. 529–538. ISBN: 978-1-4503-0691-1. DOI: 10.1145/1993636.1993707. URL: http://doi.acm.org/10.1145/1993636.1993707.

[May93] Timothy C. May. *Timed-release crypto.* 1993. URL: http://www.hks.net/cpunks/cpunks-01460.html.

[PGC14] Schizophrenia Working Group of the Psychiatric Genomics Consortium. "Biological insights from 108 schizophrenia-associated genetic loci". In: *Nature* 511 (Mar. 2014), pp. 421–427.

[RSW96] Ronald L. Rivest, Adi Shamir, and David A. Wagner. *Time-lock puzzles and timed-release crypto.* Tech. rep. 1996.

[Sha79] Adi Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (Nov. 1979), pp. 612–613. ISSN: 0001-0782.

[Wel03] The Wellcome Trust. *Sharing Data from Large-scale Biological Research Projects: A System of Tripartite Responsibility.* Report of a meeting organized by the Wellcome Trust and held on 14âĂŞ15 January 2003 at Fort Lauderdale, USA. 2003.

A Analysis of the discrete case

In this section we describe a variant of the scientific collaboration model of Section 2.1 for the discrete case when the output of the collaboration is a set of findings rather than a real value, following up on the discussion in Section 2.7. We adapt the analysis of data-sharing mechanisms for the original scientific collaboration model to this discrete model, and characterize the situations in which feasible collaborations can be efficiently computed for this setting.

The model is specified as follows.

- There is a set $[n]$ of players.
- For each $i \in [n]$, there is a set X_i of possible datasets, and a dataset $x_i \in X_i$ that the player knows. Let X denote $X_1 \times \cdots \times X_n$.
- A set of possible findings Ψ and a function $f : X \to \mathcal{P}(\Psi)$, whose output $Y^* \stackrel{\text{def}}{=} f(x_1, \ldots, x_n)$ the players wish to learn.
- All players commonly know an "initial result" Y_0. We may, without loss of generality, set $Y_0 = \varnothing$.
- For each player i, we denote by $\alpha_i \geq 0$ their reward from not collaborating. This models the best "outside payoff" that they could receive from publishing on their own. We denote by $A = \mathbb{R}_+^n$ the set of all outside option vectors.
- A *collaboration outcome* consists of a permutation $\pi : [n] \to [n]$ and sets $(Z_{\pi(1)}, \ldots, Z_{\pi(n)}) \in \mathcal{P}(\Psi)^n$ such that $Z_{\pi(1)} \subseteq \cdots \subseteq Z_{\pi(n)}$.

- If $\omega = (\pi, \mathbf{z})$ is a collaboration outcome, the player who publishes at time t obtains a reward

$$R_t(\pi, \mathbf{z}) = \beta^t \cdot (|Z_{\pi(t)}| - |Z_{\pi(t-1)}|).$$

  We define $Z_{\pi(0)}$ to be equal to $\varnothing$. Note that this reward function is identical to the reward function given in Section 2.1, for a "distance function" $d : \mathcal{P}(\Psi) \times \mathcal{P}(\Psi) \to \mathbb{Z}_+$ defined as follows[15]:

$$d(Z, Z') = |Z'| - |Z| \text{ whenever } Z \subseteq Z'.$$

- Players learn information not only from their own data, but also from the prior publications of others. A *learning bound vector* $\{\lambda_{\pi,i}\}_{\pi \in ([n] \to [n]), i \in [n]}$ characterizes, for any publication order π, the maximum amount that each player i can learn from prior publications. This notion is defined formally later.

As discussed in Section 2.7, the Output Divisibility Condition is not satisfied in the discrete setting. However, the weaker condition given below may hold. As observed in Section 2.7, it is natural to assume that the values α_i, μ_i are integers, since they are, respectively, the number of findings that player i can discover and publish on her own (without collaborating), and the number of extra findings that players can learn from player i's publication, given their own information. Given this, if we restrict β to be of the form $\beta = \frac{1}{k}$ for some integer $k \geq 1$, then we have that the following condition holds.

Integer Output Divisibility Condition. For any $Y \in \mathcal{P}(\Psi)$ and any integer $\delta \geq 1$, it is possible to find in constant time (independent of n) a $Y' \in \mathcal{P}(\Psi)$ such that $d(Y', Y) = \delta$.

We now give a definition of a data-sharing mechanism for the discrete model.

Definition A.1. *Given a function $f : X \to \mathcal{P}(\Psi)$, a* data sharing mechanism *is a function*

$$M_f : X \times A \times \Lambda_1 \to ([n] \to [n]) \times \mathcal{P}(\Psi)^n$$

which takes as inputs a vector $(x_1, \ldots, x_n)$ of datasets, a vector $(\alpha_1, \ldots, \alpha_n)$ of outside options, and $\{\lambda_{\pi,i}\}_{\pi \in ([n] \to [n]), i \in [n]}$ a learning bound vector. The outputs from such a mechanism are an ordering π of the players, and a vector of sets $\mathbf{y} = (Y_{\pi(1)}, \ldots, Y_{\pi(n)}) \in \mathcal{P}(\Psi)^n$.

Recall that each research group $\pi(t)$ will collaborate only if the credit they obtain from doing so is greater than the "outside option" reward $\alpha_{\pi(t)}$, that is, if a *collaborative equilibrium* (Definition 2.3) exists. We want to design a mechanism that guarantees collaboration whenever possible.

Assuming that the Integer Output Divisbility Condition holds, the analysis of the scientific collaboration model from Section 2 applies directly to the discrete model we have just defined. Thus, we obtain the following results for the discrete model:

- for *n-dimensional*[16] learning vectors, there is a polynomial-time algorithm SHARE-DATA′ that computes a collaborative equilibrium if one exists, or outputs `NONE` if not; and
- the problem of determining whether there exists a collaboration outcome which is a collaborative equilibrium is, in general, NP-complete.

We outline the proof structure for these results below, omitting full proofs since they are identical to those given in Section 2. The following theorem characterizes necessary and sufficient conditions for existence of collaborative equilibria.

[15] For the purposes of our model, it is only necessary to define the distance function between pairs of sets where one set is a subset of the other.

[16] See Section 2.1 for the definitions of *n-dimensional* and *n^2-dimensional* learning vectors.

Theorem A.2. *Suppose that the Integer Output Divisibility Condition holds. Let* $\mathbf{x}$ *be a vector of inputs,* α *be a vector of outside options and* λ *be an n-dimensional learning bound vector* λ *such that* $\lambda_{\pi,\pi(t)} = \sum_{\tau=1}^{t-1} \mu_{\pi(\tau)}$*. Then for* $(\pi, \mathbf{y})$ *to be a collaborative equilibrium it is necessary and sufficient that*

$$\sum_{t=1}^{n} \frac{\alpha_{\pi(t)}}{\beta^t} + \sum_{t=1}^{n} (n-t)\mu_{\pi(t)} \leq d(Y_0, Y^*) = |Y^*|.$$

Proof. The proof is identical to the proof of Theorem 2.5. □

Next, we specify a mechanism to compute feasible collaborations (or output `NONE` if none exist).

Theorem A.3. *If the sufficient conditions for existence of equilibria are satisfied, then there exists a polynomial-time data-sharing mechanism* SHARE-DATA′ : $X \times A \times \Lambda_1$ *that, given inputs* $(\mathbf{x}, \alpha, \lambda)$ *where* λ *is a n-dimensional learning vector, outputs a collaborative equilibrium* $(\pi, \mathbf{y})$ *if such an equilibrium exists.*

SHARE-DATA′$(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_n, \mu_1, \ldots, \mu_n)$

- Let $Y^* = f(x_1, \ldots, x_n)$ and $\gamma_0 = |Y^*|$. Let the elements of Y^* (in some arbitrary order) be denoted by $y_1, \ldots, y_{\gamma_0}$. For $i \in [\gamma_0]$, let S_i denote the subset $S_i = \{y_1, \ldots, y_i\}$.
- Construct a complete weighted bipartite graph $G = (L, R, E)$ where $L = [n], R = [n], E = L \times R$. For each edge (i, t), assign a weight $w(i, t) = \alpha_i + (n-t)\mu_i$.
- Let M be the minimum-weight perfect matching on G. For each node $t \in R$, let $\pi(t) \in L$ be the node that it is matched with. If the weight of M is larger than Y^*, output `NONE`. Else, define $Y_{\pi(n)} = Y^*$ and $\gamma_{\pi(n)} = 0$.
- For t from n to 2:
  - Let $\gamma_{\pi(t-1)} = \gamma_{\pi(t)} + \alpha_{\pi(t)} + \sum_{\tau=1}^{t-2} \mu_{\pi(\tau)}$.
  - Let $Y_{\pi(t-1)} = Y_{\pi(t)} \setminus S_{\gamma_{\pi(t)} - \gamma_{\pi(t-1)}}$.
- Output $\omega = (\pi, (Y_{\pi(1)}, \ldots, Y_{\pi(n)}))$.

Proof. The proof is essentially identical to the proof of Theorem 2.6. □

Finally, we show that for general learning bound vectors (in particular, n^2*-dimensional* learning vectors), computing the feasibility of collaboration is NP-complete.

When λ is a n^2*-dimensional* learning vector, the amount that player $\pi(t)$ learns from publication $\pi(\tau)$ is bounded above by $\mu_{\pi(t),\pi(\tau)}$. Thus, the total amount that player $\pi(t)$ learns from all prior publications is $\sum_{\tau=1}^{t-1} \mu_{\pi(t),\pi(\tau)}$. The corresponding necessary condition for a collaborative equilibrium is that there is a permutation π such that

$$\sum_{t=1}^{n} \alpha_{\pi(t)} + \sum_{t=1}^{n} \sum_{s>t} \mu_{\pi(s),\pi(t)} \leq d(Y_0, Y^*) = |Y^*|.$$

Even checking whether this condition holds is NP-complete.

Theorem A.4. *Given inputs* y_0*,* α *and* $\{\mu_{ij}\}_{i,j=1}^{n}$*, it is NP-complete to decide whether there exists* π *such that*

$$\sum_{t=1}^{n} \alpha_{\pi(t)} + \sum_{t=1}^{n} \sum_{s>t} \mu_{\pi(s),\pi(t)} \leq d(Y_0, Y^*) = |Y^*|.$$

Proof. The proof is identical to the proof of Theorem 2.8. □

B MPC security definition

IDEAL FUNCTIONALITY $\mathcal{F}_{\text{MPC}}$

In the ideal model, a trusted third party T is given the inputs, computes the function f on the inputs, and outputs to each player i his output y_i. In addition, we model an ideal process adversary $\mathcal{S}$ who attacks the protocol by corrupting players in the ideal setting.

Public parameters. $\kappa \in \mathbb{N}$, the security parameter; $n \in \mathbb{N}$, the number of parties; and $f : (\{0,1\}^*)^n \to (\{0,1\}^*)^n$, the function to be computed.

Private parameters. Each player $i \in [n]$ holds a private input $x_i \in \{0,1\}^*$.

1. INPUT. Each player i sends his input x_i to T.
2. COMPUTATION. T computes $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$.
3. OUTPUT. For each $i \in [n]$, T sends the output value y_i to party i.
4. OUTPUT OF VIEWS. After the protocol terminates, each party produces an output, as follows. Each uncorrupted party i outputs y_i if he has received his output, or $\perp$ if not. Each corrupted party outputs $\perp$. Additionally, the adversary $\mathcal{S}$ outputs an arbitrary function of the information that he has learned during the execution of the ideal protocol.

   Let the output of party i be denoted by $\mathscr{V}_i$, and let the view outputted by $\mathcal{S}$ be denoted by $\mathscr{V}_{\mathcal{S}}$. Let $\mathscr{V}^{\mathsf{ideal}}_{\text{MPC}}$ denote the collection of all the views:

$$\mathscr{V}^{\mathsf{ideal}}_{\text{MPC}} = (\mathscr{V}_{\mathcal{S}}, \mathscr{V}_1, \ldots, \mathscr{V}_n)\,.$$

Definition B.1 (Security)**.** *A multi-party protocol F is said to securely realize $\mathcal{F}_{\text{MPC}}$ if for any* PPT *adversary $\mathcal{A}$ attacking the protocol F by corrupting a subset of players $S \subset [n]$, there is a* PPT *ideal adversary $\mathcal{S}$ which, attacking $\mathcal{F}_{\text{MPC}}$ by corrupting the same subset S of players, can output a view $\mathscr{V}_{\mathcal{S}}$ such that*

$$V_{\mathcal{A}} \overset{c}{\approx} \mathscr{V}_{\mathcal{S}},$$

where $V_{\mathcal{A}}$ is the view outputted by the real-world adversary $\mathcal{A}$ (this may be an arbitrary function of the information that $\mathcal{A}$ learned in the protocol execution).

C Secret-sharing schemes

We recall the standard definition of a secret-sharing scheme.

Definition C.1 (Secret sharing scheme [Sha79])**.** *A* k-out-of-N secret sharing scheme *is a pair of algorithms* $(\mathsf{Share}, \mathsf{Reconstruct})$ *as follows.* Share *takes as input a secret value s and outputs a set of* shares $S = \{s_1, \ldots, s_N\}$ *such that the following two properties hold.*

- Correctness*: For any subset $S' \subseteq S$ of size $|S'| \geq k$, it holds that $\mathsf{Reconstruct}(S') = s$, and*
- Privacy*: For any subset $S' \subseteq S$ of size $|S'| < k$, it holds that $H(s) = H(s|S')$, where H denotes the binary entropy function.*

$\mathsf{Reconstruct}$ *takes as input a (sub)set* S' *of shares and outputs:*

$$\mathsf{Reconstruct}(S') = \begin{cases} \bot & \text{if} \quad |S'| < k \\ s & \text{if} \quad \exists S \text{ s.t. } S' \subseteq S \text{ and } \mathsf{Share}(s) = S \text{ and } |S'| \geq k \end{cases}.$$

D Constructions of time-line puzzles

D.1 Black-box construction from inherently-sequential hash functions

Definition D.1 (Inherently-sequential hash function)**.** *Let* $\mathcal{H}_\kappa = \{h_s : \{0,1\}^\kappa \to \{0,1\}^\kappa\}_{k \in \{0,1\}^n}$ *for* $n = \mathsf{poly}(\kappa)$ *be a family of functions and suppose that evaluating* $h_s(r)$ *for* $r \leftarrow \{0,1\}^\kappa$ *takes time* $\Omega(T)$*.* $\mathcal{H}_\kappa$ *is said to be* inherently-sequential *if evaluating* $h_s^t(r)$ *for* $s \leftarrow \{0,1\}^n, r \leftarrow \{0,1\}^\kappa$ *takes time* $\Omega(t \cdot T)$*, and the output of* $h_s^t(r)$ *is pseudorandom.*

The time-line puzzle construction in this section relies on the following assumption about the existence of inherently-sequential functions.

Assumption 1. *There exists a family of functions*

$$\widetilde{\mathcal{H}}_\kappa = \{\widetilde{h}_s : \{0,1\}^\kappa \to \{0,1\}^\kappa\}_{s \in \{0,1\}^n}$$

which is inherently-sequential (where $n = \mathsf{poly}(\kappa)$*).*

Definition D.2. $\mathsf{BB\text{-}TimeLinePuzzle}$ *is a time-line puzzle defined as follows, where* $\widetilde{\mathcal{H}}_\kappa$ *is the inherently-sequential hash function family from Assumption 1:*

- $\mathsf{Lock}_m(1^\kappa, (d_1, \ldots, d_m), (t_1, \ldots, t_m))$ *takes input data* $(d_1, \ldots, d_m) \in \{0,1\}^\kappa$*, samples random values* $s \leftarrow \{0,1\}^n, x \leftarrow \{0,1\}^\kappa$*, and outputs the puzzle*

$$P = \left(x, (t_1, \ldots, t_m), s, \left(d_1 \oplus \widetilde{h}_s^{t_1}(x), \ldots, d_m \oplus \widetilde{h}_s^{t_m}(x)\right)\right).$$

- $\mathsf{TimeStep}_m(1^\kappa, i, x', a')$ *outputs* $\widetilde{h}_{a'}(x')$*.*
- $\mathsf{Unlock}_m(1^\kappa, x', b')$ *outputs* $x' \oplus b'$*.*

It is clear that $\mathsf{BB\text{-}TimeLinePuzzle}$ satisfies correctness, so we proceed to prove security.

Theorem D.3. *If Assumption 1 holds, then* $\mathsf{BB\text{-}TimeLinePuzzle}$ *is a secure time-line puzzle.*

Proof. Given a time-line puzzle, in order to correctly output a piece of locked data d_i, the adversary $\mathcal{A}$ must compute the associated mask $\widetilde{h}_s^{t_i}(x)$. This is because

- all components of the puzzle apart from the masked value $d_i \oplus \widetilde{h}_s^{t_i}(x)$ are independent of the locked data d_i, and
- the mask $\widetilde{h}_s^{t_i}(x)$ is pseudorandom (by Assumption 1), so the masked value $d_i \oplus \widetilde{h}_s^{t_i}(x)$ is indistinguishable from a truly random value without knowledge of the mask.

Moreover, by Assumption 1, since $\widetilde{\mathcal{H}}_\kappa$ is an inherently-sequential function family, it holds that there is no (asympotically) more efficient way for a PPT adversary to compute $\widetilde{h}_s^{t_i}(x)$ than to sequentially compute $\widetilde{h}_s$ for t_i iterations. It follows that $\mathsf{BB\text{-}TimeLinePuzzle}$ is a secure time-line puzzle. □

D.2 Concrete construction based on modular exponentiation

In this subsection we present an alternative construction quite similar in structure to the above, but based on a concrete hardness assumption. Note that the [RSW96] time-lock puzzle construction was also based on this hardness assumption, and our time-line puzzle may be viewed as a natural "extension" of their construction.

Assumption 2. *Let* RSA_κ *be the distribution generated as follows: sample two* κ*-bit primes* p, q *uniformly at random and output* $N = pq$*. The family of functions* $\mathcal{H}^{square} = \{h_N : \mathbb{Z}_N \to \mathbb{Z}_N\}_{N \leftarrow \mathsf{RSA}_\kappa}$*, where the index* N *is drawn from distribution* RSA *and* $h_N(x) = x^2 \mod N$*, is inherently-sequential.*

Definition D.4. Square-TimeLinePuzzle *is a time-line puzzle defined as follows:*

- $\mathsf{Lock}_m(1^\kappa, (d_1, \ldots, d_m), (t_1, \ldots, t_m))$ *takes input data* $(d_1, \ldots, d_m) \in \{0,1\}^\kappa$*, samples random* κ*-bit primes* p, q*, sets* $N = pq$*, and outputs the puzzle*

$$P = \left(x, (t_1, \ldots, t_m), N, \left(d_1 \oplus h_N^{t_1}(x), \ldots, d_m \oplus h_N^{t_m}(x)\right)\right).$$

- $\mathsf{TimeStep}_m(1^\kappa, i, x', a')$ *outputs* $h_{a'}(x') = x'^2 \mod a'$*.*
- $\mathsf{Unlock}_m(1^\kappa, x', b')$ *outputs* $x' \oplus b'$*.*

Again, it is clear that Square-TimeLinePuzzle satisfies correctness, so we proceed to prove security.

Theorem D.5. *If Assumption 2 holds,* Square-TimeLinePuzzle *is a secure time-line puzzle.*

Proof. This follows from Assumption 2 in exactly the same way as Theorem D.3 follows from Assumption 1, so we refer the reader to the proof of Theorem D.3. □

An advantage of this construction over BB-TimeLinePuzzle is that the Lock algorithm can be much more efficient. In the case of black-box inherently-sequential hash functions, we can only assume that the values $\widetilde{h}_s^t(x)$ (which are XORed with the data values by the Lock algorithm) are computed by sequentially evaluating $\widetilde{h}_s$ for t iterations – that is, there is a linear dependence on t. However, Lock can implemented much faster with the Square-TimeLinePuzzle construction, as follows. Since p, q are generated by (and therefore, available to) the Lock algorithm, the Lock algorithm can efficiently compute $\phi(N)$. Then, $h_N^t(x)$ can be computed very efficiently by first computing $e = 2^t \mod \varphi(N)$, then computing $h_N^t(x) = x^e \mod N$. Exponentiation (say, by squaring) has only a logarithmic dependence on the security parameter.

Finally, we note that although both of the time-line puzzle constructions presented here lock κ bits of data per puzzle (for security parameter κ), this is not at all a necessary restriction. Using encryption, it is straightforwardly possible to lock much larger amounts of data for any given parameter sizes of the time-line puzzles presented here: for example, one can encrypt the data as $\mathsf{Enc}_k(d)$ using a secure secret-key encryption scheme, then use the given time-line puzzle schemes to lock the key k (which is much smaller than d) under which the data is encrypted. Such a scheme, with the additional encryption step, would be much more suitable for realistic use.