Who holds the best card?
Secure communication of optimal secret bits

Hans van Ditmarsch (CNRS / LORIA, Nancy)

joint work with:
David Fernández Duque (Ghent University)
Vaishnavi Sundararajan (IRISA, Rennes)
S.P. Suresh (CMI, Chennai)



Russian Cards

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

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

- 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 Eve 6.

Standard 7-hand solution (there are also 5 and 6 hand solutions)

Alice: "I have one of 012 034 056 135 146 236 245,"
Bob: "Eve has 6."

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

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

Standard 7-hand solution (there are also 5 and 6 hand solutions)

Alice: "I have one of 012 034 056 135 146 236 245,"
Bob: "Eve has 6."

After Alice's announcement.
After Bob'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

Who holds the best card? (Smaller is better, 0 is best)

From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ *Alice and Bob each draw three cards and Eve gets the remaining card. How can Alice and Bob openly inform each other about ~~their cards~~ the best card between them, without Eve learning of ~~any of their cards~~ that card who holds it?*

Alice: "I have one of ~~012 034 056 135 146 236 245~~ 012 034 135 246,"
Bob: ~~"Eve has 6."~~ "The best card between us is 0."

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	
135.024.6		135.026.4		135.046.2		135.246.0
	246.013.5		246.015.3		246.035.1	246.135.0

Who holds the best card? (Smaller is better, 0 is best)

From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ *Alice and Bob each draw three cards and Eve gets the remaining card. How can Alice and Bob openly inform each other about ~~their cards~~ the best card between them, without Eve learning of ~~any of their cards~~ that card who holds it?*

Alice: "I have one of ~~012 034 056 135 146 236 245~~ 012 034 135 246,"
Bob: ~~"Eve has 6."~~ "The best card between us is 0."

After A's announcement.
After Bob'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	
135.024.6		135.026.4		135.046.2		135.246.0
	246.013.5		246.015.3		246.035.1	246.135.0

Best Card Protocols

So far, we considered a pack of 7 cards, where Alice holds 3 cards, Bob holds 3 cards, and Eve holds 1 card. We call this the instance $(3, 3, 1)$ of the best-card problem. A solution consisting of two announcements is called a two-step best-card solution, with the first step (Alice's announcement) consisting of four hands. It is called best-card to distinguish it from an all-card solution, such as the seven hand solution before.

Any card that cannot be the best card between Alice and Bob is called a bad card. And those that can be, are good cards. So 0 and 1 are good cards. If there are 7 cards, $2, 3, 4, 5, 6$ *are bad. But if there are more than 7 cards, all higher cards are also bad.*

This is useful:

— Bad cards can be revealed in protocols.

— Bad cards are interchangeable in protocols.

Best Card Protocols — using bad cards

Consider again announcement 012 034 135 246.
Let Alice have another hand of cards: 146. What to do?
She applies injection $(0,0),(1,1),(2,2),(3,4),(5,6),(4,5),(6,3)$.
The injection should be the identity on the good cards 0 and 1!
The result is announcement 012 045 146 235.
This is now the solution.

Now suppose Alice has 4 cards, and hand 1467. Easy :
Same injection, and add the bad card 7: 0127 0457 1467 2357.

Now suppose Alice still has 3 cards 146 but Bob has 5 cards.
Easy : Same injection and same announcement 012 045 146 235.

Theorem If $a, b \geq 3$, then $(a, b, 1)$ is best-card solvable in two steps with four hands.

Theorem If $a, b \geq 5$, then $(a, b, 2)$ is best-card solvable in two steps with ten hands.

Best Card Protocols — protocols based on bit exchange

— Consider card deal $(012, 3456, 7)$.
— Alice holds one bad card, 2, and all Bob's cards are bad.
— Bob chooses a bad card he holds, 3,
and a bad card he does not hold, 2.
— Bob asks Alice: "Do you hold one of $\{2, 3\}$?"
— Alice answers: "Yes."
— Alice and Bob now share a secret bit.
— The secret bit is the value of the prop. 'Alice holds 2.'
— Alice says, "If I hold 2, then my best card is 0,
and if I do not hold 2, then my best card is 1 or worse."
— Bob learns that 0 is the best card between them (and says so).

If Bob had asked: "Do you hold one of $\{3, 7\}$?", Alice would have said "No." Bob now discards these cards and asks for another pair for bad cards: "Do you hold one of $\{2, 4\}$?"

We can get stuck with deal $(012, 345, 6)$ and Alice asking!

Public Code Protocol

Our Public Code Protocol, employing results for bit exchange protocols by Fischer and Wright (SODA 1993), implements these ideas for m agents and one eavesdropper. A result ($m = 2$) is that:

Corollary *Let ℓ be $\lceil \log_2(e+1) \rceil$ and suppose that (a, b, e) are such that $a, b \geq e + \ell + 1$ and at least one of the inequalities is strict. Then the Public Code Protocol gives a best-card solution.*

The lower bound satisfying this, is $(3, 4, 1)$ just illustrated.

For more than two communicating agents, the numbers of cards needed to establish shared bits are very large (thousands of cards). This is because the bits are shared between more than two agents. An alternative is:

Our Private Code Protocol, establishing chains of bits shared between two agents. This protocol gives a best card solution for $(9, 9, 9, 1)$, for $(11, 11, 11, 2)$, etc.

Best Card Protocols

We build upon a small tradition in cards cryptography involving many other works. We presented results from the first (under submission; available on request):

- HvD, D. Fernández Duque, V. Sundararajan, S.P. Suresh. Who holds the best card? Secure communication of optimal secret bits.
- M. Albert, *et al*. Safe communication for card players by combinatorial designs for two-step protocols. AJC 33:33–46, 2005.
- D. Fernández Duque, V. Goranko. Secure aggregation of distributed information. Discrete Applied Mathematics 198:118–135, 2016.
- A. Koch. The landscape of optimal card-based protocols. Cryptology ePrint Archive, Report 2018/951, 2018.
- T. Mizuki, H. Shizuya, T. Nishizeki. A complete characterization of a family of key exchange protocols. IJIS 1:131–142, 2002.

A workshop cards cryptography may be organized by David Fernandez, HvD, and others. Let me know if you are interested.

THANK YOU!