Perfect Secrecy Systems Immune to Spoofing Attacks

Michael Huber

Received: June 24, 2011 / Revised: May 9, 2012

Abstract We present novel perfect secrecy systems that provide immunity to spoofing attacks under equiprobable source probability distributions. On the theoretical side, relying on an existence result for t-designs by Teirlinck, our construction method constructively generates systems that can reach an arbitrary high level of security. On the practical side, we obtain, via cyclic difference families, very efficient constructions of new optimal systems that are onefold secure against spoofing. Moreover, we construct, by means of t-designs for large values of t, the first near-optimal systems that are 5- and 6-fold secure as well as further systems with a feasible number of keys that are 7-fold secure against spoofing. We apply our results furthermore to a recently extended authentication model, where the opponent has access to a verification oracle. We obtain this way novel perfect secrecy systems with immunity to spoofing in the verification oracle model.

Keywords Information theoretic security · perfect secrecy system · spoofing attack · verification oracle model

1 Introduction

Perfect secrecy systems (or codes) play a prominent role in information theory and cryptography. In terms of information theoretic security, these systems shall ensure protection of the confidentiality of sensitive information in the presence of eavesdropping. The information theoretic, or unconditional, security model does not depend on any complexity assumptions and hence cannot be broken given unlimited computational resources. A well-known example of a perfect secrecy system is Vernam's One-time Pad. In his landmark paper "Communication theory of secrecy systems" [23], Shannon established a fundamental characterization of optimal perfect secrecy systems: A key-minimal secrecy system achieves perfect secrecy if and only if the encryption matrix is a Latin square and the keys are used with equal probability. Important generalizations have been obtained since then (see, e.g., [11,26,27]). In addition to the concept of perfect secrecy, various scenarios require that the systems provide robustness against spoofing attacks. Concerning the aspect of authenticity, the integrity of information that is communicated via a potentially insecure channel shall be assured. Often such constructions involve a variety of tools from combinatorics (see, e.g., [13,15,16,20,26]).

In this paper, we present novel perfect secrecy systems that provide immunity to spoofing attacks under equiprobable source probability distributions. In the past decades various perfect secrecy systems have been constructed that offer zero (like Vernam's One-time Pad) or onefold security against spoofing. Recently, in [13], the first infinite classes of optimal perfect secrecy systems that achieve twofold security have been constructed as well as further optimal systems that offer up to 4-fold security against spoofing under equiproba-

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) via a Heisenberg grant (Hu954/4) and a Heinz Maier-Leibnitz Prize grant (Hu954/5).

M. Huber
Wilhelm-Schickard-Institute for Computer Science
University of Tuebingen
Sand 13, 72076 Tuebingen, Germany
E-mail: michael.huber@uni-tuebingen.de
Phone +49 7071 2977173
Fax +49 7071 295061

ble source probability distributions. This has been achieved by means of particular Steiner t-designs, e.g., the famous 5-$(12, 6, 1)$ Witt design. However, as Steiner t-designs are not known to exist for $t > 5$, the level of security cannot be augmented any further via this approach. In the present paper, we develop a more general construction method, which allows us to use t-designs for higher values of t under equiprobable source probability distributions. On the theoretical side, relying on Teirlinck's existence result for t-designs [28], our method constructively generates systems that can reach an arbitrary high security level. On the practical side, by using cyclic difference families, we give very efficient constructions of new optimal systems that are onefold secure against spoofing. By employing t-designs for large values of t, we also present the first near-optimal systems that are 5- and 6-fold secure as well as further systems with a feasible number of keys that are 7-fold secure against spoofing. Moreover, we apply our results to an extended authentication model, where the opponent has access to a verification oracle. This model, which has been recently introduced and investigated in [1, 21, 29, 30], allows a more powerful pro-active attack scenario. The opponent may send a message of the opponent's choice to the receiver and observe the receiver's response whether or not the receiver accepts it as authentic. This can be modeled in terms of a verification oracle with an online/offline variant that provides a response to a query message in the same way as the message would be accepted or not by the legitimate receiver. We obtain this way novel perfect secrecy systems with immunity to spoofing attacks in the verification oracle model.

The organization of the paper is as follows: The underlying information theoretic Shannon–Simmons model is given in Section 2. Section 3 introduces background material on combinatorial structures that is important for our further purposes. Section 4 presents a short overview of known constructions of perfect secrecy systems that provide robustness against spoofing attacks. In Section 5, a general construction method is developed and we examine the level of security from a theoretical point of view. The subsequent two sections deal then with the practical side: we give explicit constructions of optimal systems with onefold immunity to spoofing in Section 6, and of near-optimal and other feasible systems with multifold immunity in Section 7. In Section 8, we apply our constructions to the verification oracle model. The paper is concluded in Section 9.

2 The Shannon–Simmons Model

We rely on the *information theoretic* (or *unconditional*) secrecy model developed by Shannon [23], and by Simmons (e.g., [24, 25]) including authentication. Our notation follows, for the most part, that of [19,26]. In this 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. This is known as an *authentication system* (or *authentication code, A-code*).

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 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 each encoding rule $e \in \mathcal{E}$, let $M(e) := \{e(s) : s \in \mathcal{S}\}$ denote the set of *valid* messages. 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 system 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 $a_{es} := e(s)$ $(1 \leq e \leq b,\ 1 \leq s \leq k)$.

Concerning authenticity, we address the following scenario, called *spoofing attack* of order i (cf. [19]): 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, whereas less is known for higher orders.

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 *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. Combinatorial lower bounds can be given as follows (cf. [19]).

Theorem 1 (Massey) *In an authentication system with k source states and v messages, for every $0 \leq i \leq t$, the deception probabilities are bounded below by*

$$P_{d_i} \geq \frac{k-i}{v-i}.$$

An authentication system is called *t-fold secure against spoofing* if $P_{d_i} = (k-i)/(v-i)$ for all $0 \leq i \leq t$. The following theorem (cf. [19,22]) establishes a combinatorial lower bound on the number of encoding rules for this kind of attack.

Theorem 2 (Massey–Schöbi) *If an authentication system is $(t-1)$-fold against spoofing, then the number of encoding rules is bounded below by*

$$b \geq \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Such a system is called *optimal* if the number of encoding rules meets the lower bound with equality.

Concerning secrecy, we recall Shannon's fundamental idea of perfect secrecy (cf. [23]): An authentication system 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. From Bayes' Theorem follows that

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

This yields:

Lemma 1 (Stinson) *An authentication system has perfect secrecy if and only if*

$$\sum_{\{e \in \mathcal{E}: e(s)=m\}} p_E(e) = \sum_{\{e \in \mathcal{E}: m \in M(e)\}} p_E(e) p_S(e^{-1}(m))$$

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

Therefore, if the encoding rules in a system are used with equal probability, then a given message m occurs with the same frequency in each column of the encoding matrix.

3 Combinatorial Structures

We give in this section some background material on combinatorial structures that is important for our further purposes. Let us assume that $t \leq k \leq v$ and λ are positive integers.

Definition 1 Let G be a finite additive Abelian group of order v. A *difference family* DF(v,k,λ) over G is a family $\mathcal{F} = \{D_1, \ldots, D_l\}$ of subsets of G, satisfying the following properties:

(i) $|D_i| = k$ for all i with $1 \leq i \leq l$,

(ii) the multiset union

$$\bigcup_{i=1}^{l} \{x - y : x, y \in D_i,\ x \neq y\}$$

contains every nonzero element of G exactly λ times.

The sets $D_1, \ldots, D_l$ are called *base blocks*. A difference family with a single base block is called a *difference set*. A DF(v,k,λ) with G isomorphic to the cyclic group C_v of order v is called a *cyclic* difference family and denoted by CDF(v,k,λ).

We recall the notion of *authentication perpendicular arrays*. These combinatorial structures are generalizations of Latin squares.

Definition 2 An *authentication perpendicular array* APA$_\lambda(t,k,v)$ is a $\lambda\binom{v}{t} \times k$ array, A, of v symbols, which satisfies the following properties:

(i) every row of A contains k distinct symbols,

(ii) for any t columns of A, and for any t distinct symbols, there are precisely λ rows r of A such that the t given symbols all occur in row r in the given t columns,

(iii) for any $s \leq t-1$ and for any $s+1$ distinct symbols $\{x_i\}_{i=1}^{s+1}$, it holds that among all the rows of A that contain all the symbols $\{x_i\}_{i=1}^{s+1}$, the s symbols $\{x_i\}_{i=1}^{s}$ occur in all possible subsets of s columns equally often.

We present a simple example (due to van Rees, cf. [27]):

Example 1 A 55×3 array A can be constructed by developing the five rows

0 1 2
0 9 7
0 3 6
0 4 8
0 5 10

modulo 11. Every pair $\{x_1, x_2\}$ occurs in three rows of A. Within these three rows, x_1 occurs once in each of the three columns, as does x_2. This gives an $\mathrm{APA}_1(2, 3, 11)$.

We recall furthermore the definition of *combinatorial t-designs.*

Definition 3 A t-(v, k, λ) *design* $\mathcal{D}$ is a pair $(X, \mathcal{B})$, which satisfies the following properties:

(i) X is a set of v elements, called *points*,

(ii) $\mathcal{B}$ is a family of k-subsets of X, called *blocks*,

(iii) every t-subset of X is contained in exactly λ blocks.

We will denote points by lower-case and blocks by upper-case Latin letters. Via convention, let $b := |\mathcal{B}|$ denote the number of blocks. Throughout this work, 'repeated blocks' are not allowed, that is, the same k-subset of points may not occur twice as a block. If $t < k < v$ holds, then we speak of a *non-trivial* t-design. For historical reasons, a t-(v, k, λ) design with $\lambda = 1$ is called a *Steiner t-design* (sometimes also a *Steiner system*). If $\mathcal{D} = (X, \mathcal{B})$ is a t-(v, k, λ) design with $t \geq 2$, and $x \in X$ arbitrary, then the *derived design* with respect to x is $\mathcal{D}_x = (X_x, \mathcal{B}_x)$, where $X_x = X \backslash \{x\}$, $\mathcal{B}_x = \{B \backslash \{x\} : x \in B \in \mathcal{B}\}$. In this case, $\mathcal{D}$ is also called an *extension* of $\mathcal{D}_x$. Obviously, $\mathcal{D}_x$ is a $(t-1)$-$(v-1, k-1, \lambda)$ design.

For the existence of t-designs, basic necessary conditions can be obtained via elementary counting arguments (see, for instance, [2]):

Lemma 2 *Let $\mathcal{D} = (X, \mathcal{B})$ be a t-(v, k, λ) design, and for a positive integer $s \leq t$, let $S \subseteq X$ with $|S| = s$. Then the number of blocks containing each element of S is given by*

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

In particular, for $t \geq 2$, a t-(v, k, λ) design is also an s-(v, k, λ_s) design.

It is customary to set $r := \lambda_1$ denoting the number of blocks containing a given point. It follows

Lemma 3 *Let $\mathcal{D} = (X, \mathcal{B})$ be a t-(v, k, λ) design. Then the following holds:*

(a) $bk = vr$.

(b) $\displaystyle\binom{v}{t}\lambda = b\binom{k}{t}$.

(c) $r(k-1) = \lambda_2(v-1)$ *for* $t \geq 2$.

The next result (cf. [26]) uses t-designs in order to construct authentication perpendicular arrays. Further similar recursive constructions have been obtained in [31].

Theorem 3 (Stinson–Teirlinck) *Suppose there is a t-(v, k, λ) design and an authentication perpendicular array $APA_{\lambda'}(t, k, k)$, then there is an $APA_{\lambda \cdot \lambda'}(t, k, v)$.*

Concerning the existence of t-designs, a seminal result by Teirlinck [28] shows that there exist non-trivial t-designs for all possible values of t.

Theorem 4 (Teirlinck) *For given integers t and v with $v \equiv t \pmod{(t+1)!^{2t+1}}$ and $v \geq t+1 > 0$, there exists a t-$(v, t+1, (t+1)!^{2t+1})$ design.*

Teirlinck's recursive construction methods are constructive. However, for a given t, they result in t-designs with extremely large values for v and λ. For example, the smallest parameters for the case $t = 7$ are 7-$(40320^{15} + 7, 8, 40320^{15})$. Until now no non-trivial Steiner t-design with $t > 5$ has been found. Highly regular examples have been proven not to exist (cf., e.g., [12]). We refer the reader to [2, 9] for encyclopedic accounts of key results in combinatorial design theory. Various connections of t-designs with coding and information theory can be found in a recent survey [14] (with many additional references therein).

4 Constructions using Combinatorial Structures

4.1 Equiprobable Source Probability Distribution

When the source states are known to be independent and equiprobable, authentication systems which are $(t-1)$-fold secure against spoofing can be constructed via t-designs (cf. [10, 22, 26]).

Theorem 5 (De Soete–Schöbi–Stinson) *Suppose there is a t-(v, k, λ) design. Then there is an authentication system for k equiprobable source states, having v messages and $\lambda\binom{v}{t}/\binom{k}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing. Conversely, if there is an authentication system for k equiprobable source states, having v messages and $\binom{v}{t}/\binom{k}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing, then there is a Steiner t-$(v, k, 1)$ design.*

With a focus on optimal constructions, the above result has been modified in [26] and generalized recently in [13] to include also the aspect of perfect secrecy. In particular, the first infinite classes of optimal perfect secrecy systems that achieve twofold security have been constructed in [13] as well as further optimal systems that offer 3- and 4-fold security against spoofing. We give in Table 1 all presently known optimal perfect secrecy systems that are t-fold secure against spoofing with $t \geq 1$ under equiprobable source probability distributions.

4.2 Arbitrary Source Probability Distribution

For arbitrary source probability distributions, basically two construction methods have been developed for perfect secrecy systems that offer security against spoofing attacks (cf. [6,7,26,31]). These constructions inherently require larger numbers of encoding rules for achieving the same level of security. One of the two methods with the smaller number of encoding rules requires $\lambda\binom{v}{t}$ encoding rules when we want the perfect secrecy systems with k source states and v messages to be $(t-1)$-fold secure against spoofing (indeed, these systems achieve perfect t-fold secrecy), and is based on authentication perpendicular arrays $\mathrm{APA}_\lambda(t,k,v)$, cf. [26, Thm. 3.3]. For $t \geq 6$, there are — apart from two infinite series with extremely large values of λ — only a very small number of authentication perpendicular arrays $\mathrm{APA}_\lambda(t,k,v)$ known. These have been constructed via Theorem 3 or similar results using t-designs. All these $\mathrm{APA}_\lambda(t,k,v)$ have $t \leq 8$, and for $t = 6$ all have $\lambda \geq 24$, for $t = 7$ all have $\lambda \geq 70$, and for $t = 8$ all have $\lambda \geq 280$. The two infinite series were constructed by Tran van Trung [31] and have parameters $v \geq k$, $k = 2t$ resp. $2t+1$, and $\lambda = t!^2\binom{v-t}{t}/6!$ resp. $(t+1)t!^2\binom{v-t}{t+1}/6!$.

Table 1 Optimal perfect secrecy systems from Steiner designs that are t-fold secure against spoofing attacks

t	k	v	$b = b_{\mathrm{opt}}$	Ref.
1	$q+1$ q prime power	$\frac{q^{d+1}-1}{q-1}$ $d \geq 2$ even	$\frac{v(v-1)}{k(k-1)}$	[26]
1	3	$v \equiv 1 \pmod 6$	$\frac{v(v-1)}{6}$	[13]
1	4	$v \equiv 1 \pmod{12}$	$\frac{v(v-1)}{12}$	[13]
1	5	$v \equiv 1 \pmod{20}$	$\frac{v(v-1)}{20}$	[13]
2	$q+1$ q prime power	q^d+1 $d \geq 2$ even	$\frac{v(v-1)(v-2)}{k(k-1)(k-2)}$	[13]
2	4	$v \equiv 2, 10 \pmod{24}$	$\frac{v(v-1)(v-2)}{24}$	[13]
2	5	26	260	[13]
3	5	11	66	[13]
	7	23	253	[13]
	5	23	1,771	[13]
	5	47	35,673	[13]
	5	83	367,524	[13]
	5	71	194,327	[13]
	5	107	1,032,122	[13]
	5	131	2,343,328	[13]
	5	167	6,251,311	[13]
	5	243	28,344,492	[13]
4	6	12	132	[13]
	6	84	5,145,336	[13]
	6	244	1,152,676,008	[13]

5 A General Construction Method & Theoretical Point of View

We present a construction method for designing perfect secrecy systems that provide immunity to spoofing attacks under equiprobable source probability distributions.

Theorem 6 *Suppose there is a t-(v,k,λ) design, where v divides the number of blocks $b = \lambda\binom{v}{t}/\binom{k}{t}$. Then there is a perfect secrecy system for k equiprobable source states, having v messages and b encoding rules, that is $(t-1)$-fold secure against spoofing. Moreover, the system is optimal if and only if $\lambda = 1$.*

Proof Let $\mathcal{D} = (X, \mathcal{B})$ be a t-(v,k,λ) design, where v divides $b = \lambda\binom{v}{t}/\binom{k}{t}$. It follows from Theorem 5 that the system is $(t-1)$-fold secure against spoofing attacks. Thus, it remains to verify that the system also achieves perfect secrecy when we assume that the encoding rules are used with equal probability. By Lemma 1, this means that a given message must occur with the same frequency in each column of the resulting encoding matrix. This can be achieved by ordering every block of $\mathcal{D}$ in such a way that every point occurs in each possible position in precisely b/v blocks. Since every point occurs in exactly $r = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$ blocks in view of Lemma 3 (c), necessarily k must divide r. By Lemma 3 (b), this is equivalent to saying that v divides b. To show that the condition is also sufficient, we may consider the bipartite point-block incidence graph of $\mathcal{D}$ with vertex set $X \cup \mathcal{B}$, where (x, B) defines an edge if and only if $x \in B$ for $x \in X$ and $B \in \mathcal{B}$. An ordering on each block of $\mathcal{D}$ can be obtained via an edge-coloring of this graph using k colors in such a way that each vertex $B \in \mathcal{B}$ is adjacent to one edge of each color, and each vertex $x \in X$ is adjacent to b/v edges of each color. Technically, this can be achieved by first splitting up each vertex x into b/v copies, each having degree k, and then by finding an appropriate edge-coloring of the resulting k-regular bipartite graph using k colors. We can now take the ordered blocks as encoding rules, each used with equal probability. Moreover, optimality occurs if and only if $\lambda = 1$ in view of Theorem 2. □

We note that the special case when $\lambda = 1$ has been treated in [13, Thm. 6].

Using Theorem 4, we may constructively generate systems that can reach an arbitrary high level of security against spoofing.

Theorem 7 *For all integers t and v with $v \equiv t \pmod{(t+1)!^{2t+1}}$ and $v \geq t+1 > 0$, there exists a perfect secrecy system for $t+1$ equiprobable source states, having v messages and $b = (t+1)!^{2t} t! \binom{v}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing.*

Proof For the given design parameters, the division property $v \mid b$ holds:

$$v \mid \lambda \frac{\binom{v}{t}}{\binom{k}{t}} \Leftrightarrow k(k-1)\cdots(k-t+1) \mid \lambda(v-1)\cdots(v-t+1)$$

$$\Leftrightarrow (t+1)! \mid (t+1)!^{2t+1}(v-1)\cdots(v-t+1).$$

Therefore, the claim follows by applying Theorem 6. □

6 Explicit Constructions (I): Onefold Immunity

We give in this section very efficient constructions of new optimal systems that are onefold secure against spoofing.

Theorem 8 *If there exists a difference family $DF(v, k, \lambda)$ over a finite additive Abelian group G of order v, then there is a perfect secrecy system for k equiprobable source states, having v messages and $b = \lambda v(v-1)/(k^2-k)$ encoding rules, that is onefold secure against spoofing. Moreover, the system is optimal if and only if $\lambda = 1$.*

Proof Let $\mathcal{F} = \{D_1, \ldots, D_l\}$ be a $\mathrm{DF}(v, k, \lambda)$ over G. We shall need the two basic facts:

- Since $l = \frac{\lambda(v-1)}{k(k-1)}$ is a positive integer, we have

  $$\lambda(v-1) \equiv 0 \pmod{k(k-1)} \quad (*).$$

- Let $\mathrm{Orb}_G(D_i) = \{D_i + g : g \in G\}$ denote the *G-orbit* of D_i. Then the union

  $$\bigcup_{i=1}^{l} \mathrm{Orb}_G(D_i)$$

  forms the family of blocks of a 2-(v, k, λ) design admitting G as a group of automorphisms acting regularly (i.e., sharply transitively) on the points and semiregularly on the blocks.

Thus, by $(*)$ and Lemma 3, we have $v \mid b$, and the requirements for applying Theorem 6 are fulfilled. □

Table 2 Perfect secrecy system from a cyclic difference family $\mathrm{CDF}(13, 3, 1)$.

	s_1	s_2	s_3
e_1	0	1	4
e_2	1	2	5
e_3	2	3	6
e_4	3	4	7
e_5	4	5	8
e_6	5	6	9
e_7	6	7	10
e_8	7	8	11
e_9	8	9	12
e_{10}	9	10	0
e_{11}	10	11	1
e_{12}	11	12	2
e_{13}	12	0	3
e_{14}	0	2	7
e_{15}	1	3	8
e_{16}	2	4	9
e_{17}	3	5	10
e_{18}	4	6	11
e_{19}	5	7	12
e_{20}	6	8	0
e_{21}	7	9	1
e_{22}	8	10	2
e_{23}	9	11	3
e_{24}	10	12	4
e_{25}	11	0	5
e_{26}	12	1	6

In particular, when $\mathcal{F} = \{D_1, \ldots, D_l\}$ is a $\mathrm{CDF}(v, k, \lambda)$, then a perfect secrecy system can be constructed very efficiently due to the extremely simple form of its encoding matrix (cf. Table 2). We note that the special case when $l = 1$ in the above theorem has been considered in [26, Thm. 6.5 & Remark]. In this case, the respective cyclic difference set is a *Singer difference set* yielding a projective plane of prime power order as *symmetric* cyclic Steiner 2-design (i.e., $v = b$). We give an example of a perfect secrecy systems constructed via Theorem 8 based on a $\mathrm{CDF}(13, 3, 1)$.

Example 2 A $\mathrm{CDF}(13, 3, 1)$ has two base blocks $D_1 = \{0, 1, 4\}$ and $D_2 = \{0, 2, 7\}$. The orbits of D_1 and D_2 immediately form an encoding matrix as given in Table 2. The perfect secrecy system, having 3 equiprobable source states, 13 messages and 26 encoding rules, is optimal and offers onefold security against spoofing.

Example 3 The following infinite ((i)-(iii)) and finite ((iv)-(v)) families of cyclic difference families $\mathrm{CDF}(q, k, 1)$ with q a prime power are known (cf. [8] and the references therein; [9]):

(i) For $k = 3, 4$ and 5, respectively, a $\mathrm{CDF}(q, k, 1)$ exists for all prime powers $q \equiv 1 \pmod{k(k-1)}$.
(ii) A $\mathrm{CDF}(q, 6, 1)$ exists for all prime powers $q \equiv 1 \pmod{30}$ with the exception $q = 61$.
(iii) A $\mathrm{CDF}(q, 7, 1)$ exists for all prime powers $q \equiv 1 \pmod{42}$ with the exception $q = 43$, and the possible exceptions $q = 127, 211, 31^6$ as well a $q \in [261239791, 1.236597 \times 10^{13}]$ such that $(-3)^{\frac{q-1}{14}} = 1$ in $\mathbb{F}_q$.
(iv) A $\mathrm{CDF}(q, 8, 1)$ exists for all prime powers $q \equiv 1 \pmod{56} < 10^4$, with the possible exceptions $q = 113, 169, 281, 337$.
(v) A $\mathrm{CDF}(q, 9, 1)$ exists for all prime powers $q \equiv 1 \pmod{72} < 10^4$, with the possible exceptions $q = 289, 361$.

Hence, in all these cases a perfect secrecy system for k equiprobable source states, having q messages and $q(q-1)/(k^2-k)$ encoding rules, that is optimal and onefold secure against spoofing can be constructed very efficiently.

7 Explicit Constructions (II): Multifold Immunity

We construct in this section the first near-optimal systems that are 5- and 6-fold secure as well as further systems with a feasible number of keys that are 7-fold secure against spoofing. Recall that number of encoding rules in Theorem 6 is λ times the lower bound of Theorem 2. In order to construct perfect secrecy systems with a high level of security against spoofing, we are therefore interested in t-designs with large t and small values of λ. These designs must satisfy the divisibility condition $v \mid b = \lambda\binom{v}{t}/\binom{k}{t}$ of Theorem 6. When $2 \leq \lambda \leq 10$, we call such a system *near-optimal*.

Relying on the Kramer–Mesner method [18], various t-designs with large t have been constructed in recent years under some prescribed groups of automorphisms (cf. [3–5, 17]). We give some examples related to our considerations.

Example 4 A 6-(19, 7, 4) design and three 6-(19, 7, 6) designs have been constructed in [3] by prescribing the groups $Hol(C_{17})$++ and $Hol(C_{19})$, respectively (where the + operator adds a fixed point to a permutation group). The only known two smaller 6-(14, 7, 4) designs have C_{13}+ as a prescribed group of automorphisms, but do not satisfy our divisibility condition. The only known further 6-design with $\lambda = 4$ has parameters 6-(23, 7, 4), and is derived from the unique 7-(24, 8, 4) design with $PSL(2, 23)$ as a prescribed group of automorphisms.

Table 3 Near-optimal perfect secrecy systems from 6- and 7-designs that are 5- and 6-fold secure against spoofing attacks

t	k	v	b	b_{opt}	Design Parameters
5	7	19	$4 \times b_{\mathrm{opt}}$	3,876	6-(19, 7, 4)
	7	22	$8 \times b_{\mathrm{opt}}$	10,659	6-(22, 7, 8)
	7	23	$4 \times b_{\mathrm{opt}}$	14,421	6-(23, 7, 4)
	7	25	$6 \times b_{\mathrm{opt}}$	25,300	6-(25, 7, 6)
	7	32	$6 \times b_{\mathrm{opt}}$	129,456	6-(32, 7, 6)
6	8	24	$8 \times b_{\mathrm{opt}}$	43,263	7-(24, 8, 8)
	8	26	$6 \times b_{\mathrm{opt}}$	82,225	7-(26, 8, 6)
	8	33	$10 \times b_{\mathrm{opt}}$	534,006	7-(33, 8, 10)

Example 5 There are 7-(24, 8, λ) designs admitting $PSL(2, 23)$ with possible values $\lambda = 4, \ldots, 8$. However, only for $\lambda = 8$ the divisibility condition is fulfilled. There exist 7-(26, 8, 6) designs, which have been constructed with $PGL(2, 25)$ as a prescribed group of automorphisms (cf. [3]).

Example 6 The construction of 8-(31, 10, 100) designs has been established in [5] with $PSL(3, 5)$ as a prescribed group of automorphisms. The only known 8-designs with smaller λ are 8-(31, 10, 93) designs admitting $PSL(3, 5)$ again, but do not satisfy the divisibility condition.

We present in Table 3 all near-optimal perfect secrecy systems that are 5- and 6-fold secure against spoofing under equiprobable source probability distributions. We give the parameters of the systems as well as of the respective designs. We also indicate the optimal number b_{opt} of encoding rules with respect to Theorem 2. All presently known t-designs with $t > 5$ and $\lambda \leq 10$ have been considered. We generally remark that all known t-(v, k, λ) designs with $t > 5$ have $\lambda \geq 4$. Furthermore, three infinite series of 6-designs are known, however, for each λ increases rapidly.

In Table 4, we give further perfect secrecy systems with a feasible number of encoding rules that are 7-fold secure against spoofing under equiprobable source probability distributions. All presently known t-designs with $t > 7$ and $\lambda \leq 3{,}000$ have been considered.

We refer to the above references for further information on the respective designs.

Remark 1 As indicated in Table 3, a perfect secrecy system, constructed from a 6-(23, 7, 4) design, with $k = 7$

Table 4 Some perfect secrecy systems from 8-designs that are 7-fold secure against spoofing attacks

t	k	v	b	b_{opt}	Design Parameters
7	10	31	$100 \times b_{\text{opt}}$	175,305	8-$(31, 10, 100)$
	11	27	$432 \times b_{\text{opt}}$	13,455	8-$(27, 11, 432)$
	11	36	$1{,}260 \times b_{\text{opt}}$	183,396	8-$(36, 11, 1260)$
	11	40	$1{,}440 \times b_{\text{opt}}$	466,089	8-$(40, 11, 1440)$
	12	27	$1{,}296 \times b_{\text{opt}}$	4,485	8-$(27, 12, 1296)$

equiprobable source states and $v = 23$ messages that is 5-fold secure against spoofing requires 57,684 encoding rules. A perfect secrecy system, constructed from a 6-$(25, 7, 6)$ design, with $k = 7$ equiprobable source states and $v = 25$ messages that is 5-fold secure against spoofing requires 151,800 encoding rules.

For comparison, a perfect (5-fold) secrecy system, constructed from an $\mathrm{APA}_{10}(5, 6, 24)$, with $k = 6$ source states and $v = 24$ messages that offers 4-fold security against spoofing for an arbitrary source probability distribution requires 425,040 encoding rules. A perfect (5-fold) secrecy system, constructed from an $\mathrm{APA}_{60}(5, 7, 24)$, with $k = 7$ source states and $v = 24$ messages that is 4-fold secure against spoofing for an arbitrary source probability distribution requires 2,550,240 encoding rules (cf. Subsection 4.2).

8 Application to the Verification Oracle Model

We will now consider the scenario, where the opponent has access to a *verification oracle (V-oracle)*. In this extended authentication model, we assume that the opponent is no longer restricted to *passively* observing messages transmitted by the sender to the receiver. The opponent may send a message of the opponent's choice to the receiver and observe the receiver's response whether or not the receiver accepts it as authentic. This more powerful, *pro-active* attack scenario can be modeled in terms of a V-oracle that provides a response (*accept* or *reject*) to a query message in the same way as the message would be accepted or not by the legitimate receiver. This attack model was recently introduced in [1, 21]. We recall and slightly adjust the notation as far as it is necessary for our consideration. Further details on this model can be found in [1, 21, 29, 30].

In [29], the two types of *online* and *offline* attacks are studied. In the online attack, the receiver is supposed to respond to each incoming query message, and thus the opponent is successful as soon as the receiver accepts a message as authentic. Thus, every query message is at the same time a spoofing message. In the offline attack, the query and the spoofing phase are separated. First, the opponent makes all his queries to the oracle, and then uses this collected (state) information to construct a spoofing message. In both scenarios, the opponent is assumed to be adaptive. The online attack models an opponent's interaction with a verification oracle such as an ATM machine, while in the offline attack the opponent may have captured an offline verification box. Often, the offline attack model is used as an intermediate model for analyzing the online scenario. We speak in each scenario of a *spoofing attack* of order i *in the V-oracle model* if the opponent has access to i verification queries. The opponent's strategy can be modeled via probability distributions on the query set $\mathcal{M}$ of verification queries. The *online deception probability* $P_{d_i}^{\mathsf{online}}$, respectively *offline deception probability* $P_{d_i}^{\mathsf{offline}}$, denotes the probability that the opponent can deceive the receiver with a spoofing attack of order i. In [29], lower bounds on these deception probabilities have been obtained.

Theorem 9 (Tonien–Safavi-Naini–Wild) *In an authentication system with k source states and v messages, the offline and online deception probabilities in the V-oracle model are bounded below by*

$$P_{d_i}^{\mathsf{offline}} \geq \frac{k}{v} \quad \textit{and} \quad P_{d_i}^{\mathsf{online}} \geq 1 - \frac{\binom{v-k}{i+1}}{\binom{v}{i+1}}, \quad \textit{respectively.}$$

Interestingly, it furthermore follows that

$$P_{d_i}^{\mathsf{offline}} = \frac{k}{v} \quad \text{if and only if} \quad P_{d_i}^{\mathsf{online}} = 1 - \frac{\binom{v-k}{i+1}}{\binom{v}{i+1}}.$$

Thus, an authentication system that attains the bound in the offline attack is the same as in the online attack, and vice versa. Clearly, $P_{d_i}^{\mathsf{offline}}$ is independent of i. If the bound for $P_{d_i}^{\mathsf{online}}$ is satisfied with equality, then also the bound for $P_{d_{i-1}}^{\mathsf{online}}$ is satisfied with equality for $i > 1$ (cf. [29]). Hence, we call a system *t-fold secure against spoofing in the V-oracle model* if $P_{d_t}^{\mathsf{offline}} = \frac{k}{v}$ or, equivalently, $P_{d_t}^{\mathsf{online}} = 1 - \frac{\binom{v-k}{t+1}}{\binom{v}{t+1}}$. The notation of perfect secrecy holds as given in Section 2. An analogue to Theorem 2 has been derived in [29] for the V-oracle model.

Theorem 10 (Tonien–Safavi-Naini–Wild) *If an authentication system is $(t-1)$-fold secure against spoofing in the V-oracle model, then the number of encoding rules is bounded below by*

$$b \geq \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Again, we call a system *optimal* when the lower bound holds with equality. For equiprobable source states, optimal authentication systems which are $(t-1)$-fold against spoofing in the V-oracle model have been characterized in [29]. We give the result in a slightly more generalized form, which can easily be obtained from the original proof.

Theorem 11 (Tonien–Safavi-Naini–Wild) *Suppose there is a t-(v,k,λ) design. Then there is an authentication system for k equiprobable source states, having v messages and $\lambda \cdot \binom{v}{t}/\binom{k}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing in the V-oracle model. Conversely, if there is an authentication system for k equiprobable source states, having v messages and $\binom{v}{t}/\binom{k}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing in the V-oracle model, then there is a Steiner t-$(v,k,1)$ design.*

We will apply now Theorem 6 to construct perfect secrecy systems that provide a high level of security against spoofing in the V-oracle model for equiprobable source probability distributions. This generalizes the result [16, Thm. 3.27], where the case $\lambda = 1$ has been treated.

Theorem 12 *Suppose there is a t-(v,k,λ) design, where v divides the number of blocks $b = \lambda\binom{v}{t}/\binom{k}{t}$. Then there is a perfect secrecy system for k equiprobable source states, having v messages and b encoding rules, that is $(t-1)$-fold secure against spoofing in the V-oracle model. Moreover, the system is optimal if and only if $\lambda = 1$.*

Proof By Theorem 11, the system is $(t-1)$-fold secure against spoofing in the V-oracle model. Under the assumption that the encoding rules are used with equal probability, we may proceed as in the proof of Theorem 6 to verify that the system also achieves perfect secrecy. With respect to Theorem 10 optimality is obtained if and only if $\lambda = 1$. □

Clearly, Theorem 7 can also be applied to the V-oracle model.

Theorem 13 *For all integers t and v with $v \equiv t \pmod{(t+1)!^{2t+1}}$ and $v \geq t+1 > 0$, there exists a perfect secrecy system for $t+1$ equiprobable source states, having v messages and $b = (t+1)!^{2t}t!\binom{v}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing in the V-oracle model.*

All the results in Section 6 and Section 7 may be transferred accordingly.

9 Conclusion

We have given novel perfect secrecy systems that provide immunity to spoofing attacks under equiprobable source probability distributions. Our construction method generalized in a natural manner the approach in [13] and allowed us to use t-designs instead of merely Steiner t-designs in the construction process. From a theoretical point of view, we have shown that based on Teirlinck's existence result for t-designs, perfect secrecy systems can be generated that can reach an arbitrary high level of security. Concerning explicit constructions, we have obtained, via cyclic difference families, very efficient constructions of new optimal systems that are onefold secure against spoofing. By using t-designs for large values of t, we have also presented the first near-optimal systems that are 5- and 6-fold secure as well as further systems with a feasible number of keys that are 7-fold secure against spoofing. Previous constructions of multifold secure systems had been known only for arbitrary source probability distributions, which inherently result in larger numbers of encoding rules for achieving the same level of security. We have furthermore applied our results to a recently extended authentication model, where the opponent has access to a verification oracle. Novel perfect secrecy systems with immunity to spoofing in the verification oracle model have been obtained this way.

References

1. 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.
2. Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, vol. I and II, Encyclopedia of Math. and Its Applications, vol. 69/78, Cambridge Univ. Press, Cambridge, 1999.
3. A. Betten, R. Laue and A. Wassermann, "Simple 6- and 7-designs on 19 to 33 points", *Congr. Numer.*, vol. 123, pp. 149–160, 1997.
4. A. Betten, R. Laue and A. Wassermann, "Simple 7-designs with small parameters", *J. Combin. Designs*, vol. 7, pp. 79–94, 1999.
5. A. Betten, A. Kerber, R. Laue and A. Wassermann, "Simple 8-designs with small parameters", *Designs, Codes and Cryptography*, vol. 15, pp. 5–27, 1998.
6. J. Bierbrauer and Y. Edel, "Theory of perpendicular arrays", *J. Combin. Designs*, vol. 2, pp. 375–406, 1994.
7. J. Bierbrauer, "Ordered designs, perpendicular arrays, and permutation sets", in *Handbook of Combinatorial Designs*, ed. by C. J. Colbourn and J. H. Dinitz, 2nd ed., CRC Press, Boca Raton, pp. 543–547, 2006.
8. K. Chen, R. Wei and L. Zhu, "Existence of $(q, 7, 1)$ difference families with q a prime power", *J. Combin. Designs*, vol. 10, pp. 126–138, 2002.
9. C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, 2nd ed., CRC Press, Boca Raton, 2006.

10. M. De Soete, “Some constructions for authentication - secrecy codes”, in *Advances in Cryptology – EUROCRYPT ’88*, ed. by Ch. G. Günther, Lecture Notes in Computer Science, vol. 330, Springer, Berlin, Heidelberg, New York, pp. 23–49, 1988.
11. P. Godlewski and C. Mitchell, “Key-minimal cryptosystems for unconditional secrecy”, *J. Cryptology*, vol. 3, pp. 1–25, 1990.
12. M. Huber, *Flag-transitive Steiner Designs*, Birkhäuser, Basel, Berlin, Boston, 2009.
13. 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.
14. M. Huber, “Coding theory and algebraic combinatorics”, in *Selected Topics in Information and Coding Theory*, ed. by I. Woungang et al., World Scientific, Singapore, pp. 121–158, 2010.
15. M. Huber, “Constructing optimal authentication codes with perfect multi-fold secrecy”, in *Proc. International Zurich Seminar on Communications (IZS) 2010*, pp. 86–89, 2010.
16. M. Huber, *Combinatorial Designs for Authentication and Secrecy Codes*, Foundations and Trends in Communications and Information Theory, Now Publishers, Boston, Delft, 2010.
17. G. B. Khosrovshahi and R. Laue, “t-designs with $t \geq 3$”, in *Handbook of Combinatorial Designs*, ed. by C. J. Colbourn and J. H. Dinitz, 2nd ed., CRC Press, Boca Raton, pp. 79–101, 2006.
18. E. S. Kramer and D. M. Mesner, “t-designs on hypergraphs”, *Discrete Math.*, vol. 15, pp. 263–296, 1976.
19. J. L. Massey, “Cryptography – a selective survey”, in *Digital Communications*, ed. by E. Biglieri and G. Prati, North-Holland, Amsterdam, New York, Oxford, pp. 3–21, 1986.
20. D. Pei, *Authentication Codes and Combinatorial Designs*, CRC Press, Boca Raton, 2006.
21. 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*, ed. by F. Bao et al., Lecture Notes in Computer Science, vol. 2947, Springer, Berlin, Heidelberg, New York, pp. 231–248, 2004.
22. P. Schöbi, “Perfect authentication systems for data sources with arbitrary statistics” (presented at EUROCRYPT ’86), unpublished.
23. C. E. Shannon, “Communication theory of secrecy systems”, *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.
24. G. J. Simmons, “Authentication theory/coding theory”, in *Advances in Cryptology – CRYPTO ’84*, ed. by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science, vol. 196, Springer, Berlin, Heidelberg, New York, pp. 411–432, 1985.
25. G. J. Simmons, “A survey of information authentication”, in *Contemporary Cryptology: The Science of Information Integrity*, ed. by G. J. Simmons, IEEE Press, Piscataway, pp. 379–419, 1992.
26. D. R. Stinson, “The combinatorics of authentication and secrecy codes”, *J. Cryptology*, vol. 2, pp. 23–49, 1990.
27. D. R. Stinson, “Combinatorial designs and cryptography”, in *Surveys in Combinatorics*, ed. by K. Walker, London Math. Soc. Lecture Note Series, vol. 187, Cambridge Univ. Press, Cambridge, pp. 257–287, 1993.
28. L. Teirlinck, “Non-trivial t-designs without repeated blocks exist for all t”, *Discrete Math.*, vol. 65, pp. 301–311, 1987.
29. D. Tonien, R. Safavi-Naini and P. Wild, “Combinatorial characterizations of authentication codes in verification oracle model”, in *Proc. 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007)*, ed. by F. Bao and S. Miller, pp. 183–193, 2007.
30. D. Tonien, R. Safavi-Naini and P. Wild, “Authentication codes in the query model”, in *Coding and Cryptology*, ed. by Y. Li et al., World Scientific, Singapore, pp. 214–225, 2008.
31. Tran van Trung, “On the construction of authentication and secrecy codes”, *Designs, Codes and Cryptography*, vol. 5, pp. 269–280, 1995.