Combinatorial Designs for Authentication and Secrecy Codes

Combinatorial Designs for Authentication and Secrecy Codes

Michael Huber

University of Tuebingen
Sand 13, D-72076 Tuebingen
Germany
michael.huber@uni-tuebingen.de

the essence of knowledge

Boston – Delft

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is M. Huber, Combinatorial Designs for Authentication and Secrecy Codes, Foundations and Trends® in Communications and Information Theory, vol 5, no 6, pp 581–675, 2008

ISBN: 978-1-60198-358-9

Foundations and Trends® in
Communications and Information Theory
Volume 5 Issue 6, 2008

Editorial Scope

Foundations and Trends® in Communications and Information Theory will publish survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2008, Volume 5, 6 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328. Also available as a combined paper and online subscription.

Foundations and Trends® in
Communications and Information Theory
Vol. 5, No. 6 (2008) 581–675

DOI: 10.1561/0100000044

Combinatorial Designs for Authentication and Secrecy Codes

Michael Huber

Wilhelm Schickard Institute for Computer Science, University of Tuebingen, Sand 13, D-72076 Tuebingen, Germany, michael.huber@uni-tuebingen.de

Abstract

Combinatorial design theory is a very active area of mathematical research, with many applications in communications and information theory, computer science, statistics, engineering, and life sciences. As one of the fundamental discrete structures, combinatorial designs are used in fields as diverse as error-correcting codes, statistical design of experiments, cryptography and information security, mobile and wireless communications, group testing algorithms in DNA screening, software and hardware testing, and interconnection networks. This monograph provides a tutorial on combinatorial designs, which gives an overview of the theory. Furthermore, the application of combinatorial designs to authentication and secrecy codes is described in depth. This close relationship of designs with cryptography and information security was first revealed in Shannon's seminal paper on secrecy systems. We bring together in one source foundational and current contributions concerning design-theoretic constructions and characterizations of authentication and secrecy codes.

Contents

1

Introduction

Authenticity and secrecy are two crucial concepts in cryptography and information security. Concerning authenticity, typically communicating parties would like to be assured of the integrity of information they obtain via potentially insecure channels. Regarding secrecy, protection of the confidentiality of sensitive information shall be ensured in the presence of eavesdropping. Although independent in their nature, various scenarios require that both aspects hold simultaneously. For information-theoretic, or unconditional, security (i.e. robustness against an attacker that has unlimited computational resources), authentication and secrecy codes can be used to minimize the possibility of an undetected deception. The construction of such codes is of great importance and has been considered by many researchers over the last few decades. Often deep mathematical tools are involved in the constructions, mainly from combinatorics. This close relationship of cryptography and information security with combinatorics has been first revealed in Shannon's landmark paper "Communication theory of secrecy systems" [182]: a key-minimal secrecy system provides perfect secrecy if and only if the encryption matrix is a Latin square and the keys are used with equal probability. The initial construction of authentication codes goes back to Gilbert et al. [74], and uses finite projective planes. A more general and systematic theory of authenticity was developed by Simmons (see [183, 184, 185, 186, 187], and [188] for a survey). Further foundational works on authentication and secrecy codes have been carried out by Massey [152] and Stinson et al. [194, 195, 196, 201, 202]. A generalized information-theoretic framework for authentication was introduced by Maurer [157].

The purpose of this monograph is to describe in depth classical and current interconnections between combinatorial designs and authentication and secrecy codes. The latter also include the author's recent [102, 106, 107] and new contributions (cf. Section 3.4) on multi-fold secure authentication and secrecy codes in various models. Moreover, this issue provides a tutorial overview on the theory of combinatorial designs. These fundamental discrete structures find applications in fields as diverse as error-correcting codes, statistical design of experiments, cryptography and information security, mobile and wireless communications, group testing algorithms in DNA screening, software and hardware testing, and interconnection networks. In particular, the last few years have witnessed an increasing body of work in the communications and information theory literature that makes substantial use of results in combinatorial design theory.

The organization of the monograph is as follows. Section 1.1 introduces the Shannon–Simmons model of information-theoretical authentication and secrecy. We define the important concepts of spoofing attacks and perfect secrecy. A short historical account on combinatorial designs is given in Section 1.2. Since permutation groups often play a crucial role in the construction of combinatorial designs, we introduce basic notions on permutation groups and group actions in Section 1.3. Section 2 provides a tutorial account on combinatorial design theory. We emphasize on the construction of various combinatorial structures including t-designs, finite geometries, Latin squares, orthogonal arrays, perpendicular and authentication perpendicular arrays, splitting t-designs, and others. These combinatorial structures provide essential tools for the construction and characterization of authentication and secrecy codes in the following section. A special notice is placed on examples for each type of combinatorial designs. We also briefly point to the interplay between t-designs and error-correcting codes. Section 3 is devoted to various key applications of combinatorial designs to authentication and secrecy codes. Foundational and recent results concerning the construction and characterization of authentication and secrecy codes are exposed. Starting with Shannon's classical result, we first deal with secrecy codes in Section 3.1. Authentication codes without any secrecy requirements are considered in Section 3.2. In Section 3.3, codes that offer both authenticity and secrecy are discussed in detail. We distinguish between arbitrary and equiprobable source probability distributions. The advantage of the source states being equiprobable distributed is that the number of encoding rules can be reduced. Section 3.4 is devoted to an extended authentication model, where the opponent can act pro-actively by having access to a verification oracle. Authentication codes with splitting are considered in Section 3.5. In such a code, several messages can be used to communicate a particular plaintext (non-deterministic encoding). We briefly mention authentication codes that permit arbitration in Section 3.6. In Section 3.7, further recent applications are highlighted which makes substantial use of combinatorial design theory. Finally, we conclude in Section 3.8 with a synthesis of the work and some directions for future research.

1.1 Authentication and Secrecy Model

We rely on the *information-theoretical* (or *unconditional*) secrecy model developed by Shannon [182], and by Simmons [183, 184, 185, 188] including authentication. Information-theoretical security means that the security of the model is not dependent on any complexity assumptions and hence cannot be broken given unlimited computational resources. A well-known practical application of such a perfectly-secure system is the Washington–Moscow Hotline ("red telephone") during the time of the cold war. Modern applications may include protection of digital data where cryptographic long-term security and/or confidentiality is strongly required, e.g., in archiving official documents, notarial contracts, court records, medical data, state secrets, copyright protection as well as further areas concerning e-government, e-health, e-publication, etc.

The reader may be interested in the area of information-theoretical cryptography [156], long-term secure cryptography [33], post-quantum cryptography [15], and in the broad area of cryptography in general [77, 78, 159, 200].

1.1.1 Basic Preliminaries

We introduce the *basic model* of information-theoretical authentication and secrecy. Our notation follows, for the most part, that of [152, 195]. Figure 1.1 gives an illustration of the model (cf. [152, 195]).

In this basic model of authentication and secrecy three participants are involved: a *transmitter*, a *receiver*, and an *opponent*. The transmitter wants to communicate information to the receiver via a public communications channel. The receiver in return would like to be confident that any received information actually came from the transmitter and not from some opponent (*integrity* of information). The transmitter and the receiver are assumed to trust each other. Sometimes this is also called an *A-code*. Variants of this model will be discussed in Sections 3.4, 3.5, and 3.6.

In what follows, let $\mathcal{S}$ denote a set of k *source states* (or *plaintexts*), $\mathcal{M}$ a set of v *messages* (or *ciphertexts*), and $\mathcal{E}$ a set of b *encoding rules* (or *keys*). Using an encoding rule $e \in \mathcal{E}$, the transmitter encrypts a source state $s \in \mathcal{S}$ to obtain the message $m = e(s)$ to be sent over the

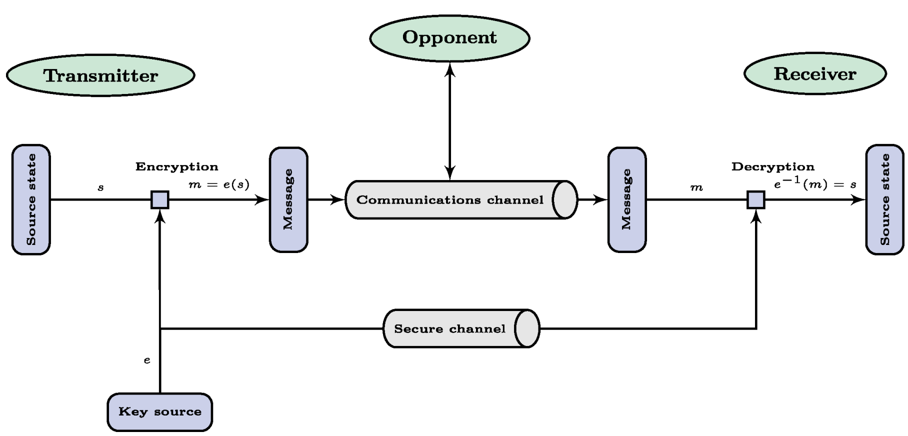

Fig. 1.1 Shannon–Simmons authentication and secrecy model.

channel. The encoding rule is an injective function from $\mathcal{S}$ to $\mathcal{M}$, and is communicated to the receiver via a secure channel prior to any messages being sent. For a given encoding rule $e \in \mathcal{E}$, let $M(e) := \{e(s) \mid s \in \mathcal{S}\}$ denote the set of *valid* messages. For an encoding rule e and a set $M^* \subseteq M(e)$ of distinct messages, we define $f_e(M^*) := \{s \in \mathcal{S} \mid e(s) \in M^*\}$, i.e., the set of source states that will be encoded under encoding rule e by a message in M^*. Furthermore, we define $E(M^*) := \{e \in \mathcal{E} \mid M^* \subseteq M(e)\}$, i.e., the set of encoding rules under which all the messages in M^* are valid. A received message m will be accepted by the receiver as being authentic if and only if $m \in M(e)$. When this is fulfilled, the receiver decrypts the message m by applying the decoding rule e^{-1}, where

$$e^{-1}(m) = s \Leftrightarrow e(s) = m.$$

An authentication code can be represented algebraically by a $(b \times k)$-*encoding matrix* with the rows indexed by the encoding rules, the columns indexed by the source states, and the entries defined by $a_{es} := e(s)$ $(1 \leq e \leq b,\ 1 \leq s \leq k)$.

1.1.2 Protection Against Spoofing Attacks

We introduce the scenario of a *spoofing attack* of order i (cf. [152]): Suppose that an opponent observes $i \geq 0$ distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message m' (being distinct from the i messages already sent), hoping to have it accepted by the receiver as authentic. The cases $i = 0$ and $i = 1$ are called *impersonation game* and *substitution game*, respectively. These cases have been studied in detail in recent years (see, for instance, [196, 201, 27, 53, 165]), however less is known for the cases $i \geq 2$. In this monograph, we especially focus on those cases where $i \geq 2$.

For any i, we assume that there is some probability distribution on the set of i-subsets of source states, so that any set of i source states has a non-zero probability of occurring. For simplification, we ignore the order in which the i source states occur, and assume that no source state occurs more than once. Given this probability distribution p_S on

$\mathcal{S}$, the receiver and transmitter choose a probability distribution p_E on $\mathcal{E}$, called an *encoding strategy*, with associated independent random variables S and E, respectively. These distributions are known to all participants and induce a third distribution, p_M, on $\mathcal{M}$ with associated random variable M. The *deception probability* P_{d_i} is the probability that the opponent can deceive the receiver with a spoofing attack of order i. The following theorem by Massey provides combinatorial lower bounds (for the proof, we follow [194, 195]).

Theorem 1.1 (Massey [152]). In an authentication code with k source states and v messages, for every $0 \le i \le t$, the deception probabilities are bounded below by

$$P_{\mathrm{d}_i} \ge \frac{k-i}{v-i}.$$

Proof. Let $M^* \subset \mathcal{M}$ denote a set of $i \le t$ distinct messages. We suppose that an opponent observes the i messages in the channel, and then sends a message $m \in \mathcal{M}$ not in M^*. Let payoff(m, M^*) denote the probability that the message m would be accepted by the receiver as authentic. Then

$$\mathrm{payoff}(m, M^*) = \frac{\sum_{e \in E(M^* \cup \{m\})} p(e) \cdot p(S = f_e(M^*))}{\sum_{e \in E(M^*)} p(e) \cdot p(S = f_e(M^*))}.$$

It follows that

$$\sum_{m \in \mathcal{M} \setminus M^*} \mathrm{payoff}(m, M^*) = k - i.$$

Hence, there exists some $m \in \mathcal{M}$ not in M^* such that payoff$(m, M^*) \ge (k-i)/(v-i)$. For every set M^* of i messages, the opponent can choose such an m. This defines a deception strategy in which the transmitter/receiver can be deceived with probability at least $(k-i)/(v-i)$. □

An authentication code is called t_A*-fold secure against spoofing* if $P_{\mathrm{d}_i} = (k-i)/(v-i)$ for all $0 \le i \le t_A$.

1.1.3 Perfect Secrecy

We address Shannon's fundamental idea of perfect secrecy (cf. [182]): An authentication code is said to have *perfect secrecy* if

$$p_S(s|m) = p_S(s)$$

for every source state $s \in \mathcal{S}$ and every message $m \in \mathcal{M}$.

That is, the *a posteriori* probability that the source state is s, given that the message m is observed, is identical to the *a priori* probability that the source state is s.

It can easily be shown via Bayes' Theorem that

$$p_S(s|m) = \frac{p_M(m|s) \cdot p_S(s)}{p_M(m)} \tag{1.1}$$

$$= \frac{\sum_{\{e \in \mathcal{E} | e(s)=m\}} p_E(e) \cdot p_S(s)}{\sum_{\{e \in \mathcal{E} | m \in M(e)\}} p_E(e) \cdot p_S(e^{-1}(m))}. \tag{1.2}$$

Moreover, we introduce the concept of perfect multi-fold secrecy established by Stinson [195], which generalizes Shannon's perfect (one-fold) secrecy. An alternative definition has been given by Godlewski and Mitchell [75]. Instead of assuming that each encoding rule is used to encode only one message, the situation is extended in a natural way: each encoding rule is used to encode up to t_S messages for some positive integer t_S. More formally, we say that an authentication code has *perfect t_S-fold secrecy* if, for every positive integer $t^* \leq t_S$, for every set M^* of t^* messages observed in the channel, and for every set S^* of t^* source states, we have

$$p_S(S^*|M^*) = p_S(S^*).$$

That is, the *a posteriori* probability distribution on the t^* source states, given that a set of t^* messages is observed, is identical to the *a priori* probability distribution on the t^* source states. Obviously, for the case $t_S = 1$ this coincides with the definition of perfect secrecy.

When clear from the context, we often only write t instead of t_A respectively t_S.

As the encoding rules have to be communicated to the receiver via a secure channel, i.e. $\log_2 b$ bits for b encoding rules, we want to minimize the number of encoding rules. With respect to the minimal number, we will deal with the construction and characterization of *optimal* authentication and secrecy codes in Section 3.

Remark 1.1. We note that the term *secrecy code* (sometimes also secrecy system) is customarily used in the above model to describe a cipher that achieves Shannon's perfect secrecy over *noiseless* channels. This should not be confused with the same expression often used today for describing codes that can achieve both reliable and secure communication over *noisy* channels (also known as wiretap channels). For recent developments on information-theoretic security for noisy channels, we refer to the monograph [142] and the references therein.

1.2 Combinatorial Designs: A Brief Historical Account

Combinatorial designs have a long and rich history of work. We briefly highlight three historical examples:

Leonhard Euler considered in 1782 the following problem [64], posed by Catherine the Great according to folklore. This problem came to known as *Euler's 36 Officers Problem*:

> "A very curious question, which has exercised for some time the ingenuity of many people, has involved me in the following studies, which seem to open a new field of analysis, in particular the study of combinations. The question resolves around arranging 36 officers to be drawn from 6 different ranks and also from 6 different regiments so that they are ranged in a square so that in each line (both horizontal and vertical) there are 6 officers of different ranks and different regiments."

This question asks for finding two orthogonal Latin squares of order 6. Euler correctly conjectured that this was impossible, and a complete proof with an exhaustive search of all Latin squares of order 6 were given in 1900 by Tarry [207, 208]. A short proof is due to Stinson [193].

The Swiss geometer Jakob Steiner posed in 1853 in his classical "Combinatorische Aufgabe" [192] the following question:

> "Welche Zahl, N, von Elementen hat die Eigenschaft, dass sich die Elemente so zu dreien ordnen lassen, dass je zwei in einer, aber nur in einer Verbindung vorkommen?"
> [Transl.: "For what number, N, of elements is it possible to arrange the elements in triplets, so that every pair of elements is contained in one and only one triplet?"]

Writing v, k, and t instead of N, 3, and 2, respectively, leads us to the definition of what is now called a *Steiner t-design* (or a *Steiner system*, cf. Definition 2.1). However, there had been earlier work on these combinatorial designs going back to, in particular, Plücker, Woolhouse, and most notably Kirkman.

Thomas Kirkman's famous *15 Schoolgirl Problem*, which he proposed in 1850 in the popular magazine *The Lady's and Gentleman's Diary* [132], states as follows:

> "Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast."

This is equivalent to the problem of constructing a Steiner 2-design with parameters $k = 3$ and $v = 15$, having the extra requirement that the set of triples can be partitioned into seven 'parallel classes'. Kirkman's problem as well as the more general case for other possible values of v attracted great interest among late 19th and early 20th century mathematicians, including contributions by Burnside, Cayley and Sylvester. However, it was not until 1971 that the general problem was completely resolved by Ray-Chaudhuri and Wilson [173], showing that there exists at least one such design for every $v \equiv 3 \pmod 6$. For $v = 15$, there are seven different solutions to the problem (up to isomorphism). For all other admissible values $v \geq 21$, the number of solutions remains unknown up to the present.

For an detailed account on the history of combinatorial designs, we refer the interested reader, e.g., to [43, Chap. I.2] and [225].

1.3 Some Group Theory

Often permutation groups play a crucial role in the construction of combinatorial designs. We introduce basic notions on permutation groups and group actions in this section. We will restrict ourselves to finite groups, although most of the concepts also make sense for infinite groups.

Let X be a non-empty finite set. The set $\mathrm{Sym}(X)$ of all permutations of X with respect to the composition

$$x^{gh} := (x^g)^h \ \text{ for } \ x \in X \ \text{ and } \ g,h \in \mathrm{Sym}(X)$$

forms a group, called the *symmetric group* on X. If $X = \{1,\ldots,v\}$, then we write S_v for the *symmetric group of degree* v. Clearly, $\mathrm{Sym}(X) \cong S_v$ if and only if $|X| = v$.

A group G *acts* (or *operates*) on X, if to each element $g \in G$ a permutation $x \mapsto x^g$ of X is assigned such that

(i) $x^1 = x$ for all $x \in X$ (where $1 = 1_G$ denotes the identity element of G),
(ii) $(x^g)^h = x^{gh}$ for all $x \in X$ and all $g, h \in G$.

Evidently, these properties are fulfilled if and only if the map

$$\varphi : g \mapsto (x \mapsto x^g)$$

of G into $\mathrm{Sym}(X)$ is a group homomorphism. In general, any homomorphism φ of G into $\mathrm{Sym}(X)$ is said to be an *action* (or a *permutation representation*) of G on X. If $\ker(\varphi) = 1$ for the kernel of φ, then G acts *faithfully* on X; in this case, G is a called a *permutation group* on X. If $\ker(\varphi) = G$, then G operates *trivially* on X. The *degree* of a permutation group is the size of X.

Example 1.1. The group of symmetries of a three-dimensional cube (cf. Figure 2.3) acts on various sets including the set of 8 vertices, the set of 6 faces, the set of 12 edges, and the set of 4 principal diagonals. Properties (i) and (ii) are clearly satisfied in each case.

Let G_1 and G_2 be permutation groups acting on the sets X_1 and X_2, respectively. Then, G_1 and G_2 are called *permutation isomorphic*, if there exists a group isomorphism $\sigma\colon G_1 \to G_2$ and a bijective map $\tau\colon X_1 \to X_2$ with

$$(x^g)^\tau = (x^\tau)^{(g^\sigma)}$$

for all $x \in X_1$ and all $g \in G_1$. Essentially, this means that the groups G_1 and G_2 are "the same" except for the labeling of the points.

Let G be a group acting on X. For $x \in X$, the subgroup

$$G_x := \{g \in G \mid x^g = x\}$$

denotes the *(point-)stabilizer* of x in G and the set

$$x^G := \{x^g \mid g \in G\}$$

is the *orbit* of x under G (or the G-*orbit* of x). For $B \subseteq X$, let

$$G_B := \{g \in G \mid B^g = B\}$$

be its *setwise stabilizer*. The *order* of G is denoted by $|G|$.

A group G acting on X is called *transitive* on X, if G has only one orbit, i.e. $x^G = X$ for all $x \in X$. Equivalently, G is transitive if for any two points $x, y \in X$ there exists an element $g \in G$ with $x^g = y$. For a positive integer $t \leq |X|$, we call G to be t-*transitive*, if for any two injective t-tuples $(x_1, x_2, \dots, x_t)$ and $(y_1, y_2, \dots, y_t)$ there exists an element $g \in G$ with ${x_i}^g = y_i$ for all $1 \leq i \leq t$. We say that G is t-*homogeneous*, if it is transitive on the set of all t-subsets of X. Obviously, t-transitive implies t-homogeneous.

Example 1.2. The symmetric group S_v is v-transitive, and the alternating group A_v (i.e., the subgroup of S_v consisting of all even permutations) is $(v-2)$-transitive in their actions on the set $\{1, \dots, v\}$ $(v \geq 3)$.

We will list all finite multiply homogeneous permutation groups in Appendix 4.1. We note that this classification relies on the Classification of the Finite Simple Groups (CFSG), one of the most powerful tools of modern algebra.

For a detailed treatment of finite group theory and permutation groups, we refer the reader to [5, 38, 41, 61, 117, 118, 139, 223].

References

[1] R. J. R. Abel, C. J. Colbourn, and J. H. Dinitz, "Mutually orthogonal Latin squares (MOLS)," in *Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), pp. 160–193, Boca Raton: CRC Press, 2006.

[2] M. Aigner, *A Course in Enumeration*. Berlin, Heidelberg, New York: Springer, 2007.

[3] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, "Construction of low-density parity-check codes based on balanced incomplete block designs," *IEEE Transactions on Information Theory*, vol. 50, pp. 1257–1269, 2004.

[4] M. Aschbacher, *Sporadic Groups*. Cambridge: Cambridge University Press, 1994.

[5] M. Aschbacher, *Finite Group Theory*. Cambridge: Cambridge University Press, 2000.

[6] E. F. Assmus Jr. and J. D. Key, *Designs and Their Codes*. Cambridge: Cambridge University Press, 1993.

[7] E. F. Assmus Jr. and J. D. Key, "Designs and codes: an update," *Designs, Codes and Cryptography*, vol. 9, pp. 7–27, 1996.

[8] E. F. Assmus Jr. and H. F. Mattson Jr., "On tactical configurations and error-correcting codes," *Journal of Combinatorial Theory, Series A*, vol. 2, pp. 243–257, 1967.

[9] E. F. Assmus Jr. and H. F. Mattson Jr., "New 5-designs," *Journal of Combinatorial Theory, Series A*, vol. 6, pp. 122–151, 1969.

[10] E. F. Assmus Jr. and H. F. Mattson Jr., "Coding and combinatorics," *SIAM Review*, vol. 16, pp. 349–388, 1974.

[11] R. A. Bailey, *Design of Comparative Experiments*. Cambridge: Cambridge University Press, 2008.

[12] R. A. Bailey, P. J. Cameron, and R. Connelly, "Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes," *The American Mathematical Monthly*, vol. 115, pp. 383–404, 2008.

[13] J. A. Barrau, "On the combinatory problem of Steiner," in *Proc. Sect. Sci. Konink. Akad. Wetensch. Amsterdam*, pp. 352–360, 1908.

[14] M. Bellare, O. Goldreich, and A. Mityagin, "The power of verification queries in message authentication and authenticated encryption," *Cryptology ePrint Archive*, Report 2004/309, 2004.

[15] D. J. Bernstein, J. Buchmann, and E. Dahmen, eds., *Post-Quantum, Cryptography.* Berlin, Heidelberg, New York: Springer, 2009.

[16] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory,* vols. I and II, Encyclopedia of Math. and Its Applications, vol. 69/78. Cambridge: Cambridge University Press, 1999.

[17] A. Betten, E. Haberberger, R. Laue, and A. Wassermann, *DISCRETA — A Program to Construct t-Designs with Prescribed Automorphism Group.* Available at http://www.algorithm.uni-bayreuth.de/en/research/discreta/index.html.

[18] A. Betten, R. Laue, S. Molodtsov, and A. Wassermann, "Steiner systems with automorphism groups $PSL(2,71)$, $PSL(2,83)$ and $P\Sigma L(2,3^5)$," *Journal of Geometry*, vol. 67, pp. 35–41, 2000.

[19] A. Betten, R. Laue, and A. Wassermann, "A Steiner 5-design on 36 points," *Designs, Codes and Cryptography*, vol. 17, pp. 181–186, 1999.

[20] A. Beutelspacher, "Projective planes," in *Handbook of Incidence Geometry*, (F. Buekenhout, ed.), pp. 101–136, Amsterdam, New York, Oxford: North-Holland, 1995.

[21] A. Beutelspacher, *Einführung in die endliche Geometrie I: Blockpläne.* Mannheim, Wien, Zürich: Bibliographisches Institut, 2006.

[22] J. Bierbrauer, "Ordered designs, perpendicular arrays, and permutation sets," in *Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), pp. 543–547, Boca Raton: CRC Press, 2006.

[23] J. Bierbrauer and Y. Edel, "Theory of perpendicular arrays," *Journal of Combinatorial Designs*, vol. 2, pp. 375–406, 1994.

[24] J. Bierbrauer and T. van Trung, "Halving $PGL(2,2^f)$, f odd: A series of cryptocodes," *Designs, Codes and Cryptography*, vol. 1, pp. 141–148, 1991.

[25] J. Bierbrauer and T. van Trung, "Some highly symmetric authentication perpendicular arrays," *Designs, Codes and Cryptography*, vol. 1, pp. 307–319, 1991.

[26] I. F. Blake, "Codes and designs," *Mathematics Magazine*, vol. 52, pp. 81–95, 1979.

[27] C. Blundo, A. De Santis, K. Kurosawa, and W. Ogata, "On a fallacious bound for authentication codes," *Journal of Cryptology*, vol. 12, pp. 155–159, 1999.

[28] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *Journal of Cryptology*, vol. 12, pp. 261–289, 1999.

[29] M. Bose and R. Mukerjee, "Optimal (k,n) visual cryptographic schemes for general k," *Designs, Codes and Cryptography*, vol. 55, pp. 19–35, 2010.

[30] E. F. Brickell, "A few results in message authentication," *Congressus Numerantium*, vol. 43, pp. 141–154, 1984.

[31] R. H. Bruck and H. J. Ryser, "The non-existence of certain finite projective planes," *Canadian Journal of Mathematics*, vol. 1, pp. 88–93, 1949.

[32] R. C. Bryce and C. J. Colbourn, "A density-based greedy algorithm for higher strength covering arrays," *Software Testing, Verification and Reliability*, vol. 19, pp. 37–53, 2009.

[33] J. Buchmann, A. May, and U. Vollmer, "Perspectives for cryptographic long-term security," *Communications of the ACM*, vol. 49, pp. 50–55, 2006.

[34] F. Buekenhout, ed., *Handbook of Incidence Geometry.* Amsterdam, New York, Oxford: North-Holland, 1995.

[35] P. J. Cameron, *Parallelisms of Complete Designs.* London Mathematical Society, Lecture Note Series, vol. 23. Cambridge: Cambridge University Press, 1976.

[36] P. J. Cameron, "Finite permutation groups and finite simple groups," *Bulletin of the London Mathematical Society*, vol. 13, pp. 1–22, 1981.

[37] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms.* Cambridge: Cambridge University Press, 1994. Reprint (1996).

[38] P. J. Cameron, *Permutation Groups.* Cambridge: Cambridge University Press, 1999.

[39] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links.* Cambridge: Cambridge University Press, 1991.

[40] Z. Cao, G. Ge, and Y. Miao, "Combinatorial characterizations of one-coincidence frequency-hopping sequences," *Designs, Codes and Cryptography*, vol. 41, pp. 177–184, 2006.

[41] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order.* Boston: Ginn, 1937. Reprint: Dover Publications, New York, 1956.

[42] C. J. Colbourn, "Triple systems," in *Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), pp. 58–71, Boca Raton: CRC Press, 2006.

[43] C. J. Colbourn and J. H. Dinitz, eds., *Handbook of Combinatorial Designs.* Boca Raton: CRC Press, 2nd ed., 2006.

[44] C. J. Colbourn, J. H. Dinitz, and D. R. Stinson, "Applications of combinatorial designs to communications, cryptography, and networking," in *Surveys in Combinatorics,* London Mathematical Society, Lecture Note Series, vol. 267, (J. D. Lamb and D. A. Preece, eds.), pp. 37–100, Cambridge: Cambridge University Press, 1999.

[45] C. J. Colbourn, T. Kløve, and A. C. H. Ling, "Permutation arrays for powerline communication and mutually orthogonal latin squares," *IEEE Transactions on Information Theory*, vol. 50, pp. 1289–1291, 2004.

[46] C. J. Colbourn and R. Mathon, "Steiner systems," in *Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), pp. 102–110, Boca Raton: CRC Press, 2006.

[47] C. J. Colbourn and A. Rosa, *Triple Systems.* Oxford: Oxford University Press, 1999.

[48] C. J. Colbourn and P. C. van Oorschot, "Applications of combinatorial designs in computer science," *ACM Computing Surveys*, vol. 21, pp. 223–250, 1989.

[49] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*. Oxford: Oxford University Press, 1985.

[50] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. Berlin, Heidelberg, New York: Springer, 3rd ed., 1998.

[51] C. W. Curtis, W. M. Kantor, and G. M. Seitz, "The 2-transitive permutation representations of the finite Chevalley groups," *Transactions of the American Mathematical Society*, vol. 218, pp. 1–59, 1976.

[52] M. De Soete, "Some constructions for authentication-secrecy codes," in *Advances in Cryptology — EUROCRYPT 1988*, Lecture Notes in Computer Science, vol. 330, (C. G. Günther, ed.), pp. 23–49, Berlin, Heidelberg, New York: Springer, 1988.

[53] M. De Soete, "New bounds and constructions for authentication-secrecy codes with splitting," *Journal of Cryptology*, vol. 3, pp. 173–186, 1991.

[54] P. Dembowski, *Finite Geometries*. Berlin, Heidelberg, New York: Springer, 1968. Reprint (1997).

[55] J. Dénes and A. D. Keedwell, *Latin Squares: New Developments in the Theory and Applications*, Annals of Discrete Math., vol. 46. Amsterdam, New York, Oxford: North-Holland, 1991.

[56] R. H. F. Denniston, "Some new 5-designs," *Bulletin of the London Mathematical Society*, vol. 8, pp. 263–267, 1976.

[57] R. H. F. Denniston, "A small 4-design," *Annals of Discrete Mathematics*, vol. 18, pp. 291–294, 1983.

[58] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/Multi-sender network security: Efficient authenticated multicast/feedback," in *Proceedings of IEEE Infocom 1992*, pp. 2045–2054, 1992.

[59] C. Ding, A. Salomaa, P. Solé, and X. Tian, "Three constructions of authentication/secrecy codes," *Journal of Pure and Applied Algebra*, vol. 196, pp. 149–168, 2005.

[60] C. Ding and X. Tian, "Three constructions of authentication codes with perfect secrecy," *Designs, Codes and Cryptography*, vol. 33, pp. 227–239, 2004.

[61] J. D. Dixon and B. Mortimer, *Permutation Groups*. Berlin, Heidelberg, New York: Springer, 1996.

[62] D.-Z. Du and F. K. Hwang, *Pooling Designs and Nonadaptive Group Testing: Important Tools for DNA Sequencing*. Singapore: World Scientific, 2006.

[63] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes and Cryptography*, vol. 25, pp. 15–61, 2002.

[64] L. Euler, "Recherches sur une nouvelle espéce de quarrès magiques," *Verh. Zeeuwsch. Genootsch. Wetensch. Vlissingen*, vol. 9, pp. 85–239, 1782.

[65] R. A. Fisher, *The Design of Experiments*. Edinburgh: Oliver and Boyd, 1935. 9th ed., NewYork: Macmillan, 1971.

[66] R. A. Fisher, "An examination of the different possible solutions of a problem in incomplete blocks," *Annals of Eugenics*, vol. 10, pp. 52–75, 1940.

[67] F. Fitting, "Zyklische Lösungen des Steiner'schen Problems," *Nieuw. Arch. Wisk.*, vol. 11, pp. 140–148, 1915.

[68] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: A combinatorial approach," *IEEE Transactions on Information Theory*, vol. 50, pp. 2408–2420, 2004.

[69] H. Fujii, W. Kachen, and K. Kurosawa, "Combinatorial bounds and design of broadcast authentication," *IEICE Transactions*, vol. E97-A, pp. 502–506, 1996.

[70] G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency-hopping sequences," *Journal of Combinatorial Theory, Series A*, vol. 113, pp. 1699–1718, 2006.

[71] G. Ge, Y. Miao, and L. Wang, "Combinatorial constructions for optimal splitting authentication codes," *SIAM Journal on Discrete Mathematics*, vol. 18, pp. 663–678, 2005.

[72] G. Ge, Y. Miao, and Z. Yao, "Optimal frequency hopping sequences: Auto- and cross-correlation properties," *IEEE Transactions on Information Theory*, vol. 55, pp. 867–879, 2009.

[73] G. Ge, Y. Miao, and L. Zhu, "GOB designs for authentication codes with arbitration," *Designs, Codes and Cryptography*, vol. 40, pp. 303–317, 2006.

[74] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *Bell System Technical Journal*, vol. 53, pp. 405–424, 1974.

[75] P. Godlewski and C. Mitchell, "Key-minimal cryptosystems for unconditional secrecy," *Journal of Cryptology*, vol. 3, pp. 1–25, 1990.

[76] M. J. E. Golay, "Notes on digital coding," *Proceedings of IRE*, vol. 37, p. 657, 1949.

[77] O. Goldreich, *Foundations of Cryptography,* vols. I and II. Cambridge: Cambridge University Press, 2001/2004.

[78] O. Goldreich, "Foundations of Cryptography — A Primer," *Foundations and Trends in Theoretical Computer Science*, vol. 1, pp. 1–116, 2005.

[79] K. Gopalakrishnan and D. R. Stinson, "Secrecy and authentication codes," in *Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), pp. 606–611, Boca Raton: CRC Press, 2006.

[80] D. Gorenstein, *Finite Simple Groups. An Introduction to Their Classification.* New York, London: Plenum Publishing Corp., 1982.

[81] R. L. Graham, M. Grötschel, and L. Lovász, eds., *Handbook of Combinatorics,* vols. I and II. Amsterdam, New York, Oxford: North-Holland, 1995.

[82] M. J. Grannell and T. S. Griggs, "On Steiner systems $S(5,6,24)$," *Ars Combinatoria*, vol. 8, pp. 45–48, 1979.

[83] M. J. Grannell, T. S. Griggs, and R. Mathon, "Some Steiner 5-designs with 108 and 132 points," *Journal of Combinatorial Designs*, vol. 1, pp. 213–238, 1993.

[84] M. J. Grannell, T. S. Griggs, and R. Mathon, "Steiner systems $S(5,6,v)$ with $v = 72$ and 84," *Mathematics of Computation*, vol. 67, pp. 357–359, 1998.

[85] A. Granville, A. Moisiadis, and R. Rees, "Nested Steiner n-gon systems and perpendicular arrays," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 3, pp. 163–167, 1988.

[86] M. Hall Jr., *Combinatorial Theory*. New York: J. Wiley, 1986.
[87] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical Journal*, vol. 29, pp. 147–160, 1950.
[88] H. Hanani, "On quadruple systems," *Canadian Journal of Mathematics*, vol. 12, pp. 145–157, 1960.
[89] H. Hanani, "A class of three-designs," *Journal of Combinatorial Theory, Series A*, vol. 26, pp. 1–19, 1979.
[90] A. Hartman, "Software and hardware testing using combinatorial covering suites," in *Interdisciplinary Applications of Graph Theory, Combinatorics, and Algorithms*, (M. C. Golumbic and I. B.-A. Hartman, eds.), pp. 237–266, Berlin, Heidelberg, New York: Springer, 2005.
[91] A. Hartman and K. T. Phelps, "Steiner quadruple systems," in *Contemporary Design Theory*, (J. H. Dinitz and D. R. Stinson, eds.), pp. 205–240, New York: Wiley, 1992.
[92] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays: Theory and Applications*. Berlin, Heidelberg, New York: Springer, 1999.
[93] C. Hering, "Transitive linear groups and linear groups which contain irreducible subgroups of prime order," *Geometriae Dedicata*, vol. 2, pp. 425–460, 1974.
[94] C. Hering, "Transitive linear groups and linear groups which contain irreducible subgroups of prime order II," *Journal of Algebra*, vol. 93, pp. 151–164, 1985.
[95] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford: Oxford University Press, 1998.
[96] M. Huber, "Classification of flag-transitive Steiner quadruple systems," *Journal of Combinatorial Theory, Series A*, vol. 94, pp. 180–190, 2001.
[97] M. Huber, "The classification of flag-transitive Steiner 3-designs," *Advances in Geometry*, vol. 5, pp. 195–221, 2005.
[98] M. Huber, "A census of highly symmetric combinatorial designs," *Journal of Algebraic Combinatorics*, vol. 26, pp. 453–476, 2007.
[99] M. Huber, "The classification of flag-transitive Steiner 4-designs," *Journal of Algebraic Combinatorics*, vol. 26, pp. 183–207, 2007.
[100] M. Huber, "Steiner t-designs for large t," in *Mathematical Methods in Computer Science (Beth Festschrift)*, Lecture Notes in Computer Science, vol. 5393, (J. Calmet et al., eds.), pp. 18–26, Berlin, Heidelberg, New York: Springer, 2008.
[101] M. Huber, *Flag-transitive Steiner Designs*. Basel, Berlin, Boston: Birkhäuser, 2009.
[102] M. Huber, "Authentication and secrecy codes for equiprobable source probability distributions," in *Proc. IEEE International Symposium on Information Theory (ISIT) 2009*, pp. 1105–1109, 2009.
[103] M. Huber, "Almost simple groups with socle $L_n(q)$ acting on Steiner quadruple systems," *Journal of Combinatorial Theory, Series A*, vol. 117, pp. 1004–1007, 2010.
[104] M. Huber, "Block-transitive designs in affine spaces," *Designs, Codes and Cryptography*, vol. 55, pp. 235–242, 2010.

[105] M. Huber, "Coding theory and algebraic combinatorics," in *Selected Topics in Information and Coding Theory*, Series on Coding Theory and Cryptology, vol. 7, (I. Woungang et al., eds.), pp. 121–158, Singapore: World Scientific, 2010.

[106] M. Huber, "Combinatorial bounds and characterizations of splitting authentication codes," *Cryptography and Communications*, in press (online first), 2010.

[107] M. Huber, "Constructing optimal authentication codes with perfect multi-fold secrecy," in *Proceedings of International Zurich Seminar on Communications (IZS) 2010*, pp. 86–89, 2010.

[108] M. Huber, "On the Cameron–Praeger conjecture," *Journal of Combinatorial Theory, Series A*, vol. 117, pp. 196–203, 2010.

[109] M. Huber, "On the existence of block-transitive combinatorial designs," *Discrete Mathematics and Theoretical Computer Science (DMTCS)*, vol. 12, pp. 123–132, 2010.

[110] S. Huczynska, "Powerline communication and the 36 officers problem," *Philosophical Transactions of the Royal Society A*, vol. 364, pp. 3199–3214, 2006.

[111] W. C. Huffman and V. Pless, eds., *Handbook of Coding Theory*, vols. I and II. Amsterdam, New York, Oxford: North-Holland, 1998.

[112] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press, 2003.

[113] D. R. Hughes and F. C. Piper, *Projective Planes*. Berlin, Heidelberg, New York: Springer, 1982.

[114] D. R. Hughes and F. C. Piper, *Design Theory*. Cambridge: Cambridge University Press, 1985.

[115] S. H. Y. Hung and N. S. Mendelsohn, "On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$," *Utilitas Mathematica*, vol. 1, pp. 5–95, 1972.

[116] B. Huppert, "Zweifach transitive, auflösbare Permutationsgruppen," *Mathematische Zeitschrift*, vol. 68, pp. 126–150, 1957.

[117] B. Huppert, *Endliche Gruppen I*. Berlin, Heidelberg, New York: Springer, 1967.

[118] B. Huppert and N. Blackburn, *Finite Groups III*. Berlin, Heidelberg, New York: Springer, 1982.

[119] Y. J. Ionin and M. S. Shrikhande, *Combinatorics of Symmetric Designs*. Cambridge: Cambridge University Press, 2006.

[120] T. Johansson, "Lower bounds on the probability of deception in authentication with arbitration," *IEEE Transactions on Information Theory*, vol. 40, pp. 1573–1585, 1994.

[121] T. Johansson, "Further results on asymmetric authentication schemes," *Information and Computation*, vol. 151, pp. 100–133, 1999.

[122] S. J. Johnson and S. J. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Transactions on Communications*, vol. 51, pp. 1413–1419, 2003.

[123] S. J. Johnson and S. R. Weller, "Codes for iterative decoding from partial geometries," *IEEE Transactions on Communications*, vol. 52, pp. 236–243, 2004.

[124] D. Jungnickel, "Lateinische Quadrate, ihre Geometrien und ihre Gruppen," *Jahresber. Deutsch. Math. Verein.*, vol. 86, pp. 69–108, 1984.

[125] W. M. Kantor, "Automorphisms of designs," *Mathematische Zeitschrift*, vol. 109, pp. 246–252, 1969.

[126] W. M. Kantor, "k-homogeneous groups," *Mathematische Zeitschrift*, vol. 124, pp. 261–265, 1972.

[127] W. M. Kantor, "Homogeneous designs and geometric lattices," *Journal of Combinatorial Theory, Series A*, vol. 38, pp. 66–74, 1985.

[128] P. Kaski and P. R. J. Östergård, "The Steiner triple systems of order 19," *Mathematics of Computation*, vol. 73, pp. 2075–2092, 2004.

[129] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs*. Berlin, Heidelberg, New York: Springer, 2006.

[130] P. Kaski, P. R. J. Östergård, and O. Pottonen, "The Steiner quadruple systems of order 16," *Journal of Combinatorial Theory, Series A*, vol. 113, pp. 1764–1770, 2006.

[131] T. P. Kirkman, "On a problem in combinatorics," *The Cambridge and Dublin Mathematical Journal*, vol. 2, pp. 191–204, 1847.

[132] T. P. Kirkman, "Query VI," *Lady's and Gentleman's Diary*, p. 48, 1850.

[133] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Transactions on Information Theory*, vol. 47, pp. 2711–2736, 2001.

[134] E. S. Kramer, D. L. Kreher, R. Rees, and D. R. Stinson, "On perpendicular arrays with $t \geq 3$," *Ars Combinatoria*, vol. 28, pp. 215–223, 1989.

[135] E. S. Kramer, S. S. Magliveras, T. van Trung, and Q. Wu, "On the construction of some perpendicular arrays for arbitrarily large t," *Discrete Mathematics*, vol. 96, pp. 101–110, 1991.

[136] K. Kurosawa, "New bound on authentication code with arbitration," in *Advances in Cryptology — CRYPTO 1994* , Lecture Notes in Computer Science, vol. 839, (Y. Desmedt, ed.), pp. 140–149, Berlin, Heidelberg, New York: Springer, 1994.

[137] K. Kurosawa and S. Obana, "Combinatorial classification of optimal authentication codes with arbitration," *Designs, Codes and Cryptography*, vol. 20, pp. 281–305, 2000.

[138] K. Kurosawa and S. Obana, "Combinatorial bounds on authentication codes with arbitration," *Designs, Codes and Cryptography*, vol. 22, pp. 265–281, 2001.

[139] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups. An Introduction*. Berlin, Heidelberg, New York: Springer, 2004.

[140] C. W. H. Lam, L. Thiel, and S. Swiercz, "The non-existence of finite projective planes of order 10," *Canadian Journal of Mathematics*, vol. 41, pp. 1117–1123, 1989.

[141] J. Lee and D. R. Stinson, "On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs," *ACM Transactions on Information and System Security (TISSEC)*, vol. 11, no. 2, Art. 1, 2008.

[142] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, pp. 355–580, 2008.

[143] M. W. Liebeck, "The affine permutation groups of rank three," *Proceedings of the London Mathematical Society*, vol. 54, pp. 477–516, 1987.

[144] C. C. Lindner and A. Rosa, "Steiner quadruple systems — A survey," *Discrete Mathematics*, vol. 22, pp. 147–181, 1978.

[145] C. C. Lindner and D. R. Stinson, "Steiner pentagon systems," *Discrete Mathematics*, vol. 52, pp. 67–74, 1984.

[146] D. Livingstone and A. Wagner, "Transitivity of finite permutation groups on unordered sets," *Mathematische Zeitschrift*, vol. 90, pp. 393–403, 1965.

[147] H. Lüneburg, *Transitive Erweiterungen Endlicher Permutationsgruppen*. Berlin, Heidelberg, New York: Springer, 1968.

[148] H. Lüneburg, *Translation Planes*. Berlin, Heidelberg, New York: Springer, 1980.

[149] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, New York, Oxford: North-Holland, 1977. 12th impression 2006.

[150] E. Maillet, "Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés," *Journal de Mathématiques Pures et Appliquées*, vol. 1, pp. 5–34, 1895.

[151] K. M. Martin, "On the applicability of combinatorial designs to key predistribution for wireless sensor networks," in *International Workshop on Coding and Cryptology — IWCC 2009*, Lecture Notes in Computer Science, vol. 5557, (C. Xing et al., eds.), pp. 124–145, Berlin, Heidelberg, New York: Springer, 2009.

[152] J. L. Massey, "Cryptography — A selective survey," in *Digital Communications*, (E. Biglieri and G. Prati, eds.), pp. 3–21, Amsterdam, New York, Oxford: North-Holland, 1986.

[153] E. Mathieu, "Mémoire sur l'étude des fonctions de plusieurs quantitiés," *Journal de Mathématiques Pures et Appliquées*, vol. 6, pp. 241–323, 1861.

[154] E. Mathieu, "Sur la fonction cinq fois transitive de 24 quantités," *Journal de Mathématiques Pures et Appliquées*, vol. 18, pp. 25–46, 1873.

[155] A. P. Mathur, *Foundations of Software Testing*. New York: Addison-Wesley, 2008.

[156] U. M. Maurer, "Information-theoretic cryptography," in *Advances in Cryptology — CRYPTO 1999*, Lecture Notes in Computer Science, vol. 1666, (M. J. Wiener, ed.), pp. 47–64, Berlin, Heidelberg, New York: Springer, 1999.

[157] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, pp. 1350–1356, 2000.

[158] B. D. McKay, *Latin Squares*. Available at http://cs.anu.edu.au/∼bdm/data/latin.html.

[159] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, eds., *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1996.

[160] W. H. Mills, "A new 5-design," *Ars Combinatoria*, vol. 6, pp. 193–195, 1978.

[161] D. E. Muller, "Application of boolean algebra to switching circuit design and to error correction," *IEEE Transactions on Computers*, vol. 3, pp. 6–12, 1954.

[162] R. C. Mullin, P. J. Schellenberg, G. H. J. van Rees, and S. A. Vanstone, "On the construction of perpendicular arrays," *Utilitas Math.*, vol. 18, pp. 141–160, 1980.
[163] S. Obana and K. Kurosawa, "Bounds and combinatorial structure of (k, n) multi-receiver A-codes," *Designs, Codes and Cryptography*, vol. 22, pp. 47–63, 2001.
[164] W. Ogata, K. Kurosawa, and D. R. Stinson, "Optimum secret sharing schemes secure against cheating," *SIAM Journal on Discrete Mathematics*, vol. 20, pp. 79–95, 2006.
[165] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido, "New combinatorial designs and their applications to authentication codes and secret sharing schemes," *Discrete Mathematics*, vol. 279, pp. 383–405, 2004.
[166] F. Oggier and H. Fathi, "Multi-receiver authentication code for network coding," in *Proceedings of IEEE 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1225–1231, 2008.
[167] F. Oggier and H. Fathi, "An authentication code against pollution attacks in network coding," Preprint arXiv:0909.3146v1, 2009.
[168] F. Özbudak and Z. Saygi, "Some constructions of systematic authentication codes using Galois rings," *Designs, Codes and Cryptography*, vol. 41, pp. 343–357, 2006.
[169] N. Pavlidou, A. J. H. Vinck, J. Yazdani, and B. Honary, "Power line communications: State of the art and future trends," *IEEE Communications Magazine*, vol. 41, pp. 34–40, 2003.
[170] D. Pei, *Authentication Codes and Combinatorial Designs*. Boca Raton: CRC Press, 2006.
[171] G. Pickert, *Projektive Ebenen*. Berlin, Heidelberg, New York: Springer, 2nd ed., 1975.
[172] D. Raghavarao and L. V. Padgett, *Block Designs: Analysis, Combinatorics and Applications*. Singapore: World Scientific, 2005.
[173] D. K. Ray-Chaudhuri and R. M. Wilson, "Solution of Kirkman's schoolgirl problem," in *Combinatorics: Proceedings of American Mathematical Society Symposium in Pure Mathematics*, pp. 187–203, 1971.
[174] D. K. Ray-Chaudhuri and R. M. Wilson, "On t-designs," *Osaka Journal of Mathematics*, vol. 12, pp. 737–744, 1975.
[175] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IEEE Transactions on Information Theory*, vol. 4, pp. 38–49, 1954.
[176] H. J. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monographs, vol. 14. Buffalo: Mathematical Association of America, 1963.
[177] R. Safavi-Naini, L. McAven, and M. Yung, "General group authentication codes and their relation to "unconditionally-secure signatures"," in *Public Key Cryptography — PKC 2004*, Lecture Notes in Computer Science, vol. 2947, (F. Bao et al., ed.), pp. 231–248, Berlin, Heidelberg, New York: Springer, 2004.
[178] R. Safavi-Naini and H. Wang, "Multireceiver authentication codes: Models, bounds, constructions, and extensions," *Information and Computation*, vol. 151, pp. 148–172, 1999.

[179] R. Safavi-Naini and H. Wang, "Broadcast authentication for group communication," *Theoretical Computer Science*, vol. 269, pp. 1–21, 2001.

[180] J. Schillewaert and K. Thas, "Authentication codes from generalized quadrangles," Preprint, 2009.

[181] P. Schöbi, "Perfect authentication systems for data sources with arbitrary statistics," (presented at EUROCRYPT 1986), unpublished.

[182] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[183] G. J. Simmons, "A game theory model of digital message authentication," *Congressus Numerantium*, vol. 34, pp. 413–424, 1982.

[184] G. J. Simmons, "Message authentication: A game on hypergraphs," *Congressus Numerantium*, vol. 45, pp. 161–192, 1984.

[185] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology — CRYPTO 1984*, Lecture Notes in Computer Science, vol. 196, (G. R. Blakley and D. Chaum, eds.), pp. 411–432, Berlin, Heidelberg, New York: Springer, 1985.

[186] G. J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," in *Advances in Cryptology — EUROCRYPT 1987*, Lecture Notes in Computer Science, vol. 304, (D. Chaum and W. L. Price, eds.), pp. 150–165, Berlin, Heidelberg, New York: Springer, 1988.

[187] G. J. Simmons, "A Cartesian product construction for unconditionally secure authentication codes that permit arbitration," *Journal of Cryptology*, vol. 2, pp. 77–104, 1990.

[188] G. J. Simmons, "A survey of information authentication," in *Contemporary Cryptology: The Science of Information Integrity*, (G. J. Simmons, ed.), pp. 379–419, Piscataway: IEEE Press, 1992.

[189] N. J. A. Sloane, ed., *A Library of Orthogonal Arrays*. Available at http://www2.research.att.com/∼njas/oadir.

[190] N. J. A. Sloane, ed., *The On-Line Encyclopedia of Integer Sequences*. Available at http://www.research.att.com/∼njas/sequences.

[191] L. H. Soicher, "The DESIGN package for GAP," Version 1.4, 2009. Available at http://designtheory.org/software/gap_design.

[192] J. Steiner, "Combinatorische Aufgabe," *Journal für die reine und angewandte Mathematik*, vol. 45, pp. 181–182, 1853.

[193] D. R. Stinson, "A short proof of the non-existence of a pair of orthogonal Latin squares of order 6," *Journal of Combinatorial Theory, Series A*, vol. 36, pp. 373–376, 1984.

[194] D. R. Stinson, "A construction for authentication/secrecy codes from certain combinatorial designs," *Journal of Cryptology*, vol. 1, pp. 119–127, 1988.

[195] D. R. Stinson, "The combinatorics of authentication and secrecy codes," *Journal of Cryptology*, vol. 2, pp. 23–49, 1990.

[196] D. R. Stinson, "Combinatorial characterizations of authentication codes," *Designs, Codes and Cryptography*, vol. 2, pp. 175–187, 1992.

[197] D. R. Stinson, "Combinatorial designs and cryptography," in *Surveys in Combinatorics*, London Mathematical Society, Lecture Note Series, vol. 187, (K. Walker, ed.), pp. 257–287, Cambridge: Cambridge University Press, 1993.

[198] D. R. Stinson, "Universal hashing and authentication codes," *Designs, Codes and Cryptography*, vol. 4, pp. 369–380, 1994.

[199] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*. Berlin, Heidelberg, New York: Springer, 2004.

[200] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton: CRC Press, 3rd ed., 2006.

[201] D. R. Stinson and R. S. Rees, "Combinatorial characterizations of authentication codes II," *Designs, Codes and Cryptography*, vol. 7, pp. 239–259, 1996.

[202] D. R. Stinson and L. Teirlinck, "A construction for authentication/secrecy codes from 3-homogeneous permutation groups," *European Journal of Combinatorics*, vol. 11, pp. 73–79, 1990.

[203] D. R. Stinson and S. A. Vanstone, "A combinatorial approach to threshold schemes," *SIAM Journal on Discrete Mathematics*, vol. 1, pp. 230–237, 1988.

[204] D. R. Stinson and R. Wei, eds., *Bibliography on Authentication Codes*. Available at http://www.cacr.math.uwaterloo.ca/∼dstinson/acbib.html.

[205] A. P. Street and D. J. Street, *Combinatorics of Experimental Design*. Oxford: Oxford University Press, 1987.

[206] L. Teirlinck, "Non-trivial t-designs without repeated blocks exist for all t," *Discrete Mathematics*, vol. 65, pp. 301–311, 1987.

[207] G. Terry, "Le problème de 36 officiers," *Compte Rendu de l'Assoc. Français Avanc. Sci. Naturel*, vol. 1, pp. 122–123, 1900.

[208] G. Terry, "Le problème de 36 officiers," *Compte Rendu de l'Assoc. Français Avanc. Sci. Naturel*, vol. 2, pp. 170–203, 1901.

[209] V. D. Tonchev, *Combinatorial Configurations: Designs, Codes, Graphs*. Harlow: Longman, 1988.

[210] V. D. Tonchev, "Codes and designs," in *Handbook of Coding Theory* vol. II, (W. C. Huffman and V. Pless, eds.), pp. 1229–1267, Amsterdam, New York, Oxford: North-Holland, 1998.

[211] V. D. Tonchev, "Codes," in *Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), pp. 677–702, Boca Raton: CRC Press, 2006.

[212] V. D. Tonchev, "Steiner systems for two-stage disjunctive testing," *Journal of Combinatorial Optimization*, vol. 15, pp. 1–6, 2008.

[213] D. Tonien, R. Safavi-Naini, and P. Wild, "Combinatorial characterizations of authentication codes in verification oracle model," in *Proceedings of 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007)*, (F. Bao and S. Miller, eds.), pp. 183–193, 2007.

[214] D. Tonien, R. Safavi-Naini, and P. Wild, "Authentication codes in the query model," in *Coding and Cryptology*, (Y. Li et al., eds.), pp. 214–225, Singapore: World Scientific, 2008.

[215] J. H. van Lint, "Codes and designs," in *Higher Combinatorics: Proceedings of NATO Advanced Study Institute*, (M. Aigner, ed.), pp. 241–256, Boston, Dordrecht: Reidel, 1977.

[216] J. H. van Lint, "Codes and combinatorial designs," in *Proceedings of Marshall Hall Conference on Coding Theory, Design Theory, Group Theory*, (D. Jungnickel and S. A. Vanstone, eds.), pp. 31–39, New York: J. Wiley, 1993.

[217] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge: Cambridge University Press, 2nd ed., 2001.

[218] H. C. A. van Tilborg, "Authentication codes: an area where coding and cryptology meet," in *Proceedings of 5th IMA Conference on Cryptography and Coding 1995*, Lecture Notes in Computer Science, vol. 1025, (C. Boyd, ed.), pp. 169–183, Berlin, Heidelberg, New York: Springer, 1995.

[219] T. van Trung, "On the construction of authentication and secrecy codes," *Designs, Codes and Cryptography*, vol. 5, pp. 269–280, 1995.

[220] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Transactions on Information Theory*, vol. 50, pp. 1156–1176, 2004.

[221] G. S. Vernam U.S. patent 1,310,719. Secret signaling system. July 22nd, 1919.

[222] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraph communications," *Journal of American Institute of Electrical Engineers*, vol. 45, pp. 109–115, 1926.

[223] H. Wielandt, *Finite Permutation Groups.* New York: Academic Press, 1964.

[224] P. Wild, "The combinatorics of cryptographic key establishment," in *Surveys in Combinatorics*, London Mathematical Society, Lecture Note Series, vol. 346, (A. Hilton and J. Talbot, eds.), pp. 223–273, Cambridge: Cambridge University Press, 2007.

[225] R. J. Wilson, "The early history of block designs," *Rend. Sem. Mat. Messina Ser. II*, vol. 9, pp. 267–276, 2003.

[226] E. Witt, "Die 5-fach transitiven Gruppen von Mathieu," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 12, pp. 256–264, 1938.

[227] E. Witt, "Über Steinersche Systeme," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 12, pp. 265–275, 1938.

[228] C. Xing, H. Wang, and K. Y. Lam, "Constructions of authentication codes from algebraic curves over finite fields," *IEEE Transactions on Information Theory*, vol. 46, pp. 886–892, 2000.