Designs, Codes and Cryptography (2022) 90:593–632
https://doi.org/10.1007/s10623-021-00994-1

Mosaics of combinatorial designs for information-theoretic security

Moritz Wiese[1,2] · **Holger Boche**[1,2,3]

Received: 25 June 2021 / Revised: 8 December 2021 / Accepted: 14 December 2021 /
Published online: 5 January 2022
© The Author(s) 2021

Abstract
We study security functions which can serve to establish semantic security for the two central problems of information-theoretic security: the wiretap channel, and privacy amplification for secret key generation. The security functions are functional forms of mosaics of combinatorial designs, more precisely, of group divisible designs and balanced incomplete block designs. Every member of a mosaic is associated with a unique color, and each color corresponds to a unique message or key value. Every block index of the mosaic corresponds to a public seed shared between the two trusted communicating parties. The seed set should be as small as possible. We give explicit examples which have an optimal or nearly optimal trade-off of seed length versus color (i.e., message or key) rate. We also derive bounds for the security performance of security functions given by functional forms of mosaics of designs.

Keywords Wiretap channel · Privacy amplification · Semantic security · Mosaic of designs · Balanced incomplete block design · Group divisible design

Mathematics Subject Classification 05B30 · 05B05 · 94A40 · 94A62

Communicated by C. J. Colbourn.

Part of this work has been presented at the IEEE International Symposium on Information Theory 2021. The conference version only treats the privacy amplification case and refers to the preprint of this paper at https://arxiv.org/abs/2102.00983v1 for details. It contains a shortened introduction. Of Sect. 2, it only contains Sect. 2.1 and examples $\mathcal{M}^{(1)}$ and $\mathcal{M}^{(4)}$ from Sect. 2.6. Of the results of Sect. 3, only Lemma 3.5 and Theorem 3.7 are stated and proved. Section 5 is omitted completely.

✉ Moritz Wiese
wiese@tum.de

Holger Boche
boche@tum.de

1 Institute of Theoretical Information Technology, Technical University of Munich, Arcisstraße 21, 80333 München, Germany

2 CASA: Cyber Security in the Age of Large-Scale Adversaries Exzellenzcluster, Ruhr-Universität Bochum, Room MC 0/75, Universitätsstraße 150, 44780 Bochum, Germany

3 BMBF Research Hub 6G-Life, Technical University of Munich, Arcisstraße 21, 80333 München, Germany

1 Introduction

1.1 Two problems of information-theoretic security

A *channel* $W : \mathcal{X} \to \mathcal{Z}$ is a stochastic matrix W with rows indexed by the finite *input alphabet* $\mathcal{X}$ and columns indexed by the finite *output alphabet* $\mathcal{Z}$. The (x, z) entry is nonnegative and denoted by $w(z|x)$. The sum of the entries of every row sums to 1, hence it defines a probability distribution on $\mathcal{Z}$. For the purpose of this paper, a *wiretap channel* is determined by a single channel W. The interpretation is that a sender, Alice, wants to transmit a confidential message to a receiver, Bob, through a channel which accepts inputs from $\mathcal{X}$ and whose output is identical to the input, or whose error probability is as small as desired. An eavesdropper, Eve, obtains a noisy version of the input symbol $x \in \mathcal{X}$ through the channel W, in other words, she observes a random variable distributed according to $w(\cdot|x)$. The task now is to devise a *security code* for the transmission of confidential messages which does not decrease the reliability of the channel to Bob, and which at the same time ensures that Eve learns nothing about the transmitted messages. In fact, we aim for *semantic security*, by which we loosely mean that the security code should guarantee security no matter how the message is distributed on the message set. Two possible rigorous definitions of this concept will be given below. They guarantee *unconditional security*, which means that no assumptions are made on Eve's computing power.

Another problem from information-theoretic security is *privacy amplification*. Here, Alice and Bob share a random variable X living on a finite set $\mathcal{X}$. Eve, the adversary, has access to a discrete random variable Z correlated with X. The task is to apply a *privacy amplification function* to X such that the resulting random variable A (the *secret key* shared by Alice and Bob) is distributed approximately uniformly and such that Eve has no information about A. Again, the goal is to achieve semantic security. Although all distributions are fixed in this setting, it makes sense to require semantic security. For instance, it guarantees that even if Eve has the a priori knowledge that the key generated in the privacy amplification process has one of only two possible values, she is unable to tell which of these two is the one actually chosen. This property is sometimes called *distinguishing security*, but it is well-known that it is equivalent to unconditional semantic security [4].

Practical scenarios will not in general translate directly into one of the two problems described above. In the wiretap scenario, the physical channel from Alice to Bob will generally be noisy as well, and an error-correcting code needs to be applied first to make the error probability on this channel as small as possible. In this case, the input alphabet $\mathcal{X}$ actually is the message set of the error-correcting code. Similarly, in secret key generation, two remote parties will not in general share a random variable X from the outset. In order to establish such a random variable, an *information reconciliation* protocol has to be performed using communication over a public channel. Eve obtains at least part of her correlated information Z about X as she observes the public messages exchanged during information reconciliation.

It follows that a security code or a privacy amplification function will generally be just one component of a modular scheme which as a whole ensures both "reliability" (viz. error-correction or information reconciliation) and semantic security as well as, in the privacy amplification setting, approximately uniform key distribution.

The two problems above are key techniques for the generation of information-theoretic security in communication and data storage systems. They can be building blocks for embedded security and security-by-design of such systems. An important feature of information-theoretic security is that it provides provable security even against attacks per-

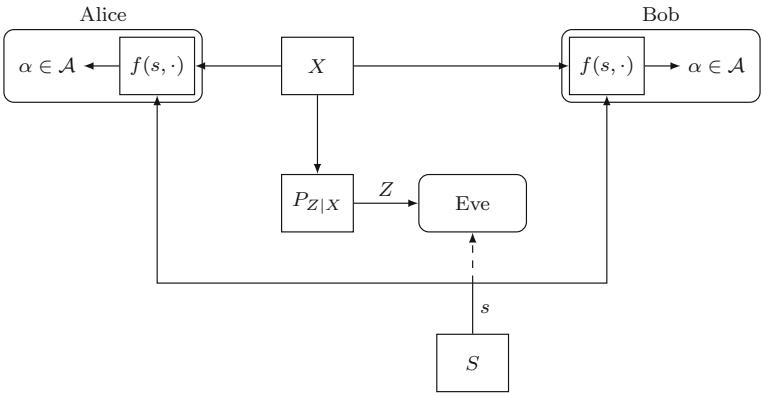

Fig. 1 The privacy amplification scenario. The correlation between X and Eve's observation Z here is represented by the conditional probability $P_{Z|X}$. Alice and Bob are usually assumed to be connected by a public channel over which they can exchange messages. In particular, they can use this channel to share the seed. The arrow from S to Eve is dashed because Eve may know the seed, but this is not necessary for the operability of the protocol

formed by a quantum computer. For this reason, the techniques developed here are of great importance for the development of future 6G mobile communication systems [16]. A first practical implementation is presented in [31].

1.2 Security functions

Both for the wiretap and the privacy amplification scenario, we will assume that Alice and Bob can share an additional resource, a publicly known *seed* s chosen uniformly at random from the finite seed set $\mathcal{S}$. Then the basis both for security codes and privacy amplification functions are onto functions $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$, where $\mathcal{A}$ is a finite set. We will call such a function a *security function*. In the wiretap scenario, $\mathcal{A}$ will be the set of confidential messages; in privacy amplification, it represents the range of possible key values. In fact, in privacy amplification, f is nothing else than the privacy amplification function, i.e., given a seed $s \in \mathcal{S}$ and a realization $x \in \mathcal{X}$ of the random variable X shared by Alice and Bob, the secret key is chosen to be $f(x, s)$ (see Fig. 1). For the wiretap channel, if Alice wants to send a confidential message $\alpha \in \mathcal{A}$ and shares the seed s with Bob, she selects an element x from the preimage $f_s^{-1}(\alpha) = \{x : f(x, s) = \alpha\}$ uniformly at random and transmits x. We call this process of selecting x the *randomized inverse* of f. By assumption, with high probability, or even with certainty, Bob receives the x that was sent and decodes it into the original confidential message $\alpha = f(x, s)$, so the reliability of message transmission is preserved (see Fig. 2).

The *color rate* of a security function $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$, both in the wiretap and in the privacy amplification context, is given by[1]

$$\varrho = \frac{\log|\mathcal{A}|}{\log|\mathcal{X}|}$$

(the name will be justified in the context of mosaics, see below). As f is onto, this is a number between 0 and 1 which indicates the cost of establishing security as well as, in the privacy

[1] Throughout the paper, log will denote the logarithm to base 2. When we write $\exp(x)$, we mean 2^x.

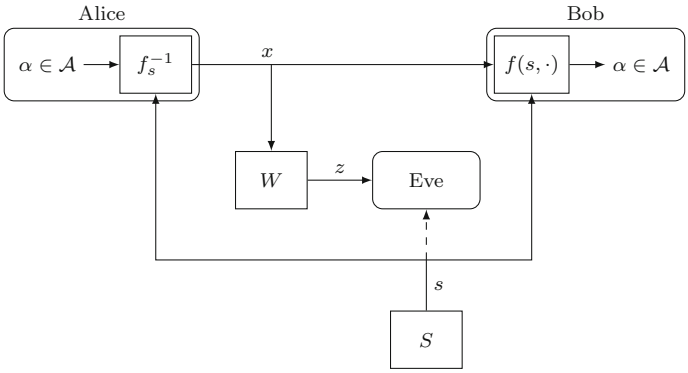

Fig. 2 The wiretap scenario in the case where the channel between Alice and Bob is the identity channel. In principle, it is immaterial where the seed is generated. In practice, Alice will generate the seed and transmit it to Bob publicly. The arrow from S to Eve is dashed because Eve may know the seed, but this is not necessary for the operability of the protocol

amplification scenario, approximately uniform key distribution. This is not a parameter to be optimized. Instead, given a required security level, the channel W in the former and the joint probability P_{XZ} in the latter situation determine a maximal possible color rate. The question is which f achieve or come close to this rate.

In the wiretap case, a common assumption is that Alice generates the seed, but then she has to use the unsecured channel to transmit it to Bob. This diminishes the overall communication rate significantly. The *block rate*

$$\frac{\log|\mathcal{S}|}{\log|\mathcal{X}|}$$

indicates how often the unsecured channel needs to be used for the transmission of the seed. It has been shown that in some scenarios the seed can be reused in order to make the loss of overall communication rate negligibly small asymptotically. Nevertheless, it is important to make the seed set $\mathcal{S}$ as small as possible.

The use of a seed is not as problematic in the privacy amplification setting, since it is commonly assumed that there exists a public channel between Alice and Bob. For the purpose of seed sharing, it is sufficient that the public channel goes in one direction only. Usually, one still wants to keep the communication overhead on this public channel small, and this overhead can again be measured by the block rate.

Finally, we would like security codes and privacy amplification functions to be efficiently computable. For an underlying security function, this translates to the efficiency of computing $f(x, s)$ and the randomized inverse $f_s^{-1}(\alpha)$. A precise definition of what we mean by efficiency will be given below.

1.3 Semantic security by mosaics of designs

Semantic security can be seen as a per-message type of security. It means that the probability distribution of Eve's observations conditional on any message or key value should be indistinguishable from an arbitrary fixed distribution on Eve's observation space which is independent of the message or key distribution. This suggests to construct security functions

$f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ whose preimages $f^{-1}(\alpha)$ for every $\alpha \in \mathcal{A}$ have a structure suitable for establishing this indistinguishability.

Our goal in this paper is to systematically study security functions where every preimage $f^{-1}(\alpha)$ is the incidence relation of a balanced incomplete block design (BIBD) or a group divisible design (GDD) with point set $\mathcal{X}$ and block index set $\mathcal{S}$. Such a function defines a *mosaic of designs* $(D_\alpha)_{\alpha\in\mathcal{A}}$, which is a family of designs on a common point set and a common block index set satisfying that every pair $(x, s) \in \mathcal{X} \times \mathcal{S}$ is incident in a unique D_α. The security function corresponding to such a mosaic will be its *functional form*. The precise definitions will be given in Sect. 2.

Two aspects guide us in the construction of mosaics of designs: the trade-off of the color rate and the block rate, and the computational complexity of the functional form and its randomized inverse. We investigate the optimal trade-off of the color rate ϱ vs. the block rate for functional forms of mosaics of BIBDs and GDDs. For mosaics of BIBDs with small color rate, the block rate can at best be equal to 1. In all other cases, the minimal block rate is approximately equal to 2ϱ. In particular, if $\varrho < 1/2$ and the mosaic consists of GDDs, then a block rate smaller than 1 is possible.

We construct families of examples which are close to optimal, or even optimal, in terms of this trade-off. Their color rates are distributed over the complete interval between 0 and 1, densely in all cases except for BIBDs of small color rate. Both for mosaics of BIBDs and GDDs, we need two different families in order to obtain sufficiently variable color rates ϱ. In both cases, at $\varrho \approx 1/2$, the type of designs which is (close to) optimal in terms of this trade-off changes.

To the best of our knowledge, we are the first to explicitly study semantic security for privacy amplification. In both scenarios, we measure the amount of semantic security offered by the functional form of a mosaic of BIBDs or GDDs using two alternative security metrics, one of them based on total variation distance, the other on Kullback-Leibler divergence. The upper bounds on these metrics rely on the local properties of the functional form, i.e., on the properties of BIBDs and GDDs. The wiretap channel and the distribution of the random variables X and Z only appear in these bounds through at most two Rényi entropies or divergences, which gives the bounds some robustness with respect to the knowledge about the channel or the random variables.

We evaluate the security bounds in the most frequently studied scenarios of memoryless discrete or Gaussian wiretap channels and of privacy amplification for secret-key generation from discrete memoryless correlated sources. Unfortunately, block rate optimal mosaics of GDDs in the range where ϱ is small only achieve a suboptimal security level in general. This is not due to our construction, but holds in general. Hence a block rate of at least 1 is necessary to achieve asymptotically perfect semantic security at the maximal message or key rate with mosaics of BIBDs or GDDs. For the other block rate optimal constructions, the bounds are asymptotically optimal in the benchmark scenarios. Additionally, in the case of privacy amplification, the regularity of BIBDs and GDDs immediately implies the perfect uniform distribution of the key generated by the functional form of a mosaic of designs.

All the mosaics we construct are explicit, by which we mean the efficient computability of the functional form and its inverse in the usual setting of asymptotic complexity. The examples are derived from well-known designs based on finite fields, so in some cases the explicitness is obvious. There is one case where some work is required to show explicitness.

1.4 Related literature

Mosaics of combinatorial designs were introduced by Gnilke, Greferath and Pavčević [17]. Our method of constructing mosaics from resolvable designs or duals thereof is essentially due to them. The application of mosaics to construct functions with special desired properties is new, in particular, the analysis of color and block rates and of efficient computability of such functions. Mosaics generalize more specialized concepts like the tiling of a group with difference sets due to Ćustić, Krčadinac and Zhou [14]. A predecessor of what now is called mosaics was presented in [18] by Greferath and Therkelsen. General background on combinatorial designs can be found in the reference work of Beth, Jungnickel and Lenz [8].

The idea of separating privacy amplification from information reconciliation goes back to Bennett, Brassard and Robert [6] and Bennett, Brassard, Crépeau and Maurer [7]. Hayashi [21] extended the idea to the construction of security codes for the wiretap channel, where error correction is separated from the establishment of security. Like in [6,7] and [21], the weaker *strong secrecy* criterion has been widely applied in information-theoretic security, where Eve's a priori knowledge is restricted to the true message or key distribution.

Semantic security ensures security no matter what the key or message distribution might be. Originating in complexity-based cryptography, it was adapted for (unconditional) information-theoretic security by Bellare, Tessaro and Vardy [4] (the shorter, published version of which is [3]). To the authors' knowledge, semantic security has only been considered for wiretap channels so far. In [20], Hayashi implicitly describes a technique for achieving semantic security for the quantum BB84 key distribution protocol.

[6,7] and [21] used universal hash functions as security functions. Alternative choices in the privacy amplification scenario with strong secrecy are ε-almost dual universal hash functions (Hayashi [22]) and strong randomness extractors (Maurer and Wolf [25]). None of these choices guarantees perfect uniform distribution of the key. However, the seed required by randomness extractors can be very short. Seedless extractors have been used by Cheraghchi, Didier and Shokrollahi [11] to ensure strong secrecy for the "wiretap channel II", where the eavesdropper may observe a fraction of his choosing of the transmitted codeword.

When applied as security functions in the wiretap scenario, it seems that the global property defining universal hash functions in general is not enough to ensure semantic security. Even with additional regularity properties (cf. [5,32]), semantic security can only be shown for sufficiently symmetric channels. Usually, only strong secrecy is achievable.

Upper bounds on the semantic security metric for the wiretap channel which are comparable to ours were given by Hayashi and Matsumoto [23, Lemma 21] and the authors [34], using security functions of a different type. The security functions of the former paper are defined in terms of group homomorphisms together with a regularity condition. The single efficiently computable example given in [23, Remark 16] exhibits a block rate ≈ 2, which is worse than for mosaics of designs with an optimal trade-off of block rate vs. color rate. The security functions of [34] are induced by decompositions of complete biregular bipartite graphs into nearly Ramanujan graphs. A nonconstructive example of such a decomposition into Ramanujan graphs is given with a block rate of 1 independent of the color rate.

1.5 Outline

In Sect. 2, we define and analyze mosaics of BIBDs and GDDs. In Sect. 3, we define how we measure semantic security and give the bounds on the security metrics obtained from functional forms of mosaics of designs. These bounds are proved in Sect. 4. In Sect. 5, we

prove the explicitness of one of the examples of Sect. 2 for which this is not immediately obvious.

2 Mosaics of combinatorial designs

2.1 Definitions

Let $\mathcal{X}$ and $\mathcal{S}$ be finite sets. An *incidence structure* $D = (\mathcal{X}, \mathcal{S}, I)$ on $(\mathcal{X}, \mathcal{S})$ is determined by the *incidence relation* I on $\mathcal{X} \times \mathcal{S}$. An incidence structure $(\mathcal{X}, \mathcal{S}, I)$ is called *empty* if $I = \emptyset$. If $x\, I\, s$, then x and s are called *incident*. The *incidence matrix* of an incidence structure $D = (\mathcal{X}, \mathcal{S}, I)$ is the 01-matrix N with rows indexed by $\mathcal{X}$ and columns indexed by $\mathcal{S}$ such that $N(x, s) = 1$ if and only if x and s are incident in D.

A *mosaic of incidence structures* on $(\mathcal{X}, \mathcal{S})$ is a family $M = (D_\alpha)_{\alpha \in \mathcal{A}}$ of nonempty incidence structures on $(\mathcal{X}, \mathcal{S})$ such that for every pair (x, s) there exists a unique incidence structure D_α in which x and s are incident. We call $\mathcal{A}$ the *color set* of M. Every D_α is called a *member* of M. If N_α is the incidence matrix of D_α, then $\sum_{\alpha \in \mathcal{A}} N_\alpha = J$, the all-ones matrix of appropriate size.

Any function $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ induces a mosaic $(D_\alpha)_{\alpha \in \mathcal{A}}$ of incidence structures, where x and s are incident in D_α if and only if $f(x, s) = \alpha$. We say that f is the *functional form* of this mosaic. Clearly, every mosaic $(D_\alpha)_{\alpha \in \mathcal{A}}$ on $(\mathcal{X}, \mathcal{S})$ has a functional form $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$.

We consider the case where every D_α is a combinatorial design. In the context of designs, we will call $\mathcal{X}$ the *point set* and $\mathcal{S}$ the *block index set*. We set $v = |\mathcal{X}|$ and $b = |\mathcal{S}|$. A (v, k, r) *tactical configuration* on $(\mathcal{X}, \mathcal{S})$ is an incidence structure where every point x is incident with precisely r block indices and every block index s is incident with precisely k points. It holds that

$$bk = vr. \tag{2.1}$$

A (v, k, λ) *balanced incomplete block design (BIBD)* on $(\mathcal{X}, \mathcal{S})$ is an incidence structure on $(\mathcal{X}, \mathcal{S})$ such that every s is incident with precisely k points from $\mathcal{X}$ and such that any two distinct points from $\mathcal{X}$ are incident with precisely $\lambda \geq 1$ common block indices. Every (v, k, λ) BIBD is a (v, k, r) tactical configuration, where

$$r(k-1) = \lambda(v-1). \tag{2.2}$$

The key equality when we want to establish security using a security function which is the functional form of a mosaic of BIBDs is that the incidence matrix N of a (v, k, λ) BIBD satisfies

$$NN^T = (r - \lambda)I + \lambda J \tag{2.3}$$

(here I is the identity matrix of appropriate dimensions).

The second type of designs we consider are *group divisible designs (GDDs)*. A $(u, m, k, \lambda_1, \lambda_2)$ GDD is based on a partition of $\mathcal{X}$ into m *point classes* of size u each, so $v = um$. Every block index is incident with precisely k points, and two points are incident with $\lambda_1 \geq 0$ common block indices if they are contained in the same point class and with $\lambda_2 \geq 1$ block indices otherwise. A $(u, m, k, \lambda_1, \lambda_2)$ GDD is a (v, k, r) tactical configuration for r satisfying

$$r(k-1) = \lambda_1(u-1) + \lambda_2(m-1)u. \tag{2.4}$$

An equality similar to (2.3) holds for the incidence matrix N of a GDD. Let C be the 01-matrix with rows and columns indexed by $\mathcal{X}$ which has a 1 in the (x, x') entry if and only if x and x' are contained in the same point class. With a suitable ordering of the elements of $\mathcal{X}$, this is a block diagonal matrix with m all-ones matrices of size u each on the diagonal. Then

$$NN^T = (r - \lambda_1)I + (\lambda_1 - \lambda_2)C + \lambda_2 J. \tag{2.5}$$

For a BIBD or GDD $(\mathcal{X}, \mathcal{S}, I)$, the sets of the form $\{x : x\, I\, s\}$, where $s \in \mathcal{S}$, are usually called *blocks* and the set $\mathcal{S}$ is identified with the multiset of blocks of the design. Occasionally, we will also speak of blocks and call the parameter k the *block size*. However, we will not identify $\mathcal{S}$ with a block multiset since we operate with multiple designs simultaneously. Hence the more cumbersome term "block index set".

All mosaics in this paper will consist of tactical configurations with the same parameters (v, k, r). Given a mosaic $(D_\alpha)_{\alpha\in\mathcal{A}}$, we will use the letter a to indicate the cardinality of its color set $\mathcal{A}$. If $(D_\alpha)_{\alpha\in\mathcal{A}}$ is a mosaic of (v, k, r) tactical configurations, then

$$a = \frac{v}{k}.$$

In fact, the examples of mosaics constructed in the present paper will exclusively consist of BIBDs only or of GDDs only. BIBDs and GDDs together allow us to construct security functions with a wide range of color rates between 0 and 1. For a mosaic of BIBDs with constant block size k, note that λ also has to be constant due to (2.1) and (2.2).

2.2 Some properties and examples of designs

If $D = (\mathcal{X}, \mathcal{S}, I)$ is an incidence structure, then its *dual* is the incidence structure $D^T = (\mathcal{S}, \mathcal{X}, I^T)$ where $s\, I^T\, x$ if and only if $x\, I\, s$. Obviously, the incidence matrix of D^T is the transpose of the incidence matrix of D. If $(D_\alpha)_{\alpha\in\mathcal{A}}$ is a mosaic of designs, then so is $(D_\alpha^T)_{\alpha\in\mathcal{A}}$.

A (v, k, r) tactical decomposition $(\mathcal{X}, \mathcal{S}, I)$ is called *resolvable* if the block index set $\mathcal{S}$ can be partitioned into subsets $\mathcal{S}_1, \ldots, \mathcal{S}_r$ such that for every $j \in \{1, \ldots, r\}$, every $x \in \mathcal{X}$ is incident with a unique $s \in \mathcal{S}_j$. (It is clear that such a partition necessarily has to have precisely r elements.) Every $\mathcal{S}_j$ is called a *parallel class* and contains v/k block indices, in particular, k divides v.

The *sum* of a mosaic is the incidence structure on $(\mathcal{X}, a\mathcal{S})$, where $a\mathcal{S}$ is the disjoint union of a copies of $\mathcal{S}$, and where a point x is incident with the α-th copy of $s \in \mathcal{S}$ if x and s are incident in D_α. Note that the sum of a mosaic of tactical configurations is resolvable.

Two incidence structures $(\mathcal{X}, \mathcal{S}, I)$ and $(\mathcal{X}', \mathcal{S}', I')$ are called *isomorphic* if there exist bijective mappings $\Phi_\mathcal{X} : \mathcal{X} \to \mathcal{X}'$ and $\Phi_\mathcal{S} : \mathcal{S} \to \mathcal{S}'$ such that $x\, I\, s$ if and only if $\Phi_\mathcal{X}(x)\, I'\, \Phi_\mathcal{S}(s)$. We also define that two mosaics $(D_\alpha)_{\alpha\in\mathcal{A}}$ on $(\mathcal{X}, \mathcal{S})$ and $(D'_{\alpha'})_{\alpha'\in\mathcal{A}'}$ on $(\mathcal{X}', \mathcal{S}')$ are isomorphic if there exist bijective mappings $\Phi_\mathcal{X} : \mathcal{X} \to \mathcal{X}'$ and $\Phi_\mathcal{S} : \mathcal{S} \to \mathcal{S}'$ and $\Phi_\mathcal{A} : \mathcal{A} \to \mathcal{A}'$ such that $x \in \mathcal{X}$ and $s \in \mathcal{S}$ are incident in D_α for $\alpha \in \mathcal{A}$ if and only if $\Phi_\mathcal{X}(x)$ and $\Phi_\mathcal{S}(s)$ are incident in $D_{\Phi_\mathcal{A}(\alpha)}$.

A BIBD is called *affine* or *affine resolvable* if it is resolvable and if there exists a number $\mu > 0$ such that any two distinct non-parallel blocks have precisely μ points in common. An *affine plane* is an affine BIBD with $\mu = 1$ and block size at least 2. Affine BIBDs have the property that their number of blocks is minimal among all resolvable BIBDs with the same number of points and parallel classes. This is a consequence of Bose's inequality, which states that

$$b \geq v + r - 1 \tag{2.6}$$

for resolvable BIBDs [8, Corollary 8.6], and that equality holds if and only if the BIBD is affine.

Here we give the classical examples of affine designs, on which our constructions below will be based. This is no restriction, since all known affine BIBDs have the same parameters as the affine-geometric ones below or are Hadamard designs [8, p. 128]. We ignore the latter since they are limited to $v/k = a = 2$, which only allows a very small color rate which vanishes asymptotically as v increases.

Let q be a prime power and $t \geq 2$. The (q^t, q^{t-1}, q^{t-2}) BIBD $AG_{t-1}(t, q)$ has as block set the vector space $\mathbb{F}_q^t$, the blocks are given by the hyperplanes of this vector space, i.e., all cosets of all $(t-1)$-dimensional subspaces, and the incidence relation is $\in$. These designs are affine resolvable, the parallel classes are given by the sets of nonintersecting hyperplanes. In the case $t = 2$, one obtains the affine plane $AG(2, q)$, where the hyperplanes are called *lines*.

2.3 Block rate optimality

We characterize block rate optimality for mosaics of BIBDs and GDDs.

Lemma 2.1 *Let $(D_\alpha)_{\alpha \in \mathcal{A}}$ be a mosaic of (v, k, λ) BIBDs with $a \geq 2$ and color rate ϱ. Then*

$$b \geq \max\left\{\frac{(v-1)ka^2}{v(k-1)}, v\right\}. \tag{2.7}$$

Setting

$$\varrho_0(v, k) = 1 - \frac{\log(v-1) + \log k - \log(k-1)}{2\log v},$$

then this means for the block rate that

$$\frac{\log b}{\log v} \begin{cases} > 2\varrho & \text{if } \varrho > \varrho_0(v, k), \\ \geq 1 & \text{if } \varrho \leq \varrho_0(v, k). \end{cases} \tag{2.8}$$

If $\varrho \geq \varrho_0(v, k)$, then equality holds in (2.7) if and only if $\lambda = 1$. If $\varrho < \varrho_0(v, k)$, then equality holds in (2.7) and (2.8) if and only if $b = v$. We call a mosaic of (v, k, λ) BIBDs satisfying equality in one of these two cases block rate optimal.

Proof Using (2.1) and (2.2),

$$b = ra = \frac{\lambda(v-1)a}{k-1} \geq \frac{(v-1)ka^2}{v(k-1)}.$$

Clearly, equality holds if and only if $\lambda = 1$. The well-known Fisher's inequality [8, Theorem II.2.6] for BIBDs states $b \geq v$ if $k < v$, which settles (2.7).

For the proof of (2.8), observe that since $a = v^\varrho$, the maximum in (2.7) is v if and only if $\varrho \leq \varrho_0(v, k)$. If $\varrho > \varrho_0(v, k)$, then strict inequality has to hold due to $v > k$. □

We note that $\varrho_0(v, k)$ quickly approaches $1/2$ from below as v increases.

We also consider the block rate for GDDs. This is connected to some subclasses of GDDs. First, we recall the classification of GDDs due to Bose and Connor [10]. A GDD is called

1) *singular* if $r = \lambda_1$,
2) *semi-regular* if $r > \lambda_1$ and $rk = v\lambda_2$,

3) *regular* if $r > \lambda_1$ and $rk > v\lambda_2$.

Every GDD falls under exactly one of these categories.

An important subclass of the semi-regular GDDs are the *transversal designs*, which satisfy that every block intersects every point class in precisely one point. In this case $m = k$ and $\lambda_1 = 0$. We call a transversal design with these parameters a (u, k, λ) TD, where $\lambda = \lambda_2$. Hanani [19] has shown that a (u, k, λ) TD necessarily satisfies

$$k \leq \frac{\lambda u^2 - 1}{u - 1}. \tag{2.9}$$

Lemma 2.2 *Let $(D_\alpha)_{\alpha \in \mathcal{A}}$ be a mosaic of GDDs of constant block size k and of color rate ϱ. Then*

$$\frac{\log b}{\log v} \geq 2\varrho.$$

Equality holds if and only if every D_α is an $(a, k, 1)$ TD. We call such a mosaic block rate optimal.

Proof The parameters v, b, k, r are the same for all members of the mosaic. Choose any $\alpha \in \mathcal{A}$ and assume that D_α is a $(u_\alpha, m_\alpha, k, \lambda_{1,\alpha}, \lambda_{2,\alpha})$ GDD. By (2.4)

$$\begin{aligned} b &= ra \\ &= \frac{\lambda_{1,\alpha}(u_\alpha - 1) + \lambda_{2,\alpha} u_\alpha (m_\alpha - 1)}{k - 1} a \\ &\geq \frac{\lambda_{2,\alpha}(v - u_\alpha)}{k - 1} a. \end{aligned}$$

Equality here implies $\lambda_{1,\alpha} = 0$, whence also $m_\alpha \geq k$. In this case,

$$\frac{\lambda_{2,\alpha}(v - u_\alpha)}{k - 1} = \frac{\lambda_{2,\alpha} ak}{k - 1}\left(1 - \frac{1}{m_\alpha}\right) = \frac{\lambda_{2,\alpha} ak(m_\alpha - 1)}{m_\alpha(k - 1)} \geq \lambda_{2,\alpha} a \geq a.$$

Equality holds for $m_\alpha = k$ and $\lambda_{2,\alpha} = 1$. Thus altogether we obtain

$$b \geq a^2,$$

with equality as claimed in the statement. □

Unfortunately, the block rate of any mosaic one of whose members is a semi-regular GDD cannot be much smaller than 1. This implies that the minimal possible color rate of a block rate optimal GDD quickly approaches $1/2$ from below as the number of colors increases.

Lemma 2.3 *Consider a mosaic M of (v, k, r) tactical configurations and of color rate $\varrho < 1/2$. Assume that its member D_α is a $(u, m, k, \lambda_1, \lambda_2)$ semi-regular GDD. If $\log a - \log(a - 1) \leq \varepsilon$, then*

$$\frac{\log b}{\varrho \log v} \geq \frac{1}{\varrho} - \frac{\varepsilon}{\log a}.$$

Proof From (2.1) and the semi-regularity of D_α, it follows that

$$b = a^2 \frac{kr}{v} = a^2 \lambda_2. \tag{2.10}$$

Since $\log a = \varrho \log v$, this means that

$$\frac{\log b}{\varrho \log v} = 2 + \frac{\log \lambda_2}{\log a}. \tag{2.11}$$

The color rate is connected to λ as follows. It was shown for semi-regular GDDs in [10] that

$$b - 1 \geq v - m = m(u - 1) \tag{2.12}$$

(this generalizes Hanani's inequality) and that m divides k, say $k = cm$. This implies $u = ac$, since $um = v = ak = acm$. Inserting this and (2.10) in (2.12), one obtains

$$\varrho = \frac{\log a}{\log a + \log k} \geq \frac{\log a}{\log a + \log(a^2\lambda_2 - 1) - \log(ac - 1)}, \tag{2.13}$$

hence

$$\log(a^2\lambda_2 - 1) \geq \frac{\log a}{\varrho} - \log a + \log(a - 1)$$

and

$$\log \lambda_2 \geq \left(\frac{1}{\varrho} - 2\right) \log a - \varepsilon.$$

Inserting this in (2.11) gives the result. □

Corollary 2.4 *A necessary condition for a mosaic $(D_\alpha)_{\alpha \in \mathcal{A}}$ of $(u, k, 1)$ TDs to be block rate optimal is that the color rate ϱ satisfies*

$$\varrho \geq \frac{\log u}{\log u + \log(u + 1)}.$$

Equality is attained if and only if every D_α is the dual of an affine plane.

Proof We know that that $\lambda = 1$ for mosaics of block rate optimal TDs. Using this and $c = 1$ in (2.13), which holds for arbitrary ϱ, gives the lower bound.

Assume that equality holds, and so Hanani's inequality holds with equality for every D_α. According to Neumaier [27, Corollary 3.8], equality holds in Hanani's inequality for a TD D if and only if D is the dual of an affine BIBD. Thus every D_α is the dual of an affine BIBD. Since every D_α is a $(u, k, 1)$ TD, any two distinct blocks of its dual D_α^T intersect in at most one point, hence D_α^T is an affine plane. □

We have seen that we cannot come close to block rate optimality for rates well below $1/2$ using mosaics which contain at least one semi-regular GDD. The same holds for mosaics which have at least one regular GDD as a member, since regular GDDs satisfy $b \geq v$ by [10], so

$$\frac{\log b}{\varrho \log v} \geq \frac{1}{\varrho}.$$

For color rates smaller than those in Corollary 2.4, the solution is to use singular GDDs. (However, we will see that singular block rate optimal GDDs give suboptimal bounds for semantic security for sufficiently large point set.) Bose and Connor show in [10] that every singular GDD is obtained by the multiplication of the points of a BIBD. We apply the same construction in order to obtain a mosaic $M = (D_\alpha)_{\alpha \in \mathcal{A}}$ of singular GDDs from a mosaic $M^* = (D_\alpha^*)_{\alpha \in \mathcal{A}}$ of (v^*, k^*, λ^*) BIBDs on $(\mathcal{X}^*, \mathcal{S}^*)$. For an arbitrary positive integer u,

replace each point $x^* \in \mathcal{X}^*$ by a class of u copies of x^*. This gives the point set $\mathcal{X}$ of M. The block index set does not change, we set $\mathcal{S} = \mathcal{S}^*$. A point x and a block index s are defined to be incident in D_α if x is a copy of an x^* which is incident with s in D^*_α. Every D_α has parameters

$$u, \quad m = v^*, \quad k = uk^*, \quad \lambda_1 = r = r^*, \quad \lambda_2 = \lambda^*.$$

Note that all members of M have the same point class partition. We call M the *u-fold point multiple* of M^*.

Conversely, one shows in the same way as in [10] that every mosaic of singular GDDs with the same parameters and the same point class partition is the u-fold point multiple of a mosaic of BIBDs.

Lemma 2.5 *Let $M^* = (D^*_\alpha)_{\alpha \in \mathcal{A}}$ be a mosaic of (v^*, k^*, λ^*) BIBDs with color rate ϱ^*. For a positive integer u, let M be the u-fold point multiple of M^*. Then M has the color rate*

$$\varrho = \frac{\varrho^* \log v^*}{\log v^* + \log u},$$

and satisfies

$$\frac{\log b}{\varrho \log v} = \frac{\log b^*}{\varrho^* \log v^*}.$$

Proof For the color rate, observe that $a = a^*$, and so

$$\varrho = \frac{\log a}{\log v^* + \log u} = \frac{\log a^*}{\log v^*} \cdot \frac{\log v^*}{\log v^* + \log u},$$

as claimed. The claim about the block rates follows from $v^\varrho = a = a^* = (v^*)^{\varrho^*}$ and $b = b^*$. □

We see that if M^* is close to block rate optimality and $\varrho^* \geq \varrho_0(v^*, k^*)$, then M is close to block rate optimality as well. The color rates can be chosen arbitrarily small by choosing u accordingly. A block rate optimal mosaic M^* of BIBDs with color rate larger than $1/2$ will be constructed in Sect. 2.6.

2.4 Complexity

With a view towards applications, we would like to be able to find examples of mosaics of designs whose functional form and randomized inverse are efficiently computable (in the Turing model of computation). By efficiency, we mean that it must be possible to do the computations in time polylogarithmic in v and b. This is compatible with the usual requirements in coding theory, where encoding and decoding must be done in time polynomial in the blocklength. For this asymptotic definition to make sense, we will implicitly assume that the mosaic is part of an infinite family of mosaics where each color rate can be attained infinitely often and where v is unbounded. This will be satisfied by all examples we give below.

Since $\mathcal{X}$ and $\mathcal{S}$ do not necessarily have a natural representation as a set of consecutive bit sequences, we define efficiency in terms of the functional form of an isomorphic mosaic defined on sets of integers. The choice of integers instead of bit strings allows us to ignore questions arising when the cardinality of a set is not a power of 2.

For any positive integer n, we write $[n] = \{1, \ldots, n\}$. We call the mosaic $M = (D_\alpha)_{\alpha \in \mathcal{A}}$ *explicit* if there exists a mosaic $\tilde{M} = (\tilde{D}_j)_{j \in [a]}$ with point set $[v]$ and block index set $[b]$ which is isomorphic to M and whose functional form $\tilde{f} : [v] \times [b] \to [a]$ satisfies

(M1) $\tilde{f}(\tilde{x}, \tilde{s})$ can be computed in time poly$(\log v, \log b)$ (polynomial in $\log v$ and $\log b$) for all $\tilde{x} \in [v]$ and $\tilde{s} \in [b]$;

(M2) there exists a mapping $g : [b] \times [a] \times [k] \to [v]$ such that $g(\tilde{s}, \tilde{\alpha}, \kappa)$ can be computed in time poly$(\log b, \log v)$ for all $\tilde{s}, \tilde{\alpha}, \kappa$ and which for fixed $\tilde{s} \in [b]$ and $\tilde{\alpha} \in [a]$ is a bijection between $[k]$ and $\tilde{f}_{\tilde{s}}^{-1}(\tilde{\alpha})$.

Remark 2.6 Condition (M2) corresponds to the usual complexity-theoretic definition of *strong explicitness* of graph families [1]. Condition (M1) means the efficient distinction between different graphs, which is only of concern in the context of mosaics.

If, in the wiretap channel case, Alice chooses the seed, which is the most likely scenario, then the order of the choice of seed s and channel input x can be reversed. So far, we have assumed that s is chosen first and x is chosen from $f_s^{-1}(\alpha)$. Due to (2.1), it is equivalent to first choose x uniformly at random from $\mathcal{X}$ and then to choose s from $f_x^{-1}(\alpha) = \{s \in \mathcal{S} : f(x, s) = \alpha\}$. We will see in one of the mosaics which we are going to construct that this can reduce the cost of computation.

However, reversing the order of choosing s and x has a drawback. We already mentioned above that if the channel from Alice to Bob is used to first transmit the seed and then the confidential message, this incurs a loss of total communication rate, and that it is possible to make up for this by reusing the seed. Since s depends on x if the latter is chosen first, seed reuse is impossible in this case.

All functions constructed in this paper will be based on finite-field arithmetic. For real implementations, not all finite fields are equally suitable. However, in principle, the complexities are comparable. If $q = p^t$ for a prime p, then $\mathbb{F}_q$ can be regarded as a vector space over $\mathbb{F}_p$. If $\mathbb{F}_q$ is represented in a polynomial basis, i.e., a basis of the form $\{1, \vartheta, \vartheta^2, \ldots, \vartheta^{t-1}\}$, then addition and subtraction in the field $\mathbb{F}_q$ can be done in time $O(\log q)$. For multiplication and division, $O((\log q)^2)$ time is sufficient [26]. A polynomial basis exists for all prime powers q [24].

2.5 A general construction

We next present a method from which all examples of mosaics below will be constructed. A key ingredient for its construction are *quasigroups.* A quasigroup on the finite set $\mathcal{A}$ is an array L with entries from $\mathcal{A}$ and rows and columns indexed by $\mathcal{A}$ and which satisfies

1) for every $\alpha, \gamma \in \mathcal{A}$ there is a unique $\beta \in \mathcal{A}$ such that $L(\alpha, \beta) = \gamma$,
2) for every $\beta, \gamma \in \mathcal{A}$ there is a unique $\alpha \in \mathcal{A}$ such that $L(\alpha, \beta) = \gamma$.

Every finite group is a quasigroup. If one labels the rows and columns of a quasigroup by a set which is not necessarily the same as $\mathcal{A}$, one obtains a *Latin square*. Using quasigroups instead of Latin squares is more convenient in our setting.

A quasigroup L on $\mathcal{A}$ and a quasigroup $\tilde{L}$ on $\tilde{\mathcal{A}}$ are called *isomorphic* if there exists a bijective mapping $\Phi : \mathcal{A} \to \tilde{\mathcal{A}}$ such that $\tilde{L}(\Phi(\alpha), \Phi(\beta)) = \Phi(\gamma)$ for all $\alpha, \beta, \gamma \in \mathcal{A}$.

The following theorem was already shown in [17] for the case of resolvable BIBDs, using Latin squares instead of quasigroups (which combinatorially amounts to the same thing). It is based on the idea that it should be possible to obtain a mosaic if one starts with a resolvable incidence structure, since the sum of a mosaic is resolvable.

Theorem 2.7 *Let D be a resolvable (v, k, r) tactical configuration with incidence relation I. Let $\mathcal{A}$ be an index set for every parallel class of the blocks of D, and let L be a quasigroup on $\mathcal{A}$. Then there exists a mosaic $M = (D_\alpha)_{\alpha\in\mathcal{A}}$ where each D_α is isomorphic to D, and there exists a mosaic $M^T = (D_\alpha^T)_{\alpha\in\mathcal{A}}$ where each D_α^T is isomorphic to D^T.*

If D is a GDD, then all D_α share their point class partitions with D. If D^T is a GDD, then every D_α^T has the same point class partition as D^T and $\lambda_1 = 0$.

Proof The proof essentially is a reformulation of the proof of [17] together with the observation, already mentioned above, that if one has a mosaic and passes to the dual of every member of this mosaic, then one again obtains a mosaic. Our formulation of the proof will make it straightforward to derive the functional form of a mosaic constructed in this way.

The block index set of D can be written as $\mathcal{R} \times \mathcal{A}$, where $\mathcal{R}$ is an index set of cardinality r for the parallel classes, and the blocks of each parallel class are labeled with a unique symbol from $\mathcal{A}$. Denote the point set of D by $\mathcal{P}$. For every $p \in \mathcal{P}$ and $i \in \mathcal{R}$ there exists a unique $\alpha \in \mathcal{A}$ such that $p\, I\, (i, \alpha)$. We define the incidence structure $D_\alpha = (\mathcal{P}, \mathcal{R} \times \mathcal{A}, I_\alpha)$ by saying that $p\, I_\alpha\, (i, \beta)$ if and only if $p\, I\, (i, \gamma)$ for the unique γ satisfying $L(\beta, \gamma) = \alpha$. This gives a mosaic. It follows directly from the construction and the quasigroup property of L that all members of this mosaic are isomorphic to D. By dualization, one obtains a mosaic all members of which are isomorphic to D^T.

It is clear that if D is a GDD, then all D_α must have the same point class partition. For D^T, the point class partition corresponds to the partition of the blocks of D into parallel classes, which is shared by all D_α. This shows that all D_α^T have the same point class partition with $\lambda_1 = 0$. □

Corollary 2.8 *Assume the same conditions as in Theorem 2.7. Let $\mathcal{P}$ be the point set of D and $\mathcal{R} \times \mathcal{A}$ its block set, where $\mathcal{R}$ is an index set for the parallel classes and $\mathcal{A}$ is an index set for the elements of any parallel class. The functional form $f : \mathcal{P} \times (\mathcal{R} \times \mathcal{A}) \to \mathcal{A}$ of the mosaic M constructed in Theorem 2.7 satisfies*

$$f(p; i, \beta) = L(\beta, \gamma) \quad \textit{for the unique } \gamma \in \mathcal{A} \textit{ with } p\, I\, (i, \gamma).$$

The functional form $f^T : (\mathcal{R} \times \mathcal{A}) \times \mathcal{P} \to \mathcal{A}$ of M^T satisfies $f^T(i, \beta; p) = f(p; i, \beta)$.

The explicitness of a mosaic constructed as in Theorem 2.7 follows from the explicitness of the involved design D and the quasigroup L. This is important in those cases where explicitness is not immediately clear from the functional form of the mosaic, like for the mosaics $\mathcal{M}^{(2)}$ of the next section.

We say that a quasigroup L on $\mathcal{A}$ is *explicit* if there exists an isomorphic quasigroup $\tilde{L}$ over $[a]$ such that

(L1) $\tilde{L}(\tilde{\beta}, \tilde{\gamma})$ can be computed in time poly$(\log a)$ for all $\tilde{\beta}, \tilde{\gamma} \in [a]$,
(L2) $\tilde{L}(\tilde{\beta}, \cdot) = \tilde{\alpha}$ can be solved in time poly$(\log a)$ for all $\tilde{\beta}, \tilde{\gamma} \in [a]$.

Let $D = (\mathcal{X}, \mathcal{S}, I)$ be a resolvable (v, k, r) tactical configuration with $\mathcal{S} = \mathcal{R} \times \mathcal{A}$, where $\mathcal{R}$ is an index set for the parallel classes and $\mathcal{A}$ for the elements of each parallel class. We call D *explicit* if there exists an isomorphic resolvable tactical configuration $\tilde{D} = ([v], [r] \times [a], \tilde{I})$ satisfying

(D1) for every $\tilde{x} \in [v]$ and $\tilde{\imath} \in [r]$, the unique $\tilde{\alpha} \in [a]$ satisfying $\tilde{x}\, \tilde{I}\, (\tilde{\imath}, \tilde{\alpha})$ can be computed in time poly$(\log v, \log r)$;
(D2) there exists a mapping $g : [r] \times [a] \times [k] \to [v]$ whose values are computable in time poly$(\log b, \log k)$ and which satisfies that $\tilde{\kappa} \mapsto g(\tilde{\imath}, \tilde{\alpha}, \tilde{\kappa})$ is a bijection between $[k]$ and the set of points in $[v]$ incident in $\tilde{D}$ with the block index $(\tilde{\imath}, \tilde{\alpha})$.

We call the dual D^T of D *explicit* if there exists a resolvable tactical configuration $\tilde{D} = ([v], [r] \times [a], \tilde{I})$ isomorphic to D which satisfies (D1) and

(D2)^T there exists a mapping $g^T : [k] \times [r] \times [a] \to [v]$ whose values are computable in time poly$(\log b, \log k)$ and which satisfies that $(\tilde{\iota}, \tilde{\alpha}) \mapsto g^T(\tilde{\kappa}, \tilde{\iota}, \tilde{\alpha})$ is a bijection between $[r] \times [a]$ and the set of blocks in $[b]$ incident in $\tilde{D}$ with the point $\tilde{\kappa}$.

Theorem 2.9 *Assume the conditions as in Theorem 2.7. The mosaic M constructed in Theorem 2.7 is explicit if both D and L are explicit. Its dual M^T is explicit if D^T and L are explicit.*

Proof Let $\tilde{D}$ be a design as in the definition of explicitness of D and let $\tilde{L}$ a quasigroup as in the definition of explicitness of L. The design $\tilde{M}$ constructed from $\tilde{D}$ and $\tilde{L}$ is isomorphic to M.

In order to check (M1), let $\tilde{f} : [v] \times [r] \times [a] \to [a]$ be the functional form of $\tilde{M}$. Choose any $\tilde{x} \in [v], \tilde{\iota} \in [r]$ and $\tilde{\beta} \in [a]$. Then by Corollary 2.8, $\tilde{f}(\tilde{x}; \tilde{\iota}, \tilde{\beta}) = \tilde{L}(\tilde{\beta}, \tilde{\gamma})$ for the unique $\tilde{\gamma}$ satisfying $\tilde{x}\, \tilde{I}\, (\tilde{\iota}, \tilde{\gamma})$. By (D1), this $\tilde{\gamma}$ can be found in time poly$(\log v, \log r)$, and $\tilde{L}(\tilde{\beta}, \tilde{\gamma})$ can be computed in time poly$(\log a)$ by (L1). Thus $\tilde{f}(\tilde{x}; \tilde{\iota}, \tilde{\beta})$ can be computed in time poly$(\log v, \log b)$.

In order to check (M2), fix any $(\tilde{\iota}, \tilde{\beta}) \in [r] \times [a]$ and $\tilde{\alpha} \in [a]$. By (L2), the $\tilde{\gamma}$ satisfying $\tilde{L}(\tilde{\beta}, \tilde{\gamma}) = \tilde{\alpha}$ can be found in time poly$(\log a)$. By (D2), there exists a mapping $\kappa \mapsto g(\tilde{\iota}, \tilde{\gamma}, \kappa)$ which enumerates all points incident with $(\tilde{\iota}, \tilde{\gamma})$ in $\tilde{D}$ and whose values can be computed in time poly$(\log b, \log k)$. The set of these points equals $\tilde{f}^{-1}_{(\tilde{\iota}, \tilde{\beta})}(\tilde{\alpha})$.

Altogether, this proves the explicitness of M. The explicitness of M^T is shown similarly. □

2.6 Examples of (nearly) block rate optimal mosaics

We present four families of mosaics. Not all of these are block rate optimal, but those which are not are arbitrarily close to optimality for sufficiently large point sets. There is a family for each combination of the cases

1) color rate $\varrho \geq 1/2$ or $\varrho \leq 1/2$ (roughly),
2) BIBD or GDD.

The sets of color rates will be dense except for the case of BIBDs with small color rates.

In all cases we will use Theorem 2.7. Thus in every case the key is to find a single resolvable design with the desired parameters.

BIBD and $\varrho \leq 1/2$: For this case we build our construction on the affine designs. Fix an integer $t \geq 2$ and a prime power q and let v, k, λ etc. be the parameters of the BIBD $AG_{t-1}(t, q)$. Then

$$v = q^t, \quad b = \frac{q(q^t - 1)}{q - 1}, \quad r = \frac{q^t - 1}{q - 1}, \quad k = q^{t-1}, \quad \lambda = q^{t-2}, \quad a = q.$$

Hence the color rate of the mosaic $M^{(1)}_{t,q}$ we obtain from $AG_{t-1}(t, q)$ with the construction of Theorem 2.7 is

$$\varrho = \frac{1}{t}.$$

We have $1/t > \varrho_0(v, k)$ only if $t = 2$. In this case, $M^{(1)}_{t,q}$ is block rate optimal since $\lambda = 1$.

If $t \geq 3$, then $M_{t,q}^{(1)}$ could only be block rate optimal if it were square, which is not the case. However, since $AG_{t-1}(t,q)$ is affine, it is a consequence of Bose's inequality (2.6) that the block rate of $M_{t,q}^{(1)}$ is minimal among those mosaics constructed from any of the known resolvable BIBDs with $v = q^t$ and color rate $1/t$. The block rate satisfies

$$\frac{\log b}{\log v} \leq 1 + \frac{1}{t}\left(1 - \frac{\log(q-1)}{\log q}\right).$$

Thus for fixed color rate $1/t$, one gets closer to block rate optimality by increasing q.

Every hyperplane of $AG_{t-1}(t,q)$ can be represented by a unique pair (h,α), where $\alpha \in \mathbb{F}_q$ and h is a nonzero element of $\mathbb{F}_q^t$ whose first nonzero component is normalized to 1. We denote the set of these h by $\mathcal{R}$. The hyperplane corresponding to (h,α) is the set of points x satisfying $h \cdot x = \alpha$, where $h \cdot x = \sum_i h_i x_i$. Different h give different parallel classes and different α with a fixed h indicate different parallel hyperplanes in the parallel class corresponding to h.

The natural quasigroup to construct a mosaic from $AG_{t-1}(t,q)$ is the additive group of $\mathbb{F}_q$. Then a point $x \in \mathbb{F}_q^t$ and an element (h,β) of the block index set are incident in D_α if and only if x is incident with $(h, \alpha-\beta)$ in $AG_{t-1}(t,q)$. The functional form $f : \mathbb{F}_q^t \times (\mathcal{R} \times \mathbb{F}_q) \to \mathbb{F}_q$ of $M_{t,q}^{(1)}$ is given by

$$f(x;h,\beta) = h \cdot x + \beta.$$

This immediately shows that the family

$$\mathcal{M}^{(1)} = \{M_{t,q}^{(1)} : t \geq 2, q \text{ prime power}\}$$

is explicit.

BIBD and $\varrho \geq 1/2$: Fix a positive integer $t \geq 2$ and an integer ℓ between 1 and t. For $q = 2^t$, let $Q : \mathbb{F}_q^2 \to \mathbb{F}_q$ be an irreducible quadratic form, i.e., a polynomial of the form

$$Q(x,y) = \eta_1 x^2 + \eta_2 xy + \eta_3 y^2$$

which cannot be factored into linear forms. Such a quadratic form exists for all q. Choose an arbitrary subgroup H of order 2^ℓ of the additive group of $\mathbb{F}_q$ and consider the set

$$\mathcal{X} = \{(x,y) : Q(x,y) \in H\}.$$

It was proved by Denniston [15] that $\mathcal{X}$ has

$$v = 1 + (2^t+1)(2^\ell - 1) \tag{2.14}$$

elements and that every line of $AG(2,q)$ has either 2^ℓ or no points in common with $\mathcal{X}$.

We will regard $\mathcal{X}$ as a subset of $AG(2,q)$. It is not hard to see [8, Corollary VIII.5.21] that if we denote by $\mathcal{S}$ the set of nontrivial intersections of lines of $AG(2,q)$ with $\mathcal{X}$, then $D = (\mathcal{X}, \mathcal{S}, \in)$ is a resolvable $(v,k,1)$ BIBD with $k = 2^\ell$. Since $r = 2^t + 1$ by (2.2), the set of parallel classes of D is in one-to-one relation with the set of parallel classes of lines in $AG(2,q)$. In fact, if $\ell = t$, then $D = AG(2,q)$.

Applying Theorem 2.7, one constructs a mosaic $M_{t,\ell,H}^{(2)}$ with the parameters

$$\begin{aligned} &v = 2^\ell(2^t + 1 - 2^{t-\ell}), \quad b = (2^t+1)(2^t+1-2^{t-\ell}), \\ &r = 2^t + 1, \quad k = 2^\ell, \quad \lambda = 1, \quad a = 2^t + 1 - 2^{t-\ell}, \\ &\varrho = \frac{\log(2^t+1-2^{t-\ell})}{\ell + \log(2^t+1-2^{t-\ell})} \approx \frac{t}{t+\ell}. \end{aligned}$$

Since $\lambda = 1$, the mosaic $M^{(2)}_{t,\ell,H}$ is block rate optimal and satisfies

$$\frac{\log b}{\varrho \log v} = \frac{\log b}{\log a} = 2 + \left(\frac{\log(2^t + 1)}{\log(2^t + 1 - 2^{t-\ell})} - 1 \right). \tag{2.15}$$

For every t and ℓ, it is possible to choose a subgroup $H_{t,\ell}$ such that the resulting family

$$\mathcal{M}^{(2)} = \{M^{(2)}_{t,\ell,H_{t,\ell}} : t \geq 2, 1 \leq \ell \leq t\}$$

is explicit. Some work has to be done in order to show this, which we postpone to Sect. 5. Moreover, every number between 1/2 and 1 can be approximated arbitrarily closely by the color rates of elements of $\mathcal{M}^{(2)}$ for sufficiently large t and ℓ.

GDD and $\varrho < 1/2$: Fix a positive integer t and a nonnegative ℓ between 0 and t. Denote the elements of the explicit family $\mathcal{M}^{(2)}$ constructed above by $M^{(2)}_{t,\ell}$ (we omit the subgroups here in order to simplify notation). Choose an integer u and let $M^{(3)}_{t,\ell,u}$ be the u-fold point multiple of $M^{(2)}_{t,\ell}$. Its parameters are

$$\begin{aligned} &u, \quad m = 2^\ell(2^t + 1 - 2^{t-\ell}), \quad b = (2^t + 1)(2^t + 1 - 2^{t-\ell}), \\ &r = 2^t + 1, \quad k = 2^\ell u, \quad \lambda_1 = 2^t + 1, \quad \lambda_2 = 1, \quad a = 2^t + 1 - 2^{t-\ell}. \end{aligned}$$

By Lemma 2.5, its color rate is

$$\varrho = \frac{\log(2^t + 1 - 2^{t-\ell})}{\ell + \log(2^t + 1 - 2^{t-\ell}) + \log u} \approx \frac{t}{t + \ell + \log u}$$

and the ratio of the block rate and the color rate is given by (2.15). The color rate is smaller than $1/2$ for sufficiently large u.

Denote the point set of $M^{(2)}_{t,\ell}$ by $\mathcal{X}^*$ and its block index set by $\mathcal{S}^*$. Let $f^* : \mathcal{X}^* \times \mathcal{S}^* \to \mathcal{A}^*$ be the functional form of $M^{(2)}_{t,\ell}$. The point set of $M^{(3)}_{t,\ell,u}$ can be taken to be $\mathcal{X} = \mathcal{X}^* \times [u]$, the block index set and the color set remain the same as for D^*, so $\mathcal{S} = \mathcal{S}^*$ and $\mathcal{A} = \mathcal{A}^*$. The functional form $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ of $M^{(3)}_{t,\ell,u}$ satisfies

$$f(x^*, i; s) = \alpha \quad \text{if and only if} \quad f^*(x^*, s) = \alpha$$

for $x^* \in \mathcal{X}^*$, $i \in [u]$, $s \in \mathcal{S}$ and $\alpha \in \mathcal{A}$. The explicitness of the family

$$\mathcal{M}^{(3)} = \{M^{(3)}_{t,\ell,u} : t \geq 2, 1 \leq \ell \leq t, u \geq 1\}$$

follows from that of $\mathcal{M}^{(2)}$.

By the discussion in Sect. 2.3, mosaics of singular GDDs give the best approximation to block rate optimality among mosaics of GDDs with a small color rate if the point set is sufficiently large. The ratio of the block and the color rates is given by (2.15). All numbers between 0 and 1 can be approximated arbitrarily well by the color rates of suitable members of $\mathcal{M}^{(3)}$.

GDD and $\varrho \geq 1/2$: If one deletes some of the parallel classes from the block set of $AG(2, q)$, where q is a prime power, then one obtains the dual of a transversal design. Assume we keep $k \geq 2$ of the parallel classes of $AG(2, q)$. Call the resulting design D^T and set $D = (D^T)^T$. The point set $\mathcal{X}$ of D consists of lines of $AG(2, q)$ and the block index set $\mathcal{S}$ of D consists of all the points of $AG(2, q)$. Two points $x, x' \in \mathcal{X}$ are incident with a common block index s if and only if they intersect as lines in $AG(2, q)$, and so parallel classes of D^T translate into point classes of D. If x, x' are not in the same point class of D, then in D^T, their corresponding

lines intersect in a unique point. In D, this means that two points from different point classes are incident with a unique block index, and so D is a $(q, k, 1)$ TD.

Letting $\mathcal{R}$ denote the set of remaining parallel classes of lines, we construct from this transversal design a mosaic $M^{(4)}_{k,q,\mathcal{R}}$ as in Theorem 2.7, using the natural additive group structure of $\mathbb{F}_q$ on every parallel class of $AG(2, q)$. We obtain a mosaic with

$$u = q, \quad k, \quad b = q^2, \quad \lambda = 1, \quad a = q.$$

Thus $M^{(4)}_{k,q,\mathcal{R}}$ has color rate

$$\varrho = \frac{\log q}{\log q + \log k}.$$

Since k ranges between 2 and $q + 1$, ϱ is a number between

$$\frac{\log q}{\log q + \log(q + 1)} \quad \text{and} \quad \frac{\log q}{1 + \log q}.$$

The block rate is optimal by Lemma 2.2.

The point set $\mathcal{X}$ of $M^{(4)}_{k,q,\mathcal{R}}$ has the structure of a Cartesian product, $\mathcal{X} = \mathcal{R} \times \mathbb{F}_q$. For the discussion of the functional form of the mosaic, we assume that $k \leq q$ and that $\mathcal{R}$ is given by a subset of $\mathbb{F}_q$. Then $x = (c, d) \in \mathcal{X}$ corresponds to the line $\{(u, cu + d) : u \in \mathbb{F}_q\}$ in $AG(2, q)$. The case $k = q + 1$ can be treated analogously and corresponds to a mosaic whose members all are isomorphic to the dual of $AG(2, q)$.

A point $x = (c, d) \in \mathcal{X}$ and a block $s = (s_1, s_2) \in \mathcal{S} = \mathbb{F}_q^2$ are incident in D if $cs_1 + d = s_2$. They are incident in D_α if $cs_1 + d - \alpha = s_2$, where $\alpha \in \mathbb{F}_q$. Thus

$$f(x, s) = f(c, d; s_1, s_2) = s_2 - cs_1 + d.$$

Given $\alpha \in \mathbb{F}_q$ and $s = (s_1, s_2) \in \mathbb{F}_q^2$, one can find those $x \in \mathcal{X}$ which are incident with s by taking any $c \in \mathcal{R}$ and solving for $d = \alpha - s_2 + cs_1$. In this way, one obtains the randomized inverse of f. This can be done efficiently if $\mathcal{R}$ can be enumerated efficiently. Clearly, such an $\mathcal{R} = \mathcal{R}_{k,q}$ exists for every k. This gives us an explicit family

$$\mathcal{M}^{(4)} = \{M^{(4)}_{k,q,\mathcal{R}_{k,q}} : 2 \leq k \leq q + 1, q \text{ prime power}\}.$$

All numbers between $1/2$ and 1 can be approximated arbitrarily well by the color rates of members of this family.

Discussion. All our examples are constructed using Theorem 2.7, hence all members of these designs are either themselves resolvable or duals of resolvable designs. We do not know whether mosaics of BIBDs or GDDs with constant block size exist which are not resolvable or dually resolvable. Such a construction would be particularly relevant for cases where mosaics of resolvable designs cannot be block rate optimal. For instance, a block rate optimal mosaic of BIBDs with color rate smaller than $1/2$ must be square, and consequently cannot be resolvable.

It would also be desirable to construct a family of mosaics of BIBDs which is close to block rate optimality and whose color rates are dense in the interval between 0 and $1/2$.

2.7 Related structures

2.7.1 Universal hash functions.

A function $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ is called a *universal hash function* if for all distinct $x, x' \in \mathcal{X}$,

$$\frac{|\{s : f(x,s) = f(x',s)\}|}{b} \leq \frac{1}{a} \tag{2.16}$$

(where, as usual, $|\mathcal{X}| = v$, $|\mathcal{S}| = b$ and $|\mathcal{A}| = a$). The left-hand side of (2.16) can be interpreted as the probability that the values assigned to x and x' by f "collide" if the seed is chosen uniformly at random. Let $(D_\alpha)_{\alpha\in\mathcal{A}}$ be the mosaic of incidence structures induced by f as described in Sect. 2.1. Stinson [29] has shown that the maximal collision probability of f is minimal if the sum D of $(D_\alpha)_{\alpha\in\mathcal{A}}$ is a BIBD (recall the definition of the sum of a mosaic in Sect. 2.2).

Lemma 2.10 [29] *Any onto function $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ satisfies*

$$\frac{|\{s : f(x,s) = f(x',s)\}|}{b} \geq \frac{v-a}{a(v-1)}$$

for at least one pair of distinct points $x, x' \in \mathcal{X}$. Equality holds for all distinct $x, x' \in \mathcal{X}$ if and only if the sum D of the mosaic of incidence structures $(D_\alpha)_{\alpha\in\mathcal{A}}$ induced by f is a resolvable BIBD.

A universal hash function f for which the sum D of the corresponding mosaic $(D_\alpha)_{\alpha\in\mathcal{A}}$ is a BIBD is called *optimally universal*. It follows immediately that a mosaic $(D_\alpha)_{\alpha\in\mathcal{A}}$ of BIBDs with common parameters (v, k, λ) gives rise to an optimally universal hash function, since all blocks have the same size, and for distinct $x, x' \in \mathcal{X}$

$$|\{s : f(s,x) = f(s,x')\}| = \sum_{\alpha\in\mathcal{A}} |\{s : f(s,x) = f(s,x') = \alpha\}| = a\lambda.$$

This proves the first part of the following lemma.

Lemma 2.11 *Let $M = (D_\alpha)_{\alpha\in\mathcal{A}}$ be a mosaic of (v, k, r) tactical configurations on $(\mathcal{X}, \mathcal{S})$ with functional form $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$.*

1) If every D_α is a (v, k, λ) BIBD, then f is optimally universal.
2) If M consists of $(u, m, k, \lambda_1, \lambda_2)$ GDDs with a common point class partition, then

a) if every D_α is either semi-regular, or singular with $a = 1$, then f is a universal hash function;
b) if the D_α are singular with $a \geq 2$, then f is not a universal hash function.

Proof It remains to prove the second part of the lemma. We analyze the parameters of the mosaic. For distinct points x, x',

$$\begin{aligned} |\{s : f(s,x) = f(s,x')\}| &= \sum_{\alpha\in\mathcal{A}} |\{s : f(s,x) = f(s,x') = \alpha\}| \\ &= \begin{cases} a\lambda_1 & \text{if } x, x' \text{ are contained in the same point class,} \\ a\lambda_2 & \text{else.} \end{cases} \end{aligned}$$

Since $a/b = 1/r$ and $a = v/k$, we have for $i = 1, 2$

$$\frac{a\lambda_i}{b} \leq \frac{1}{a} \quad \text{if and only if} \quad \lambda_i v \leq kr.$$

A singular GDD satisfies $r = \lambda_1$, and so f is a universal hash function if and only if $v = k$, which means that every block covers the whole point set. Equivalently, $a = 1$.

A semi-regular GDD is characterized by the equality $\lambda_2 v = kr$. Further, (2.4) and semi-regularity imply $(\lambda_1 - \lambda_2)u = \lambda_1 - r \leq 0$, whence $\lambda_1 \leq \lambda_2$, and so $\lambda_1 v \leq kr$. □

We do not have a simple criterion for when regular GDDs induce a universal hash function. Since a regular GDD D satisfies $kr > \lambda_2 v$ by definition, one only needs to check whether $kr \geq \lambda_1 v$. This is obviously true if $\lambda_1 \leq \lambda_2$. If $\lambda_1 > \lambda_2$, then some parameter choices result in mosaics whose functional form is a universal hash function, while this is not true for other parameter choices.

For instance, the regular GDD R1 from Clatworthy's list [12] has parameters $v = 4, r = 4, k = 2, \lambda_1 = 2, \lambda_2 = 1$, and thus satisfies $kr = 8 = \lambda_1 v$. Since it is resolvable, an application of Theorem 2.7 gives a mosaic of regular GDDs whose functional form is a universal hash function.

On the other hand, the regular GDD R2 from [12] has parameters $v = 4, r = 5, k = 2, \lambda_1 = 3, \lambda_2 = 1$, hence $kr = 10 < 12 = \lambda_1 v$. This GDD is resolvable as well, and the functional form of the resulting mosaic is not a universal hash function.

We conclude from Lemma 2.11 that not all of the functions constructed in Sect. 2.6 are universal hash functions. The mosaics of singular GDDs from the family $\mathcal{M}^{(3)}$ have functional forms which are not universal hash functions. Similarly, there exist universal hash functions which cannot be decomposed as a mosaic of BIBDs or GDDs. For instance, the optimally universal hash function induced by the resolvable BIBD $AG_{t-1}(t, q)$ (i.e., where the sum of the induced mosaic is $AG_{t-1}(t, q)$) does not have the additional substructure we require from the security functions in this paper.

2.7.2 Orthogonal arrays

A $v \times b$ array M with entries from the alphabet $\mathcal{A}$ is called a (b, v, a) *orthogonal array* if every $2 \times b$ subarray of M contains each pair of entries (α, α') from $\mathcal{A}$ exactly $\lambda = b/a^2$ times as a column.

If we denote the set of rows by $\mathcal{X}$ and the set of columns by $\mathcal{S}$, then an orthogonal array gives rise to a function $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ which associates to the pair (x, s) the symbol from $\mathcal{A}$ which is at the intersection of column s with row x. By definition, f satisfies for distinct $x, x' \in \mathcal{X}$ and for any $\alpha, \alpha' \in \mathcal{A}$

$$|\{s : f(x, s) = \alpha,\ f(x', s) = \alpha'\}| = \lambda.$$

This means that f is an *ε-almost strongly universal hash function* for $\varepsilon = \lambda a/b$ [30]. In particular,

$$|\{s : f(x, s) = f(x', s) = \alpha\}| = \lambda. \tag{2.17}$$

Moreover, if we set $r = a\lambda$, then

$$|\{s : f(x, s) = \alpha\}| = r.$$

It is not in general the case that also

$$|\{x : f(x, s) = \alpha\}| \tag{2.18}$$

is constant in s and α.

Assume (2.18) is constant in s and α and denote this number by k. Then M gives a mosaic of (v, k, λ) BIBDs with functional form f.

Lemma 2.12 *If M is a mosaic of BIBDs induced by an orthogonal array, then $a = 1$.*

Proof From $r = a\lambda$ we conclude $rk = v\lambda$. Then (2.2) gives $r = \lambda$, hence $v = k$. □

Corollary 2.13 *There does not exist any nontrivial orthogonal array for which (2.18) is constant in α and s.*

3 Semantic security from mosaics of combinatorial designs

3.1 Distances and divergences

The degree of semantic security offered by a security function when applied to a wiretap channel or in privacy amplification can be measured using various distances, divergences and entropies of probability measures.

Let P, Q be probability distributions on a finite set $\mathcal{Z}$. The *total variation distance* of P and Q is

$$\|P - Q\| = \sum_z |P(z) - Q(z)|.$$

This is a metric on the space of probability measures on $\mathcal{Z}$. The χ^2 divergence

$$\chi^2(P, Q) = \sum_{z:Q(z)>0} Q(z) \left(\frac{P(z)}{Q(z)} - 1 \right)^2$$

satisfies

$$\|P - Q\| \le \sqrt{\chi^2(P, Q)} + P(\{z : Q(z) = 0\}), \tag{3.1}$$

which is an immediate consequence of Cauchy-Schwarz. The *Kullback-Leibler divergence* of P and Q is given by

$$D(P\|Q) = \begin{cases} \sum_z P(z) \log \frac{P(z)}{Q(z)} & \text{if } P(\{z : Q(z) = 0\}) = 0, \\ +\infty & \text{else,} \end{cases}$$

and the *Rényi* 2*-divergence* by

$$D_2(P\|Q) = \begin{cases} \log \sum_z \frac{P(z)^2}{Q(z)} & \text{if } P(\{z : Q(z) = 0\}) = 0, \\ +\infty & \text{else.} \end{cases}$$

They are nonnegative and related by [33]

$$D(P\|Q) \le D_2(P\|Q). \tag{3.2}$$

It is a straightforward calculation to show that if $D_2(P\|Q) < \infty$, then

$$\chi^2(P, Q) = \exp\big(D_2(P\|Q)\big) - 1. \tag{3.3}$$

We also introduce averaged versions of these divergences. If $W : \mathcal{X} \to \mathcal{Z}$ is a channel, and additionally P is a probability distribution on $\mathcal{X}$ and Q on $\mathcal{Z}$, then we set

$$D(W\|Q|P) = \sum_{x\in\mathcal{X}} P(x)D(W(\cdot|x)\|Q)$$

and

$$D_2(W\|Q|P) = \log \sum_{x\in\mathcal{X}} P(x)\exp\bigl(D_2(W(\cdot|x)\|Q)\bigr).$$

Let X, Y be discrete random variables with joint distribution P_{XY}. Denote the marginal distributions by P_X and P_Y and the conditional distribution of Y given the event $X = x$ by $P_{Y|X=x}$. Then the *mutual information* of X and Y is defined by

$$I(X \wedge Y) = \sum_x P_X(x)D(P_{Y|X=x}\|P_Y) = D(P_{Y|X}\|P_Y|P_X).$$

The bounds obtained in the privacy amplification scenario involve *Rényi 2-entropy*, which for a random variable X on $\mathcal{X}$ is defined as

$$H_2(X) = -\log \sum_x P_X(x)^2.$$

3.2 Wiretap channel

Let $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ be the functional form of a mosaic $(D_\alpha)_{\alpha\in\mathcal{A}}$ of (v, k, r) tactical configurations and let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel. Assume that the confidential messages to be transmitted are represented by the random variable A on $\mathcal{A}$. The random seed is represented by S, uniformly distributed on $\mathcal{S}$ and independent of A. Application of the randomized inverse of f determines the random input X to W, and the random output of W seen by Eve is denoted by Z. The joint probability distribution of these four random variables is

$$P_{ZXSA}(z, x, s, \alpha) = \frac{1}{bk} w(z|x)N_\alpha(x, s)P_A(\alpha), \tag{3.4}$$

where N_α is the incidence matrix of D_α.

The two security metrics by which we measure the degree of security offered by f for W are defined in terms of the joint distribution of Z, S and A with a worst-case choice of A. The first security metric is defined as the mutual information between the message A and the eavesdropper's information Z, S, maximized over all possible message distributions,

$$\max_{P_A} I(A \wedge Z, S). \tag{3.5}$$

The best case would be that Eve's observations are independent of the message, no matter what the message distribution is, in which case the mutual information would vanish. This is not achievable in general, even for a fixed message distribution. Instead, we try to make the maximum in (3.5) as small as possible. Like the other security criteria defined below, the requirement that (3.5) be small does not make any assumptions on Eve's computing power. Thus we aim for *unconditional security*.

Remark 3.1 For the *strong secrecy* criterion mentioned in Sect. 1.4, it is assumed that the distribution P_A is fixed, so that only the corresponding $I(A \wedge Z, S)$ has to be small. Usually, one takes A to be uniformly distributed on $\mathcal{A}$.

In order to formulate the upper bound for (3.5), we need to introduce additional notation. If $\mathcal{U}$ is a finite set and $R : \mathcal{U} \to \mathcal{X}$ a channel, then the usual matrix product RW of the stochastic matrices R and W gives the channel with input alphabet $\mathcal{U}$ and output alphabet $\mathcal{Z}$ resulting from concatenating R and W. If P is a probability measure on $\mathcal{X}$, then this also defines the probability measure PW on $\mathcal{Z}$ by regarding P as a channel with a single row.

The uniform distribution on any set $\mathcal{X}$ is denoted by $P_{\mathcal{X}}$. Also, recall Rényi 2-divergence defined in Sect. 3.1.

Theorem 3.2 *1) Let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel and let $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ be the functional form of a mosaic of (v, k, λ) BIBDs. Then*

$$\max_{P_A} \exp\big(I(A \wedge Z, S)\big) \le \left(1 - \frac{r-\lambda}{kr}\right) + \frac{r-\lambda}{kr} \exp\big(D_2(W \| P_{\mathcal{X}} W | P_{\mathcal{X}})\big).$$

2) Let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel and let $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ be the functional form of a mosaic of $(u, m, k, \lambda_1, \lambda_2)$ GDDs with a common point class partition $\Pi = \{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$. Let P_Π be the uniform distribution on Π and $R_\Pi : \Pi \to \mathcal{X}$ the channel which associates to an element $\mathcal{X}_j$ of Π the uniform distribution on $\mathcal{X}_j$. Then

$$\begin{aligned}
&\max_{P_A} \exp\big(I(A \wedge Z, S)\big) \\
&\quad \le \left(1 - \frac{(r-\lambda_1) + (\lambda_1 - \lambda_2)u}{kr}\right) + \frac{(\lambda_1 - \lambda_2)u}{kr} \exp\big(D_2(R_\Pi W \| P_{\mathcal{X}} W | P_\Pi)\big) \\
&\qquad + \frac{r-\lambda_1}{kr} \exp\big(D_2(W \| P_{\mathcal{X}} W | P_{\mathcal{X}})\big).
\end{aligned}$$

This theorem is proved in Sect. 4. The main observation is Proposition 4.2, which both for the BIBD and the GDD case states equality between $\exp(D_2(P_{Z|S,A=\alpha} \| P_{Z|S} | P_{\mathcal{S}}))$ and the respective upper bounds in the statement. Since this equality for every α only depends on D_α, it really is a statement about BIBDs and GDDs.

Clearly, a GDD with $\lambda_1 = \lambda_2$ is a BIBD, so the first part of the theorem is implied by the second one. The same holds for Theorems 3.3, 3.6 and 3.7 below.

An alternative measure of semantic security is formulated in terms of total variation distance. Denote the product of probability distributions P and Q by PQ. Then, with the random variables Z, S, A as defined in (3.4), we would like

$$\max_{P_A} \| P_{ZSA} - P_{ZS} P_A \| \tag{3.6}$$

to be small. If it equals zero, then the eavesdropper's observations are independent of the message, for all possible message distributions.

Theorem 3.3 *1) Let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel and let $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ be the functional form of a mosaic of (v, k, λ) BIBDs. Then*

$$\max_{P_A} \| P_{ZSA} - P_{ZS} P_A \| \le 2 \left(\frac{(r-\lambda)}{kr}\right)^{1/2} \big(\exp\big(D_2(W \| P_{\mathcal{X}} W | P_{\mathcal{X}})\big) - 1\big)^{1/2}.$$

2) Let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel and let $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ be the functional form of a mosaic of $(u, m, k, \lambda_1, \lambda_2)$ GDDs with a common point class partition Π. Define P_Π and R_Π as in Theorem 3.2. Then

$$\max_{P_A} \|P_{ZSA} - P_{ZS}P_A\| \leq 2\left(\frac{r-\lambda_1}{kr}\exp\big(D_2(W\|P_{\mathcal{X}}W|P_{\mathcal{X}})\big) + \frac{(\lambda_1-\lambda_2)u}{kr}\exp\big(D_2(R_{\Pi}W\|P_{\mathcal{X}}W|P_{\Pi})\big) - \frac{(r-\lambda_1)+(\lambda_1-\lambda_2)u}{kr}\right)^{1/2}.$$

This theorem is also proved in Sect. 4. It essentially follows from Theorem 3.2 and the relations (3.1) and (3.3).

Interpretation. The importance of the bounds of Theorems 3.2 and 3.3 is that they show how much randomness k is sufficient in the randomized inverse in order to obtain a desired level of semantic security. Since v non-confidential messages can be reliably transmitted to Bob, this transforms into a lower bound on the number a of confidential messages.

The bounds of Theorems 3.2 and 3.3 can be improved by "smoothing" W. This means that the outputs of W are restricted to being "typical", i.e., outputs of low probability are cut off. This idea goes back to Renner and Wolf [28]. By smoothing, the conditional divergences can be reduced substantially at the cost of a small additive term in each bound. After smoothing, the channel will in general not be stochastic any more, but only substochastic. The proofs of the theorems remain valid for substochastic channels since they only use the nonnegativity of the entries of W. All that needs to be done is to generalize the Rényi divergences to substochastic channels like in [34].

The bounds can be evaluated by comparing them with the benchmark cases of memoryless discrete and Gaussian wiretap channels (see [9] or [34] for a definition). These wiretap channels actually are families $\{W_n : n \geq 1\}$ of channels; the parameter n indicates the *blocklength*. For these channels, a sequence of security codes achieves *asymptotic optimality* as the blocklength goes to infinity if the largest possible asymptotic communication rate for confidential message transmission, the *secrecy capacity*, is achieved subject to the condition that either (3.5) or (3.6) goes to zero.

Theorems 3.2 and 3.3 show that security functions given by suitable mosaics of BIBDs or of semi-regular GDDs achieve asymptotic optimality when applied to memoryless discrete or Gaussian wiretap channels after smoothing each W_n. This holds even if the channel between Alice and Bob is not perfect, in which case the W_n are concatenations of an encoder and a memoryless channel. For the proof, one proceeds like in [34]. Functional forms of block rate optimal mosaics of singular GDDs turn out to be suboptimal security functions, as discussed below.

We would like to stress, however, that the theorems hold without any further structural assumptions on the channel W. For a targeted level of security and a given channel, they can be used to determine an achievable communication rate at which confidential messages can be sent through the channel using an efficiently computable security code.

Note that both in Theorems 3.2 and 3.3, the wiretap channel enters into the upper bounds only through the conditional Rényi 2-divergences. This gives some robustness against channel variations or limited channel knowledge.

The bounds in the GDD case. Assume that N is the incidence matrix of a $(u, m, k, \lambda_1, \lambda_2)$ GDD and $w \in \mathbb{R}^{\mathcal{X}}$ a nonnegative vector. Set $\lambda_{\max} = \max\{\lambda_1, \lambda_2\}$. Then

$$w^T NN^T w \leq (r - \lambda_{\max})w^T w + \lambda_{\max}(w^T j)^2. \tag{3.7}$$

In the proofs of the GDD cases of Theorems 3.2 and 3.3 , the relation (2.5) is used with equality. By using (3.7) instead of (2.5), one obtains an upper bound of the same form as that obtained in the BIBD case of the theorems, with λ replaced by $\lambda_{\max}$. Since the point

class decomposition of $\mathcal{X}$ associated with the applied mosaic of GDDs will not in general have any special relation to the channel, using this looser upper bound might save the work of estimating the additional Rényi divergence or entropy and give a bound which, for the benchmark cases and for mosaics of BIBDs or of semi-regular GDDs, is asymptotically equivalent to the one appearing in the theorems.

The GDD bounds of Theorems 3.2 and 3.3 can also be simplified without using the upper bound (3.7) by taking the type of the members of the mosaic $M = (D_\alpha)_{\alpha\in\mathcal{A}}$ into consideration.

In the case where the members of M are singular GDDs, every D_α is induced by a BIBD D_α^*. Since the point class partitions of all D_α are the same, all D_α^* have the same parameters v^*, k^*, λ^* and form a mosaic of BIBDs. The coefficients of $D_2(W\|P_\mathcal{X}W|P_\mathcal{X})$ vanish, hence only the divergence involving the point class partition is relevant. In Theorem 3.2, the two nonzero coefficients have the form

$$1 - \frac{r^* - \lambda^*}{k^* r^*} \quad \text{and} \quad \frac{r^* - \lambda^*}{k^* r^*}. \tag{3.8}$$

In Theorem 3.3, both remaining coefficients equal $(r^* - \lambda^*)/k^* r^*$.

Semi-regular GDDs satisfy $rk = \lambda_2 v$. Hence if M consists of semi-regular GDDs, then the three coefficients in Theorem 3.2, in the order of their appearance, equal

$$1, \quad -\frac{r - \lambda_1}{kr}, \quad \frac{r - \lambda_1}{kr}. \tag{3.9}$$

For the case where $\lambda_1 = 0$, in particular, in the case of transversal designs, the same coefficients become

$$1, \quad -\frac{1}{k}, \quad \frac{1}{k}.$$

The coefficients obtain a similarly simple form in Theorem 3.3.

Suboptimality of singular GDDs. When applied in Theorems 3.2 and 3.3, approximately block rate optimal mosaics of singular GDDs with a small color rate and a sufficiently large point set achieve strictly lower color rates than mosaics of BIBDs or of semi-regular GDDs at the same security level. In particular, they turn out to be asymptotically suboptimal in the case of memoryless discrete or Gaussian wiretap channels, where the size of the point set goes to infinity with increasing blocklength. This means that asymptotically optimal sequences of security functions given by mosaics of BIBDs or GDDs for these channels have block rates at least 1.

We only discuss Theorem 3.2 here, the situation is analogous in Theorem 3.3. We begin with the following simple lemma which is the basis of our discussion.

Lemma 3.4 *For a wiretap channel $W : \mathcal{X} \to \mathcal{Z}$ and a partition $\Pi = \{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$ of $\mathcal{X}$ into sets of size u, it holds that*

$$D_2(W\|P_\mathcal{X}W|P_\mathcal{X}) - \log u \le D_2(R_\Pi W\|P_\mathcal{X}W|P_\Pi) \le D_2(W\|P_\mathcal{X}W|P_\mathcal{X}).$$

Equality is possible on both sides. It holds on the left-hand side if and only if for every $z \in \mathcal{Z}$ and $1 \le i \le m$, there exists at most one $x \in \mathcal{X}_i$ such that $w(z|x) > 0$. Equality holds on the right-hand side if and only if for every $z \in \mathcal{Z}$ and every $1 \le i \le m$, the entries $w(z|x)$ are constant for x ranging over $\mathcal{X}_i$.

If one applies Theorem 3.2 with a mosaic of semi-regular GDDs, then one sees from (3.9) that a security level $\max_{P_A} I(A \wedge Z, S)$ smaller than $\delta > 0$ is achieved by choosing $\log k$ equal to $D_2(W\|P_\mathcal{X}W|P_\mathcal{X}) + \log(1/\delta)$. This results in the color rate

$$\tilde{\varrho} = 1 - \frac{D_2(W\|P_\mathcal{X}W|P_\mathcal{X}) + \log(1/\delta)}{\log v}.$$

The same holds in the simpler situation of mosaics of BIBDs.

Now assume that $\tilde{\varrho} < 1/2$. By Sect. 2.3, the only possibility to achieve a security level smaller than δ for the same channel W with an approximately block rate optimal mosaic could be a mosaic M of singular GDDs which is the u-fold multiple of a mosaic M^* of block rate optimal BIBDs and of color rate ϱ^*. When Theorem 3.2 is applied with the security function determined by M, the $D_2(W \| P_{\mathcal{X}} W | P_{\mathcal{X}})$ term vanishes in the upper bound of Theorem 3.2. By (3.8), a security level smaller than δ is achieved by choosing $\log k^*$ equal to $D_2(R_\Pi W \| P_{\mathcal{X}} W | P_\Pi) + \log(1/\delta)$, and without any further information about the channel, this latter expression can be as large as $D_2(W \| P_{\mathcal{X}} W | P_{\mathcal{X}}) + \log(1/\delta)$ by Lemma 3.4.

For the color rate ϱ of M, this means that

$$\varrho = 1 - \frac{\log k}{\log v} = 1 - \frac{\log k^* + \log u}{\log v} \leq \tilde{\varrho} - \frac{\log u}{\log v}. \tag{3.10}$$

This is at most $\tilde{\varrho}$. In fact, for fixed $\tilde{\varrho}$, it is easy to see that $\log u / \log v$ is bounded from below for large v. This is because the approximate block rate optimality of M requires ϱ^* to be at least $\varrho_0(v^*, k^*)$, which tends to $1/2$ as v^* grows. And if v^* is kept small, then u necessarily has to be large.

The loss of color rate as in (3.10) can be avoided if one knows that equality is satisfied in the left-hand inequality of Lemma 3.4 for a certain partition Π. However, an application of this in the security bounds would require knowledge of $D_2(R_\Pi W \| P_{\mathcal{X}} W | P_\Pi)$ and the adaptation of the point class partition of the GDDs to that of the wiretap channel, which is not necessary in the case of mosaics of BIBDs or of semi-regular GDDs.

3.3 Privacy amplification

Now we turn to privacy amplification. Assume that the random variable X is shared by Alice and Bob and that Eve observes a random variable Z correlated with X. Without loss of generality, we assume that $P_Z(z) > 0$ for all $z \in \mathcal{Z}$. Moreover, Alice and Bob both are given the functional form $f : \mathcal{X} \times \mathcal{S} \to \mathcal{A}$ of a mosaic $(D_\alpha)_{\alpha \in \mathcal{A}}$ of (v, k, r) tactical configurations. In order to generate a secret key, Alice and Bob observe a realization x of X, choose a seed $s \in \mathcal{S}$ uniformly at random, and take $\alpha = f(x, s)$ as the secret key. Denote the random variable generated by applying f as described above by A. The joint distribution of X, Z, S and A is

$$P_{XZSA}(x, z, s, \alpha) = \frac{1}{b} P_{XZ}(x, z) N_\alpha(x, s), \tag{3.11}$$

where N_α is the incidence matrix of D_α. The key A should be nearly uniformly distributed on $\mathcal{A}$ and semantically secure with respect to Eve's observation. The first condition is satisfied perfectly.

Lemma 3.5 *The distribution of A is uniform on $\mathcal{A}$.*

Proof Note that $N_\alpha j = rj$, where j denotes the all-ones vector of appropriate dimension. Hence, considering P_X as a vector in $\mathbb{R}^{\mathcal{X}}$ and using (2.1),

$$\begin{aligned} P_A(\alpha) &= \sum_{x,z,s} P_{XZSA}(x, z, s, \alpha) \\ &= \frac{1}{b} \sum_{x,s} P_X(x) N_\alpha(x, s) j(s) = \frac{1}{b} P_X^T N_\alpha j = \frac{r}{b} P_X^T j = \frac{k}{v} = \frac{1}{a}. \end{aligned}$$

□

For semantic security, we can again use total variation distance or mutual information as the security measure. One equivalent formulation of semantic security is the indistinguishability of two possible realizations of the secret. In terms of total variation distance, this means that for any two distinct $\alpha, \alpha' \in \mathcal{A}$, one wants

$$\| P_{ZS|A=\alpha} - P_{ZS|A=\alpha'} \|$$

to be uniformly small. By the triangle inequality, this is true if

$$\| P_{ZS|A=\alpha} - P_Z P_{\mathcal{S}} \| \tag{3.12}$$

is small, uniformly in $\alpha \in \mathcal{A}$.

For any point class partition $\Pi = \{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$ of $\mathcal{X}$, we define the random variable X_Π whose conditional distribution given Z is

$$P_{X_\Pi|Z}(i|z) = P_{X|Z}(\mathcal{X}_i|z).$$

Then we have the following result.

Theorem 3.6 *1) Let P_{XZSA} be the joint distribution (3.11) generated by the functional form of a mosaic of (v, k, λ) BIBDs. Then*

$$\max_{\alpha\in\mathcal{A}} \| P_{ZS|A=\alpha} - P_Z P_{\mathcal{S}} \| \le \left(\frac{r-\lambda}{r}\right)^{1/2} \left(a 2^{-\min_z H_2(X|Z=z)} - \frac{1}{k}\right)^{1/2}$$

2) Let P_{XZSA} be the joint distribution (3.11) generated by the functional form of a mosaic of $(u, m, k, \lambda_1, \lambda_2)$ GDDs with a common point class partition Π. Then

$$\begin{aligned}
&\max_{\alpha\in\mathcal{A}} \| P_{ZS|A=\alpha} - P_Z P_{\mathcal{S}} \| \\
&\quad \le \max_{z\in\mathcal{Z}} \left\{ \frac{a(r-\lambda_1)}{r} 2^{-H_2(X|Z=z)} + \frac{a(\lambda_1-\lambda_2)}{r} 2^{-H_2(X_\Pi|Z=z)} \right. \\
&\qquad \left. - \frac{(r-\lambda_1)+(\lambda_1-\lambda_2)u}{kr} \right\}^{1/2}.
\end{aligned}$$

This is proved in Sect. 4 as a consequence of the next theorem.

If we prefer to measure the indistinguishability of key values with respect to Kullback-Leibler divergence, we should ensure that there exists a probability measure Q on $\mathcal{Z} \times \mathcal{S}$ such that $P_{ZS|A=\alpha}$ is close to Q in terms of Kullback-Leibler divergence, uniformly in $\alpha \in \mathcal{A}$. This is analogous to (3.12). If we choose $Q = P_Z P_{\mathcal{S}}$, then we have the following bound.

Theorem 3.7 *1) Let P_{XZSA} be the joint distribution (3.11) generated by the functional form of a mosaic of (v, k, λ) BIBDs. Then*

$$\max_{\alpha\in\mathcal{A}} \exp\big(D(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}})\big) \le \frac{a(r-\lambda)}{r} 2^{-\min_z H_2(X|Z=z)} + \left(1 - \frac{r-\lambda}{kr}\right).$$

2) Let P_{XZSA} be the joint distribution (3.11) generated by the functional form of a mosaic of $(u, m, k, \lambda_1, \lambda_2)$ GDDs with a common point class partition Π. Then

$$\begin{aligned}
&\max_{\alpha\in\mathcal{A}} \exp\big(D(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}})\big) \\
&\quad \le \max_{z\in\mathcal{Z}} \left\{ \frac{a(r-\lambda_1)}{r} 2^{-H_2(X|Z=z)} + \frac{a(\lambda_1-\lambda_2)}{r} 2^{-H_2(X_\Pi|Z=z)} \right. \\
&\qquad \left. + \left(1 - \frac{(r-\lambda_1)+(\lambda_1-\lambda_2)u}{kr}\right) \right\}.
\end{aligned}$$

The theorem is proved in Sect. 4. As in the wiretap case, its core is Proposition 4.4, proving the equality of $\exp(D_2(P_{S|Z=z,A=\alpha} \| P_{\mathcal{S}}))$ with the z-term in the upper bound.

Remark 3.8 The *strong secrecy* criterion usually applied in information theoretic security for secret key generation assumes that the adversary's a priori knowledge is restricted to the true key distribution. A security function which establishes semantic security also guarantees strong secrecy, since

$$I(A \wedge Z, S) \leq \max_{\alpha \in \mathcal{A}} D(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}}). \tag{3.13}$$

We prove this inequality. It is straightforward to check that for any pair of random variables X, Y on $\mathcal{X} \times \mathcal{Y}$ and any probability measure Q on $\mathcal{Y}$, one has

$$I(X \wedge Y) = D(P_{XY} \| P_X P_Y) = \sum_x P_X(x) D(P_{Y|X=x} \| Q) - D(P_Y \| Q).$$

We use this with $Y = (Z, S)$, $X = A$ and $Q = P_Z P_{\mathcal{S}}$. Then

$$\begin{aligned} I(A \wedge Z, S) &= D(P_{ZSA} \| P_{ZS} P_{\mathcal{A}}) \\ &= \sum_\alpha P_A(\alpha) D(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}}) - D(P_{ZS} \| P_Z P_{\mathcal{S}}) \\ &\leq \max_\alpha D(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}}). \end{aligned}$$

This shows (3.13).

Interpretation. The interpretation of Theorems 3.6 and 3.7 is analogous to that of Theorems 3.2 and 3.3 . The number of interest is a, the size of the key space. Theorems 3.6 and 3.7 give a lower bound on the maximal possible a given a required degree of security, and show that this lower bound is achievable using the functional form of a mosaic of BIBDs or GDDs.

It is proved in [7, Corollary 4] that

$$\exp\big(I(A \wedge S|Z = z)\big) \leq a 2^{-\min_z H_2(X|Z=z)} + 1$$

if the security function is a universal hash function. The upper bound is very similar to the one proved in the first part of Theorem 3.7 for mosaics of BIBDs or of semi-regular GDDs, but only gives strong secrecy. (The conditioning on the event $Z = z$ is also possible in our setting, see (4.7).) It follows that these mosaics yield the same key size as universal hash functions, but resulting in a stronger notion of security and generating a perfectly uniformly distributed key. Mosaics of singular GDDs only involve the $\min_z H_2(X_\Pi|Z = z)$ term and are discussed in more detail below.

If Alice and Bob are connected by a public two-way channel without rate constraint, the secret-key capacity in the benchmark case of a memoryless discrete source model can be achieved by a sequential key distillation protocol guaranteeing semantic security, using functional forms of mosaics of BIBDs or suitable GDDs in the privacy amplification step (cf. [9, Theorem 4.5]).

The bounds in the GDD case. By applying (3.7), the bounds for the GDD cases of Theorems 3.6 and 3.7 can be given the same form as the ones for the BIBD case, with λ replaced by $\lambda_{\max}$.

If the mosaic consists of singular GDDs, then the coefficient of the $H_2(X|Z = z)$ term vanishes. The second and third terms in Theorem 3.7 are

$$\frac{a(r^* - \lambda^*)}{r^*} \quad \text{and} \quad -\frac{r^* - \lambda^*}{k^* r^*},$$

where, like in the wiretap scenario, k^*, r^*, λ^* are parameters of the underlying BIBDs.

In the case of semi-regular GDDs, one has, in the order of their appearance, the three terms

$$\frac{a(r-\lambda_1)}{r}, \quad -\frac{a(r-\lambda_1)}{ur}, \quad 0.$$

In particular, for transversal designs, one obtains

$$a, \quad -1, \quad 0.$$

Similar simplifications are possible for the bounds of Theorem 3.6.

Suboptimality of singular GDDs. As in the wiretap scenario, mosaics of singular GDDs are suboptimal compared with mosaics of BIBDs or of semi-regular GDDs since they require a larger k in order to achieve a comparable security level.

The reasons are analogous to those for the wiretap case, based on the inequalities

$$H_2(X|Z=z) - \log u \le H_2(X_\Pi|Z=z) \le H_2(X|Z=z) \tag{3.14}$$

for any partition $\Pi = \{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$ of $\mathcal{X}$ into sets of size u, and any $z \in \mathcal{Z}$. The condition for equality in the right-hand inequality is that there exist at most one x per $\mathcal{X}_i$ with $P_{X|Z}(x|z) > 0$. On the left-hand side, equality holds if and only if $P_{X|Z}(\cdot|z)$ is constant on each $\mathcal{X}_i$ for every z.

With a mosaic of BIBDs or of semi-regular GDDs, a key size $\log a$ approximately equal to $\min_z H_2(X|Z=z) + \log(1/\delta)$ gives a security level δ.

Now assume that the security function is given by a mosaic of singular GDDs. If one only knows $\min_z H_2(X|Z=z)$, then the largest possible key size $\log a$ by which to guarantee a security level of δ is $H_2(X|Z=z) - \log u + \log(1/\delta)$. The key can be chosen larger if one also knows $\min_z H_2(X_\Pi|Z=z)$. However, the same key size as in the case of BIBDs or semi-regular GDDs is achievable only if there exists a partition Π such that equality is satisfied on the right-hand side of (3.14). If one knows that the joint distribution P_{XZ} has this property for a partition Π, then a mosaic of singular GDDs incurs no rate loss, but the security function has to be adapted to Π.

4 Proofs of the security results

4.1 Proof of Theorems 3.2 and 3.3

We first prove Theorem 3.2. It is sufficient to do the proof for mosaics of GDDs. We start with an upper bound on $\max_{P_A} I(A \wedge Z, S)$ in terms of Kullback-Leibler divergence. The all-ones vector of suitable dimension will be denoted by j, and for each $z \in \mathcal{Z}$, we let w_z be the z-th column of W

Lemma 4.1 *For every joint distribution* (3.4),

$$I(A \wedge Z, S) \le \max_{\alpha \in \mathcal{A}} D(P_{Z|S,A=\alpha} \| P_Z | P_S),$$

and the right-hand side of this inequality is independent of P_A.

Proof The inequality is the statement of [34, Corollary 16], whose proof we will just sketch here. The independence of A and S implies $I(A \wedge Z, S) \le I(A, S \wedge Z)$ using elementary

properties of mutual information. The right-hand mutual information can be expressed as

$$\frac{1}{b}\sum_{s\in\mathcal{S}}\sum_{\alpha\in\mathcal{A}} P_A(\alpha)D(P_{Z|S=s,A=\alpha}\|P_Z) \le \max_{\alpha\in\mathcal{A}} D(P_{Z|S,A=\alpha}\|P_Z|P_{\mathcal{S}}).$$

This gives the claimed inequality.

In order to prove that the upper bound is independent of P_A, we note that (3.4) and (2.1) imply

$$P_Z(z) = \frac{1}{bk}\sum_{\alpha\in\mathcal{A}} P_A(\alpha)w_z^T N_\alpha j = \frac{1}{v}w_z^T j = (P_{\mathcal{X}}W)(z). \tag{4.1}$$

Thus P_Z is independent of P_A. Since $P_{\mathcal{S}}$ and $P_{Z|S,A=\alpha}$ do not depend on P_A either, this proves the lemma. □

Note that, since the eavesdropper also knows S, the validity of (4.1) is not enough to guarantee security.

If we want to use (2.3) or (2.5), we need to pass from Kullback-Leibler to Rényi 2-divergence. By Lemmas 4.1 and (3.2), it is sufficient to show that the upper bound of Theorem 3.2 is an upper bound for

$$\max_{\alpha\in\mathcal{A}} D_2(P_{Z|S,A=\alpha}\|P_Z|P_{\mathcal{S}}). \tag{4.2}$$

$P_{Z|S,A=\alpha}$ is fully determined by N_α and W. Hence for each of the divergence terms in (4.2) it is no longer important that N_α is the incidence matrix of a member of a mosaic. It follows that Theorem 3.2 is a consequence of the following equality.

Proposition 4.2 *Let N be the incidence matrix of a $(u, m, k, \lambda_1, \lambda_2)$ GDD with point set $\mathcal{X}$, block index set $\mathcal{S}$ and point class partition Π, and let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel. Define the random variables Z, X, S on $\mathcal{Z}\times\mathcal{X}\times\mathcal{S}$ by*

$$P_{ZXS}(z, x, s) = \frac{1}{bk}w(z|x)N(x, s). \tag{4.3}$$

Then

$$\begin{aligned}
&\exp\big(D_2(P_{Z|S}\|P_Z|P_{\mathcal{S}})\big)\\
&\quad= \left(1-\frac{(r-\lambda_1)+(\lambda_1-\lambda_2)u}{kr}\right)+\frac{(\lambda_1-\lambda_2)u}{kr}\exp\big(D_2(R_\Pi W\|P_{\mathcal{X}}W|P_\Pi)\big)\\
&\qquad+\frac{r-\lambda_1}{kr}\exp\big(D_2(W\|P_{\mathcal{X}}W|P_{\mathcal{X}})\big).
\end{aligned}$$

Proof As in (4.1), one shows that $P_Z = P_{\mathcal{X}}W$. Since also

$$P_{Z|S}(z|s) = \frac{(w_z^T N)(s)}{k},$$

we can apply (2.5) and obtain

$$\begin{aligned}
&\exp\big(D_2(P_{Z|S}\|P_Z|P_{\mathcal{S}})\big)\\
&\quad= \frac{v}{bk^2}\sum_{s\in\mathcal{S}}\sum_{z\in\mathcal{Z}}\frac{(w_z^T N)(s)^2}{w_z^T j}\\
&\quad= \frac{1}{kr}\sum_{z\in\mathcal{Z}}\frac{w_z^T NN^T w_z}{w_z^T j}
\end{aligned}$$

$$= \frac{r-\lambda_1}{kr} \sum_{z\in\mathcal{Z}} \frac{w_z^T w_z}{w_z^T j} + \frac{\lambda_1-\lambda_2}{kr} \sum_{z\in\mathcal{Z}} \frac{w_z^T C w_z}{w_z^T j} + \frac{\lambda_2}{kr} \sum_{z\in\mathcal{Z}} w_z^T j.$$

Now, observe that

$$\sum_{z\in\mathcal{Z}} \frac{w_z^T w_z}{w_z^T j} = \frac{1}{v} \sum_{x\in\mathcal{X}} \sum_{z\in\mathcal{Z}} \frac{w(z|x)^2}{(P_{\mathcal{X}} W)(z)} = \exp\big(D_2(W \| P_{\mathcal{X}} W | P_{\mathcal{X}})\big).$$

In the second summand, we have

$$\sum_{z\in\mathcal{Z}} \frac{w_z^T C w_z}{w_z^T j} = \frac{u}{m} \sum_{i=1}^{m} \sum_{z\in\mathcal{Z}} \frac{\left(u^{-1} \sum_{x\in\mathcal{X}_i} w(z|x)\right)^2}{(P_{\mathcal{X}} W)(z)} = u \exp\big(D_2(R_\Pi W \| P_{\mathcal{X}} W | P_\Pi)\big).$$

For the third summand, we observe that $\sum_z w_z^T j = v$ and

$$\lambda_2 v = kr - (r-\lambda_1) - (\lambda_1-\lambda_2)u, \tag{4.4}$$

which follows from (2.4). Inserting all this above yields the claimed equality. □

Turning to the proof of Theorem 3.3, we first state the following simple analog of Lemma 4.1.

Lemma 4.3 ([13], Lemma 2)

$$\| P_{ZSA} - P_{ZS} P_A \| \le 2 \| P_{ZSA} - P_Z P_{\mathcal{S}} P_A \|. \tag{4.5}$$

By (4.1), $P_Z(z) = 0$ only if z is not reachable with positive probability from any input of W. Thus

$$P_{ZS|A=\alpha}(\{(z,s) : P_Z(z) P_{\mathcal{S}}(s) = 0\}) = 0.$$

Hence one can apply (3.1) and (3.3) to upper-bound the right-hand side of (4.5) by

$$\begin{aligned} 2 \max_{\alpha\in\mathcal{A}} \| P_{ZS|A=\alpha} - P_Z P_{\mathcal{S}} \| &\le 2 \max_{\alpha\in\mathcal{A}} \sqrt{\chi^2(P_{ZS|A=\alpha} - P_Z P_{\mathcal{S}})} \\ &= 2 \max_{\alpha\in\mathcal{A}} \sqrt{\exp\big(D_2(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}})\big) - 1} \\ &= 2 \max_{\alpha\in\mathcal{A}} \sqrt{\exp\big(D_2(P_{Z|S,A=\alpha} \| P_Z | P_{\mathcal{S}})\big) - 1}. \end{aligned}$$

Theorem 3.3 now follows from Proposition 4.2.

4.2 Proof of Theorems 3.6 and 3.7

We start by proving Theorem 3.7. Define the $\mathbb{R}^{\mathcal{X}}$-vector p_z by

$$p_z(x) = P_{XZ}(x,z).$$

From (3.11), Lemmas 3.5 and (2.1), it follows that

$$P_{Z|A}(z|\alpha) = a \sum_{x,s} P_{XZSA}(x,z,s,\alpha) = \frac{a}{b} p_z^T N_\alpha j = \frac{ar}{b} p_z^T j = p_z^T j. \tag{4.6}$$

In particular, Z is independent of A. (Of course, since the eavesdropper also knows S, this is not yet enough to guarantee security.) A straightforward computation gives

$$D(P_{ZS|A=\alpha} \| P_Z P_{\mathcal{S}}) \leq \max_{z \in \mathcal{Z}} D(P_{S|Z=z,A=\alpha} \| P_{\mathcal{S}}). \tag{4.7}$$

As in the wiretap case, one passes to Rényi 2-divergence, and so it remains to bound

$$D_2(P_{S|Z=z,A=\alpha} \| P_{\mathcal{S}}),$$

uniformly in z and α.

We compute $P_{S|Z=z,A=\alpha}$ as follows. Recall the assumption that $P_Z(z) > 0$ for all $z \in \mathcal{Z}$. Let $\alpha \in \mathcal{A}$ and $s \in \mathcal{S}$. The uniform distribution of A and (4.6) imply that $P_{ZA}(z,\alpha) = a^{-1} p_z^T j$. Hence, again applying (2.1),

$$\begin{aligned} P_{S|Z=z,A=\alpha}(s) &= \frac{a \sum_x P_{XZSA}(x,z,s,\alpha)}{p_z^T j} \\ &= \frac{a}{b p_z^T j} \sum_x P_{XZ}(x,z) N_\alpha(x,s) = \frac{(p_z^T N_\alpha)(s)}{r p_z^T j}. \end{aligned} \tag{4.8}$$

This only depends on the incidence matrix N_α, and so as in the wiretap case, we can reduce the proof of Theorem 3.7 to a proposition which holds for GDDs without any reference to mosaics.

Proposition 4.4 *Let N be the incidence matrix of a $(u,m,k,\lambda_1,\lambda_2)$ GDD with point set $\mathcal{X}$, block index set $\mathcal{S}$ and point class partition Π. Let $\mathcal{Z}$ be a finite set and define the random variables X, Z, S on $\mathcal{X}, \mathcal{Z}, \mathcal{S}$, respectively, by their joint distribution*

$$P_{XZS}(x,z,s) = \frac{1}{r} P_{XZ}(x,z) N(x,s). \tag{4.9}$$

Then

$$\begin{aligned} \exp\big(D_2(P_{S|Z=z} \| P_{\mathcal{S}})\big) = \frac{v(r-\lambda_1)}{kr} 2^{-H_2(X|Z=z)} + \frac{v(\lambda_1-\lambda_2)}{kr} 2^{-H_2(X_\Pi|Z=z)} \\ + \left(1 - \frac{(r-\lambda_1)+(\lambda_1-\lambda_2)u}{kr}\right). \end{aligned}$$

Proof As in (4.8), it holds that $P_{S|Z}(s|z) = (p_z^T N)(s)/r p_z^T j$. Using (2.5), one obtains

$$\begin{aligned} &\exp\big(D_2(P_{S|Z=z} \| P_{\mathcal{S}})\big) \\ &= \sum_s \frac{b (p_z^T N)(s)^2}{r^2 (p_z^T j)^2} \\ &= \frac{v p_z^T N N^T p_z}{kr (p_z^T j)^2} \\ &= \frac{v}{kr (p_z^T j)^2} \left((r-\lambda_1) p_z^T p_z + (\lambda_1-\lambda_2) p_z^T C p_z + \lambda_2 (p_z^T j)^2\right) \\ &= \frac{v(r-\lambda_1)}{kr} 2^{-H_2(X|Z=z)} + \frac{v(\lambda_1-\lambda_2)}{kr} 2^{-H_2(X_\Pi|Z=z)} + \frac{v\lambda_2}{kr}. \end{aligned}$$

The proof is complete upon replacing the last summand using (4.4). □

This completes the proof of Theorem 3.7.

In order to prove Theorem 3.6, we can appeal to the case where security is measured using divergence, just like in the wiretap case. It is a straightforward computation to show that

$$\|P_{ZS|A=\alpha} - P_Z P_{\mathcal{S}}\| \leq \max_z \|P_{S|Z=z,A=\alpha} - P_{\mathcal{S}}\|$$

for all $\alpha \in \mathcal{A}$. Using (3.1) and (3.3), we see that Theorem 3.6 follows from Proposition 4.4.

Remark 4.5 Let N be the incidence matrix of a (v, k, r) tactical decomposition for which there exist nonnegative numbers c and d such that

$$w^T N N^T w \leq c w^T w + d(w^T j)^2 \tag{4.10}$$

for all nonnegative vectors w. Propositions 4.2 and 4.4 can be generalized for such matrices, with an inequality instead of an equality.

Let $W : \mathcal{X} \to \mathcal{Z}$ be a wiretap channel and define the random variables Z, X, S on $\mathcal{Z} \times \mathcal{X} \times \mathcal{S}$ as in (4.3). Proceeding as in the proof of Proposition 4.2, one can show that

$$\exp\big(D_2(P_{Z|S}\|P_Z|P_{\mathcal{S}})\big) \leq \frac{dv}{kr} + \frac{c}{kr}\exp\big(D_2(W\|P_{\mathcal{X}}W|P_{\mathcal{X}})\big).$$

Similarly, in privacy amplification with source distribution P_{XZ} and with the seed jointly distributed with Z according to (4.9), one obtains

$$\exp\big(D_2(P_{S|Z=z}\|P_{\mathcal{S}})\big) \leq \frac{ac}{r}2^{-H_2(X|Z=z)} + \frac{ad}{r},$$

proceeding as in the proof of Proposition 4.4.

For example, if NN^T has largest eigenvalue μ_1 and second-largest eigenvalue μ_2, then

$$w^T N N^T w \leq \mu_2 w^T w + \frac{\mu_1 - \mu_2}{v}(w^T j)^2.$$

Mosaics of such matrices were studied in the wiretap scenario in [34].

Another example of a matrix satisfying (4.10) arises from the incidence matrix of a $(u, m, k, \lambda_1, \lambda_2)$ GDD, see (3.7).

Theorems 3.2, 3.3, 3.6 and 3.7 can also be generalized to mosaics of tactical configurations whose incidence matrices satisfy (4.10), since the reduction of the theorems to Propositions 4.2 and 4.4 only used that the security functions are functional forms of mosaics of tactical configurations.

5 Explicitness of Denniston's BIBD

Let $t \geq 2$ and $1 \leq \ell \leq t$. Set $q = 2^t$. Recall that Denniston's design D, defined in Sect. 2.6, has the point set

$$\mathcal{X} = \{(x, y) \in \mathbb{F}_q^2 : Q(x, y) \in H\},$$

where Q is an irreducible quadratic form and H a subgroup of $\mathbb{F}_q$ of order ℓ. We will consider $\mathbb{F}_q$ as a t-dimensional vector space over $\mathbb{F}_2$, which makes H an ℓ-dimensional subspace of $\mathbb{F}_q$. The blocks of D are given by the nontrivial intersections of lines of $AG(2, q)$ with $\mathcal{X}$.

Proposition 5.1 *There exists an H such that D is explicit.*

The proof of this proposition will be done in the subsections following below. We first observe that the proposition implies that the mosaic $M^{(2)}_{t,\ell,H}$ whose members are isomorphic to D is explicit. This follows from Theorem 2.9 together with the efficiency of addition and subtraction on the cyclic group $\mathbb{Z}_a$, which serves as the color set for the mosaic.

5.1 Characterization of $\mathcal{X}$ and $\mathcal{S}$

Denote by $L_{c,d} = \{(x, cx + d) : x \in \mathbb{F}_q\}$ the line in $AG(2, q)$ with *slope* $c \in \mathbb{F}_q$ and *intercept* $d \in \mathbb{F}_q$. This are all lines of $AG(2, q)$ except the "vertical" ones with infinite slope, given by $L_{\infty,d} = \{(d, y) : y \in \mathbb{F}_q\}$, for any $d \in \mathbb{F}_q$. For these lines, we call d the *intercept*.

For the characterization of $\mathcal{X}$ and $\mathcal{S}$, we choose H arbitrary. Note that $0 \in \mathcal{X}$. Thus every line $L_{c,0}$ ($c \in \mathbb{F}_q \cup \{\infty\}$) has nontrivial intersection $\mathcal{X}_c$ with $\mathcal{X}$. Since any two of these lines only meet in 0, the union of all these $\mathcal{X}_c$ has precisely

$$v = 1 + (2^t + 1)(2^\ell - 1) = 2^{t+\ell} + 2^\ell - 2^t$$

elements, and so $\mathcal{X}$ must equal the union of all $\mathcal{X}_c$ by (2.14). Now assume $c \in \mathbb{F}_q$. An element (x, cx) of $L_{c,0}$ is contained in $\mathcal{X}_c$ if and only if

$$x^2(\eta_1 + \eta_2 c + \eta_3 c^2) \in H,$$

or equivalently, $x^2 \in (\eta_1 + \eta_2 c + \eta_3 c^2)^{-1} H$ (the irreducibility of Q ensures that $\eta_1 + \eta_2 c + \eta_3 c^2$ is nonzero). In an analogous way one sees that $(0, y) \in \mathcal{X}_\infty$ if and only if $y^2 \in \eta_3^{-1} H$.

Lemma 5.2 *The set $\mathcal{X}$ is given by the disjoint union*

$$\{(0,0)\} \cup \bigcup_{c \in \mathbb{F}_q} \left\{ (x, cx) : x \neq 0, x^2 \in \frac{1}{\eta_1 + \eta_2 c + \eta_3 c^2} H \right\}$$
$$\cup \left\{ (0, y) : y \neq 0, y^2 \in \frac{1}{\eta_3} H \right\}.$$

Next we turn to $\mathcal{S}$. We already noted in Sect. 2 that the parallel classes of D are in one-to-one correspondence with those of $AG(2, q)$, i.e., with the slopes from $\mathbb{F}_q \cup \{\infty\}$.

For the description of the elements of a parallel class, we need the *(absolute) trace* of an element x of $\mathbb{F}_q$ defined by

$$\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{t-1}}.$$

The trace is an $\mathbb{F}_2$-linear form from $\mathbb{F}_q$ onto $\mathbb{F}_2$. Every linear form ξ from $\mathbb{F}_q$ to $\mathbb{F}_2$ corresponds to a unique element $\beta \in \mathbb{F}_q$ such that $\xi(x) = \mathrm{Tr}(\beta x)$ for all $x \in \mathbb{F}_q$ (see [24, Theorem 2.23]). We denote by $H^\perp$ the $(t-\ell)$-dimensional subspace of $\mathbb{F}_q$ consisting of those elements whose corresponding linear form vanishes on H.

We will also use the following facts on polynomials. The first one is [24, Theorem 2.25], the second one is elementary.

Fact 5.3 1) The polynomial $x^2 + x + \alpha$, with $\alpha \in \mathbb{F}_q$, has a root in $\mathbb{F}_q$ if and only if $\mathrm{Tr}(\alpha) = 0$.

2) Let $F(x) = \alpha x^2 + \beta x + \gamma$ be a polynomial over $\mathbb{F}_q$. Then $F(c) = 0$ if and only if $\alpha c/\beta$ is a root of

$$x^2 + x + \frac{\alpha\gamma}{\beta^2}.$$

We have the following lemma.

Lemma 5.4 *For any $c \in \mathbb{F}_q \cup \{\infty\}$, denote by $\mathcal{U}_c$ the set of those $d \in \mathbb{F}_q$ for which $L_{c,d}$ has nonempty intersection with $\mathcal{X}$. If $c \in \mathbb{F}_q$, then*

$$\mathcal{U}_c = \left\{ d \neq 0 : d^{-2} \notin \frac{\eta_2^2}{\eta_1 + \eta_2 c + \eta_3 c^2} H^\perp \right\} \cup \{0\}. \tag{5.1}$$

If $c = \infty$, then

$$\mathcal{U}_c = \left\{ d \neq 0 : d^{-2} \notin \frac{\eta_2^2}{\eta_3} H^\perp \right\} \cup \{0\}.$$

Proof We use Fact 5.3. Let $c, d \in \mathbb{F}_q$. For $L_{c,0}$ we already know that it has nonempty intersection with $\mathcal{X}$, so assume $d \neq 0$. Then $L_{c,d}$ has nonempty intersection with $\mathcal{X}$ if and only if the polynomial

$$F(x) = (\eta_1 + \eta_2 c + \eta_3 c^2)x^2 + \eta_2 dx + \eta_3 d^2$$

assumes a value in H for some $x \in \mathbb{F}_q$. By Fact 5.3, this is the case if and only if there exists a $z \in H$ such that

$$\mathrm{Tr}\left(\frac{(\eta_1 + \eta_2 c + \eta_3 c^2)(\eta_3 d^2 + z)}{\eta_2^2 d^2} \right) = 0.$$

The term inside the trace can be written as

$$\frac{(\eta_1 + \eta_2 c + \eta_3 c^2)z}{\eta_2^2 d^2} + \frac{\eta_1 \eta_3}{\eta_2^2} + \left(\frac{\eta_3 c}{\eta_2} + \frac{\eta_3^2 c^2}{\eta_2^2} \right).$$

The sum inside the large brackets has trace zero since $\mathrm{Tr}(\alpha) + \mathrm{Tr}(\alpha^2) = 0$ for all $\alpha \in \mathbb{F}_q$. The trace of $(\eta_1\eta_3)/\eta_2^2$ equals 1 due to the irreducibility of Q. It follows that $z \in H$ satisfies $F(x) = z$ for some $x \in \mathbb{F}_q$ if and only if

$$\mathrm{Tr}\left(\frac{(\eta_1 + \eta_2 c + \eta_3 c^2)z}{\eta_2^2 d^2} \right) = 1.$$

Hence a nonzero $d \in \mathbb{F}_q$ is *not* contained in $\mathcal{U}_c$ if and only if

$$\frac{(\eta_1 + \eta_2 c + \eta_3 c^2)}{\eta_2^2 d^2} \in H^\perp,$$

which immediately shows (5.1). The proof for $c = \infty$ is analogous. □

5.2 Property (D1)

D is explicit if it satisfies properties (D1) and (D2) formulated in Sect. 2.5. Here we show that it satisfies (D1) for suitable H. Let $\Theta = \{1, \vartheta, \vartheta^2, \ldots, \vartheta^{t-1}\}$ be a polynomial basis of $\mathbb{F}_q$. We take H as the span of $1, \ldots, \vartheta^{\ell-1}$. Let $\Phi_H : [k] \to \mathbb{F}_2^\ell$ be a bijection which in time poly$(\log k)$ associates to every number from $[k]$ a unique element of H, represented in terms of Θ, such that $\Phi_H(0) = 0$.

Denote by $\Phi_{\mathcal{R}} : [q+1] \to \mathbb{F}_2^t \cup \{\infty\}$ a poly$(\log q)$ time bijection between $[q+1]$ and the set of slopes $\mathcal{R} = \mathbb{F}_q \cup \{\infty\}$, where $\Phi(\tilde{\imath})$ for any $\tilde{\imath} \in [q]$ is the representation in the basis Θ of a unique element of $\mathbb{F}_q$.

Arithmetic operations in $\mathbb{F}_q$ can be performed efficiently in Θ, as well as the computation of the square root [2, Corollary 7.1.2]. Hence using $\Phi_{\mathcal{R}}$ and Φ_H, one obtains a mapping $\Phi_{\mathcal{X}} : [v] \to \mathbb{F}_2^t$ which to every element of $[v]$ associates the Θ-representation of a unique element of $\mathcal{X}$ (see Lemma 5.2). This mapping is computable in time poly$(\log v)$.

To the basis Θ there exists a *dual* basis $Z = \{\zeta_1, \ldots, \zeta_t\}$ satisfying

$$\mathrm{Tr}(\zeta_i \vartheta^j) = \delta_{ij}.$$

$H^\perp$ is the span of $\{\zeta_\ell, \ldots, \zeta_{t-1}\}$. Denote by T the change-of-basis matrix representing every ζ_i in terms of Θ. Then for any c, there exists a bijective mapping $\Phi_{\mathcal{U}_c} : [a] \to \mathbb{F}_2^t$ which to any element of $[a]$ first associates the Z-representation of an element of $(\mathbb{F}_q \setminus H^\perp) \cup \{0\}$, then changes the basis to Θ using T, and finally does the necessary arithmetic to obtain an element of $\mathcal{U}_c$. The values of this mapping can be computed in time poly$(t) =$ poly$(\log a)$.

Now assume we are given numbers $\tilde{x} \in [v]$ and $\tilde{\imath} \in [q+1]$, corresponding to the point $(x, \tilde{c}x) \in \mathcal{X}$ and the parallel class $c \in \mathbb{F}_q \cup \{\infty\}$ via $\Phi_{\mathcal{X}}$ and $\Phi_{\mathcal{R}}$. We want to find the intercept d such that $(x, \tilde{c}x) \in L_{c,d}$. If $c \in \mathbb{F}_q$, then $d = (c + \tilde{c})x$. If $c = \infty$, then $d = x$. It is straightforward to do these computations in Θ. The result is transformed to a number from $[a]$ via $\Phi_{\mathcal{U}_c}^{-1}$. The representation of d in $[a]$ can be found from inputs $\tilde{x}$ and $\tilde{\imath}$ in poly$(\log v)$ time.

5.3 Property (D2)

Let $(c, d) \in \mathcal{S}$ be given. We want to find the set $B_{c,d}$ of those elements of $\mathcal{X}$ which are incident with (c, d) in D. For $d = 0$, we have $L_{c,d} = \mathcal{X}_c \cup \{0\}$. Now we consider the case $d \neq 0$. Let

$$\mathcal{R}_{c,d} = \{\tilde{c} \in \mathcal{R} : L_{c,d} \cap \mathcal{X}_{\tilde{c}} \neq \emptyset\}.$$

Once we know the set $\mathcal{R}_{c,d}$, we can for every $\tilde{c} \in \mathcal{R}_{c,d}$ find the unique point at the intersection of $L_{c,d}$ and $\mathcal{X}_{\tilde{c}}$. If $\tilde{c} \in \mathbb{F}_q$, this point has the form $(x, \tilde{c}x)$ for

$$x = \frac{d}{c + \tilde{c}}$$

(clearly, $c \neq \tilde{c}$). If $\tilde{c} = \infty$, the point at the intersection of $L_{c,d}$ and $\mathcal{X}_\infty$ is given by $(0, d)$.

For $c \in \mathbb{F}_q$, define the set

$$H_{c,d} = \left\{ z \in H : \mathrm{Tr}\left(\frac{(\eta_1 + \eta_2 c + \eta_3 c^2) z}{\eta_2^2 d^2} \right) = 1 \right\}$$

and, for every $z \in H_{c,d}$, the polynomial

$$G_{c,d,z}(w) = w^2 + w + \frac{(\eta_1 d^2 + c^2 z)(z + \eta_3 d^2)}{\eta_2^2 d^4}.$$

For $c = \infty$, we set

$$H_{c,d} = \left\{ z \in H : \mathrm{Tr}\left(\frac{\eta_3 z}{\eta_2^2 d^2} \right) = 1 \right\}$$

and define, for all $z \in H_{c,d}$, the polynomial

$$G_{c,d,z}(w) = w^2 + w + \frac{\eta_3 d^2(\eta_1 d^2 + z)}{\eta_2^2 d^4}.$$

All $H_{c,d}$ are nonempty due to the proof of Lemma 5.4.

Lemma 5.5 *If $c \in \mathbb{F}_q$ and $\eta_3 d^2 \notin H$, then*

$$\mathcal{R}_{c,d} = \left\{ \frac{\eta_2 d^2 w}{z + \eta_3 d^2} : w \text{ root of } G_{c,d,z},\ z \in H_{c,d} \right\}.$$

If $c \in \mathbb{F}_q$ and $\eta_3 d^2 \in H$, then

$$\mathcal{R}_{c,d} = \left\{ \frac{\eta_2 d^2 w}{z + \eta_3 d^2} : w \text{ root of } G_{c,d,z},\ z \in H_{c,d} \setminus \{\eta_3 d^2\} \right\} \cup \left\{ \frac{\eta_1 + \eta_3 c^2}{\eta_2}, \infty \right\}.$$

If $c = \infty$, then

$$\mathcal{R}_{c,d} = \left\{ \frac{\eta_2 w}{\eta_3} : w \text{ root of } G_{c,d,z},\ z \in H_{c,d} \right\}.$$

Proof We start with the case $c \in \mathbb{F}_q$ and $\eta_3 d^2 \notin H$. There exists an $x \in \mathbb{F}_q$ such that $(x, \tilde{c}x) \in \mathcal{X}_{\tilde{c}} \cap L_{c,d}$ if and only if

$$\frac{d^2}{c^2 + \tilde{c}^2} \in \frac{1}{\eta_1 + \eta_2 \tilde{c} + \eta_3 \tilde{c}^2} H,$$

which is equivalent to the existence of a $z \in H$ such that

$$(z + \eta_3 d^2)\tilde{c}^2 + \eta_2 d^2 \tilde{c} + \eta_1 d^2 + c^2 z = 0. \tag{5.2}$$

By Fact 5.3.2), $\tilde{c}$ is a root of this equation if and only if $\eta_2^{-1} d^{-2}(z + \eta_3 d^2)\tilde{c}$ is a root of $G_{c,d,z}$.

It follows from the proof of Lemma 5.4 that the set of $z \in H$ for which $G_{c,d,z}$ has a root in $\mathbb{F}_q$ necessarily is equal to $H_{c,d}$. One can also check this directly using Fact 5.3. Write the constant term of $G_{c,d,z}$ as

$$\frac{\eta_1 \eta_3}{\eta_2^2} + \frac{(\eta_1 + \eta_2 c + \eta_3 c^2) z}{\eta_2^2 d^2} + \left(\frac{cz}{\eta_2 d^2} + \frac{c^2 z^2}{\eta_2^2 d^4} \right).$$

As in the proof of Lemma 5.4, one concludes that the set of $z \in H$ where $G_{c,d,z}$ has a root in $\mathbb{F}_q$ is given by $H_{c,d}$, as claimed. Each root w of $G_{c,d,z}$ gives a root $\tilde{c}$ of (5.2), and this gives the claimed form of $\mathcal{R}_{c,d}$.

Now assume $c \in \mathbb{F}_q$ and $\eta_3 d^2 \in H$. Then (5.2) has two distinct roots as in the previous case unless $z = \eta_3 d^2$, in which case the quadratic term vanishes. This gives $\tilde{c} = (\eta_1 + \eta_3 c^2)/\eta_2$ (the irreducibility of Q ensures $\eta_2 \neq 0$). One checks directly that $\infty \in \mathcal{R}_{c,d}$.

The case $c = \infty$ is treated analogously to the first case. □

Remark 5.6 We note that for distinct $z, z' \in H_{c,d}$, the roots of the corresponding $G_{c,d,z}$ and $G_{c,d,z'}$ are different. This follows from a simple counting argument. Assume $c \in \mathbb{F}_q$ and $\eta_3 d^2 \notin H$, the other cases are analogous. Since $|\mathcal{R}_{c,d}| = |B_{c,d}| = 2^\ell$, we know from the proof of Lemma 5.5 that the total number of roots of $G_{c,d,z}$ as z ranges over $H_{c,d}$ is 2^ℓ.

Now $G_{c,d,z}$ has two distinct roots in $\mathbb{F}_q$ for every $z \in H_{c,d}$, for if $G_{c,d,z}(w) = 0$, then $G_{c,d,z}(w+1) = 0$. Moreover, $H_{c,d}$ is the coset of an $(\ell - 1)$-dimensional subspace of H.

It remains to check that (D2) is satisfied. Let $\tilde{\imath} \in [q+1]$ correspond to a parallel class and $\tilde{\kappa} \in [a]$ to an element of this parallel class. Through the mapping $\Phi_{\mathcal{R}}$, one associates to $\tilde{\imath}$ a slope $c \in \mathbb{F}_q \cup \{\infty\}$. Then $\Phi_{\mathcal{U}_c}(\tilde{\kappa})$ gives an intercept d such that $(c, d) \in \mathcal{S}$, where both c and d are represented in the basis Θ. It remains to show that the set $\mathcal{R}_{c,d}$ can be enumerated in polylogarithmic time. The first task is to find $H_{c,d}$. We shall use that if $\beta = \sum_{i=0}^{t-1} \beta_i \zeta_i$ and $z = \sum_{i=0}^{t-1} z_i \vartheta^i$, then $\mathrm{Tr}(\beta z) = \sum_{i=0}^{t-1} \beta_i z_i$.

Assume that $c \in \mathbb{F}_q$ and $\eta_3 d^2 \notin H$ (which can be checked by representing $\eta_3 d^2$ in the basis Z). The other cases are similar. Using the Θ-representations of c and d, compute

$$\beta = \frac{\eta_1 + \eta_2 c + \eta_3 c^2}{\eta_2^2 d^2}.$$

Transform the result to Z. Now assume that $\beta = \sum_{i=0}^{t-1} \beta_i \zeta_i$. Since $H_{c,d}$ is nonempty, the linear form $z \mapsto \mathrm{Tr}(\beta z)$ does not vanish on H. Hence $\beta_i = 1$ for some $0 \le i \le \ell - 1$, say $\beta_{\ell-1} = 1$. One can now enumerate the Θ-representations of all elements of $H_{c,d}$ by enumerating all sequences $z_0, \ldots, z_{\ell-2}$ and choosing $z_{\ell-1}$ such that $\sum_{i=0}^{\ell-1} \beta_i z_i = 1$.

Given $z \in H_{c,d}$, it remains to find both roots of $G_{c,d,z}$. This means that one has to solve the inhomogeneous linear equation

$$\tilde{c}^2 + \tilde{c} = \frac{(\eta_1 d^2 + z)(\eta_1 d^2 + c^2 z)}{\eta_2^2 d^2}.$$

If $\tilde{c}$ satisfies this equation, then $\tilde{c} + 1$ is the other solution. This equation can be solved in polylogarithmic time in q, and so it is possible to find the points of $\mathcal{X}$ incident with (c, d) in polylogarithmic time.

Remark 5.7 In the way they were described here, it appears obvious that property (D1) requires less computation than (D2) for Denniston's BIBD, although both operations have the same complexity class. For the computation of the functional form, only the former operation is necessary.

For the computation of the randomized inverse of the functional form, recall that it is possible, as pointed out in Sect. 2.4, to first choose the point from $\mathcal{X}$ uniformly at random, and then to choose an $s \in \mathcal{S}$ such that $f(x, s) = \alpha$ if α is the message to be transmitted. In this approach, it is sufficient to randomly choose $c \in \mathcal{R}$ and then to solve for the intercept $d \in \mathcal{A}$ as in (D1).

Acknowledgements The authors would like to thank Eike Kiltz for discussions about the achievability of semantic security using modular coding schemes. H. Boche would also like to thank Marc Geitz, Oliver Holschke and Frank Fitzek for discussions about the application of modular wiretap coding schemes in communication networks.
Both authors were supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. H. Boche was also partly supported by the National Research Initiative of the German Ministry for Education and Research (BMBF) on 6G Communication Systems through the research hub 6G-life (16KISK002).

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence,

and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Arora S., Barak B.: Computational Complexity: A Modern Approach. Cambridge University Press, New York (2009).
2. Bach E., Shallit J.: Algorithmic Number Theory. Efficient Algorithms, vol. 1. MIT Press, Cambridge (1996).
3. Bellare M., Tessaro S., Vardy A.: Semantic security for the wiretap channel. In: Safavi-Naini R., Canetti R. (eds.) CRYPTO 2012, vol. 7417, pp. 294–311. Lecture Notes in Computer Science. Springer, Berlin Heidelberg (2012).
4. Bellare, M., Tessaro, S., Vardy, A.: A cryptographic treatment of the wiretap channel (2012). arxiv:1201.2205v2
5. Bellare, M., Tessaro, S.: Polynomial-time, semantically-secure encryption achieving the secrecy capacity (2012). arxiv:1201.3160v2
6. Bennett C.H., Brassard G., Robert J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988).
7. Bennett C.H., Brassard G., Crépeau C., Maurer U.M.: Generalized privacy amplification. IEEE Trans. Inform. Theory **41**(6), 1915–1923 (1995).
8. Beth T., Jungnickel D., Lenz H.: Design Theory. Cambridge University Press, Cambridge (1999).
9. Bloch M., Barros J.: Physical-Layer Security. Cambridge University Press, Cambridge (2009).
10. Bose R.C., Connor W.S.: Combinatorial properties of group divisible incomplete block designs. Ann. Math. Stat. **23**(3), 367–383 (1952).
11. Cheraghchi M., Didier F., Shokrollahi A.: Invertible extractors and wiretap protocols. IEEE Trans. Inform. Theory **58**(2), 1254–1274 (2012).
12. Clatworthy W.H.: Tables of Two-Associate-Class Partially Balanced Designs. U.S. Department of Commerce, National Bureau of Standards, Washington, D.C. (1973).
13. Csiszár I.: Almost independence and secrecy capacity. Probl. Inform. Transm. **32**(1), 40–47 (1996).
14. Ćustić, A., Krčadinac, V., Zhou, Y.: Tiling groups with difference sets. Electron. J. Combin. **22**(2) (2015)
15. Denniston R.: Some maximal arcs in finite projective planes. J. Comb. Theory **6**(3), 317–319 (1969).
16. Fettweis, G.P., Boche, H.: 6G: the personal tactile internet-and open questions for information theory. IEEE BITS the Information Theory Magazine (2021)
17. Gnilke O.W., Greferath M., Pavčević M.O.: Mosaics of combinatorial designs. Des. Codes Cryptogr. **86**(1), 85–95 (2017).
18. Greferath M., Therkelsen R.K.: On coloured constant composition designs. Discret. Math. **309**(8), 2410–2416 (2009).
19. Hanani, H.: On transversal designs. In: Combinatorics, Part 1, Mathematical Centre tracts, vol. 55, pp. 43–53. Mathematisch Centrum, Amsterdam (1975)
20. Hayashi M.: Upper bounds of eavesdropper's performances in finite-length code with the decoy method. Phys. Rev. A **76**(1), 012329 (2007).
21. Hayashi M.: Exponential decreasing rate of leaked information in universal random privacy amplification. IEEE Trans. Inform. Theory **57**(6), 3989–4001 (2011).
22. Hayashi M.: Security analysis of ε-almost dual universal$_2$ hash functions: smoothing of min entropy versus smoothing of Rényi entropy of order 2. IEEE Trans. Inform. Theory **62**(6), 3451–3476 (2016).
23. Hayashi M., Matsumoto R.: Secure multiplex coding with dependent and non-uniform multiple messages. IEEE Trans. Inform. Theory **62**(5), 2355–2409 (2016).
24. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1996).
25. Maurer U., Wolf S.: Information-theoretic key agreement: from weak to strong secrecy for free. In: Preneel B. (ed.) Advances in Cryptology—EUROCRYPT 2000, vol. 1807, pp. 351–368. Lecture Notes in Computer Science. Springer, Berlin (2000).
26. Menezes A.J., van Oorschot P.C., Vanstone S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1997).
27. Neumaier A.: $t\frac{1}{2}$-designs. J. Combin. Theory Ser. A **28**(3), 226–248 (1980).

28. Renner R., Wolf S.: Simple and tight bounds for information reconciliation and privacy amplification. In: Roy B. (ed.) ASIACRYPT 2005, vol. 3788, pp. 199–216. Lecture Notes in Computer Science. Springer, Berlin (2005).
29. Stinson D.R.: Combinatorial techniques for universal hashing. J. Comput. Syst. Sci. **48**(2), 337–346 (1994).
30. Stinson D.R.: Universal hashing and authentication codes. Des. Codes Cryptogr. **4**(3), 369–380 (1994).
31. Torres-Figueroa L., Mönich U.J., Voichtleitner J., Frank A., Andrei V.C., Wiese M., Boche H.: Experimental evaluation of a modular coding scheme for physical layer security. In: Proc. IEEE Global Communications Conference (GLOBECOM) (2021).
32. Tyagi H., Vardy A.: Universal hashing for information-theoretic security. Proc. IEEE **103**(10), 1781–1795 (2015).
33. van Erven T., Harremoës P.: Rényi divergence and Kullback-Leibler divergence. IEEE Trans. Inform. Theory **60**(7), 3797–3820 (2014).
34. Wiese M., Boche H.: Semantic security via seeded modular coding schemes and Ramanujan graphs. IEEE Trans. Inform. Theory **67**(1), 52–80 (2021).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.