Additional Constructions to Solve the Generalized Russian Cards Problem using Combinatorial Designs

Colleen M. Swanson[1] ⋆ and Douglas R. Stinson[2] ⋆⋆

[1] Computer Science & Engineering Division
University of Michigan
Ann Arbor, MI 48109, USA
cmswnsn@umich.edu
[2] David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1 Canada
dstinson@uwaterloo.ca

Abstract. In the generalized Russian cards problem, we have a card deck X of n cards and three participants, Alice, Bob, and Cathy, dealt a, b, and c cards, respectively. Once the cards are dealt, Alice and Bob wish to privately communicate their hands to each other via public announcements, without the advantage of a shared secret or public key infrastructure. Cathy, for her part, should remain ignorant of all but her own cards after Alice and Bob have made their announcements. Notions for Cathy's ignorance in literature range from Cathy not learning the fate of any individual card with certainty (*weak* 1-*security*) to not gaining any probabilistic advantage in guessing the fate of some set of δ cards (*perfect* δ-*security*). As we demonstrate in this work, the generalized Russian cards problem has close ties to the field of combinatorial designs, on which we rely heavily, particularly for perfect security notions. Our main result establishes an equivalence between perfectly δ-secure strategies and $(c+\delta)$-designs on n points with block size a, when announcements are chosen uniformly at random from the set of possible announcements. We also provide construction methods and examples solutions, including a construction that yields perfect 1-security against Cathy when $c = 2$. Finally, we consider a variant of the problem that yields solutions that are easy to construct and optimal with respect to both the number of announcements and level of security achieved. Moreover, this is the first method obtaining weak δ-security that allows Alice to hold an arbitrary number of cards and Cathy to hold a set of $c = \lfloor \frac{a-\delta}{2} \rfloor$ cards. Alternatively, the construction yields solutions for arbitrary δ, c and any $a \geq \delta + 2c$.

1 Introduction

In the generalized Russian cards problem, we have a card deck X and three participants, Alice, Bob, and Cathy. Once the cards are dealt, Alice and Bob wish to privately communicate their hands to each other via public announcements, without the advantage of a shared secret or public key infrastructure. Here we focus on protocols of length two, which allows us to consider only Alice's announcement. That is, Alice should make an *informative* announcement, so that Bob learns the card deal. Bob, after hearing Alice's informative announcement, can always announce Cathy's hand. Cathy, for her part, should remain ignorant of all but her own cards after Alice and Bob have made their announcements.

Much of this work appears in the PhD thesis of the first author [28].

⋆ This work was supported in part by the TerraSwarm Research Center, one of six centers supported by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.
⋆⋆ Research supported by NSERC grant 203114-11

Notions for Cathy's ignorance in literature range from Cathy not learning the fate of any individual card with certainty (*weak* 1-*security*) to not gaining any probabilistic advantage in guessing the fate of some set of δ cards (*perfect* δ-*security*). As we discuss in this work, the generalized Russian cards problem has close ties to the field of combinatorial designs, on which we rely heavily, particularly for perfect security notions.

If a scheme satisfies weak 1-security, Cathy should not be able to say whether a given card is held by Alice or Bob (unless she holds the card herself). If a scheme satisfies perfect 1-security, each card is equally likely to be held by Alice. When Alice's strategy is *equitable* (in the sense that Alice picks uniformly at random from some set of possible announcements), we show an equivalence between perfectly secure strategies and sets of 2-designs on n points with block size a.

Generalizing these notions of weak and perfect security, which focus on the probability that individual cards are held by Alice, we consider instead the probability that a given set of δ cards is held by Alice. If the probability distribution is uniform across δ-sets, we say the scheme satisfies perfect δ-security, and if the distribution is not uniform (but positive for every possible δ-set), then we have weak δ-security. We consider equitable strategies and show an equivalence between perfectly δ-secure strategies and $(c+\delta)$-designs on n points with block size a. For equitable, informative, and perfectly $(a-c-1)$-secure strategies, we show $c=1$ and demonstrate an equivalence between these strategies and *Steiner systems* $S(a-1,a,n)$, a result first shown in Swanson and Stinson [27], albeit with a much more complicated proof than we present here.

Building on results in Swanson and Stinson [27], we show how to use a t-$(n,a,1)$-design to construct equitable (a,b,c)-strategies that are informative for Bob and perfectly $(t-c)$-secure against Cathy for any choice of c satisfying $c \leq \min\{t-1, a-t\}$. In particular, this indicates that if an appropriate t-design exists, it is possible to achieve perfect security for deals where Cathy holds more than one card. We present an example construction, based on *inversive planes*, for $(q+1, q^2-q-2, 2)$-strategies which are perfectly 1-secure against Cathy and informative for Bob, where q is a prime power. This example, first given in Swanson [28], is among the first strategies presented in the literature that is informative for Bob and achieves perfect 1-security against Cathy for $c>1$. This example was found independently from the work of Cordón-Franco et al. [8], discussed later, which presents a protocol that for certain parameters achieves perfect 1-security against Cathy for $c=2$.

Finally, we discuss a variation on the generalized Russian cards problem, where the card deck is first split into a piles, and Alice and Cathy's hands consist of at most one card from each pile, with Bob receiving the remaining cards. This variant admits a nice solution using *transversal designs* with $\lambda=1$ that achieves weak $(a-2c)$-security. In particular, this solution is easy to construct and is optimal with respect to both the number of announcements and level of security achieved. Moreover, this is the first method obtaining weak δ-security that allows Alice to hold an arbitrary number of cards and Cathy to hold a set of $c=\lfloor\frac{a-\delta}{2}\rfloor$ cards. Alternatively, the construction yields solutions for arbitrary δ, c and any $a \geq \delta+2c$.

1.1 Paper outline

After reviewing basic results from combinatorial designs in Section 2, we review the basic framework for the generalized Russian cards problem and establish relevant notation in Section 3. In Section 4, we study and define the notion of an informative strategy. We then move to a formal discussion of secure strategies in Section 5. In Section 6, we explore strategies that are simultaneously informative and either weakly or perfectly δ-secure, discussing construction methods and examples in Section 7.

In Section 8 we discuss a variant of the generalized Russian cards problem and present a solution using transversal designs. We discuss related work in Section 9. Finally, we give some concluding remarks in Section 10.

2 Combinatorial Designs

In this section, we present fundamental definitions and standard results from the theory of combinatorial designs needed in this paper. For general references on this material, we refer the reader to Stinson [25] and Colbourn and Dinitz [5]. All results stated in this section without proof can be found in [5, 25].

2.1 t-designs

Definition 2.1. Let v, k, λ, and t be positive integers with $v > k \geq t$. A t-(v, k, λ)-*design* is a set system $(X, \mathcal{B})$ such that the following are satisfied:

1. $|X| = v$,
2. each block contains exactly k points, and
3. every subset of t distinct points from X occurs in precisely λ blocks.

Remark 2.2. A 2-(v, k, λ)-design is also called a (v, k, λ) *balanced incomplete block design*, or (v, k, λ)-*BIBD*.

Definition 2.3. A *symmetric BIBD* is a (v, k, λ)-BIBD in which there are v blocks.

Theorem 2.4. *In a symmetric BIBD, any two blocks intersect in exactly λ points.*

Definition 2.5. The design formed by taking λ copies of every k-subset of a v-set as blocks is a t-$\left(v, k, \lambda\binom{v-t}{k-t}\right)$-design, called a *trivial t-design*.

The following theorems are standard results for t-designs:

Theorem 2.6. *Let $(X, \mathcal{B})$ be a t-(v, k, λ)-design. Let $Y \subseteq X$ such that $|Y| = s \leq t$. Then there are precisely*

$$\lambda_s = \frac{\lambda\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$$

blocks in $\mathcal{B}$ that contain Y.

Theorem 2.7. *Let $(X, \mathcal{B})$ be a t-(v, k, λ)-design. Let $Y \subseteq X$ and $Z \subseteq X$ such that $Y \cap Z = \emptyset$, $|Y| = i$, $|Z| = j$, and $i + j \leq t$. Then there are precisely*

$$\lambda_i^j = \frac{\lambda\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}$$

blocks in $\mathcal{B}$ that contain all the points in Y and none of the points in Z.

Example 2.8. A 3-$(8, 4, 1)$-design.

$$X = \{0, 1, 2, 3, 4, 5, 6, 7\} \text{ and}$$

$$\mathcal{B} = \{3456, 2567, 2347, 1457, 1367, 1246, 1235, 0467, 0357, 0245, 0236, 0156, 0134, 0127\}.$$

Definition 2.9. A t-$(v, k, 1)$-design is called a *Steiner system with parameters t, k, v* and is denoted by $\mathrm{S}(t, k, v)$.

Remark 2.10. A *Steiner triple system of order* v, or $\mathrm{STS}(v)$, is an $\mathrm{S}(2, 3, v)$, i.e., a Steiner system in which $k = 3$. It is known that an $\mathrm{STS}(n)$ exists if and only if $n \equiv 1, 3 \bmod 6$, $n \geq 7$.

Definition 2.11. A *large set of* t-$(v, k, 1)$-*designs* is a set $\{(X, \mathcal{B}_1), \ldots, (X, \mathcal{B}_N)\}$ of t-$(v, k, 1)$-designs (all of which have 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. That is, the $\mathcal{B}_i$s form a partition of $\binom{X}{k}$.

Remark 2.12. It is easy to prove that there must be exactly $N = \binom{v-t}{k-t}$ designs in a large set of t-$(v, k, 1)$-designs.

Remark 2.13. There are $v-2$ designs in a large set of $\mathrm{STS}(v)$. It is known that a large set of $\mathrm{STS}(v)$ exists if and only if $v \equiv 1, 3 \bmod 6$ and $v \geq 9$.

Example 2.14. A large set of STS(9) [22].

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \text{ and } \mathcal{B}_1, \ldots, \mathcal{B}_7,$$

where the 7 block sets $\mathcal{B}_1, \ldots, \mathcal{B}_7$ are given by the rows of the following table:

123 145 169 178 249 257 268 348 356 379 467 589
124 136 158 179 235 267 289 349 378 457 468 569
125 137 149 168 238 247 269 346 359 458 567 789
126 139 148 157 234 259 278 358 367 456 479 689
127 135 146 189 239 248 256 347 368 459 578 679
128 134 159 167 236 245 279 357 389 469 478 568
129 138 147 156 237 246 258 345 369 489 579 678

2.2 Transversal Designs

Definition 2.15. Let t, v, k, and λ be positive integers satisfying $k \geq t \geq 2$. A *transversal design* $\mathrm{TD}_\lambda(t, k, v)$ is a triple $(X, \mathcal{G}, \mathcal{B})$ such that the following properties are satisfied:

1. X is a set of kv elements called *points*,
2. $\mathcal{G}$ is a partition of X into k subsets of size v called *groups*,
3. $\mathcal{B}$ is a set of k-subsets of X called *blocks*,
4. any group and any block contain exactly one common point, and
5. every subset of t points from distinct groups occurs in precisely λ blocks.

Many of the standard results for t-designs can be extended to transversal designs. The following terminology and results are useful:

Definition 2.16. Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}_\lambda(t, k, v)$ and write $\mathcal{G} = \{G_j : 1 \leq j \leq k\}$. Suppose $Z \subseteq X$ such that $|Z| = i \leq k$ and $|Z \cap G_j| \leq 1$ for $1 \leq j \leq k$. We say Z is a *partial transversal of* $\mathcal{G}$. If $i = k$, then we say Z is a *transversal of* $\mathcal{G}$.

Definition 2.17. For a partial transversal Z of $\mathcal{G}$, we let $G_Z = \{G_j \in \mathcal{G} : Z \cap G_j \neq \emptyset\}$ denote the set of groups that intersect Z. If Y, $Z \subseteq X$ are partial transversals of $\mathcal{G}$ such that $G_Z \cap G_Y = \emptyset$, we say Y, Z are *group disjoint*.

Theorem 2.18. *Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}_\lambda(t, k, v)$. Suppose $Y \subseteq X$ such that $|Y| = s \leq t$ and Y is a partial transversal of $\mathcal{G}$. Then there are exactly $\lambda_s = \lambda v^{t-s}$ blocks containing all the points in Y.*

Proof. Fix a subset of $t - s$ groups disjoint from Y, say $G'_1, \ldots, G'_{t-s}$. Consider a t-subset X consisting of all the points from Y and one point from each of $G'_1, \ldots, G'_{t-s}$. In particular, there are v^{t-s} such t-subsets X, and each such X occurs in precisely λ blocks. Note that every block that contains Y is a transversal of $\mathcal{G}$, so every such block contains exactly one such t-subset X. Therefore Y occurs in precisely λv^{t-s} blocks, as desired.

Theorem 2.19. *Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}_\lambda(t, k, v)$. Suppose Y, $Z \subseteq X$ are group disjoint partial transversals of $\mathcal{G}$ such that $|Y| = i$, $|Z| = j$, and $i + j \leq t$. Then there are exactly*

$$\lambda_i^j = \lambda v^{t-i-j}(v-1)^j$$

blocks in $\mathcal{B}$ that contain all the points in Y and none of the points in Z.

Proof. Consider the set of groups G_Z that intersect Z. There are $(v-1)^j$ subsets X such that X consists of all the points from Y and one point from each group in G_Z, but X contains no points from Z. Each such $(i+j)$-subset X occurs in precisely λ_{i+j} blocks by Theorem 2.18. Therefore there are $\lambda_{i+j}(v-1)^j = \lambda v^{t-i-j}(v-1)^j$ blocks that contain all the points of Y but none of the points of Z.

We can also apply the notion of *large sets* to transversal designs:

Definition 2.20. A *large set of* $\mathrm{TD}_\lambda(t, k, v)$ *on the point set X and group partition $\mathcal{G}$* is a set $\{(X, \mathcal{G}, \mathcal{B}_1), \ldots, (X, \mathcal{G}, \mathcal{B}_N)\}$ of $\mathrm{TD}_\lambda(t, k, v)$ in which every set of k points from distinct groups of X occurs as a block in precisely one of the $\mathcal{B}_i$s.

Remark 2.21. It is easy to see that there must be $N = \frac{v^k}{\lambda v^t}$ transversal designs in a large set of $\mathrm{TD}_\lambda(t, k, v)$.

Transversal designs are equivalent to *orthogonal arrays*:

Definition 2.22. Let t, v, k, and λ be positive integers satisfying $k \geq t \geq 2$. An *orthogonal array* $\mathrm{OA}_\lambda(t, k, v)$ is a pair (X, D) such that the following properties are satisfied:

1. X is a set of v elements called *points*,
2. D is a λv^t by k array whose entries are elements of X, and
3. within any t columns of D, every t-tuple of points occurs in precisely λ rows.

Example 2.23. An $\mathrm{OA}_1(2, 4, 3)$.

1 1 1 1
1 2 3 3
1 3 2 2
2 1 2 3
2 2 1 2
2 3 3 1
3 1 3 2
3 2 2 1
3 3 1 3

It is easy to see the correspondence between orthogonal arrays and transversal designs. Suppose (X, D) is an $\mathrm{OA}_\lambda(t, k, v)$. We define a bijection ϕ between the rows r_j of D and the blocks B_j of a $\mathrm{TD}_\lambda(t, k, v)$ as follows. For each row $r_j = [x_{j1}x_{j2}\cdots x_{jk}]$ of D, let

$$\phi(r_j) = \{(x_{j1}, 1), (x_{j2}, 2), \ldots (x_{jk}, k)\} = B_j$$

define a block B_j. Define $G_i = \{1, \ldots, v\} \times \{i\}$ for $1 \le i \le k$. Then $(X \times \{1, \ldots, k\}, \mathcal{G}, \mathcal{B})$ is a $\mathrm{TD}_\lambda(t, k, v)$ with $\mathcal{G} = \{G_i : 1 \le i \le k\}$ and $\mathcal{B} = \{B_j : 1 \le j \le \lambda v^t\}$.

Example 2.24. The blocks of the $\mathrm{TD}_1(2, 4, 3)$ obtained from the $\mathrm{OA}_1(2, 4, 3)$ in Example 2.23:

B_1: (1, 1) (1, 2) (1, 3) (1, 4)
B_2: (1, 1) (2, 2) (3, 3) (3, 4)
B_3: (1, 1) (3, 2) (2, 3) (2, 4)
B_4: (2, 1) (1, 2) (2, 3) (3, 4)
B_5: (2, 1) (2, 2) (1, 3) (2, 4)
B_6: (2, 1) (3, 2) (3, 3) (1, 4)
B_7: (3, 1) (1, 2) (3, 3) (2, 4)
B_8: (3, 1) (2, 2) (2, 3) (1, 4)
B_9: (3, 1) (3, 2) (1, 3) (3, 4)

The above construction method can be reversed for an arbitrary $\mathrm{TD}_\lambda(t, k, v)$, say $(X, \mathcal{G}, \mathcal{B})$. To see this, note that we can relabel the points such that $X = \{1, \ldots, v\} \times \{1, \ldots, k\}$ and $\mathcal{G} = \{G_i : 1 \le i \le k\}$. Then the fact that any block and any group must contain exactly one common point implies that for each $B \in \mathcal{B}$, we can form the k-tuple $(b_1, \ldots, b_k)$, where $b_i \in B \cap G_i$ for $1 \le i \le k$. We can form an orthogonal array $\mathrm{OA}_\lambda(t, k, v)$ by taking all of these k-tuples as rows.

Definition 2.25. A *large set of* $\mathrm{OA}_\lambda(t, k, v)$ *on the point set* X is a set of $\mathrm{OA}_\lambda(t, k, v)$, say $\{(X, D_1), \ldots, (X, D_N)\}$, in which every k-tuple of elements from X occurs as a row in precisely one of the D_is. That is, the D_is form a partition of the set X^k of k-tuples with entries from X.

Remark 2.26. It is easy to see that there must be $N = \frac{v^k}{\lambda v^t}$ orthogonal arrays in a large set of $\mathrm{OA}_\lambda(t, k, v)$.

A useful type of orthogonal array is a *linear array*, especially for constructing large sets:

Definition 2.27. Let (X, D) be an $\mathrm{OA}_\lambda(t, k, v)$. We say (X, D) is *linear* if $X = \mathbb{F}_q$ for some prime power q and the rows of D form a subspace of $(\mathbb{F}_q)^k$ of dimension $\log_q|D|$.

Linear orthogonal arrays (and hence the corresponding transversal designs) are easy to construct. In particular, the following is a useful construction method.

Theorem 2.28. *Suppose q is a prime power and k and ℓ are positive integers. Suppose M is an ℓ by k matrix over $\mathbb{F}_q$ such that every set of t columns of M is linearly independent. Then (X, D) is a linear $\mathrm{OA}_{q^{\ell-t}}(t, k, q)$, where D is the q^ℓ by k matrix formed by taking all linear combinations of the rows of M.*

Let q be a prime power and for every $x \in \mathbb{F}_q$, let $\boldsymbol{x} = [1, x, x^2, \ldots, x^{t-1}] \in (\mathbb{F}_q)^t$ for some integer $t \geq 2$. Construct the t by q matrix M by taking the columns to be the vectors $(\boldsymbol{x})^T$ for every $x \in \mathbb{F}_q$, where here $(\boldsymbol{x})^T$ means the transpose of $\boldsymbol{x}$. Applying Theorem 2.28 to M yields the following result:

Corollary 2.29. *Let $t \geq 2$ be an integer and let q be a prime power. Then there exists a linear $\mathrm{OA}_1(t, q, q)$.*

The following result is immediate.

Corollary 2.30. *Let $t \geq 2$ be an integer and let q be a prime power. Then there exists a linear $\mathrm{TD}_1(t, q, q)$.*

Remark 2.31. The constructions discussed in Corollaries 2.29 and 2.30 are known as *Reed-Solomon codes* [25].

We now discuss how to construct a large set of linear orthogonal arrays from a "starting" linear orthogonal array. Suppose (X, D) is a linear $\mathrm{OA}_\lambda(t, k, v)$. We can obtain a large set of orthogonal arrays (and therefore transversal designs) from (X, D) by taking the set of cosets of D in $(\mathbb{F}_q)^k$. In particular, D is a subspace of $(\mathbb{F}_q)^k$, so the cosets of D form a partition of $(\mathbb{F}_q)^k$.

3 Terminology and Notation

We review the terminology and notation established by Swanson and Stinson [27]. Throughout, we let $\binom{X}{t}$ denote the set of $\binom{n}{t}$ t-subsets of X, where t is a positive integer.

Let X be a deck of n cards. In an (a, b, c)-*deal* of X, 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, such that $a + b + c = n$. That is, it must be the case that $H_A \cup H_B \cup H_C = X$. We assume these hands are random and dealt by some external entity.

An *announcement* by Alice is a subset of $\binom{X}{a}$ containing Alice's current hand, H_A. More generally, Alice chooses a set of m announcements $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \subseteq \binom{X}{a}$ satisfying $\cup_{i=1}^m \mathcal{A}_i = \binom{X}{a}$. For every $H_A \in \binom{X}{a}$, we define $g(H_A) = \{i : H_A \in \mathcal{A}_i\}$, i.e., the set of possible announcements for Alice given the hand H_A. Alice's *announcement strategy*, or simply *strategy*, consists of a probability distribution p_{H_A} defined on $g(H_A)$, for every $H_A \in \binom{X}{a}$.

In keeping with Kerckhoffs' principle, we assume the set of announcements and probability distributions are fixed ahead of time and public knowledge. For a given hand $H_A \in \binom{X}{a}$, Alice randomly chooses an index $i \in g(H_A)$ according to the probability distribution p_{H_A}. Alice broadcasts the integer i to specify her announcement $\mathcal{A}_i$. Without loss of generality, we assume that $p_{H_A}(i) > 0$ for all $i \in g(H_A)$.

For the purposes of this paper, we assume there exists some constant γ such that $|g(H_A)| = \gamma$ for every H_A and that every probability distribution p_{H_A} is *uniform*; such strategies are termed

γ-*equitable*, or simply *equitable*. Throughout, we use the phrase (a, b, c)-*strategy* $\mathcal{A}$ to denote a strategy for an (a, b, c)-deal, where $\mathcal{A}$ is the associated set of possible announcements for Alice.

The following notation is useful in discussing the properties of a given strategy $\mathcal{A}$. For any subset $Y \subseteq X$ and any announcement $\mathcal{A}_i \in \mathcal{A}$, we define

$$\mathcal{P}_{\mathcal{A}}(Y, i) = \{H_A \in \mathcal{A}_i : H_A \cap Y = \emptyset\}.$$

That is, $\mathcal{P}_{\mathcal{A}}(Y, i)$ is the set of hands of $\mathcal{A}_i$ that do not intersect the subset Y. When the strategy $\mathcal{A}$ is clear from context, we write $\mathcal{P}_{\mathcal{A}}(Y, i)$ as $\mathcal{P}(Y, i)$.

4 Informative strategies

Suppose we have an (a, b, c)-deal and Alice chooses announcement $\mathcal{A}_i$ from the set $\mathcal{A}$ of possible announcements. From Bob's point of view, the set of possible hands for Alice given Alice's announcement $\mathcal{A}_i$ and Bob's hand $H_B \in \binom{X}{b}$ is

$$\mathcal{P}(H_B, i) = \{H_A \in \mathcal{A}_i : H_A \cap H_B = \emptyset\}.$$

We say Alice's strategy is *informative for Bob* provided that

$$|\mathcal{P}(H_B, i)| \leq 1 \tag{1}$$

for all $H_B \in \binom{X}{b}$ and for all i. That is, if Equation (1) is satisfied, Bob can determine the set of a cards that Alice holds from Alice's announcement. In particular, this implies that Bob can announce Cathy's hand, thereby informing Alice of the card deal as well. Specified on the level of individual announcements, we say an announcement $\mathcal{A}_i$ is *informative* provided $|\mathcal{P}(H_B, i)| \leq 1$ for any hand $H_B \in \binom{X}{b}$.

The following theorem, first shown by Albert et al. [1], is a useful equivalence condition for informative announcements:

Theorem 4.1. *[1] 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 $|H_A \cap H'_A| \geq a - c$.*

The following is an immediate corollary.

Corollary 4.2. *Suppose there exists a strategy for Alice that is informative for Bob. Then $a > c$.*

We make the following observation, which follows directly from Theorem 4.1 and the definition of a t-design.

Corollary 4.3. *Suppose $a > c$ and each announcement $\mathcal{A}_i$ in an (a, b, c)-strategy is a t_i-$(n, a, 1)$-design, where $t_i \leq a - c$. Then the strategy is informative for Bob.*

It is possible to have informative (a, b, c)-strategies using announcements which are t-designs with $\lambda > 1$. In particular, Theorem 4.1 indicates that the block intersection properties of the chosen design are relevant to whether or not the strategy is informative. If every announcement is a symmetric BIBD, for example, then the strategy is guaranteed to be informative when $a - c > \lambda$. This is because the intersection of any two blocks in a symmetric BIBD contains exactly λ points, as stated in Theorem 2.4.

We make one more observation relating combinatorial designs and informative strategies.

Lemma 4.4. *Suppose $a > c$ and each announcement $\mathcal{A}_i$ in an (a, b, c)-strategy $\mathcal{A}$ is a t_i-(n, a, λ_i)-design, where $t_i \geq a - c$. If $\mathcal{A}$ is informative for Bob, then $t_i = a - c$ and $\lambda_i = 1$ for all i.*

Proof. Consider an announcement $\mathcal{A}_i \in \mathcal{A}$. If $\lambda_i > 1$, then there exist two blocks whose intersection has cardinality at least $t_i \geq a - c$. This contradicts Theorem 4.1, so $\lambda_i = 1$, as desired.

If $t_i > a - c$, then from Theorem 2.6, there are

$$\frac{v - (t_i - 1)}{k - (t_i - 1)} > 1$$

blocks that contain $t_i - 1$ fixed points. Since $t_i - 1 \geq a - c$, this contradicts Theorem 4.1, so $t_i = a - c$, as desired.

5 Secure strategies

We provide the general security definitions and state the equivalent combinatorial characterization of secure equitable strategies from Swanson and Stinson [27].

Definition 5.1. Let $1 \leq \delta \leq a$.

1. Alice's strategy is *weakly δ-secure against Cathy* provided that for any announcement $\mathcal{A}_i$, for any $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, and for any δ'-subset $Y \subseteq X \backslash H_C$ where $1 \leq \delta' \leq \delta$, it holds that
$$0 < \Pr[Y \subseteq H_A \mid i, H_C] < 1.$$
Weak security means that, from Cathy's point of view, any set of δ or fewer elements from $X \backslash H_C$ may or may not be held by Alice.
2. Alice's strategy is *perfectly δ-secure against Cathy* provided that for any announcement $\mathcal{A}_i$, for any $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, and for any δ'-subset $Y \subseteq X \backslash H_C$ where $1 \leq \delta' \leq \delta$, it holds that
$$\Pr[Y \subseteq H_A \mid i, H_C] = \frac{\binom{a}{\delta'}}{\binom{a+b}{\delta'}}.$$
Perfect security means that, from Cathy's point of view, the probability that any set of δ or fewer cards from $X \backslash H_C$ is held by Alice is a constant.

Swanson and Stinson [27] show that in an equitable strategy any hand $H_A \in \mathcal{P}(H_C, i)$ is equally likely from Cathy's point of view:

Lemma 5.2. *[27] Suppose that Alice's strategy is γ-equitable, Alice's announcement is $\mathcal{A}_i$, $H_C \in \binom{X}{c}$ and $H_A \in \mathcal{P}(H_C, i)$. Then*

$$\Pr[H_A \mid H_C, i] = \frac{1}{|\mathcal{P}(H_C, i)|}. \tag{2}$$

Swanson and Stinson [27] also establish the following equivalent combinatorial conditions:

Theorem 5.3. *[27] Suppose that Alice's strategy is γ-equitable. Then the following hold:*

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

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

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

$$|\{H_A \in \mathcal{P}(H_C, i) : Y \subseteq H_A\}| = \frac{\binom{a}{\delta} \; |\mathcal{P}(H_C, i)|}{\binom{a+b}{\delta}}$$

for any δ-subset $Y \subseteq X \backslash H_C$.

We have the following elementary result:

Lemma 5.4. *Consider an (a, b, c)-strategy $\mathcal{A}$ that is weakly 1-secure. Then for all $\mathcal{A}_i \in \mathcal{A}$ and $x \in X$, we have $\mathcal{P}(\{x\}, i) \neq \emptyset$.*

Proof. We proceed by contradiction. Suppose $\mathcal{P}(\{x\}, i) = \emptyset$ for some $\mathcal{A}_i \in \mathcal{A}$ and $x \in X$. Then x occurs in every hand of $\mathcal{A}_i$. That is, if Alice announces $\mathcal{A}_i$, then Alice must hold x. In particular, this implies that Cathy's hand, say H_C, does not contain x and $\Pr[x \in H_A \mid i, H_C] = 1$.

Here is a sufficient condition for an equitable strategy to be perfectly 1-secure against Cathy, first shown by Swanson and Stinson [27]:

Lemma 5.5. *[27] Suppose that each announcement $\mathcal{A}_i$ in an equitable $(a, b, 1)$-strategy $\mathcal{A}$ is a 2-(n, a, λ_i)-design. Then the strategy is perfectly 1-secure against Cathy.*

In fact, the condition that every announcement $\mathcal{A}_i$ be a 2-(n, a, λ_i)-design is also a necessary condition for an equitable $(a, b, 1)$-strategy to be perfectly 1-secure, as the following Theorem shows.

Theorem 5.6. *Suppose we have an equitable $(a, b, 1)$-strategy $\mathcal{A}$ that is perfectly 1-secure against Cathy. Then every announcement $\mathcal{A}_i \in \mathcal{A}$ is a 2-(n, a, λ_i)-design.*

Proof. First observe that since Cathy holds only one card, Lemma 5.4 immediately implies that any element $x \in X$ is a possible hand for Cathy. Consider an announcement $\mathcal{A}_i \in \mathcal{A}$. We proceed by showing that every pair of distinct elements x, $y \in X$ occurs in a constant number of hands of $\mathcal{A}_i$.

Let $x \in X$. Define r_x to be the number of hands of $\mathcal{A}_i$ containing x. We proceed by counting r_x in two different ways. On the one hand, we immediately have

$$r_x = |\mathcal{A}_i| - |\mathcal{P}(\{x\}, i)|. \tag{3}$$

On the other hand, we can relate r_x to $\mathcal{P}(\{y\}, i)$ for any $y \neq x \in X$ as follows. Since the strategy is perfectly 1-secure, x occurs a constant number of times in $\mathcal{P}(\{y\}, i)$, namely $\frac{a}{a+b} |\mathcal{P}(\{y\}, i)|$ times. In particular, this is the number of times x occurs in a hand of $\mathcal{A}_i$ without y. That is, letting λ_{xy} denote the number of times x occurs together with y in a hand of $\mathcal{A}_i$, we have

$$r_x = \lambda_{xy} + \frac{a}{a+b} |\mathcal{P}(\{y\}, i)|. \tag{4}$$

This gives us

$$|\mathcal{A}_i| = \lambda_{xy} + \frac{a}{a+b}\left|\mathcal{P}\left(\{y\}, i\right)\right| + \left|\mathcal{P}\left(\{x\}, i\right)\right|. \tag{5}$$

Now, following the same logic for y, we also have

$$|\mathcal{A}_i| = \lambda_{xy} + \frac{a}{a+b}\left|\mathcal{P}\left(\{x\}, i\right)\right| + \left|\mathcal{P}\left(\{y\}, i\right)\right|. \tag{6}$$

Equating Equations (5) and (6) shows that $|\mathcal{P}(\{x\}, i)|$ is independent of the choice of $x \in X$. That is, r_x is independent of x (by Equation (3)), so every point of X occurs in a constant number of hands of $\mathcal{A}_i$, say r hands. Moreover, Equation (4) then gives

$$\lambda_{xy} = r - \frac{a}{a+b}\left|\mathcal{P}\left(\{y\}, i\right)\right| = r - \frac{a}{a+b}\left(|A_i| - r\right),$$

so λ_{xy} is independent of x and y. That is, every pair of points x, $y \in X$ occurs a constant number of times, which we denote by λ_i. This implies $\mathcal{A}_i$ is a 2-(n, a, λ_i)-design.

The relationship between combinatorial designs and strategies that satisfy our notion of perfect security is quite deep. We now generalize the results from Swanson and Stinson [27] and Theorem 5.6 above to account for perfect δ-security and card deals with $c \geq 1$. We begin with a generalization of Lemma 5.5 that shows that in an equitable (a, b, c)-strategy, if each announcement is a t-design with block size a, the strategy satisfies perfect $(t - c)$-security.

Theorem 5.7. *Suppose that each announcement $\mathcal{A}_i$ in an equitable (a, b, c)-strategy $\mathcal{A}$ is a t-(n, a, λ_i)-design, where $c \leq t - 1$. Then the strategy is perfectly $(t - c)$-secure against Cathy.*

Proof. Consider an announcement $\mathcal{A}_i \in \mathcal{A}$ and a possible hand H_C for Cathy. Since $c \leq t$, Theorem 2.7 implies there are

$$\left|\mathcal{P}\left(H_C, i\right)\right| = \frac{\lambda_i \binom{n-c}{a}}{\binom{n-t}{a-t}} = \frac{\lambda_i \binom{a+b}{a}}{\binom{n-t}{a-t}}$$

blocks in $\mathcal{A}_i$ that do not contain any of the points of H_C.

Let $\delta \leq t - c$. Then Theorem 2.7 also implies that each set of δ points $x_1, \ldots, x_\delta \in X \backslash H_C$ is contained in precisely

$$\left|\{H_A \in \mathcal{P}\left(H_C, i\right) : x_1, \ldots, x_\delta \in H_A\}\right| = \frac{\lambda_i \binom{n-\delta-c}{a-\delta}}{\binom{n-t}{a-t}} = \frac{\lambda_i \binom{a+b-\delta}{a-\delta}}{\binom{n-t}{a-t}}$$

of these blocks.

Thus, for any set of δ points $x_1, \ldots, x_\delta \in X \backslash H_C$, we have

$$\frac{\left|\mathcal{P}\left(H_C, i\right)\right|}{\left|\{H_A \in \mathcal{P}\left(H_C, i\right) : x_1, \ldots, x_\delta \in H_A\}\right|} = \frac{(a+b)!(a-\delta)!}{a!(a+b-\delta)!} = \frac{\binom{a+b}{\delta}}{\binom{a}{\delta}},$$

so Condition 2 of Theorem 5.3 is satisfied.

We approach a true generalization of Theorem 5.6 incrementally for readability. For deals satisfying $c = 1$, we have the following necessary condition for an equitable strategy to be perfectly δ-secure.

Theorem 5.8. *Suppose we have an equitable $(a, b, 1)$-strategy $\mathcal{A}$ that is perfectly δ-secure against Cathy. Then every announcement $\mathcal{A}_i \in \mathcal{A}$ is a $(\delta + 1)$-(n, a, λ_i)-design.*

Proof. We proceed by induction on δ. The base case ($\delta = 1$) is shown in Theorem 5.6.

Consider an announcement $\mathcal{A}_i \in \mathcal{A}$. For a subset $Y \subseteq X$, let λ_Y denote the number of hands of $\mathcal{A}_i$ that contain Y. We show $\mathcal{A}_i$ must be a $(\delta + 1)$-design as follows.

Suppose we have $Y \subseteq X$, where $|Y| = \delta + 1$. Pick an element $y \in Y$. Since $c = 1$, we have by Lemma 5.4 that $\{y\}$ is a possible hand for Cathy. Since $\mathcal{A}$ is equitable and perfectly δ-secure, we have (by Theorem 5.3)

$$|\{H_A \in \mathcal{P}(\{y\}, i) : Y \backslash \{y\} \subseteq H_A\}| = \frac{\binom{a}{\delta} \, |\mathcal{P}(\{y\}, i)|}{\binom{a+b}{\delta}}.$$

Moreover, since perfect δ-security implies perfect 1-security, $|\mathcal{P}(\{y\}, i)|$ is independent of y, as shown in the proof of Theorem 5.6. That is, the number of hands of $\mathcal{A}_i$ that contain the δ-subset $Y \backslash \{y\}$ but do not contain y is independent of the choice of Y and $y \in Y$, i.e. is some constant, say s.

Now, $\mathcal{A}$ must be perfectly $(\delta - 1)$-secure (since $\mathcal{A}$ is perfectly δ-secure), so by the inductive hypothesis, $\mathcal{A}_i$ is a δ-(n, a, λ_i')-design for some λ_i'. Therefore, the number of hands of $\mathcal{A}_i$ that contain the δ-subset $Y \backslash \{y\}$ is precisely λ_i'.

We have

$$\begin{aligned} \lambda_{Y \backslash \{y\}} &= \lambda_Y + \frac{\binom{a}{\delta} \, |\mathcal{P}(\{y\}, i)|}{\binom{a+b}{\delta}} \\ \iff \lambda_i' &= \lambda_Y + s. \end{aligned}$$

Therefore, λ_Y is some constant independent of Y, so every $(\delta + 1)$-subset occurs in a constant number of hands of $\mathcal{A}_i$, say λ_i. This implies $\mathcal{A}_i$ is a $(\delta + 1)$-(n, a, λ_i)-design, as desired.

We are now ready to give a combinatorial characterization of general (a, b, c)-strategies that are equitable and perfectly δ-secure for some $\delta \geq 1$. We give an inductive proof that relies on Theorem 5.8 as the base case.

Theorem 5.9. *Suppose we have an equitable (a, b, c)-strategy $\mathcal{A}$ that is perfectly δ-secure against Cathy. Then every announcement $\mathcal{A}_i \in \mathcal{A}$ is a $(c + \delta)$-(n, a, λ_i)-design.*

Proof. We proceed by induction on c. The base case $c = 1$ is shown in Theorem 5.8. Recall that for a strategy $\mathcal{A}$, an announcement $\mathcal{A}_i \in \mathcal{A}$, and a subset $Y \subseteq X$, we make the strategy $\mathcal{A}$ explicit in the notation $\mathcal{P}(Y, i)$ by writing $\mathcal{P}_{\mathcal{A}}(Y, i)$.

Let $y \in X$ and define $X' = X \backslash \{y\}$. Define an $(a, b, c-1)$-strategy $\mathcal{A}'$ by

$$\mathcal{A}' = \left\{ \mathcal{A}_i' : \mathcal{A}_i' = \mathcal{P}_{\mathcal{A}}(\{y\}, i), A_i \in \mathcal{A} \right\}.$$

We now show $\mathcal{A}'$ is perfectly δ-secure. Suppose Cathy holds a $(c-1)$-subset $Y \subseteq X'$ satisfying $\mathcal{P}_{\mathcal{A}'}(Y, i) \neq \emptyset$ for some $\mathcal{A}_i'$. In particular, note that if no such $\mathcal{A}_i'$ exists, then $\mathcal{A}'$ is trivially perfectly δ-secure.

Consider a δ-subset $Z \subseteq X' \backslash Y = X \backslash (Y \cup \{y\})$. We wish to count the number of hands in $\mathcal{P}_{\mathcal{A}'}(Y, i)$ that contain Z. Now, $\mathcal{P}_{\mathcal{A}'}(Y, i) = \mathcal{P}_{\mathcal{A}}(Y \cup \{y\}, i)$, so $\mathcal{P}_{\mathcal{A}}(Y \cup \{y\}, i) \neq \emptyset$ and hence

$Y \cup \{y\}$ is a possible hand for Cathy in the original strategy $\mathcal{A}$. Since $\mathcal{A}$ is perfectly δ-secure, we see that (by Theorem 5.3)

$$|\{H_A \in \mathcal{P}_{\mathcal{A}}(Y \cup \{y\}, i) : Z \subseteq H_A\}| = \frac{\binom{a}{\delta}\ |\mathcal{P}_{\mathcal{A}}(Y \cup \{y\}, i)|}{\binom{a+b}{\delta}},$$

which together with the fact that $\mathcal{P}_{\mathcal{A}'}(Y, i) = \mathcal{P}_{\mathcal{A}}(Y \cup \{y\}, i)$, immediately implies $\mathcal{A}'$ is perfectly δ-secure. Moreover, since $\mathcal{A}'$ is a perfectly δ-secure $(a, b, c-1)$-strategy, we have by the inductive hypothesis that every announcement $\mathcal{A}'_i \in \mathcal{A}'$ is a $(c-1+\delta)$-$(n-1, a, \lambda_i)$-design for some λ'_i (where λ'_i may depend on i).

That is, every $(c-1+\delta)$-subset of $X \backslash \{y\}$ occurs in λ'_i hands of $\mathcal{A}'_i = \mathcal{P}_{\mathcal{A}}(\{y\}, i)$. Since we chose y to be an arbitrary element of X, this implies $\mathcal{A}$ is a $(c-1+\delta)$-perfectly secure $(a, b+c-1, 1)$-strategy. Then the base case (Theorem 5.8) implies that every announcement $\mathcal{A}_i \in \mathcal{A}$ is a $(c+\delta)$-(n, a, λ_i)-design for some λ_i (where λ_i may depend on i), as desired.

Theorem 5.9 immediately implies the following bound on the security parameter δ for equitable strategies:

Corollary 5.10. *Suppose we have an equitable (a, b, c)-strategy $\mathcal{A}$ that is perfectly δ-secure against Cathy. Then $\delta \leq a - c$.*

Remark 5.11. If we have an equitable (a, b, c)-strategy $\mathcal{A}$ that is perfectly δ-secure against Cathy, where $\delta = a - c$, then each announcement $\mathcal{A}_i \in \mathcal{A}$ is an a-design. In fact, since every a-subset of X must appear a constant number of times in each $\mathcal{A}_i$, we see that each $\mathcal{A}_i$ is a *trivial a-design*. In this case, we see Alice's strategy is not informative for Bob.

Together, Theorem 5.7 and Theorem 5.9 show a direct correspondence between t-designs and equitable announcement strategies that are perfectly δ-secure for some δ satisfying $\delta \leq t - c$. We state this result in the following theorem for clarity.

Theorem 5.12. *A γ-equitable (a, b, c)-strategy $\mathcal{A}$ on card deck X that is perfectly δ-secure against Cathy is equivalent to a set of $(c+\delta)$-designs with point set X and block size a having the property that every a-subset of X occurs in precisely γ of these designs.*

6 Simultaneously Informative and Secure Strategies

In general, we want to find an (a, b, c)-strategy (for Alice) that is simultaneously informative for Bob and (perfectly or weakly) δ-secure against Cathy. We first consider informative strategies that provide security for individual cards and then consider informative strategies that provide security for multiple cards.

The following was first shown by Albert et al. [1]:

Theorem 6.1. *[1] 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.*

It is worth observing that a strategy that is not informative for Cathy implies, for any announcement $\mathcal{A}_i$ by Alice and possible hand $H_C \in \binom{X}{c}$ such that $\mathcal{P}(H_C, i) \neq \emptyset$, that $|\mathcal{P}(H_C, i)| \geq 2$. That is, there must exist distinct $H_A, H'_A \in \mathcal{P}(H_C, i)$. Following the same technique as in the proof of Lemma 4.1, this implies $|H_A \cap H'_A| \geq a - b$. If in addition the strategy is informative for Bob, by Lemma 4.1 we have $a - c > |H_A \cap H'_A| \geq a - b$, so $c < b$. This gives us the following result (which is also discussed by Albert et al. [1]):

Theorem 6.2. *If $c \geq b$, then there does not exist a strategy for Alice that is simultaneously informative for Bob and weakly* 1*-secure against Cathy.*

We now focus on $(3, n-4, 1)$-deals and examine the relationship between informative and perfectly 1-secure strategies and Steiner triple systems.

The following is an immediate consequence of Theorem 5.6 and Lemma 4.4.

Corollary 6.3. *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 a Steiner triple system.*

In fact, any $(a, b, a-2)$-strategy that is informative, equitable, and perfectly 1-secure also satisfies $c = 1$ (and hence $a = 3$). This result was first shown in Swanson and Stinson [27], but the proof provided here is greatly simplified.

Theorem 6.4. *Consider an (a, b, c)-deal such that $a - c = 2$. Suppose that Alice's strategy is equitable, informative for Bob, and perfectly 1-secure against Cathy. Then $a = 3$ and $c = 1$.*

Proof. Theorem 5.9 implies that every announcement is an $(a-1)$-design. Since $c \geq 1$, we have $a - 1 \geq a - c$, so we may apply Lemma 4.4. This implies $a - 1 = a - c$, so we have $c = 1$, as desired.

Our proof technique works for the generalizations of Theorem 6.4 and Corollary 6.3 shown in Swanson and Stinson [27] as well. That is, strategies that are equitable, informative for Bob, and perfectly $(a - c - 1)$-secure against Cathy must satisfy $c = 1$ and each announcement must be an $(a-1)$-$(n, a, 1)$-design, also known as a Steiner system $S(a-1, a, n)$.

Theorem 6.5. *Consider an (a, b, c)-deal. Suppose that Alice's strategy is equitable, informative for Bob, and perfectly $(a - c - 1)$-secure against Cathy. Then $c = 1$.*

Proof. The proof is identical to the proof of Theorem 6.4.

Corollary 6.6. *Consider an equitable $(a, b, 1)$-strategy that is informative for Bob and perfectly $(a-2)$-secure against Cathy. Then every announcement is a Steiner system $S(a-1, a, n)$.*

Proof. The fact that every announcement is an $(a-1)$-design follows immediately from Theorem 5.9. To see that $\lambda = 1$, we may apply Lemma 4.4. This is easy to see, however: since every $(a-1)$-subset occurs λ times, the fact that the strategy is informative for Bob implies $\lambda = 1$.

In fact, we can use Theorem 5.9 and Lemma 4.4 to derive the following bound on the security parameter δ for perfectly δ-secure and informative strategies, which helps put the above results in context.

Corollary 6.7. *Suppose we have an equitable (a, b, c)-strategy that is perfectly δ-secure against Cathy and informative for Bob. Then $\delta \leq a - 2c$.*

Proof. If the strategy is perfectly δ-secure, then by Theorem 5.9, every announcement is a $(c+\delta)$-design. Now, if $c + \delta < a - c$ holds, then $\delta < a - 2c$, as desired. If $c + \delta \geq a - c$, then since the strategy is informative for Bob, we can apply Lemma 4.4. This yields $c + \delta = a - c$, so we have $\delta = a - 2c$ in this case.

7 Construction methods and examples

Theorem 5.7 indicates that we can use t-designs to construct equitable strategies that are perfectly δ-secure against Cathy for $\delta = t - c$, where $c \leq t - 1$. In fact, so long as we use t-designs with $\lambda = 1$ and $c \leq a - t$, such a strategy will also be informative for Bob (Corollary 4.3). This is a very interesting result, as we can use a single "starting design" to obtain equitable strategies that are informative for Bob and perfectly δ-secure against Cathy. We give a general method for this next. First we require some definitions.

Definition 7.1. Suppose that $\mathcal{D} = (X, \mathcal{B})$ is a t-(v, k, λ)-design. An *automorphism* of $\mathcal{D}$ is a permutation π of X such that π fixes the multiset $\mathcal{B}$. We denote the collection of all automorphisms of $\mathcal{D}$ by $\mathsf{Aut}(\mathcal{D})$.

Remark 7.2. It is easy to see that $\mathsf{Aut}(\mathcal{D})$ is a subgroup of the symmetric group $S_{|X|}$.

Theorem 7.3. *Suppose $\mathcal{D} = (X, \mathcal{B})$ is a t-$(n, a, 1)$-design. Then there exists a γ-equitable $(a, n - a - c, c)$-strategy with m announcements that is informative for Bob and perfectly $(t - c)$-secure against Cathy for any choice of c such that $c \leq \min\{t - 1, a - t\}$, where $m = n!/|\mathsf{Aut}(\mathcal{D})|$ and $\gamma = m \Big/ \binom{n-t}{a-t}$.*

Proof. Let the symmetric group S_n act on $\mathcal{D}$. We obtain a set of designs isomorphic to $\mathcal{D}$, which are the announcements in our strategy. Since each announcement is a t-$(n, a, 1)$-design, the resulting scheme is perfectly $(t - c)$-secure against Cathy by Theorem 5.7. Furthermore, since $a - c \geq t$ and $\lambda = 1$, no two blocks have more than $a - c - 1$ points in common, so Theorem 4.1 implies the scheme is informative for Bob.

The total number of designs m is equal to $n!/|\mathsf{Aut}(\mathcal{D})|$ (as this is the index of $\mathsf{Aut}(\mathcal{D})$ in S_n). To see that $\gamma = m \Big/ \binom{n-t}{a-t}$, consider a fixed t-subset A of X. Then in particular, there are $\binom{n-t}{a-t}$ possible blocks of size a that contain A. Now, every one of the m designs contains exactly one of these $\binom{n-t}{a-t}$ blocks, and these $\binom{n-t}{a-t}$ blocks occur equally often among the m designs. Thus, a given block B occurs in $m \Big/ \binom{n-t}{a-t}$ of the designs, as desired.

Remark 7.4. Theorem 7.3 is a generalization of a result in Swanson and Stinson [27], in which the case $c = 1$ is treated.

Remark 7.5. The technique described in Theorem 7.3 shows how to use a single "starting design" $\mathcal{D}$ on n points to construct a strategy that inherits its properties from $\mathcal{D}$. That is, the strategy obtained by letting the symmetric group S_n act on $\mathcal{D}$ will be informative and perfectly δ-secure if $\mathcal{D}$ is an informative announcement that satisfies Condition 2 of Definition 5.1 for the fixed announcement $\mathcal{D}$.

We now discuss some other constructions of strategies using results from design theory, including some applications of Remark 7.5. All constructions discussed may be found in Colbourn and Dinitz [5].

It is clear that we can use any Steiner triple system, or 2-$(n, 3, 1)$-design, as a starting design to obtain an equitable $(3, n - 4, 1)$-strategy that is informative for Bob and perfectly 1-secure against Cathy. It is known that an STS(n) exists if and only if $n \equiv 1, 3 \bmod 6$, $n \geq 7$. We state this result in the following Corollary.

Corollary 7.6. *There exists an equitable* $(3, n-4, 1)$*-strategy for Alice that is informative for Bob and perfectly* 1*-secure against Cathy for any integer* n *such that* $n \equiv 1, 3 \bmod 6$*,* $n \geq 7$*.*

Similarly, *Steiner quadruple systems*, or 3-$(n, 4, 1)$-designs, exist if an only if $n \equiv 2, 4 \bmod 6$, which yields the following result:

Corollary 7.7. *There exists an equitable* $(4, n-5, 1)$*-strategy for Alice that is informative for Bob and perfectly* 1*-secure against Cathy for any integer* n *such that* $n \equiv 2, 4 \bmod 6$*.*

More generally, we can use any Steiner system $S(t, a, n)$ as a starting design to obtain an equitable $(a, n-a-c, c)$-strategy that is perfectly $(t-c)$-secure against Cathy for $c \leq \min\{t-1, a-t\}$. Known infinite families of $S(2, a, n)$ include *affine geometries*, *projective geometries*, *unitals*, and *Denniston designs* [5], which together give the following result:

Corollary 7.8. *Let* q *be a prime power and* $\ell \geq 2$*. There exist the following equitable strategies that are perfectly* 1*-secure against Cathy:*

1. *A* $(q, q^\ell - q - 1, 1)$*-strategy (constructed from affine geometries);*
2. *A* $(q+1, q^\ell + \cdots + q^2 - 1, 1)$*-strategy (constructed from projective geometries);*
3. *A* $(q+1, q^3 - q - 1, 1)$*-strategy (constructed from unitals); and*
4. *A* $(2^r, 2^{r+s} - 2^s - 1, 1)$*-strategy, for* $2 \leq r < s$ *(constructed from Denniston designs).*

In fact, we can use the same method to construct equitable (a, b, c)-strategies that are perfectly δ-secure against Cathy, informative for Bob, and *allow Cathy to hold more than one card*. Such a solution to the generalized Russian cards problem has not yet been presented in the literature. We next give an infinite class of equitable and perfectly 1-secure strategies where Cathy holds two cards.

Example 7.9. Consider the *inversive plane* with $q = 2^3$; this is a 3-$(65, 9, 1)$-design. The construction method in Theorem 7.3 yields an equitable $(9, 55, 1)$-strategy that is perfectly 2-secure against Cathy and informative for Bob and (more interestingly) a $(9, 54, 2)$-strategy that is perfectly 1-secure against Cathy and informative for Bob.

It is known that 3-$(q^2+1, q+1, 1)$-designs (or inversive planes) exist whenever q is a prime power. This gives us the following result.

Corollary 7.10. *There exists an equitable* $\big(q+1, q^2-q-2, 2\big)$*-strategy that is informative for Bob and perfectly* 1*-secure against Cathy and an equitable* $\big(q+1, q^2-q-1, 1\big)$*-strategy that is informative for Bob and perfectly* 2*-secure against Cathy, for every prime power* $q \geq 4$*.*

More generally, we can use *spherical geometries*, which are 3-$(q^n+1, q+1, 1)$-designs (or, equivalently, $S(3, q+1, q^n+1)$) for q a prime power and $n \geq 2$ to construct strategies allowing Cathy to hold two cards:

Corollary 7.11. *There exists an equitable* $(q+1, q^n-q-2, 2)$*-strategy that is informative for Bob and perfectly* 1*-secure against Cathy and an equitable* $(q+1, q^n-q-1, 1)$*-strategy that is informative for Bob and perfectly* 2*-secure against Cathy, for every prime power* q *and* $n \geq 2$*.*

Table 1. Perfectly $(t-c)$-secure strategies from Steiner t-designs for $t = 4, 5$

5-design	(a,b,c)-strategy	$5-c$	Derived 4-design	(a,b,c)-strategy	$4-c$
$S(5,8,24)$	$(8,15,1)$	4	$S(4,7,23)$	$(7,15,1)$	3
	$(8,14,2)$	3		$(7,14,2)$	2
	$(8,13,3)$	2		$(7,13,3)$	1
$S(5,7,28)$	$(7,20,1)$	4	$S(4,6,27)$	$(6,20,1)$	3
	$(7,19,2)$	3		$(6,19,2)$	2
$S(5,6,12)$	$(6,5,1)$	4	$S(4,5,11)$	$(5,5,1)$	3
$S(5,6,24)$	$(6,17,1)$	4	$S(4,5,23)$	$(5,17,1)$	3
$S(5,6,48)$	$(6,41,1)$	4	$S(4,5,47)$	$(5,41,1)$	3
$S(5,6,72)$	$(6,65,1)$	4	$S(4,5,71)$	$(5,65,1)$	3
$S(5,6,84)$	$(6,77,1)$	4	$S(4,5,83)$	$(5,77,1)$	3
$S(5,6,108)$	$(6,101,1)$	4	$S(4,5,107)$	$(5,101,1)$	3
$S(5,6,132)$	$(6,125,1)$	4	$S(4,5,131)$	$(5,125,1)$	3
$S(5,6,168)$	$(6,161,1)$	4	$S(4,5,167)$	$(5,161,1)$	3
$S(5,6,244)$	$(6,137,1)$	4	$S(4,5,243)$	$(5,137,1)$	3

However, only finitely many Steiner t-designs are known for $t > 3$ and none are known for $t > 5$. Table 1 lists strategies resulting from known Steiner 5- and 4-designs. All known $S(4,a,n)$ designs are *derived designs* from $S(5,a+1,n+1)$ designs, formed by choosing an element x, selecting all blocks containing x and then deleting x from these blocks.

We next discuss existence results for *optimal* strategies. As shown in Swanson and Stinson [27], the number of announcements m in an informative (a,b,c)-strategy must satisfy $m \geq \binom{n-a+c}{c}$. A strategy is *optimal* if $m = \binom{n-a+c}{c}$. The following result by Swanson and Stinson [27] follows immediately from the existence of large sets of Steiner triples, discussed in Remark 2.13, and Lemma 5.5.

Theorem 7.12. *[27] 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.*

Example 7.13. Consider the large set of STS(9) from Example 2.14. This set of announcements is an optimal $(3,5,1)$ strategy that is perfectly 1-secure against Cathy and informative for Bob.

As discussed in Theorem 7.12, if we can construct a large set of 2-$(n,3,1)$-designs, this set forms an optimal strategy that is informative and perfectly 1-secure, and a large set of STS(n) exists whenever $n \equiv 1, 3 \bmod 6$ and $n > 7$. However, there are certain choices of n for which there is a particularly nice construction for a large set of STS(n), such that it would be easy for Alice and Bob to create this large set on their own. We forego the details of this construction, which is due to Schreiber [24], but remark that this construction method applies whenever each prime divisor p of $n-2$ has the property that the order of (-2) modulo p is congruent to 2 modulo 4.

Two other types of designs that can be used to construct informative and perfectly 1-secure strategies where Cathy holds one card are *hyperplanes* in projective spaces and *Hadamard designs*. For a discussion of these constructions, we refer the reader to Stinson [25]. We have the following results.

Corollary 7.14. *There exists an equitable $\left(\frac{q^d-1}{q-1}, q^d-1, 1\right)$-strategy that is informative for Bob and perfectly 1-secure against Cathy, where $q \geq 2$ is a prime power and $d \geq 2$ is an integer.*

Proof. It is known that there exists a symmetric $\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$-BIBD $\mathcal{D}$ for every prime power $q \geq 2$ and integer $d \geq 2$. The design $\mathcal{D}$ is a hyperplane in a projective space (or, in the case $d = 2$, a finite projective plane). Let the symmetric group S_n act on $\mathcal{D}$ as in the proof of Theorem 7.3, where $n = (q^{d+1} - 1)/(q - 1)$, to obtain Alice's strategy.

Lemma 5.5 immediately implies that this strategy is perfectly 1-secure against Cathy. To see that this strategy is informative, recall that the intersection of two blocks in a symmetric BIBD has size $\lambda = (q^{d-1} - 1)/(q - 1)$. It is easy to see that the strategy will be informative provided $a - c > \lambda$, which is the case here.

Corollary 7.15. *There exists an equitable* $\left(\frac{q-1}{2}, \frac{q-1}{2}, 1\right)$*-strategy that is informative for Bob and perfectly* 1*-secure against Cathy, where* $q \equiv 3 \bmod 4$ *is an odd prime power.*

Proof. It is known that there exists a symmetric $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$-BIBD $\mathcal{D}$ for every odd prime power q such that $q \equiv 3 \bmod 4$. The design $\mathcal{D}$ is a Hadamard design. Let the symmetric group S_q act on $\mathcal{D}$ as in the proof of Theorem 7.3 to obtain Alice's strategy.

Lemma 5.5 immediately implies that this strategy is perfectly 1-secure against Cathy. To see that this strategy is informative, recall that the intersection of two blocks in a symmetric BIBD has size $\lambda = (q - 3)/4$. It is easy to see that the strategy will be informative provided $a - c > \lambda$, which is the case here.

Remark 7.16. Any symmetric BIBD may be used to construct equitable strategies that are perfectly 1-secure against Cathy for $c = 1$. If $\mathcal{D}$ is a symmetric 2-(n, a, λ)-design, the *order* of $\mathcal{D}$ is $a - \lambda$. The block intersection property we need to guarantee that the strategy is informative is that the order is greater than 1, which will always be the case. Colbourn and Dinitz [5] list known families of symmetric BIBDs.

7.1 Cordón-Franco et al. Geometric Protocol

Cordón-Franco et al. [8] present a geometric protocol based on hyperplanes that yields informative and weakly δ-secure equitable (a, b, c)-strategies for arbitrary $c, \delta > 0$ and appropriate parameters a and b. The geometric protocol is stated as follows.

Protocol 1 (Geometric Protocol [8]) *Let p be a prime power and let d and $s < p$ be positive integers. Let X be a deck of p^{d+1} cards and suppose we have an (a, b, c)-deal such that $a = sp^d$. Given a hand $H_A \in \binom{X}{a}$, the set of possible announcements for Alice is the set of bijections from X to $\mathrm{AG}_{d+1}(p)$ satisfying the condition that H_A maps to the union of s parallel hyperplanes in $\mathrm{AG}_{d+1}(p)$. For every $H_A \in \binom{X}{a}$, assume Alice picks uniformly at random from the set of possible bijections.*

In particular, the geometric protocol defines an equitable strategy in which Cathy may hold more than one card. We analyze when the geometric protocol achieves perfect, rather than weak, security, whereas Cordón-Franco et al. [8] show that the general case achieves weak s-security for a card deck of size p^{d+1}, where $a = sp^d$, if $c < sp^d - s^2p^{d-1}$ and $\max\{c + s, cs\} \leq p$.

We translate the geometric protocol into our model in the next observation.

Observation 7.17 *Let $\mathcal{A}$ be the strategy defined by the geometric protocol. An announcement $\mathcal{A}_i \in \mathcal{A}$ is equivalent to the set of all possible unions of s parallel hyperplanes. In particular, there are $\binom{p}{s}(p^{d+1} - 1)/(p - 1)$ possible hands for Alice in each $\mathcal{A}_i$.*

We first consider general results from design theory with respect to the above construction. Let us view X as the set of points in $\mathrm{AG}_{d+1}(p)$, and let $\mathcal{B}$ be denote the set of all hyperplanes in $\mathrm{AG}_{d+1}(p)$. It is well-known that $(X, \mathcal{B})$ is a resolvable $\big(p^{d+1}, p^d, \lambda\big)$-BIBD, where $\lambda = (p^d - 1)/(p - 1)$. Moreover, each point has degree $r = (p^{d+1} - 1)/(p - 1)$, and there are r equivalance classes of parallel hyperplanes, each of size p. Let $\Pi_1, \ldots, \Pi_r$ denote these equivalence classes. Note that in each such equivalence class, every point of $\mathbb{F}_p^{d+1}$ occurs exactly once.

Define the design $(X, \mathcal{C})$ by forming a collection of all possible unions of s parallel hyperplanes. Stated formally, for $1 \le i \le r$, define B_i to be the collection of all s-subsets of the parallel class Π_i, and define $\mathcal{C}$ to be the union of the B_i over the parallel classes. That is,

$$B_i = \{C \subseteq \Pi_i : |C| = s\} \text{ and } \mathcal{C} = \bigcup_{i=1}^{r} B_i.$$

Then $(X, \mathcal{C})$ is a $\big(p^{d+1}, sp^d, \lambda'\big)$-BIBD, where $\lambda' = \binom{p-1}{s-1}\frac{sp^d-1}{p-1}$. The above discussion immediately implies the following observation:

Observation 7.18 *Let p be a prime power and let $d \ge 1$ be a positive integer. Let X be a deck of p^{d+1} cards and fix an (a, b, c)-deal with $a = sp^d$. Then in the strategy $\mathcal{A}$ defined by the geometric protocol, each announcement $\mathcal{A}_i$ is a 2-$\big(p^{d+1}, sp^d, \lambda\big)$-design, where $\lambda = \binom{p-1}{s-1}\frac{sp^d-1}{p-1}$.*

Observation 7.18 and Theorem 5.7 imply that the Geometric Protocol achieves perfect 1-security when Cathy holds one card, i.e., for $(sp^d, p^{d+1} - sp^d - 1, 1)$-deals where p is a prime power and $s < p$.

Moreover, as shown by Stinson et al. [26], the design $(X, \mathcal{C})$ is a 3-design precisely when $p = 2s$, so p must be an even prime power. In this case, $(X, \mathcal{C})$ is a 3-$\big(p^{d+1}, p^{d+1}/2, \lambda''\big)$-design, where

$$\lambda'' = \binom{p-1}{p/2-1}\frac{p^{d+1} - 4}{4(p-1)}.$$

That is, for card decks and deals satisfying certain parameters, the strategy defined by the geometric protocol is a 3-design. This implies that we can sometimes achieve perfect 2-security for deals in which Cathy holds one card, or perfect 1-security for deals in which Cathy holds two cards. We state the result in the following theorem for clarity.

Theorem 7.19. *Let p be a prime power and let $d \ge 1$ be a positive integer. Let X be a deck of p^{d+1} cards and fix an (a, b, c)-deal with $a = sp^d$. Then in the strategy $\mathcal{A}$ defined by the geometric protocol, each announcement $\mathcal{A}_i$ is a 3-design if and only if $p = 2^\ell$ for some positive integer ℓ and $s = 2^{\ell-1}$.*

8 A Variant of the Russian Cards Problem

In this section, we consider a variation of the generalized Russian cards problem, in which we change the manner in which the cards are dealt. Our motivation for restricting the deal is to widen the solution space. Since the generalized Russian cards problem requires a suitable set of t-designs to maximize security against Cathy—and constructing t-designs for $t > 2$ is in general quite difficult—we explore certain types of deals where suitable constructions are more readily available. An added

advantage of our deal restriction is that in this new framework, we can view Alice's hand as an a-tuple over an alphabet of size v. If Alice's hand represents a secret key, this variation is more in keeping with traditional key agreement schemes in cryptography, as typically secret keys are tuples rather than sets.

Suppose our deck X consists of $n = va$ cards, where v and a are positive integers such that $v > a$. Rather than allowing Alice, Bob, and Cathy to have any hand of the appropriate size, we first split the deck X into a piles, each of size v. Alice is given a hand H_A of a cards, such that she holds exactly one card from each pile. Cathy's hand H_C of c cards is assumed to contain no more than one card from each pile. The remainder of the deck becomes Bob's hand, H_B. Observe that we can use the same framework for this problem as for the original; we have only placed a limitation on the set of possible hands Alice, Bob, and Cathy might hold. The necessary modifications to the security definitions and the definition of an informative strategy are straightforward.

This variant admits a nice solution using *transversal designs*; we refer the reader to Section 2.2 for the relevant definitions and a discussion of these designs. In the context of a transversal design $\mathrm{TD}_\lambda(t, a, v)$, we can view the piles of cards as the groups $G_1, \ldots, G_a$ of the design. In this case, Alice's hand is a transversal and Cathy's hand is a partial transversal of $G_1, \ldots, G_a$. Note that Cathy therefore only considers transversals as possible hands for Alice. When we discuss weak (or perfect) δ-security, we are interested in the probability (from Cathy's point of view) that Alice holds partial transversals of order δ.

We first show Theorem 4.1 holds for this variant of the Russian cards problem:

Theorem 8.1. *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 $|H_A \cap H'_A| \geq a - c$. We proceed by constructing a card deal consistent with the announcement $\mathcal{A}_i$ such that $\{H_A, H'_A\} \subseteq \mathcal{P}(H_B, i)$, which implies the announcement is not informative for Bob.

Write $|H_A \cap H'_A| = \ell$. Let Alice's hand be H_A, so it is possible for Alice to announce $\mathcal{A}_i$. Let Cathy's hand contain all the cards in H'_A that are not also contained in H_A; this is possible since $c \geq a - \ell$. Then Bob's hand H_B contains all the remaining cards. In particular, we have $H_B \cap (H_A \cup H'_A) = \emptyset$, so $\{H_A, H'_A\} \subseteq \mathcal{P}(H_B, i)$, as desired.

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 $|H_A \cap H'_A| \geq a - c$.

In light of Theorem 8.1, the following result is straightforward.

Theorem 8.2. *Consider an (a, b, c)-deal following the above rules and suppose that each announcement in an equitable (a, b, c)-strategy is a $\mathrm{TD}_1(t, a, v)$ satisfying $t \leq a - c$. Then the strategy is informative for Bob.*

We can use an argument similar to that of Swanson and Stinson [27] to derive a lower bound on the size of Alice's announcement.

Theorem 8.3. *Suppose $a > c$ and there exists a strategy for Alice that is informative for Bob. Then the number of announcements m satisfies $m \geq v^c$.*

Proof. Fix a set of cards X' of size $a - c$, no two of which are from the same pile. There are v^c possible hands for Alice that contain X'. These hands must occur in different announcements, by Theorem 4.1 (which holds for this variation of the problem). Therefore $m \geq v^c$.

As before, we refer to a strategy that meets this bound as *optimal*. We have the following result.

Theorem 8.4. *Suppose that $a > c$. An optimal (a, b, c)-strategy for Alice that is informative for Bob is equivalent to a large set of $\mathrm{TD}_1(t, a, v)$, where $t = a - c$.*

Proof. Suppose there exists a large set of $\mathrm{TD}_1(a - c, a, v)$. Recall from Definition 2.20 that the set of all blocks sets (i.e., possible announcements) in this large set form a partition of the set of all transversals and that there are precisely v^c designs in such a set. Then it is easy to see that this immediately yields an optimal (a, b, c)-strategy for Alice that is informative for Bob.

Conversely, suppose there is an optimal (a, b, c)-strategy for Alice that is informative for Bob. We need to show that every announcement is a $\mathrm{TD}_1(a - c, a, v)$. As in the proof of Theorem 8.3, fix a set of cards X' of size $a - c$, no two of which are from the same pile. The v^c possible hands for Alice that contain X' must occur in different announcements. However, there are a total of v^c announcements, so every announcement must contain exactly one block that contains X'.

The following result shows how transversal designs with arbitrary t can be used to achieve weak δ-security for permissible parameters $\delta \leq t - c$. As in Definition 2.17, for a transversal design $\mathrm{TD}_\lambda(t, a, v)$, say $(X, \mathcal{G}, \mathcal{B})$, and a partial transversal Y of $\mathcal{G}$, we let G_Y denote the set of groups of the transversal design that have nonempty intersection with the partial transversal Y.

Theorem 8.5. *Consider an (a, b, c)-deal following the above rules and suppose that each announcement in an equitable (a, b, c)-strategy is a $\mathrm{TD}_\lambda(t, a, v)$, where $c \leq t - 1$. Then the strategy is weakly $(t - c)$-secure against Cathy.*

Proof. Fix an announcement $\mathcal{A}_i$ for Alice. Suppose $\mathcal{A}_i$ is a $\mathrm{TD}_\lambda(t, a, v)$, say $(X, \mathcal{G}, \mathcal{B})$. Consider a possible hand H_C for Cathy. In particular, H_C is a partial transversal of the groups $G_1, \ldots, G_a \in \mathcal{G}$.

Since $c \leq t$, Theorem 2.19 implies there are

$$|\mathcal{P}(H_C, i)| = \lambda v^{t-c}(v-1)^c$$

blocks in $\mathcal{A}_i$ that do not contain any of the points of H_C.

Consider a partial transversal Y of order $\delta \leq t - c$. Since Y is not necessarily group disjoint from H_C, we must consider the number of groups which intersect both Y and H_C. In particular, the δ-subset Y never occurs with any other cards from $G_Y \cap G_{H_C}$, by definition of transversal designs.

Let $\ell = |G_{H_C} \backslash G_Y|$. That is, ℓ is the number of groups that do not intersect Y, but from which Cathy has cards. Write $z_1, \ldots, z_\ell$ for Cathy's cards from these ℓ groups. We wish to compute the number of blocks which contain all the points in Y but miss all of the points of H_C. This is the same as the number of blocks that contain all the points in Y but miss all the points in $\{z_1, \ldots, z_\ell\}$. Since $\ell + \delta \leq t$, by Theorem 2.19, we have $\lambda v^{t-\ell-\delta}(v-1)^\ell$ such blocks.

That is, a given set of points $x_1, \ldots, x_\delta \in X \backslash H_C$ that might be held by Alice is contained in precisely

$$|\{H_A \in \mathcal{P}(H_C, i) : x_1, \ldots, x_\delta \in H_A\}| = \lambda v^{t-\ell-\delta}(v-1)^\ell$$

of the blocks in $\mathcal{P}(H_C, i)$, where $\ell = \left|G_{H_C} \backslash G_{\{x_1,\ldots,x_\delta\}}\right|$.

Thus, for any partial transversal of δ distinct points $x_1, \ldots, x_\delta \in X \backslash H_C$, we have

$$\frac{|\{H_A \in \mathcal{P}(H_C, i) : x_1, \ldots, x_\delta \in H_A\}|}{|\mathcal{P}(H_C, i)|} = \frac{\lambda v^{t-\ell-\delta}(v-1)^\ell}{\lambda v^{t-c}(v-1)^c} = \frac{1}{v^{\delta+\ell-c}(v-1)^{c-\ell}},$$

so Condition 1 of Theorem 5.3 is satisfied.

Remark 8.6. We do not achieve perfect $(t-c)$-security in Theorem 8.5 because the number of hands of $\mathcal{P}(H_C, i)$ containing a given partial transversal Y of δ distinct points, where $\delta \leq t-c$, depends on $\ell = |G_{H_C} \backslash G_Y|$. In fact, we cannot expect to achieve better security than that of the construction given in Theorem 8.5 for this variant of the generalized Russian cards problem. This is because the rules for the deal imply that for each pile from which Cathy holds a card, Cathy knows that Alice holds one of the other $(v-1)$ cards, and for every other pile, Cathy knows only that Alice holds one of the other v cards.

As discussed in Section 2.2, large sets of transversal designs $\mathrm{TD}_\lambda(t,k,v)$ are easy to construct when you have a linear $\mathrm{TD}_\lambda(t,k,v)$ "starting design". As stated in Theorem 2.29, a linear $\mathrm{TD}_1(t,q,q)$ exists whenever the point set $X = (\mathbb{F}_q)^2$ and q is a prime power. The construction method for such a transversal design is simple; we refer the reader to the relevant discussion in Section 2.2 on Theorem 2.28 and Corollaries 2.29 and 2.30.

In particular, we can construct a linear $\mathrm{TD}_1(t,a,q)$ for a prime power $q \geq a$ by first constructing a $\mathrm{TD}_1(t,q,q)$ and then (if necessary) deleting $q-a$ groups. This yields a wide range of informative and weakly $(t-c)$-secure $(a, n-a-c, c)$-strategies for card decks of size $n = aq$ and any choice of c satisfying $c \leq \min\{t-1, a-t\}$. If we take $t = a-c$, these strategies are optimal. We summarize this result in the following theorem.

Theorem 8.7. *Consider the above variant of the generalized Russian cards problem. Let q be a prime power such that $q \geq a$ and $c \leq \frac{a-1}{2}$. Then there exists an equitable $(a, aq-a-c, c)$-strategy that is optimal, informative for Bob, and weakly $(a-2c)$-secure against Cathy.*

9 Discussion and Comparison with Related Work

The Russian cards problem and variants of it has received a fair amount of attention in the literature, with focus ranging from possible applications to key generation [2,3,15–19,21,23], to analyses based on epistemic logic [9–12], to card deals with more than three players [14,20]. Of more relevance to our work is the recent research that takes a combinatorial approach [1–4,6,27], on which we now focus.

Many useful results concerning parameter bounds and announcement sizes for weak 1-security, some of which we use in this paper, are given by Albert et al. [1]. Albert et al. [2,3] and Cordón-Franco et al. [6] discuss protocols for card deals of a particular form that achieve weak 1-security, using card sums modulo an appropriate parameter for announcements. Atkinson et al. [4] is the only work of which we are aware that treats security notions stronger than weak 1-security, other than work by Swanson and Stinson [27] and subsequent work by Cordón-Franco et al. [8].

In addition, there has been recent work [7,13] in which protocols consisting of more than one announcement by Alice and Bob are considered, which is a generalization of the problem which we consider here. van Ditmarsch and Soler-Toscano [13] show that no good announcement exists for card deals of the form $(4,4,2)$ using bounds from Albert et al. [1]. The authors instead give an interactive protocol that requires at least three rounds of communication in order for Alice and Bob to learn each other's hands; their protocol uses combinatorial designs to determine the initial announcement by Alice and the protocol analysis is done using epistemic logic.

Cordón-Franco et al. [7] consider four-step solutions for the generalized Russian cards problem with parameters (a,b,c) such that $c > a$. Although Cordón-Franco et al. [7] present a "protocol", their solution is not a protocol in the typical sense of the word, as it is unclear if the protocol

is executable or not. The authors demonstrate the existence of a necessary construction for their protocol when the card deal parameters satisfy specific conditions, but do not address the feasibility of finding such constructions in practice. In particular, the security of the protocol itself relies heavily on the ability of the players to pick such a construction uniformly at random from all possible constructions. Since it is unclear if this is feasible, the protocol is questionable, albeit theoretically interesting in that it attempts to treat cases where $c > a$.

In this paper, we build extensively on results by Swanson and Stinson [27]. In particular, we greatly simplify the proofs for results connecting certain types of perfectly δ-secure deals and Steiner systems, originally shown in Swanson and Stinson [27]. The construction technique using a "starting design", given in Theorem 7.3 is a generalization of the technique given by Swanson and Stinson [27]. This generalized construction technique allows us to answer in the affirmative the question on the existence of perfectly secure and informative strategies for deals in which Cathy holds more than one card.

Cordón-Franco et al. [8] further elaborate on protocols of length two and the notion of weak δ-security. The authors present a geometric protocol, discussed in Section 7.1, based on hyperplanes that yields informative and weakly δ-secure equitable (a, b, c)-strategies for appropriate parameters. In particular, this protocol allows Cathy to hold more than one card. In certain card deals, this protocol achieves perfect δ-security for δ equal to one or two. We remark that with the exception of Section 7.1, our results were completed independently of Cordón-Franco et al. [8].

10 Concluding Remarks and Future Work

We give a characterization for solutions to the generalized Russian cards problem that are perfectly δ-secure. That is, we show an equivalence between a γ-equitable strategy that is perfectly δ-secure for some δ and a set of $(c + \delta)$-designs on n points with block size a, where this set must satisfy the additional property that every a-subset of X occurs in precisely γ of these designs.

Building on the results of Swanson and Stinson [27], we show how to use a "starting" t-$(n, a, 1)$-design to construct equitable (a, b, c)-strategies that are informative and perfectly $(t - c)$-secure against Cathy for any choice of c satisfying $c \leq \min\{t - 1, a - t\}$. In particular, this indicates that if an appropriate t-design exists, it is possible to achieve perfect security for deals where Cathy holds more than one card. We present an example construction, based on inversive planes, for $(q + 1, q^2 - q - 2, 2)$-strategies which are perfectly 1-secure against Cathy and informative for Bob, where q is a prime power. We also analyze the security properties of Cordón-Franco et al.'s [8] geometric protocol, remarking that this protocol yields a nice construction for a 3-design for certain parameters.

In addition, we discuss a variation of the Russian cards problem which admits nice solutions using transversal designs. The variant changes the manner in which the cards are dealt, but the resulting problem can be solved using large sets of transversal designs with $\lambda = 1$ and arbitrary t, which are easy to construct. In particular, this solution is optimal in terms of the number of announcements and provides the strongest possible security for appropriate parameters. That is, for card decks of size aq, where $q \geq a$ is a prime power, we achieve $(a, aq - a - c, c)$-strategies that are optimal, informative for Bob, and weakly $(a - 2c)$-secure against Cathy for $c \leq \frac{a-1}{2}$.

There are many open problems in the area, especially for deals with $c > 1$. Given the general difficulty of constructing t-designs for $t > 2$ and $\lambda = 1$, we see that constructing perfectly δ-secure and informative strategies for $c > 1$ is a difficult combinatorial problem. A more promising direction

for the case $c > 1$ may be strategies that are weakly δ-secure for $\delta > 1$, a concept first introduced by Swanson and Stinson [27], which has received some attention in current literature [8]. In particular, further characterizing such strategies using combinatorial notions might prove informative.

References

1. Albert, M.H., Atkinson, M.D., van Ditmarsch, H.P., Handley, C., Aldred, R.E.L.: Safe communication for card players by combinatorial designs for two-step protocols. Australasian Journal of Combinatorics 33, 33–46 (2005)
2. Albert, M.H., Cordón-Franco, A., van Ditmarsch, H.P., Fernández-Duque, D., Joosten, J.J., Soler-Toscano, F.: Secure communication of local states in multi-agent systems. http://personal.us.es/hvd/newpubs/fLiSsecretl.pdf (2010), extended version of [3]
3. Albert, M.H., Cordón-Franco, A., van Ditmarsch, H.P., Fernández-Duque, D., Joosten, J.J., Soler-Toscano, F.: Secure communication of local states in interpreted systems. In: Abraham, A., Corchado, J.M., Rodríguez-González, S., Santana, J.F.D.P. (eds.) Distributed Computing and Artificial Intelligence (DCAI 2011). Advances in Soft Computing, vol. 91, pp. 117–124. Springer (2011)
4. Atkinson, M.D., van Ditmarsch, H.P., Roehling, S.: Avoiding bias in cards cryptography. Australasian Journal of Combinatorics 44, 3–18 (2009)
5. Colbourn, C.J., Dinitz, J.H.: The CRC Handbook of Combinatorial Designs. Chapman & Hall/CRC, 2nd edn. (2006)
6. Cordón-Franco, A., van Ditmarsch, H.P., Fernández-Duque, D., Joosten, J.J., Soler-Toscano, F.: A secure additive protocol for card players. Australasian Journal of Combinatorics 54, 163–176 (2012)
7. Cordón-Franco, A., van Ditmarsch, H.P., Fernández-Duque, D., Soler-Toscano, F.: A colouring protocol for the generalized Russian cards problem. CoRR abs/1207.5216 (2013)
8. Cordn-Franco, A., Ditmarsch, H., Fernndez-Duque, D., Soler-Toscano, F.: A geometric protocol for cryptography with cards. Designs, Codes and Cryptography pp. 1–13 (2013), http://dx.doi.org/10.1007/s10623-013-9855-y
9. Cyriac, A., Krishnan, K.M.: Lower bound for the communication complexity of the Russian cards problem. CoRR abs/0805.1974 (2008)
10. van Ditmarsch, H.P., van der Hoek, W., van der Meyden, R., Ruan, J.: Model checking Russian cards. Electronic Notes in Theoretical Computer Science 149(2), 105–123 (2006)
11. van Ditmarsch, H.P.: The Russian cards problem. Studia Logica 75(1), 31–62 (2003)
12. van Ditmarsch, H.P.: The case of the hidden hand. Journal of Applied Non-Classical Logics 15(4), 437–452 (2005)
13. van Ditmarsch, H.P., Soler-Toscano, F.: Three steps. In: Leite, J., Torroni, P., Ågotnes, T., Boella, G., van der Torre, L. (eds.) Computational Logic in Multi-Agent Systems (CLIMA XII). Lecture Notes in Computer Science, vol. 6814, pp. 41–57. Springer (2011)
14. Duan, Z., Yang, C.: Unconditional secure communication: a Russian cards protocol. Journal of Combinatorial Optimization 19, 501–530 (2010)
15. Fischer, M.J., Paterson, M.S., Rackoff, C.: Secret bit transmission using a random deal of cards. In: Discrete Mathematics and Theoretical Computer Science. DIMACS, vol. 2, pp. 173–181. American Mathematical Society (1991)
16. Fischer, M.J., Wright, R.N.: Multiparty secret key exchange using a random deal of cards. In: Feigenbaum, J. (ed.) Advances in Cryptology – CRYPTO '91. Lecture Notes in Computer Science, vol. 576, pp. 141–155. Springer (1991)
17. Fischer, M.J., Wright, R.N.: An application of game theoretic techniques to cryptography. In: Discrete Mathematics and Theoretical Computer Science. DIMACS, vol. 13, pp. 99–118. American Mathematical Society (1993)
18. Fischer, M.J., Wright, R.N.: An efficient protocol for unconditionally secure secret key exchange. In: ACM-SIAM Symposium on Discrete algorithms (SODA '93). pp. 475–483. Society for Industrial and Applied Mathematics (1993)
19. Fischer, M.J., Wright, R.N.: Bounds on secret key exchange using a random deal of cards. Journal of Cryptology 9(2), 71–99 (1996)
20. He, J., Duan, Z.: Public communication based on Russian cards protocol: A case study. In: Wang, W., Zhu, X., Du, D.Z. (eds.) Combinatorial Optimization and Applications (COCOA 2011). Lecture Notes in Computer Science, vol. 6831, pp. 192–206. Springer (2011)
21. Koizumi, K., Mizuki, T., Nishizeki, T.: Necessary and sufficient numbers of cards for the transformation protocol. In: Chwa, K.Y., Munro, J.I. (eds.) Computing and Combinatorics (COCOON 2004). Lecture Notes in Computer Science, vol. 3106, pp. 92–101. Springer (2004)

22. Mathon, R., Street, A.P.: Partitions of sets of designs on seven, eight and nine points. Journal of Statistical Planning and Inference 58(1), 135–150 (1997)
23. Mizuki, T., Shizuya, H., Nishizeki, T.: A complete characterization of a family of key exchange protocols. International Journal of Information Security 1(2), 131–142 (2002)
24. Schreiber, S.: Covering all triples on n marks by disjoint steiner systems. Journal of Combinatorial Theory, Series A 15(3), 347–350 (1973)
25. Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer-Verlag (2003)
26. Stinson, D.R., Swanson, C.M., van Trung, T.: A new look at an old construction: constructing (simple) 3-designs from resolvable 2-designs. CoRR abs/1207.5216 (2013)
27. Swanson, C.M., Stinson, D.R.: Combinatorial solutions providing improved security for the generalized Russian cards problem. Designs, Codes and Cryptography pp. 1–23 (2012)
28. Swanson, C.M.: Unconditionally Secure Cryptography: Signature Schemes, User-Private Information Retrieval, and the Generalized Russian Cards Problem. Ph.D. thesis, University of Waterloo (2013)