# A diagrammatic approach to information flow in encrypted communication

Peter M. Hines

University of York

**Abstract.** *We give diagrammatic tools to model and reason about information flow within encrypted communication. These are based on using a single categorical diagram to model the underlying mathematics, the epistemic knowledge of the participants, and potential or actual communication between participants.*
*A key part of this is a 'correctness' criterion that ensures we accurately & fully account for the distinct routes by which information may come to be known (i.e. communication and / or calculation).*
*We demonstrate how this formalism may be applied to answer questions about communication scenarios where we have the partial information-about the participants and their interactions. Similarly, we show how to analyse the consequences of changes to protocols or communications, and to enumerate the distinct orders in which events may have occurred.*
*We use various forms of Diffie-Hellman key exchange as an illustration of these techniques. However, they are entirely general; we illustrate in an appendix how other protocols from non-commutative cryptography may be analysed in the same manner.*

## 1 Introduction

This paper is about using categorical diagrams to study the flow of information in scenarios involving encrypted communication; it is not about the difficulty or otherwise of solving mathematical problems on which security is based.

Our starting point is the common category-theoretic technique of expressing algebraic identities via commuting diagrams. Drawing such diagrams for the algebra behind cryptographic protocols makes their structure clear (see, for example [7]), and gives a clear representation of the underlying mathematics; this paper also extends such diagrams to include the participants, their knowledge, and interactions.

Mathematically, we do this by moving beyond commuting diagrams, and modeling the information flow between participants as 2-categorical structure.

Based on this, we give a 'correctness' criterion that ensures that potential or actual information flow within the diagram is modelled correctly – i.e. nothing has been 'left out' and we have not overlooked any route by which a participant may come to know some information.

We give a series of illustrative examples based on Diffie-Hellman key exchange protocols, and demonstrate how several useful tasks may be automated within this framework. These include calculating *distinct paths by which information may come to be known*, deciding *causality and ordering of events*, and *finding the consequences of changes in the epistemic knowledge of the participants.*

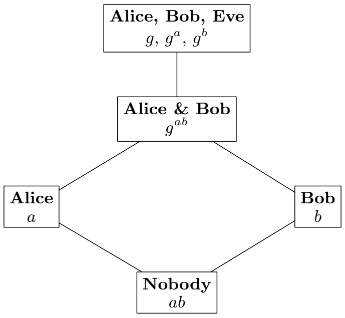
## 2 Bipartite Diffie-Hellman, diagramatically

Our aim is to present a formalism for modelling cryptographic and communication protocols in terms of categorical diagrams. In order to illustrate and test this formalism, we will use it to study various forms of *Diffie-Hellman* or *D-H* key exchange.

The basic bipartite D-H protocol is remarkable well-known [1, 6]; the underlying algebra, communications, and knowledge of participants are we summarised in Table 1.

**Table 1.** A concise summary of D-H key exchange

| **Alice** | **Public** | **Bob** |
|---|---|---|
| | Public prime $p$<br>Public root $g \in \mathbb{Z}_p$ | |
| Selects private<br>$a \in \mathbb{Z}_p$ | | Selects private<br>$b \in \mathbb{Z}_p$ |
| Computes $g^a$ | Announces $g^a$<br>$\longrightarrow$ | |
| | Announces $g^b$<br>$\longleftarrow$ | Computes $g^b$ |
| Computes: $\left(g^b\right)^a$ | | Computes: $\left(g^a\right)^b$ |
| *By elementary arithmetic, these are equal.*<br>$\left(g^b\right)^a \; = \; g^{ab} \; = \; \left(g^a\right)^b$ | | |



The tabular presentation simply distinguishes **public** and **private** information; by contrast, a fine-grained description of the knowledge of the participants (Alice, Bob, and some putative evesdropper Eve) is given in lattice form, by 'tagging' each algebraic element by a member of the power set lattice $2^{\{A,B,E\}}$ of participants.

### 2.1 Expressing algebraic identities diagrammatically

A core category-theoretic practice is giving identities as *commuting diagrams.*

**Definition 1.** *A* **diagram** *over a category $\mathcal{C}$ is simply a directed graph with nodes labeled by objects. Each edge is labeled by an arrow whose source / target is given by the labels on the initial / final nodes. A diagram* **commutes** *when the composites along all paths with the same starting / finishing node are equal.*

Although the concept is simple, commuting diagrams provide a very efficient and visual way to express algebraic identities. In Figure 1 we express the identies from Table 1 as a commuting diagram over the following category:

**Definition 2.** *Given prime $p \in \mathbb{N}$, we define the category $\mathbf{DH_p}$ to have two objects: a singleton object $\{*\}$ and the set $\mathbb{Z}_p = \{0, \ldots, p-1\}$.*

*For all $x = 0, \ldots, p-1$, we have the following arrows:*

- *The* **selection** *arrows $[x] : \{*\} \to \mathbb{Z}_p$, defined by $[x](*) = x \in \mathbb{Z}_p$.*
- *The* **modular exponentiation** *arrows $(\_)^x : \mathbb{Z}_p \to \mathbb{Z}_p$, defined in the usual arithmetic manner.*

**Fig. 1.** Bipartite Diffie-Hellman key exchange

$$\begin{tikzcd}
 & \mathbb{Z}_P \arrow[dl, "(\_)^a"'] \arrow[dr, "(\_)^b"] & \\
\mathbb{Z}_p \arrow[dr, "(\_)^b"'] & \{*\} \arrow[u, "{[g]}" description] \arrow[l, "{[g^a]}" description] \arrow[r, "{[g^b]}" description] \arrow[d, red, "{[g^{ab}]}" description] & \mathbb{Z}_p \arrow[dl, "(\_)^a"] \\
 & \mathbb{Z}_p &
\end{tikzcd}$$

*Remark 1 (Interpretation).* A key part of our diagrammatic calculus is that the arrows of the above category should be though of as *operations* that may reliably be *performed by participants*. As part of this, when we refer to the *epistemic knowledge* of participants in a protocol, this should be interpreted as *"who is able to perform a given operation?"* For example, Bob is able to perform the exponentiation $(\_)^b : \mathbb{Z}_p \to \mathbb{Z}_p$; similarly, both Alice and Bob are able reliably to select the secret key from $\mathbb{Z}_p$, but Eve cannot.

### 2.2 Combining algebraic & epistemic data

We now combine the algebraic and epistemic aspects of the D-H protocol into a single categorical diagram (Figure 2), by 'tagging' each categorical arrow by the subset of participants that are able to perform that operation.

By treating $2^{\{A,B,E\}}$ as a monoid with composition given by intersection we consider Figure 2 to be a categorical diagram over the product category $\mathbf{DH_p} \times 2^{\{A,B,C\}}$. Note that this categorical diagram *fails to commute.*

**Fig. 2.** The Algebraic-Epistemic diagram for Diffie-Hellman key exchange

$$\begin{tikzcd}
 & & \mathbb{Z}_P \arrow[dll, "(\_)^a{,}\{A\}"'] \arrow[drr, "(\_)^b{,}\{B\}"] & & \\
\mathbb{Z}_p \arrow[drr, "(\_)^b{,}\{B\}"'] & & \{*\} \arrow[ll, "{[g^a],\{A,B,E\}}"'] \arrow[rr, "{[g^b],\{A,B,E\}}"] \arrow[u, "{[g],\{A,B,E\}}"] \arrow[d, "{[g^{ab}],\{A,B\}}"] & & \mathbb{Z}_p \arrow[dll, "(\_)^a{,}\{A\}"] \\
 & & \mathbb{Z}_p & &
\end{tikzcd}$$

# 3 Information flow as failure of commutativity

The failure of commutativity in Figure 2 is obvious. Our claim is that this is a feature rather than a bug: it captures key features of communication protocols in graphical form. Precisely, the points at which commutativity fails are those where either 1/ a public announcement has taken place, or 2/ there exists more than one route to calculating the same result.

**Fig. 3.** Announcements as failure of commutativity in D-H key exchange

$$\begin{tikzcd}
\boxed{\text{Alice's announcement}} & & \mathbb{Z}_P \arrow[ddll, "(\_)^a{,}\{A\}"'] \arrow[ddrr, "(\_)^b{,}\{B\}"] & & \boxed{\text{Bob's announcement}} \\
 & \Swarrow & & \Searrow & \\
\mathbb{Z}_p & & \{*\} \arrow[ll, "{[g^a],\{A,B,E\}}"'] \arrow[rr, "{[g^b],\{A,B,E\}}"] \arrow[uu, "{[g],\{A,B,E\}}"] & & \mathbb{Z}_p
\end{tikzcd}$$

Consider the subdiagram of Figure 2 given in Figure 3. This fails to commute because $((\_)^a, \{A\})([g], \{A, B, E\}) = ([g^a], \{A\}) \neq ([g^a], \{A, B, E\})$. Similarly, $\left((\_)^b, \{B\}\right)([g], \{A, B, E\}) = \left(\left[g^b\right], \{B\}\right) \neq \left(\left[g^b\right], \{A, B, E\}\right)$.

The underlying cause in both cases is the public announcements: we would see the label $([g^a], \{A\}) = ((\_)^a, \{A\})([g], \{A, B, E\})$ in the case where Alice had raised the publicly known root to her secret key, but *kept the result to herself*. Similarly, we see an edge labeled by $\left(\left[g^b\right], \{A, B, E\}\right)$, rather than $\left(\left[g^b\right], \{B\}\right) = \left((\_)^b, \{B\}\right)([g], \{A, B, E\})$ because Bob has *publicly shared the result of his computation.*

**Fig. 4.** Failure of commutativity via distinct paths to the same result

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[drr, "{(\_)^b,\{B\}}"'] & \arrow[d, phantom, "\Rightarrow"] & \{*\} \arrow[ll, "{[g^a],\{A,B,E\}}"'] \arrow[rr, "{[g^b],\{A,B,E\}}"] \arrow[d, "{[g^{ab}],\{A,B\}}"] & \arrow[d, phantom, "\Leftarrow"] & \mathbb{Z}_p \arrow[dll, "{(\_)^a,\{A\}}"] \\
\boxed{\text{Bob's computation}} & & \mathbb{Z}_p & & \boxed{\text{Alice's computation}}
\end{tikzcd}$$

Communication between participants clearly causes failure of commutativity; however, there is another significant reason why a diagram may fail to commute. Figure 4 gives another subdiagram of Figure 2 that also fails to commute, since $\big((\_)^b, \{B\}\big)\,([g^a], \{A, B, E\}) = \big([g^{ab}], \{B\}\big) \neq \big([g^{ab}], \{A, B\}\big)$. In a similar way, $((\_)^a, \{A\})\,\big([g^b], \{A, B, E\}\big) = \big([g^{ab}], \{A\}\big) \neq \big([g^{ab}], \{A, B\}\big)$.

However, no announcements or sharing of information have taken place in this part of the protocol. Rather commutativity fails because Alice and Bob have separately arrived at the same information (i.e. their shared secret $g^{ab}$) via two distinct paths.

The fact that they both know it (and only they know it) is accounted for by the fact that the label on shared secret is the *join* of the labels of the two paths with the same source and target.

## 4 Algebraic-Epistemic diagrams, and a correctness condition

The above considerations apply generally, and motivate the following definitions:

**Definition 3.** *We define the* **Algebraic-Epistemic** *or* **A-E diagram** *for a communication protocol or scenario to be a commuting diagram giving a complete representation of the operations that may be performed by the participants, together with tags representing who is able to carry out which operation. Note that there is no notion of causality or ordering of events; rather (as discussed in Remark 5) this emerges from the underlying category theory.*

*Remark 2.* This paper uses Diffie-Hellman key exchange as illustration because it is simple and well-understood. We emphasise that these techniques are general; we may draw similar diagrams for other communication protocols or scenarios. Appendix A gives A-E diagrams for the 'Commuting Action Key Exchange' family of protocols from non-commutative cryptography [12], and demonstrates that the same interpretations and correctness criteria hold.

We now introduce a general 'correctness' criterion on A-E diagrams. This is based on 2-categories, where as well as objects and arrows between objects, we have 'higher-level' notion of 2-morphisms between arrows in the same homset. We refer to [8] for a good exposition of the general theory, but use a very restrictive special case, where the 2-morphisms are simply partial order relations between arrows in the same homset. The following is standard:

**Definition 4.** *A category $\mathcal{C}$ is* **poset–enriched** *when each homset $\mathcal{C}(X,Y)$ has a partial ordering $\leq_{XY}$ compatible with composition:*

$$f \leq_{XY} a \in \mathcal{C}(X,Y) \quad \text{and } g \leq_{YZ} b \in \mathcal{C}(Y,Z) \;\Rightarrow\; gf \leq_{XZ} ba \in \mathcal{C}(X,Z)$$

*(It is common to elide the object subscripts, when these are clear from the context).*

*Any category may be considered to be enriched over the partial order given by equality on homsets. The product of two poset-enriched categories is also assumed to be enriched over the product partial order: $(a,b) \leq (c,d)$ iff $a \leq c$ and $b \leq d$. Thus we may assume the category $\mathbf{DH_p} \times 2^{\{A,B,E\}}$ used in Section 2.2 to be poset-enriched.*

Based on this, we give a general definition on diagrams over poset–enriched categories that we will claim as a general 'correctness criterion' for Algebraic-Epistemic diagrams.

**Definition 5.** *Given a poset-enriched category $(\mathcal{C}, \leq)$, we treat it as a 2-category where the 2-cells are simply given by the partial ordering. We then say that a diagram $\mathfrak{D}$ over $\mathcal{C}$ satisfies the* **information flow ordering (IFO) condition***, or is an* **information flow ordered diagram** *when:*

1. *The underlying diagraph of $\mathfrak{D}$ is acyclic.*
2. *For any edge $e$ and path $p = p_k \ldots p_1$ with the same source and target node, the label on $p$ is $\leq$ the label on $e$.*

*It is standard to draw 2-morphisms in categorical diagrams as "two-cells"; for our purposes these are simply labeled by the partial order relation, so condition 2. is drawn as follows:*

$$\begin{tikzcd}
{} \arrow[r, "e"] \arrow[d, "p_1"'] \arrow[dr, phantom, "\Uparrow \leq"] & {} \\
{} \arrow[r, dotted] & {} \arrow[u, "p_k"']
\end{tikzcd}$$

*An immediate consequence of this condition is that any pair of edges with the same source and target nodes have the same label. We therefore include the assumption there is at most one edge with a given source / target.*

*Remark 3 (The IFO condition as a correctness criterion).* The IFO condition is proposed as a correctness criterion for Algebraic-Epistemic diagrams generally. This 'correctness' is simply about about accurately accounting for 1/ information flow between participants, and 2/ what this enables them to calculate. Our claim is that if we find that the IFO condition is not satisfied, we have failed to account for either 1/ or 2/. Further, we may often recover this additional information in a systematic and easily automated manner.

### 4.1 Justifying the IFO condition

The prescription for drawing A-E diagrams is entirely generic. Diagrams are drawn over a category of the form $\mathcal{C} \times \mathcal{L}$, where $\mathcal{C}$ is the algebraic setting for the protocol, and $\mathcal{L}$ is a meet-semilattice (generally the powerset-lattice $2^P$ of the participants in the protocol). We assume $\mathcal{C}$ to be poset-enriched over the equality relation, so the product category $\mathcal{C} \times 2^P$ is then enriched via the product partial ordering.

The Algebraic-Epistemic diagram $\mathfrak{D}$ for a protocol is a diagram over this category. The projection onto the first component $\pi_1(\mathfrak{D})$ is an acyclic commuting diagram over $\mathcal{C}$ that expresses the relationships between operations performed by participants in the protocol. By construction, this commutes, and therefore trivially satisfies the IFO condition. The additional lattice labels in $\mathfrak{D}$ itself are 'tags' giving the subset of participants that are able to perform the operation on that edge.

Based on this generic description, the interpretation of the IFO condition is straightforward. Consider (a fragment of) the A-E diagram for some protocol consisting of one edge and one path between nodes $H$ and $K$, as follows:

$$\begin{tikzcd}
\bullet \arrow[r, "{a_2,P_2}"] & \cdots \arrow[r, "{a_{n-1},P_{n-1}}"] & \bullet \arrow[d, "{a_n,P_n}"] \\
H \arrow[u, "{a_1,P_1}"] \arrow[rr, "{b,Q}"'] & & K
\end{tikzcd}$$

The IFO condition in this simple case states that $\bigwedge_{j=1}^{n} P_j \leq Q$. Given our interpretation, the IFO condition is an axiomatisation of the triviality that any individual who is able to perform each of the operations $a_1, \ldots, a_n$ is also able to perform their composite $a_n a_{n-1} \ldots a_1$.

Conversely, consider some diagram consisting of a single edge from node $H$ to node $K$, and multiple paths $\{\mathit{\Pi}_1, \ldots \mathit{\Pi}_n\}$with the same source and target, where the meet of the labels along $\mathit{\Pi}_k$ is denoted $R_k$, as follows:

$$\begin{tikzcd}
H \arrow[rr, squiggly, bend left=70, "{b,R_1}" description] \arrow[rr, squiggly, bend left=60, "{b,R_2}" description] \arrow[rr, squiggly, bend left=15, "{b,R_n}" description] \arrow[rr, "{b,Q}" description] & \vdots & K
\end{tikzcd}$$

The interpretation of the IFO condition is again straightforward. Every member of $R_1, R_2, \ldots, R_n$ is able to perform $b$; thus $R_j \leq Q$ for all $j = 1..n$. Using the additional lattice operations of $2^P$ we may also write this as $\bigvee_{j=1}^{n} R_j \leq Q$. However, the possibility that additional communication / announcements have also taken place prevents us from writing $\bigvee_{j=1}^{n} R_j = Q$; indeed, failure of this condition is a clear signal that additional communication has taken place.

*Remark 4 (The IFO condition and deadlock-freeness).* A further consequence of the IFO condition is *deadlock-freeness*; for example, it rules out the situation where Alice is waiting for a communication from Bob before she may continue, whilst simultaneously, Bob is waiting for a communication from Alice before he may take his next step.

Based on the interpretation of communication as 2-cells, we may axiomatise a deadlock situation as a *closed loop* of 2-morphisms. As the 2-arrows are simply order-relationships within a poset-enriched category, the anti-symmetry axiom $a \leq b \ \& \ b \leq a \ \Rightarrow \ a = b$ implies a collapse; we cannot draw a well-formed diagram where Alice is waiting for a result from Bob, whilst simultaneously Bob is waiting for a result from Alice.

## 5 Tripartite Diffie-Hellman key exchange

We now use diagrammatic methods to compare and contrast two approaches to tripartite secret sharing based on Diffie-Hellman key exchange. Multi-partite generalisations of Diffie-Hellman key exchange are well-established (see, for example, [5]). We consider the case where three participants construct a *single shared secret*, and where each pair of the three participants has a *distinct shared secret*. We refer to these as $\binom{3}{3}$ Diffie-Hellman and $\binom{3}{2}$ Diffie-Hellman respectively.

They are of course special cases of the situation where there are $n$ participants, and each subset of $k$ participants constructs a distinct shared secret – what we refer to as the general $\binom{n}{k}$ Diffie-Hellman protocol. This, including its diagrammatics, is considered in Appendix C.

**Definition 6 ($\binom{3}{3}$ Diffie-Hellman key exchange).** *Let us assume participants $\{Alice, Bob, Carol, Eve\}$ where Eve is the evesdropper, and Alice, Bob, and Carol will construct a mutual shared secret. Alice, Bob and Carol choose private keys $a, b, c \in \mathbb{Z}_p$ respectively, and their shared secret $g^{abc} = g^{bca} = g^{cab}$ is constructed as follows:*

1. *Alice computes $g^a$ and communicates the result to Bob.*
2. *Bob computes $g^b$ and communicates the result to Carol.*
3. *Carol computes $g^c$ and communicates the result to Alice.*

4. *Alice computes $(g^c)^a = g^{ca}$ and communicates the result to Bob.*
5. *Bob computes $(g^a)^b = g^{ab}$ and communicates the result to Carol.*
6. *Carol computes $\left(g^b\right)^c = g^{bc}$ and communicates the result to Alice.*

7. *Alice computes $\left(g^{bc}\right)^a = g^{abc}$.*
8. *Bob computes $(g^{ca})^b = g^{abc}$*
9. *Carol computes $\left(g^{ab}\right)^c = g^{abc}$.*

*It is of course assumed that Eve is party to all communication. We have made a slight break with convention, simply in order to test the formalism, and assumed that for whatever reason, Carol is not party to the communications between Alice and Bob, etc.*

The Algebraic-Epistemic diagram for this is given in Figure 16, and – should it be needed – a step-by-step description of how this diagram is derived is given in Appendix B. It may be verified that this diagram satisfies the IFO condition, and it is also unambiguous who has communicated what information to whom.

**Fig. 5.** Algebraic-Epistemic diagram for $\binom{3}{3}$ Diffie-Hellman

$$\begin{tikzcd}
 & & \mathbb{Z}_p \arrow[dddd, "{(\_)^c,\{C\}}"] & \\
\mathbb{Z}_p \arrow[dddd, "{(\_)^b,\{B\}}"'] & \mathbb{Z}_p \arrow[l, "{(\_)^a,\{A\}}"'] \arrow[ur, "{(\_)^b,\{B\}}"] \arrow[drr, "{(\_)^c,\{C\}}"] & & \\
 & & & \mathbb{Z}_p \arrow[dddd, "{(\_)^a,\{A\}}"] \\
 & \{*\} \arrow[uu, "{[g],\top}"] \arrow[uul, "{[g^a],\{A,B,E\}}"] \arrow[uuur, "{[g^b],\{B,C,E\}}"] \arrow[urr, "{[g^c],\{C,A,E\}}"] \arrow[dr, "{[g^{bc}],\{C,A,E\}}"] \arrow[ddl, "{[g^{ab}],\{B,C,E\}}"] \arrow[dd, "{[g^{abc}],\{A,B,C\}}"] \arrow[dddrr, "{[g^{ca}],\{A,B,E\}}"] & & \\
 & & \mathbb{Z}_p \arrow[dl, "{(\_)^a,\{A\}}"] & \\
\mathbb{Z}_p \arrow[r, "{(\_)^c,\{C\}}"'] & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \arrow[ull, "{(\_)^b,\{B\}}"]
\end{tikzcd}$$

An obvious alternative to three participants calculating a single shared secret is the scenario where each pair of participants has a distinct shared secret via the standard Diffie-Hellman protocol.

**Definition 7.** *(The* $\binom{3}{2}$ **Diffie Hellman protocol***) We again assume participants* $\{Alice, Bob, Carol, Eve\}$ *where Eve is the evesdropper. Alice, Bob and Carol choose private keys* $a, b, c \in \mathbb{Z}_p$*, and each pair, Alice-Bob, Bob-Carol, and Carol-Alice uses the bipartite D-H protocol to construct a shared secret.*

- *Alice, Bob, and Carol compute $g^a$ and $g^b$ and $g^c$ respectively. They publicly announce their results.*
- *Alice computes $g^{ba}$ (shared with Bob) and $g^{ca}$ (shared with Carol).*
- *Bob computes $g^{cb}$ (shared with Carol) and $g^{ab}$ (shared with Alice).*
- *Carol computes $g^{ac}$ (shared with Alice) and $g^{bc}$ (shared with Bob).*

We jump straight to the A-E diagram for the above protocol, given in Figure 6. This uses the same colour-coding as above.

**Fig. 6.** $\binom{3}{2}$ Diffie-Hellman

$$\begin{tikzcd}
 & \mathbb{Z}_p & & \mathbb{Z}_p \arrow[ll, "( \ )^a{,}\{A\}"'] \arrow[dd, "( \ )^c{,}\{C\}"] \\
\mathbb{Z}_p \arrow[ur, "( \ )^b{,}\{B\}"] \arrow[dd, "( \ )^c{,}\{C\}"'] & & \mathbb{Z}_p \arrow[ll, "( \ )^a{,}\{A\}"'] \arrow[ur, "( \ )^b{,}\{B\}"] \arrow[dd, "( \ )^c{,}\{C\}"] & \\
 & \{*\} \arrow[uu, red, "{[g^{ab}]}{,}\{A{,}B\}"] \arrow[ul, "{[g^a]}{,}\top"] \arrow[ur, "g{,}\top"'] \arrow[uurr, "{[g^b]}{,}\top"'] \arrow[rr, green, "{[g^{bc}]}{,}\{B{,}C\}"] \arrow[dl, blue, "{[g^{ca}]}{,}\{C{,}A\}"] \arrow[dr, "{[g^c]}{,}\top"] & & \mathbb{Z}_p \\
\mathbb{Z}_p & & \mathbb{Z}_p \arrow[ll, "( \ )^a{,}\{A\}"] \arrow[ur, "( \ )^b{,}\{B\}"'] &
\end{tikzcd}$$

*Remark 5 (Timing and ordering of steps in tripartite Diffie-Hellman).* A notable difference between the step-by-step descriptions of Definitions 6 and 7, and the A-E diagram of Figures 16 and 6, is that in the tabular description the order of steps is fixed. In the categorical diagrams, it becomes clear how this particular ordering of steps is not essential; rather, the only real restrictions are that a participant can only communicate a value *after* she has calculated it, and a value can only be calculated once the pre-requisites for this calculation have been received.

Based on the diagram we may consider alternative orderings of the steps given in Definition 6; it may be verified that these correspond to alternative, but operationally equivalent, presentations multipartite Diffie-Hellman protocols.

Should we wish to introduce explicit timing and ordering of events to A-E diagrams, this may be done by altering the underlying categories. Replacing the lattice $2^P$ of participants by its product with some total order $(T, \leq)$ gives the intuition of $(f, (A, t))$ as, "after time $t$, Alice is able to perform the operation $f$", and the IFO condition may again be used to enforce consistency with respect to this notion of causality.

## 6 A-E Diagrams as graphical tools for protocols

Although a diagrammatic approach may give a path to intuitive descriptions of protocols via pictures, we also wish to show how these pictures provide concrete tools for reasoning about information flow.

A diagrammatic calculus allows us easily to answer certain questions such as, 'how much information does a given participant have?', 'what are the routes by which an evesdropper may become aware of a given secret?', and 'what are the consequences of this particular value becoming known?'. We first illustrate this using various forms of Diffe-Hellman key exchange, then give general techniques for finding implicit or hidden information via diagrams.

### 6.1 Manipulating A-E diagrams

We make some straightforward definitions that will have useful interpretations when applied to A-E diagrams. A key concept is ordering categorical diagrams.

**Definition 8.** *Let $(\mathcal{C}, \leq)$ be a poset-enriched category, and let $\mathfrak{H}, \mathfrak{K}$ be diagrams (not necessarily commutative) over $\mathcal{C}$. We say $\mathfrak{H} \leq \mathfrak{K}$ iff the underlying directed graph of $\mathfrak{H}$ is a subgraph*[1] *of the underlying digraph of $\mathfrak{K}$, and for all edges of $\mathfrak{H}$, the label in $\mathfrak{H}$ is less than or equal to the label of the same edge in $\mathfrak{K}$. It is immediate that this a partial order on diagrams over $\mathcal{C}$.*

The above is of course applicable to IFO diagrams. Of particular interest is the poset of IFO diagrams that are above an arbitrary diagram, and whether this poset has a bottom element. In general there may not be a *unique* minimal IFO diagram above an arbitrary diagram.

### 6.2 Participants' views of protocols

A natural example of the ordering of diagrams is given by taking the A-E diagram for a given protocol, and erasing all edges whose 'tag' does not include some participant, or set of participants.

In Figure 7, we consider the A-E diagram for the $\binom{3}{3}$ Diffie-Hellman protocol, given in Figure 16, and do this for for the subsets $\{A\}$, $\{A, B\}$, $\{A, B, C\}$ and $\{E\}$. This gives a convenient graphical illustration of the information available to Alice, Alice and Bob, Alice and Bob and Carol, and the evesdropper respectively.

It is immediate that these subdiagrams also satisfy the IFO condition, and similarly that taking any A-E diagram satisfying the IFO condition, and erasing all edges according to a simlar criterion, will result in a diagram that again satisfies the IFO condtion. In particular, it is simple to take the diagram of Figure 6 and erase all edges not accessible to some (non-evesdropper) participant, to recover the A-E diagram for bipartite D-H key exchange given in Figure 1.

[1] We assume an implicit, fixed, embedding in order not to have to consider the graph embedding or graph isomorphism problem. In practice, this embedding is immediate from the interpretation

**Fig. 7.** $\binom{3}{3}$ Diffie-Hellman as seen by various sets of participants

**Alice: The $\{A\}$ restriction**

$$\begin{tikzcd}
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p \arrow[l, "{(-)^a,\{A\}}"'] & & \\
 & & & \mathbb{Z}_p \arrow[dddd, "{(-)^a,\{A\}}"] \\
 & \{*\} \arrow[uul, "{[g^a],\{A,B,E\}}"] \arrow[uu, "{[g],\top}"] \arrow[urr, "{[g^c],\{C,A,E\}}"] \arrow[dr, "{[g^{bc}],\{C,A,E\}}"] \arrow[dd, "{[g^{abc}],\{A,B,C\}}"'] \arrow[dddrr, "{[g^{ca}],\{A,B,E\}}"] & & \\
 & & \mathbb{Z}_p \arrow[dl, "{(-)^a,\{A\}}"] & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p
\end{tikzcd}$$

**Alice & Bob: The $\{A, B\}$ restriction**

$$\begin{tikzcd}
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \\
 & \{*\} \arrow[uul, "{[g^a],\{A,B,E\}}"] \arrow[uu, "{[g],\top}"] \arrow[dd, "{[g^{abc}],\{A,B,C\}}"'] \arrow[dddrr, "{[g^{ca}],\{A,B,E\}}"] & & \\
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p
\end{tikzcd}$$

**Alice, Bob & Carol: The $\{A, B, C\}$ restriction**

$$\begin{tikzcd}
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \\
 & \{*\} \arrow[uu, "{[g],\top}"] \arrow[dd, "{[g^{abc}],\{A,B,C\}}"'] & & \\
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p
\end{tikzcd}$$

**Eve: The $\{E\}$ restriction**

$$\begin{tikzcd}
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \\
 & \{*\} \arrow[uul, "{[g^a],\{A,B,E\}}"] \arrow[uu, "{[g],\top}"] \arrow[uuur, "{[g^b],\{B,C,E\}}"] \arrow[urr, "{[g^c],\{C,A,E\}}"] \arrow[dr, "{[g^{bc}],\{C,A,E\}}"] \arrow[ddl, "{[g^{ab}],\{B,C,E\}}"] \arrow[dddrr, "{[g^{ca}],\{A,B,E\}}"] & & \\
 & & \mathbb{Z}_p & \\
\mathbb{Z}_p & \mathbb{Z}_p & & \\
 & & & {}
\end{tikzcd}$$

### 6.3 Updating A-E diagrams based on additional information

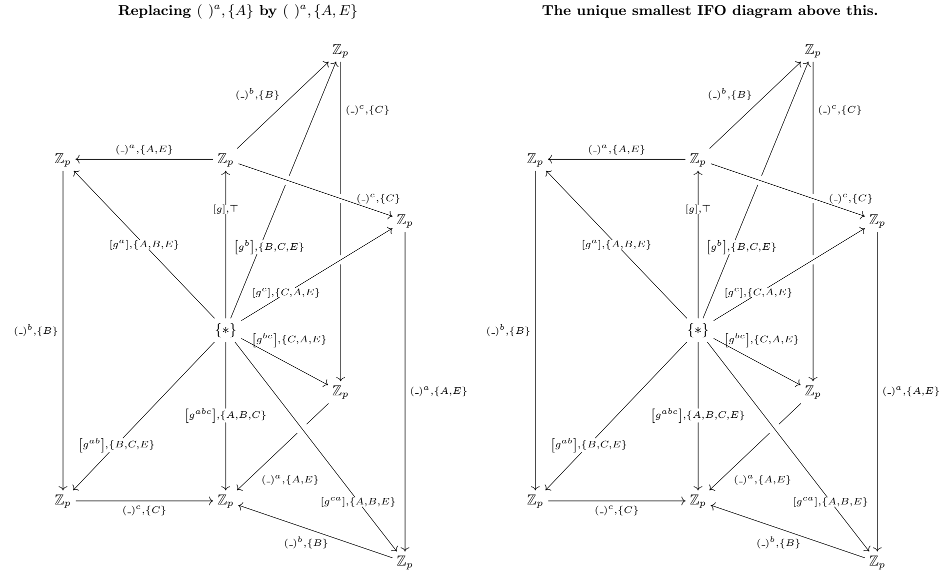
We now consider the more interesting case of when a diagram is modified to reflect some additional information. The resulting diagram may fail to satisfy the IFO condition.

Under these circumstances, the partial ordering of diagrams becomes a useful practical tool: given a diagram $\mathfrak{D}$ that does not satisfy the IFO condition, we consider the poset of diagrams above it that do satisfy this condition. Under very light assumptions, this will have a bottom element — we may analyse this to establish the consequences of this additional information.

This is best illustrated by a somewhat trivial example; we take both the $\binom{3}{3}$ and the $\binom{3}{2}$ Diffie-Hellman protocols and update them both with some additional information: **Eve has become aware of the private key of one of the participants**.

To analyse the $\binom{3}{3}$ protocol, we modify the diagram of Figure 16 to replace every ocurrence of $(\ )^a, \{A\}$ by $(\ )^a, \{A, E\}$. This will result in the diagram on the lhs of Figure 8.

**Fig. 8.** Eve knows Alice's private key!



**Replacing $(\ )^a, \{A\}$ by $(\ )^a, \{A, E\}$**

**The unique smallest IFO diagram above this.**

This diagram does *not* satisfy the IFO condition; it is missing either some communication or some route to participants calculating a given value. Fortunately, the poset of IFO diagrams above this has a smallest element: given on the rhs of Figure 8.

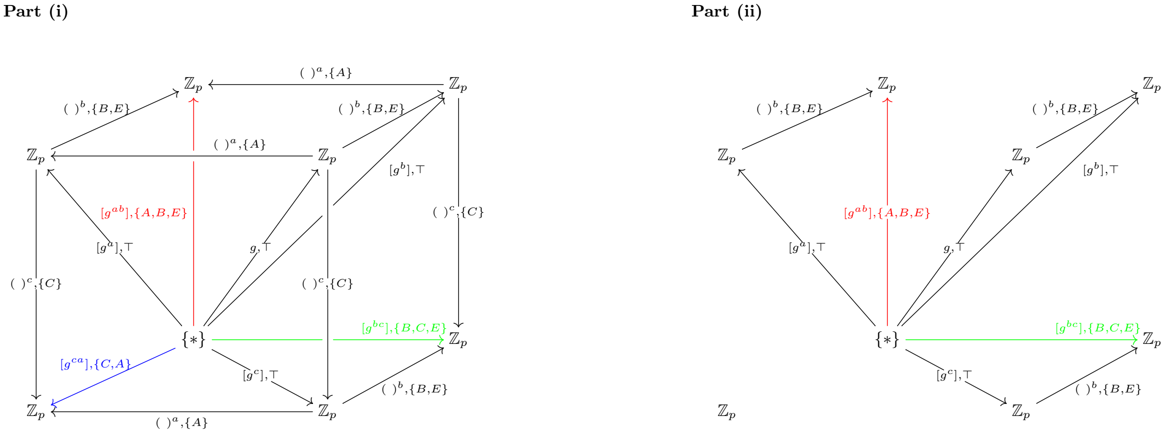
This particular case is straightforward; the lhs diagram has failed to satisfy the IFO condition because of the following single subdiagram:

$$\begin{tikzcd}
\{*\} \arrow[rd, "{\left[g^{bc}\right],\{C,A,E\}}"] \arrow[dd, "{\left[g^{abc}\right],\{A,B,C\}}"'] & \\
& \mathbb{Z}_p \arrow[ld, "{(\_)^a,\{A,E\}}"] \\
\mathbb{Z}_p &
\end{tikzcd}$$

whereas the smallest IFO diagram above this is given by replacing the edge labelled $\left[g^{abc}\right], \{A, B, C\}$ with an edge labelled by $\left[g^{abc}\right], \{A, B, C, E\}$. This single change corresponds to the observation that Eve now has a route to calculating Alice, Bob and Carol's shared secret.

By contrast, let us now assume that Eve is in fact aware of Bob's secret key in the $\binom{3}{2}$ version of D-H key exchange. We modify the diagram of Figure 6 to take this into account; we replace each ocurrence of $(\ )^b, \{B\}$ by $(\ )^b, \{B, E\}$ and find the minimal A-E above the result. This gives the diagram of Part **(i)** of Figure 9. Using the techniques of Section 6.2, we then consider Eve's view of the result, giving part **(ii)** of Figure 9. It is clear from the diagrams that Eve now has knowledge of the shared secrets of Alice & Bob, and Bob & Carol. However, she is not able to discover the shared secret of Alice & Carol.

**Fig. 9.** When Eve knows Bob's private key



*Remark 6.* Both the above results are course utterly trivial to anyone even slightly familiar with Diffie-Hellman key exchange. The intention is to demonstrate the reliability of the formalism, before moving on to demonstrate its utility.

## 7 Ambiguity, incompleteness, and algorithmics

In the above diagrammatic manipulations, information about which participant has made a particular announcement is not explicitly included in the A-E diagram for a protocol; rather, it must be deduced from the context. This is by design, and should be seen as a desirable feature, rather than a flaw[2]. In particular, it allows us to model ambiguous situations, where uncertainty exits as to, for example, who has shared or made public certain information — and potentially to deduce this information from the remainder of the diagram.

This is less relevant for analysing existing protocols, which are carefully designed to avoid ambiguity, and more applicable to real-world situations involving partial information about public and private communications.

**Definition 9.** *Let $\mathfrak{D}$ be a diagram satisfying the IFO condition. We say that $\mathfrak{D}$ is* **triangulated** *when every non-identity 2-cell is decomposed into composites of identity two-cells, and non-identity two-cells whose source is a path of length two and whose target is a single edge, such as:*

$$\begin{tikzcd}
\bullet \arrow[r] & \bullet \\
\bullet \arrow[u] \arrow[ur] \arrow[ur, phantom, "\Searrow" near end, shift left=3] &
\end{tikzcd}$$

*We say that a* **triangulation** *of a diagram $\mathfrak{D}$ is a triangulated diagram $\mathfrak{T}$ with the same nodes as $\mathfrak{D}$, that contains $\mathfrak{D}$ as a sub-diagram.*

No ambiguity can exist about communication / announcements in a triangulated diagram (beyond the inherent ambiguities given in the original data, such as, 'Both $A$ and $B$ know the values $x$ and $y$; one of them subsequently announces the composite $xy$.'). Weaker conditions often suffice to avoid ambiguity. However, for algorithmic purposes the notion of forming triangulations of a given diagram is useful.

Consider the situation described by the following diagram:

$$\begin{tikzcd}
& \bullet \arrow[dr, "{c,P_3}"] & \\
\bullet \arrow[ur, "{b,P_2}"] & & \bullet \arrow[d, "{d,P_4}"] \\
\bullet \arrow[u, "{a,P_1}"] \arrow[rr, "{dcba,\top}"'] & & \bullet
\end{tikzcd}$$

It is of course inaccurate to declare that, based on the information represented in this diagram, some individual or collection of individuals, in $\bigwedge_{j=1}^{4} P_j$ must

[2] Readers who disagree are invited to modify the formalism somewhat, so that 2-cells are labelled explicitly with this information. Categorically this task is simple; the resulting structures may be useful in some settings but in general are less flexible.

have publicly announced the result of the composition *dcba*. A counterexample is given by taking $P_1 = \{V, W\}$, $P_2 = \{W, X\}$, $P_3 = \{X, Y\}$, and $P_4 = \{Y, Z\}$, so $\bigwedge_{j=1}^{4} P_j = \bot$.

Instead, it is clear that when analysing who has shared what information with whom, we require additional edges in that diagram that provide additional *epistemic* data but do not add anything to the underlying *algebraic* structure.

Diagrams $\mathfrak{D}_1$ and $\mathfrak{D}_2$ below give two possible ways in which the composite *dcba* came to be public knowledge:

$\mathfrak{D}_1$

$$\begin{tikzcd}
\bullet \arrow[r, "{b,P_2}"] & \bullet \arrow[r, "{c,P_3}"] \arrow[dr, "{dc,\top}"] & \bullet \arrow[d, "{d,P_4}"] \\
\bullet \arrow[u, "{a,P_1}"] \arrow[ur, "{ba,\top}"] \arrow[rr, "{dcba,\top}"'] & & \bullet
\end{tikzcd}$$

$\mathfrak{D}_2$

$$\begin{tikzcd}
& \bullet \arrow[dr, "{c,P_3}"] & \\
\bullet \arrow[ur, "{b,P_2}"] \arrow[rr, "{cb,\top}"] & & \bullet \arrow[d, "{d,P_4}"] \\
\bullet \arrow[u, "{a,P_1}"] \arrow[rr, "{dcba,\top}"'] & & \bullet
\end{tikzcd}$$

Diagram $\mathfrak{D}_1$ is triangulated; we see that $W$ has publicly announced the composite *ba* and $Z$ has publicly announced *dc*, resulting in any participant being able to compute *dcba*.

However, $\mathfrak{D}_2$ is still not triangulated; although we can see that $X$ has publicly announced *cb* there still remains some ambiguity about how *dcba* came to be public knowledge.

To resolve the ambiguity in $\mathcal{D}_2$, note that it is a sub-diagram of both the following triangulated diagrams:

$\mathfrak{D}_3$

$$\begin{tikzcd}
& \bullet \arrow[dr, "{c,P_3}"] & \\
\bullet \arrow[ur, "{b,P_2}"] \arrow[rr, "{cb,\top}"] & & \bullet \arrow[d, "{d,P_4}"] \\
\bullet \arrow[u, "{a,P_1}"] \arrow[urr, "{cba,\top}"] \arrow[rr, "{dcba,\top}"'] & & \bullet
\end{tikzcd}$$

$\mathfrak{D}_4$

$$\begin{tikzcd}
& \bullet \arrow[dr, "{c,P_3}"] & \\
\bullet \arrow[ur, "{b,P_2}"] \arrow[rr, "{cb,\top}"] \arrow[drr, "{dcb,\top}"] & & \bullet \arrow[d, "{d,P_4}"] \\
\bullet \arrow[u, "{a,P_1}"] \arrow[rr, "{dcba,\top}"'] & & \bullet
\end{tikzcd}$$

In $\mathfrak{D}_3$, we see that either $V$ or $W$ has announced *cba*, then either $Y$ or $Z$ has announced *dcba*. Alternatively, in $\mathfrak{D}_4$, we see that either $Y$ or $Z$ has announced *dca* followed by either $U$ or $V$ announcing *dcba*.

The diagrams $\mathfrak{D}_1, \mathfrak{D}_3, \mathfrak{D}_4$ are of course not the only routes by which *dcba* may have come to be public knowledge. The two remaining possibilities are left as a straightforward exercise. In general, it is a simple, and easily automated, task to take an A-E diagram and derive the possible ways (if any!) in which communications amongst the participants which may have lead to this situation.

*Remark 7.* We should be aware that simply drawing such diagrams reflects our own epistemic beliefs; when we tag an edge with the pair $(x, \{U, V\})$ we are making the assumption that, for example, neither $U$ nor $V$ has publicly announced the value $x$. Triangulating a diagram is a method of making deductions about what actions participatns may have taken, *based on a priori assumptions.*

For deducing additional information of which we are not aware (e.g. participant $U$ has communicated the value of $x$ to another participant $W$), we must combine the above notion of *triangulating diagrams* with the tools derived from considering the poset of diagrams above or below a given diagram.

## 8 Future directions

Although it is visually appealing to be able to draw protocols for communication in diagrammatic form, the intention is also to develop concrete tools. These must be shown to be both accurate and useful; so far, this paper has concentrated on demonstrating that they accurately model the phenomena in question. This was done via their application to some very simple cryptographic protocols, where the answers to the questions considered are not only well-known, but almost trivially established.

What remains is to apply them to more complex situations; in particular, using them to reason about situations with incomplete knowledge appears to be potentially more fruitful.

From a more mathematical point of view, there are hints that the connection between categorical diagrams and cryptographic protocols may be more fundamental. Appendix A uses Commuting Action Key Exchange (CAKE) as an alternative illustration of A-E diagrams. The first concrete application of CAKE was in [11], where Thompson's group $\mathcal{F}$ was proposed as a platform.

It is by now almost folklore that Thompson's $\mathcal{F}$ consists entirely of canonical associativity isomorphisms, as found in the foundations of category theory [3]. This makes the relevant diagrams from Appendix A precisely *canonical coherence diagrams* — which are absolutely fundamental to much of category theory. Although the protocol of [11] was rapidly discovered to be insecure [4, 9], it is still worthwhile to consider its interpretations as category theory rather than cryptography – this program is carried out in [2].

## 9 Acknowledgements

I have had the good fortune to encounter several cryptographically-minded category theorists, and category-curious cryptographers. Thanks are due to Chris Heunen (Edinburgh), Delaram Kahrobaei (York), Dusko Pavlovic (Hawaii), and Noson Yanofsky (New York). Thanks are also due to Morgan Hines, for finding the regular 3D polyhedron associated with the protocol of Appendix C.

## References

1. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976.

2. P. Hines. Categorical coherence in cryptography, algebra, & number theory. *(Under revision, following referees comments)*, 2020.
3. S. MacLane. *Categories for the working mathematician.* Springer-Verlag, New York, second edition, 1998.
4. Francesco Matucci. Cryptanalysis of the shpilrain– ushakov protocol for thompson's group. *Journal of Cryptology*, 21(3):458–468, 2008.
5. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* Discrete Mathematics and Its Applications. 1996.
6. R. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21 (4).
7. D. Pavlovic. Chasing diagrams in cryptography. In Claudia Casadio, Bob Coecke, Michael Moortgat, and Philip Scott, editors, *Categories and Types in Logic, Language, and Physics: Essays Dedicated to Jim Lambek on the Occasion of His 90th Birthday*, pages 353–367. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
8. John Power. 2-categories. Technical Report NS-98-7, August 1998. 18 pp.
9. Dima Ruinskiy, Adi Shamir, and Boaz Tsaban. Length-based cryptanalysis: The case of thompson's group. 1, 07 2006.
10. V. Shpilrain and G. Zapata. Combinatorial group theory and public key cryptography. *http://arXiv.org/abs/math/0410068v1*, 2004.
11. Vladimir Shpilrain and Alexander Ushakov. *Thompson's Group and Public Key Cryptography*, pages 151–163. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.
12. Vladimir Shpilrain and Gabriel Zapata. Combinatorial group theory and public key cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 17, 11 2004.

## A A-E diagrams from non-commutative cryptography

Although this paper uses various forms of Diffie-Hellman key exchange as illustrative examples, we emphasise that the techniques are entirely general. To this end, we take a brief diversion, and present A-E diagrams for a family of significantly different cryptographic protocols, from the general field of non-commutative cryptography.

We do this in order to point out how the techniques for constructing A-E diagrams, their interpretation in terms of information flow, and the correctness criterion, are equally valid in different settings.

A general prescription for public-key protocols in non-commutative cryptography is that of Commuting Action Key Exchange (CAKE), introduced in [10]. Many familiar examples arise from this general prescription. In [10], the following particular form establishes a shared secret (a member of a given monoid) between the usual two parties, Alice and Bob, as follows:

**Definition 10 (The semigroup CAKE protocol).** *Given a monoid $M$,* **Alice** *and* **Bob** *may come to share a private element $\sigma \in M$ via public communication as follows:*

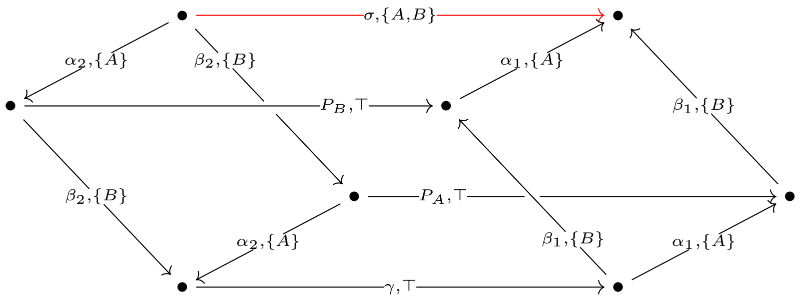
1. *Alice and Bob agree on two subsets $A, B \subseteq S$ (their respective* **key pools***) that point-wise commute i.e. $ab = ba$ for all $a \in A$ and $b \in B$.*
2. *A fixed* **root element** *$\gamma \in S$ is agreed upon.*

3. *Alice chooses her* **private key**, *a pair of elements* $\alpha_1, \alpha_2 \in A$, *and publicly broadcasts* $\alpha_1\gamma\alpha_2$
4. *Bob chooses his* **private key**, *a pair of elements* $\beta_1, \beta_2 \in B$, *and publicly broadcasts* $\beta_1\gamma\beta_2$.
5. *Alice then computes* $\alpha_1\beta_1\gamma\beta_2\alpha_2$ *and Bob computes* $\beta_1\alpha_1\gamma\alpha_2\beta_2$. *By the pointwise commutativity of* $A, B \subseteq S$, *these are equal, giving Alice and Bob's* **shared secret** *as* $\sigma = \alpha_1\beta_1\gamma\beta_2\alpha_2 = \beta_1\alpha_1\gamma\alpha_2\beta_2$.

*The traditional evesdropper* **Eve** *is assumed to be party to all communications.*

We treat the monoid $M$ as a category in the usual way, and denote its unique object by $\bullet \in Ob(M)$. The A-E diagram over $M \times 2^{\{A,B,E\}}$ for the CAKE family of protocols is given in Figure 10.

**Fig. 10.** The Algebraic-Epistemic diagram for semigroup CAKE



It is straightforward to verify that the A-E diagram of Figure 10 satisfies the IFO condition. The non-trivial 2-categorical information (i.e. the two-cells filled in with inequalities) illustrates both public announcements (Figure 11) and distinct routes to calculating the same value (Figure 12).

**Fig. 11.** Alice and Bob's public CAKE announcements

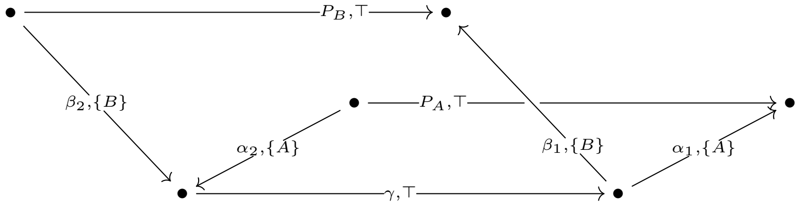


**Fig. 12.** Distinct paths to the same result in CAKE

$$\begin{tikzcd}
 & \bullet \arrow[rrr, "{\sigma,\{A,B\}}"] \arrow[dl, "{\alpha_2,\{A\}}"'] \arrow[ddr, "{\beta_2,\{B\}}"] & & & \bullet & \\
\bullet \arrow[rrr, "{P_B,\{A,B,E\}}"] & & & \bullet \arrow[ur, "{\alpha_1,\{A\}}"] & & \\
 & & \bullet \arrow[rrr, "{P_A,\{A,B,E\}}"] & & & \bullet \arrow[uul, "{\beta_1,\{B\}}"']
\end{tikzcd}$$

## B Step-by-step construction of A-E diagrams for $\binom{3}{3}$ DH

In Section 5, the A-E diagram for the $\binom{3}{3}$ Diffie-Hellman protocol is presented with no indication as to how it was derived. We now give a step-by-step description of the construction of the A-E diagram for the above protocol. The algebraic core is the identity $(\_)^{abc} = (\_)^{bca} = (\_)^{cab}$, which we draw as the commuting diagram of Figure 13. The protocol itself relies on these equalities *when applied to a specific root element* $g \in \mathbb{Z}$, so we introduce the singleton object $\{*\}$ and the element maps $[g], [g^{abc}] : \{*\} \to \mathbb{Z}_p$, giving the commuting diagram of Figure 14:

**Fig. 13.** The algebraic core of $\binom{3}{3}$ D-H key exchange

$$\begin{tikzcd}
 & & \mathbb{Z}_p \arrow[dd, "{(\_)^c}"] & \\
\mathbb{Z}_p \arrow[dd, "{(\_)^b}"'] & \mathbb{Z}_p \arrow[l, "{(\_)^a}"'] \arrow[ur, "{(\_)^b}"] \arrow[drr, "{(\_)^c}"] & & \\
 & & \mathbb{Z}_p \arrow[dl, "{(\_)^a}"'] & \mathbb{Z}_p \arrow[dd, "{(\_)^a}"] \\
\mathbb{Z}_p \arrow[r, "{(\_)^c}"] & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \arrow[ull, "{(\_)^b}"]
\end{tikzcd}$$

The elements $g^a, g^{ab}, g^b, g^{bc}, g^c, g^{ca}$ also play an explicit part in the protocol, so we add in the appropriate arrows from the central point to the outer corners of each vertical rectangle, to give the commuting diagram of Figure 15 that describes the interaction of all algebraic entities in $\binom{3}{3}$ Diffie-Hellman key exchange.

It finally remains to add in the epistemic data. This is routine, given that

**Fig. 14.** The algebra of $\binom{3}{3}$ D-H, applied to a root element

$$\begin{tikzcd}
 & & \mathbb{Z}_p \arrow[dddd, "(\_)^c"] & \\
\mathbb{Z}_p \arrow[dddd, "(\_)^b"'] & \mathbb{Z}_p \arrow[l, "(\_)^a"'] \arrow[ur, "(\_)^b"] \arrow[drr, "(\_)^c"] & & \\
 & & & \mathbb{Z}_p \arrow[dddd, "(\_)^a"] \\
 & \{*\} \arrow[uu, "{[g]}"] \arrow[dd, "{[g^{abc}]}"] & & \\
 & & \mathbb{Z}_p \arrow[dl, "(\_)^a"] & \\
\mathbb{Z}_p \arrow[r, "(\_)^c"] & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \arrow[ull, "(\_)^b"]
\end{tikzcd}$$

1. only Alice (resp. Bob, resp. Carol) can perform $(\ )^a$ (resp. $(\ )^b$, resp. $(\ )^c$).
2. Except for the computations in the bottom triangle,
   - Alice communicates the results of all her computations to Bob,
   - Bob communicates the results of all his computations to Carol,
   - Carol communicates the results of all her computations to Alice.
3. Eve is aware of the results of all communications.

Adding in this information gives the Algebraic-Epistemic diagram of Figure 16; it may be verified that this diagram satisfies the IFO condition, and it is also unambiguous who has communicated what information to whom.

*Remark 8 (Generalising to arbitrary numbers of participants).* It is notable that the diagram of Figure 16 consists of three isomorphic diagrams pasted along a common edge, with these three diagrams being related by a cyclic permutation of the symbols $(A, a)$, $(B, b)$ and $(C, c)$. This clearly generalises to a higher number of participants.

## C Diagrammatics for the $\binom{4}{2}$ Diffie Hellman protocol

As an exercise in diagrammatics, we extend the diagrams of Section 5 to the case where there are four participants, and each pair of them establishes a shared secret – i.e. the $\binom{4}{2}$ D-H key exchange protocol.

**Fig. 15.** All the algebraic entities of $\binom{3}{3}$ D-H key exchange

$$\begin{tikzcd}
 & & & \mathbb{Z}_p \arrow[dddd, "(\_)^{c}"] & \\
\mathbb{Z}_p \arrow[dddd, "(\_)^{b}"'] & & \mathbb{Z}_p \arrow[ll, "(\_)^{a}"'] \arrow[ur, "(\_)^{b}"] \arrow[drr, "(\_)^{c}"] & & \\
 & & & & \mathbb{Z}_p \arrow[dddd, "(\_)^{a}"] \\
 & & \{*\} \arrow[uu, "{[g]}"] \arrow[uull, "{[g^{a}]}"] \arrow[uuur, "{[g^{b}]}"] \arrow[urr, "{[g^{c}]}"] \arrow[ddll, "{[g^{ab}]}"'] \arrow[dd, "{[g^{abc}]}"] \arrow[dr, "{[g^{bc}]}"] \arrow[dddrr, "{[g^{ca}]}"] & & \\
 & & & \mathbb{Z}_p \arrow[dl, "(\_)^{a}"] & \\
\mathbb{Z}_p \arrow[rr, "(\_)^{c}"] & & \mathbb{Z}_p & & \\
 & & & & \mathbb{Z}_p \arrow[ull, "(\_)^{b}"]
\end{tikzcd}$$

**Definition 11.** *(The* $\binom{4}{2}$ **Diffie Hellman protocol***) We assume participants* $\{$*Alice*, *Bob*, *Carol*, *Dave*, *Eve*$\}$ *where Eve is the evesdropper. Alice, Bob, Carol, and Dave each choose private keys* $a, b, c, d \in \mathbb{Z}_p$*, and each pair uses the pair-wise Diffie-Hellman protocol to construct a shared secret.*

As a starting point to drawing the A-E diagram for this protocol, let us adopt yet another colour-coding convention, and denote operations applied by each participant by a consistent colour. Each participant then applies the 'exponentiation by their private key' on four different occasions, as illustrated in Figure 17. Recalling commutativity of modular exponentiation operations (i.e. $\left(g^b\right)^c = (g^c)^b$, &c.), we observe that a total of six distinct private keys are calculated, each one in two different ways.

Let us now take the graph of Figure 17 and identify nodes that have the same value (e.g. the top $g^{ca}$ and the bottom $g^{ac}$). We may draw the resulting figure as a regular three-dimensional figure where all lines have equal length, and all edges with the same colour are parallel. As these identifications are valid regardless of the value of the root $g \in \mathbb{Z}_p$, we have replaced the individual values by the object $\mathbb{Z}_p$. We have also added in the epistemic operation – this step is trivial, since as each operation shown(i.e. exponentiation by a private key) this may only be performed by the respective owner. We derive the (commuting) diagram of Figure 18.

**Fig. 16.** Algebraic-Epistemic diagram for $\binom{3}{3}$ Diffie-Hellman

$$\begin{tikzcd}
 & & \mathbb{Z}_p \arrow[dddd, "{(\_)^c,\{C\}}"] & \\
\mathbb{Z}_p \arrow[dddd, "{(\_)^b,\{B\}}"'] & \mathbb{Z}_p \arrow[l, "{(\_)^a,\{A\}}"'] \arrow[ur, "{(\_)^b,\{B\}}"] \arrow[drr, "{(\_)^c,\{C\}}"] & & \\
 & & & \mathbb{Z}_p \arrow[dddd, "{(\_)^a,\{A\}}"] \\
 & \{*\} \arrow[uu, "{[g],\top}"] \arrow[uul, "{[g^a],\{A,B,E\}}"] \arrow[uuur, "{\left[g^b\right],\{B,C,E\}}"] \arrow[urr, "{[g^c],\{C,A,E\}}"] \arrow[dr, "{\left[g^{bc}\right],\{C,A,E\}}"] \arrow[ddl, "{\left[g^{ab}\right],\{B,C,E\}}"] \arrow[dd, "{\left[g^{abc}\right],\{A,B,C\}}"'] \arrow[dddrr, "{[g^{ca}],\{A,B,E\}}"] & & \\
 & & \mathbb{Z}_p \arrow[dl, "{(\_)^a,\{A\}}"] & \\
\mathbb{Z}_p \arrow[r, "{(\_)^c,\{C\}}"'] & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \arrow[ull, "{(\_)^b,\{B\}}"]
\end{tikzcd}$$

**Fig. 17.** Each participant applies their secret operation four times

$$\begin{tikzcd}
 & & & g^{ac} & & & \\
 & & g^{ad} & g^{a} \arrow[u, blue, "(\ )^{c}" description] \arrow[l, magenta, "(\ )^{d}" description] \arrow[r, green, "(\ )^{b}" description] & g^{ab} & & \\
 & g^{da} & & & & g^{ba} & \\
g^{db} & g^{d} \arrow[l, green, "(\ )^{b}" description] \arrow[u, red, "(\ )^{a}" description] \arrow[d, blue, "(\ )^{c}" description] & & g \arrow[ll, magenta, "(\ )^{d}" description] \arrow[rr, green, "(\ )^{b}" description] \arrow[uu, red, "(\ )^{a}" description] \arrow[dd, blue, "(\ )^{c}" description] & & g^{b} \arrow[r, magenta, "(\ )^{d}" description] \arrow[u, red, "(\ )^{a}" description] \arrow[d, blue, "(\ )^{c}" description] & g^{bd} \\
 & g^{dc} & & & & g^{bc} & \\
 & & g^{cd} & g^{c} \arrow[l, magenta, "(\ )^{d}" description] \arrow[r, green, "(\ )^{b}" description] \arrow[d, red, "(\ )^{a}" description] & g^{cb} & & \\
 & & & g^{ca} & & &
\end{tikzcd}$$

Note that this diagram does indeed commute – there are no non-trivial 2-cells. The composite along any two paths with the same source and target is of the form $(\ )^s, \{\}$, for some shared secret $s \in \mathbb{Z}_p$. This emphasises that no single individual is able to calculate a shared secret without a public announcement from another participant! Adding in the key singleton object, and the respective 'select an element' arrows will provide for non-trivial 2-cells, and hence models of knowledge & information flow.

Unfortunately, three spacial dimensions do not suffice for drawing this as a *regular* shape; we therefore adopt the following simplifications in order to make our diagram manageable:

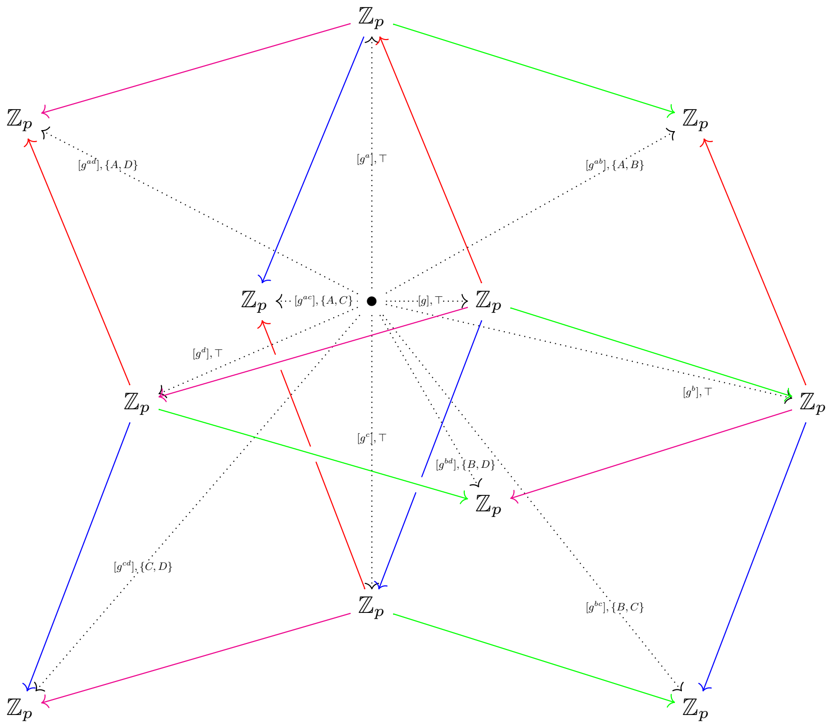
- As both the algebraic and epistemic labels on the coloured edges are uniquely determined by the colour, we omit these labels in favour of the colour-coding only.
- The 'select an element' arrows are drawn as dotted lines, with no attempt made to distinguish over- and under- crossings.
- The unique singleton element is represented by a bullet $\bullet = \{*\}$.

This then leads to the diagram shewn in Figure 19, which may be verified to satisfy the IFO condition.

**Fig. 18.** Exponentiation by a private key, performed by its owner

$$\begin{tikzcd}
 & & & \mathbb{Z}_p \arrow[dlll, "(\ )^{d}{,}\{D\}"'] \arrow[drr, "(\ )^{b}{,}\{B\}"] \arrow[ddl, "(\ )^{c}{,}\{C\}"'] & & & \\
\mathbb{Z}_p & & & & & \mathbb{Z}_p & \\
 & & \mathbb{Z}_p & & \mathbb{Z}_p \arrow[uul, "(\ )^{a}{,}\{A\}"'] \arrow[dlll, "(\ )^{d}{,}\{D\}"'] \arrow[drr, "(\ )^{b}{,}\{B\}"] \arrow[dddl, "(\ )^{c}{,}\{C\}"] & & \\
 & \mathbb{Z}_p \arrow[uul, "(\ )^{a}{,}\{A\}"] \arrow[drrr, "(\ )^{b}{,}\{B\}"'] \arrow[dddl, "(\ )^{c}{,}\{C\}"'] & & & & & \mathbb{Z}_p \arrow[uul, "(\ )^{a}{,}\{A\}"'] \arrow[dll, "(\ )^{d}{,}\{D\}"] \arrow[dddl, "(\ )^{c}{,}\{C\}"] \\
 & & & & \mathbb{Z}_p & & \\
 & & & \mathbb{Z}_p \arrow[uuul, "(\ )^{a}{,}\{A\}"] \arrow[dlll, "(\ )^{d}{,}\{D\}"] \arrow[drr, "(\ )^{b}{,}\{B\}"'] & & & \\
\mathbb{Z}_p & & & & & \mathbb{Z}_p &
\end{tikzcd}$$

**Fig. 19.** The A-E diagram for $\binom{4}{2}$ Diffie-Hellman



*Remark 9 (Combinatorics, diagrams, and polyhedra for $\binom{n}{k}$ Diffie-Hellman).* Combinatorially, it is relatively easy to write down an abstract characterisation – in terms of nodes, edges, and labels – of the A-E diagram for the $\binom{n}{k}$ Diffie-Hellman protocol, where there are $n$ participants, and every subgroup of $k$ individuals comes to share a secret. What is less intuitive is the description of these diagrams in terms of regular figures in $d$-dimensional space. A suitable geometric characterisation surely exists, although it is far from the stated aims of this paper! It is therefore left as a potentially non-trivial exercise.