New results and generalizations of the "Russian cards problem"

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

WilsonFest
California Institute of Technology
Tuesday, March 27, 2012

This is joint work with Colleen Swanson.

The "Russian cards problem"

- Suppose X is a deck of n cards, and we have three participants, *Alice*, *Bob* and *Cathy*.
- *Alice* is dealt a hand H_A of a cards, *Bob* is dealt a hand H_B of b cards and *Cathy* is dealt a hand H_C of c cards, where $a + b + c = n$.
- This is an (a, b, c)-deal of the cards.
- For $t > 0$, let $\binom{X}{t}$ denote the set of $\binom{n}{t}$ t-subsets of X.
- An announcement by *Alice* is a subset of $\mathcal{A} \subseteq \binom{X}{a}$.
- It is required that when *Alice* makes an announcement $\mathcal{A}$, the hand she holds is one of the a-subsets in $\mathcal{A}$.
- The goal of the scheme is that, after a deal has taken place and *Alice* has made an announcement, *Bob* should be able to determine *Alice's* hand, but *Cathy* should not be able to determine if *Alice* holds any particular card not held by *Cathy*.

Our approach

- This problem was introduced in the case $(a, b, c) = (3, 3, 1)$ in the 2000 Moscow Mathematics Olympiad.
- Since then, there have been numerous papers investigating the problem and generalizations of it.
- Several papers examine the problem from the point of view of epistemic logic, and some recent papers have considered combinatorial aspects of the problem.
- We take a combinatorial point of view motivated by cryptographic considerations.
- We provide definitions based on security conditions in the unconditionally secure framework, phrased in terms of probability distributions regarding information available to the various players.
- We give necessary conditions and provide constructions for schemes that satisfy the relevant definitions.
- Here there is a natural interplay with combinatorics.

Our mathematical model

- *Alice* will choose a set of announcements, say $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$ such that every $H_A \in \binom{X}{a}$ is in at least one of the m announcements.
- This set of announcements is fixed ahead of time and it is public knowledge.
- For $H_A \in \binom{X}{a}$, define $g(H_A) = \{i : H_A \in \mathcal{A}_i\}$. *Alice's* announcement strategy, or more simply, strategy, consists of a probability distribution p_{H_A} on $g(H_A)$, for every $H_A \in \binom{X}{a}$.
- We will assume without loss of generality that $p_{H_A}(i) > 0$ for all $i \in g(H_A)$.
- These probability distributions are also fixed ahead of time and public knowledge.
- We will also use the phrase (a, b, c)-strategy to denote a strategy for an (a, b, c)-deal.

Mathematical model (cont.)

- When *Alice* is dealt a hand $H_A \in \binom{X}{a}$, she randomly chooses $i \in g(H_A)$ according to the probability distribution p_{H_A}.
- *Alice* broadcasts i to specify her announcement $\mathcal{A}_i$.
- We define the communication complexity of the protocol to be $\log_2 m$ bits.
- In order to minimize the communication complexity of the scheme, our goal will be to minimize m.
- If $|g(H_A)| = 1$ for every H_A, then we have a deterministic scheme, because the hand H_A held by *Alice* uniquely determines the index i that she will broadcast.
- More generally, suppose there exists a constant γ such that $|g(H_A)| = \gamma$ for every H_A. Further, suppose that every probability distribution p_{H_A} is uniform, i.e., $p_{H_A}(i) = 1/\gamma$ for every H_A and for every $i \in g(H_A)$. We refer to such a strategy as a γ-equitable strategy.
- A deterministic scheme is just a 1-equitable strategy.

A deterministic $(3,3,1)$-strategy

We present a partition of $\binom{X}{3}$ into six subcollections of 3-subsets that is due to Charlie Colbourn and Alex Rosa. This yields a deterministic $(3,3,1)$-strategy having $m = 6$ possible announcements.

i	$\mathcal{A}_i$
1	$\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{0,4,5\},\{1,5,6\},\{0,2,6\}$
2	$\{0,2,3\},\{1,3,4\},\{2,4,5\},\{3,5,6\},\{0,4,6\},\{0,1,5\},\{1,2,6\}$
3	$\{0,2,4\},\{0,3,5\},\{1,2,3\},\{0,1,6\},\{1,4,5\},\{2,5,6\}$
4	$\{0,1,2\},\{2,3,4\},\{4,5,6\},\{1,3,5\},\{0,3,6\}$
5	$\{1,2,5\},\{0,5,6\},\{1,4,6\},\{0,3,4\},\{2,3,6\}$
6	$\{3,4,5\},\{0,1,4\},\{0,2,5\},\{2,4,6\},\{1,3,6\}$

A 2-equitable $(3, 3, 1)$-strategy

We present a set of ten announcements found by Don Kreher that yields a 2-equitable $(3, 3, 1)$-strategy having $m = 10$ possible announcements.

i	$\mathcal{A}_i$
1	$\{2,5,6\},\{2,3,4\},\{1,4,5\},\{1,3,6\},\{0,4,6\},\{0,3,5\},\{0,1,2\}$
2	$\{2,5,6\},\{2,3,4\},\{1,4,6\},\{1,3,5\},\{0,4,5\},\{0,3,6\},\{0,1,2\}$
3	$\{3,4,5\},\{2,4,6\},\{1,3,6\},\{1,2,5\},\{0,5,6\},\{0,2,3\},\{0,1,4\}$
4	$\{3,4,5\},\{2,4,6\},\{1,5,6\},\{1,2,3\},\{0,3,6\},\{0,2,5\},\{0,1,4\}$
5	$\{3,4,6\},\{2,3,5\},\{1,4,5\},\{1,2,6\},\{0,5,6\},\{0,2,4\},\{0,1,3\}$
6	$\{3,4,6\},\{2,3,5\},\{1,5,6\},\{1,2,4\},\{0,4,5\},\{0,2,6\},\{0,1,3\}$
7	$\{3,5,6\},\{2,4,5\},\{1,3,4\},\{1,2,6\},\{0,4,6\},\{0,2,3\},\{0,1,5\}$
8	$\{3,5,6\},\{2,4,5\},\{1,4,6\},\{1,2,3\},\{0,3,4\},\{0,2,6\},\{0,1,5\}$
9	$\{4,5,6\},\{2,3,6\},\{1,3,4\},\{1,2,5\},\{0,3,5\},\{0,2,4\},\{0,1,6\}$
10	$\{4,5,6\},\{2,3,6\},\{1,3,5\},\{1,2,4\},\{0,3,4\},\{0,2,5\},\{0,1,6\}$

Information for Bob

- Suppose that $H_B \in \binom{X}{b}$ and $i \in \{1, \dots, m\}$. Define
$$\mathcal{P}(H_B, i) = \{H_A \in \mathcal{A}_i : H_A \cap H_B = \emptyset\}.$$
$\mathcal{P}(H_B, i)$ denotes the set of possible hands that *Alice* might hold, given *Bob's* hand H_B and *Alice's* announcement $\mathcal{A}_i$.
- *Alice's* strategy is informative for *Bob* provided that
$$|\mathcal{P}(H_B, i)| \leq 1$$
for all $H_B \in \binom{X}{b}$ and for all i.
- If *Bob* holds the cards in H_B and *Alice* broadcasts i, then *Bob* can determine the set of a cards that *Alice* holds.

Example

In the Colbourn-Rosa example, suppose that $H_B = \{1, 3, 4\}$ and *Alice* announces $i = 3$.

i	$\mathcal{A}_i$
1	$\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{0,4,5\},\{1,5,6\},\{0,2,6\}$
2	$\{0,2,3\},\{1,3,4\},\{2,4,5\},\{3,5,6\},\{0,4,6\},\{0,1,5\},\{1,2,6\}$
3	$\{0,2,4\},\{0,3,5\},\{1,2,3\},\{0,1,6\},\{1,4,5\},\{2,5,6\}$
4	$\{0,1,2\},\{2,3,4\},\{4,5,6\},\{1,3,5\},\{0,3,6\}$
5	$\{1,2,5\},\{0,5,6\},\{1,4,6\},\{0,3,4\},\{2,3,6\}$
6	$\{3,4,5\},\{0,1,4\},\{0,2,5\},\{2,4,6\},\{1,3,6\}$

Bob can deduce that $H_B = \{2, 5, 6\}$.

A theorem

Theorem (Albert *et al.* 2005)

The announcement $\mathcal{A}_i$ is informative for Bob if and only if there do not exist two distinct sets $H_A, H'_A \in \mathcal{A}_i$ such that $|H_A \cap H'_A| \geq a - c$.

Proof.

Suppose there exist two distinct sets $H_A, H'_A \in \mathcal{A}_i$ such that $|H_A \cap H'_A| \geq a - c$. Then

$$|H_A \cup H'_A| \leq 2a - (a - c) = a + c = n - b.$$

Hence, there exists $H_B \in \binom{X}{b}$ such that $H_B \cap (H_A \cup H'_A) = \emptyset$. Then $\{H_A, H'_A\} \subseteq \mathcal{P}(H_B, i)$, and therefore the announcement is not informative for *Bob*.

Conversely, suppose $\{H_A, H'_A\} \subseteq \mathcal{P}(H_B, i)$, where $H_A \neq H'_A$. Then $|H_A \cup H'_A| \leq n - b = a + c$, and hence $|H_A \cap H'_A| \geq a - c$. □

Some bounds

The Colbourn-Rosa example and the Kreher example are both informative for *Bob* because no announcement contains two three-subsets that have more than one point in common (i.e., each announcement is a packing of pairs).

The following is an immediate corollary of the previous theorem.

Corollary

Suppose there exists a strategy for Alice with $m < \binom{n}{a}$ that is informative for Bob. Then $a > c$.

Proof.

Since $m < \binom{n}{a}$, there is an announcement $\mathcal{A}_i$ with $|\mathcal{A}_i| \geq 2$. Apply the previous theorem. □

Some bounds (cont.)

When $a > c$, we can derive a simple lower bound on the number of possible announcements, m.

Theorem

Suppose $a > c$ and there exists a strategy for Alice that is informative for Bob. Then $m \geq \binom{n-a+c}{c}$.

Proof.

Let $X' \subseteq X$ where $|X'| = a - c$. There are precisely $\binom{n-a+c}{c}$ a-subsets of X that contain X'. These a-subsets must occur in different announcements. Therefore, $m \geq \binom{n-a+c}{c}$. □

An (a, b, c)-strategy for *Alice* that is informative for *Bob* is said to be optimal if $m = \binom{n-a+c}{c}$.

Designs and large sets

Definition

An $S_\lambda(t,k,v)$ is a pair $(X,\mathcal{B})$, where X is a set of v points and $\mathcal{B}$ is a collection of k-subsets of X (called blocks) such that every subset of t points occurs in exactly λ blocks. If $\lambda = 1$, we use the notation $S(t,k,v)$.

Definition

A large set of $S(t,k,v)$ is a set of $S(t,k,v)$'s, say $(X,\mathcal{B}_1),\ldots,(X,\mathcal{B}_N)$, (on the same point set, X), in which every k-subset of X occurs as a block in precisely one of the $\mathcal{B}_i$'s. Equivalently, the $\mathcal{B}_i$'s form a partition of $\binom{X}{k}$.

It is easy to prove that there must be exactly $N = \binom{v-t}{k-t}$ designs in the large set.

Large sets and informative strategies

Theorem

For $a > c$, an optimal (a, b, c)-strategy for Alice that is informative for Bob is equivalent to a large set of $S(a - c, a, n)$.

The non-existence of a large set of $S(2, 3, 7)$, along with the Colbourn-Rosa example, establishes the following:

Theorem

The minimum m such that there exists a $(3, 3, 1)$-strategy for Alice that is informative for Bob is $m = 6$.

Theorem

For $n \equiv 1, 3 \mod 6$, $n > 7$, there is a large set of $S(2, 3, n)$, and hence the minimum m such that there exists a $(3, n - 4, 1)$-strategy for Alice that is informative for Bob is $m = n - 2$.

Security against Cathy

1. *Alice's* strategy is weakly 1-secure against *Cathy* provided that, for any announcement i, for any $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, and for any $x \in X \backslash H_C$, it holds that

$$0 < \mathsf{Pr}[x \in H_A | i, H_C] < 1.$$

   Weak security means that, from *Cathy's* point of view, any individual card in $X \backslash H_C$ could be held by either *Alice* or *Bob*.

2. *Alice's* strategy is perfectly 1-secure against *Cathy* provided that for any announcement i, for any $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, and for any $x \in X \backslash H_C$, it holds that

$$\mathsf{Pr}[x \in H_A | i, H_C] = \frac{a}{a+b}.$$

   Strong security means that, from *Cathy's* point of view, the probability that any individual card in $X \backslash H_C$ is held by *Alice* is a constant. This probability must equal $a/(a+b)$ because *Alice* holds a of the $a+b$ cards not held by *Cathy*.

Security for equitable strategies

- The conditions for weak and perfect 1-security depend on the probability distributions p_{H_A} and the possible announcements.
- There are simpler, but equivalent, conditions of a combinatorial nature when *Alice's* strategy is equitable.
- First we state a useful lemma which establishes that, from *Cathy's* point of view, any hand $H_A \in \mathcal{P}(H_C, i)$ is equally likely if *Alice's* strategy is equitable.

Lemma

Suppose that Alice's strategy is γ-equitable, Alice's announcement is i, $H_C \in \binom{X}{c}$ and $H_A \in \mathcal{P}(H_C, i)$. Then

$$\mathsf{Pr}[H_A | H_C, i] = \frac{1}{|\mathcal{P}(H_C, i)|}.$$

Security for equitable strategies (cont.)

Theorem

Suppose that Alice's strategy is γ-equitable. Then the following hold:

1. *Alice's strategy is weakly 1-secure against Cathy if and only if, for any announcement i, for any $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, and for any $x \in X \backslash H_C$, it holds that*

$$1 \leq |\{H_A \in \mathcal{P}(H_C, i) : x \in H_A\}| \leq |\mathcal{P}(H_C, i))| - 1.$$

2. *Alice's strategy is perfectly 1-secure against Cathy if and only if, for any announcement i and for any $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, it holds that*

$$|\{H_A \in \mathcal{P}(H_C, i) : x \in H_A\} = \frac{a\,|\mathcal{P}(H_C, i)|}{a + b}$$

for any $x \in X \backslash H_C$.

Example

In the Colbourn-Rosa example, suppose that $H_C = \{0\}$ and *Alice* announces $i = 3$.

i	$\mathcal{A}_i$
1	$\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{0,4,5\},\{1,5,6\},\{0,2,6\}$
2	$\{0,2,3\},\{1,3,4\},\{2,4,5\},\{3,5,6\},\{0,4,6\},\{0,1,5\},\{1,2,6\}$
3	$\{0,2,4\},\{0,3,5\},\{1,2,3\},\{0,1,6\},\{1,4,5\},\{2,5,6\}$
4	$\{0,1,2\},\{2,3,4\},\{4,5,6\},\{1,3,5\},\{0,3,6\}$
5	$\{1,2,5\},\{0,5,6\},\{1,4,6\},\{0,3,4\},\{2,3,6\}$
6	$\{3,4,5\},\{0,1,4\},\{0,2,5\},\{2,4,6\},\{1,3,6\}$

- Then $\mathcal{P}(H_C, 3) = \{\{1,2,3\},\{1,4,5\},\{2,5,6\}\}$.
- Within these three blocks, 1, 2 and 5 each occur twice and 3, 4 and 6 each occur once.
- This particular scenario achieves the condition required for weak 1-security, but not perfect 1-security.

A sufficient condition

Theorem

Suppose that each announcement in an equitable $(a, b, 1)$-strategy is an $S_\lambda(2, a, n)$. Then the strategy is perfectly 1-secure against Cathy.

Proof.

Given an announcement $\mathcal{A}_i = (X, \mathcal{B})$ and a point x, there are

$$|\mathcal{B}| - r = \lambda \left(\frac{n(n-1)}{a(a-1)} - \frac{n-1}{a-1} \right)$$

blocks in $\mathcal{A}_i$ that do not contain x. Each of the points in $X \setminus \{x\}$ is contained in precisely

$$r - \lambda = \lambda \left(\frac{n-1}{a-1} - 1 \right)$$

of these blocks. □

Some existence results when $a = 3$ and $c = 1$

Using a large set of $S(2, 3, n)$, we obtain the following:

Theorem

Suppose $(a, b, c) = (3, n-4, 1)$*, where* $n \equiv 1, 3 \bmod 6$*,* $n > 7$*. Then there exists an optimal strategy for Alice that is informative for Bob and perfectly* 1*-secure against Cathy.*

The Kreher example is the best solution (i.e., having the smallest value of m) we know for the parameter triple $(a, b, c) = (3, 3, 1)$. It provides us with a 2-equitable strategy having $m = 10$ announcements that is informative for *Bob* and perfectly 1-secure against *Cathy*. This is because every announcement in this strategy is an $S(2, 3, 7)$.

A nonexistence result

Theorem (Albert *et al*, 2005)

If $a \leq c + 1$, then there does not exist a strategy for Alice that is simultaneously informative for Bob and weakly 1-secure against Cathy.

Proof.

We only need to consider the case $a = c + 1$. In this case, any two a-subsets in an announcement must be disjoint. For any announcement $\mathcal{A}_i$ and any $x \in X$, the definition of weak 1-security necessitates the existence of a block in $\mathcal{A}_i$ that contains x. It follows that every $\mathcal{A}_i$ forms a partition of X into n/a blocks. Now, suppose that *Alice's* announcement is $\mathcal{A}_i$ and *Cathy's* hand is H_C. There exists at least one $H_A \in \mathcal{A}_i$ such that $H_A \cap H_C \neq \emptyset$. Now, $|H_C| < |H_A|$, so there is a point $x \in H_A \backslash H_C$. The existence of this point violates the requirement of weak 1-security. □

A construction in the case $c = 1$

Theorem

Suppose that $a \geq 3$ and $\mathcal{D} = (X, \mathcal{B})$ is an $S(a-1, a, n)$. Then there exists a γ-equitable $(a, n-a-1, 1)$-strategy with m announcements that is informative for Bob and perfectly 1-secure against Cathy, where $\gamma = n!/|\mathrm{Aut}(\mathcal{D})|$ and $m = \gamma(n-a+1)$.

Proof.

Let the symmetric group S_n act on $\mathcal{D}$. We obtain a set of designs isomorphic to $\mathcal{D}$. Every one of these designs is a 2-design because $a \geq 3$, so the resulting scheme is perfectly 1-secure against *Cathy*. Every design is also an $(a-1)$-design with $\lambda = 1$, so the scheme is informative for *Bob*.

Finally, every block is in $n!/|\mathrm{Aut}(\mathcal{D})|$ of the resulting set of designs and the total number of designs is equal to $\gamma(n-a+1)$. □

Some necessary conditions in the case $a - c = 2$

Theorem

Suppose $(a, b, c) = (3, n-4, 1)$ and suppose that Alice's strategy is equitable, informative for Bob, and perfectly 1-secure against Cathy. Then every announcement is an $S(2, 3, n)$.

Theorem

Suppose $a - c = 2$ and suppose that Alice's strategy is equitable, informative for Bob, and perfectly 1-secure against Cathy. Then $a = 3$ and $c = 1$.

A Scheme for $a = 4$, $b = 7$ and $c = 2$

- Chouinard constructed a large set of 55 designs $S(2,4,13)$.
- The deterministic $(4,7,2)$-strategy is informative for *Bob*.
- Suppose that *Alice's* announcement is $\mathcal{A}_i$ and $H_C = \{y, z\}$.
- There is a unique block in $\mathcal{A}_i$ that contains the pair $\{y, z\}$, say $\{w, x, y, z\}$.
- There are three blocks that contain y but not z, and three blocks that contain z but not y.
- It follows that the set $\mathcal{P}(\{y, z\}, i)$ consists of six blocks.
- Within these six blocks, w and x occur three times, and every point in $X\backslash\{w, x, y, z\}$ occurs twice.
- Therefore, we have

$$\mathsf{Pr}[w \in H_A | H_C] = \mathsf{Pr}[x \in H_A | H_C] = \frac{1}{2}$$

and

$$\mathsf{Pr}[u \in H_A | H_C] = \frac{1}{3}$$

for all $u \in X\backslash\{w, x, y, z\}$.

Example

Suppose that *Alice's* announcement is the following $S(2,4,13)$:

0 1 3 9	1 2 4 10	2 3 5 11	3 4 6 12	4 5 7 0
5 6 8 1	6 7 9 2	7 8 10 3	8 9 11 4	9 10 12 5
10 11 0 6	11 12 1 7	12 0 2 8		

Suppose *Cathy's* hand is $H_C = \{6, 8\}$. Then there remain six possible hands for *Alice*:

0 1 3 9	1 2 4 10	2 3 5 11	3 4 *6* 12	4 5 7 0
5 *6* *8* 1	*6* 7 9 2	7 *8* 10 3	*8* 9 11 4	9 10 12 5
10 11 0 *6*	11 12 1 7	12 0 2 *8*		

In these six possible hands, 1 and 5 occur three times, while 0, 2, 3, 4, 7, 9, 10, 11 and 12 each occur twice.

Schemes with $c > 1$?

Very little is known about schemes with $c > 1$. We conjecture that there are no equitable schemes that are informative for *Bob* and perfectly 1-secure against *Cathy*.

Thank you for your attention!