AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **80(1)** (2021), Pages 1–29

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

Hans van Ditmarsch*

LORIA, CNRS
University of Lorraine, France
hans.van-ditmarsch@loria.fr

David Fernández Duque

Department of Mathematics
Ghent University, Belgium
David.FernandezDuque@UGent.be

Vaishnavi Sundararajan†

University of California
Santa Cruz, U.S.A.
vasundar@ucsc.edu

S. P. Suresh‡

Chennai Mathematical Institute
Chennai, India
spsuresh@cmi.ac.in

Abstract

In the Russian cards problem, a group of communicating agents and an eavesdropper, Eve, draw cards from a deck. The agents then wish

* This work was partially carried out while Hans van Ditmarsch was affiliated to Institute of Mathematical Sciences and to CNRS UMI 2000 ReLaX, Chennai, India.

† This work was carried out while Vaishnavi Sundararajan was affiliated to the Chennai Mathematical Institute and to CNRS UMI 2000 ReLaX, Chennai, India, and was partially supported by a grant from the Infosys Foundation and a TCS Research Fellowship.

‡ Partially supported by a grant from the Infosys Foundation. Also at CNRS UMI 2000 ReLaX, Chennai, India.

ISSN: 2202-3518

to inform each other about their hand without Eve learning any 'protected' information, typically in the sense of weak possibilistic security. We consider a weakening of this original problem, whereby the cards are linearly ordered by value. The agents wish to know the value of the best card held between them, without Eve knowing who holds said card. We consider standard solutions to the problem based on combinatorial designs, as well as novel solutions based on secret-bit-exchange protocols. Our results show that this version of the problem can be solved in many instances where the size of each agent's hand is linear on that of the eavesdropper's.

1 Introduction

The *Russian cards problem* is a combinatorial puzzle dating back to Kirkman [10], whereby two card-holding players try to communicate information about their hands without another player learning any 'protected' information. All cards are distributed over the players, players can only see their own cards, and they know what cards are in the deck and how many cards each player has drawn. Typically, Alice and Bob wish to inform each other their *entire* hand, without Eve learning who holds *any* card that is not hers. This version of the problem has been extensively studied [1, 3, 16, 17, 18]; we will refer to it as the *all-card Russian cards problem.* More generally, we can consider a case where there are m communicating agents and an eavesdropper [5, 6].

However, it may be the case that Alice and Bob do not need to know the entire deal. Consider a scenario where different cards hold different value; we may number the cards so that 0 is the most valuable, then 1, and so on. In such a context, it may suffice for Alice and Bob to know the value of the best card they hold between them, without Eve learning who holds this card. Meanwhile, it is unimportant if Eve learns who holds the 'worse' cards, or for Alice and Bob to learn them for that matter.

Essentially, Alice and Bob must employ a form of cryptography using their hands and their knowledge about the deck. Cryptography with decks of cards has been investigated in various ways since the 1980s, motivated, for example, by the formalization of bidding in bridge [20]. Since then, card-based protocols have been used for secret-bit exchange [7, 9], in which the players secretly learn one or more secret bits (where a bit typically represents the ownership of a particular card that is held between the communicating players), but do not necessarily learn the entire deal. Card-based protocols have also been studied in the otherwise unrelated context of binary computations [11, 13, 14, 15]. The cryptographic algorithm Solitaire (https://www.schneier.com/academic/solitaire/) uses a deck of cards wherein cards are sequentially numbered (valued), and where the deck is randomly shuffled, as in our case. However, there are no better or worse cards; the values only play a role in the encryption. We are unaware of any prior research on protocols wherein the

communicating players are only required to learn their best card. It seems a natural intermediate condition between the all-card problem and secret-bit exchange: if the communicating players (but not the eavesdropper) know all cards, then they know what the best card is, and if they know what the best card is, then they share at least one secret bit.

In intuitive terms, the *best-card Russian cards problem* can be defined as follows:

> *A group of m agents, with m at least 2, and Eve each draw cards from a publicly known deck. The cards in the deck are linearly ordered by value, and the agents wish to communicate in order to know the value of the best card between them, without Eve learning which of them holds this card. However, the agents in the group share no private information, and Eve, who has unlimited computational capacity, can intercept all communications between them. Can the group of agents achieve this?*

As we have mentioned, this is a weakening of the *all-card Russian cards problem,* where the agents wish to inform each other their *entire* hand (and hence the whole deal) without Eve learning which of them holds *any* card, aside from those in her possession. For notational convenience we may identify the deck with the set $\Omega = [0, d)$ of natural numbers, where d is the number of cards. (We use interval notation for natural numbers, such that $[i, j) = \{k \in \mathbb{N}, i \leq k < j\}$, etc.)

Two-step protocols

In the two-agent case, classical solutions to the all-card problem typically consist of two-step protocols (i.e., each of Alice and Bob successively makes one announcement) often based on combinatorial designs [1], with three- [19] or four-step [3] protocols appearing exceptionally. As an illustrating example, suppose that there are seven cards numbered $0, 1, \ldots, 6$, Alice and Bob each draw three cards, and Eve draws one. Suppose that the resulting *deal* is $(012, 345, 6)$, meaning that Alice holds the set of cards $H_{\mathcal{A}} = \{0, 1, 2\}$, Bob holds $H_{\mathcal{B}} = \{3, 4, 5\}$, and Eve holds $H_{\mathcal{E}} = \{6\}$. An announcement may be a set of possible hands of cards held by Alice, including her actual one. For example, Alice may announce *My hand belongs to the set* $\{012, 034, 056, 135, 246\}$; it can be checked that after Alice's announcement, Bob may deduce Alice's actual hand, but Eve cannot. Since Bob now knows the entire deal, the second step of the protocol then consists simply of Bob announcing Eve's hand. Note that Eve may be able to make an informed guess about individual card ownership. As she holds card 6, she now knows that Alice holds one of $\{012, 034, 135\}$. In the absence of information on how Alice produced her announcement, Eve may now consider it twice as likely that Alice holds 0 than that she holds 5. In this card cryptographic community 'secure' means that all messages such as this announcement have strictly positive probability, and typically not that all messages are equally probable, as in the perfect security of [17].

Note that any all-card solution can immediately be applied to the best-card problem, but there are also best-card solutions that are not all-card solutions. For exam-

ple, given the deck of cards $0, 1, \ldots, 6$ and the deal $(012, 345, 6)$, a best-card solution instance of a two-step protocol would be Alice's announcement of the four possible hands $\{012, 046, 156, 234\}$. From such an announcement Eve would learn that Alice holds the card 2, but this is allowed in best-card protocols. In contrast, as we will discuss later, the first announcement in a two-step all-card solution must consist of at least five hands [1]. A portion of this article is devoted to showing how small best-card solutions consisting of sets of hands can be relative to all-card solutions.

Protocols based on exchanged bits

In the deal $(012, 3456, 7)$, Eve already knows that the best card held by Alice and Bob is 0, even though she does not know *who* holds it. If the deal were instead $(127, 3456, 0)$, Eve would know that the best card is 1. However, regardless of the deal, the best card cannot be 2 or worse. Let us call the cards that could possibly be the best card *good cards,* and the rest of the cards *bad.*

Since the bad cards play a somewhat secondary role in the best-card problem, Alice and Bob can use them to their advantage, for example by performing a secret-bit-exchange protocol on them. The secret bits obtained can then be used as a one-time pad, even if the two have not privately communicated previously and hence do not share any private information.

In the case of the deal $(012, 3456, 7)$, Bob holds many bad cards, as $H_{\mathcal{B}} \cap [2, 7] = H_{\mathcal{B}} = \{3, 4, 5, 6\}$. He will use these cards to generate a shared secret code with Alice. One way for Bob to do this is to choose two cards $\{x_0, x_1\} \subset [2, 7]$ such that he holds exactly one of these two, and ask Alice, *Do you hold one of* (x_0, x_1)*?*[1] If Alice answers *yes,* then this produces a secret bit between them: namely, this bit is i if Alice holds x_i.

For example, Bob could ask Alice whether she holds one of $\{2, 3\}$, to which Alice answers *yes.* This allows them to share a secret bit ι, where for example $\iota = 0$ if Alice holds 2 and otherwise $\iota = 1$. This secret bit can be used as a one-time pad for Alice to let Bob know the value of her best card: for example, she can say, *If* $\iota = 0$ *then my best card is* 0*, and if* $\iota = 1$ *my card is* 1 *or worse.* By comparing Alice's best card to his own, Bob can deduce the best card held between Alice and him.

However, there is some luck involved in Bob's selection of these two cards. If instead Bob asked Alice whether she holds a card in $\{4, 7\}$, she would answer *no.* Now Eve knows that Bob holds the card 4; fortunately this is not an issue, as 4 is one of the bad cards. Moreover, unlike Alice, Bob holds many bad cards, so he can 'afford' to waste some of them. In the next step Bob can ask Alice if she holds a card in $\{2, 5\}$, to which Alice would answer *yes,* once again giving them a shared secret bit.[2]

[1]Note that it is important that Bob either randomizes the order in which he mentions the two cards, or always mentions them in some fixed order (e.g., in increasing order), so that Eve does not know which of the two cards is actually held by him.

[2] In this particular example Bob knows Eve's *only* card, and thus the entire deal. However, as we have already seen above, it is not necessary for Bob to learn Eve's full hand during the exchange.

As we will see, secret-bit protocol solutions exist for card deals for three or more communicating players for which no all-card solutions have been reported.

Outline

The outline of the paper is as follows. Section 2 introduces terminology for cards cryptography. In Section 3 we survey solutions to the all-card problem and show how they can be used to obtain preliminary results for best-card solvability. Section 4 presents two-step protocols for cases where the eavesdropper holds one or two cards. In Section 5 we discuss bit-exchange protocols, which are used in Section 6 for the *public code protocol,* from which we obtain results for arbitrarily many communicating agents, and in Section 7, where applications of private bit exchange are discussed, obtaining some improved bounds for three communicating agents. Finally, Section 8 presents some concluding remarks and open questions.

2 Preliminaries

In this section we establish basic notation and terminology, including a formalization of card-based protocols as in e.g. [6, 9]. In order to compare our work with the literature, we will discuss both all-card, best-card and bit-exchange notions of security and informativity.

2.1 Basic terminology and notation

Definition 2.1. Let $\mathfrak{A}$ be a finite set representing a group of $m+1$ agents, including a designated *eavesdropper* $\mathcal{E} \in \mathfrak{A}$, which we also refer to as *Eve.* Elements of $\mathfrak{A} \setminus \{\mathcal{E}\}$ are the *communicating agents* or *players.* By a *distribution type* we mean a vector $\tau = (\tau_{\mathcal{P}})_{\mathcal{P}\in\mathfrak{A}}$ of positive integers. We write $|\tau|$ for $\sum_{\mathcal{P}\in\mathfrak{A}} \tau_{\mathcal{P}}$.

The deck, Ω, is a finite set of cards with cardinality $|\tau|$. A *deal of type* τ *over* Ω is a partition $H = (H_{\mathcal{P}})_{\mathcal{P}\in\mathfrak{A}}$ of Ω such that $|H_{\mathcal{P}}| = \tau_{\mathcal{P}}$ for each agent $\mathcal{P}$. We say $H_{\mathcal{P}}$ is the *hand* of $\mathcal{P}$. We denote the set of all deals of type τ over Ω by $\binom{\Omega}{\tau}$.

We will omit parentheses and commas when writing out τ in an expression $\binom{\Omega}{\tau}$. We assume an initial secure dealing phase in which a card deal is selected at random from the set of all possible deals. Afterwards, the agents have knowledge of their own hand and of the distribution type τ of the deal, but know nothing more about others' cards. Thus, they are not able to distinguish between different deals where they hold the same hand. We model this by equivalence relations between deals; since from the perspective of agent $\mathcal{P}$, a deal H is indistinguishable from H' whenever $H_{\mathcal{P}} = H'_{\mathcal{P}}$, we define $H \sim_{\mathcal{P}} H'$ if and only if $H_{\mathcal{P}} = H'_{\mathcal{P}}$. If the communicating agents are numbered $\mathcal{P}_0, \ldots, \mathcal{P}_{m-1}$ (we exclude Eve from the enumeration), we may write $\sim_k$ instead of $\sim_{\mathcal{P}_k}$.

We will fix a set Λ representing a language which the agents use to encode information. In a practical setting, elements of Λ would be strings of symbols, but

could also be modelled as natural numbers; we will refer to them simply as *public tokens.* Similarly we let Θ be a set whose elements are *private tokens,* which agents use internally to randomize their behaviour. We will assume that agents take turns, so that if the communicating agents are listed by $\mathcal{P}_0, \ldots, \mathcal{P}_{m-1}$, then $\mathcal{P}_0$ places a public and a private token first, followed by $\mathcal{P}_1$, etc.[3]

Definition 2.2 (run)**.** Let Λ be a set of *public tokens* and Θ a set of *private tokens.* An *action* is any $\alpha = (\lambda, \theta) \in \Lambda \times \Theta$, and we write $\lambda = \alpha^{\text{pub}}$. A *(finite) run* is a (possibly empty) sequence $\rho = \alpha_0, \ldots, \alpha_n$ of actions. The empty run is denoted by ϵ. If $\rho = \alpha_0, \ldots, \alpha_n$ and α is an action we write $\rho * \alpha$ for $\alpha_0, \ldots, \alpha_n, \alpha$; $\alpha * \rho$ and $\rho * \rho'$ are defined analogously. We denote the length of a run ρ by $|\rho|$. We denote the set of finite runs by Run.

We now define the notion of *protocol* we will use. Below we use $(x)_d$ to mean the remainder of x modulo d. Since we assume that in a run $\rho = \alpha_0, \ldots, \alpha_n$ the agent $\mathcal{P}_i$ has played exactly those actions α_j for $j \equiv i \pmod m$, she has access to the private information of only these actions. Thus we define $\rho[\mathcal{P}_i] = \alpha'_0, \ldots, \alpha'_n$ where $\alpha'_j = \alpha_j$ if $j \equiv i \pmod m$ and $\alpha'_j = \alpha_j^{\text{pub}}$ otherwise; when the enumeration of the agents is clear we may write $\rho[i]$ instead of $\rho[\mathcal{P}_i]$. We also write $\rho^{\text{pub}} = \alpha_0^{\text{pub}}, \ldots, \alpha_n^{\text{pub}}$; note that, aside from her own hand, this is the only information that Eve has access to.

Intuitively, a protocol Π is a non-deterministic strategy for the communicating agents to make announcements. The protocol Π generates a tree-like set of runs X^Π consisting of all possible executions. Once a deal has been fixed, a protocol assigns to each run a set of actions out of which the agent whose turn it is must choose one at random. These actions are determined exclusively by the information the agent has access to, which is assumed to be *only:* (*i*) her hand, (*ii*) the distribution type τ and the deck Ω, (*iii*) the announcements that have been made previously and (*iv*) the protocol being executed. The following definition makes this precise.

Definition 2.3 (protocol)**.** Let τ be a distribution type over $\mathfrak{A} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{m-1}, \mathcal{E}\}$. A *protocol* (for τ) is a function Π with domain $X^\Pi \subset \binom{\Omega}{\tau} \times \text{Run}$ assigning to each pair $(H, \rho) \in X^\Pi$ a set $\Pi(H, \rho) \subset \Lambda \times \Theta$ such that:

1. $(H, \epsilon) \in X^\Pi$ for every $H \in \binom{\Omega}{\tau}$.
2. For every deal H, every run ρ and every action α, $(H, \rho * \alpha) \in X^\Pi$ if and only if $(H, \rho) \in X^\Pi$ and $\alpha \in \Pi(H, \rho)$.
3. If $k = (|\rho|)_m$ (so that it is the turn of the agent $\mathcal{P}_k$), $(H, \rho), (H', \rho') \in X^\Pi$, $H \sim_k H'$ and $\rho[k] = \rho'[k]$, then $\Pi(H, \rho) = \Pi(H', \rho')$.

If $(H, \rho) \in X^\Pi$, we will say that (H, ρ) is an *execution* of Π and ρ is a *run* of Π. If $(H, \rho) \in X^\Pi$ but $\Pi(H, \rho) = \varnothing$, we say that (H, ρ) is *terminal.* If there is some $n \in \mathbb{N}$ bounding the length of every execution of Π, we say that Π is *terminating.*

[3] An alternate approach is for agents to decide when to communicate depending on their cards. However, this leads to slightly more cumbersome definitions, and can be simulated by adding a 'pass' token that agents can use when they do not wish to take a turn.

Note that protocols are generally non-deterministic and hence a deal H may have many possible executions assigned to it. Observe that a terminating protocol Π is uniquely determined by its set of terminating executions, so we will often present protocols by describing this set. In many of the protocols we will present, the private or the public parts of certain actions may be unimportant. Technically this can be modelled by assuming that Λ and Θ both contain 'empty tokens' that are used for such steps, but in informal descriptions we simply state that an agent has played a private or a public action. More formally, a *private action* is one of the form $(\lambda_\epsilon, \theta)$ and a *public action* is one of the form $(\lambda, \theta_\epsilon)$, where λ_ϵ, θ_ϵ are the designated 'empty' tokens.

2.2 Informative and secure protocols

The intention of a protocol Π is for the communicating agents to exchange information, modelled as elements of an *information space* $\mathfrak{I}$; for example, in ℓ-bit-exchange protocols we may have $\mathfrak{I} = [0, 2^\ell)$. Executions of Π will code messages in $\mathfrak{I}$ via the information function μ.

Definition 2.4. Let $\mathfrak{I}$ be a finite set, τ a distribution type over $\mathfrak{A}$ and Π a protocol. An *information function for* Π *over* $\mathfrak{I}$ is a function $\mu\colon X^\Pi \to \mathfrak{I}$.

With this we will define some desirable properties that protocols may have. The first property is *informativity*: that agents in the team learn the desired message at the end of its execution.

Definition 2.5 (informativity)**.** Let Π be a protocol and μ be a information function for Π over some set $\mathfrak{I}$. An execution (H, ρ) of a protocol Π is *informative for* μ *for an agent* $\mathcal{P}_i$ if whenever (H', ρ') is an execution of Π with $H' \sim_i H$ and $\rho'[i] = \rho[i]$, it follows that $\mu(H', \rho') = \mu(H, \rho)$ (i.e., at the end of the run the agent knows the precise message).

A terminating protocol Π is *informative for* μ *for an agent* $\mathcal{P}$ if every terminal execution of Π is informative for $\mathcal{P}$; it is *informative for* μ if it is informative for μ for every agent in $\mathfrak{A} \setminus \{\mathcal{E}\}$.

In addition to the communicating agents learning the message, we also want Eve to *not* learn it. This corresponds to the *security* of a protocol, as we define below.

Definition 2.6 (security of protocols)**.** Let μ be an information function with codomain $\mathfrak{I}$. An execution (H, ρ) of a protocol Π is *secure for the information function* μ if for every $x \in \mathfrak{I}$ there is an execution (K, σ) with $H \sim_\mathcal{E} K$, $\rho^{\text{pub}} = \sigma^{\text{pub}}$, and $\mu(K, \sigma) = x$.

The protocol Π is secure for μ if every execution of Π is secure for μ.

This notion of security corresponds to *strong security* in [6], but is weaker than that considered in e.g. [9], where the eavesdropper should consider all possible messages equally probable, sometimes known as *perfect security* [17]. The instances of

the Russian cards problem that we are interested in can then be defined by choosing suitable information functions.

Definition 2.7. Given a set of agents $\mathfrak{A}$, a distribution type τ, $i < |\tau| - \tau_{\mathcal{E}}$, and a protocol Π, define an information function $\mathsf{own}_i \colon X^{\Pi} \to \mathfrak{A} \setminus \{\mathcal{E}\}$ as follows. For an execution (H, ρ), enumerate $\Omega \setminus H_{\mathcal{E}}$ by $c_0 < c_1 < \ldots < c_{|\tau|-\tau_{\mathcal{E}}-1}$. Then, $\mathsf{own}_i(H, \rho) = \mathcal{P}$ if and only if $c_i \in H_{\mathcal{P}}$.

Define $\mathsf{best} \colon X^{\Pi} \to \Omega$ by $\mathsf{best}(H, \rho) = c$ if and only if $\min(\Omega \setminus H_{\mathcal{E}}) = c$. Finally, define $\mathsf{h}_{\mathcal{E}}(H, \rho) = H_{\mathcal{E}}$.

We say that Π is:

1. *best-card informative* if it is informative for best and for own_0;
2. *best-card secure* if it is secure for own_0;
3. *all-card informative* if it is informative for $\mathsf{h}_{\mathcal{E}}$ and for every own_i with $i < |\tau| - \tau_{\mathcal{E}}$; and
4. *all-card secure* if it is secure for every own_i with $i < |\tau| - \tau_{\mathcal{E}}$.

A distribution type τ is *best-card/all-card solvable* if there is a secure and informative best-card/all-card terminating protocol for τ.

The information function own_i maps a deal and a run to an agent $\mathcal{P}_a$ for each card c_i not held by Eve, meaning that the agent $\mathcal{P}_a$ holds the card c_i. In particular, own_0 maps a run to the agent holding the best card between all agents except Eve. Note that none of own_i, $\mathsf{h}_{\mathcal{E}}$ or best depend on ρ, but for bit-exchange protocols we will be interested in other information functions that do depend on it. In the latter protocols it does not matter whether the agents share any pre-specified information (say, about who owns a certain card), provided that they share *some* information not known to Eve.

Definition 2.8. A *public ℓ-bit-exchange protocol* is a protocol Π equipped with an information function μ onto a set $\mathfrak{I}$ with $|\mathfrak{I}| = 2^{\ell}$. The protocol Π is informative/secure if it is informative/secure for μ.

Similarly, a *private k-pair ℓ-bit-exchange protocol* is a protocol Π equipped with information functions $\mu_{\mathcal{P}\mathcal{Q}}$ onto a set $\mathfrak{I}$, where $\mathcal{P}, \mathcal{Q}$ range over all pairs of distinct communicating agents, such that for every execution of Π there are k distinct pairs $\{\mathcal{P}_i, \mathcal{Q}_i\}_{i<k}$ so that Π is informative for $\mu_{\mathcal{P}_i\mathcal{Q}_i}$ for players $\mathcal{P}_i$ and $\mathcal{Q}_i$, and so that Π is secure for

$$\bigotimes_{i<k} \mu_{\mathcal{P}_i\mathcal{Q}_i} := (\mu_{\mathcal{P}_0\mathcal{Q}_0}, \ldots, \mu_{\mathcal{P}_{k-1}\mathcal{Q}_{k-1}}).$$

Thus, after executing a secure ℓ-bit-exchange protocol, Eve considers any element of $\mathfrak{I}$ to possibly be the information shared by the communicating agents. In public bit-exchange protocols all agents will share ℓ fixed secret bits; in private bit-exchange

protocols, bits will only be shared pairwise by agents that are not necessarily determined a priori. In such cases, μ is a vector containing each of the values of μ_i, meaning that Eve should consider every combination of shared bits between the different agents to be possible. Note that Eve may learn which agents share bits.

2.3 Two-step protocols

An n-step protocol is one where every terminal execution has n actions. Many of the protocols we will discuss here consist of two steps. In the case of a two-step protocol Π for $\tau = (a, b, e)$, we may without loss of generality assume that Alice's announcement is a set[4] $\phi \subset \binom{\Omega}{a}$, corresponding to the statement *My hand is an element of* ϕ. We make the assumption that, if $\phi \in \Pi(H, \epsilon)$, then $H_{\mathcal{A}} \in \phi$ (the announcement X is *truthful*), and if $H' \in \binom{\Omega}{\tau}$ is such that $H'_{\mathcal{A}} \in \phi$, then $\phi \in \Pi(H', \epsilon)$. This is not a strong assumption, as any other announcement can easily be converted into one of this form (although this is trickier for longer protocols, as is done in some detail in [6]).

After Alice's announcement, Bob must already be informed (either of the best card or of all cards, depending on the protocol). In the all-card case, he may simply reply by announcing the set consisting of Eve's cards. In the best-card case, he instead announces the value m of the best card held between him and Alice. Observe that Eve already knows this value, so this does not provide her with any information that she did not already have. Note that both Alice's and Bob's announcements are public.

Not all of the protocols presented in this text will consist of two steps, but those that do will be assumed to follow the conventions detailed above.

3 Reduction to Known Solutions

In this section we discuss how known solutions to the Russian cards problem can be adapted to generate new best-card solutions. We begin by discussing how all-card solutions relate to best-card solutions.

3.1 All-card solvability

In the all-card Russian cards problem, Alice and Bob must communicate *all* of their cards to each other without Eve learning *any* of them. Of course it follows that, in particular, Alice and Bob learn the *best* card between them, and Eve does not learn who holds it.

Proposition 3.1. *If a protocol* Π *is an all-card solution for a distribution type* τ*, then* Π *is also a best-card solution for* τ*.*

[4] Two-step protocols do not require private tokens, so to conform to Definition 2.3 we view ϕ as a public action, i.e., we tacitly identify it with the pair (ϕ, θ_ϵ), where θ_ϵ is the empty private action. Similarly, Bob's subsequent action in a best-card protocol will be identified with the pair (m, θ_ϵ).

Proof. This is because all-card secure implies best-card secure and all-card informative implies best-card informative; see Section 2. □

As an immediate application, we see that distribution types that have been solved in the all-card literature are also best-card solvable. For example, the distribution type $(3, 3, 1)$ is already known to be all-card solvable; this is one of the oldest results in combinatorics [10]. Similarly, it is shown in [19] that $(4, 4, 2)$ is all-card solvable, although it requires at least three steps. From this we obtain the following.

Proposition 3.2. *There is a best-card, two-step protocol for the distribution type* $(3, 3, 1)$*, and a best-card, three-step protocol for* $(4, 4, 2)$*.*

We remark that all known all-card solutions for $(3, 3, 1)$ are two-step protocols where Alice announces between five and seven possible hands; we will return to this point in Section 4. There are also solutions that work for more general classes of distribution types, as the following first presented in [1] and discussed further in [16, 12]:

Theorem 3.3. *For any prime power* q *and any* $e < q$*, there exists a two-step, all-card solution for* $(q + 1, q^2 - e, e)$*.*

In fact, it is possible to find all-card solutions even when Eve holds more cards than Alice, as shown in [3]:

Theorem 3.4. *If* q *is a large enough prime power, then:*

1. *for all* $e < \frac{q^{3/2}}{2}$*, there is a four-step solution for* $(q, q^3 - q - e, e)$*, and*
2. *for all* $e < q^2/9$*, there is a four-step solution for* $(q, q^4 - q - e, e)$*.*

There are some other constructions to solve the Russian cards problem; see e.g. [4, 12, 16]. However, they all have in common that the size of the deck is at least quadratic on e. There are also solutions with a larger number of agents [5, 6], albeit where Eve holds *no* cards. In contrast, as we will see, there are many best-card solvable cases where the deck is *linear* on e. However, Theorems 3.3 and 3.4 can be used to solve some additional cases, in particular when a is small relative to e. Before stating this, let us show that the best-card problem (unlike the all-card problem) enjoys a sort of monotonicity property.

3.2 Monotonicity

Best-card protocols can be adapted to cases where each of the communicating agents has a larger number of cards. To be precise, if τ, τ' are distribution types, write $\tau \sqsubset \tau'$ if $|\tau| \leq |\tau'|$ and whenever $\mathcal{P} \neq \mathcal{E}$, it follows that $\tau_{\mathcal{P}} \leq \tau'_{\mathcal{P}}$. Similarly, given decks Ω, Ω' such that $\Omega \subset \Omega'$ and partitioned into respectively card deals H, H', we write $H \sqsubset H'$ if for any $\mathcal{P} \neq \mathcal{E}$, $H_{\mathcal{P}} \subset H'_{\mathcal{P}}$. If $\tau \sqsubset \tau'$, protocols for τ can be used to produce

protocols for τ'. Given $\Omega \subset \Omega'$, deal $H' \in \binom{\Omega'}{\tau'}$ and $f\colon \Omega \to \Omega'$, we define a new deal $H = f^{-1}[H']$ such that for all communicating agents $\mathcal{P}$, $H_\mathcal{P} = f^{-1}[H'_\mathcal{P}]$, and $H_\mathcal{E} = \Omega \setminus \bigcup_{\mathcal{P}\in\mathfrak{A}} f^{-1}[H'_\mathcal{P}]$. We may view H as a sequence of private actions, namely $(\lambda_\epsilon, H_0), \dots (\lambda_\epsilon, H_{m-1})$, recalling that λ_ϵ is the empty public action.

Definition 3.5. Let $\tau \sqsubset \tau'$ be distribution types, Ω and Ω' be decks of $|\tau|$ and $|\tau'|$ cards, respectively, Π be a protocol for τ on the deck Ω, and H be a τ'-deal.

Then, if $K \sqsubset H$ has distribution type τ and $\bigcup_{\mathcal{P}\in\mathfrak{A}} K_\mathcal{P} = \Psi \subset \Omega'$, a *simulation of* Π *with virtual deal* K *on the sub-deck* Ψ is any run ρ such that there is a bijection $f\colon \Omega \to \Psi$, where $(f^{-1}[K], \rho)$ is a run of Π.

Note that in $f^{-1}[K]$, Eve may hold more cards than she did in H, but all other agents hold at most as many cards as they held before. Simulations of protocols will yield a monotonicity property for best-card solvability. As we mentioned in the introduction, *good cards* are those that may be the best card in at least one possible deal, and it is not hard to see that c is good if and only if $c \leq e$. If $c > e$, c is *bad,* and we often denote the set of bad cards by Δ.

Proposition 3.6. *Let $\tau' \sqsubset \tau$ be distribution types such that for all communicating agents $\mathcal{P}$, either $\tau'_\mathcal{P} = \tau_\mathcal{P}$ or $\tau'_\mathcal{P} \geq \tau'_\mathcal{E}$. If there exists a best-card protocol Π' for τ', then there also exists a best-card protocol Π for τ.*

Proof. We consider two cases: one where $\tau_\mathcal{E} = \tau'_\mathcal{E}$ but $|\tau| < |\tau'|$, and the other where $\tau_\mathcal{E} > \tau'_\mathcal{E}$ but $|\tau| = |\tau'|$. It should be clear that the general case follows by applying one case and then the other. We focus on the first case.

Informally, each agent discards $\tau_\mathcal{P} - \tau'_\mathcal{P}$ of their bad cards (chosen randomly), obtaining a new deal H' over some deck $\Psi \subset \Omega$. Then, the agents simulate Π' using the deal H'.

More formally, we define a protocol Π whose terminal executions are pairs $\big(H, (H', f) * \rho\big)$ as follows. Given $H \in \binom{\Omega}{\tau}$, each agent $\mathcal{P}$ privately chooses $H'_\mathcal{P} \subset H_\mathcal{P}$ such that $|H'_\mathcal{P}| = \tau'_\mathcal{P}$ and $H_\mathcal{P} \setminus H'_\mathcal{P}$ consists only of bad cards. She then announces $H_\mathcal{P} \setminus H'_\mathcal{P}$. We set $H'_\mathcal{E} = H_\mathcal{E}$ and $\Psi = \bigcup_{\mathcal{P}\in\mathfrak{A}} H'_\mathcal{P}$. In addition, the last agent chooses a bijection $f\colon \Omega' \to \Psi$ which is the identity on the good cards, and publicly announces f so that her public token is of the form $(H_\mathcal{P} \setminus H'_\mathcal{P}, f)$. We identify the pair (H', f) with this sequence of announcements, one for each communicating agent. Then, ρ is such that $(f^{-1}[H'], \rho)$ is an execution of Π'.

Let us check that Π is best-card informative. Suppose that $\mathcal{P}$ is a communicating agent and $K \sim_\mathcal{P} H$. Then, an execution of Π on the deal H consists of a suitable choice of (H', f) and a run ρ of Π'. Similarly, an execution of Π on K consists of a suitable choice of (K', g) and a run σ of Π'. If the two executions are indistinguishable to $\mathcal{P}$, then $H'_\mathcal{P} = K'_\mathcal{P}$, $f = g$ and $\rho[\mathcal{P}] = \sigma[\mathcal{P}]$. But then $f^{-1}[H'] \sim_\mathcal{P} f^{-1}[K']$, and since Π' was informative we conclude that the best card in $f^{-1}[H']$ and $f^{-1}[K']$ is the same and held by the same agent. Since H and H' coincide on the good cards, as do K and K', and f is the identity on the good cards, the best card in H and K is also the same and held by the same agent.

To check that Π is secure, if $\big(H, (H', f) * \rho\big)$ is an execution of the protocol and $\mathcal{Q}$ is a communicating agent, since Π' is secure there is a deal $K' \in \binom{\Omega'}{\tau'}$ and a run σ so that $K' \sim_{\mathcal{E}} f^{-1}[H']$, $\rho^{\text{pub}} = \sigma^{\text{pub}}$, (K', σ) is an execution of Π' and $\mathcal{Q}$ holds the best card in K'. Now consider a deal $K \in \binom{\Omega}{\tau}$ by letting $K_{\mathcal{E}} = f[K'_{\mathcal{E}}]$ and for any communicating agent $\mathcal{P} \neq \mathcal{E}$, $K_{\mathcal{P}} = f[K'] \cup (H_{\mathcal{P}} \setminus H'_{\mathcal{P}})$. One can see that $\big(K, (K', f) * \sigma\big)$ is an execution of Π in which $\mathcal{Q}$ holds the best card.

The case where $|\tau| = |\tau'|$ but $\tau_{\mathcal{E}} > \tau'_{\mathcal{E}}$ is similar, the difference being that the agents do not announce $H_{\mathcal{P}} \setminus H'_{\mathcal{P}}$. Instead, the cards in $f^{-1}(H_{\mathcal{P}} \setminus H'_{\mathcal{P}})$ are assigned to Eve. Aside from this, the protocol and proof are essentially identical. □

As an application, we see that (a, b, e) is almost always best-card solvable when $e \leq 2$:

Proposition 3.7. *If $a, b \geq 3$, then $(a, b, 1)$ is best-card solvable, and if $a, b \geq 4$, then $(a, b, 2)$ is best-card solvable.*

Proof. Immediate from Propositions 3.2 and 3.6. □

It should be noted that if (a, b, e) is all-card solvable then not necessarily all (a', b', e) for $a' > a$ or $b' > b$ are all-card solvable. For example, the construction used for Theorem 3.3 requires that the deck have exactly $q^2 + q + 1$ cards [1]. On the other hand, we can use Propositions 3.1 and 3.6 to 'import' all-card protocols:

Proposition 3.8. *Given a prime power q, if $e + 1 \leq q \leq a - 1$ and $b \geq q^2 - e$, then (a, b, e) is best-card solvable.*

Proof. By Theorem 3.3, $(q + 1, q^2 - e, e)$ is all-card solvable for all $e \leq q - 1$, hence it is best-card solvable by Proposition 3.1. Thus, we may apply Proposition 3.6. □

We may also use Theorem 3.4 to obtain best-card solutions in cases where e may be greater than a.

Proposition 3.9. *If a is a large enough prime power, then:*

1. *there exists a best-card solution for any distribution type (a, b, e) such that $b \geq a^3 - a - e$ and $e < \frac{a^{3/2}}{2}$, and*
2. *there exists a best-card solution for any distribution type (a, b, e) such that $b \geq a^4 - a - e$ and $e < a^2/9$.*

Proof. In both cases it suffices to check that $b > e$ (since a is assumed large enough, it suffices to look at the corresponding degrees), hence we can apply Proposition 3.6. □

Thus we can adapt all-card solutions to obtain best-card solutions. For multiple agents one can derive similar results from the all-card protocols in [5]; note however that in these cases, Eve holds no cards.

Next we will see that there are many ways to produce best-card solutions that are not all-card solutions.

4 Two-Step Protocols

In this section we construct two-step solutions to the problem in the cases where $e \leq 2$. Unlike in the all-card case, it suffices to solve a 'small' case, and then extend it using the following. From here on we will often assume that the cards are sequentially numbered $0, ..., a+b+e-1$ where lower means better. The good cards are therefore defined as the cards in $[0, e]$, just as in the example in the introductory section. We will often denote card deals $(H_{\mathcal{A}}, H_{\mathcal{B}}, H_{\mathcal{E}})$ of distribution type (a, b, e) as (A, B, E).

Proposition 4.1. *If there exists a two-step, best-card solution for a distribution type (a, b, e) such that $a, b > e$ and Alice's announcement has (at most) m hands, then there exists a solution with the same properties for any (a', b', e) with $a' \geq a$ and $b' \geq b$.*

Proof. The proof mimics that of Proposition 3.6, but tailored for two-step protocols. Let $\Omega = [0, a+b+e)$ and $\Omega' = [0, a'+b'+e)$, with $a' \geq a$ and $b' \geq b$, and fix a protocol Π for (a, b, e) satisfying the conditions of the proposition. We define a new protocol Π' for (a', b', e) in the following way: for a deal $H \in \binom{\Omega'}{a'\ b'\ e}$, we have that $\phi \in \Pi'(H, \epsilon)$ if there exist:

1. an injection $f\colon \Omega \to \Omega'$ which is the identity on the good cards and such that $|f(\Omega) \cap H_{\mathcal{A}}| = a$,
2. a deal $K \in \binom{\Omega}{a\ b\ e}$ such that $f(K_{\mathcal{A}}) = H_{\mathcal{A}} \cap f(\Omega)$, and
3. an announcement $\psi \in \Pi(K, \epsilon)$,

such that, setting $H^-_{\mathcal{A}} = H_{\mathcal{A}} \setminus f(\Omega)$, we have that

$$\phi = \{f(A) \cup H^-_{\mathcal{A}} : A \in \psi\}. \tag{1}$$

It is not hard to check that a suitable injection f and a suitable deal K can be chosen (randomly) by Alice, and moreover that Π' is indeed a protocol.

To see that Π' is best-card informative, suppose that $f(A) \cup H^-_{\mathcal{A}} \in \phi$ is a hand avoiding $H_{\mathcal{B}}$. Note that $f^{-1}(H_{\mathcal{B}})$ has at least b elements, since Ω has cardinality $a+b+e$, $|f(\Omega) \cap H_{\mathcal{A}}| = a$ and $|f(\Omega) \cap H_{\mathcal{E}}| \leq e$. Choose $B \subset f^{-1}(H_{\mathcal{B}})$ with exactly b elements and containing all of the good elements of $f^{-1}(H_{\mathcal{B}})$. Since Π was best-card informative, it follows that $\min(A \cup B) = \min(f^{-1}(H_{\mathcal{A}}) \cup B) \leq e$, and since f fixes the good cards and $H^-_{\mathcal{A}}$ contains only bad cards,

$$\min((f(A) \cup H^-_{\mathcal{A}}) \cup f(B)) = \min(H_{\mathcal{A}} \cup H_{\mathcal{B}}),$$

as needed. This shows that Π' is best-card informative to Bob. Given Bob's subsequent announcement of the value of the best card, it is clear that the protocol is also informative to Alice.

As for best-card security, we must construct for a given execution $(H, \phi * m)$ of the protocol a deal K such that $H_{\mathcal{E}} = K_{\mathcal{E}}$, $(K, \phi * m)$ is also an execution of Π, and a different agent holds the best card in each of H and K. Without loss of generality, we assume that Bob holds the best card in H. Let ψ and f be such that (1) holds. Since Π is best-card secure, there is a deal $K \in \binom{\Omega}{a\ b\ e}$ in which Alice holds the best card and such that $\psi \in \Pi(K, \epsilon)$. Define a deal $K' \in \binom{\Omega'}{a'\ b'\ e}$ with $K'_{\mathcal{A}} = f(K_{\mathcal{A}}) \cup H^-_{\mathcal{A}}$, $K'_{\mathcal{E}} = H_{\mathcal{E}}$, and $K'_{\mathcal{B}} = \Omega' \setminus (K'_{\mathcal{A}} \cup K'_{\mathcal{E}})$. Then, $(K', \phi * m)$ is a terminal execution of Π' in which Alice holds the best card. □

Below, we will use Proposition 4.1 to show that there are relatively simple two-step solutions when Eve holds one or two cards.

4.1 A two-step, four-hand solution for $e = 1$

We recall the introductory example, wherein for the distribution type $(3, 3, 1)$, there is a two-step all-card solution where Alice's first announcement consists of a tuple of five possible hands, whereas a best-card solution required only four hands. Thus a natural question is whether there is a two-step all-card solution to the problem which uses only four hands; however, a negative answer is immediately given by the following result combining [1, Prop. 1 & 2].

Theorem 4.2. *In any two-step all-card secure and informative protocol for any distribution type (a, b, e), Alice's first announcement must contain at least*

$$\max\left(\frac{(a+b+e)(e+1)}{a}, \frac{(a+b+e)(a+b)}{b(b+e)}\right)$$

possible hands.

From this we immediately obtain the following:

Corollary 4.3. *In any two-step all-card secure and informative protocol for any distribution type $(a, b, 1)$, Alice's first announcement must contain at least five possible hands.*

Indeed, if $a \leq b$ and $e = 1$ then the left-hand expression is easily seen to be greater than four, while for $a > b$ (and hence $a \geq b + 1$) the right-hand expression is greater than four. Moreover, observe that these bounds can become arbitrarily large if we fix one of a, b and let the other parameter grow. However, as we will see, for any $(a, b, 1)$ with $b \geq a \geq 3$ there is a simple protocol using four a-tuples as Alice's announcement. First, let us give a combinatorial characterization of informative announcements.

Lemma 4.4. *Alice's announcement in a two-step protocol for (a, b, e) is best-card informative to Bob if and only if whenever ϕ is an announcement of the protocol and $A_0, A_1 \in \phi$ are such that $\min A_0 \neq \min A_1$ and $\min(A_0 \cup A_1) \leq e$, then $|A_0 \setminus A_1| > e - \min(A_0 \cup A_1)$.*

Proof. Let $\Omega = [0, a+b+e)$. First assume that for any announcement ϕ of the protocol, if $A_0, A_1 \in \phi$ are such that $\min A_0 \neq \min A_1$ and $\min(A_0 \cup A_1) \leq e$, then $|A_0 \setminus A_1| > e - \min(A_0 \cup A_1)$. Consider an announcement ϕ of the protocol, and suppose that (A_0, B, E_0) and (A_1, B, E_1) are two deals with $A_0, A_1 \in \phi$. We claim that $\min(A_0 \cup B) = \min(A_1 \cup B)$.

Let $m = \min(A_0 \cup A_1)$. If $\min B < m$, we have that $\min B$ is the best card on both deals. Otherwise, note that $m \leq e$, and assume towards a contradiction that $\min A_0 \neq \min A_1$. It follows from our hypothesis that $|A_0 \setminus A_1| > e - m$. Note moreover that $[0, m-1] \subset E_0 \cap E_1$ (as m is the best card between Alice and Bob). We then have that

$$\begin{aligned} |\Omega| &\geq |[0,m)| + |A_0 \setminus A_1| + |A_1| + |B| \\ &> m + (e-m) + a + b \\ &= a + b + e, \end{aligned}$$

a contradiction.

For the other direction, assume that there is an announcement ϕ of the protocol and two hands $A_0, A_1 \in \phi$ such that, for $m = \min A_0 < \min A_1$, we have that $m \leq e$ and $|A_0 \setminus A_1| \leq e - m$. Choose two deals $H^i = (A_i, B_i, E_i)$, $i \in \{0, 1\}$ as follows. Choose a (possibly empty) set

$$D \subset \Omega \setminus ([0,m) \cup A_0 \cup A_1)$$

with $e - m - |A_0 \setminus A_1|$ elements, which is possible since

$$\begin{aligned} |D| &= |\Omega \setminus ([0,m) \cup A_0 \cup A_1)| \geq (a+b+e) - m - a - |A_0 \setminus A_1| \\ &= b + e - m - |A_0 \setminus A_1|. \end{aligned}$$

Then, set $E_i = [0,m) \cup (A_i \setminus A_{1-i}) \cup D$, and

$$B_0 = B_1 = \Omega \setminus ([0,m) \cup A_0 \cup A_1 \cup D).$$

It is easy to see that Alice holds the best card m in H^0, and that m is not the best card in H^1 (in this case, it may that Alice or that Bob holds the best card). From this it is easy to see that $H^0 \sim_{\mathcal{B}} H^1$, that the announcement ϕ is executable on both, yet each deal has a different best card. It follows that such an announcement is not best-card informative to Bob. □

We conclude that Alice's first announcement in a two-step best-card protocol must satisfy the constraints of Lemma 4.4, because with a subsequent second announcement by Bob, he cannot inform himself.

Lemma 4.5. *In any two-step best-card protocol for any distribution type (a, b, e), Alice's announcement must contain at least $\frac{e(e+3)}{2} + 2$ possible hands.*

Proof. Consider any deal H and any set $\phi \subset \binom{\Omega}{a}$ and suppose that ϕ is the first announcement in some best-card secure protocol. First we claim that there must be some $A^\infty \in \phi$ with $\min A^\infty > e$. Otherwise, let m_* be the maximum number such that $m_* = \min A$ for some $A \in \phi$. If $m_* \leq e$, consider a deal where Eve holds $[0, m_*)$ and does not hold any cards in A; in such a deal, Eve would know that the best card, m_*, is held by Alice, as Eve can rule out any hand of Alice whose best card is less than m_*, and there are no hands in the announcement whose best card is greater than m_*. Thus we must have that $m_* > e$. Similarly, there must be a hand A^e such that $\min A^e = e$; for, otherwise, if Eve held $[0, e)$, then she would know that the best card, e, was held by Bob.

Finally, fix $m < e$; we claim that there must be at least $e+1-m$ hands $A \in \phi$ such that $\min A = m$. Let $\{A_1^m, \ldots, A_k^m\}$ be the set of hands $A \in \phi$ with $\min A = m$, and toward a contradiction, assume $k \leq e-m$. Construct a hand E for Eve as follows. For each $i \leq k$, we have by Lemma 4.4 that $|A_i^m \setminus A^\infty| > e - \min(A_i^m \cup A^\infty) = e - m \geq 1$, and hence we can choose a card $x_i \in (A_i^m \setminus A^\infty) \setminus \{m\}$. Let $E' = [0, m) \cup \{x_i\}_{i=1}^k$ and choose $E \supset E'$ with e elements such that $A^\infty \cap E = \varnothing$, and moreover E' does not intersect A^∞. This is possible since by assumption $k \leq e - m$, so that $k + m \leq (e - m) + m = e$, hence $|E'| \leq e$. Consider a deal where Alice holds A^∞ and Eve holds E; then, Eve would know that the best card, m, is held by Bob, as Eve can rule out any hand of the form A_i^m.

Adding these lower bounds together and counting the extra hands A^e, A^∞, we conclude that there must be at least

$$2 + \sum_{m=0}^{e-1} (e + 1 - m) = \frac{e(e+3)}{2} + 2$$

possible hands in ϕ. □

Thus any best-card, two-step protocol when $e = 1$ must use at least four hands. Let us show that this is indeed possible.

Theorem 4.6. *If $a, b \geq 3$, then there is a two-step, four-hand, best-card solution for $(a, b, 1)$.*

Proof. The announcement

$$\phi^{\texttt{four}} = \{016, 025, 123, 456\}$$

is readily verified to be best-card secure and informative. Moreover, if Alice's hand is not contained in $\phi^{\texttt{four}}$, she can produce a suitable announcement by permuting the bad cards in Ω; note that since $\phi^{\texttt{four}}$ contains hands where Alice holds any possible set of good cards (i.e., $\varnothing$, $\{0\}$, $\{1\}$, $\{0, 1\}$), such a permutation can always be found.

It follows that $(3, 3, 1)$ is best-card solvable in two steps with four hands, and by Proposition 4.1, so is $(a, b, 1)$ for all $a, b \geq 3$. □

Example 4.7. Consider card deal $(678, 01234, 5)$ of distribution type $(3, 5, 1)$. A secure and informative announcement is

$$\{017, 058, 145, 678\}$$

after which Bob announces that the best card between them is 0. The announcement can be obtained from $\phi^{\texttt{four}}$ by defining an injection

$$f = \{(0,0), (1,1), (2,5), (3,4), (4,6), (5,8), (6,7)\},$$

as in the proof of Proposition 4.1. Note that the cards 2 and 3 do not occur in the announcement, as they are not in the image of f; Eve therefore learns from the announcement that Bob holds 2 and 3. However, this does not matter as these are bad cards, and Eve remains uncertain between Alice holding 017 or 678.

Example 4.8. A best-card solution for card deal distribution type $(4, 4, 1)$ is as follows. The pack consists of the cards $0, \ldots, 8$. Suppose that the card deal is $(5678, 0123, 4)$. Alice announces

$$\{0158, 0378, 1348, 5678\}.$$

This announcement is obtained from $\phi^{\texttt{four}}$ and Proposition 4.1 by the injection

$$f = \{(0,0), (1,1), (2,3), (3,4), (4,6), (5,7), (6,5)\}.$$

Note that at this stage Alice does not know yet whether Bob holds 0, as she also considers it possible that Bob's hand is 1234. Bob then announces that the best card between him and Alice is 0, from which Alice but not Eve learns that Bob holds 0.

Alternatively, Alice and Bob may use Proposition 3.6 as follows. Alice announces one of the bad cards that she holds; for example, she may announce that she holds 8. Similarly, Bob announces that he holds (say) 2, and they proceed to apply the four hand protocol for the distribution type $(3, 3, 1)$ on the card deal $(567, 013, 4)$. For example, Alice announces $\{015, 037, 134, 567\}$, then Bob announces that the best card between him and Alice is 0.

Observe that even though the second approach requires more announcements, the information shared is essentially the same: for example, in both cases Eve learns that Alice holds 8. Indeed, Proposition 4.1 is basically an adaptation of Proposition 3.6 to a two-announcement format.

4.2 A two-step, ten-hand solution for $e = 2$

Now, we consider deals of distribution type $(a, b, 2)$, with $a, b \geq 5$. Since we will be considering a deck with twelve elements, we will use hexadecimal notation and number the cards $0, \ldots, 9, \mathrm{A}, \mathrm{B}$.

If Eve holds two cards, the combinatorial requirements for an announcement ϕ by Alice (that is truthful, i.e. contains her actual hand) are that:

1. if $A_1, A_2 \in \phi$ are such that $\min A_1 \neq \min A_2$ and $\min(A_1 \cup A_2) \leq e$, then $|A_1 \setminus A_2| > e - \min(A_1 \cup A_2)$;
2. the card 2 is secure against the hand 01;
3. for all $x \geq 2$, 1 is secure against $0x$, and
4. for all $x, y \neq 0$, 0 is secure against xy.

where a card x is *secure against* yz if there are hands A_1 and A_2 in ϕ not containing y or z with $x \in A_1$ but $x \notin A_2$ (compare to the notion of security for the information function own_x mapping executions with the announcement ϕ to $\{\mathcal{A}, \mathcal{B}\}$). By Lemma 4.4, the first item guarantees that Alice's announcement is best-card informative to Bob. The other three items guarantee that it is best-card secure against Eve. We implemented a Haskell program to check the above conditions, and showed the following.

Theorem 4.9. *If $a, b \geq 5$, then $(a, b, 2)$ is best-card solvable in two steps with ten hands.*

Proof. A best-card solution for $(5, 5, 2)$ that consists of ten hands (quintuples) for Alice's announcement, represented hexadecimally, is

$$\{0147\mathrm{B}, 0259\mathrm{A}, 13489, 156\mathrm{AB}, 23456,$$
$$789\mathrm{AB}, 05689, 0368\mathrm{A}, 1237\mathrm{A}, 12679\}.$$

As usual in a two-announcement solution, following Alice's announcement, Bob announces which is the best card held between Alice and him. Given an arbitrary card deal of distribution type $(5, 5, 2)$, a permutation of the set of bad cards $[3, \mathrm{B}]$ can always make Alice's actual hand of cards match one in the announcement above.

We then use Proposition 4.1 to lift this construction to all $(a, b, 2)$ with $a, b \geq 2$. □

It is tedious, but possible, to check by hand that this is indeed a best-card solution. Note that Bob may not learn all of Alice's cards. For example, if Bob holds 0458B he remains uncertain between Alice holding 1237A and 12679, so that he does not learn whether Alice holds the card 3 (or 6, or A).

Example 4.10. By Theorem 4.9, there is a ten-hand, two-step, best-card solution for $(5, 10, 2)$. However, by Theorem 4.2, no such protocol can be an all-card solution. Note that 10 is the smallest value of $b \geq 5$ for which $(5, b, 2)$ violates the bounds of Theorem 4.2; we do not know if there are all-card, ten-hand solutions for smaller b.

We did not find any solution with fewer than ten hands for $(5, 5, 2)$, but do not know if ten is the minimal required number of hands (we found many solutions of more than ten hands). However, it is possible to prove that the lower bound of seven hands obtained from Lemma 4.5 cannot be attained; we omit the details. We did not find two-announcement solutions for $(a, b, 2)$ with a or b smaller than 5 by Haskell programming; however, for protocols consisting of more than two announcements these sometimes do exist, as we have seen in Proposition 3.2.

5 Bit-Exchange Protocols

As mentioned in Section 2, an ℓ-bit-exchange protocol allows the communicating agents to share one of 2^ℓ possible messages so that Eve considers each one equally possible. As was the case for best-card protocols, bit-exchange protocols enjoy a monotonicity property.

Proposition 5.1. *If there exists a secure public (k-pair private) ℓ-bit-exchange protocol for a distribution type τ and $\tau \sqsubset \tau'$, then there also exists a secure public (k-pair private) ℓ-bit-exchange protocol for τ'.*

The proof is similar to that of Proposition 3.6. Fischer and Wright construct protocols between arbitrarily many players holding a small portion of the deck. We present a slight variant of their result.

Theorem 5.2 ([8], Corollary 4.4)**.** *There exist positive constants $c_1 < 2.7096$ and $c_2 < 0.0647$ such that for any distribution type τ with $m \geq 2$ communicating agents and real number $r \in (0, 1/m]$, if for each $\mathcal{P} \neq \mathcal{E}$ we have that $\tau_\mathcal{P} \geq r|\tau|$ and $|\tau| \geq (4/r)^{c_1}(\ell + c_2)$, then there is a secure ℓ-bit-exchange protocol for τ.*

In [8] it is assumed that $\tau_\mathcal{P} = \lfloor r|\tau| \rfloor$, but the inequality $\tau_\mathcal{P} \geq \lfloor r|\tau| \rfloor$ suffices in view of Proposition 5.1. For the case of two communicating agents it will be better to use a simpler solution which nevertheless provides bounds that are more convenient in our setting. The following protocol is an adaptation of a 1-bit secret key exchange protocol from [7], modified for ℓ-bit exchange.

Protocol 5.3 (card pair protocol)**.** *Let τ be a distribution type over $m+1$ agents. The card pair bit-exchange protocol proceeds as follows. Let H be a deal. If there are fewer than two communicating agents holding cards, the protocol terminates. Otherwise, let $\mathcal{P}$ be any communicating agent holding a maximal number of cards.*

$\mathcal{P}$ chooses a card w she holds, a card v she does not hold, and asks:

Who holds one of $\{w, v\}$?

For $\mathcal{Q} \neq \mathcal{P}$, if $\mathcal{Q}$ holds one of $\{w, v\}$ then $\mathcal{Q}$ answers I do, *otherwise $\mathcal{Q}$ answers* I do not; *all communicating agents answer the question.*

1. *If $\mathcal{Q}$ answers* I do, *the protocol is then repeated recursively on the deal H' with $H'_\mathcal{P} = H_\mathcal{P} \setminus \{w\}$, $H'_\mathcal{Q} = H_\mathcal{Q} \setminus \{v\}$, and $H'_\mathcal{X} = H_\mathcal{X}$ for all $\mathcal{X} \notin \{\mathcal{P}, \mathcal{Q}\}$.*

   For the resulting run $\rho = \alpha * \rho'$ we recursively set $\mu_{\mathcal{P}\mathcal{Q}}(H, \rho) = \gamma * \mu_{\mathcal{P}\mathcal{Q}}(H', \rho')$, where $\gamma = 0$ if $\mathcal{P}$ held $\min\{w, v\}$, otherwise $\gamma = 1$. For all other pairs of communicating agents $\mathcal{X}, \mathcal{Y}$ we set $\mu_{\mathcal{X}\mathcal{Y}}(H, \rho) = \mu_{\mathcal{X}\mathcal{Y}}(H', \rho')$.

2. *If all agents answer* I do not, *the protocol is then repeated recursively on the deal H' given by $H'_\mathcal{P} = H_\mathcal{P} \setminus \{w\}$, $H'_\mathcal{E} = H_\mathcal{E} \setminus \{v\}$, $H'_\mathcal{X} = H_\mathcal{X}$ for all $\mathcal{X} \notin \{\mathcal{P}, \mathcal{E}\}$ with $\ell' = \ell$. For all pairs of communicating agents $\mathcal{X}, \mathcal{Y}$ we set $\mu_{\mathcal{X}\mathcal{Y}}(H, \rho) = \mu_{\mathcal{X}\mathcal{Y}}(H', \rho')$.*

Once an agent has asked who holds one of $\{w, v\}$, we will say that the cards w, v have been *named;* until then, they are *unnamed.* In the case of two communicating agents, Protocol 5.3 provides secure ℓ-bit exchange, provided Alice and Bob have enough cards. Note that in this case there is no difference between private and public bit exchange (see Definition 2.8).

Theorem 5.4. *If $a, b \geq \ell$ and $a + b \geq e + 2\ell$ then Protocol 5.3 performs secure ℓ-bit exchange for (a, b, e).*

Proof. If $x = (x_0, \ldots, x_n)$ is a sequence and ℓ a natural number we introduce the notation $x \restriction \ell = (x_0, \ldots, x_{\ell-1})$, with the convention that x_i is understood as 0 if $i > n$. We will replace the information functions $\mu_{\mathcal{XY}}$ by $\mu_{\mathcal{XY}} \restriction \ell$, to ensure they have the right length.

Then, proceed by induction on the number of cards. If (say) Alice asks *Do you hold one of $\{w, v\}$?* on the first round and Bob answers *I do,* then Alice and Bob share a bit γ. This bit is not known by Eve, as we can easily define a deal $\tilde{H}$ where Alice and Bob trade w and v, and clearly Alice could have asked the same question and obtained the same answer if the deal were $\tilde{H}$, but then they would instead share the bit $1 - \gamma$. If we let $a' = |A'|$, $b' = |B'|$ and $e' = |E'|$, then $a' = a - 1 \geq \ell - 1 = \ell'$, and similarly $b' \geq \ell'$, while $a' + b' \geq e + 2\ell - 2 = e + 2\ell'$. Hence by the induction hypothesis the recursive application of the protocol performs secure ℓ'-bit exchange, and in total Alice and Bob exchange ℓ bits.

Otherwise since Alice held more than ℓ cards then $a' \geq \ell$, while $b' = b \geq \ell$ and $a' + b' \geq e - 1 + 2\ell = e' - 2\ell$. Hence the recursive application of the protocol performs secure ℓ-bit exchange. □

Theorem 5.5. *If $a = b = c = e + 2\ell$ then Protocol 5.3 performs secure two-pair private ℓ-bit exchange for (a, b, c, e).*

Proof. Once again we work with the information functions $\mu_{\mathcal{XY}} \restriction \ell$. First we observe by induction on the number of rounds in the protocol that the two agents holding the most unnamed cards differ by at most one in number of unnamed cards. More precisely, suppose that at some round of the game, $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2$ are ordered in non-decreasing order according to the number of cards they hold that have not previously been named: then, $\mathcal{P}_2$ holds at most one more unnamed card than $\mathcal{P}_1$. This is seen by a case-by-case analysis: for the first case, if at one stage of the protocol each agent $\mathcal{P}_i$ holds k_i unnamed cards and $k_1 = k_2$, then after $\mathcal{P}_2$ asks *Who holds one of $\{w, v\}$?*, $\mathcal{P}_2$ holds $k_2' = k_2 - 1$ unnamed cards, while $\mathcal{P}_1$ holds either $k_1' = k_2$ or $k_1' = k_2 - 1$. Meanwhile, $\mathcal{P}_0$ holds $k_0' \leq k_2$ cards, so the agent with the most unnamed cards has at most k_2 unnamed cards and the second agent has at least $k_2 - 1$ unnamed cards. The other case is where $k_1 < k_2$, which by induction implies that $k_1 = k_2 - 1$; this case can be checked similarly.

It follows from this that when the protocol terminates each agent holds at most one unnamed card, for otherwise one of the agents can make a question. Now consider Alice's hand. She has at most one unnamed card, which means that each of her other

$e+2\ell-1$ cards was mentioned in a question *Who holds one of* $\{w,v\}$*?* In at most e cases, Alice asked the question and Eve held the other card. The other $2\ell-1$ cards correspond to secret bits shared with Bob or Carol, so by the pigeonhole principle Alice shares at least ℓ bits with at least one of the two.

By similar considerations, Bob and Carol each share at least ℓ bits with another agent, and this is only possible if there are (at least) two ℓ-bit exchange pairs. □

6 The Public Code Protocol

We now show how bit-exchange protocols can be used to provide solutions to the best-card problem. We call this method the *public code protocol*. In this protocol, the communicating agents use the 'bad' cards to share secret bits between them, use those bits to produce a code, and then communicate their best card using that code. Recall that a card x is good if $x \leq e$ and bad otherwise; a card is bad if it cannot be the best card of one of the communicating agents. Recall also that $(p)_q$ denotes the remainder of p modulo q.

Protocol 6.1 (public code protocol)**.** *Let τ be a distribution type with $m \geq 2$ communicating agents $\mathcal{P}_0, \ldots, \mathcal{P}_{m-1}$. Let*

- $\eta = \tau_{\mathcal{E}}$ *if* $m = 2$, $\eta = \tau_{\mathcal{E}} + 1$ *otherwise,*
- $\ell = \lceil \log_2(\eta+1) \rceil$*, and*
- $\Delta = \Omega \setminus [0, \tau_{\mathcal{E}}]$*; elements of* Δ *are 'bad cards'.*

For $H \in \binom{\Omega}{\tau}$, the protocol proceeds as follows.

1. *Each agent $\mathcal{P}$ privately chooses a maximal hand $H'_{\mathcal{P}} \subset H_{\mathcal{P}} \cap \Delta$ at random such that $H'_{\mathcal{P}} \neq H_{\mathcal{P}}$. Setting $H'_{\mathcal{E}} = \Delta \setminus \bigcup_{\mathcal{P} \neq \mathcal{E}} H'_{\mathcal{P}}$, we thus obtain a deal $H' \in \binom{\Delta}{\tau'}$.*
2. *The agents simulate an $(m-1)\ell$-bit-exchange protocol on the deck Δ using the deal H', if one exists (otherwise the protocol fails).*
3. *Let $(x_1, \ldots, x_{m-1})$ be the exchanged bits, where $x_i \in [0, 2^\ell)$. For $i \in [1, m]$, let c_i^* be the best card of $\mathcal{P}_i$.*

   Then, $\mathcal{P}_1, \ldots, \mathcal{P}_{m-1}$ successively announce the value of $\big(\min\{c_i^*, \eta\} + x_i\big)_{\eta+1}$.
4. *Finally, $\mathcal{P}_0$ announces the value c^* of the best card held between the communicating agents.*

Observe that in step 1, the agent $\mathcal{P}$ must choose $H'_{\mathcal{P}}$ as follows. If $\mathcal{P}$ holds any good cards, then $H_{\mathcal{P}} \cap \Delta \subsetneq H_{\mathcal{P}}$, so that $H'_{\mathcal{P}} = H_{\mathcal{P}} \cap \Delta$ is the only maximal sub-hand satisfying the required conditions. Otherwise $H_{\mathcal{P}} \cap \Delta = H_{\mathcal{P}}$, which (as we will see later) is undesirable. Thus $\mathcal{P}$ randomly chooses $b \in H_{\mathcal{P}}$ and sets $H'_{\mathcal{P}} = H_{\mathcal{P}} \setminus \{b\}$.

Finally, note that Eve may hold more cards in H' than in H, i.e. it may be that $\tau'_{\mathcal{E}} > \tau_{\mathcal{E}}$.

Next we give sufficient conditions for which the secret code protocol is a solution for the best-card problem. Below, the general intuition is that each agent $\mathcal{P}$ will hold $k_{\mathcal{P}}$ good cards, where $k_{\mathcal{P}} \leq \tau_{\mathcal{E}} + 1$. These cards will have to be discarded in order to perform a bit-exchange protocol. Moreover, it is crucial for security that at least one card is discarded by each communicating agent, and thus $\mathcal{P}$ will discard a total of $\max\{k_{\mathcal{P}}, 1\}$ cards in order to perform the bit-exchange. Note that the precise value of $k_{\mathcal{P}}$ depends on the particular deal and thus we do not know it *a priori.*

Theorem 6.2. *Let τ be a distribution type over a set $\mathfrak{A}$ with m communicating agents and Eve, and define η, ℓ as in Protocol 6.1.*

Suppose that for any vector $(k_{\mathcal{P}})_{\mathcal{P}\in\mathfrak{A}}$ of natural numbers such that $\sum_{\mathcal{P}\in\mathfrak{A}} k_{\mathcal{P}} = \tau_{\mathcal{E}} + 1$, there is an $(m-1)\ell$-secret bit-exchange protocol for the distribution type τ' defined by

- $\tau'_{\mathcal{P}} = \tau_{\mathcal{P}} - \max\{k_{\mathcal{P}}, 1\}$ *if* $\mathcal{P} \neq \mathcal{E}$, *and*
- $\tau'_{\mathcal{E}} = \tau_{\mathcal{E}} - k_{\mathcal{E}} + |\{\mathcal{P} \in \mathfrak{A} \setminus \{\mathcal{E}\} : k_{\mathcal{P}} = 0\}|$.

Then, Protocol 6.1 satisfies

1. Correctness: *it is a protocol in the sense of Definition 2.3 and never terminates on step 2,*
2. Informativity: *it is best-card informative, and*
3. Security: *it is best-card secure.*

Proof. Correctness. Let H be any τ-deal. For $\mathcal{P} \in \mathfrak{A}$, let $k_{\mathcal{P}}$ be the number of good cards that $\mathcal{P}$ holds. Note that $\sum_{\mathcal{P}\in\mathfrak{A}} k_{\mathcal{P}} = \tau_{\mathcal{E}} + 1$. Let τ' be as in the statement of the theorem. Each agent $\mathcal{P} \neq \mathcal{E}$ privately chooses a hand $H'_{\mathcal{P}} \subset H_{\mathcal{P}} \cap \Delta$ with $\tau'_{\mathcal{P}}$ cards, and Eve is assigned $H'_{\mathcal{E}} = \Delta \setminus \bigcup_{\mathcal{P}\in\mathfrak{A}\setminus\{\mathcal{E}\}} H'_{\mathcal{P}}$; it is not hard to check that H' is a τ'-deal. It follows from the assumptions that there is a protocol for τ' for the agents to securely share $(m-1)\ell$ secret bits, so the protocol does not terminate at step 2. The secret bits uniquely determine a sequence $(x_1, \ldots, x_{m-1}) \in [0, 2^\ell)^{m-1}$, allowing the agents to perform step 3.

Since $\mathcal{P}_0$ can then compute each value of $\min\{c_i^*, \eta\}$, she can tell if either all other agents hold bad cards (and hence she holds the best card), or if at least one other agent holds good cards, she can compare them to her own and determine the value of the best card. Therefore $\mathcal{P}_0$ can perform step 4.

Informativity. To see that Protocol 6.1 is informative, clearly after step 4, all agents know the value of the best card. They also know who holds it, which we show considering two cases. First assume that $m > 2$. If the best card is held by $\mathcal{P}_i$ with $i \geq 1$, then the best card of $\mathcal{P}_i$ is a good card, and hence others can compute its

value using $\mathcal{P}_i$'s announcement in step 3. Otherwise, by computing each agent's best card they know it is worse than the one announced by $\mathcal{P}_0$, hence $\mathcal{P}_0$ must hold the best card.

If instead $m = 2$, we have that $\eta = \tau_{\mathcal{E}}$. Let $\mathcal{P}_0$ be Alice and $\mathcal{P}_1$ be Bob, with best cards $c^*_{\mathcal{A}}$ and $c^*_{\mathcal{B}}$, respectively. If $c^*_{\mathcal{B}} < \eta$ or $c^*_{\mathcal{A}} < \eta$, we can reason as in the general case. Otherwise, $c^*_{\mathcal{A}}, c^*_{\mathcal{B}} \geq \eta$; but since the best card is at most η, then either Alice holds η, and hence she knows that she holds the best card, or she holds a card worse than η, and can deduce that Bob holds η and it is his best card. In either case Alice announces that η is the value of the best card, and by similar reasoning this is informative to Bob.

Security. Finally we check that the protocol is secure. Suppose that the agent $\mathcal{A}$ holds the best card, c^*, and let $\mathcal{B} \neq \mathcal{A}$ be another communicating agent. Let (H, ρ) be an execution of the protocol so that H' is the deal chosen by the agents in step 1. For $\mathcal{P} \in \mathfrak{A} \setminus \{\mathcal{E}\}$, set $D_{\mathcal{P}} = H_{\mathcal{P}} \setminus H'_{\mathcal{P}}$; note that $D_{\mathcal{P}}$ is the set of cards discarded by $\mathcal{P}$ when choosing $H'_{\mathcal{P}}$, so that $D_{\mathcal{P}} \neq \varnothing$ for all $\mathcal{P}$. In particular, we may define $c = \min D_{\mathcal{B}}$. We remark that since $D_{\mathcal{B}}$ contains all good cards held by $\mathcal{B}$, $\mathcal{B}$ must have announced $\min\{c^*_{\mathcal{B}}, \eta\} = \min\{c, \eta\}$. The idea will be for $\mathcal{A}$ and $\mathcal{B}$ to swap c^* and c.

To do this, consider a deal $\tilde{H}$ as follows. First, define $\tilde{c}$ to be the best card of $(H_{\mathcal{A}} \cup \{c\}) \setminus \{c^*\}$. Using the assumption that the bit-exchange protocol of step 2 is secure, let $K' \sim_{\mathcal{E}} H'$ be a deal on Δ according to which the agents share $(x'_1, \ldots, x'_{m-1})$, defined by

$$x'_i = \begin{cases} \big(\min\{c^*, \eta\} - \min\{\tilde{c}, \eta\} + x_i\big)_{\eta+1} & \text{if } \mathcal{P}_i = \mathcal{A}, \\ \big(\min\{c, \eta\} - \min\{c^*, \eta\} + x_i\big)_{\eta+1} & \text{if } \mathcal{P}_i = \mathcal{B}, \text{ and} \\ x_i & \text{otherwise.} \end{cases}$$

We will replace $H'_{\mathcal{P}}$ by $K'_{\mathcal{P}}$, allowing $\mathcal{A}$ and $\mathcal{B}$ to swap c^* and c. Formally, for $\mathcal{P} \neq \mathcal{E}$, define $K_{\mathcal{P}} = D_{\mathcal{P}} \cup K'_{\mathcal{P}}$, then set

$$\widetilde{H}_{\mathcal{P}} = \begin{cases} (K_{\mathcal{A}} \setminus \{c^*\}) \cup \{c\} & \text{if } \mathcal{P} = \mathcal{A}, \\ (K_{\mathcal{B}} \setminus \{c\}) \cup \{c^*\} & \text{if } \mathcal{P} = \mathcal{B}, \text{ and} \\ K_{\mathcal{P}} & \text{otherwise.} \end{cases}$$

Finally, define $\widetilde{H}_{\mathcal{E}} = \Omega \setminus \bigcup_{\mathcal{P} \in \mathfrak{A} \setminus \{\mathcal{E}\}} \widetilde{H}_{\mathcal{P}}$. It is not too hard to check that $(\widetilde{H}, \rho)$ is an execution of Protocol 6.1 where $\mathcal{B}$ holds the best card, and $H \sim_{\mathcal{E}} \tilde{H}$. Since $\mathcal{B} \neq \mathcal{A}$ was arbitrary, we conclude that Protocol 6.1 is secure. □

From this, we obtain many instances of best-card solvable distribution types.

Corollary 6.3. *Let $\ell = \lceil \log_2(e+1) \rceil$ and suppose that (a, b, e) are such that $a, b \geq e + \ell + 1$ and at least one of the two inequalities is strict. Then, Protocol 6.1 is best-card secure and informative for (a, b, e).*

Proof. Let $(k_{\mathcal{A}}, k_{\mathcal{B}}, k_{\mathcal{E}})$ be a vector of natural numbers with $k_{\mathcal{A}} + k_{\mathcal{B}} + k_{\mathcal{E}} = e + 1$ and define $\tau' = (a', b', e')$ as in the statement of Theorem 6.2. It not hard to check that $a', b' \geq \ell$ and that

$$a' + b' \geq a + b - e - 2 \geq e + 1 + 2\ell.$$

If $e' \leq e + 1$, we may use Theorem 5.4 to see that there is an $(m-1)\ell$-secret bit-exchange protocol for (a', b', e'), so that from Theorem 6.2 we can conclude that the public code protocol is a best-card solution for (a, b, e). So it remains to check that indeed $e' \leq e + 1$.

First note that this inequality holds trivially if Eve holds at least one good card, since $e' \leq e - k_{\mathcal{E}} + 2$. So suppose that she holds no good cards. Note that we cannot have $k_{\mathcal{A}} = k_{\mathcal{B}} = 0$ since at least one of the two holds a good card; but then $|\{\mathcal{P} \in \mathfrak{A} \setminus \{\mathcal{E}\} : k_{\mathcal{P}} = 0\}| \leq 1$, so that $e' \leq e + 1$, as claimed. □

In particular, Protocol 6.1 is best-card secure and informative for distribution types $(a, b, 1)$ with $a \geq 3$ and $b \geq 4$ and $(a, b, 2)$ with $a \geq 5$ and $b \geq 6$. These distribution types are not lower bounds: we recall Proposition 3.2 for $(3, 3, 1)$ and $(4, 4, 2)$. Some open cases for small decks of cards are discussed in the concluding section.

Example 6.4. Let us reconsider the example in the introduction, for distribution type $(3, 4, 1)$. The deal is $(012, 3456, 7)$; $\{0, 1\}$ is the set of good cards and $[2, 7]$ is the set of bad cards, and $\ell = \lceil \log_2(e + 1) \rceil = 1$. Therefore, Alice holds the bad card 2 and all of Bob's cards are bad. Alice and Bob now execute Protocol 6.1.

In step 1 we get that $H'_{\mathcal{A}} = \{2\}$, and suppose that $H'_{\mathcal{B}} = \{3, 4, 6\}$ (Bob has to choose a proper subset of $\{3, 4, 5, 6\}$). So, $H'_{\mathcal{E}} = \{5, 7\}$, and $H' = (2, 346, 57)$.

In step 2 Alice and Bob simulate a 1-bit-exchange protocol using $H' = (2, 346, 57)$. For example, Bob asks Alice: *Do you hold one of* $\{2, 3\}$*?,* the answer is *Yes,* and the protocol terminates (Alice has no unnamed card and Bob has two unnamed cards).

In step 3 Alice announces the value of $(\min\{c_i^*, \eta\} + x_i)_{\eta+1}$. Let us suppose that $x_i = 0$ when Alice holds 2 and that $x_i = 1$ when Alice holds 3. Then, this amounts to $(0+0)_2 = 0$. Eve cannot learn Alice's card from this announcement: she is uncertain whether Alice holds 2 or 3, therefore she is uncertain whether Alice's announcement one is the result of $(0 + 0)_2 = 0$ or $(1 + 1)_2 = 0$. In the latter case, Alice's best card would have been 1 and she would also have held 3.

In step 4 Bob announces that the value of the best card held between him and Alice is 0. We note that Eve who holds 6 already knows this, so that this is also secure.

Now we consider larger groups of agents.

Corollary 6.5. *There exist constants* κ_1, κ_2 *such that for any distribution type* τ *with* $m \geq 3$ *communicating agents,* $r \in (0, 1/m]$ *and* $\ell = (m-1)\lceil \log_2(\tau_{\mathcal{E}} + 2) \rceil$*, if for each* $\mathcal{P} \neq \mathcal{E}$ *we have that* $\tau_{\mathcal{P}} \geq \tau_{\mathcal{E}} + r|\tau| + 1$ *and* $|\tau| - \tau_{\mathcal{E}} \geq (4/r)^{\kappa_1}(\ell + \kappa_2)$*, then there is a secure* ℓ*-bit-exchange protocol for* τ*.*

Proof. Let c_1, c_2 be the constants of Theorem 5.2. Define $\kappa_1 = c_1$ and $\kappa_2 = c_2 + 1/12^{c_1}$. Then, if $|\tau| - \tau_{\mathcal{E}} \geq (4/r)^{\kappa_1}(\ell + \kappa_2)$, since $r \leq 1/m \leq 1/3$ we have that $4/r \geq 12$, from which it follows that

$$\begin{aligned} |\tau| - \tau_{\mathcal{E}} - 1 &\geq (4/r)^{\kappa_1}(\ell + \kappa_2) - \left(\tfrac{4/r}{12}\right)^{c_1} \\ &= (4/r)^{c_1}(\ell + c_2). \end{aligned}$$

Then, as before we can check that the assumptions of Theorem 6.2 hold, but now using Theorem 5.2. □

In view of the estimates given in Theorem 5.2 of c_1 and c_2, we can set $\kappa_1 = 2.7096$ and $\kappa_2 = 0.0659$.

Example 6.6. As an illustration of Corollary 6.5, let there be three agents Alice, Bob, Carol, and an eavesdropper Eve, where Eve holds two cards. To minimize the size of the deck, take $r = 1/3$, so that

$$\ell = (m-1)\lceil \log_2(\tau_{\mathcal{E}} + 2)\rceil = (3-1)\lceil \log_2(2+2)\rceil = 4.$$

From the requirements $\tau_{\mathcal{P}} \geq \tau_{\mathcal{E}} + r|\tau| + 1$ and $|\tau| - \tau_{\mathcal{E}} \geq (4/r)^{\kappa_1}(\ell + \kappa_2)$ the second requirement calculates to $12^{2.7096}(4 + 0.0659) = 3414.3355$ which gives a lower bound of the size of the deck of 3437. The first requirement is then easily met by equally distributing the remaining cards over the three communicating players, so that giving them each somewhat under 1200 cards guarantees the existence of a 4-bit-exchange protocol. Once these bits have been gathered, two can be used as a one-time-pad by Alice to communicate whether her best card is 0 (the best card in the deck), 1 or 2 or worse, and the other two for Bob to similarly communicate whether his best card is 0, 1 or 2 or worse. After this, Carol can publicly announce the best card between Alice, Bob, and herself, from which all agents can deduce who holds this best card.

7 Private Code Protocols

Having all agents share all secret bits may be overkill: it may be enough to have bits shared between pairs of agents, who can then spread secrets throughout the group. As we will see, this idea can lead to better bounds. We present a variation of Protocol 6.1 tailored for three communicating agents.

Protocol 7.1 (private code protocol)**.** *Let (a, b, c, e) be a distribution type. Let $\ell = \lceil \log_2(e+2)\rceil$ and $\Delta = \Omega \setminus [0, e]$. For $H \in \binom{\Omega}{\tau}$, the protocol proceeds as follows.*

1. *Each agent $\mathcal{P}$ privately chooses a maximal hand $H'_{\mathcal{P}} \subset H_{\mathcal{P}} \cap \Delta$ at random such that $H'_{\mathcal{P}} \neq H_{\mathcal{P}}$.*
2. *Set $H'_{\mathcal{E}} = \Delta \setminus \bigcup_{\mathcal{P} \neq \mathcal{E}} H'_{\mathcal{P}}$. The agents simulate a two-pair $(\ell+1)$-bit-exchange protocol on the deck Δ using the deal H', if such a protocol exists. We let $\mathcal{P}, \mathcal{Q}_0$ and $\mathcal{P}, \mathcal{Q}_1$ be two pairs of agents who share $\ell + 1$ bits.*

3. *$\mathcal{Q}_0$ and $\mathcal{Q}_1$ use ℓ bits shared with $\mathcal{P}$ to securely tell her the least between their best card and $e+1$.*

4. *$\mathcal{P}$ announces the value c^* of the best card held between the communicating agents. She then uses the remaining bit shared with each of $\mathcal{Q}_0$ and $\mathcal{Q}_1$ to indicate whether it is $\mathcal{P}$ who holds the best card or not.*

The security and informativity of this protocol can be checked similarly to those of Protocol 6.1, giving the following.

Theorem 7.2. *Let τ be a distribution type over $\mathfrak{A} = \{\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{E}\}$ and define ℓ as in Protocol 7.1.*

Suppose that for any vector $k = (k_\mathcal{A}, k_\mathcal{B}, k_\mathcal{C}, k_\mathcal{E})$ of natural numbers such that $\sum k = e+1$, there is a two-pair private $(\ell+1)$-secret bit-exchange protocol for the distribution type τ' defined by

- $\tau'_\mathcal{P} = \tau_\mathcal{P} - \max\{k_\mathcal{P}, 1\}$ *if* $\mathcal{P} \neq \mathcal{E}$, *and*
- $\tau'_\mathcal{E} = \tau_\mathcal{E} - k_\mathcal{E} + |\{\mathcal{P} \in \mathfrak{A} \setminus \{\mathcal{E}\} : k_\mathcal{P} = 0\}|$.

Then, Protocol 6.1 satisfies Correctness, Informativity *and* Security, *as defined in Theorem 6.2.*

Corollary 7.3. *Let (a, b, c, e) be a distribution type and $\ell = \lceil \log_2(e+2) \rceil$. Then, if $a, b, c > 2(e+\ell+1)$, Protocol 7.1 is best-card secure and informative for (a, b, c, e).*

Proof. Fix $(k_\mathcal{A}, k_\mathcal{B}, k_\mathcal{C}, k_\mathcal{E})$ and $\tau' = (a', b', c', e')$ as in the statement of Theorem 7.2. If $k_\mathcal{E} > 0$ then $e' \leq e - 1 + 3 = e + 2$, and if $k_\mathcal{E} = 0$ then at least one of $k_\mathcal{A}, k_\mathcal{B}, k_\mathcal{C}$ is positive and $e' \leq e + 2$; in either case, $e' \leq e + 2$. From this it is easy to check that $a', b', c' \geq e' + 2\ell$, and thus Protocol 7.1 performs two-pair $(\ell+1)$-bit exchange by Theorem 5.5 and Proposition 3.6. Thus we may apply Theorem 7.2. □

Example 7.4. Let Eve hold a single card. Corollary 7.3 prescribes that $a, b, c > 2(1+2+1) = 8$. So for the distribution type $(9, 9, 9, 1)$, Protocol 7.1 is already a best-card solution. If Eve holds two cards, we similarly obtain a solution to $(11, 11, 11, 2)$. This is a stark contrast with Example 6.6, wherein a best-card solution was only guaranteed for $(1145, 1145, 1145, 2)$.

We remark that it is also possible to modify Protocol 7.1 for a larger number of agents. For example, suppose that we could always use the bad cards so that some agent $\mathcal{P}$ could share $\ell + \lceil \log(m) \rceil$ private bits with each other agent. Then, each agent $\mathcal{Q}$ uses ℓ shared bits to tell $\mathcal{P}$ her best card, after which $\mathcal{P}$ announces the value of the best card held between them and uses the remaining $\lceil \log(m) \rceil$ bits shared with each other agent to let them know who holds the best card.

Alternately, we can have $\mathcal{P}_i$ share sufficiently many bits with $\mathcal{P}_{i+1}$ for all $i < m-1$. Indeed, suppose that each such pair shares $\ell + 2\lceil \log(m) \rceil$ bits. Then, $\mathcal{P}_i$ successively uses ℓ bits to let $\mathcal{P}_{i+1}$ know the value of the best card held by any $\mathcal{P}_j$ with $j \leq i$ and

$\lceil \log(m) \rceil$ to let her know who holds this card, until we reach $\mathcal{P}_{m-1}$, who then knows the best card and who holds it. $\mathcal{P}_{m-1}$ publicly announces the value of the best card, then tells $\mathcal{P}_{m-2}$ who holds it using the remaining $\lceil \log(m) \rceil$ bits they share, and so on until we reach $\mathcal{P}_0$ again.

However, we are not aware of any protocols that achieve such a private, but not public, bit exchange. It is likely that private bit exchange with more than three communicating agents can be achieved using a smaller deck than is required for public bit exchange, but we leave the development of such protocols for future work.

8 Concluding Remarks

We introduced the *best-card Russian cards problem,* where given $m + 1$ players and a pack of ranked cards, m of the players wish to know the value of the best card between them without the remaining player getting to know who holds said card. We used methods inspired by both block design as well as secret bit sharing schemes. This problem is a weakening of the more standard, *all-card* Russian cards problem, and thus one would expect the best-card problem to be better-behaved. Indeed, this is the case, both with respect to the complexity of the solutions and the sets of solvable instances of the problem.

As we have shown, whenever Alice and Bob each hold at least three cards and Eve holds one, it suffices for Alice to announce that her hand is one of four possibilities. Contrast this with the fact that the maximum length of an all-card secure and informative $(5, 5, 1)$-announcement is 66 quintuples [1]. However, fewer hands leak more information to Eve, so an alternative goal (for a two-step protocol) could be to maximize the number of hands. Either way, the number of hands in an announcement is only a crude measure of complexity; while typically one may require less bits to communicate a small number of hands, oftentimes a set consisting of a large number of hands may be represented by a small amount of information, for example by the sum of a player's cards modulo a suitable prime [2].

If we allow longer protocols, then many distribution types for which we have no known all-card solutions become best-card solvable. Generally speaking, it is hard to determine whether a given distribution type (a, b, e) is best-card or all-card solvable (although the all-card unsolvability of $(1, 1, 1)$ is proved in [9]). For example, we currently do not know whether $(3, 2, 1)$ or $(4, 3, 2)$ is best-card solvable.

Nevertheless, all known all-card solutions (be it in two or more steps) require the deck to be at least quadratic on e (see e.g. [1, 3]). On the other hand, the public code protocol only requires Alice and Bob to have linearly many cards as Eve. This suggests that there are many best-card solvable cases that are not all-card solvable.

With more than two communicating agents the contrast between all-card and best-card solvability is starker; in fact, *no* all-card solutions are currently known when Eve holds cards and there are at least three communicating agents. The solution we propose also allows the size of the deck to grow linearly on Eve's hand (for a fixed number of agents holding a fixed portion of the deck).

There are several directions for future work, but we mention two natural possibilities. First, observe that Proposition 3.9 shows that there are many best-card solvable cases with $e > a$. Nevertheless, the deck grows quadratically on e, which is not surprising since the protocol relies on an all-card solution. For ℓ-bit-exchange protocols there are solutions where the eavesdropper holds most of the cards [8]. Thus it is natural to ask if there are best-card protocols where Eve holds more cards than one or more of the communicating agents, with the size of the deck linear on Eve's hand.

Finally, we remark that the protocols we have presented are not *perfectly* secure, as Eve may learn probabilistic information about the owner of the best card even if she does not learn who it is with certainty. The development of perfectly secure best-card protocols is another interesting direction for future inquiry.

References

[1] M. H. Albert, R. E. L. Aldred, M. D. Atkinson, H. van Ditmarsch and C. C. Handley, Safe communication for card players by combinatorial designs for two-step protocols, *Australas. J. Combin.* 33 (2005), 33–46.

[2] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque, J. J. Joosten and F. Soler-Toscano, A secure additive protocol for card players, *Australas. J. Combin.* 54 (2012), 163–176.

[3] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque and F. Soler-Toscano, A colouring protocol for the generalized Russian cards problem, *Theor. Comput. Sci.* 495 (2013), 81–95.

[4] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque and F. Soler-Toscano, A geometric protocol for cryptography with cards, *Des. Codes Crypto.* 74(1) (2015), 113–125.

[5] D. Fernández-Duque, Perfectly secure data aggregation via shifted projections, *Inf. Sci.* 354 (2016), 153–164.

[6] D. Fernández-Duque and V. Goranko, Secure aggregation of distributed information, *Discret. Appl. Math.* 198 (2016), 118–135.

[7] M.J. Fischer, M. S. Paterson and C. Rackoff, Secret bit transmission using a random deal of cards, In: *Distributed Computing and Cryptography*, 1989, pp. 173–182.

[8] M. J. Fischer and R. N. Wright, An efficient protocol for unconditionally secure secret key exchange, In: *SODA*, 1993, pp. 475–483, Philadelphia, PA, USA; Society for Industrial and Applied Mathematics.

[9] M. J. Fischer and R. N. Wright, Bounds on secret key exchange using a random deal of cards, *J. Cryptol.* 9(2) (1996), 71–99.

[10] T. P. Kirkman, On a problem in combinations, *Camb. Dublin Math. J.* 2 (1847), 191–204.

[11] A. Koch and S. Walzer, Foundations for actively secure card-based cryptography, In: *FUN*, 2021, pp. 17:1–17:23.

[12] E. Landerreche and D. Fernández-Duque, A case study in almost-perfect security for unconditionally secure communication, *Des. Codes Crypto.* 83(1) (2017), 145–168.

[13] T. Mizuki, H. Shizuya and T. Nishizeki, A complete characterization of a family of key exchange protocols, *Int. J. Inf. Sec.* 1 (2002), 131–142.

[14] V. Niemi and A. Renvall, Secure multiparty computations without computers, *Theor. Comput. Sci.* 191(1) (1998), 173–183.

[15] A. Stiglic, Computations with a deck of cards, *Theor. Comput. Sci.* 259(1-2) (2001), 671–678.

[16] C. M. Swanson and D. R. Stinson, Additional constructions to solve the generalized Russian cards problem using combinatorial designs, *Electron. J. Combin.* 21(3) (2014), #P3.29, 31 pp.

[17] C. M. Swanson and D. R. Stinson, Combinatorial solutions providing improved security for the generalized Russian cards problem, *Des. Codes Crypto.* 72(2) (2014), 345–367.

[18] H. van Ditmarsch, The Russian cards problem, *Stud. Logica* 75 (2003), 31–62.

[19] H. van Ditmarsch and F. Soler-Toscano, Three steps, In: *CLIMA*, LNCS 6814, Springer, 2011, pp. 41–57.

[20] P. Winkler, My night at the cryppie club, *Bridge Magazine*, August 1981, 60–63.

(Received 23 Oct 2018; revised 4 Oct 2020, 10 Mar 2021)