Unconditionally secure protocols with card deals

Hans van Ditmarsch
University of Otago, New Zealand & IRIT, France

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

Russian Cards

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

- **near-solution – analysis in epistemic logic NOT TODAY**
  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 – to a different problem**
  A: "I have one of 012 034 056," B: "C has 6."
- **longer protocols, different problem**
  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	236.145.0
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~~

Thomas Kirkman
On a problem in combinations
Cambridge and Dublin Mathematical Journal 2: 191-204, 1847

Card deals - logic (after all?)

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.

Sufficient 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	$C_{ABC} \bigwedge_{i\neq i\neq k=0,1,\ldots} (ijk_A \rightarrow K_B ijk_A)$
A knows B's hand	$C_{ABC} \bigwedge_{i\neq i\neq k=0,1,\ldots} (ijk_B \rightarrow K_A ijk_B)$
C is ignorant	$C_{ABC} \bigwedge_{i=0,1,\ldots} (\neg K_C i_A \wedge \neg K_C i_B)$

Announcements

$$012_A \vee 034_A \vee \ldots$$

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 $v = a + b + c$ cards into blocks of a cards, ...
Design theory!

Card deals - logic and combinatorics

Knowledge conditions

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 (seven hands)

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	236.145.0
245.013.6			245.016.3		245.036.1	245.136.0

Combinatorial axioms for Russian Cards (five hands)

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 012 034 056 135 246."

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?
We now know two good announcements for parameters $(3, 3, 1)$.

C must hold fewer cards than A

CA_{BKA} can only hold if $c < a$.

Suppose that CA_{BKA} holds. Then for two a-sets $L_1, L_2 \in \mathcal{L}$, the set $\Omega \setminus (L_1 \cup L_2)$ consists of less than b cards, because any b-set can avoid only one but not a-sets. We now have:

$$\begin{aligned} |\Omega \setminus L_1 \cup L_2| &< b \\ a + b + c - 2a + |L_1 \cap L_2| &< b \\ |L_1 \cap L_2| &< a - c \end{aligned}$$

A bit harder to prove (counting the number of card occurrences in $\mathcal{L}$ gives upper and lower bounds for its size) is that:

CA_{BKA} can only hold if $c < a - 1$.

C must hold fewer cards than B

For the three combinatorial axioms to hold simultaneously, C must hold fewer cards than B.

In plain words: B must have an informational advantage over C.

Good announcement: given a and c, for sufficiently large b

Choose a prime $p \geq a - 1$ such that $v = a + b + c = p^2 + p + 1$.
Choose a *difference set* when counting modulo v.
Differences construct all non-zero members.
Add these to (any a-subset of) the difference set.
This is a good announcement.

Example Let $p = 2$. Then $p^2 + p + 1 = 7$.
Consider $\{0, 1, 2, 3, 4, 5, 6\}$ and subset (difference set) $\{0, 1, 5\}$.

$$1 - 0 = 1 \quad 0 - 1 = 6 \quad 0 - 5 = 2$$
$$5 - 0 = 5 \quad 5 - 1 = 4 \quad 1 - 5 = 3$$

A good announcement (modulo permutation same as previous) is:

015 126 230 341 452 563 604

Good announcement for $(3, b, 1)$, if $b \geq 3$

Suppose the number of points $v = b + 4$ is a multiple of 3, say $3m$.
As points we take symbols $0_i, 1_i, 2_i$ with $0 \leq i < m$.
Consider the set of $2m$ lines

$$\{0_i, 1_i, 2_i\}, \{0_i, 1_{i+1}, 2_{i+2}\}$$

where $0 \leq i < m$ and subscripts are interpreted modulo m.
This is a good announcement if $m \geq 3$.

(Simple adjustments for $v = 1 \mod 3$ and for $v = 2 \mod 3$.)

Example Let $m = 3$. Then the announcement is:

$$\begin{array}{ll} 0_0 1_0 2_0 & 0_0 1_1 2_2 \\ 0_1 1_1 2_1 & 0_1 1_2 2_0 \\ 0_2 1_2 2_2 & 0_2 1_0 2_1 \end{array}$$

More good announcements

From a good ann. for $(a, b, c+1)$ *we construct one for* (a, b, c)*.*

Given (a, b, c), A publicly announces a virtual card q.
Then A makes a good announcement for $(a, b, c+1)$.

There may be a good ann. for (a, b, c) *but not for* (b, a, c)*.*

There is one for $(4, 2, 1)$ (next slide), but not for $(2, 4, 1)$.
Parameters $(2, 4, 1)$ do not satisfy that $a \leq c - 1$.

Good announcement for $(a, 2, 1)$ if $a = 0, 4 \mod 6$

If D is a $b-(a+2b-1, 2b-1, 1)$-design, then $\overline{D}$ is a good announcement for $(a, b, b-1)$ where $\overline{D}$ denotes the set of lines that are the complements of the blocks of D.

There is such a design for $(a, 2, 1)$ if $a = 0, 4 \mod 6$.

Good announcement for $(a, 2, 1)$ if $a = 0, 4 \mod 6$

If D is a $b-(a+2b-1, 2b-1, 1)$-design, then $\overline{D}$ is a good announcement for $(a, b, b-1)$ where $\overline{D}$ denotes the set of lines that are the complements of the blocks of D.

There is such a design for $(a, 2, 1)$ if $a = 0, 4 \mod 6$.

Let's skip this....
What is a $b-(a+2b-1, 2b-1, 1)$ design anyway?

Block designs

What is a $b-(a+2b-1, 2b-1, 1)$ design?

What is a t-(v, k, λ) design?

Given a v-set Ω this is a collection of k-subsets of Ω called *blocks* such that every t-subset of Ω is contained in exactly λ blocks.

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 three 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 one hand.
- It is not a 3-design. It contains 012, but not 013.

Card occurrence bias

- 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?
  That depends on the protocol producing the announcement.
  We present biased and unbiased protocols.
- Both announcements satisfy the combinatorial axioms.
  How about an additional axiom that makes a difference?
  We formulate such an axiom.

Card occurrence bias – an additional combinatorial axiom

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.

For each possible hand of cards for C, all other cards occur equally often in the hands of A's announcement that avoid it.

CA_{BIAS} For every c-set X there is a number n_X such that for every point $x \notin X$ there are n_X lines in $\mathcal{L}$ avoiding X that contain x.

Binary designs

Consider the design whose points are the 2^n points of a n-dimensional vector space over $GF(2)$ and whose lines are the affine hyperplanes ($(n-1)$-dimensional subspaces and their complementary cosets), of which there are $2(2^n - 1)$.

Binary designs

Consider the design whose points are the 2^n points of a n-dimensional vector space over $GF(2)$ and whose lines are the affine hyperplanes ($(n-1)$-dimensional subspaces and their complementary cosets), of which there are $2(2^n - 1)$.

Here we go again...

Binary designs

Let $n \geq 3$. For all $2^n - 1$ n-bit vectors $(y_1, y_2, ..., y_n)$ (all zeros excluded) solve $x_1y_1 + x_2y_2 + ... + x_ny_n = 0$, where $x_i = 0, 1$. Each of 2^{n-1} solutions $x_1x_2...x_n$ represents a point in binary. Together they constitute a line. The binary points *not* present in it also form a line. The total of $2(2^n - 1)$ lines constitutes a binary design.

Binary designs are good announcements for *some* $(a, b, c) = (2^{n-1}, 2^{n-1} - c, c)$.

Example $(4, 3, 1)$, $(8, 7, 1)$, $(8, 6, 2)$, not $(8, 5, 3)$, ...

Example binary design: Steiner quadruples

A binary design for $n = 3$ (Steiner quadruples) is a good announcement for $(4, 3, 1)$.

Each line (hand) consists of $2^{3-1} = 4$ points. The $2^3 - 1 = 7$ non-zero 3-bit vectors are

001 010 011 100 101 110 111.

Take their orthogonal complements (and cosets). For 001 these are

000 010 100 110 (0246) and 001 011 101 111 (1357).

The resulting announcement of $2(2^3 - 1) = 14$ lines is

0246 0145 0347 0123 0257 0167 0356 1357 2367 1256 4567 1346 2345 1247

CA_{BIAS} is satisfied:
For each card, each other card occurs in *four* remaining hands.

Card occurrence bias – results

CA_{BIAS} For every c-set X there is a number n_X such that for every point $x \notin X$ there are n_X lines in $\mathcal{L}$ avoiding X that contain x.

Given parameters $(a, b, 1)$.
If CA_{BIAS} holds then n_x is independent of x.

Binary designs satisfy CA_{BIAS} for $c = 1$.

Binary designs are good announcements for $c = 1$.
(They also satisfy combinatorial axioms CA_{BKA}, CA_{CIA}, CA_{CIB}.)

Card occurrence bias - unbiased protocols

A says "My hand is one of 012, 034, 056, 135, 246."
Does this imply that A is more likely to have 0 than other cards?

What is the protocol producing this announcement?

60 five-hand announcements contain a given actual hand:

- 36 containing a card in the actual hand thrice.
  3 actual cards $\times$ *3 ways to make three hands with actual card* $\times$ $(2 \cdot 2)$ *ways to make remaining two hands*
- 24 not containing a card in the actual hand thrice.
  4 non-actual cards thrice $\times$ $(2 \cdot 2)$ *ways to make those hands (one of remaining is actual hand, other fixed)*

Choose randomly between the 36 and the 24: unbiased.
Choose randomly among 60: odds 3 to 2 that triple card is actual.

Card occurrence bias - unbiased protocols

A: "In all my announcements 0 will occur thrice."
A: "I have one of 012, 034, 056, 135, 246."
This does not imply that A is more likely to have 0.

12 announcements containing actual card 0 thrice – assume 012:

012 034 056 135 246	012 034 056 136 245
012 034 056 145 236	012 034 056 146 235
012 035 046 134 256	012 035 046 136 245
012 035 046 145 236	012 035 046 156 234
012 036 045 134 256	012 036 045 135 246
012 036 045 146 235	012 036 045 156 234

6 announcements containing other card 0 thrice – assume 135:

012 034 056 135 246	012 036 045 135 246
014 023 056 135 246	014 025 036 135 246
016 023 045 135 246	016 025 034 135 246

Choose between the 12 and the 6 with odds 4 to 3: unbiased.
Choose randomly among 18: odds 3 to 2 that triple card is actual.

Communication of local states only

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."

Communication of local states only

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."

Parameters $(2, 3, 1)$ (assume card deal 12.345.6)
A: "I have one of 12 34 56," B: "C has 6."

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. C knows that too, and thus eliminates such hands from her consideration. Repeating this, at most one hand will remain. (If $\mathcal{L}$ consists of more than three hands, all hands have non-empty intersection with at least one other 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	

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."

The underlying protocol is

A: 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. B: Let ij be my own cards. If after A's announcement I do not know the card deal and (thus) consider it possible that C's card is k or l, then I announce that C's card is k or l. If after A's announcement I know the card deal, and (thus) that C's card is k, then I choose a card l from A's cards, and I announce (in random order) that C's card is k or l. A: I announce C's card.

Combinatorial axioms

LS1a For every b-set, there must be at most one a-set in $\mathcal{L}_A$ avoiding it.

LS1b For every a-set, there must be at most one b-set in $\mathcal{L}_B$ avoiding it.

LS2a For every c-set, there must be at least two a-sets in $\mathcal{L}_A$ avoiding it.

LS2b For every c-set, there must be at least two b-sets in $\mathcal{L}_B$ avoiding it.

Some general constructions are in progress.

What this is good for? What has been done?

- 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*)
- block ciphers?
- large card deals to reducing probability of correct guesses *In 012 034 056 135 146 236 245, probability is 25 %.*

Work done:

- Albert et al., *Safe communication for card players by combinatorial designs for two-step protocols*
- Atkinson, van Ditmarsch, Roehling, *Avoiding bias in cards cryptography* (under submission)
- van Ditmarsch, *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*