Secure communication of local states in multi-agent systems

Michael Albert[1], Andrés Cordón–Franco[2], Hans van Ditmarsch[2], David Fernández–Duque[2], Joost J. Joosten[2], and Fernando Soler–Toscano[2]

[1] University of Otago, New Zealand
malbert@cs.otago.ac.nz
[2] University of Sevilla, Spain
{acordon,hvd,dfduque,jjoosten,fsoler}@us.es

Abstract. Given a deal of cards over three agents, we investigate ways for two agents to communicate secrets by public announcements. The problem to keep all of your cards a secret (i) can be distinguished from the problem to keep some of your cards a secret (ii). For (i): we characterize a novel class of protocols consisting of two announcements, for the case where two agents both hold n cards and the third agent a single card; the communicating agents announce the sum of their cards modulo $2n + 1$. For (ii): we show that the problem to keep at least one of your cards a secret is equivalent to the problem to keep your local state (hand of cards) a secret; we provide a large class of card deals for which exchange of secrets is possible; and we give an example for which there is no protocol of less than three announcements.

1 Introduction

Alice and Bob, draw a and b cards from a deck of $a + b + c$ cards, and Eve, the eavesdropper, receives the remaining c cards. Alice and Bob wish to communicate their cards to each other by way of public announcements, without informing Eve of any of their cards. The investigation of the generalized problem with card deal size parameters (a, b, c) was inspired by its $(3, 3, 1)$ instance that was coined in [12] the *Russian Cards Problem*, and that originates with Kirkman [9]. A standard solution for $(3, 3, 1)$ is as follows. Suppose Alice holds 0, 1, and 2, Bob holds 3, 4, and 5, and Eve holds 6. Alice announces that her hand of cards is one of $012, 034, 056, 135, 146, 236, 245$, i.e., one of the seven hands $\{0, 1, 2\}$, etc., after which Bob announces that Eve holds 6. Another solution is that Alice announces that she holds one of the five hands $012, 034, 056, 135, 246$, again followed by Bob announcing that Eve holds 6. We can view such solutions as the execution sequences of an underlying protocol. Some general patterns and special cases of card deal sizes (a, b, c) for which two-announcement solutions exist are found in [2], but a complete characterization is not known.

We can relax the constraints for secrecy in the Russian Cards Problem somewhat. Suppose that the eavesdropper may learn single card ownership for Alice and Bob, but just not their entire holding, i.e., the eavesdropper may not learn

the card deal. In that case, simpler protocols suffice. In terms of interpreted systems, Alice and Bob attempt to communicate their local state to each other, without Eve learning their local states. Note that, if Eve were to learn the local state of Alice or the local state of Bill, she would learn the entire deal of cards.

A simple way for Alice to communicate her local state to Bob, in the $(3, 3, 1)$ case, is to announce that she holds one of 012, 034, and 056. In other words, she gives away that she holds card 0, but this does not disclose her whole hand. After that announcement, Bob as before responds that Eve holds 6. We may call Alice's announcement *state safe*, as opposed to *card safe*, above. There is a relation to *bit exchange* problem: is it possible for Alice and Bob to share a secret bit (i.e., the value of a proposition) by public communication. The seminal publication for the latter is [7].

Motivation We are motivated in our investigations by the ground separating unconditionally secure (also known as information-based) from conditionally secure protocols. The security of the latter are based on computational features: the intractability of some computation, a one-way function between some cryptographic primitives, etc. It is tempting to say that unconditionally secure protocols are abstractions of conditionally secure protocols. But this high and dry ground seems very poor: abstracting away from keys and one-way functions seems to remove the essence from reasoning about protocols, and it is therefore unclear what results for the abstraction have to bear on practical security matters and protocol design. We do not bridge that gap. But anything we do, aims to bridge that gap.

Our slightly less ulterior motive is to design fast unconditionally secure protocols for information exchange in multi-agent systems. Within the more specific bounds that we have set, such as card secure protocol or state secure protocols, we aim to find minimum-length protocols, to find the maximum number of bits that can be exchanged, and to analyze multi-agent versions of protocols ('multi-party' in security jargon; with 'multi' as 'more than two') where the intention to securely exchange information about the ignorance and knowledge of other agents (also known as higher-order preconditions in protocol execution) inevitably draws in dynamic epistemic methodology. An additional challenge in that setting is the reconciliation of what may be called more embedded methods with the more abstract logical and combinatorial approaches. Somewhere on the far horizon remains a link with conditional security.

Results This work contains the following contributions. For the card exchange problem for card deal size $(n, n, 1)$ we characterize a novel class of protocols consisting of two announcements. In that case, we treat the set of cards not as a set of (interchangable) labels as in design theory [11], but as set of consecutive numbers $0, 1, ..., 2n$ and employ number theoretical methods and brute force (Haskell). The protocol is simple: both A and B announce the sum of their cards modulo $2n + 1$. The method has promising generalizations. Further, we show that state safe is equivalent to bit safe, and provide a large class of card deal sizes (a, b, c) for which bit exchange is possible (this should be seen as a

special case of results in [6]). These protocols typically consist of various announcements, without a claim that these are minimal. We also give an example of a bit exchange protocol consisting of three announcements where no solution of two announcements exists.[3]

2 Card deal terminology and known results

The three *agents* Alice, Bob, and Eve are abbreviated as $\mathsf{A}, \mathsf{B}, \mathsf{C}$. Given a set/*deck* D of $d = a + b + c$ *cards*, their hands of cards A, B, C consist of a, b, c cards. The *card deal* (A, B, C) is the triple of the three hands of cards, and we call this a card deal of *size* (a, b, c). The cards in the deck may be called anything whatsoever, but it is customary to name them $0, 1, ..., d-1$.

Given that cards are numbers, and that our examples use small numbers, we allow ourselves some abus de langage. Consider size $(3, 3, 1)$. For hand of cards $\{0, 1, 2\}$ we write 012 (and the cards in a hand always in this ascending order), and for deal $(\{0, 1, 2\}, \{3, 4, 5\}, \{6\})$ we write 012.345.6.

We can distinguish the information requirement—what A and B are supposed to learn from each other—from the safety requirement—what C is not supposed to learn from the communications taking place between A and B. The information requirement is for A and B to learn all of their cards (and therefore the entire deal of cards). We call an information state satisfying that requirement *state informative*. The *card safe* requirement is for C to remain ignorant of the ownership of all of A's and B's cards; whereas in *state safe*, the requirement is for C to remain ignorant of the ownership of at least one of those cards (and therefore ignorant about the hand of cards of the other agents, their *local state*).

Protocols to solve these problems consist of a finite number of alternating truthful public announcements by A and B, all of which are informative (trivial announcements are not allowed), and where each announcement consists of a number of alternatives for the hand of cards of the announcing agent. These are not truly restrictive conditions: for a finite number of cards, there are only a finite number of possible card deals, and each informative announcement results in a reduction of these alternatives.

An information state is represented by a Kripke model for what agents know, 'informative announcement' can be defined as one resulting in a proper model restriction, any complex logical statement that is announced is equivalent to an announcement of a number of alternatives for the actual hand of cards, and all states in (a bisimulation contraction of) that Kripke model are about different card deals [12]. (Results we do not explain in technical detail here.) The various safety and information requirements are formulas that can be checked in such a model. In this work we only consider protocols of length two where first A and then B makes an announcement, and protocols of length three where the announcements are made by A, then B, and then A again.

[3] This is interesting, because at the time of submission no such protocol was known for the card exchange problem, although we have now found one for parameters $(4, 4, 2)$, and no other such example is known for the state exchange problem.

All the following should hold for any deal of cards for which a given sequence of announcements can be made truthfully. An announcement is *card safe* / *state safe* if it preserves ignorance of C of all cards / some card (the safety requirement). We will normally call them safe, and let the context determine if card safe or state safe is intended. A sequence of announcements is a protocol.[4] A protocol is safe if it consists of safe announcements. A protocol is state informative if A and B know the card deal after termination, i.e., if the information state reached is state informative. (This implies that the last announcement in the protocol informs the agent addressed by that announcement of the hand of cards of the announcing agent, and that the second-to-last announcement informs the other agent.) A protocol is good if it is safe and state informative.

In [2] some sizes (a, b, c) are listed for which good protocols consisting of two announcements exist, e.g., (a, b, c) such that $a + b + c = p^2 + p + 1$ for any prime $p \leq a - 1$, and $(3, b, 1)$ if $b \geq 3$, and $(a, 2, 1)$ if $a = 0, 4 \mod 6$. In a two-announcement protocol the second announcement is always equivalent to B announcing the cards of C. There may be protocols for (a, b, c) but *not* for (b, a, c), e.g., there is a protocol for $(4, 2, 1)$ but not for $(2, 4, 1)$.

2.1 Subgroup common knowledge or public knowledge?

The role of common knowledge in protocols is of logical interest. The solution requirements discussed in [12] and [2] are formulated for an actual deal of cards, and *not*, as above, for any deal of cards for which the announcements can be truthfully made. Given that, they are required to be commonly known. (The contribution of [12] is to show what can go wrong if that does not hold, by an analysis in public announcement logic.) However, there is a subtlety: it must be common knowledge among all three agents, i.e. *public* knowledge, that the safety requirement is satisfied, and it must be common knowledge among A and B (also known as subgroup common knowledge) that the information requirement is satisfied. An open question remained if the information requirement should also be publicly known. If not, Eve is uncertain whether Alice and Bob have terminated the protocol. In all known cases of this kind, announcing that the protocol is finished then results in Eve learning some of Alice's or Bob's cards. We investigated the matter thoroughly but not exhaustively, and were also greatly helped by the program DEMO [13] for model checking dynamic epistemics. An open question remains:

> Are there protocols after which it is common knowledge to A and B that they know each other's cards (and thus the card deal), and where this is not public knowledge, and where the announcement is safe that the protocol is terminated (after which it is public knowledge that A and B know the card deal)?

[4] Strictly, it is only an execution sequence of an underlying protocol; see the section 'Further Research' and the example on page 13.

Open questions are nice, but they should be relevant. The literature on security protocols suggests that this is not an interesting question:

A time-honoured principle by Kerckhoffs [8] states that the safety of a protocol should not depend on whether the protocol is public or not, with the exception of the 'private' keys of the agents performing in the protocol. For card deal protocols the role of the private keys is played by actual hand of cards of A and B. Protocols ending in common knowledge between A and B that the secret has been exchanged, but where this is not publicly known, are therefore ruled out.

If we do not reason from the perspective of an actual deal of cards, but from the perspective of all cards deals consistent with the announcements made so far, the discussion on subgroup or public common knowledge evaporates: the information and security requirements should then be model validities, from which it follows that they are publicly known. From now on, we assume that the requirements should be met for any card deal consistent with the announcements.

3 Card safe protocols for size $(n, n, 1)$

The five hand solution for the $(3, 3, 1)$ case is also known under the form of the 'sum modulo number of cards' [10]. For example, when Alice holds 012, she announces that the sum of her cards modulo 7 is 3. There are five hands of cards having that sum: 012, 046, 136, 145, 235. Not all hands in the five hand announcement 012, 034, 056, 135, 246 in the introductory section have the same sum, but subject to the permutation of cards $s(0) = 1, s(1) = 0, s(2) = 2, s(3) = 4, s(4) = 5, s(5) = 6, s(6) = 3$ it can be transformed in the modulo 7 solution. And instead of responding by announcing Eve's card, Bob could equivalently have announced the sum of his cards modulo 7.

In [2] an 18 hand solution for $(4, 4, 1)$ and a 66 hand solution for $(5, 5, 1)$ are given, but no general method was known for $(n, n, 1)$. In this section we will present conditions for (a, b, c) for which the announcement by Alice and Bob of the sum of their cards is card safe and state informative. For $(n, n, 1)$ the answer will be: always, if $n \geq 3$.

It should be noted that the sum announcement is not always safe. For example, take card deal size $(4, 2, 1)$. Assume that A holds 0123. It is not (card) safe for A to announce that the sum of her cards is 6. The quadruples summing to 6 are: 0123 0346 0256 1246 1345. If C holds 4, then she learns that A holds 0.

Let $\sum A$ denote the sum of A's cards modulo d, and similarly for other agents, and for the deck $D = 0, 1, ..., d - 1$. For our purposes we can equate D with the ring $\mathbb{Z}_d$ of d elements, and $+$ to the sum operation defined on that ring. The announcement by an agent of the sum modulo the total number of cards is called the *sum announcement*, and the protocol consisting of A and then B announcing their sum is called the *sum announcement protocol*.

First let us note that if $c = 1$, the sum announcement informs the other agent of your cards.

Proposition 1. *If $c = 1$ and* A *announces the sum of her cards, then* B *knows* A*'s cards.*

Proof. Let x denote C's only card. Then B can easily compute

$$\sum \mathbb{Z}_d = \frac{d(d-1)}{2}$$

This sum is actually 0 when d is odd, but this is unimportant. We then have the equation

$$\sum A + \sum B + x = \sum \mathbb{Z}_d.$$

Clearly, after A's announcement, B knows all the terms in this equation, and thus can easily solve it for x. Agent A must then have the remaining cards.

The same argument applies if B announces the sum of his cards, so that:

Corollary 1. *For $(a, b, 1)$, the protocol where first* A *announces the sum of her cards and then* B *announces the sum of his cards is state informative.*

A direct result from the proof of Proposition 1 is that

Corollary 2. *A good sum announcement protocol for (a, b, c) is also good for (b, a, c).*

As we have seen in Section 2, this is not necessarily the case for other than sum announcement protocols. Now, let us characterize (card) safety. Consider the 'pair swap' property:

Pair swap (for A)
For every $x_0 \in \mathbb{Z}_d$ and every deal (A, B, C) such that $x_0 \in A$, there exist $x_1 \in A$ and $y_0, y_1 \in B$ with $x_0 \neq x_1$, $y_0 \neq y_1$, and $x_0 + x_1 = y_0 + y_1$. (1)

Proposition 2. *Suppose that the triple (a, b, c) satisfies pair swap for* A*. Then,* C *does not know any of* A*'s cards after $\sum A$ is announced.*

Proof. Let $x_0 \in \mathbb{Z}_d$. Suppose that pair swap for A holds and consider any assignment (A, B, C) with $x_0 \in A$. We will produce a new assignment (A', B', C') such that C cannot distinguish between (A, B, C) and (A', B', C'), even after the announcement of $\sum A$, and $x_0 \notin A'$. This means that C cannot know that A has x_0, and since x_0 is arbitrary, C cannot know any of A's cards.

Pick x_1, y_0 and y_1 satisfying pair swap for A and set

$$\begin{aligned} A' &= (A \setminus \{x_0, x_1\}) \cup \{y_0, y_1\} \\ B' &= (B \setminus \{y_0, y_1\}) \cup \{x_0, x_1\} \\ C' &= C. \end{aligned}$$

Then, C cannot distinguish between (A, B, C) and (A', B', C') because her cards are unchanged, and

$$\begin{aligned} \sum A' &= \sum A - (x_0 + x_1) + (y_0 + y_1) \\ &= \sum A \end{aligned}$$

(because $x_0 + x_1 = y_0 + y_1$). Thus A would have made the same announcement in both cases, and C cannot distinguish the two deals, hence cannot know that A has x_0.

Here we must note that it does not matter whether A announces $\sum A$ or B announces $\sum B$ as far as C is concerned, since she can compute one using the other. Hence for C to remain truly ignorant, we would want not only pair swap to hold for A but also the analogous property we obtain when switching A and B:

Pair swap (for B)
For every $x_0 \in \mathbb{Z}_d$ and every deal (A, B, C) such that $x_0 \in B$, there exist $x_1 \in B$ and $y_0, y_1 \in A$ with $x_0 \neq x_1$, $y_0 \neq y_1$, and $x_0 + x_1 = y_0 + y_1$. (2)

It is clear that an announcement is (card) safe if (1) and (2) hold.[5] We will now investigate when they hold. For this we need a combinatorial theorem, conjectured by Erdös and Heilbronn in [4] and proven by Dias da Silva and Hamidoune in [3]:

Proposition 3 ([3]). *Let d be a prime. For a set $A \subseteq \mathbb{Z}_d$, denote $S^n(A)$ as the set of all sums $x_1 + ... + x_n$ of n distinct elements of A. Then,*

$$|S^n(A)| \geq \min\left\{d, n|A| - n^2 + 1\right\}.$$

In particular for a prime d, any set A defines at least $2|A| - 2^2 + 1 = 2|A| - 3$ sums of pairs, if not all of $\mathbb{Z}_d$. This gives us the following:

Proposition 4. *If d is prime and both*

$$2a - 3 + (b - 1) \geq d + 1$$
$$(a - 1) + 2b - 3 \geq d + 1,$$

then announcing $\sum A$ (or $\sum B$) is card safe.

Proof. We must prove that (1) holds, as well as (2). The situation is symmetric and we shall only prove the former.

Given a card deal (A, B, C), pick $x_0 \in A$. Then,

$$|x_0 + (A \setminus \{x_0\})| = a - 1$$

since $x_0 + x_1 = x_0 + x_2$ would imply that $x_1 = x_2$ and hence we get one distinct value for each sum $x_0 + x_1$. On the other hand, by Proposition 3, $|S^2(B)| \geq 2b - 3$. Since by assumption

$$(a - 1) + 2b - 3 \geq d + 1,$$

we see that

$$|x_0 + (A \setminus \{x_0\})| + |S^2(B)| \geq d + 1.$$

[5] The two conditions also imply CA2 and CA3, respectively, in [2].

Now, there are at most d different sums modulo d. Therefore, by the pigeonhole principle, two pairs must have the same sum, and we can find

$$z \in (x_0 + (A \setminus \{x_0\}) \cap S^2(B)$$

satisfying (1).

In the case of $(n, n, 1)$ we do not need $d = 2n + 1$ to be prime, due to the following proposition.

Proposition 5. *If $|A| = n \geq 9$ and $A \subseteq \mathbb{Z}_{2n+1}$, then $|S^2(A)| \geq n + 3$.*

The proof of Proposition 5 is found in the appendix. This gives us the following

Corollary 3. *For any $n \geq 9$, announcing $\sum A$ is card safe in the $(n, n, 1)$ case.*

Proof. For $n \geq 9$, we note that given a deal (A, B, C) and $x_0 \in A$ we have $n - 1$ different sums of the form $x_0 + x_1$ with $x_0 \neq x_1$ and $x_1 \in A$. Further, by Proposition 5, $|S^2(B)| \geq n + 3$, and since

$$n - 1 + |S^2(B)| > 2n + 1,$$

there must be an element of $\mathbb{Z}_{2n+1}$ which can be written both in the form $x_0 + x_1$ with $x_1 \in A$ and $y_0 + y_1$ with $y_0, y_1 \in B$. These elements then satisfy pair swap for A. Once again, pair swap for B follows by symmetry.

We also have that

Lemma 1. *For any $3 \leq n \leq 8$, announcing $\sum A$ is card safe in the $(n, n, 1)$ case.*

Proof. The case for 3 started this section. We have used a simple Haskell script to check that the sum announcement is safe for $4 \leq n \leq 8$. (And we also note that, independently, the cases $(5, 5, 1)$ and $(6, 6, 1)$ are treated in [2].) Indeed, we have checked not only that the security result remains true for $4 \leq n \leq 8$, but also that the method of proof employed in Proposition 2 applies equally well. Namely, for each $4 \leq n \leq 8$, in every card deal of the $(n, n, 1)$ distribution, each of A's cards can be interchanged in a pair with a pair from B's cards with the same sum (modulo $2n + 1$). Pair swap for B follows by symmetry. The Haskell script and some further explanations are found in the appendix.

From Corollary 1, Corollary 3 and Lemma 1 we now obtain that

Theorem 1. *For $n \geq 3$, the sum announcement protocol is a good protocol for size $(n, n, 1)$.*

Protocols for one announcement Alice and Bob can announce their sum at the same time, and this is card safe and state informative. So we can shorten the sum announcement protocol into a single announcement protocol. This is an elementary observation, but still remarkable: for the protocols in [2] (and for all other card protocols that we know off) Bob can only make a specific response *after* Alice's announcement.

Protocols for more than two announcements For (a, b, c) where $c > 1$, the two announcement protocol of both agents announcing the sum does not work. From A's announcement, B still learns the sum of C's cards, but two cards that are held by A instead of C may also have that sum. It is conceivable that B then makes some other informative response (other than announcing *his* sum of cards!), from which A learns his cards, and may then make yet another announcement informing B of C's cards. In other words, number theory may assist us to find good protocols consisting of more than two announcements. For that, we also need to be more general than just swapping pairs.

From swapping pairs to swapping n-tuples Interestingly, in the original Russian cards problem for parameters $(3, 3, 1)$ the swapping pairs argument for showing safety fails. Let us consider the card deal 013.245.6. There is no pair of cards from 013 with the same sum as a pair of cards from 245, for otherwise the remaining cards in each hand would be equal since $0+1+3 = 2+4+5$ modulo 7. Observe that, however, safety can be easily shown by a swapping triples argument: it suffices to interchange the whole players' hands. Indeed, this is a general fact. Given a card deal of the $(3, 3, 1)$ case, if the sum of A's cards is different from the sum of B's cards, the swapping pairs argument works. Otherwise, safety can be shown by exchanging the whole hand of both players.

Employing Haskell, we have encountered several other examples (than $(3, 3, 1)$) where card safety can be shown by a swapping n–tuples argument. Given parameters (a, b, c), for each deal (A, B, C) of that size that may be a different n. This is for instance also the case for deals of size $(4, 4, 2)$, $(4, 4, 3)$, $(5, 5, 2)$, $(5, 5, 3)$, $(5, 5, 4)$, $(6, 6, 2)$, $(6, 6, 4)$, $(6, 6, 5)$, $(7, 7, 2)$, and $(7, 7, 4)$. (As C holds more than one card, none of these are state informative.) It can be even worse: for parameters $(5, 5, 9)$ the sum announcement is still card safe (checked in Haskell), but for a given deal (A, B, C) of that size, n may even vary for different cards $x \in A$. This suggests that other methods of proof for showing card safety should also be investigated.

Finally, back to swapping pairs of cards, we conjecture a strengthening of Proposition 5 that may help us find good protocols consisting of more than two announcements: *In $\mathbb{Z}_{2n+1}$, any set of size n defines at least $2n-3$ different sums of pairs.* From this conjecture follows that (straightforward proof omitted): *Given is card deal size $(a, b, 1)$. If $a + b$ is even, $b \geq a$ and $a > 5$, then after the announcement of $\sum A$ agent C does not know a single of A's cards.* For card safety, we would also need that C does not know a single of B's cards, but as a may be different from b, this now requires a separate proof.

4 Communicating local states

The models encoding what agents know in a card deal can also be seen as an interpreted system [5], namely where each processor/agent only knows his local state (namely his hand of cards), and where there is public knowledge among all agents of the set of possible global states of the system, where a global state is

an n-tuple of local states (given n agents). That a local state consists of several cards is somewhat less relevant from this perspective. The concern of the agents communicating to each other may simply be to keep their local state a secret, but they may not care about each and every of their cards. That is, the protocols should be *state safe*, but not necessarily *card safe*.

In works like [7] the basic building block for secrecy is not a card, or a state, but a *bit*. A bit may be any proposition that the communicating agents wish to share while keeping it a secret from intruders. Given a card deal of size (a, b, c), 'A and B share a secret' means that there is a proposition p such that it is public knowledge (i.e., common knowledge to A, B, and C) that A and B commonly know the value of p but that C remains ignorant of the value of p. A protocol can be called *bit safe* and *bit informative* (or 'a good protocol for bit exchange') if for each initial state of information a sequence of A, B announcements results in an information state with a shared secret.[6] We note that p typically is some factual proposition p (such as 'A holds card 0', 'the deal of cards is 012.345.6', ...), but it can be any proposition, also an epistemic statement; but this is not the situation typically considered in information theory, nor in security protocol analysis. From this perspective, *state informative is bit informative for the proposition describing the deal of cards*; and we note that this is a different proposition in every different state. There are also less obvious correspondences:

Proposition 6. *State safe is bit safe.*

Proof. Assume a state safe protocol. Let $\mathcal{L}$ be a sequence of announcements after which A and B know the card deal, but not C. Then C considers at least two deals (A, B, C) and (A', B', C') possible. As $C = C'$, $A \neq A'$. Let p be the proposition 'Agent A holds A'. Then A and B have common knowledge of p, but C does not know if p. Therefore, the protocol is bit safe.

Now, assume a bit safe protocol, with $\mathcal{L}$ the sequence of announcements realizing the shared bit p such that C does not know the value of p. (The next part of the proof refers to modal logical semantics not explained in detail, and results from [12].) From the last follows, directly from the semantics of the epistemic modal operator, that C considers at least two different possible states in the Kripke model encoding what agents know about each other in card deals. As different states are about different card deals (see Section 2), C considers at least two deals (A, B, C) and (A', B', C') possible. As $C = C'$, $A \neq A'$. Therefore, the protocol is state safe.

Similarly, one might wonder if bit informative is state informative. As said, state informative is bit informative: the description of a state is a bit. But it is quite possible to share a secret bit without disclosing all your cards. But, if it is possible to share a secret bit, is there then also another protocol to safely disclose all of your cards? We think the answer is yes, but we do not know the answer.

[6] A logical analogue exists in group announcement logic [1] with common knowledge where this corresponds to the property that there is a φ, not necessarily a propostional variable, such that $\langle \mathsf{AB} \rangle ((C_{\mathsf{AB}}\varphi \vee C_{\mathsf{AB}}\neg\varphi) \wedge \neg K_{\mathsf{C}}\varphi \wedge \neg K_{\mathsf{C}}\neg\varphi)$ is valid for initial models of card deals.

We continue by showing for a large class of (a, b, c) that they are bit safe.

4.1 Bit exchange protocols

Lemma 2 (type >). *If $a, b > c$, A and B can share a secret after public communication.*

Proof. The proof is by induction on c.

$c = 0$:

A and B already share a secret. Because C does not hold any cards, A knows that B holds the cards A does not hold, and vice versa. The entire deal of cards is common knowledge between A and B. E.g., let x be any card, then A and B now share the secret of the value of 'A holds x'.

$c > 0$:

Suppose that $a \leq b$ (or else, swap the roles of A and B). A chooses one of her own cards, say x, and two of the remaining cards, say y, z. A announces: "I hold exactly one of $\{x, y, z\}$." (Given set notation, there is no order among the three. Else, assume that A randomizes the order before the announcement.) B has either two, one, or zero of these cards. We proceed by these cases.

- If B holds both y and z, B says: "I hold two of these cards."
  A and B now share the secret of (e.g.) the value of 'A holds x'.
- If B holds one of y and z, say y, B says: "I hold one of these cards, namely y. What is your card?" A responds by saying "My card is x." It is now public knowledge that C must have card z. Continue by repeating the procedure for $(a-1, b-1, c-1)$. Note this case is also (type >). By induction hypothesis, A and B can share a secret as a result.
- If B holds neither y nor z, B says: "I hold none of those. Which one was yours?"; after which A responds by saying "My card is x." It is now public knowledge that A must have card x. Note this is only possible if $c \geq 2$. Continue by repeating the procedure for $(a-1, b, c-2)$. Note this case is also (type >). By induction hypothesis, A and B can share a secret as a result.

Lemma 3 (type =). *If $a > b = c > 0$ or $b > a = c > 0$, A and B can share a secret after public communication.*

Proof. Assume that $a > b = c > 0$ (or else, swap the roles of A and B). (Note that, if $c = b = 0$, no secret can be exchanged, as it is then public knowledge that A holds all cards.) Agent A chooses a card x from her own cards and a card y from the remaining cards. Agent A now announces: "I hold exactly one of $\{x, y\}$." (Again, assume there is no order among the two, or else A should randomize before the announcement.) If B holds y, B responds: "So do I." A and B now share a secret, e.g. that A holds x. Otherwise, B responds: "I hold neither x nor y." (It is now common knowledge to A and C that A holds x and that C holds y.) There are now two cases. (It is not an induction.)

$c = 1$:
A continues by saying: "C holds y." A and B now know the card deal.
$c > 1$:
A continues by saying: "I hold x and C holds y." Proceed with case $(a-1, b, c-1)$ of (type $>$). (If $a > b = c > 0$, then $a - 1, b > c - 1 > 0$.) In Lemma 2 we proved that A and B can then share a secret after public communication.

We combine Lemmas 2 and 3 in

Theorem 2. *Let $a, b > c$, or $a > b = c > 0$, or $b > a = c > 0$. Then* A *and* B *can share a secret after public communication.*

Theorem 2 follows from [6, Theorem 2.1] (also cited in [7]) of which the special case for two agents sharing a secret is that $a + b \geq c + 2$. We note that this involves cases where either a or b is smaller than c, unlike our conditions, so their results are more general. Like ours, the bound in [6] employs a specific construction. It is therefore unclear if that bound is sharp and if for all other card deal size (a, b, c), no secret can be shared between A and B.

At least, also a negative result is found in [7]. The special case for three agents of the matter treated in Section 6 of [7] shows that no bit exchange is possible between two given agents for card deal size $(1, 1, 1)$.

For 'can be shared' we should of course read 'can be *guaranteed* to be shared'. For any (a, b, c) with $a, b \geq 1$, if B responds: "So do I." to A's announcement "I hold exactly one of $\{x, y\}$," then A, B share a secret bit. This observation leads to (we think) a somewhat strange result—strange because it cannot be used to design safe protocols between two *given* agents A, B, and because this observation seems not to have been made in [7], a paper that is otherwise pretty comprehensive on such matters. (We write 'seems' because their terminology is different from ours and hides many implicit consequences, such as the cited [6, Theorem 2.1].) Note that for any (a, b, c): $a, b, c \geq 1$ iff there is uncertainty about the card deal.

Proposition 7. *Given (a, b, c) where there is uncertainty about the card deal, two agents can share a secret.*

Proof. Take any agent i. Let i announce: "I hold exactly one of $\{x, y\}$. The (single!) other agent j for which this also holds now responds: "So do I." Now, i and j share a secret bit. (Namely, the value of the proposition 'i holds card x'.)

4.2 A protocol for $(2, 2, 1)$ of length strictly larger than two

The bit exchange protocols above may consist of more than two announcements. But it is not proved that no shorter protocol to exchange a secret exists in those cases. For card safe protocols there are no known cases (a, b, c) for which only protocols of three or more announcements exist. In this section we present a state informative and state safe protocol of length 3.

Consider card deal size $(2, 2, 1)$. Let the actual card deal be 01.23.4. Now consider the sequence of announcements

Alice says: "I have one of 01 12 23 34 40," after which Bob says: "Eve has card 4 or card 1," after which Alice says: "Eve has card 4."

We show that this sequence is state safe and state informative. Initially, there are $\binom{5}{2} \cdot \binom{3}{2} = 30$ possible card deals. After Alice's announcement there are 15 remaining deals. In their informational setting they are:

```
01.23.4  01.24.3  01.34.2
12.03.4  12.04.3                    12.34.0
23.01.4                   23.04.1   23.14.0
                 34.01.2  34.02.1   34.12.0
         04.12.3 04.13.2  04.23.1
```

The lines stand for A-equivalence classes and the columns for C-equivalence classes. There is no visual equivalent for B-classes in this two-dimensional representation. All A-classes and all C-classes consist of three card deals, whereas some B-classes have size 2 and other B-classes have size 1. For example, if the actual deal is 01.23.4, Bob has not learnt Alice's cards, as he cannot distinguish that deal from 04.23.1. After Bob's announcement, the remaining deals are

```
01.23.4
12.03.4
         34.02.1
         04.23.1
```

It is essential that Bob's announcement is not merely 'Eve has card 1 or 4' but 'I know that Eve has card 1 or 4.' Therefore a deal like 23.01.4 is now eliminated from consideration: although Eve has card 4 in that deal, Bob cannot distinguish it from the other deal 34.01.2. Therefore, Bob considers it possible that 'Eve has card 1 or 4' is false (namely when she holds 2), and therefore he does not *know* that Eve has card 1 or 4.

Bob (of course) still doesn't know Alice's cards, Alice now knows the card deal, and again Eve remains ignorant of Alice's and Bob's hands, although she now has learnt that Alice hold card 1 and Bob holds card 3. After Alice's final announcement we retain

```
01.23.4
12.03.4
```

and we are done. For a change, let us give the protocol underlying this sequence of three announcements:

Protocol
Alice: Let ij be my own cards. Let klm be the remaining cards. My announcement is a random order of the hands ij jk kl lm mi. *Bob*: Let ij be my own cards. If after Alice's announcement I do not know the card deal and (thus) consider it possible that Eve's card is k or l, then I announce that Eve's card is k or l. If after Alice's announcement I know

the card deal, and (thus) that Eve's card is k, then I choose a card l from Alice's cards, and I announce (in random order) that Eve's card is k or l. *Alice*: I announce Eve's card.

It should be noted that for other card deals Bob would already have learnt the entire card deal from Alice's first announcement, but that he should not disclose that, because Eve would then learn the entire card deal, whatever her card was. This is because the card deals remaining if Bob announces that in response to Alice are

```
23.14.0  34.02.1  04.13.2  01.24.3  12.03.4
```

after which Eve always knows the card deal. So even when Bob knows the card deal after Alice announcement, he 'has to feign' not knowing it, by continuing to execute the protocol above.

We still have to show that there is no protocol of length two for parameters $(2, 2, 1)$. This is easy. First, observe that there is no way for Alice to inform Bob of her cards in an announcement where all hands have empty intersection: that would restrict the announcements to two hands only, e.g. 01 23. Therefore, consider an announcement wherein two hands have a card in common. If Alice were to have one of those hands (comprising three of the five cards), she considers it possible that Bob holds the remaining two cards, and thus would not be able to learn her hand of cards. Eve knows that too, and thus eliminates such hands from her consideration. Then at most one hand will remain in the announcement, so that Eve learns the card deal. For example, suppose Alice announces 01 23 04. Her hand cannot be 01 nor 04 for the reasons above. But then Eve concludes she must hold 23! In any announcement consisting of more than three 2-hands, all hands have non-empty intersection with at least one other hand.

Proposition 8. *There are* (a, b, c) *for which good protocols satisfying state safety always require more than two announcements.*

Although an elementary result, it is a remarkable result: no other case is known to us, and (despite a lot of effort) no such case is known to us for card safety.

5 Further research

We are still investigating generalizations of the sum announcement method, using n-tuple swap instead of pair swap (such as the conjectured results in Section 3). It is already clear that sum announcements are good protocols for far more (a, b, c) than just $(n, n, 1)$, and that this also goes beyond the results in [2].

We mentioned some specific open questions. Are there protocols of length three or more and that cannot be reduced to protocols of shorter length, so that A and B inform each other of their cards and C does not learn any card? Are there protocols wherein A and B inform each other of their cards, and where making this termination public keeps their secret safe? Are there card deals where you can share a bit but not your hand of cards?

Of further logical interest is a language of protocols, and a logic to check protocol properties. As known, in dynamic epistemic logics one can refer to sequences of announcements, and thus to protocols as sets of sequences of announcements. This extensional view of protocols goes a long way, but a more intensional modelling that sees a protocol as a function from agent's local states histories to announcements, would, we think, be progress. A promising logic having such features is found in [14].

Acknowledgement

Hans van Ditmarsch is also affiliated to the University of Otago. We thank Marco Vervoort for first proving an $n + 1$ lower bound version of Proposition 5. We thank the LiS anonymous reviewers for their comments.

References

1. T. Ågotnes, P. Balbiani, H. van Ditmarsch, and P. Seban. Group announcement logic. *Journal of Applied Logic*, 8:62–81, 2010.
2. M.H. Albert, R.E.L. Aldred, M.D. Atkinson, H. van Ditmarsch, and C.C. Handley. Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, 33:33–46, 2005.
3. J.A. Dias da Silva and Y.O. Hamidourne. Cyclic spaces for Grassmann derivatives and additive theory. *Bull. London Math. Soc.*, 26:140–146, 1994.
4. P. Erdös and H. Heilbronn. On the addition of residue classes modulo p. *Acta Arithmetica*, 9:149–159, 1964.
5. R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge MA, 1995.
6. M.J. Fischer and R.N. Wright. Multiparty secret key exchange using a random deal of cards. In *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 141–155. Springer-Verlag, 1992.
7. M.J. Fischer and R.N. Wright. Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology*, 9(2):71–99, 1996.
8. A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38 and 161–191, 1883.
9. T. Kirkman. On a problem in combinations. *Camb. and Dublin Math. J.*, 2:191–204, 1847.
10. K.S. Makarychev and Yu.S. Makarychev. The importance of being formal. *Mathematical Intelligencer*, 23(1):41–42, 2001.
11. D.R. Stinson. *Combinatorial Designs – Constructions and Analysis*. Springer, 2004.
12. H. van Ditmarsch. The russian cards problem. *Studia Logica*, 75:31–62, 2003.
13. J. van Eijck. DEMO — a demo of epistemic modelling. In J. van Benthem, D. Gabbay, and B. Löwe, editors, *Interactive Logic — Proceedings of the 7th Augustus de Morgan Workshop*, pages 305–363. Amsterdam University Press, 2007. Texts in Logic and Games 1.
14. Y. Wang, L. Kuppusamy, and J. van Eijck. Verifying epistemic protocols under common knowledge. In *TARK '09: Proceedings of the 12th Conference on Theoretical Aspects of Rationality and Knowledge*, pages 257–266, New York, NY, USA, 2009. ACM.

Appendix: Proof of Proposition 5 on page 8

Let us denote the elements of $\mathbb{Z}_{2n+1}$ by $0, 1, \ldots, 2n$. Throughout this proof we shall sometimes numbers as elements of $\mathbb{Z}_{2n+1}$ or just as integers so that we can, for example speak of an order. The context will always clarify which of the two is meant.

We shall consider any subset A of $\{0, 1, \ldots, 2n\}$ of size n. We are interested in the amount of different sums of pairs of two different numbers from A that we can form. This amount is invariant under shifting the whole set A along some distance. That is, $|S^2(w + A)| = |S^2(A)|$: we are interested in the number of different sums and if $x+y \neq u+v$ then $x+y+2w \neq u+v+2w$, whence shifting all points along a distance w does not affect the number of different sums of pairs. Thus, we may always assume that $0 \in A$.

We call two points $x, y \in A$ *consecutive* when either $x < y$ and for no $z \in A$ we have $x < z < y$ or when x is the largest point in A and y is the smallest point in A. Let us look at the *minimal distance between two consecutive points* in A and call this *dist*.

What can the value of *dist* be? Clearly it can be 1 but it cannot be larger than 2. For, if we fix the first point, say, at 0, then there are $2n$ points left to allocate the remaining $n-1$ points. But $3(n-1) > 2n$ for $n > 3$ thus the remaining points cannot be all at distance 3 from each other. It is easy to see that $dist = 2$ is possible. Thus our proof has two cases.

dist $= 2$

What about distance 2? The first point after 0 would be at 2 and the last point at $2n + 1 - 3$. Hence we see that necessarily we fill the remaining space with one distance of 3 and the remaining distances of 2. Without loss of generality we may assume that our first point is at 0 and the second point is at 3 and the $n-2$ remaining points all are of the form $2m+3$. It is now clear that the element 0 defines $n-1$ sums, namely $3, 5, \ldots$ Moreover, it is clear that the element 3 together with each of the $n-2$ elements of the form $3+2m$ defines a new sum. Thus, we count $(n-1)+(n-2) = 2n-3$ which is certainly at least $n+3$ for $n \geq 6$.

dist $= 1$

This case is rather more involved and needs some case distinctions. We define a *gap* to be a pair (x, y) of consecutive elements $\pmod{2n+1}$ such that $y - x \neq 1$. For example, if $n = 3$ and we consider the set $\{2, 3, 5\}$, then $(2, 3)$ are considered consecutive and not a gap, while $(5, 2)$ are considered also consecutive (given that we are looking at these as elements of the cyclic group $\mathbb{Z}_7$) but are a gap, since $2 - 5 \equiv 4 \pmod 7$.

An *interval* is a set of consecutive elements (without gaps), for example $\{2, 3, 4\}$ but not $\{2, 4\}$. Let $E \subseteq \mathbb{Z}_{2n+1}$. By SE we mean the set of sums of pairs of elements in E. Clearly $E \setminus \{0\}$ is always a subset of SE, since 0 is an element of E; we will use this fact throughout the following. We consider five cases, according to the number of gaps.

1. If we have only one gap, that means we have an interval $\{0, 1, ..., n\}$ and this gives us $2n - 3$ sums of pairs. Of course we cannot have zero gaps.
2. If we have two gaps, then E consists of two intervals, one of which has at least five elements (we are using the assumption that $n \geq 9$). We can then assume without loss of generality that $\{0, ..., 4\} \subseteq E$. Now, if we add the differences between consecutive elements this must be $2n + 1$; since we have only two gaps of width (say) g_1, g_2 this becomes $n - 2 + g_1 + g_2$. Here the $n - 2$ comes from the pairs of consecutive elements which do not form gaps. So we must have

   $$(n - 2) + g_1 + g_2 = 2n + 1$$

   which becomes

   $$g_1 + g_2 = n + 3,$$

   and thus one of the two must be at least $\lfloor \frac{n+3}{2} \rfloor$, which because $n \geq 9$ is at least 6. Then, let (x_1, y_1) and (x_2, y_2) be the two gaps, with $y_1 - x_1 \geq 6$. $E \setminus \{0\} \subseteq SE$ gives us $n - 1$ elements. Further, $x_1 + i \in SE$ with $i = 1, 2, 3$ and $x_2 + 1 \in SE$, adding up to $(n - 1) + 3 + 1 = n + 3$ elements.
3. If we have three gaps, S consists of three intervals, and at least one has three elements. Further, one gap has width at least 3, because if no gaps had width 3 we would have that the sums of differences of consecutive elements is $(n-3)+6 = n+3$, which is smaller than $2n+1$ provided that $n > 2$. We now consider two subcases:
   (a) E contains an interval with four elements. Then, we can assume without loss of generality that $\{0, 1, 2, 3\} \subseteq E$. Now, if (x, y) is a gap of width at least 3, $x + 1, x + 2 \in SE$, while the other two gaps contribute at least one element each, plus $E \setminus \{0\} \subseteq SE$ giving us a total of at least $2 + 2 + (n - 1) = n + 3$ elements.
   (b) E contains no interval with four elements. Then, E contains more than two intervals with three elements. This can be shown as follows. Let (x, y) be a gap of width at least 3. There exist three consecutive elements $z, z + 1, z + 2$ such that $z + 2 \neq x$ (since we have at least two such intervals we can pick one or the other accordingly), and thus we can assume without loss of generality that $\{0, 1, 2\} \subseteq S$ and there is a gap (x, y) of width ≥ 3 such that $x \neq 2$. But then once again $x+1, x+2 \in SE$, and the same computation as above gives us the desired bound.
4. If we have four gaps, S consists of four intervals, and at least one of them must have three elements. Thus we can assume $\{0, 1, 2\} \subseteq E$. As always $E \setminus \{0\} \subseteq SE$, and if (x, y) is a gap, then $x + 1 \in E$ giving us an extra four elements, for a total of $(n - 1) + 4 = n + 3$.
5. If there are at least five gaps, then assume without loss of generality that $\{0, 1\} \subseteq E$. In that case, at least four of the gaps are of the form (x, y) with x not equal to 1, and hence we have that $x + 1$ is an element of SE, giving us four new elements for a total of $(n - 1) + 4 = n + 3$.

```
import Data.List
-- (subsets n xs) outputs the list of all the subsets of xs of n elements.
subsets :: Int -> [Int] -> [[Int]]
subsets 0 _ = [[]]
subsets _ [] = []
subsets (n+1) (x:xs) = [x:ys | ys <- subsets n xs] ++ subsets (n+1) xs
-- (subsetSum m n xs) outputs the list of all the sums (modulo m) of the subsets of xs of n elements.
subsetSum :: Int -> Int-> [Int] -> [Int]
subsetSum m n xs =  nub [mod (sum ys) m | ys <- subsets n xs]
-- (deals a b c) generates all the deals in an (a,b,c) card distribution.
deals a b c = [[xs,ys,zs] | xs <- subsets a [0..(a+b+c-1)],
                            ys <- subsets b ([0..(a+b+c-1)] \\ xs),
                            zs <- [([0..(a+b+c-1)] \\ xs) \\ ys]]
-- (check m n as bs) checks whether each card of as can be interchanged in an n-tuple with an
-- n-tuple of elements of bs with the same sum (modulo m).
check m n as bs = and [ or [elem (mod (x+y) m) ys | y <- subsetSum m (n-1) (as \\ [x])]| x <- as]
                  where ys = subsetSum m n bs
-- (secure a b c n) checks whether for each deal of an (a,b,c) card distribution, [as,bs,cs],
-- each card of as can be interchanged in an n-tuple with an n-tuple of elements of bs with
-- the same sum (modulo a+b+c).
secure a b c n = and [check (a+b+c) n as bs | [as,bs,_] <- deals a b c]
-- (secure2 a b c) checks whether for each deal of an (a,b,c) card distribution, [as,bs,cs],
-- there exists some n <= min(a,b) such that each card of as can be interchanged in an n-tuple
-- with an n-tuple of elements of bs with the same sum (modulo a+b+c)"
secure2 a b c = and [or [check (a+b+c) n as bs | n <- [2..min a b] ]| [as,bs,_] <- deals a b c]
```

Fig. 1. The Haskell script `subsets.hs`

Appendix: Haskell script used in Lemma 1 on page 8

Figure 1 shows the Haskell script `subsets.hs`. The implemented algorithm is the natural brute force one. In the general setting of an (a, b, c) card distribution, we firstly define a function

```
deals :: Int -> Int -> Int ->  [[Int]]
```

so that `deals a b c` generates all the $\binom{a+b+c}{a} \cdot \binom{b+c}{b}$ possible card deals in an (a, b, c) card distribution. Observe that for parameters $(8, 8, 1)$ this amounts to generating 218790 card deals. Next, we define an auxiliary predicate

```
check :: Int -> Int -> [Int] -> [Int] ->  Bool
```

so that `check d k as bs` checks whether each card of A's hand as can be interchanged in an k–tuple with a k–tuple of elements of B's hand bs with the same sum (modulo d). Finally, combining `deals` and `check` we define the main *generate and test* predicate

```
secure :: Int -> Int -> Int -> Int ->  Bool
```

so that `secure a b c k` checks whether for each card deal of an (a, b, c) card distribution each card of A's hand can be interchanged in a k–tuple with a k–tuple of elements of B's hand with the same sum (modulo $a + b + c$). (For *card safety* we also have to check `secure b a c k`, namely that each card of B's hand can be interchanged in a k–tuple with a k–tuple of elements of A's hand with the same sum – but when $a = b$ this holds by symmetry, as in the case $(n, n, 1)$ below.)

Therefore, the following Haskell evaluation gives us the proof that the announcement of the sum of A's cards is also secure for $4 \leq n \leq 8$ (as well as the additional information that this fact can be established by a *swapping pairs* argument):

```
Main> and [secure n n 1 2 | n <- [4..8]] True
```

In view of the remarks in Section 3 on generalizing pair swap to swap of n-tuples, it is natural to add to our Haskell script a nonuniform version of the predicate `secure`

```
secure2 ::  Int -> Int -> Int ->  Bool
```

so that `secure2 a b c` checks whether for each card deal of an (a, b, c) card distribution there is some $k \leq min(a, b)$ such that each card of A's hand can be interchanged in a k–tuple with a k–tuple of elements of B's hand.