Secure Communication of Local States in Interpreted Systems

Michael Albert, Andrés Cordón-Franco, Hans van Ditmarsch,
David Fernández-Duque, Joost J. Joosten, and Fernando Soler-Toscano

Abstract. Given an interpreted system, we investigate ways for two agents to communicate secrets by public announcements. For card deals, 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

Interpreted systems and security. A well-known abstract architecture for distributed systems such as multi-agent systems is that of an *interpreted system* [4]. An interpreted system is a collection of global states, where a global state is an n-tuple of local states (one for each agent, given n agents). Each processor/agent only knows its local state, and there is public knowledge among all agents of the set of global states constituting the system. This creates a setting wherein we can investigate two of the agents sending messages to each other, with the intention to communicate information that remains a *secret* from other agents. The worst case scenario for security is when all messages are public. In that case, the protocol executed when sending messages can be modelled as successive *model restrictions* of the given interpreted system. We investigate two cases: that of interpreted systems

Michael Albert
University of Otago, New Zealand
e-mail: `malbert@cs.otago.ac.nz`

Andrés Cordón · Hans van Ditmarsch · David Fernández · Joost Joosten · Fernando Soler
University of Sevilla, Spain
e-mail: `{acordon,hvd,dfduque,jjoosten,fsoler}@us.es`

where the agents are card players and the secrets concern ownership of cards (an aspect of the agent's local state) (Sections 2 and 3), and that of interpreted systems in general, where the secret is the local state (Section 4).

Example. 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 [2] the *Russian Cards Problem*, and that originates with Kirkman [7]. 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 [1], 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 [6].

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 interpreted 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 [10], 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 [5]). 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.

An extended version, presented at the (informal) ESSLLI 2010 workshop Logics in Security, is available at `http://personal.us.es/hvd/newpubs/fLiSsecret1.pdf`

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. In this work we only consider protocols of length two or three.

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 [2]. The various safety and information requirements are formulas that can be checked in such a model.

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. 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. A protocol is good if it is safe and state informative.

In [1] 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 $(2,4,1)$.

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' [8]. 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 [1] 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 give such a general method for $(n,n,1)$, for $n \geq 3$.

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. 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.*

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. We only summarize the results. 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.*

A similar property, (2), must hold for B. An announcement is (card) safe if (1) and (2) hold. To find out when this is the case, we proceed combinatorially, building on results of [3] and [9].

Proposition 3 ([9]). *Let d be a prime. For a set $A \subseteq \mathbb{Z}_d$, denote $S^n(A)$ as the set of all sums $x_1 + \ldots + x_n$ of n distinct elements of A. Then, $|S^n(A)| \geq \min\left\{d, n|A| - n^2 + 1\right\}$.*

Proposition 4. *If d is prime and both $2a - 3 + (b-1) \geq d + 1$ and $(a-1) + 2b - 3 \geq d + 1$, then announcing $\sum A$ (or $\sum B$) is card safe.*

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

This gives us the following

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

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.*

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 [1] (and for all other card protocols that of which we know) 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 cases where card safety can be shown by a swapping n–tuples argument. We also conjecture a strengthening of Proposition 5. (Details omitted.)

4 Communicating Local States

As said, the models encoding what agents know in a card deal can also be seen as an interpreted system [4], 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 [6] 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. 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.*

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.

One can show for a large class of (a,b,c) that they are bit safe. Our results can be summarized as follows. Theorem is a straight consequence of Lemma's 2 and 3.

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

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

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 also follows from [5, Theorem 2.1] 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. However, it is unclear if our (or their) bounds are sharp and if for all other card deal size (a,b,c), no secret can be shared between A and B. There are cases for which no secret can be shared, e.g., $(1,1,1)$.

We have two other interesting results to report. First, if you don't care *which* two agents share the secret, a secret can always be shared (even for $(1,1,1)$!).

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’.)

Second, bit exchange protocols above may consist of (strictly) more than two announcements. One case is $(2,2,1)$. (Details omitted.)

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

5 Further Research

Of further logical interest is a language of protocols, and a logic to check protocol properties. A promising logic having such features is found in [11].

Acknowledgement. We thank Marco Vervoort for first proving an $n+1$ lower bound version of Proposition 5. We thank the PAAMS anonymous reviewers for their comments. Joost Joosten is currently affiliated to Dept. Lògica, Història i Filosofia de la Ciència, Universitat de Barcelona. Hans van Ditmarsch is also affiliated to the Institute of Mathematical Sciences Chennai (IMSC), India.

References

1. Albert, M., Aldred, R., Atkinson, M., van Ditmarsch, H., Handley, C.: Safe communication for card players by combinatorial designs for two-step protocols. Australasian Journal of Combinatorics 33, 33–46 (2005)
2. van Ditmarsch, H.: The Russian cards problem. Studia Logica 75, 31–62 (2003)
3. Erdös, P., Heilbronn, H.: On the addition of residue classes modulo p. Acta Arithmetica 9, 149–159 (1964)
4. Fagin, R., Halpern, J., Moses, Y., Vardi, M.: Reasoning about Knowledge. MIT Press, Cambridge (1995)
5. Fischer, M., Wright, R.: Multiparty secret key exchange using a random deal of cards. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 141–155. Springer, Heidelberg (1992)
6. Fischer, M., Wright, R.: Bounds on secret key exchange using a random deal of cards. Journal of Cryptology 9(2), 71–99 (1996)
7. Kirkman, T.: On a problem in combinations. Camb. and Dublin Math. J. 2, 191–204 (1847)
8. Makarychev, K., Makarychev, Y.: The importance of being formal. Mathematical Intelligencer 23(1), 41–42 (2001)
9. da Silva, J.D., Hamidourne, Y.: Cyclic spaces for Grassmann derivatives and additive theory. Bull. London Math. Soc. 26, 140–146 (1994)
10. Stinson, D.: Combinatorial Designs – Constructions and Analysis. Springer, Heidelberg (2004)
11. Wang, Y.: Epistemic modelling and protocol dynamics. Ph.D. thesis, University of Amsterdam, ILLC Dissertation Series DS-2010-06 (2010)