Avoiding bias in cards cryptography

M.D. Atkinson*, H.P. van Ditmarsch†, and S. Roehling‡

April 8, 2008

1 Introduction

Public key cryptography bases its security on mathematical problems that are computationally hard to solve, such as the discrete logarithm problem or factoring the product of two large primes. Advances in technology and new discoveries in mathematics make it more feasible to solve these problems, i.e. it becomes more feasible to break the encryption.

An example of the former is the furore in the Netherlands early 2008 over the breaking of the code of the OV-chipcard, a smartcard to be introduced in public transport, such as already in use in London and Hongkong. This is a Mifare Classic card, and its security is based on the secrecy of the CRYPT01 algorithm. This algorithm was reconstructed by Nijmegen University students, after which a brute force attack was effective because the keys used *were only 48 bits long*. When the Dutch public transport companies decided to develop this card 48 bit keys were deemed secure, but today 96 bits is considered the minimum. The Nijmegen students only needed 9 hours on advanced equipment to try out all 48 bit keys. (See `http://www.ru.nl/ds/group/press_release/` and `http://www.smartcard.co.uk/mifare.html`.)

An example of the latter is that Agrawal *et al.* (2004) show that to determine whether a number is prime can be done in polynomial time. Until then, this complexity was thought to be higher. This discovery is not necessarily related to the complexity of determining whether a number is a product of primes. No polynomial time factorization algorithm for that is known (Vasilenko, 2006), so that cryptography based on products of large primes is not directly threatened by Agrawal *et al.*'s discovery. Still, further theoretical progress may render known algorithms for encryption useless. Of course one might then use larger prime numbers—but that brings us back to the former.

There are also cryptographic protocols wherein discovering the secret is not too complex given the current state of technology, but logically impossible. These cryptographic protocols are developed with computationally unlimited agents in mind. It is impossible for the attacker to learn the secret from the communication, but it is possible for the sender and receiver to share the secret. This is on the assumption that sender and receiver already share some other information prior to the start of the protocol. One such approach involves the use of a random deck of cards. In that case, the information you initially share with other players is that your cards cannot be theirs. There are also relations to bit-exchange protocols using card deals

*Computer Science, University of Otago, New Zealand, `mike@cs.otago.ac.nz`

†Computer Science, University of Otago, New Zealand & IRIT, France, `hans@cs.otago.ac.nz`

‡Dept. of Electrical and Computer Engineering, University of Auckland, New Zealand, `sroehling@gmx.net`

(Fischer and Wright, 1996) and to cards cryptography for computations with committed bits as in Stiglic (2001).

The general scenario is as follows: Two agents, Alice and Bob, draw a and b cards from a deck of $a + b + c$ cards, and Cathy, the attacker (a.k.a. Eve, the eavesdropper), receives the remaining c cards. Alice wishes to communicate her cards to Bob by making a public announcement without informing Cathy of any of her cards. The investigation of the generalised problem with parameters (a, b, c) was inspired by its $(3, 3, 1)$ instance that was coined in van Ditmarsch (2003) the *Russian Cards problem*. This is because the $(3, 3, 1)$ instance was presented as a problem at the Moscow Mathematical Olympiad in 2000. But it is older than that: it is a classic in design theory (Kirkman, 1847).[1]

Previous work on the Russian Cards problem involved using epistemic logic to describe its properties and to find its solutions (van Ditmarsch, 2003, 2005), including the analysis of protocols wherein Alice communicates her hand of cards to Bob with more than one announcement, depending on Bob's response to her initial announcement. In van Ditmarsch (2003) it is shown that however Alice structures her announcement, it always corresponds to an announcement of the form "I hold one of the following hands: ...". The generalised version has also been investigated by Albert, Aldred, Atkinson, van Ditmarsch, and Handley (2005); they devise combinatorial analogues CA1, CA2 and CA3 of the epistemic requirements for Alice to communicate her hand of cards safely to Bob, and they have found various methods to construct 'good announcements' that satisfy these combinatorial axioms.

For the $(3, 3, 1)$ instance, suppose Alice announces that she holds one of $\{012, 034, 056, 135, 246\}$ (by 012 we mean the set $\{0, 1, 2\}$, etc.). Her announcements are supposed to be truthful, and her actual hand must therefore be among those five. No matter which of those Alice holds, and no matter what Bob holds, he can infer Alice's cards. For example, if Bob held 126, then he could eliminate 012, 056, 135 and 246, leaving only 034, that must therefore be Alice's actual hand. And no matter what Cathy holds, she cannot infer any card of Alice or Bob. Say Cathy held card 5, then she could eliminate 056 and 135, leaving her with 012, 034 and 246 for Alice's hand and (by considering the remaining cards) 346, 126 and 013 for Bob's hand. One can establish that the combinatorial axioms CA1, CA2 and CA3 are indeed satisfied, and that this is therefore a good announcement.

Also for the $(3, 3, 1)$ instance, and supposing Alice holds 034, she could announce that she holds one of $\{012, 034, 056, 135, 146, 236, 245\}$. This is a seven-hand announcement. We can similarly to the method demonstrated in the previous paragraph establish that this is a good announcement.

Some of the constructions proposed by Albert *et al.*, while not giving away enough information for Cathy to *determine* any card held by Alice or Bob, appear to result in situations where Cathy can make an *educated guess* based on the relative frequency of the cards. For example, consider again the announcement for $(3, 3, 1)$ given as $\{012, 034, 056, 135, 246\}$. Card 0 occurs three time in this announcement, and the other cards only twice. On the assumption that all holdings in the announcement are equally likely to be the actual one, it seems reasonable for an outside observer to conclude that it is more likely for Alice to hold card 0 than another card. The eavesdropper Cathy is not exactly an outside observer. She also holds a

[1] The (maximal) solution is found on the very first pages of standard textbooks in design theory as Wallis (1988) and Stinson (2004). Its roots can (at least...) be traced back to Kirkman (1847) where the solution is found on page 194 as Q_7; Q_i is the maximum set of triples made from i points such that no pair occurs more than once. Kirkman is better known for Q_{15}, the Fifteen Schoolgirls Problem, which is found on the next page in Kirkman (1847).

card. If that were card 0, the tentative conclusion of the outsider evaporates, as Alice now cannot hold card 0: Cathy can exclude all but 135 and 246 from the announcement. All cards occur just once in these two holdings, and she has no reason to prefer one over the other. If instead Cathy holds card 3, she can exclude all but 012, 056 and 246 from the announcement. Among these, card 6 occurs more often than card 1. It is now attractive for Cathy to conclude that Alice is more likely to hold card 6 than card 1—and that would be justified if Alice produced her announcement based on one of these three holdings, although, again, only on the assumption that all such announcements are equally likely to be produced. In other words: even though the announcement is unbiased with respect to holdings, the announcement may be biased with respect to card occurrences, or otherwise biased with respect to patterns in the announcement, and this information may be valued by the eavesdropper (attacker) Cathy. The other announcement, $\{012, 034, 056, 135, 146, 236, 245\}$, does not contain card occurrence bias.

From the perspective of cryptography there are two ways to overcome such bias: *either* use protocols that produce announcements that are unbiased for card occurrence (or more complex patterns), *or* use protocols that (may) produce biased announcements but ensure that there is no relation between patterns in the announcement, such as card occurrence, and the actual holding. We focus on the first, in Section 2, using design theory. We devise an additional requirement for the announcement in order to eliminate the possibility of making educated guesses. To that effect we propose an additional combinatorial axiom CA4. We give a method to design announcements that meet this requirement, *unbiased announcements* therefore, and we prove some relevant results. Those are our main contributions. Additionally, in Section 3, we present *unbiased protocols* for the $(3, 3, 1)$ case, counteracting single card occurrence bias in announcements.

2 Unbiased announcements

2.1 Combinatorial axiom CA4

We will use terminology as in Albert *et al.* (2005). Cards are commonly referred to as points, are all distinct, and are labeled with consecutive natural numbers. The set of all cards (or deck of cards) is denoted by Ω. An *i-set* is a set of i cards. A possible holding (or hand) of Alice is called a *line* (in other words, a line is an a-set). Thus, an announcement $\mathcal{L}$ by Alice consists of one or more lines. We write X, Y, Z for i-sets, x, y, z for points in such sets, and in particular also L for a-sets (lines). Alice, Bob, and Cathy hold, respectively, a, b, and c cards. These are the parameters of the card deal, for which we write (a, b, c). 'Elimination' refers to Cathy or Bob eliminating those lines from the announcement that are impossible holdings for Alice because they contain one or more of their own cards.

Albert *et al.* proposed three axioms CA1, CA2, and CA3, that correspond to the informal requirements given in the problem description for Alice to inform Bob of her cards. An announcement satisfying those axioms is called a *good announcement*. A good announcement guarantees that it is common knowledge among Alice, Bob, and Cathy that Bob knows Alice's holding. The axioms are as follows (CA stands for 'Combinatorial Axiom').

CA1 For every b-set X there is at most one line in $\mathcal{L}$ that avoids X.

CA2 For every c-set X the lines in $\mathcal{L}$ avoiding X have empty intersection.

CA3 For every c-set X the lines in $\mathcal{L}$ avoiding X have union consisting of all cards except those of X.

Combinatorial Axiom 1 states that, given the announcement, Bob must be able to infer what Alice is holding. In order for Bob to figure out which line of the announcement is Alice's holding, he has to eliminate lines from the announcement based on his knowledge of his own cards. For example, because cards are distinct, if Bob holds card 4, then he can eliminate all lines that contain card 4 since those cannot be a possible holding of Alice. Similarly, Bob can eliminate any other line that contains a card that he himself holds. A line in the announcement that contains none of the cards held by Bob is said to avoid Bob's hand (here denoted by b-set X). If there are two or more such lines in the announcement, then Bob is left with more than one possibility for Alice's hand and cannot state with certainty which is the correct one. Therefore, there should be at most one line in the announcement that avoids Bob's hand. (As we are assuming that the announcement is truthful and that Alice's hand is among the lines, there is even *exactly* one line that avoids Bob's hand.)

Combinatorial Axiom 2 states that, given the announcement, Cathy must not be able to infer *any* card held by Alice. Cathy employs the same process of eliminating lines from the announcement as Bob by looking at her own hand (denoted by c-set X). After elimination, she examines the remaining lines. If there is one card common to all these lines, then Cathy can conclude that Alice holds that card. So, there must be no card common to all remaining lines. In other words, all remaining lines taken together must have empty intersection.

Combinatorial Axiom 3 states that, given the announcement, Cathy must not be able to infer *any* card held by Bob. If it is not satisfied, there is a card that does not occur among the lines avoiding Cathy's holding X. This card is therefore not held by Alice, nor is it held by Cathy. It must therefore be a card held by Bob.

For parameters $(3, 3, 1)$, the announcements $\{012, 034, 056, 135, 246\}$ and $\{012, 034, 056, 135, 146, 236, 245\}$ both satisfy CA1, CA2, and CA3, as can be easily checked. We propose to distinguish between these announcements by means of another, new, combinatorial axiom. This is CA4. It expresses absence of card occurrence bias. We also propose yet another axiom, CA5, that will then be shown equivalent to CA4.

CA4 For every c-set X there is a number n_X such that for every point $x \notin X$ there are n_X lines in $\mathcal{L}$ avoiding X that contain x.

CA5 For every c-set X there is a number m_X such that for every point $y \notin X$ there are m_X b-sets Y avoiding X that contain y and that avoid an $L \in \mathcal{L}$ also avoiding X.

Combinatorial Axiom 4 states that, given Alice's announcement and Cathy's hand of cards, no card occurs more often than another one in the lines Cathy considers possible. Combinatorial Axiom 5 states that, given Alice's announcement and Cathy's hand of cards, no card occurs more often than another one in the b-sets Cathy considers possible for Bob.

The new combinatorial axioms become more readable if we introduce additional formalisation. Given a collection $\mathcal{Z}$ of i-sets $Z \subseteq \Omega$ (lines, b-sets, c-sets, ...), the subset of $\mathcal{Z}$ with all points contained in $X \subseteq \Omega$ is denoted $\mathcal{Z}(X)$, i.e.

$$\mathcal{Z}(X) = \{Z \in \mathcal{Z} \mid Z \subseteq X\}.$$

On the other hand, the set of i-sets in $\mathcal{Z}$ containing (all) points in X is denoted $\mathcal{Z}[X]$, i.e.

$$\mathcal{Z}[X] = \{Z \in \mathcal{Z} \mid X \subseteq Z\}.$$

For $\mathcal{Z}(\{x\})$, write $\mathcal{Z}(x)$, and for $\mathcal{Z}[\{x\}]$, write $\mathcal{Z}[x]$; for $\mathcal{Z}(X \cup \{x\})$ we write $\mathcal{Z}(X + x)$, for $\mathcal{Z}(\{x, y\})$ we write $\mathcal{Z}(xy)$, etc. The complement of X in Ω is $\overline{X}$. We combine the notations, e.g. we write $\mathcal{L}(\overline{X})[x]$ for the set of lines in $\mathcal{L}$ avoiding X and containing x. Finally, somewhat arbitrarily, $b(\mathcal{L}(\overline{X}))$ is the set of b-sets Y avoiding X and an $L \in \mathcal{L}$ also avoiding X, i.e.

$$b(\mathcal{L}(\overline{X})) = \{Y \mid Y = \Omega - X - L, L \in \mathcal{L}, L \cap X = \emptyset\}.$$

We now can rephrase the combinatorial axioms as

Definition 1 (Combinatorial Axioms)**.** *We distinguish five axioms.*

CA1 *For every b-set X: $|\mathcal{L}(\overline{X})| \leq 1$.*

CA2 *For every c-set X: $\bigcap \mathcal{L}(\overline{X}) = \emptyset$.*

CA3 *For every c-set X: $\bigcup \mathcal{L}(\overline{X}) = \overline{X}$.*

CA4 *For every c-set X there is a number n_X such that for every $x \notin X$: $|\mathcal{L}(\overline{X})[x]| = n_X$.*

CA5 *For every c-set X there is a number m_X such that for every $x \notin X$: $|b(\mathcal{L}(\overline{X}))[x]| = m_X$.*

Announcement $\{012, 034, 056, 135, 246\}$ does not satisfy CA4. Take $X = \{5\}$. The lines not containing 5 (i.e., avoiding $\{5\}$) are 012, 034 and 246. *Two* of those contain 2 but only *one* line contains 1. Therefore, no number n_5 (i.e., $n_{\{5\}}$) exists in this case. On the other hand, announcement $\{012, 034, 056, 135, 146, 236, 245\}$ satisfies CA4, with $n_y = 2$ for all points $y = 0, \ldots, 6$. E.g., $\{135, 146, 236, 245\}$ avoid 0; point 1 occurs twice in those, namely in 135 and 146; and so on for other points. Announcement $\{012, 034, 056, 135, 246\}$ does not satisfy CA5. Take $X = \{5\}$. The b-sets not containing 5 and avoiding one of $012, 034$ and 246 are: $346, 126$ and 013. Two of those contain a 1 but only one contains a 2. Again, the seven-line announcement satisfies CA5.

Many other, and more generic, examples can be found using design theory, see Wallis (1988); Hughes (1962); Stinson (2004). The mathematical theory of block designs deals with collections of special subsets, called blocks (or lines), of a given set. It provides a convenient framework for studying the relation between the proposed combinatorial axioms CA4 and CA5. A t-design with parameters (v, k, λ) has the property that any combination of t distinct elements of a set of $v = |\Omega|$ points occurs in the same number λ of k-blocks (or k-lines, sets with k elements). The number λ is the *covalency* of the design. Thus, in 2-designs, also known as balanced incomplete block designs, any pair of distinct cards occurs in the same number of lines. This is relevant for our investigation, because it entails that in the subset of lines containing any given card (such as a singleton c-set), any other card occurs in the same number of lines. Similarly, in 3-designs any 3-tuple of distinct cards occurs in the same number of lines. This can be further generalised to 4-designs, 5-designs, etc., but such designs are far less common and few general constructions are available that may help us here. Every t-design is also a 1-design, 2-design, $\ldots$, $(t-1)$-design. The seven-hand announcement $\{012, 034, 056, 135, 146, 236, 245\}$ is a 2-design, with block size 3 and covalency 1. CA4 can be also be formulated as follows.

Definition 2 (CA4, alternative formulation)**.** *For every c-set X, $\mathcal{L}(\overline{X})$ is a 1-design with covalency n_X.*

We can construct designs satisfying CA4 using the various methods known for constructing designs, such as from projective planes and binary designs. Incidental results are reported in Yates (1936) and Bose (1939). For details, we refer to Roehling (2005). As an illustration of such constructions we consider the design whose points are the 2^n points of a n-dimensional vector space over $GF(2)$ and whose lines are the affine hyperplanes ($(n-1)$-dimensional subspaces and their complementary cosets), of which there are $2(2^n-1)$. For brevity we shall call these *binary* designs. It is well-known that their automorphism group is triply transitive (Dembowski, 1997) and so they are 3-designs. We shall prove that they can be used to construct good announcements satisfying CA4.

For an example, we construct a binary design with $n = 3$. The points of the design in this case are known as Steiner quadruples (Colbourn and Dinitz, 1996, p.71). Each line consists of $2^{3-1} = 4$ points. The lines can be found as the orthogonal complements (and their cosets) of the $2^3 - 1 = 7$ non-zero 3-bit vectors $001, 010, 011, 100, 101, 110, 111$. The two lines corresponding to the first vector are $\{000, 010, 100, 110\}$ (in decimal notation $\{0, 2, 4, 6\}$, i.e. 0246) and $\{001, 011, 101, 111\}$ (in decimal 1357). Proceed similarly for the remaining 3-bit vectors. The resulting announcement consisting of the $2(2^3 - 1) = 14$ lines is

$$\{0246, 0145, 0347, 0123, 0257, 0167, 0356, 1357, 2367, 1256, 4567, 1346, 2345, 1247\}$$

Given parameters $(4, 3, 1)$, this announcement $\mathcal{L}$ satisfies CA4: for all points y, $n_y = 4$. For example, for $y = 0$ we get $\mathcal{L}(\overline{0}) = \{4567, 2367, 2345, 1357, 1346, 1256, 1247\}$ and all other points occur exactly four times in this set: point 1 in the last four lines, point 2 in lines 2, 3, 6, and 7; etc. It is also easy to check that the announcement satisfies CA1, CA2, and CA3. Of course, for parameters $(4, 2, 2)$ this same 14-line announcement is not good. This is obvious, as Bob needs to have an informational advantage over Cathy (he must have more cards) for the announcement to succeed. So they either both learn the secret, or neither. In case neither is informed, for example, if Bob holds cards 0 and 1, he cannot determine from the design whether Alice's holding is 2367, 4567, or 2345.

The same binary design may be associated with more than one instance of the (a, b, c) parameters. For example, the binary design for $n = 4$ is a good announcement for parameters $(8, 7, 1)$ and $(8, 6, 2)$, but not for $(8, 5, 3)$ (in which case CA1 and CA2 are satisfied, but not CA3), see Roehling (2005). Obviously, it is also not a good announcement for $(8, 4, 4)$.

Apart from the requirement CA4, which for parameters $(a, b, 1)$ amounts to checking whether $\mathcal{L}(\overline{x})$ is a 1-design for arbitrary x, one could imagine strengthening the requirements, for example, demand that $\mathcal{L}(\overline{x})$ is a 2-design for all points x as well. We have already seen that the seven-hand announcement for $(3, 3, 1)$ also satisfies this requirement. We will feature an incidental result for this stronger requirement in the next section, in Proposition 8.

2.2 Theoretical results

Theorem 1 shows that CA4 and CA5 are equivalent; this is followed by a result relating CA4 with t-designs. Our other main results are for the case that $c = 1$: Theorem 4 proves that the pattern required for CA4 is independent from the chosen card (n_x is independent of x), in Theorem 6 we show that binary designs satisfy CA4 if $c = 1$, and in Theorem 7 we show that binary designs are good announcements (i.e., they satisfy CA1, CA2, and CA3) if $c = 1$. There are also some minor results.

Theorem 1. *CA4 if and only if CA5.*

Proof. Assume CA4 holds. Let X be any set of c points. For every line L in $\mathcal{L}(\overline{X})$ there is a b-set $\Omega - X - L$ in $b(\mathcal{L}(\overline{X}))$. Therefore, $|b(\mathcal{L}(\overline{X}))| = |\mathcal{L}(\overline{X})|$. Also, for all points $y \in X$, if $y \in Y \in \mathcal{L}(\overline{X})$ then $y \notin Z \in b(\mathcal{L}(\overline{X}))$ where $Z = \Omega - Y - X$. Point y occurs in n_X lines in $\mathcal{L}(\overline{X})$. It therefore does *not* occur in n_X lines in $b(\mathcal{L}(\overline{X}))$, and it therefore occurs in $|b(\mathcal{L}(\overline{X}))| - n_X$ lines in $b(\mathcal{L}(\overline{X}))$. As this is for arbitrary y, this defines the number m_X. The argument runs both ways. □

In other words, we can forget about CA5 from here on.

Proposition 2. *Let $c = 1$. (CA4 holds and $\mathcal{L}$ is a 1-design) if and only if $\mathcal{L}$ is a 2-design.*

Proof. Assume $\mathcal{L}$ is a 1-design and that CA4 holds, and that $c = 1$. CA4 says that every $\mathcal{L}(\overline{x})$ is a 1-design. Its size $|\mathcal{L}(\overline{x})|$ is independent of x, as $\mathcal{L}$ is a 1-design. For arbitrary $y \in \mathcal{L}(\overline{x})$, $|\mathcal{L}(\overline{x})[y]| + |\mathcal{L}[x + y]| = |\mathcal{L}[y]|$ (note that $|\mathcal{L}[x + y]| = |\mathcal{L}[x][y]|$). As $|\mathcal{L}(\overline{x})[y]|$ and $|\mathcal{L}(y)|$ are independent of x and y (by CA4, and because $\mathcal{L}$ is a 1-design, respectively), so is $|\mathcal{L}[x + y]|$. Therefore $\mathcal{L}$ is a 2-design.

Assume $\mathcal{L}$ is a 2-design, i.e. $|\{L \in \mathcal{L} \mid x, y \in L\}| = \lambda_2$ is independent of x and y. We want to show that $|\{L \in \mathcal{L}(\overline{x}) \mid z \in L\}| = n_x$ is independent of z, for any holding x of Cathy. Note that when she eliminates lines from $\mathcal{L}$ that contain x, she reduces the number of lines containing any $y \neq x$ by λ_2. Let $\lambda_1 = |\{L \in \mathcal{L} \mid y \in L\}|$, which is independent of y because $\mathcal{L}$ is also a 1-design. Before elimination λ_1 lines contained y. After elimination, $\lambda_1 - \lambda_2$ lines contain y. This is the number of lines n_x in $\mathcal{L}(\overline{x})$ that contain y. Since it is independent of y, CA4 holds. □

Proposition 3. *If CA4 holds then $n_X = \frac{a|\mathcal{L}(\overline{X})|}{a+b}$.*

Proof. Count the total number of cards occurring in $\mathcal{L}(\overline{X})$ in two ways. Assuming CA4 holds there are $a + b$ distinct cards and each of them occurs n_X times. There are $|\mathcal{L}(\overline{X})|$ lines and each of them contains a cards. Thus $(a + b)n_X = a|\mathcal{L}(\overline{X})|$. □

Theorem 4. *Let $c = 1$. If CA4 holds then n_x is independent of x.*

Proof. Assume $c = 1$ and CA4 holds. Take two arbitrary distinct $X_1 = \{x_1\}$ and $X_2 = \{x_2\}$. Consider $\mathcal{L}(\overline{x_1})$. It contains no lines that contain card x_1 and n_{x_1} lines that contain card x_2. It must therefore contain $|\mathcal{L}(\overline{x_1})| - n_{x_1}$ lines that contain neither card x_1 nor card x_2. And due to construction of the set, this is the exact number of lines in $\mathcal{L}$ that contain neither card. Now consider $\mathcal{L}(\overline{x_2})$. It contains no lines that contain card x_2 and n_{x_2} lines that contain card x_1. It must therefore contain $|\mathcal{L}(\overline{x_2})| - n_{x_2}$ lines that contain neither card x_1 nor card x_2. And due to construction of the set, this is the exact number of lines in $\mathcal{L}$ that contain neither card. Thus, we get the following equation

$$\begin{aligned}
|\mathcal{L}(\overline{x_1})| - n_{x_1} &= |\mathcal{L}(\overline{x_2})| - n_{x_2} \\
n_{x_1}\frac{a+b}{a} - n_{x_1} &= n_{x_2}\frac{a+b}{a} - n_{x_2} \\
n_{x_1}\left(\frac{a+b}{a} - 1\right) &= n_{x_2}\left(\frac{a+b}{a} - 1\right) \\
n_{x_1}\left(\frac{b}{a}\right) &= n_{x_2}\left(\frac{b}{a}\right) \\
n_{x_1} &= n_{x_2}
\end{aligned}$$

Because x_1 and x_2 were chosen arbitrarily we conclude that n_x is independent of x. □

Directly from Proposition 3 and Theorem 4 follows:

Corollary 5. *Let $c = 1$. If CA4 holds, then $|\mathcal{L}(\overline{x})|$ is independent of x.*

Theorem 6. *Binary designs satisfy CA4 for $c = 1$.*

Proof. Let $\mathcal{L}$ be a binary design. Since $\mathcal{L}$ is a 3-design it is also a 2-design. From that and $c = 1$ it follows by Proposition 2 that CA4 holds. □

Theorem 7. *Binary designs are good announcements for $c = 1$.*

Proof. Let $\mathcal{L}$ be a binary design. We shall prove that the axioms CA1, CA2, and CA3 are satisfied with $a = 2^{n-1}$, $b = 2^{n-1} - 1$, $c = 1$.

CA1: Assume towards a contradiction that more than one line in $\mathcal{L}$ has empty intersection with a given b-set Y. However, two such lines intersect in an $(n-1)$-dimensional affine subspace. Such intersections contain 2^{n-2} points and therefore there are at most $2^n - 2^{n-1} - 2^{n-1} + 2^{n-2} = 2^{n-2}$ points in neither line. This is impossible since $2^{n-1} - 1 > 2^{n-2}$ if $n \geq 3$.

CA2: Because $\mathcal{L}$ is a resolvable design (pairs of a-sets partition the set of cards), every card x occurs in half the number of lines. Suppose some other card y would occur in all lines of $\mathcal{L}(\overline{x})$. As y also occurs in half the number of $\mathcal{L}$ lines, there would be no line wherein x and y both occur. But then, $\mathcal{L}$ would not be a 3-design (or even a 2-design): the pair xy would never occur, nor any triple containing x and y.

CA3: Let x be given. As CA4 is satisfied, $\mathcal{L}(\overline{x})$ is a 1-design with covalency n_x. From Theorem 4 follows that this covalency is independent of x. Also, it is larger than or equal to 1. That means that each other card than x occurs in at least one line in $\mathcal{L}(\overline{x})$, thus $\bigcup \mathcal{L}(\overline{x}) = \overline{x}$. □

We close this section with two additional minor results relating 3-designs, 2-designs, and binary designs.

Proposition 8. *$\mathcal{L}$ is a 3-design if and only if $\mathcal{L}(\overline{x})$ is a 2-design for all points x and $\mathcal{L}$ is a 1-design.*

Proof. Let $\mathcal{L}$ be a 3-design. Trivially, it is also a 2-design, and also a 1-design. The last satisfies one proof obligation. As $\mathcal{L}$ is a 3-design, $|\mathcal{L}[yzx]|$ is independent of y, z, x. As $\mathcal{L}$ is a 2-design, $|\mathcal{L}[yz]|$ is independent of y, z; and therefore independent of y, z, x (note that x does not occur at all in $|\mathcal{L}[yz]|$). As $|\mathcal{L}[yz]| = |\mathcal{L}[yzx]| + |\mathcal{L}[yz](\overline{x})|$, also $|\mathcal{L}[yz](\overline{x})|$ is independent of y, z, x, i.e., for every x, $\mathcal{L}(\overline{x})$ is a 2-design.

Assume $\mathcal{L}(\overline{x})$ is a 2-design for all x, and that $\mathcal{L}$ is a 1-design. Similarly to above it immediately follows that $\mathcal{L}$ is a 3-design. □

Corollary 9. *Binary designs $\mathcal{L}$ satisfy that $\mathcal{L}(\overline{x})$ is a 2-design for all points x.*

Proof. Directly, from Proposition 8 and because binary designs are 3-designs. □

3 Unbiased protocols

In the previous section we focussed on avoiding bias in an announcement. Such bias resulted from the overrepresentation of certain patterns, such as single cards, or pairs of cards, or triples of cards, in the announcement or in the lines of an announcement that avoid a given

c-set (i.e., the eavesdropper's hand of cards). Announcements where arbitrary c-set avoiding lines always are, respectively, 1-designs, or 2-designs, or 3-designs, guarantee that such bias is absent. The implicit assumption that relates the overrepresentation of patterns in an announcement to the probability that this pattern occurs in the actual holding, is that

> *each line in an announcement is equally likely to be the actual holding.*

Given an underlying protocol to produce such an announcement, this is achieved when each announcement resulting from the protocol's execution is equally likely to be produced. In the absence of information to the contrary, that may be a reasonable assumption.

But another way to avoid bias in cryptographic communication is to apply a protocol that takes such overrepresentation of patterns in announcements into account. By making that protocol public, the sender removes the relation between the bias in the announcement and the actual holding—but just as well he may keep it secret, and in that case have a cutting edge over an unsuspecting eavesdropper. In other words, by applying protocols that make some lines in an announcement more likely to be the actual holding than others, the sender can also remove bias. In this section we investigate that matter. Our results are less general than those in the previous section: we present two different 'unbiasing' protocols for parameters $(3, 3, 1)$. To investigate unbiased announcements, we have over 100 years of design theory to comfortably fall back on. But the investigation of unbiased protocols to produce card deal announcements has not been investigated in a combinatorial setting, as far as we know.

3.1 Unbiased protocol for Russian Cards

Given parameters $(3, 3, 1)$, consider again the five-hand announcement $\{012, 034, 056, 135, 246\}$. There are 60 different five-line announcements containing an arbitrary actual hand. We summarize the details found in (van Ditmarsch, 2003, p.56):

> One of the seven points has to occur thrice in the announcement. In case this is one of the **three** actual cards, one of the three lines containing it will be the actual hand, the four remaining points are distributed over the other two of the three. Given an assignment of any of those four, we can choose one of the remaining **three** to match it. That determines the third of those lines too. Suppose that i is the chosen actual card, j, k the other actual cards, and that the other two lines containing it are ilm and ino. Now consider the two lines not containing i. One will contain j, the other k. For the line containing j we can choose one (out of **two**) l, m and one (out of **two**) n, o. That determines the fifth hand too. Altogether:
>
> $$3 \cdot 3 \cdot 2 \cdot 2 = 36.$$
>
> Else, the triple point occurrence is not an actual card, but one of the **four** other points; say l. This fixes the lines not containing that point: one of those is now the actual hand, say ijk again, and the other contains the remaining three points, m, n, o. Consider the three lines containing l. Points (actual cards) i, j, k must be in three different lines containing l. For any of those, we can now choose between **three** of the remaining points m, n, o, and for another of those, between **two** of the points still remaining after that choice. Altogether:
>
> $$4 \cdot 3 \cdot 2 = 24.$$

For an example, if 012 is the actual hand, of the 60 announcements containing 012, 36 contain an actual card 0, 1, or 2 thrice; the remaining 24 contain one of the cards 3, 4, 5, and 6 three times. A point occurring thrice in this five-line announcement is more likely to be an actual card, and the odds are 3 against 2 (36 against 24). A protocol randomly selecting an announcement containing the actual hand therefore propagates this bias, and could rightfully be called a biased protocol. If we choose one from the 36, and one from the 24, and then between those two, we can adjust for this bias. (Where 'choose' mean 'randomly choose'.) We summarize the results:

Definition 3 (bias5: biased five-hand protocol)**.** *Given are parameters* $(3, 3, 1)$*. Given an actual hand, produce the 60 five-hand announcements above, and choose one among them. We call this protocol* bias5*.*

Proposition 10. *If sender Alice executes protocol* bias5 *to produce a good announcement solving* $(3, 3, 1)$*, a point occurring thrice in the announcement is more likely to be a card in her actual holding than not.*

Definition 4 (nobias5: unbiased five-hand protocol)**.** *Given are parameters* $(3, 3, 1)$*. Given an actual hand, choose one among the 36 five-hand announcements containing an actual card thrice, and choose one among the 24 not containing an actual card thrice. Now choose between those two. We call this protocol* nobias5*.*

Proposition 11. *If sender Alice executes protocol* nobias5 *to produce a good announcement solving* $(3, 3, 1)$*, a point occurring thrice in the announcement is equally likely to be a card in her actual holding or not.*

3.2 Unbiased protocol for Russian Cards, with designated point

Given that one point occurs thrice in a five-line announcement and that this must be meaningless information, sender Alice might as well make *public* which point that will be before being dealt a hand of cards. We call this card the *special point*. She can then execute a protocol that results in an announcement containing her actual hand and the pre-announced point, whether it is in the actual hand or not. (Pre-announcing the point was suggested by Ron van der Meyden.)

Given an arbitrary point and an arbitrary line (actual hand), the probability that that point avoids that line is $\frac{6}{7} \cdot \frac{5}{6} \cdot \frac{4}{5} = \frac{4}{7}$, so that the probability that the point is in the line, is $\frac{3}{7}$.

There are twelve announcements where the pre-announced point is an actual card, and six where this is not the case. This we can see as follows. In the first case, as before, the four remaining points are distributed over the other two of the three: $3 \cdot 2 \cdot 2 = 12$. Else, also as before, each of the three actual cards *must* be in three different lines containing the preselected point, for which our options are: $3 \cdot 2 = 6$. In that case, the fifth line is the (unique) line not containing the actual points nor the preselected point.

For an example, let 0 be the publicly known thrice occurring point, let in the first case 012 be the arbitrary line containing 0, and let in the second case 135 be the arbitrary line not containing 0 (so that this fixes the other line not containing 0 to 246). Then the twelve announcements are:

012 034 056 135 246	012 034 056 136 245
012 034 056 145 236	012 034 056 146 235
012 035 046 134 256	012 035 046 136 245
012 035 046 145 236	012 035 046 156 234
012 036 045 134 256	012 036 045 135 246
012 036 045 146 235	012 036 045 156 234

and the 6 announcements are:

012 034 056 135 246	012 036 045 135 246
014 023 056 135 246	014 025 036 135 246
016 023 045 135 246	016 025 034 135 246

As $12 \cdot \frac{3}{7} = \frac{36}{7}$, and $6 \cdot \frac{4}{7} = \frac{24}{7}$, then if we randomly select among these 18 our bias is as before: the odds are 3 to 2 that a point occurring in an announcement is an actual card. This protocol was implemented in the model checker MCK to solve 'Russian Cards', see (van Ditmarsch *et al.*, 2006), because its time complexity is lower than that of the protocol bias5 without special card.

Again, we can adjust the protocol, in this case by choosing with probability $\frac{4}{7}$ an announcement among the twelve and with probability $\frac{3}{7}$ an announcement among the six. We summarize our results.

Definition 5 (bias5sp: biased five-hand protocol with special point)**.** *Given are parameters* $(3, 3, 1)$*. Given a special point and an actual hand, produce the 18 five-hand announcements as above, and choose one among them. We call this protocol* bias5sp*.*

Proposition 12. *If sender Alice executes protocol* bias5sp *to produce a good announcement solving* $(3, 3, 1)$*, a point occurring thrice in the announcement is more likely to be a card in her actual holding than not.*

Definition 6 (nobias5sp: unbiased five-hand protocol with special point)**.** *Given are parameters* $(3, 3, 1)$*. Given a special point and an actual hand, choose one among the 12 five-hand announcements containing an actual card thrice, and choose one among the 6 not containing an actual card thrice. Choose between those two with probability* $\frac{4}{7}$ *for the first and* $\frac{3}{7}$ *for the second. We call this protocol* nobias5sp*.*

Proposition 13. *If sender Alice executes protocol* nobias5sp *to produce a good announcement solving* $(3, 3, 1)$*, a point occurring thrice in the announcement is equally likely to be a card in her actual holding or not.*

3.3 Strategic behaviour for protocol disclosure

We close with an additional observation on the status of such protocols. If they are *public*, the combination of the protocol and a resulting announcement makes that announcement unbiased *for an eavesdropper* with regard to single point occurrence. If they are not public, but, for example, only known between sender and receiver, the situation becomes much more complex. For example, in the absence of information to the contrary, the eavesdropper may *incorrectly assume* that each line in an announcement is equally likely, and from that *correctly infer* that

a thrice occurring point is therefore more likely to be an actual card. But this conclusion is then false. Also, if the sender assumes that the eavesdropper follows that line of argument, it would even make sense not to apply an unbiased protocol, but one that is even biased the other way, namely towards triple occurrence of points that are *not* actual points. Then again, the eavesdropper may anticipate such behaviour of the sender, etc. In other words, the optimal strategies for sender and eavesdropper under conditions where announcements are always truthful but knowledge of applied protocols is incomplete, are unclear.

On the other hand, incomplete knowledge of a protocol is an unreasonable assumption in our current setting: given the 'worst case' assumption where eavesdroppers intercept the entire communication, in other words, where it is a public communication, we might as well assume the 'worst case' concerning protocol knowledge: the protocol is public.

4 Conclusions

We outlined the need for stricter requirements for cryptographic protocols inspired by the Russian Cards problem than the requirements CA1-CA3 and we proposed a new requirement CA4. This CA4 is shown to be equivalent to an alternative formulation CA5. Announcements satisfying CA4 are 2-designs. We also introduced binary designs and showed that these satisfy CA1-CA4. Instead of avoiding bias in announcements produced by protocols, one also adjust the protocol such the relation between patterns in announcements and the actual hand disappears. We gave two examples of such protocols for card deal parameters $(3, 3, 1)$.

References

Agrawal, M., Kayal, N., and Saxena, N. (2004). PRIMES is in P. *Annals of Mathematics*, *160(2)*, 781–793.

Albert, M., Aldred, R., Atkinson, M., van Ditmarsch, H., and Handley, C. (2005). Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, *33*, 33–46.

Bose, R. C. (1939). On the construction of balanced incomplete block designs. *Annals of Eugenics*, *9*, 353–399.

Colbourn, C. and Dinitz, J. (1996). *CRC Handbook of Combinatorial Designs*. Boca Raton, FL, USA: CRC Press. Discrete Mathematics and Its Applications Volume: 42.

Dembowski, P. (1997). *Finite geometries*. Classics in Mathematics. Berlin: Springer-Verlag. Reprint of the 1968 original.

Fischer, M. and Wright, R. (1996). Bounds on Secret Key Exchange Using a Random Deal of Cards. *Journal of Cryptology*, *9(2)*, 71–99.

Hughes, D. (1962). t-designs and permutation groups. In *Proceedings of Symposia in Pure Mathematics*, 39–41. American Mathematical Society.

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

Roehling, S. (2005). Cards and Cryptography. Report in partial fulfilment of MSc in Computer Science, University of Otago.

Stiglic, A. (2001). Computations with a deck of cards. *Theoretical Computer Science*, *259*(1–2), 671–678.

Stinson, D. (2004). *Combinatorial Designs – Constructions and Analysis*. Springer.

van Ditmarsch, H. (2003). The Russian cards problem. *Studia Logica*, *75*, 31–62.

van Ditmarsch, H. (2005). The case of the hidden hand. *Journal of Applied Non-Classical Logics*, *15(4)*, 437–452.

van Ditmarsch, H., van der Hoek, W., van der Meyden, R., and Ruan, J. (2006). Model Checking Russian Cards. *Electronic Notes in Theoretical Computer Science*, *149*, 105–123. Presented at MoChArt 05 (Model Checking in Artificial Intelligence).

Vasilenko, O. (2006). *Number-theoretic Algorithms in Cryptography (Translations of Mathematical Monographs)*. Boston, MA, USA: American Mathematical Society.

Wallis, W. (1988). *Combinatorial Designs*. New York: M. Dekker.

Yates, F. (1936). Incomplete randomized blocks. *Annals of Eugenics*, *7*, 121–140.