Des. Codes Cryptogr. (2017) 83:145–168
DOI 10.1007/s10623-016-0210-y

A case study in almost-perfect security for unconditionally secure communication

Esteban Landerreche[1] · **David Fernández-Duque**[2,3]

Received: 18 June 2015 / Revised: 14 December 2015 / Accepted: 7 April 2016 /
Published online: 23 April 2016

Abstract In the Russian cards problem, Alice, Bob and Cath draw a, b and c cards, respectively, from a publicly known deck. Alice and Bob must then communicate their cards to each other without Cath learning who holds a single card. Solutions in the literature provide *weak security,* where Alice and Bob's exchanges do not allow Cath to know with certainty who holds each card that is not hers, or *perfect security,* where Cath learns no probabilistic information about who holds any given card. We propose an intermediate notion, which we call ε-strong security, where the probabilities perceived by Cath may only change by a factor of ε. We then show that strategies based on affine or projective geometries yield ε-strong safety for arbitrarily small ε and appropriately chosen values of a, b, c.

Keywords Information-based cryptography · Secure communication · Secret-exchange protocols

Mathematics Subject Classification 94A60 · 94A62 · 11T71 · 68P25

Communicated by K. Matsuura.

✉ Esteban Landerreche
estebanlan@gmail.com

David Fernández-Duque
david.fernandez@irit.fr

1 Institute for Logic, Language and Computation, University of Amsterdam, Science Park 107, 1098 XG Amsterdam, The Netherlands

2 Centre for Mathematics and Computer Science, University of Toulouse, 118 Route de Narbonne, 31062 Toulouse Cedex 9, France

3 Instituto Tecnológico Autónomo de México, Río Hondo 1 Col. Progreso Tizapán, Mexico, DF, Mexico

1 Introduction

Consider the following scenario:

> *Bob is the commander of a team of $a + b + c$ agents and must coordinate a covert operation. To do this, he must choose $a + c$ of his agents to each carry out an individual mission and then rendezvous with Alice behind enemy lines. For the safety of the operation, none of the agents know who else is involved before meeting Alice, and the only information they can provide her with is their own identity. When they reach the rendezvous point, only a of them show up and the other c are assumed captured by the enemy leader, Cath.*
> *In order to coordinate their rescue, Alice and Bob must let each other know which agents are currently in their camp (and, hence, which are held by Cath). Alice, Bob and Cath all know the full team's roster as well as how many men participated in the operation, but otherwise know only which agents are currently in their own camp.*
> *Moreover, Alice and Bob may only communicate over insecure channels, share no private information, and are not able to encrypt messages in any way that cannot be decyphered by Cath. Nevertheless, it is imperative for security reasons that Cath does not learn the identity of any of the agents in Alice's camp. Is there a way for Alice and Bob to share this information securely?*

This is a retelling of the **Russian cards problem** [21], where the 'team' is a deck of cards and the 'agents' in Alice, Bob and Cath's camps are the set of cards in their hand. In more realistic applications, these soldiers could represent confidential information, such as private keys, which must be retrieved in case some are lost or leaked to an intruder. The use of a random deal of cards is convenient in that it allows Alice and Bob to share information with *unconditional security,* as described below.

1.1 Notions of cryptographic security

Claude Shannon was one of the first to formalize the study of cryptography. He proposed several notions of cryptographic security:

Definition 1 Let $\mathfrak{S}$ be a strategy for sharing information securely. We say that $\mathfrak{S}$ is

1. **computationally secure** for a natural number n if at least n operations are needed for an eavesdropper to obtain a message sent using $\mathfrak{S}$ (i.e., **break** $\mathfrak{S}$);
2. **provably secure** with respect to a problem Π (not necessarily related to cryptography) if Π can be reduced in polynomial time to breaking $\mathfrak{S}$, and
3. **unconditionally secure** if $\mathfrak{S}$ cannot be broken even with unlimited computational resources; the eavesdropper simply does not have enough information to reconstruct the original message.

It is usually very difficult to prove that $\mathfrak{S}$ is computationally secure, as we would need to know all possible strategies for an attack. However, it is a good measure of when a system *isn't* secure, that is, when it fails to be secure for a relatively small n. If $\mathfrak{S}$ is provably secure with respect to Π, we know that we need at least as many operations to break $\mathfrak{S}$ as we need to solve Π. Typically, Π is a 'hard' problem, known to be in NP but believed not to be in P. Many of the cryptographic protocols in use today are based on this notion of security.

On the other hand, it should be clear that unconditional security implies both computational and provable security. As such it would be ideal to develop unconditionally secure

cryptographic protocols. These, however, have some disadvantages; typically, one requires a key that is at least the same size as the message and agreeing on the key is generally as complex as communicating secretly [18], although there are exceptions, e.g. quantum key distribution, which requires special hardware and currently has other practical limitations [16]. Regardless, unconditional security is desirable in some settings where concerns about efficiency are superceded by the need for absolute security. In particular, the Russian cards problem provides a setting for simultaneous, unconditionally secure communication of multiple datapoints.

1.2 Related work

The use of a deck of cards to communicate securely is not new. For example, [10] considers a setting where Alice, Bob and Cath each draw cards from a deck. Alice and Bob wish to share a value which is unknown to Cath; this value is typically one of the cards that is held by either Alice or Bob. Such a protocol may be used for establishing shared secret keys.

The Russian cards problem uses a similar setup, but instead Alice and Bob wish to communicate their *entire* hand to each other without Cath knowing who holds *any* card that is not hers. The problem may be traced back more than 150 years to Kirkman [12], but recently it has received renewed attention after its inclusion in the 2000 Mathematics Olympiad. Rather than produce a new secret, its goal is to distribute information among Alice and Bob in such a way that neither possesses the original data, but the two may reconstruct it by pooling together their individual shares.

Schemes for information-safeguarding protocols have also appeared previously [2,17]. Nevertheless, the Russian cards problem has some unique features. First, the original information may be reconstructed securely even if the agents pool together their information over insecure channels; second, the data may contain multiple bits, each of which is kept secret after the exchange. A possible drawback is that in the Russian cards literature, there are typically only two communicating agents, whereas it may be desirable to distribute the data among a larger number. However, recent work has explored multi-agent generalizations [7–9].

An instance of the Russian cards problem is parametrized by its **distribution type,** which is a triple of natural numbers (a, b, c) indicating how many cards Alice, Bob and Cath hold, respectively. The problem was originally posed for deals of distribution type (3, 3, 1), and one proposed solution uses the Fano plane, a special case of a combinatorial design, which can also be used for many other distribution types [1]. Another solution uses modular arithmetic, which can also be generalized for many distribution types where the eavesdropper holds one card [3]. These solutions use only two announcements, but some distribution types are known to require more. A solution using three announcements for (4, 4, 2) is reported in [22], and a four-step protocol where Cath holds approximately the square of the number of cards of Alice is presented in [4]. The solutions we will work with in this paper are similar to the one reported in [5], which also takes two steps.

However, while the protocols mentioned above provide unconditionally secure solutions to the Russian cards problem in that the eavesdropper may not *know with certainty* who holds a given card, that does not mean that she may not have a high probability of *guessing* this information correctly. To this end, stronger notions of security are studied in [20]. There, a distinction is made between **weak** and **perfect** security; in perfectly secure solutions, Cath does not acquire any probabilistic information about the ownership of any specific card. All of the above solutions provide weak security in this sense, but Swanson and Stinson show how designs may be used to achieve perfect security, an idea further developed in [19].

The solutions we present here will provide an intermediate level of security between weak and perfect, controlling the amount of probabilistic information that may be acquired by the eavesdropper, while having the advantage of being much easier to construct than perfectly secure solutions.

1.3 Basic notions from finite geometry

The main constructions we will use arise from discrete geometry, and we assume that the reader has some familiarity with the subject. Recall that if q is a natural number, there exists a finite field with cardinality q if and only if q is of the form p^n, with p a prime and n a positive integer. This field is unique up to isomorphism and is called the **Galois Field of order** q, often denoted $\mathrm{GF}(q)$, although we will write it more briefly as $\mathbb{F}_q$.

We denote the affine space of dimension δ over $\mathbb{F}_q$ by $\mathrm{AG}(\delta, q)$. We will refer to an affine subspace of dimension α as an **α-plane**, while an α-plane passing through the origin (i.e., a linear subspace of dimension α) will be referred to as an **α-space**. Two α-planes $X, Y \subset \mathrm{AG}(\delta, q)$ are **parallel** if they are distinct and there exists $y \in \mathrm{AG}(\delta, q)$ such that $Y = y + X$.

The projective space of dimension δ over $\mathbb{F}_q$ is denoted $\mathrm{PG}(\delta, q)$, and we will also call α-dimensional subspaces **α-planes**. For a more thorough treatment of finite fields and finite geometry, the reader may consult a text such as [6,13].

1.4 Layout of the article

In Sect. 2 we give an informal discussion of our problem, which we formalize in Sect. 3. Section 4 then reviews some counting results from finite geometries, and in Sect. 5 we define the geometric strategies. Section 6 gives a rough security analysis which is nevertheless sufficient to prove that many ε-strong solutions exist, while Sect. 7 gives a more fine-grained analysis which is useful for finding relatively small triples for which the strategies are ε-strongly safe. In Sect. 8 we discuss schemes for finding balanced triples and provide many examples. Finally, Sect. 9 gives a few concluding remarks.

2 A worked example

Let us illustrate the notion of strong security through a relatively small example. Let's suppose we have 49 cards, with Alice holding 7, Cath holding 5 and Bob the rest. In this case, Alice may identify each point in the two-dimensional vector space over $\mathbb{F}_7$, denoted $\mathrm{AG}(2, 7)$, with a card. Moreover, she can do this in such a way that her cards (marked by ♠) form a line. Suppose then that Cath holds the cards marked by ♣, while Bob holds the rest of the cards (♢) (Fig. 1).

Alice then announces how she has distributed the cards on the plane. In this particular announcement, Cath's cards all fall within the same line. This is an extreme case, but it is a real possibility, as Alice only knows the amount of cards that Cath holds and nothing else when she makes her announcement. Bob and Cath know that Alice's hand falls on a line, but they do not know which line. Bob then knows exactly which cards Alice holds (since there is only one complete line that he does not hold), but Cath does not. However, she may consider it more likely that Alice holds one card over another. To illustrate this, let us consider the points labeled x and y in Fig. 2.

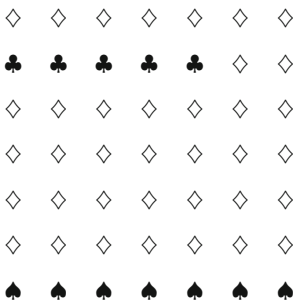

Fig. 1 Alice (♠) assigns each card to a point on the plane in such a way that her hand forms a line. She does not know how the other cards will fall, since she can only see her own hand. In this example, all of Cath's cards (♣) happen to fall on another line

First we will take a look at x. Cath knows that, in order for Alice to hold x, one of the lines that passes through x must be Alice's hand. We draw these lines on the plane.

Cath knows that not all the lines that pass through x can be Alice's hand, because if a line contains a card that belongs to Cath, it clearly cannot be held in its entirety by Alice . In this case, only one line fits that description, so Cath takes it out of consideration. We denote this by drawing the line dotted. Every point in the plane has 8 lines that cross it; therefore, the point x still belongs to 7 hands that could possibly belong to Alice.

However, this is not the case for all cards that Cath does not hold. Let us now turn our attention to y. While x was colinear with Cath's hand, all the lines that contain y and one of Cath's cards are different. In this case Cath can discard more lines than she could when considering x. Only 3 possible lines remain, compared to the 7 lines that pass through x and avoid Cath's hand. Therefore, it seems to Cath that the point x would be more likely to belong to Alice's hand than the point y as there are more possible hands that contain it. Before the announcement, both cards had the same probability to be in Alice's hand but after the announcement, x seems far more likely.

Note that the total number of lines in the announcement is 56. We also know that 36 of these lines contain a card that Cath holds. This is because there are 8 lines touching each point, but the 5 points all share 1 line. Therefore Alice's hand is one of the 20 lines that avoid Cath's hand. Of those 20 only 3 contain y compared to the 7 that contain x. Thus, it seems to Cath that there is a $7/20 = 0.35$ probability that Alice holds x compared to $3/20 = 0.15$ that she holds y. Thus, according to the information that Cath has, it is more than twice as likely that Alice holds x as it is that she holds y.

In this case, we know neither of the cards actually belongs to Alice, but we want to be able to quantify this information and control it, especially in higher dimensions where it is not as simple to visualize. Our goal is to show that, by choosing different parameters appropriately, we can make the probabilities of any two points be arbitrarily close to each other. But first we need some preliminaries to make this precise.

3 Strategies and probabilistic security

In this section we will set up the basic concepts needed to formalize the Russian cards problem and different notions of security that one may require from its possible solutions. We will assume that Alice holds a cards, Bob b and Cath c, and Ω is the set of cards with $|\Omega| = a + b + c$. A **deal (of size** (a, b, c)) is a partition (A, B, C) of Ω such that $|A| = a$, $|B| = b$ and $|C| = c$; each of A, B, C represent the hand of Alice, Bob and Cath, respectively.

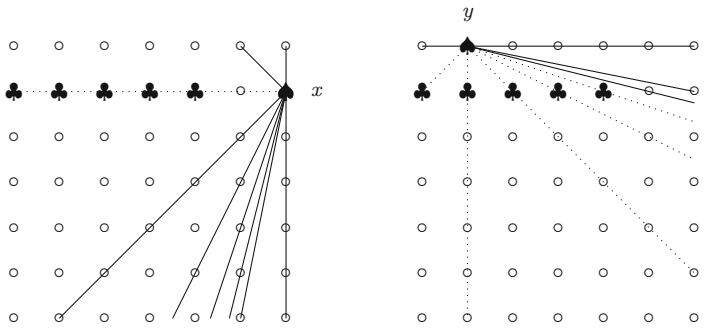

Fig. 2 Lines that Cath may discard from Alice's announcement. It is important to note that most of the lines are truncated, as the natural representation of AG(2, 7) is as a torus and lines are harder to visualize in two dimensions

3.1 Equitable strategies

In most solutions to the Russian cards problem, Alice makes an announcement, after which Bob knows the entire deal and thus can make a second (trivial) announcement where he tells Alice which cards Cath holds. Thus we need only model Alice's first announcement, and we follow [20] in referring to the way that Alice is to choose her announcement as a **strategy.**

Suppose that Alice holds a cards, Bob holds b and Cath holds c. Given a set X and a natural number n, we denote by $\binom{X}{n}$ the set of n-element subsets of X, and we will refer to such sets as n**-sets.** We denote the cardinality of X by $|X|$. A possible hand for Alice is then an element of $\binom{\Omega}{a}$. In Alice's first announcement she gives a set of possible hands that she may hold, and thus we may consider an announcement simply as a set $\mathcal{A} \subset \binom{\Omega}{a}$.

However, there are many possible announcements that may inform Bob of Alice's hand, and Alice must have a non deterministic way to choose one out of all the possible announcements. Thus a strategy for Alice consists on a probability distribution among the possible announcements that she may choose from.

Definition 1 A **strategy** (on $\binom{\Omega}{a}$) is a function $\mathfrak{S}$ that assigns to each hand $A \in \binom{\Omega}{a}$ a probability distribution over $2^{\binom{\Omega}{a}}$. We denote the probability of an announcement $\mathcal{A}$ given the hand A as $P_{\mathfrak{S}}(\mathcal{A}|A)$.

Given a strategy $\mathfrak{S}$ and a hand A, we will say that $\mathcal{A}$ is a **possible announcement** if $P_{\mathfrak{S}}(\mathcal{A}|A) > 0$. The set of possible announcements for A will be denoted by $\mathfrak{S}_A$.

When it is clear from context, we will drop the subindex $\mathfrak{S}$ and write simply $P(\mathcal{A}|A)$ to simplify notation. It will also be convenient for computations if the number of possible announcements is independent of Alice's hand. If we could guarantee that there are m possible announcements for each hand, we could always assign a probability of $1/m$ to each individual announcement. If a strategy has this property, we will say it is equitable [20].

Definition 2 A strategy $\mathfrak{S}$ is **equitable** if there exists a positive integer m such that, for every a-set A, $|\mathfrak{S}_A| = m$ and the probability of choosing a particular announcement $\mathcal{A} \in \mathfrak{S}_A$ is $P(\mathcal{A}|A) = 1/m$.

One advantage of equitable strategies is that we need less information to specify them than more general strategies. In particular, we may model equitable strategies merely as a function

$$\mathfrak{S}\colon \binom{\Omega}{a} \to 2^{2^{\binom{\Omega}{a}}},$$

where $\mathfrak{S}_A$ is the set of announcements with positive probability (and thus with probability $1/m$). Since the geometric strategy, which will be our main focus, is equitable, we will adopt this presentation.

The first condition that a two-step solution to the Russian cards problem should satisfy is that Bob should be informed of Alice's hand after an announcement. Let us make this precise. First, we introduce an abuse of notation that we will use throughout the text.

If $\mathcal{X} \subset 2^{\Omega}$ and $Y \subset \Omega$, define

$$\mathcal{X}\backslash Y = \{X \in \mathcal{X} : X \cap Y = \varnothing\}.$$

Thus, $\mathcal{X}\backslash Y$ is the set of elements of $\mathcal{X}$ avoiding Y.

Definition 3 Fix integers a, b, c and a deck Ω with $|\Omega| = a + b + c$. A strategy $\mathfrak{S}$ on $\binom{\Omega}{a}$ is **informative for** (a, b, c) if, for every $A \in \binom{\Omega}{a}$, $B \in \binom{\Omega\backslash A}{b}$ and $\mathcal{A} \in \mathfrak{S}_A$, we have that $\mathcal{A}\backslash B = \{A\}$.

Thus after an informative announcement, Bob knows exactly which hand A Alice is holding. But an informative strategy may also give Cath information, and we also require for Alice's strategy to be secure.

3.2 Probabilistic security

Before Alice makes an announcement, Cath knows that Alice can possibly hold any hand that doesn't contain one of Cath's cards. Hence, there are $\binom{a+b}{a}$ possible hands for Alice. However, after an announcement, Cath can discard any hand that isn't found in the announcement. After doing so, it is possible that Cath acquires new information about the cards she does not hold. In particular, she may know that there is a high probability that Alice holds a given card. If Alice and Bob want to communicate securely, it would be desirable to avoid giving Cath such information.

There are three different notions of probabilistic security for strategies: weak, perfect, and our notion of ε-strong security, which lies between the other two. Unconditional security guarantees weak security but nothing more. If we wanted to avoid Cath learning any probabilistic information after an announcement, we would need to ensure that no card seems more likely after the announcement than it did before. For this, the number of hands in the announcement (after Cath eliminates the ones which have a card that she holds) that contain a given card must be equal for every card that Cath does not hold. In this case, the probability of Alice having a set card should stay the same after Alice's announcement. As a matter of fact, we know the value of this probability; we must only count the hands that could contain that card given Cath's hand and divide it by the number of remaining hands in the announcement:

$$P(x \in A|C) = \frac{\binom{a+b-1}{a-1}}{\binom{a+b}{a}} = \frac{a}{a+b}.$$

If this number stays constant after Alice's announcement, we will say that Alice's strategy is perfectly secure.

Definition 4 A strategy $\mathfrak{S}$ on $\binom{\Omega}{a}$ is **perfectly secure for** (a, b, c) if for every $C \in \binom{\Omega}{c}$, every card $x \in \Omega\backslash C$, and every announcement $\mathcal{A}$ with $P(\mathcal{A}|C) \neq 0$, we have that

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} = 1.$$

This notion is equivalent to 1-perfect security in [20] and represents Cath's inability to glean information about the position of individual cards. Compare this to *weak security,* where we only require that Cath is not certain about the position of any card she does not hold.

Definition 5 A strategy $\mathfrak{S}$ on $\binom{\Omega}{a}$ is **weakly secure for** (a, b, c) if for every $C \in \binom{\Omega}{c}$, every card $x \in \Omega \backslash C$, and every announcement $\mathcal{A}$ with $P(\mathcal{A}|C) \neq 0$, we have that

$$0 < P(x \in A|C, \mathcal{A}) < 1.$$

In [19], Swanson and Stinson proved that that for a strategy to be perfectly secure, Alice's announcement must be a t-design for some $t > c$. They use this to present examples of perfectly secure strategies when Cath has at most three cards. In principle this can be extended to larger values of c, since it is known that t-designs exist for arbitrarily large t [11]; however, they can be difficult to construct. Instead, we will define an intermediate level of security, where the constraint is relaxed so we can have more flexibility and can work more easily with cases where Cath's hand is larger. In fact, this notion will permit us to easily find secure protocols for any possible hand size that Cath may hold.

Definition 6 Let $\varepsilon > 0$. A strategy $\mathfrak{S}$ on $\binom{\Omega}{a}$ is **ε-strongly secure for** (a, b, c) if for every $C \in \binom{\Omega}{c}$, every card $x \in \Omega \backslash C$, and every announcement $\mathcal{A}$ with $P(\mathcal{A}|C) \neq 0$, we have that

$$\left| \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} - 1 \right| < \varepsilon.$$

As mentioned above, equitable strategies are useful for simplifying computations. In particular, the above probabilities may be computed by counting. The following result can be found in [20].

Lemma 7 *Let $\mathfrak{S}$ be an equitable strategy on $\binom{\Omega}{a}$ and (A, B, C) be a deal. Suppose that $C \in \binom{\Omega}{c}$ and $\mathcal{A}$ is an announcement with $P(\mathcal{A}|C) > 0$ and $A \in \mathcal{A}$. Then, $P(A|C, \mathcal{A}) = \frac{1}{|\mathcal{A} \backslash C|}$.*

In other words, the probability that A is Alice's hand given Cath's hand C and the announcement $\mathcal{A}$ (when A is a valid hand given C) is given by the quotient of one over the number of hands in the announcement that avoid C.

Thus the probability of Alice having a set hand A according to Cath is $1/|\mathcal{A} \backslash C|$. However, what we want to calculate is the probability that Alice holds a given card x. For this, we introduce a new abuse of notation: for $\mathcal{X} \subset 2^{\Omega}$ and $y \in \Omega$, set

$$\mathcal{X}_y = \{X \in \mathcal{X} : y \in X\}.$$

Thus for $Z \subset \Omega$, $\mathcal{X}_y \backslash Z$ denotes the set of elements of $\mathcal{X}$ which contain y but avoid Z. The following can also be found in [20].

Lemma 8 *Let $\mathfrak{S}$ be an equitable strategy on $\binom{\Omega}{a}$ and (A, B, C) be a deal. If $z \in \Omega \backslash C$, then*

$$P(z \in A|C, \mathcal{A}) = \frac{|\mathcal{A}_z \backslash C|}{|\mathcal{A} \backslash C|}.$$

Our goal is to show that affine and projective spaces can be used to construct ε-strongly safe strategies for any positive ε. Before we can do this, however, we must review some results from discrete geometry.

4 Combinatorics of finite geometry

In this section we review some results in finite geometry that will be useful to construct and analyze the geometric strategies. In particular, we will focus on bounding the number of subspaces that fulfil certain properties, which will allow us to bound the number of possible hands in an announcement and estimate the probabilities mentioned in the last section. The results in this section are presented without proof.

4.1 Construction of affine and projective spaces

Recall that the δ-dimensional projective space $\mathrm{AG}(\delta, q)$ arises from $(\mathbb{F}_q)^\delta$ with the standard vector space structure. With this, the δ-dimensional projective space $\mathrm{PG}(\delta, q)$ can be constructed as a quotient of $\mathrm{AG}(\delta+1, q)\backslash\{0\}$ under the equivalence relation $\sim$ given by $x \sim y$ if and only if $x = \lambda y$ for some $\lambda \in \mathbb{F}_q$. We denote the equivalence class of y by $[y]$.

However, we may also choose to 'center' our projective space around any other point of $\mathrm{AG}(\delta+1, q)$. Given $x \in \mathrm{AG}(\delta+1, q)$, we define a map $\pi_x : \mathrm{AG}(\delta+1, q) \to \mathrm{PG}(\delta, q)$ by $\pi_x(y) = [y - x]$. Then, $V \subset \mathrm{PG}(\delta, q)$ is an α-plane if and only if there is an $(\alpha+1)$-plane $W \subset \mathrm{AG}(\delta+1, q)$ meeting x such that $V = \pi_x(W)$, in which case we also write $W = \iota_x(V)$.

We have a similar projection from $\mathrm{PG}(\delta+1, q)$ into $\mathrm{PG}(\delta, q)$. Let $x \in \mathrm{PG}(\delta+1, q)$ and H be any hyperplane not meeting x. Then, for $y \in \mathrm{PG}(\delta+1, q)\backslash\{x\}$ we define $\pi_x^H(y)$ to be the unique $z \in H$ such that x, y, z are collinear. Once again, $V \subset \mathrm{PG}(\delta, q)$ is an α-plane if and only if there is an $(\alpha+1)$-plane $W \subset \mathrm{PG}(\delta+1, q)$ meeting x such that $V = \pi_x^H(W)$, in which case we also write $W = \iota_x^H(V)$.

These projections commute with intersections with subspaces through x:

Lemma 9 *Let q be a prime power and $0 < \alpha \leq \delta$.*

1. *If $W \subset \mathrm{AG}(\delta+1, q)$ is any α-plane touching x and $C \subset \mathrm{AG}(\delta+1, q)\backslash\{x\}$, then $\pi_x(W \cap C) = \pi_x(W) \cap \pi_x(C)$.*
2. *Similarly, if $W \subset \mathrm{PG}(\delta+1, q)$ is any α-plane touching x, H is a hyperplane avoiding x and $C \subset \mathrm{AG}(\delta+1, q)\backslash\{x\}$, then $\pi_x^H(W \cap C) = \pi_x^H(W) \cap \pi_x(C)$.*

This will be useful later for transferring counting results from one space to another. Now let us show how to compute some of the basic quantities we will be interested in.

4.2 Counting results in finite geometry

Recall that the Gaussian binomial coefficients $\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q$ may be defined recursively by $\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q = 0$ if $\delta < \alpha$, $\begin{bmatrix}\delta\\ 0\end{bmatrix}_q = 1$ and $\begin{bmatrix}\delta+1\\ \alpha+1\end{bmatrix}_q = \left(\frac{q^{\delta+1}-1}{q^{\alpha+1}-1}\right)\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q$. These coefficients are the building block of many of the counting results we need. It is useful to compute their leading terms:

Lemma 10 *Given positive integers α and δ,*

$$\left(\begin{bmatrix}\delta+1\\ 1\end{bmatrix}_q\right)^\alpha = q^{\alpha\delta} + \alpha q^{\alpha\delta-1} + o(q^{\alpha\delta-1}).$$

As an easy consequence it follows that if $\alpha < \delta$, then $\left(\begin{bmatrix}\delta+1\\ 1\end{bmatrix}_q\right)^\alpha < \left(\begin{bmatrix}\alpha+1\\ 1\end{bmatrix}_q\right)^\delta$ for large q. The following is well-known:

Lemma 11 *If q is a prime power and $0 \leq \alpha \leq \delta$, any α-plane in $\mathrm{AG}(\delta, q)$ has q^α points and any α-plane in $\mathrm{PG}(\delta, q)$ has $\begin{bmatrix}\alpha+1\\ 1\end{bmatrix}_q$ points.*

Meanwhile, the intersection of two distinct α-planes is either empty or a η-plane for some $\eta < \alpha$, which has the following consequence.

Lemma 12 *Let q be a prime power and $0 < \alpha \leq \delta$.*

1. *If $U, W \subset \mathrm{AG}(\delta, q)$ are distinct α-planes of $\mathrm{AG}(\delta, q)$, then $|U \cap W| \leq q^{\alpha-1}$ and $|U \cup W| \geq 2q^{\alpha} - q^{\alpha-1}$.*
2. *Similarly, if $U, W \subset \mathrm{PG}(\delta, q)$ are distinct α-planes of $\mathrm{PG}(\delta, q)$, then $|U \cap W| \leq \begin{bmatrix}\alpha\\1\end{bmatrix}_q$ and $|U \cup W| \geq q^{\alpha} + \begin{bmatrix}\alpha+1\\1\end{bmatrix}_q$.*

We may use Gaussian binomial coefficients to count the number of α-planes, either in the whole space or meeting some specified set of points.

Lemma 13 *Let q be a prime power and $0 < \alpha \leq \delta$.*

1. *The number of α-planes in $\mathrm{AG}(\delta, q)$ is $q^{\delta-\alpha}\begin{bmatrix}\delta\\\alpha\end{bmatrix}_q$.*
2. *If $\gamma \geq 1$, given $x_1, \ldots, x_\gamma \in \mathrm{AG}(\delta, q)$ that span a $(\gamma-1)$-plane, the number of α-planes in $\mathrm{AG}(\delta, q)$ meeting all x_i is $\begin{bmatrix}\delta-\gamma+1\\\alpha-\gamma+1\end{bmatrix}_q$.*
3. *If $\gamma \geq 0$, given $x_1, \ldots, x_\gamma \in \mathrm{PG}(\delta, q)$ that span a $(\gamma-1)$-plane, the number of α-planes in $\mathrm{PG}(\delta, q)$ meeting all x_i is $\begin{bmatrix}\delta-\gamma+1\\\alpha-\gamma+1\end{bmatrix}_q$.*

The following bound from [15] will be essential.

Definition 14 We define a function $M : \mathbb{N}^5 \to \mathbb{N}$ given by

$$M(\alpha, \gamma, \delta, q, c) = q^{(\alpha+1)(\gamma+1)}\begin{bmatrix}\delta-\gamma\\\alpha+1\end{bmatrix}_q + \left(\begin{bmatrix}\gamma+1\\1\end{bmatrix}_q - c\right)q^{\alpha\gamma}\begin{bmatrix}\delta-\gamma\\\alpha\end{bmatrix}_q.$$

We call the value $M(\alpha, \gamma, \delta, q, c)$ **Metsch's bound**.

Theorem 15 *If $\delta \geq \alpha + \gamma$ and $C \subset \mathrm{PG}(\delta, q)$ is such that $|C| < \begin{bmatrix}\gamma+1\\1\end{bmatrix}_q$, then the number of α-planes not meeting C is at least $M(\alpha, \gamma, \delta, q, |C|)$.*

Equality holds when there is a $(\gamma+1)$-plane D such that $C \subset D$ and C meets all lines of D, in which case we must have $|C| \geq \begin{bmatrix}\gamma\\1\end{bmatrix}_q$. Moreover, if C is fixed, this bound attains its highest value when taking γ as small as possible so that $|C| < \begin{bmatrix}\gamma+1\\1\end{bmatrix}_q$.

The following is an immediate corollary of Theorem 15, although it was known previously [14]. Recall that an **α-blocking set** is a subset C of $\mathrm{PG}(\delta, q)$ such that every α-plane meets C.

Corollary 16 *Let $0 < \alpha \leq \delta$ and q be a prime power. Given a positive integer $c \leq \begin{bmatrix}\delta+1\\1\end{bmatrix}_1$, there is an α-blocking set of size c in $\mathrm{PG}(\delta, q)$ if and only if $c \geq \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$.*

We can also use Theorem 15 to give a similar bound in $\mathrm{AG}(\delta, q)$.

Corollary 17 *If $\delta \geq \alpha + \gamma$ and $C \subset \mathrm{AG}(\delta, q)$ is such that $|C| < \begin{bmatrix}\gamma+1\\1\end{bmatrix}_q$, then the number of α-planes not meeting C is at least*

$$M(\alpha, \gamma, \delta, q, c) - \begin{bmatrix}\delta\\\alpha+1\end{bmatrix}_q.$$

Proof Consider the embedding $e\colon \mathrm{AG}(\delta, q) \to \mathrm{PG}(\delta, q)$ given by $e(x_1, \ldots, x_\delta) = [(x_1, \ldots, x_\delta, 1)]$. Let $H \subset \mathrm{PG}(\delta, q)$ be the hyperplane defined by $x_{\delta+1} = 0$. Given an α-plane $V \subset \mathrm{AG}(\delta, q)$, define $\tilde{e}(V)$ to be the least subspace W of $\mathrm{PG}(\delta, q)$ such that $e[V] \subset W$. Then, it is readily checked that $\tilde{e}(V)$ is an α-space in $\mathrm{PG}(\delta, q)$, and moreover that $\tilde{e}$ is a bijection between the α-planes in $\mathrm{AG}(\delta, q)$ and the α-planes in $\mathrm{PG}(\delta, q)$ not contained in H.

Then, if $C \subset \mathrm{AG}(\delta, q)$ has c elements, by Theorem 15, there are at least $M(\alpha, \gamma, \delta, q, c)$ α-planes in $\mathrm{PG}(\delta, q)$ not meting C, and each one is of the form $\tilde{e}(V)$ for some α-plane $V \subset \mathrm{AG}(\delta, q)$, *unless* it is contained in H. But there are $\begin{bmatrix} \delta \\ \alpha+1 \end{bmatrix}_q$ α-planes contained in H, so we subtract them to obtain our bound. □

We remark, however, that the bound from Corollary 17 is not necessarily tight.

5 The geometric strategies

We've informally presented the affine solution to the Russian Cards problem, and will now formalize it to construct the geometric strategies. The protocols we will use have essentially appeared in [1,5,19], although we seem to be the first to consider $\alpha < \delta - 1$. The basic idea is to construct a finite geometry where every point represents a different card and Alice's hand forms an α-plane. Below, we use $f[X]$ to denote the set $\{f(x)\colon x \in X\}$. Each announcement is parametrized by a **suitable map.**

Definition 18 Fix a prime power q, natural numbers $0 < \alpha < \delta$ and $A \in \binom{\Omega}{a}$. Let $\mathbb{G}$ be either $\mathrm{AG}(\delta, q)$ or $\mathrm{PG}(\delta, q)$. We define a **suitable map for** A to be a bijection $f\colon \Omega \to \mathbb{G}$ such that $f[A]$ is an α-plane.

Given a suitable map f, we define

$$\mathcal{A}[f] = \{X \subset \Omega : f[X] \text{ is an } \alpha\text{-plane}\}.$$

The geometric strategies are then defined by letting Alice choose uniformly from all suitable maps f and announcing $\mathcal{A}[f]$.

Definition 19 *(The geometric strategies)* Let q be a prime power and $0 < \alpha < \delta$.

We define the *affine strategy (with parameters* q, α, δ*)*, to be the strategy $\mathfrak{S}$ such that $\mathfrak{S}_A$ is the set of all announcements of the form $\mathcal{A}[f]$, where $f\colon \Omega \to \mathrm{AG}(\delta, q)$ is suitable for A, and Alice chooses uniformly from $\mathfrak{S}_A$, in which case we write $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$. A *distribution type for* $\mathrm{AS}(\alpha, \delta, q)$ is a triple (a, b, c), where $a = q^\alpha$ and $a + b + c = q^\delta$.

We similarly define the *projective strategy* to be the strategy $\mathfrak{S}$ such that $\mathfrak{S}_A$ is the set of all announcements of the form $\mathcal{A}[f]$, where $f\colon \Omega \to \mathrm{PG}(\delta, q)$ is suitable for A, and Alice chooses uniformly from $\mathfrak{S}_A$, in which case we write $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$. A *distribution type for* $\mathrm{PS}(\alpha, \delta, q)$ is a triple (a, b, c), where $a = \begin{bmatrix} \alpha+1 \\ 1 \end{bmatrix}_q$ and $a + b + c = \begin{bmatrix} \delta+1 \\ 1 \end{bmatrix}_q$.

Before continuing, let us now show that both strategies are equitable.

Lemma 20 *Let q be a prime power and $0 < \alpha < \delta$. Let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$, with distribution type (a, b, c). Then, if $A, A' \in \binom{\Omega}{a}$, $|\mathfrak{S}_A| = |\mathfrak{S}_{A'}|$.*

Proof Let $A, A' \in \binom{\Omega}{a}$. To show that $|\mathfrak{S}_A| = |\mathfrak{S}_{A'}|$, we will define a bijection $\Sigma\colon \mathfrak{S}_A \to \mathfrak{S}_{A'}$. As a first step, we will build a function σ that permutes the elements of Ω. We know that $|A \backslash A'| = |A' \backslash A|$, so we can find a bijection $s\colon A \backslash A' \to A' \backslash A$.

Using the function s we will define a permutation $\sigma : \Omega \to \Omega$ given by

$$\sigma(x) = \begin{cases} s(x) & \text{if } x \in A \backslash A' \\ s^{-1}(x) & \text{if } x \in A' \backslash A \\ x & \text{otherwise.} \end{cases}$$

Since s is invertible, σ is well-defined, and it is easy to check that σ is bijective. We then define $\Sigma : \mathfrak{S}_A \to \mathfrak{S}_{A'}$ given by $\Sigma(\mathcal{A}) = \{\sigma[H] | H \in \mathcal{A}\}$ for $\mathcal{A} \in \mathfrak{S}_A$. Then, it is easy to see that Σ has an inverse given by $\Sigma^{-1}(\mathcal{A}') = \{\sigma^{-1}[H] : H \in \mathcal{A}'\}$, where $\mathcal{A}' \in \mathfrak{S}_{A'}$, and hence Σ is a bijection, so that $|\mathfrak{S}_A| = |\mathfrak{S}_{A'}|$ as claimed. □

We have now proven that for every hand that Alice can have there is the same number m of possible announcements. This permits us to set the probability of a particular announcement to be chosen to $1/m$, and thus the geometric strategies are equitable. As mentioned above, this will simplify some computations, even without explicitly knowing the value of m.

In the remainder of this section we will prove that the geometric strategies give informative and weakly safe solutions to the Russian cards problem, provided c satisfies certain bounds.

Lemma 21 *Let q be a prime power and $1 \leq \alpha < \delta$. Let $\mathfrak{S}$ be either* $\mathrm{AS}(\alpha, \delta, q)$ *or* $\mathrm{PS}(\alpha, \delta, q)$*, with distribution type (a, b, c). Then, $\mathfrak{S}$ is informative for (a, b, c) if and only if*

1. $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$ *and* $c < q^\alpha - q^{\alpha-1}$*, or*
2. $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ *and* $c < q^\alpha$.

Proof First assume $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$. Let $A \in \binom{\Omega}{a}$ and $B \in \binom{\Omega \backslash A}{b}$. Let $f : \Omega \to \mathrm{AG}(\delta, q)$ be suitable for A and $\mathcal{A} = \mathcal{A}[f]$. Clearly $A \in \mathcal{A}$, so it remains to check that if $A' \in \binom{\Omega \backslash B}{a}$ is such that $\mathcal{A} \in \mathfrak{S}_{A'}$, then $A = A'$.

If this were not the case, then $U = f[A]$ would be an α-space different from $U' = f[A']$. Since both U and U' are disjoint from $f[B]$, then so is $U \cup U'$. By Lemma 12, $|U \cup U'| \geq 2q^\alpha - q^{\alpha-1}$. But f is a bijection, so it follows that $a + c = |A| + |C| \geq 2q^\alpha - q^{\alpha-1}$, and thus $c \geq q^\alpha - q^{\alpha-1}$, contradicting our hypothesis.

We conclude that $U = U'$, so that also $A = A'$ and thus the affine strategy is informative in this case. For the other implication, assume that $c \geq q^\alpha - q^{\alpha-1}$. Choose two α-planes V, V' such that $V \cap V'$ is an $(\alpha - 1)$-plane. Then, choose any W not meeting $V \cup V'$ and such that $|W| = c - q^\alpha - q^{\alpha-1}$. Finally, set $A = f^{-1}[V]$ and $C = f^{-1}[(V' \backslash V) \cup W]$. It is clear that $\mathcal{A}[f]$ is not informative for Bob, since he does not know if Alice holds $f^{-1}[V]$ or $f^{-1}[V']$.

The claim for $\mathrm{PS}(\alpha, \delta, q)$ is proven similarly, except that here we would have that $|U \cup U'| \geq q^\alpha + \begin{bmatrix} \alpha+1 \\ 1 \end{bmatrix}_q$, so that $c < \begin{bmatrix} \alpha+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} \alpha \\ 1 \end{bmatrix}_q = q^\alpha$. □

Next we must see that, given a card x not held by Cath, there is a nonzero probability that Alice holds x, which means that it is impossible that there is $x \in \Omega \backslash C$ such that all α-spaces passing through x meet C. In the following proofs, we will use the notation from Sect. 4.1.

Lemma 22 *Let q be a prime power and $1 \leq \alpha < \delta$. Let $\mathfrak{S}$ be either* $\mathrm{AS}(\alpha, \delta, q)$ *or* $\mathrm{PS}(\alpha, \delta, q)$*, with distribution type (a, b, c). Let $\mathcal{A}$ be any announcement of $\mathfrak{S}$. Then, if $c < \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q$ and $x \in \Omega \backslash C$, there is $A \in \mathcal{A}$ such that $x \in A$. Moreover, this bound is optimal.*

Proof First, assume that $c < \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q$ and let $\mathcal{A}[f]$ be any announcement of $\mathrm{AS}(\alpha, \delta, q)$. Let x be any card and $s = f(x)$. Consider the projection $\pi_s(C)$. Since $|\pi_s(C)| \leq c < \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q$,

it is not an $(\alpha-1)$-blocking set, and thus there is an $(\alpha-1)$-plane $W \subset \mathrm{PG}(\delta-1,q)$ not meeting $\pi_s(C)$. But then, $U = \iota_s(W)$ is an α-plane containing s and not meeting C. Setting $A' = f^{-1}[U]$, we have that $A' \in \mathcal{A}[f]$, and $x \in A'$.

Now suppose instead that $c \geq \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$. Choose W avoiding 0 such that $\pi_0(W)$ is an $(\alpha-1)$-blocking set. Then, it is clear that if $C = f^{-1}[W]$, there is no A'' disjoint from C such that $0 \in A'' \in \mathcal{A}[f]$.

For the projective case, first assume that $c+1 < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$ and let $\mathcal{A}[f]$ be any announcement of the protocol. As before, let x be any card and $s = f(x)$. Choose any hyperplane H not meeting x and let π_x^H be the projection onto H through x.

Consider the projection $\pi_x^H(C)$. If $c < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$ then $|\pi_x^H(C)| \leq c < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$, so it is not an $(\alpha-1)$-blocking set in H, and thus there is an $(\alpha-1)$-plane U on H not meeting $\pi_x(C)$. But then, $\iota_x^H(U)$ is an α-plane containing x and not meeting C, so that if $A' = f^{-1}[U]$, once again $A' \in \mathcal{A}[f]$, and $x \in A'$. For the other implication, if $c \geq \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$ we let W be an $(\alpha-1)$-blocking set in H and proceed as in the affine case. □

There should also be a nonzero probability that any card not held by Cath is held by Bob. In other words, if y is not held by Cath, there should be an α-plane avoiding y and Cath's hand.

Lemma 23 *Let q be a prime power and $1 \leq \alpha < \delta$. Let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha,\delta,q)$ or $\mathrm{PS}(\alpha,\delta,q)$, with distribution type (a,b,c), and $\mathcal{A}$ be any announcement of $\mathfrak{S}$. Let $C \in \binom{\Omega}{c}$ and $y \in \Omega\backslash C$. Suppose moreover that either*

1. *$\mathfrak{S} = \mathrm{AS}(\alpha,\delta,q)$ and $c < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$, or*
2. *$\mathfrak{S} = \mathrm{PS}(\alpha,\delta,q)$ and $c+1 < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$.*

Then, there is $A \in \mathcal{A}$ such that $y \notin A$ and $A \cap C = \varnothing$. Moreover, the bound in item 2 is optimal.

Proof First consider the affine case and suppose that $c < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$. Let x be any card and $s = f(x)$. Consider two cases; either $f[C]\cup\{s\}$ is a plane or it is not. If it is, it has dimension at most $\delta-\alpha$. Extend $f[C]\cup\{s\}$ to a plane U of dimension $\max(\delta-\alpha,\alpha) < \delta$. Then, there is a plane V parallel to U. If U has dimension α, so does V, and we are done, since if Alice holds $f^{-1}[V]$, then Bob holds x. If not, $\alpha < \delta-\alpha$, and we can find $V' \subset V$ of dimension α. Once again, if Alice holds $f^{-1}[V']$, then Bob holds x.

If $f[C]\cup\{s\}$ is not a plane, then there are three collinear points u, v, w such that $u, v \in f[C]\cup\{s\}$ but $w \notin f[C]\cup\{s\}$. Consider $\pi_w(f[C]\cup\{s\})$. Then, $|\pi_w(f[C]\cup\{s\})| \leq c < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$ (since $\pi_w(u) = \pi_w(v)$), and as before there is a plane V meeting w but avoiding $f[C]\cup\{w\}$. This gives us a possible deal where Bob holds x, by setting $A' = f^{-1}[V]$.

Now consider the projective case and assume $c+1 < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$. Once again, let x be any card and $s = f(x)$. Observe that $f[C]\cup\{s\}$ has $c+1 < \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$ points and is thus not an α-blocking set of $\mathrm{PG}(\delta,q)$. It follows that there is an α-plane V not meeting $f[C]\cup\{s\}$. If Alice holds $f^{-1}[V]$, then Bob holds s.

To see that this bound is optimal, suppose instead that $c \geq \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$. Choose C of the form $f^{-1}[(W\backslash\{s\})\cup W']$, where W is a $(\delta-\alpha)$-plane and W' is any set of $c - \begin{bmatrix}\delta-\alpha+1\\1\end{bmatrix}_q$ points disjoint from W. Then, every α-plane intersects $f[C]$, so Bob cannot hold x. □

We may summarize Lemmas 22 and 23 in the following:

Lemma 24 *Let q be a prime power and $1 \leq \alpha < \delta$. Let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$, with distribution type (a, b, c). Then, $\mathfrak{S}$ is weakly secure for (a, b, c) if and only if*

1. $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$ *and* $c < \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q$, *or*
2. $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ *and* $c + 1 < \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q$.

Putting together Lemmas 21 and 24 we obtain the main result of this section.

Theorem 25 *Let q be a prime power and $1 \leq \alpha < \delta$. Let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$, with distribution type (a, b, c). Then, $\mathfrak{S}$ is weakly secure and informative for (a, b, c) if and only if*

1. $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$ *and* $c < \min\left(q^\alpha - q^{\alpha-1}, \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q\right)$, *or*
2. $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ *and* $c < \min\left(q^\alpha, \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q - 1\right)$.

We may use Theorem 25 to find many tuples (a, b, c) for which the geometric strategies are weakly secure. If Alice holds a line in the plane, then we may take c to be almost as large as a:

Corollary 26 *There are infinitely many values of a such that for any $c \leq a - 2$ there is $b < a^2$ such that there is an informative and weakly safe strategy for (a, b, c).*

Proof Take $\alpha = 1$, $\delta = 2$ and q an arbitrary prime power and apply Theorem 25 to either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$. □

On the other hand, if c is much smaller, then we can give Alice a higher-dimensional plane to ensure that the number of cards is not too large relative to Alice and Cath's hands.

Corollary 27 *Given rational $\rho \in (0, 1)$, there are infinitely many values of a such that for any $c < a^\rho$ there is $b < a^{1+\rho}$ such that there is an informative and weakly safe strategy for (a, b, c).*

Proof Since ρ is rational, so is $1 + \rho$, so we can find $1 \leq \alpha < \delta$ such that $1 + \rho = \delta/\alpha$. Since $\rho < 1$, for large enough q we have that $q^{\rho\alpha} < q^\alpha - q^{\alpha-1}$. Thus for such a q we may use Theorem 25 to see that, for $a = q^\alpha$, $c < q^{\delta-\alpha}$ and $b = q^\delta - a - c$, $\mathrm{AS}(\alpha, \delta, q)$ is informative and weakly safe. Moreover, we have that $b < q^\delta = q^{(1+\rho)\alpha} = a^{(1+\rho)}$, whereas $c < q^{\delta-\alpha} = q^{\rho\alpha} = \alpha^\rho$ was arbitrary, so all desired conditions are met.

Alternately, one may use $\mathrm{PS}(\alpha, \delta, q)$ setting $a = \begin{bmatrix} \alpha+1 \\ 1 \end{bmatrix}_q$, $c < \begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q - 1$ and $b = \begin{bmatrix} \delta+1 \\ 1 \end{bmatrix}_q - a - c$. By Lemma 10, for large q we have that $b < a^{1+\rho}$ and $\begin{bmatrix} \delta-\alpha+1 \\ 1 \end{bmatrix}_q - 1 \geq a^\rho$. □

Observe that in either case, the geometric strategies give us infinitely many solutions for tuples (a, b, c) with $c < a$ and $b < ac$.

6 Strong safety of the geometric strategy

Since the geometric strategies are equitable, we may apply the results in Sect. 3 in order to find parameters for which they are ε-strongly safe. As we have seen, these strategies are weakly safe if c is relatively small with respect to a and b. Our goal now will be to show how, for any given ε, one can find tuples for which they are ε-strongly safe.

6.1 Some auxiliary estimates

We will need to find bounds on the number of hands that Cath considers possible. We begin by counting the total number of hands in an announcement. The following is a direct consequence of Lemma 13.

Lemma 28 *Let q be a prime power and $1 \leq \alpha < \delta$. The number of a-sets in an announcement of* $\mathrm{AS}(\alpha, \delta, q)$ *is* $q^{\delta-\alpha} \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$, *and in an announcement of* $\mathrm{PS}(\alpha, \delta, q)$ *is* $\begin{bmatrix} \delta+1 \\ \alpha+1 \end{bmatrix}_q$.

Now let us see how many hands Cath can discard from this announcement. Recall that $\mathcal{A}\backslash C$ denotes the set of lines avoiding C and $\mathcal{A}_x\backslash C$ denotes the set of lines avoiding C that also pass through x. We may compute the probability that Alice holds x from Cath's perspective as

$$P(x \in A|C, \mathcal{A}) = \frac{|\mathcal{A}_x\backslash C|}{|\mathcal{A}\backslash C|}.$$

What we are interested in is bounding the quotient of Cath's perceived probabilities before and after the announcement, that is,

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} = \frac{|\mathcal{A}_x\backslash C|/|\mathcal{A}\backslash C|}{a/a+b}. \tag{1}$$

As we will see, by modifying the parameters, this quotient can become arbitrarily close to 1.

In order to find bounds for (1), it suffices to bound the numerator, since the denominator is constant. Thus we need to estimate $|\mathcal{A}_x\backslash C|$ and $|\mathcal{A}\backslash C|$. Let us begin with the latter.

Lemma 29 *Let q be a prime power and $1 \leq \alpha < \delta$. If $\mathcal{A}$ is an announcement of the geometric strategy with parameters α, δ, q and $C \in \binom{\Omega}{c}$ is non-empty, then*

$$\left(q^{\delta-\alpha} - c\right)\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q \leq |\mathcal{A}\backslash C| \leq q^{\delta-\alpha}\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q. \tag{2}$$

If $\mathcal{A}$ is any announcement of $\mathrm{PS}(\alpha, \delta, q)$, *then*

$$\begin{bmatrix} \delta+1 \\ \alpha+1 \end{bmatrix}_q - c\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q \leq |\mathcal{A}\backslash C| \leq \begin{bmatrix} \delta+1 \\ \alpha+1 \end{bmatrix}_q. \tag{3}$$

Proof By Lemma 28, $|\mathcal{A}| = q^{\delta-\alpha}\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$. Thus we may estimate the number of α-planes that meet C and subtract to obtain our bounds.

Suppose that $\mathcal{A} = \mathcal{A}[f]$. To bound $|\mathcal{A}\backslash C|$ from below, observe that there are $\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$ α-planes passing through each point in $f[C]$ and there are c such points, so that the number of hands in $\mathcal{A}$ meeting C, which is equal to the number of α-planes touching $f[C]$, is at most $c\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$. It follows that

$$\left(q^{\delta-\alpha} - c\right)\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q \leq |\mathcal{A}\backslash C|.$$

The right-hand inequality is obvious, and the argument for $\mathrm{PS}(\alpha, \delta, q)$ is analogous. □

Lemma 30 *Let q be a prime power and $1 \leq \alpha < \delta$.*

1. *If $\mathcal{A}$ is any announcement of* $\mathrm{AS}(\alpha, \delta, q)$ *and $C \in \binom{\Omega}{c}$, then*

$$\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q - c\begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q \leq |\mathcal{A}_x\backslash C| \leq \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q. \tag{4}$$

2. *If $\mathcal{A}$ is any announcement of* $\mathrm{PS}(\alpha, \delta, q)$*, then*

$$\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q - c\begin{bmatrix}\delta-1\\ \alpha-1\end{bmatrix}_q \leq |\mathcal{A}_x \backslash C| \leq \begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q. \tag{5}$$

Proof Once again suppose that $\mathcal{A} = \mathcal{A}[f]$. First let us bound $|\mathcal{A}_x \backslash C|$ from below. To give our estimate, we will take the number of α-planes passing through $f(x)$ and subtract the number of α-planes passing through $f(x)$ and $f(y)$ for each $y \in C$, *without* taking into account that many α-planes will be subtracted twice. Evidently this bound will not be tight, but it will be sufficient to establish the existence of ε-strongly safe strategies.

Recall that $\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q$ counts *all* of the α-planes passing through a given point. But, there are $\begin{bmatrix}\delta-1\\ \alpha-1\end{bmatrix}_q$ α-planes passing through $f(x)$ and $f(y)$ for each $y \in C$, and thus there are at most $c\begin{bmatrix}\delta-1\\ \alpha-1\end{bmatrix}_q$ planes meeting both $f(x)$ and $f[C]$, hence also hands in $\mathcal{A}$ meeting x and C. It follows that

$$\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q - c\begin{bmatrix}\delta-1\\ \alpha-1\end{bmatrix}_q \leq |\mathcal{A}_x \backslash C|.$$

Once again, the upper bound is obvious and the projective case is analogous. □

6.2 Bounding probabilities

The counting lemmas we have given above may be used to bound the probabilities we are interested in.

Lemma 31 *Let q be a prime power and $1 \leq \alpha < \delta$. Then, if $\mathcal{A}$ is an announcement of either* $\mathrm{AS}(\alpha, \delta, q)$ *or* $\mathrm{PS}(\alpha, \delta, q)$ *and $C \in \binom{\Omega}{c}$ is non-empty, then*

$$1 - \frac{cq^\alpha}{q^\delta - 1} \leq \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \leq 1 + \frac{cq^\alpha}{q^\delta - cq^\alpha}. \tag{6}$$

Proof We will compute the lower bounds; the upper bounds follow from similar considerations. First assume that $\mathcal{A}$ is an announcement of $\mathrm{AS}(\alpha, \delta, q)$. In this case, using the lower bound of (4) and the upper bound of (2) we have that

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} = \frac{(q^\delta - c)|\mathcal{A}_x \backslash C|}{q^\alpha |\mathcal{A} \backslash C|} \geq 1 - c\left(\frac{q^{\delta+\alpha} - cq^\alpha + c - 1}{q^\delta(q^\delta - 1)}\right) > 1 - \frac{cq^\alpha}{q^\delta - 1},$$

where the last inequality uses the fact that $cq^\alpha - c + 1 > 0$.

If instead $\mathcal{A}$ is an announcement of $\mathrm{PS}(\alpha, \delta, q)$, we use the lower bound of (5) and the upper bound of (3) to obtain

$$\begin{aligned}\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} &= \frac{\left(\begin{bmatrix}\delta+1\\ 1\end{bmatrix}_q - c\right)|\mathcal{A}_x \backslash C|}{\begin{bmatrix}\alpha+1\\ 1\end{bmatrix}_q |\mathcal{A} \backslash C|} \geq \frac{\left(\begin{bmatrix}\delta+1\\ 1\end{bmatrix}_q - c\right)\left(\begin{bmatrix}\delta\\ \alpha\end{bmatrix}_q - c\begin{bmatrix}\delta-1\\ \alpha-1\end{bmatrix}_q\right)}{\begin{bmatrix}\alpha+1\\ 1\end{bmatrix}_q \begin{bmatrix}\delta+1\\ \alpha+1\end{bmatrix}_q} \\ &= \left(1 - c\left(\frac{q-1}{q^{\delta+1}-1}\right)\right)\left(1 - c\left(\frac{q^\alpha - 1}{q^\delta - 1}\right)\right) \\ &> 1 - c\left(\frac{q-1}{q^{\delta+1}-1} + \frac{q^\alpha - 1}{q^\delta - 1}\right) > 1 - \frac{cq^\alpha}{q^\delta - 1}.\end{aligned}$$

The upper bound of (6) follows from using the upper bounds of Lemma 30 together with the lower bounds of Lemma 29. Details are left to the reader. □

6.3 Convergence

Our simple bounds from Lemma 31 will be enough to yield many tuples for which the geometric strategy is ε-strongly safe for arbitrarily small ε. It is based on the following.

Theorem 32 *Let $\varepsilon > 0$, $1 \leq \alpha < \delta$ and $\bar{c}\colon \mathbb{N} \to \mathbb{N}$ be such that $\bar{c}(q) = o(q^{\delta-\alpha})$. Then, if q is a large enough prime power, both $\mathrm{AS}(\alpha, \delta, q)$ and $\mathrm{PS}(\alpha, \delta, q)$ are ε-strongly safe for any $c < \bar{c}(q)$.*

Proof Let $\mathcal{A}$ be any announcement of either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$, and x be any card. If $\bar{c}(q) = o(q^{\delta-\alpha})$ then $1 - \frac{\bar{c}(q)\, q^\alpha}{q^\delta - 1}$ and $1 + \frac{\bar{c}(q)\, q^\alpha}{q^\delta - \bar{c}(q)\, q^\alpha}$ both converge to 1 as $q \to \infty$. It follows from Lemma 31 that if q is large and $c < \bar{c}(q)$,

$$|P(x \in A|C, \mathcal{A})P(x \in A|C) - 1| < \varepsilon,$$

which means that the geometric strategy is ε-strongly safe. □

However, convergence may be quicker or slower depending on how we choose $\bar{c}$. For example, if we fix $\xi > 0$ and take $\bar{c}(q) = \lfloor q^{\delta-\alpha-\xi} \rfloor$, then this quotient will tend to 1, but if ξ is very small we may need a very large number of cards for it to be less than some given ε. More generally, we have the following:

Theorem 33 *Fix $1 \leq \alpha < \delta$, $\xi \in (0, \delta - \alpha)$ and $\bar{c}\colon \mathbb{N} \to \mathbb{N}$ with $\bar{c}(q) \leq q^{\delta-\alpha-\xi}$, and let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$. Then, for q a prime power, any announcement $\mathcal{A}$ of $\mathfrak{S}$, any card x and any set of C cards with at most $\bar{c}(q)$ elements,*

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} = 1 + O(1/q^\xi).$$

Proof If we take $c = \bar{c}(q) \leq q^{\delta-\alpha-\xi}$, we have that $\frac{cq^\alpha}{q^\delta - 1} \leq \frac{q^{\delta-\xi}}{q^\delta - 1} = O(1/q^\xi)$, whereas $\frac{cq^\alpha}{q^\delta - cq^\alpha} \leq \frac{q^{\delta-\xi}}{q^\delta - q^{\delta-\xi}} = O(1/q^\xi)$.

The theorem then follows from Lemma 31. □

Here we see a trade-off between keeping Cath's hand relatively large and obtaining a good rate of convergence for our bounds. Observe, however, that the larger c is, the less tight our bounds are, so despite our bounds converging rather slowly there may be smaller examples with a large degree of security. Because of this, in the next section we turn our attention to finding tighter bounds.

7 Improved bounds

As we have seen, ε-strongly safe solutions to the Russian cards problem exist provided we take large enough q and c relatively small. However, the bounds we have given, while suitable for establishing existence, are not too precise. In this section, we will provide improvements to Lemmas 29 and 30 that will later be useful in identifying triples (a, b, c) which are not too large and for which the geometric protocols are ε-strongly safe.

We will use the following, which is an immediate consequence of Lemma 9:

Lemma 34 *Let $1 \leq \alpha < \delta$ and q be a prime power.*

1. *If $x \notin C \subset \mathrm{AG}(\delta + 1, q)$ the number of α-planes touching x and avoiding C is equal to the number of $(\alpha - 1)$-planes on $\mathrm{PG}(\delta, q)$ avoiding $\pi_x(C)$, and*

2. *if* $x \notin C \subset \mathrm{AG}(\delta+1, q)$ *the number of* α*-planes on* $\mathrm{PG}(\delta+1, q)$ *touching* x *and avoiding* C *is equal to the number of* $(\alpha-1)$*-planes on* $\mathrm{PG}(\delta, q)$ *avoiding* $\pi_x^H(C)$*, where* H *is any hyperplane not meeting* x*.*

With this we obtain some exact bounds for the affine and projective protocols. Recall that $M(\alpha, \gamma, \delta, q, c)$ denotes Metsch's bound (see Definition 14).

Lemma 35 *Let* $q, \alpha, \delta, \gamma, c$ *be such that* q *is a prime power,* $1 \leq \alpha < \delta$*,* $\delta \geq \alpha + \gamma$ *and* $c < \begin{bmatrix} \gamma+1 \\ 1 \end{bmatrix}_q$*. Let* $\mathfrak{S}$ *be either* $\mathrm{AS}(\alpha, \delta, q)$ *or* $\mathrm{PS}(\alpha, \delta, q)$*,* $\mathcal{A} = \mathcal{A}[f]$ *for some suitable function* f*,* $C \in \binom{\Omega}{c}$ *and* $x \in \Omega \backslash C$*.*

1. *If* $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$*, then*
   (a) $M(\alpha-1, \gamma, \delta-1, q, c) \leq |\mathcal{A}_x \backslash C|$ *and*
   (b) $M(\alpha, \gamma, \delta, q, c) - \begin{bmatrix} \delta \\ \alpha+1 \end{bmatrix}_q \leq |\mathcal{A} \backslash C|$.
2. *If* $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$*, then*
   (a) $M(\alpha-1, \gamma, \delta-1, q, c) \leq |\mathcal{A}_x \backslash C|$ *and*
   (b) $M(\alpha, \gamma, \delta, q, c) \leq |\mathcal{A} \backslash C|$.

Proof Let $s = f(x)$ and $W = f[C]$. First assume that $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$. To bound $|\mathcal{A}_x \backslash C|$, note that by Lemma 34, the number of α-planes in $\mathrm{AG}(\delta, q)$ touching s but missing W is the same as the number of $(\alpha-1)$-planes in $\mathrm{PG}(\delta-1, q)$ missing $\pi_s[W]$. But by Theorem 15 applied to $\pi_s[W]$, there are at least $M(\alpha-1, \gamma, \delta-1, q, c)$ such $(\alpha-1)$-planes, giving us a lower bound for $|\mathcal{A}_x \backslash C|$, as claimed. The lower bound for $|\mathcal{A} \backslash C|$ follows similar considerations and is a direct consequence of Corollary 17.

Now consider $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$. To bound $|\mathcal{A}_x \backslash C|$, choose a hyperplane H not meeting s and consider the projection $\pi_s^H[W]$, which has less than $\begin{bmatrix} \gamma+1 \\ 1 \end{bmatrix}_q$ points. Thus we can apply Theorem 15 on H to see that there are at least $M(\alpha-1, \gamma, \delta-1, q, c)$ $(\alpha-1)$-planes on H not intersecting $\pi_s^H[W]$, thus this also gives a lower bound for the number of α-planes meeting s but not W and thus on $|\mathcal{A}_x \backslash C|$. The last bound arises directly from applying Theorem 15 on $\mathrm{PG}(\delta, q)$. □

Now let us turn our attention to our upper bounds, which may also be improved quite a bit.

Lemma 36 *Let* q, α, δ *be such that* q *is a prime power and* $1 \leq \alpha < \delta$*. Let* $\mathfrak{S}$ *be either* $\mathrm{AS}(\alpha, \delta, q)$ *or* $\mathrm{PS}(\alpha, \delta, q)$*,* $\mathcal{A} = \mathcal{A}[f]$ *for some suitable function* f*,* $C \in \binom{\Omega}{c}$ *and* $x \in \Omega \backslash C$*.*

1. *If* $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$*, then*

$$|\mathcal{A}_x \backslash C| \leq \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q - \left\lceil \frac{c}{q-1} \right\rceil \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q + \begin{pmatrix} \left\lceil \frac{c}{q-1} \right\rceil \\ 2 \end{pmatrix} \begin{bmatrix} \delta-2 \\ \alpha-2 \end{bmatrix}_q;$$

2. *if* $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$*, then*

$$|\mathcal{A}_x \backslash C| \leq \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q - \left\lceil \frac{c}{q} \right\rceil \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q + \begin{pmatrix} \left\lceil \frac{c}{q} \right\rceil \\ 2 \end{pmatrix} \begin{bmatrix} \delta-2 \\ \alpha-2 \end{bmatrix}_q.$$

Proof We prove the first claim. Set $s = f(x)$ and $W = f[C]$. We first show that there are at least

$$\left\lceil \frac{c}{q-1} \right\rceil \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q - \binom{\left\lceil \frac{c}{q-1} \right\rceil}{2} \begin{bmatrix} \delta-2 \\ \alpha-2 \end{bmatrix}_q \tag{7}$$

α-planes meeting both s and W.

To see this, let $y_1, \ldots, y_n$ be elements of W so that no two are collinear with s; we can find at least $\left\lceil \frac{c}{q-1} \right\rceil$ of these. There are $\begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q$ α-planes passing through each of these points and s, but we are counting many of them twice. Thus we must subtract $\binom{\left\lceil \frac{c}{q-1} \right\rceil}{2} \begin{bmatrix} \delta-2 \\ \alpha-2 \end{bmatrix}_q$ of them, possibly with repetitions, obtaining (7). The first item of the lemma is then immediate from subtracting (7) from the total $\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$ points meeting s.

The argument for $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ is analogous. □

Lemma 37 *Let q, α, δ be such that q is a prime power and $1 \leq \alpha < \delta$. Let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$, $\mathcal{A} = \mathcal{A}[f]$ for some suitable function f and $C \in \binom{\Omega}{c}$.*

1. *If $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$, then*

$$|\mathcal{A}\backslash C| \leq q^{\delta-\alpha} \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q - c \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q + \binom{c}{2} \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q;$$

2. *if $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$, then*

$$|\mathcal{A}\backslash C| \leq \begin{bmatrix} \delta+1 \\ \alpha+1 \end{bmatrix}_q - c \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q + \binom{c}{2} \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q.$$

Proof This is similar to the proof of Lemma 36. We consider the affine case; the argument for $\mathrm{PS}(\alpha, \delta, q)$ is analogous. Let $W = f[C]$. We first show that there are at least

$$c \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q - \binom{c}{2} \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q \tag{8}$$

α-planes meeting W. This is because there are $\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$ α-planes meeting each element of W and there are c elements, but given two distinct elements $u, v \in W$ there are $\begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_q$ meeting both, and $\binom{c}{2}$ such pairs, so we subtract to obtain (8). The first item of the lemma is then immediate from subtracting (8) from the total $q^{\delta-\alpha} \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_q$ α-planes. □

Example 38 In floating-point arithmetic, one represents real numbers using a fixed, finite number of digits; very commonly, eight digits are used. In this setting, it may be that the rounding error when computing our probability quotient is larger than the quotient itself. If this is the case, we may obtain a level of security which is indistinguishable from perfect security with respect to the representation method chosen to store numbers. Thus we will say that a strategy $\mathfrak{S}$ is **floating point-perfectly secure** for the triple (a, b, c) if it is 10^{-8}-strongly secure.

We can use the bounds provided in this section to find parameters for which the affine strategy is floating point-perfectly secure. Indeed, let $q = 13$, $\alpha = 2$ and $\delta = 10$. This gives rise to the triple (a, b, c) where $a = 169$, $b = 137{,}858{,}491{,}676$ and $c = 4$. Although the number of cards is rather large, this triple is remarkable in that the affine strategy is floating-point perfectly secure for it; indeed, $\mathrm{AS}(2, 10, 13)$ is 3.65×10^{-9}-strongly secure for this choice of parameters. Following this idea, we can always find triples for which we can construct floating-point perfectly secure strategies for any c, although as this example shows the deck may be quite large.

Table 1 Some choices of parameters for the geometric strategy along with their respective lower and upper bounds computed using Lemmas 35, 36 and 37. These triples were found by fixing c, α, δ and searching for small values of q such that the protocols became at least 0.05-strongly safe

a	b	c	$\mathfrak{S}$	q	α	δ	Lower	Upper
8	53	3	AS	2	3	6	0.9838	1.0205
8	117	3	AS	2	3	7	0.9968	1.0041
16	236	4	AS	2	4	8	0.9952	1.0051
7	501	3	PS	2	2	8	0.9998	1.0121
9	4666	6	PS	8	1	4	0.9999	1.0086
13	3259	8	PS	3	2	7	0.9998	1.0186

8 Choosing good parameters

In this section we will focus on finding specific choices of parameters for which the geometric strategies are ε-strongly safe. For illustration, we will fix $\varepsilon = 0.05$, and use our bounds to find several explicit tuples for which the geometric strategies are at least ε-strongly safe (Table 1). It is interesting to compare this to [19], where many choices of parameters for which the protocol is perfectly safe are exhibited. All of the tuples presented there have $c \leq 3$, and the authors discuss the difficulty of finding perfectly safe strategies for larger c. As we shall see this becomes substantially simpler if we weaken our requirements to, e.g., 0.05-strong safety. Thus we may argue that passing to a weaker notion of security allows us to make the Russian cards problem substantially easier to solve while providing Cath with an arbitrarily small amount of probabilistic information.

8.1 Perfectly secure strategies

The notion of perfect security for the Russian cards problem was introduced in [20], where several examples with $c = 1$ are provided. In [19], it is further shown that an equitative strategy $\mathfrak{S}$ is perfectly secure if and only if each of its announcements is a $(c+1)$-design. In this subsection we will show how perfect security for $c = 1$ follows from our bounds and extend this to some instances with $c = 2$ (Table 2).

Corollary 39 *Let $1 \leq \alpha < \delta$ and q be a prime power. Let $\mathfrak{S}$ be either $\mathrm{AS}(\alpha, \delta, q)$ or $\mathrm{PS}(\alpha, \delta, q)$ and $(a, b, 1)$ be a distribution type for $\mathfrak{S}$. Then, $\mathfrak{S}$ is perfectly safe for $(a, b, 1)$.*

Proof The lower bounds from Lemmas 30 and 29 are equal to the upper bounds from Lemmas 36 and 37, respectively (recall that $\binom{n}{m} = 0$ when $n < m$). Thus equality holds in both cases, and it is then straightforward to check that $P(x \in A|C, \mathcal{A}) = P(x \in A|C)$. □

Hence our bounds give an alternative proof that the geometric strategies are perfectly secure when $c = 1$. In fact, a simple counting argument shows that when $q = 2 = c$ we also attain perfect security, which is consistent with the results from [19].

Theorem 40 *Let $3 \leq \alpha < \delta$ and $(a, b, 2)$ be a distribution type for $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, 2)$. Then, $\mathfrak{S}$ is perfectly safe for $(a, b, 2)$.*

Proof No three points in $\mathrm{AS}(\alpha, \delta, 2)$ can be collinear. Thus, equality holds in Lemma 13.2, and using this we obtain, by the computations used for proving Lemmas 36 and 37, that for any announcement $\mathcal{A}$, any $C \in \binom{\Omega}{2}$ and any $x \in \Omega \backslash C$:

$$|\mathcal{A}_x \backslash C| = \begin{bmatrix} \delta \\ \alpha \end{bmatrix}_2 - 2\begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_2 + \begin{bmatrix} \delta-2 \\ \alpha-2 \end{bmatrix}_2$$
$$|\mathcal{A} \backslash C| = 2^{\delta-\alpha}\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_2 - 2\begin{bmatrix} \delta \\ \alpha \end{bmatrix}_2 + \begin{bmatrix} \delta-1 \\ \alpha-1 \end{bmatrix}_2.$$

Table 2 Choices of parameters (a, b, c) for $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$ or $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ such that $\mathfrak{S}$ is informative and perfectly safe for (a, b, c)

a	b	c	$\mathfrak{S}$	q	α	δ
3	5	1	AS	3	1	2
8	6	2	AS	2	3	4
16	14	2	AS	2	4	5
3	3	1	PS	2	1	2
4	8	1	PS	3	1	2
7	7	1	PS	2	2	3

It is then straightforward to check that $\frac{|\mathcal{A}_x \backslash C|}{|\mathcal{A} \backslash C|} = \frac{2^\alpha}{2^\delta - 2}$, and thus $P(x \in A|C, \mathcal{A}) = P(x \in A|C)$. □

8.2 Making Cath's hand large

Suppose that we wish to obtain good tuples for which c is as large as possible relative to Alice's hand. Cath's hand is bounded by two expressions on α, one which increases when α grows ($c < q^\alpha - q^{\alpha-1}$) and one which, instead, decreases ($c = o(q^{\delta-\alpha})$). Thus, the maximum value that c may take is when the two bounds coincide, which occurs approximately when $\delta = 2\alpha$ or $\delta = 2\alpha + 1$.

The latter case is interesting, since we already have that $q^\alpha - q^{\alpha-1} < q^{\delta-\alpha-1}$. Thus in cases that Alice holds relatively few cards, less than the square root of the deck, our informativity bound will already give us ε-strong safety for large values of q. To be precise, we have the following:

Corollary 41 *Let $\varepsilon, \beta > 0$ and $\rho \in (0, 1)$. Then, there are infinitely many values of a such that for any $c < \rho a$ there is $b < a^{2+\beta}$ so that there is an informative and ε-strongly safe strategy for (a, b, c).*

Proof Let $\varepsilon, \beta > 0$ and $\rho \in (0, 1)$. Pick α large enough so that $1/\alpha \leq \beta$ and Q large enough so that $1/Q < (1-\rho)/2$. Set $\delta = 2\alpha + 1$ and $\bar{c}(q) = q^\alpha + q^{\alpha-1} - 1$. Then, since $\delta - \alpha = \alpha + 1$ we have that $\bar{c}(q) = o(q^{\delta-\alpha})$, from which it follows from Theorem 32 that for large q, $\mathrm{AS}(\alpha, \delta, q)$ is informative and ε-strongly safe for $a = q^\alpha$, $c \leq \bar{c}(q)$ and $b = q^\delta - a - c$. In particular we may also take $q > Q$, so that

$$\bar{c}(q) = q^\alpha - q^{\alpha-1} - 1 = (1 - 1/q - 1/q^\alpha)a > \rho a.$$

Meanwhile, $b < q^\delta = (q^\alpha)^{\frac{2\alpha+1}{\alpha}} < a^{2+\beta}$, so all desired conditions are met.

Alternately, one can take $\bar{c}(q) = q^\alpha$. Then, $\left(\begin{bmatrix}\alpha+1\\1\end{bmatrix}_q\right)^{2+\beta} = O(q^{\alpha(2+\beta)})$, whereas $\begin{bmatrix}2\alpha+2\\1\end{bmatrix}_q = O(q^{2\alpha+1})$. In particular, we may choose α large enough so that $\alpha(2+\beta) > 2\alpha+1$. Then, for large q we obtain $\left(\begin{bmatrix}\alpha+1\\1\end{bmatrix}_q\right)^{2+\beta} > \begin{bmatrix}2\alpha+2\\1\end{bmatrix}_q$, as well as $q^\alpha > \rho\begin{bmatrix}\alpha+1\\1\end{bmatrix}_q$. Thus if we set $a = \begin{bmatrix}\alpha+1\\1\end{bmatrix}_q$, $c < q^\alpha$ and $b = \begin{bmatrix}\delta+1\\1\end{bmatrix}_q - a - c$ with q large enough, $\mathrm{PS}(\alpha, \delta, q)$ is informative and ε-strongly safe with all desired properties. □

Compare the above result to Corollary 26. As before we can have $c = O(a)$, but this time instead of having $b < ac$ we must take $b = O(ac^{1+\beta})$. Thus the price of obtaining ε-strong security is to make Bob's hand a bit larger than we would need for weak security. In Table 3, we fix values of ρ and β and use the strategy of Corollary 41 and its proof to find tuples for which the strategies are 0.05-strongly secure.

Table 3 Choices of parameters (a, b, c) for $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$ or $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ with $b < a^{2+\beta}$ and $c \approx \rho a$ such that $\mathfrak{S}$ is informative and at least 0.05-strongly safe strategy for (a, b, c), using the constructions of Corollary 41

a	b	c	$\mathfrak{S}$	q	α	δ	ρ	Lower	Upper
8	117	3	AS	2	3	7	3/8	0.9968	1.0041
9	231	3	AS	3	2	5	1/3	0.9986	1.0357
16	489	7	AS	2	4	9	7/16	0.9926	1.0081
25	3091	9	AS	5	2	5	9/25	0.999	1.0482
32	2001	15	AS	2	5	11	9/20	0.9895	1.0109
64	8105	23	AS	2	6	13	7/20	0.9952	1.0048
31	989	3	PS	2	4	9	3/16	0.999	1.0312
127	16,253	3	PS	2	6	13	1/32	0.9999	1.0078
21	1339	5	PS	4	2	5	5/16	0.9985	1.0468
255	65,275	5	PS	2	7	15	3/80	0.9999	1.0078
31	3867	8	PS	5	2	5	3/10	0.9991	1.0481
121	29,386	17	PS	3	4	9	1/5	0.9991	1.0466

8.3 Making Bob's hand small

We may also give a ε-strongly secure analogue of Corollary 27. Suppose that we instead want to have a small number of cards in Bob's hand relative to Alice's. In our above construction Bob's hand grew relatively quickly, so we want a different strategy for selecting parameters. The trade-off will be that Cath's hand may be substantially smaller than Alice's. In general if we want Bob to have less than $a^{1+\beta}$ cards, then Cath must have less than a^{ρ} for some $\rho < \beta$.

Corollary 42 *Let $\varepsilon > 0$, $\rho \in (0, 1)$ and $\beta > \rho$ be such that $\beta \in \mathbb{Q}$. Then, there are infinitely many values of a such that for any $c < a^{\rho}$ there is $b < a^{1+\beta}$ such that there is an informative and ε-strongly safe strategy for (a, b, c).*

Proof Similar to the proof of Corollary 27, but taking $c < q^{\rho\alpha}$ and using Theorem 32. □

Once again, we may obtain ε-strong security for infinitely many tuples (a, b, c) where $c < a$ and $b = O(ac^{1+\beta})$. So the takeaway in either case is that, making Bob's hand only a bit bigger compared to the rest of the deck and choosing an appropriately large deck, we may obtain ε-strong security instead of merely weak security. In Table 4 we use this idea to find additional tuples for which the geometric strategies are 0.05-safe or better.

Table 4 Choices of parameters (a, b, c) for $\mathfrak{S} = \mathrm{AS}(\alpha, \delta, q)$ or $\mathfrak{S} = \mathrm{PS}(\alpha, \delta, q)$ such that $c \approx a^{\rho}$, $b < a^{1+\beta}$ and $\mathfrak{S}$ is informative and at least 0.05-strongly safe for (a, b, c)

a	b	c	$\mathfrak{S}$	q	α	δ	ρ	Lower	Upper
32	477	3	AS	2	5	9	4/5	0.9956	1.0045
256	3837	3	AS	2	8	12	1/2	0.9953	1.0047
16	108	4	AS	2	4	7	3/4	0.9721	1.0294
64	1978	6	AS	2	6	11	5/6	0.9952	1.0048
400	19,205	3	PS	7	3	5	2/3	0.9995	1.0424
341	21,499	5	PS	4	4	7	3/4	0.9984	1.0498
1365	348,157	3	PS	4	5	9	4/5	0.9999	1.0078
3906	2,437,492	8	PS	5	5	9	4/5	0.9999	1.0096

9 Concluding remarks

While the Russian cards provides a setting for unconditionally safe communication, many known solutions to the Russian cards problem are only weakly safe, meaning that they may provide the eavesdropper with probabilistic information. Although perfectly secure solutions are known to exist, it is somewhat difficult to construct the designs required to attain this level of security. In this paper we have shown, however, that the amount of probabilistic information obtained by the eavesdropper may be controlled, to the extent that in some cases we can obtain a degree of safety indistinguishable from perfect safety with respect to floating point computation. Weakening the notion of perfect security has led to an infinite number of new tuples for which we may still obtain a high degree of security, and indeed the bounds we have given may be used to analyze the level of security in any instance of the geometric strategies. Moreover, our techniques had the added bonus of replicating some results of [20].

There are further directions that may be explored. Although many of our bounds are tight, some of them can be improved using a deeper combinatorial analysis. This might lead to smaller values of (a, b, c) for which the geometric strategies are ε-strongly safe that we were not able to identify.

Finally, this analysis could be generalized further to include other combinatorial constructions, for example considering a wider class of designs. Such efforts could very well lead to more flexible methods of finding tuples for which there are strategies with very high levels of security.

Acknowledgements We are grateful to Geertrui van de Voorde and Klaus Metsch for their comments, which led to the bounds of Sect. 7. David Fernández-Duque's work was partially supported by ANR-11-LABX-0040-CIMI within the Program ANR-11-IDEX-0002-02.

References

1. Albert M.H., Aldred R.E.L., Atkinson M.D., van Ditmarsch H., Handley C.C.: Safe communication for card players by combinatorial designs for two-step protocols. Australas. J. Comb. **33**, 33–46 (2005).
2. Blakley G.R.: Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS National Computer Conference, vol. 48, pp. 313–317 (1979).
3. Cordón-Franco A., van Ditmarsch H., Fernández-Duque D., Joosten J.J., Soler-Toscano F.: A secure additive protocol for card players. Australas. J. Comb. **54**, 163–176 (2012).
4. Cordón-Franco A., van Ditmarsch H., Fernández-Duque D., Soler-Toscano F.: A colouring protocol for the generalized Russian cards problem. Theor. Comput. Sci. **495**, 81–95 (2013).
5. Cordón-Franco, A., van Ditmarsch, H., Fernández-Duque D., Soler-Toscano F.: A geometric protocol for cryptography with cards. Des. Codes Cryptogr. **74**(1), 113–125 (2015).
6. Dembowski P.: Finite Geometries (reprint). Springer, New York (1997).
7. Duan Z., Yang C.: Unconditional secure communication: a Russian cards protocol. J. Comb. Optim. **19**, 501–530 (2010).
8. Fernández-Duque, D.: Perfectly secure data aggregation via shifted projections. Inform. Sci. **354**, 153–164 (2016).
9. Fernández-Duque D., Goranko V.: Secure aggregation of distributed information: how a team of agents can safely share secrets in front of a spy. Discret. Appl. Math. **198**, 118–135 (2016).
10. Fischer M.J., Wright R.N.: Bounds on secret key exchange using a random deal of cards. J. Cryptol. **9**(2), 71–99 (1996).
11. Keevash P.: The existence of designs. arXiv:1401.3665 (2014).

12. Kirkman T.P.: On a problem in combinations. Camb. Dublin Math. J. **2**, 191–204 (1847).
13. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1997).
14. Metsch K.: Blocking sets in projective spaces and polar spaces. J. Geom. **76**, 216–232 (2003).
15. Metsch K.: How many S-subspaces must miss a point set in PG(d, q). J. Geom. **86**(1–2), 154–164 (2007).
16. Ouellette J.: Quantum key distribution. Ind. Phys. **10**(6), 22–25 (2004).
17. Shamir A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979).
18. Stinson D.R.: Cryptography: Theory and Practice. CRC Press, Boca Raton (2005).
19. Swanson C.M., Stinson D.R.: Additional constructions to solve the generalized Russian cards problem using combinatorial designs. Electron. J. Comb. **21**(3), P3.29 (2014).
20. Swanson C.M., Stinson D.R.: Combinatorial solutions providing improved security for the generalized Russian cards problem. Des. Codes Cryptogr. **72**(2), 345–367 (2014).
21. van Ditmarsch H.: The Russian cards problem. Stud. Log. **75**, 31–62 (2003).
22. van Ditmarsch H., Soler-Toscano F.: Three steps. In: Proceedings of CLIMA XII. Lecture Notes in Computer Science, vol. 6814, pp. 41–57. Springer, New York (2011).