

Secure protocols using card deals

Hans van Ditmarsch
University of Sevilla, Spain
hvd@us.es

Secure protocols using card deals

The setting:

- ▶ We assume a set of players and a set of cards.
- ▶ The cards are randomly distributed over the players.
- ▶ The result is uncertainty over the card deal.
- ▶ Can players share a secret?

Problems to solve:

- ▶ What secrets can be shared?
- ▶ What protocols are allowed?
- ▶ Does a protocol exist to exchange a particular secret?
- ▶ What is the minimum length of such a protocol?
- ▶ What other information leaks while sharing the secret?
- ▶ How does this relate to key encryption and key decryption?

Secure protocols using card deals

The setting:

- ▶ We assume a set of players and a set of cards.
Three players A, B, C and a finite set of all different cards $0, 1, \dots, n$.
- ▶ The cards are randomly distributed over the players.
Three players A, B, C draw a, b, c cards from the set.
- ▶ The result is uncertainty over the card deal.
Three cards. If A, B, C hold card $0, 1, 2$ resp., A does not know if B holds 1 or if B holds 2.

Secure protocols using card deals

Problems to solve:

- ▶ What secrets can be shared?
Seven cards. If A, B, C hold $\{0, 1, 2\}$, $\{3, 4, 5\}$, 6 resp., A can inform B of her cards such that all her cards remain secret to C , or such that some of her cards remain secret to C .
- ▶ What protocols are allowed?
Protocols consist of public announcements. (And not private actions, such as handing over cards, whispering, ...)
- ▶ Does a protocol exist to exchange a particular secret?
For seven cards: yes. For less than seven: no.

The remaining questions will be dealt with later.

Russian Cards

From a pack of seven known cards 0, 1, 2, 3, 4, 5, 6 Alice (A) and Bob (B) each draw three cards and Cathy (C) gets the remaining card. How can Alice and Bob openly (publicly) inform each other about their cards, without Cathy learning of any of their cards who holds it?

- ▶ Presented at Moscow Mathematics Olympiad 2000.
- ▶ Thomas Kirkman, *On a problem in combinations*, Cambridge and Dublin Mathematical Journal 2: 191-204, 1847.



Russian Cards

Suppose Alice draws $\{0, 1, 2\}$, Bob draws $\{3, 4, 5\}$, and Cathy 6.

- ▶ **near-solution – analysis in epistemic logic**

A: “I have 012 or B has 012,” B : “I have 345 or A has 345.”

- ▶ **solution**

A: “I have one of 012 034 056 135 146 236 245,” B : “ C has 6.”

- ▶ **solution – with bias?**

A: “I have one of 012 034 056 135 246,” B : “ C has 6.”

- ▶ **solution – other secret exchanged**

A: “I have one of 012 034 056,” B : “ C has 6.”

- ▶ **longer protocols, other secrets**

From a pack of **five** known cards 0, 1, 2, 3, 4 Alice and Bob each draw **two** cards and Cathy gets the remaining card.

Russian Cards

A: "I have one of 012 034 056 135 146 236 245," B: "C has 6."

Initially, there are $\binom{7}{3} \cdot \binom{4}{3} = 140$ card deals.

After A's announcement.

012.345.6	012.346.5	012.356.4	012.456.3		
034.125.6	034.126.5			034.156.2	034.256.1
		056.123.4	056.124.3	056.134.2	056.234.1
135.024.6		135.026.4		135.046.2	135.246.0
	146.023.5		146.025.3	146.035.2	146.235.0
	236.014.5	236.015.4			236.045.1
245.013.6			245.016.3		245.036.1
					245.136.0

Russian Cards

A: "I have one of 012 034 056 135 146 236 245," B: "C has 6."

Initially, there are $\binom{7}{3} \cdot \binom{4}{3} = 140$ card deals.

After A's announcement.

After B's announcement.

012.345.6	012.346.5	012.356.4	012.456.3			
034.125.6	034.126.5			034.156.2	034.256.1	
		056.123.4	056.124.3	056.134.2	056.234.1	
135.024.6		135.026.4		135.046.2	135.246.0	
	146.023.5		146.025.3	146.035.2	146.235.0	
	236.014.5	236.015.4			236.045.1	236.145.0
245.013.6			245.016.3		245.036.1	245.136.0

Russian Cards — near-solutions

A: “I have 012 or B has 012,” B: “I have 345 or A has 345.”

If “A has 012 or B has 012” is announced by an outsider, C is (still) ignorant. If announced by A, the card deal is common knowledge. Agents do not merely announce what is true, but what they *know* to be true.

A: “I do not have card 6,” B: “C has card 6.”

C is ignorant, but A does not know that C is ignorant. A different execution of the underlying protocol (I do not have 5) would be informative for C.

A: “I have 012, or none of these cards,” ...

C is ignorant, A knows that C is ignorant, but C does not know that A knows that C is ignorant. All executions (one!) of the underlying protocol are safe; but C may assume that A executes a safe protocol. A's intention to keep the secret, reveals the secret.

C is ignorant, A knows that C is ignorant, C knows that A knows that C is ignorant, ...? Common knowledge that C is ignorant!

Card deals - logic

Sets of possible card deals

Interpreted system, Kripke model, state transition system ...

Players only know their own cards.

A hand of cards is a local state.

A deal of cards is a global state.

Epistemic postconditions

agent n holds card i

i_n

n 's hand of cards is $\{i, j, k\}$

$ijk_n \quad (i_n \wedge j_n \wedge k_n)$

B knows A 's hand

$\bigwedge_{i \neq j \neq k=0,1,\dots} (ijk_A \rightarrow K_B ijk_A)$

A knows B 's hand

$\bigwedge_{i \neq j \neq k=0,1,\dots} (ijk_B \rightarrow K_A ijk_B)$

C is ignorant

$\bigwedge_{i=0,1,\dots} (\neg K_C i_A \wedge \neg K_C i_B)$

Announcements

$012_A \vee 034_A \vee \dots$

Card deals - issues with common knowledge

There are situations where C is ignorant but where this cannot be revealed by A or B , at the price of informing C . Announcing that the protocol has terminated is such a dangerous revelation.

It is not sufficient that C is ignorant. It is also not sufficient that A and B have common knowledge of C 's ignorance. We need public knowledge (common knowledge of A, B, C) of C 's ignorance.

It is also not sufficient that A and B have common knowledge that they know each other's cards. We need public knowledge that A and B know each other's cards.

Necessary and sufficient epistemic postconditions

B knows A 's hand $C_{ABC} \bigwedge_{i \neq j \neq k=0,1,\dots} (ijk_A \rightarrow K_B ijk_A)$

A knows B 's hand $C_{ABC} \bigwedge_{i \neq j \neq k=0,1,\dots} (ijk_B \rightarrow K_A ijk_B)$

C is ignorant $C_{ABC} \bigwedge_{i=0,1,\dots} (\neg K_C i_A \wedge \neg K_C i_B)$

On Kripke models this amounts to requiring that the postconditions are model validities.

Card deals - common knowledge and Kerckhoffs' principle

The requirement that postconditions are public knowledge is according to Kerckhoffs' principle in cryptography:

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Auguste Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires 9:5–83, 1883.



Card deals - combinatorics

Sets of possible card deals

Sets of possible hands of cards for each player

Parameters (a, b, c) .

A holds a cards, B holds b cards, C holds c cards.

An announcement \mathcal{L} by A is a collection of a -sets.

Ways to partition $n = a + b + c$ cards into *blocks* of a cards.

Design theory!

Design theory — block designs

What is a t - (n, k, λ) design?

Given a set N of n points a *design* is a collection of subsets of N of size k called *blocks* such that every subset of N of size t is contained in exactly λ blocks. A design *may* help us find announcements after which the epistemic conditions are satisfied.

Example 012 034 056 135 146 236 245

- ▶ 1- $(7, 3, 3)$ design: Given a set of 7 cards $\{0, 1, 2, 3, 4, 5, 6\}$ this is an announcement of hands (3-sets) with the property that every card (1-subset) is contained in exactly 3 hands.
- ▶ 2- $(7, 3, 1)$ design: Given a set of 7 cards $\{0, 1, 2, 3, 4, 5, 6\}$ this is an announcement of hands (3-sets) with the property that every pair (2-subset) is contained in exactly 1 hand.
- ▶ It is not a 3-design. It contains 012, but not 013.

Card deals - logic and combinatorics

Knowledge conditions (model validities, com. knowl. implicit!)

Whenever \mathcal{L} can be announced, then after doing so:

BKA B knows A 's hand.

(**AKB** A knows B 's hand.)

CIA C does not know any of A 's cards.

CIB C does not know any of B 's cards.

Combinatorial axioms

CA_{BKA} For every b -set X there is at most one member of \mathcal{L} that avoids X .

CA_{CIA} For every c -set X the members of \mathcal{L} avoiding X have empty intersection.

CA_{CIB} For every c -set X the members of \mathcal{L} avoiding X have union consisting of all cards except those of X .

Combinatorial axioms for Russian Cards

CA_{BKA} For every b -set X there is at most one member of \mathcal{L} that avoids X .

CA_{CIA} For every c -set X the members of \mathcal{L} avoiding X have empty intersection.

CA_{CIB} For every c -set X the members of \mathcal{L} avoiding X have union consisting of all cards except those of X .

A: "I have 012 034 056 135 146 236 245."

012.345.6	012.346.5	012.356.4	012.456.3		
034.125.6	034.126.5			034.156.2	034.256.1
		056.123.4	056.124.3	056.134.2	056.234.1
135.024.6		135.026.4		135.046.2	135.246.0
	146.023.5		146.025.3	146.035.2	146.235.0
	236.014.5	236.015.4			236.045.1
245.013.6			245.016.3		245.036.1
					245.136.0

The case (a, b, c)

An announcement is good if it satisfies CA_{BKA} , CA_{CIA} , CA_{CIB} .

For which (a, b, c) are there good announcements?

Modulo symmetry and other equivalence considerations, there are two good announcements for parameters $(3, 3, 1)$.

A characterization is unknown, but there are some general results. There is a good announcement for (a, b, c) :

- ▶ only if $c < a - 1$, only if $c < b$;
- ▶ given a and b , for sufficiently large b ;
(Choose b such that $a + b + c = p^2 + p + 1$ for a prime p .)
- ▶ for $(a, 2, 1)$ if $a = 0, 4 \pmod{6}$;
(It is the complement of a $b - (a + 2b - 1, 2b - 1, 1)$ -design.)
- ▶ for $(3, b, 1)$ if $b \geq 3$;
- ▶ for $(a, b, c + 1)$ if we have one for (a, b, c) .

Card occurrence bias

- ▶ Two different solutions for Russian Cards are
012 034 056 135 146 236 245
012 034 056 135 246
- ▶ All cards occur equally often in *012 034 056 135 146 236 245*.
- ▶ 0 occurs more often than other cards in *012 034 056 135 246*.
- ▶ **Is *A* therefore more likely to have 0 than another card?**

There are two approaches to solve this problem:

- ▶ Additional combinatorial axiom requiring that all cards occur equally often in the announcement.
- ▶ Protocols such that card occurrence in the announcement is unrelated to the actual hand. (The announcement should be seen as the execution of the protocol.)

Longer protocols to communicate hands of cards

We have seen protocols **to communicate hands of cards** that consist of one announcement by A , after which B knows the card deal, followed by B revealing the cards of C .

It is unknown if there are card deals for which more than two announcements are required.

To communicate other secrets there are card deals for which more than two announcements are required.

Communication of local states

Parameters (3, 3, 1) (assume card deal 012.345.6)

Russian Cards:

A: "I have one of 012 034 056 135 146 236 245," B: "C has 6."

When individual cards may be learnt, but not the entire hand:

A: "I have one of 012 034 056," B: "C has 6."

C knows that A has 0, but does not know that A's hand is 012.

No good protocol for $(2, 2, 1)$ with two ann.!

If a good protocol consists of two announcements only, A *must* inform B in her first announcement.

Given is an announcement \mathcal{L} by A .

There are only two possibilities:

- ▶ All hands have empty intersection. She can then only announce two hands. A can inform B of her hand, but cannot prevent C from learning it too.
- ▶ Two hands have a card in common. If A were to have one of those hands (comprising three of the five cards), she considers it possible that B holds the remaining two cards. Then B would not learn A 's hand.

Therefore, such an announcement is not good.

A protocol of three announcements for (2, 2, 1)

Suppose the actual card deal is 01.23.4.

A: "I have one of 01 12 23 34 40,"

B: "C has card 4 or card 1,"

A: "C has card 4."

There are $\binom{5}{2} \cdot \binom{3}{2} = 30$ possible card deals.

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	

A protocol of three announcements for (2, 2, 1)

Suppose the actual card deal is 01.23.4.

A: "I have one of 01 12 23 34 40,"

B: "C has card 4 or card 1,"

A: "C has card 4."

There are $\binom{5}{2} \cdot \binom{3}{2} = 30$ possible card deals.

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	

A protocol of three announcements for (2, 2, 1)

Suppose the actual card deal is 01.23.4.

A: "I have one of 01 12 23 34 40,"

B: "C has card 4 or card 1,"

A: "C has card 4."

There are $\binom{5}{2} \cdot \binom{3}{2} = 30$ possible card deals.

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	

Protocols for communication of local states

Agents can communicate local states to each other if and only if they can share a secret bit after communication. For which (a, b, c) can A and B share a secret bit? We have some results in ongoing work.

- ▶ If $a, b > c$, A and B can share a secret.
- ▶ If $a > b = c > 0$, then A and B can share a secret
- ▶ If $a, b, c > 0$, then A can share a secret with B or with C .

But not when choosing either one in advance! Ask B if he has one of $\{x, y\}$ — where x is one of A 's cards and y is one of the other cards. If B answers 'yes', A shares a secret with B . (E.g., the value of the proposition 'A has card x .) Otherwise, A shares a secret with C .

Novel ideas — abduction

- ▶ The initial model where players only know their hands of cards is described by a theory T .

This is a theory in multi-agent epistemic logic with common knowledge.

- ▶ Initially, the epistemic postconditions C do not hold:

$$T \not\models_{\text{dyn}} C.$$

- ▶ The epistemic postconditions C are conclusions to be derived from a dynamic expansion of that theory: we are looking for a sequence of announcements A_1, \dots, A_n such that

$$T, A_1, \dots, A_n \models_{\text{dyn}} C.$$

This is a dynamic consequence relation \models_{dyn} such that

$$T \models [A_i] \dots [A_n] C \iff T, A_1, \dots, A_n \models_{\text{dyn}} C$$

Note that \models_{dyn} is substructural, premisses A_i do not commute!

- ▶ Abductive techniques for tableaux completion may apply to solve this problem.

Novel ideas — infinite card deals

From protocols for card deals to protocols with key encryption.

- ▶ Suppose we have an infinite set of cards.
- ▶ In Russian Cards, actual hand 012 is weakened in the message to 012 034 056 135 146 234 256: a finite disjunction of hands.
- ▶ Given infinitely many cards, we can weaken the actual hand in the message to an infinite disjunction. “My hand of cards is 012 or 034 or ...”
- ▶ The operation of weakening to an infinite disjunction is like applying a one-way function: encryption.
- ▶ A player holding infinitely many cards, can eliminate infinitely many disjuncts from such a message. He has the power of decryption.
- ▶ To be continued...

Other work, further plans

- ▶ bit exchange protocols (Fischer & Wright, *Bounds on secret key exchange using a random deal of cards*; Stiglic, *Computations with a deck of cards*)
- ▶ authentication codes using orthogonal arrays (Stinson, *Combinatorial Designs*)
- ▶ large card deals to reducing probability of correct guesses
In 012 034 056 135 146 236 245, probability is 25 %.

Own references

- ▶ Albert et al., *Safe communication for card players by combinatorial designs for two-step protocols*
- ▶ Atkinson, van Ditmarsch, Roehling, *Avoiding bias in cards cryptography*
- ▶ van Ditmarsch et al., *Secure communication of local states in multi-agent systems* (in progress)
- ▶ van Ditmarsch, *The Russian Cards problem*
- ▶ van Ditmarsch, *The case of the hidden hand*