AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **31** (2005), Pages 179–187

Minkowski tangent-circle structures and key distribution patterns*

S. Bonvicini

Dipartimento di Matematica
Università di Modena e Reggio Emilia
via Campi 213/B, 41100 Modena
Italy
bonvicini.simona@unimore.it

G. Rinaldi

Dipartimento di Scienze Agrarie
Università di Modena e Reggio Emilia
via Kennedy 17, 42100 Reggio Emilia
Italy
rinaldi.gloria@unimore.it

Abstract

Key distribution patterns, as defined in Mitchell and Piper, *Discrete Applied Math.* 21 (1988), 215–228, are finite incidence structures satisfying a certain property which enables them to be applied to a problem in network key distribution. Few examples of key distribution patterns are known. In this paper we present new examples of finite Minkowski tangent-circle structures, (Quattrocchi and Rinaldi, *Research and Lecture Notes in Mathematics, Combinatorics '88, Mediterranean Press* 2 (1988), 349–357) and show how to construct key distribution patterns from them.

1 Introduction

The Minkowski tangent-circle structures were introduced in [13] and [14] as a generalization of Minkowski planes. More precisely, a Minkowski tangent-circle structure of finite order s, $s \geq 2$, is an incidence structure $\mathcal{M} = (\mathcal{P}, \mathcal{B}, \mathcal{G}_1, \mathcal{G}_2)$ where $\mathcal{P}$ is a set of $(s+1)^2$ *points*, $\mathcal{B}$ is a set of subsets of $\mathcal{P}$ (*circles*), $\mathcal{G}_1$ and $\mathcal{G}_2$ are respectively sets of $s+1$ disjoint subsets of $\mathcal{P}$ (*generators*) which partition $\mathcal{P}$ and:

(i) Each circle has exactly one point in common with each generator;

* Research done within the activity of GNSAGA–INdAM with the financial support of MIUR (project "Strutture Geometriche, Combinatoria e loro applicazioni")

(ii) Each generator contains $s+1$ points and each generator of $\mathcal{G}_1$ intersects each generator of $\mathcal{G}_2$ at exactly one point;

(iii) For every pair of points P and Q not lying on the same generator and for every circle B with $P \notin B$ and $Q \in B$, there exists a unique circle C such that $P, Q \in C$ and C and B are tangent at Q.

A set of points no two of which belong to the same generator is called a set of *independent* points.
The incidence structure $\mathcal{M}$ satisfies the following properties (see [14]):

(i) There is a fixed number u of circles, $1 \leq u \leq s-1$, containing any two given independent points;

(ii) At most one circle contains any three given independent points;

(iii) There are su circles containing any given point;

(iv) The total number of circles is $s(s+1)u$.

The number u is called the *degree* of $\mathcal{M}$. Each Minkowski plane of order s is a Minkowski tangent-circle structure of order s and degree $s-1$, as well as each affine plane of order s is a Minkowski tangent-circle structure of order $s-1$ and degree 1. If $s \equiv 1(2)$, the relation $u = \frac{s-1}{2}$ is a necessary condition for a finite Minkowski tangent-circle structure to be contained in a Minkowski plane of the same order, [13], [14]. The known finite Minkowski planes of odd order p^m, p prime, [9], properly contain Minkowski tangent-circle structures of the same order p^m and degree $\frac{p^m-1}{2}$, [14]. Moreover a Minkowski plane of even order (which is necessarily the (B)-geometry associated with a group $PGL(2, 2^m)$, [12]) does not contain Minkowski tangent-circle structures of the same order properly, [14]. It is still an open problem to find examples which cannot be embedded in a Minkowski plane. An example was constructed in [13] using points and lines of the affine plane $\mathrm{AG}(2, 2^m)$ together with a family of conics. In this paper we generalize this example using a suitable family of ovals. We show that the method given in [15] can be applied to these new examples to construct key distribution patterns.

2 Examples of finite Minkowski tangent-circle structures of even order

Let $\mathbb{K} = GF(2^m)$ and $\sigma \in Aut\mathbb{K}$ with $\sigma : x \mapsto x^2$. Let $I = \{h \in \mathbb{N} | 1 \leq h < m, (h, m) = 1\}$, and $a, b \in \mathbb{K}$, $a \neq 0$; the set $\theta^h_{a,b} = \{(x, y) | y = ax^{2^h} + b\}$ is an oval in $AG(2, 2^m)$ which is tangent to the line at infinity, [5]. Its tangent lines are all those of equation $y = k, k \in \mathbb{K}$, together with the line at infinity. The lines of equation $x = k$ contain the point at infinity of the oval and intersect the oval in exactly one affine point. For every pair of points (x_1, y_1), (x_2, y_2) with $x_1 \neq x_2$ and $y_1 \neq y_2$ and for every $h \in I$ there exists exactly one oval $\theta^h_{a,b}$ passing through (x_1, y_1), (x_2, y_2). In fact the equations $y_1 = ax_1^{2^h} + b$, $y_2 = ax_2^{2^h} + b$ have exactly one common solution for (a, b). Let $p \neq 1$ be the smallest factor of m. We prove the following:

Proposition 1. *Let $h, k \in I$. If $h \neq k$ and $(k-h, m) = 1$, then $|\theta^h_{a,b} \cap \theta^k_{c,d}| \in \{0, 2\}$. If $h = k$ and $\theta^h_{a,b} \neq \theta^k_{c,d}$, then $|\theta^h_{a,b} \cap \theta^k_{c,d}| = 0, 1$ according to $a = c$ or $a \neq c$.*

Proof. Suppose $|\theta^h_{a,b} \cap \theta^k_{c,d}| = s$, then the equation $ax^{2^h} + b = cx^{2^k} + d$ or equivalently $a^{2^{n-h}}x + b^{2^{n-h}} = c^{2^{n-h}}x^{2^{k-h}} + d^{2^{n-h}}$ has exactly s solutions in $\mathbb{K}$. If $(k-h, m) = 1$, the curve $y = c^{2^{n-h}}x^{2^{k-h}} + d^{2^{n-h}}$ is an oval in $AG(2, 2^m)$, [5], and $s \in \{0, 2\}$. Suppose now $h = k$, then we obtain $a^{2^{n-h}}x + b^{2^{n-h}} = c^{2^{n-h}}x + d^{2^{n-h}}$ and the assertion follows. ☐

Let $T \subset I$ be a set such that $k - h \in I \cup \{0\}$ for every $h, k \in T$.

Proposition 2. *If $m \equiv 0(2)$, then $|T| = 1$. If $m \equiv 1(2)$, then $|T| \leq p - 1$, where p is the smallest prime dividing m.*

Proof. Suppose $m \equiv 0(2)$, let h, k be distinct elements of I, then $h - k \equiv 0(2)$, $h - k \notin I$ and the first assertion follows. Let now $m \equiv 1(2)$, let $h, k \in T$, $h \neq k$, let q be a factor of m, then the relation $(h-k, m) = 1$ implies $h \not\equiv k(q)$. The prime p is the smallest factor of m, then $h \not\equiv k(p)$. This implies $|T| \leq p - 1$. ☐

We can find a set T of maximal length $p - 1$ simply taking $T = \{i | 1 \leq i < p\}$. Denote by $\mathcal{R}$ the set of lines of $AG(2, 2^m)$ with equation $y = ax + b$, $a \neq 0$. Let $h \in T$ and $\Theta^h = \{\theta^h_{a,b}, a, b \in \mathbb{K}, a \neq 0\}$. To standardize the notation set $\mathcal{R} = \Theta^0$ and $\overline{T} = T \cup \{0\}$. For each subset $J \subset \overline{T}$, $J \neq \emptyset$, denote by $\mathcal{M}_J = (\mathcal{P}, \mathcal{B}, \mathcal{G}_1, \mathcal{G}_2)$ the incidence structure defined in the following manner: $\mathcal{P}$ is the set of points of $AG(2, 2^m)$, $\mathcal{B} = \{\Theta^h | h \in J\}$, $\mathcal{G}_1$ and $\mathcal{G}_2$ are the sets of lines of $AG(2, 2^m)$ with equation $x = k$ and $y = k$, $k \in \mathbb{K}$, respectively.

Proposition 3. *The incidence structure $\mathcal{M}_J$ is a Minkowski tangent-circle structure of order $2^m - 1$ and degree $|J| \leq p$.*

Proof. It follows from Proposition 1 observing that for each pair of independent points (x_1, y_1), (x_2, y_2) there is exactly one oval of Θ^h, $h \in T$, containing them, and from the fact that each line of $\mathcal{R}$ intersects each oval of Θ^h, $h \in T$, in either 0 or 2 points. ☐

When $J = \{0, 2\}$ we reobtain the example of [13], when $J = \{0\}$, we have the affine plane of order 2^m which is a finite tangent-circle structure of order $2^m - 1$ and degree 1.

3 Examples of Key Distribution Patterns

A *key distribution scheme* (KDS) is a method of distributing secret pieces of information to nodes in a network in such a way that any pair of nodes can compute a secure common key. This information is generated and distributed by a trusted server which is active only at the distribution stage. In [8] Mitchell and Piper proposed the use of a certain special kind of incidence structure to give a KDS. They called such an incidence structure a *key distribution pattern* (KDP). Their basic idea was that of issuing each node with a set of subkeys and each key to be used by a pair of nodes is made up from a combination of some of these subkeys. The combining should be done using a publicly known function which takes a specified number of subkeys as arguments and yields an n-bit symmetric key. For increased security, the function should be one-way. Suppose we think of the set of nodes as the set of points $\mathcal{P}$ and the set of subkeys as the set of blocks $\mathcal{B}$ of an incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. The incidence relation $\mathcal{I}$ between points and blocks is defined so that a point is incident with a block if the corresponding node posesses the corresponding subkey. Denote by (P) the set of blocks incident with the point P, then the symmetric key K_{ij} of P_i and P_j is generated by the subkeys in $(P_i) \cap (P_j)$. Following Mitchell and Piper, let $|\mathcal{P}| = v$, $v \geq 3$, and let w be an integer with $1 \leq w \leq v-2$. The incidence structure $\mathcal{K} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a w-KDP (w-key distribution pattern) if for every pair of points P_i, P_j we have:

$$(P_i) \cap (P_j) \not\subseteq \bigcup_{i=1}^{w} (Q_i) \quad (*)$$

for any point $Q_1, \ldots, Q_w \in \mathcal{P} - \{P_i, P_j\}$.
Condition (*) ensures that P_i and P_j share at least one subkey not in any of $(Q_1), \ldots, (Q_w)$. Let $\mathbb{N}$ be the set of positive integers and let $l : \mathcal{B} \to \mathbb{N}$ be a mapping which simply assigns to each subkey x the number $l(x)$ of bits it contains; we call such a mapping a *length mapping*. Denote by L_s the mapping $L_s : \mathcal{B} \to \{s\}$. A length mapping l is said to be *w-secure* if for each pair $P_i, P_j \in \mathcal{P}$ and for each set of w points $Q_1, \ldots Q_w \in \mathcal{P} - \{P_i, P_j\}$ we have:

$$\sum_{x \in ((P_i) \cap (P_j)) - \bigcup_{i=1}^{w} (Q_i)} l(x) \geq n \qquad (*)'$$

where n is the number of bits comprising each key. The condition insures that even if $Q_1, \ldots, Q_w$ pool their subkey sets, their chance of guessing the common key $K_{i,j}$ between P_i and P_j is no greater than that of someone who knows none of the subkeys in $(P_i) \cap (P_j)$. Obviously L_n is a w-secure length mapping for any w-KDP.
Let $\mathcal{K} = (\mathcal{P}, \mathcal{B}, I)$ be a w-KDP and let P be a point of $\mathcal{K}$. Let l be a w-secure length mapping for $\mathcal{K}$. The *node storage* ρ_P at P is defined as follows: $\rho_P = \sum_{x \in (P)} l(x)$. The average node storage $\overline{\rho}$ of $(\mathcal{K}, l)$ is the average of the node storages. The *total storage* β of $(\mathcal{K}, l)$ is the total number of bits in the subkeys of $\mathcal{K}$, that is: $\beta = \sum_{x \in \mathcal{B}} l(x)$. The length mapping l is said to be *optimal* if there is no w-secure length mapping l' such that either the node storage of $(\mathcal{K}, l')$ is less than $\overline{\rho}$ or the total node storage of $(\mathcal{K}, l')$ is less than β.
Let m be the greatest value such that

$$|((P_i) \cap (P_j)) - \bigcup_{k=1}^{w} (Q_k)| \geq m$$

for every pair P_i, $P_j \in \mathcal{P}$ and for any $Q_1, \dots, Q_w \in \mathcal{P} - \{P_i, P_j\}$. Quinn proved that $L_{\lceil \frac{n}{m} \rceil}$ is an optimal constant w-secure length mapping for $\mathcal{K}$, [10]. The number m is said to be a *w-residue* of $\mathcal{K}$.

If we consider the trivial w-KDP on v nodes, that is a $2-(v,2,1)$ design, then $w = v-2$, L_n is an optimal $(v-2)$-secure length mapping, $\overline{\rho} = (v-1)n$ and $\beta = \frac{v(v-1)n}{2}$. This is the standard against which all other w-KDPs are compared. Examples of KDPs have been constructed using the so called circle geometries (Inversive, Laguerre and Minkowski planes), [6], [7], using families of conics in finite affine Deasrguesian planes [11], and using tangent-circle structures, [15]. All these examples work on either r^{2m}, $(r^{2m}+1)$, $r^{2m}+r^m$ or $(r^m+1)^2$ points, r a prime. In this paper we give a family of examples working on 2^{2m} points, m odd. More precisely, let $m \in \mathbb{N}$ be an odd positive integer and let $p \neq 1$ be the smallest factor of m. Let $\mathcal{M}_J$ be the Minkowski tangent-circle structure of order $s = 2^m - 1$ and degree $u = |J|$, constructed in Proposition 3. When $u \geq 2$, $\mathcal{M}_J$ provides an example of $w-$KDP, with $1 \leq w \leq u-1$ ([15, Proposition 2]). Denote by $\overline{\mathcal{B}}$ the set of circles of $\mathcal{M}_J$ together with the pairs $\{P_i, P_j\}$ where P_i and P_j are distinct points which lie on one and the same generator. Let $l : \overline{\mathcal{B}} \to \mathbb{N}$ be the length mapping defined by either $l(x) = \lceil \frac{n}{u-w} \rceil$ or n, according to x is a circle of $\mathcal{M}_J$ or not. The map l is a w-secure length mapping, [15], leading to the storage:

$\overline{\rho} = su\lceil \frac{n}{u-w} \rceil + 2sn$

$\beta = s(s+1)u\lceil \frac{n}{u-w} \rceil + s(s+1)^2 n$

and we obtain the following table:

	$\mathcal{M}_J$
u	$2 \leq u \leq p$
w	$u-1$
v	2^{2m}
$\overline{\rho}$	$u(2^m-1)\lceil \frac{n}{u-w} \rceil + 2(2^m-1)n$
β	$u(2^m-1)2^m\lceil \frac{n}{u-w} \rceil + (2^m-1)2^{2m}n$

Another KDP can be obtained from $\mathcal{M}_J$ applying [15, Proposition 3]. Precisely, suppose the existence of $t \geq 2$ permutations $\pi_1 \dots \pi_t$ on the point-set of $\mathcal{M}_J$ satisfying the following property:

(i) for each ordered pair (i,j), with $1 \leq i,j \leq t$, $i \neq j$ and for each pair P_1, P_2 of points, if $\pi_i(P_1)$ and $\pi_i(P_2)$ lie on a same generator, then $\pi_j(P_1)$ and $\pi_j(P_2)$ are independent.

Under this condition denote by $\mathcal{M}'_J$ the incidence structure $(\overline{\mathcal{P}}, \overline{\mathcal{B}})$ which is defined as follows. The point-set $\overline{\mathcal{P}}$ is the point-set $\mathcal{P}$. The block-set $\overline{\mathcal{B}}$ is the set of all blocks $\pi_i^{-1}(C)$ as C varies in $\mathcal{B}$ and π_i varies in $\{\pi_1, \dots, \pi_t\}$. It does not matter if some blocks are repeated. For each w with $1 \leq w \leq u-1$, let $l : \overline{\mathcal{B}} \longrightarrow \mathbb{N}$ be the length mapping defined by $l(x) = \lceil \frac{n}{(u-w)(t-1)} \rceil$. It was proved in [15] that l is a w-secure length mapping leading to the following storages: $\overline{\rho} = u(2^m-1)t\lceil \frac{n}{(u-w)(t-1)} \rceil$, $\beta = u(2^m-1)t2^m\lceil \frac{n}{(u-w)(t-1)} \rceil$ and to the following table:

	$\mathcal{M}'_J$
u	$2 \leq u \leq p$
w	$u-1$
v	2^{2m}
$\overline{\rho}$	$u(2^m-1)t\lceil \frac{n}{(t-1)(u-w)} \rceil$
β	$u(2^m-1)t2^m\lceil \frac{n}{(t-1)(u-w)} \rceil$

If we take the maximal values $u = p$ and $w = p-1$ then we have the maximal security. Furthermore the storages $\overline{\rho}$ and β depend on t. In particular their values decrease as t increases. A minor adaptation of the proof of [6, Lemma 3.3] shows that the existence of N mutually orthogonal latin squares of order 2^m give rise to $\lfloor \frac{N}{2}+1 \rfloor$ permutations with the property (i). In particular 2^m is a power of a prime so that we can take for N each value from 1 to 2^m-1, [2], therefore we have $t \leq \lfloor \frac{2^m-1}{2}+1 \rfloor = 2^{m-1}$. We can compare our new models to those obtained from circle geometries, see [7], [11] and [15]. Our models involve 2^{2m} nodes. The same number 2^{2m} can be found in the models constructed in [7] starting from a Laguerre plane of order s, when $s = 2^m$, and in [11, Theorem 7.8]. In some cases our examples yield better parameters, in fact the models of [7] and [11] both lead to the following table, see [7, Table 1]:

	$\mathcal{K}_4(s,u,t)$
u	$2 \leq u \leq s$
t	$2 \leq t \leq s+1$
w	$u-1$
v	s^2
$\overline{\rho}$	$tus\lceil \frac{n}{(t-1)(u-w)} \rceil$
β	$tus^2\lceil \frac{n}{(t-1)(u-w)} \rceil$

If $s = 2^m$ and $u = p$, where p is the smallest prime factor of m, we can compare the two models. In $\mathcal{M}'_J$ the best chioce for t is $t = 2^{m-1}$ which leads to the storages: $\overline{\rho} = p(2^m-1)2^{m-1}\lceil \dfrac{n}{2^{m-1}-1} \rceil$ and $\beta = p(2^m-1)2^{m-1}2^m\lceil \dfrac{n}{2^{m-1}-1} \rceil$.

In the models of [7] and [11] the best choice for t is $t = 2^m + 1$ which leads to: $\overline{\rho} = (2^m+1)p2^m\lceil\frac{n}{2^m}\rceil$ and $\beta = (2^m+1)p2^{2m}\lceil\frac{n}{2^m}\rceil$.

The total number of subkeys in $\mathcal{M}'_J$ is less then the total number of subkeys of $\mathcal{K}_4(s,u,t)$. Despite that we take the same n, the length of each subkey in $\mathcal{M}'_J$ is greater than the length of each subkey in $\mathcal{K}_4(s,u,t)$, but a suitable choice for n (for example take n in such a way that $2\lceil\frac{n}{2^m}\rceil \geq \lceil\frac{n}{2^{m-1}-1}\rceil$) leads to smaller storages in $\mathcal{M}'_J$.

4 Information rates and resilient functions

Let $\mathcal{K} = (\mathcal{P},\mathcal{B},\mathcal{I})$ be a $w-$KDP. Let $\mathcal{U}$ be the finite set of keys. There will be some probability distribution associated with each key K_{ij} and $\bar{K}_{ij}$ will denote a random variable defined on $\mathcal{U}$ having that probability distribution. Denote by U_{P_i} the set of all possible secrete subkeys distributed to user P_i and $\bar{U}_{P_i}$ denotes a random variable which assumes values U_{P_i} according to a probability distribution. Following the lines of [16] the efficiency of the KDP can be mesured by the amount of secret information that is distributed to each user. The *information rate* is thus defined to be $min\{\frac{H(\bar{K}_{ij})}{H(\bar{U}_{P_i})} : P_i \in \mathcal{P}\}$, where H denotes the entropy function, (for a definition of the entropy function see [17]). Let q be a prime power and suppose each subkey of $\mathcal{K}$ to be an element of $GF(q)$. The symmetric key K_{ij} of two points P_i and P_j is thus the sum of their common subkeys. A key K_{ij} is equally likely to be any element of $GF(q)$, in which case $H(\bar{K}_{ij}) = \log q$. Furthermore a user P_i recives (P_i) values of $GF(q)$, and each value is equally likely to be any element of $GF(q)$, so that $H(P_i) = (P_i)\log q$. Therefore the information rate of a KDP is $\frac{1}{\{max(P_i) : P_i \in \mathcal{P}\}}$ and the *total information rate* is $\frac{1}{|\mathcal{B}|}$, [16, Theorem 3.1]. The information rate and the total information rate of a KDP are in general low values.

In [16] Stinson described a method to improve them, and then to improve the efficiency of a KDP, using *resilient functions*. We review this approach. An (n,l,t,q)-resilient function is a function $f : [GF(q)]^n \mapsto [GF(q)]^l$ which satisfies the property that if the values of t of the n inputs are fixed, and the remaining $n-t$ inputs are chosen independently at random from $GF(q)$, then all possible output $l-$tuple are equally likely to occur. Resilient functions were introduced in [1] and [3]. As an example, the function $f : [GF(q)]^n \mapsto GF(q)$ defined as $f(x_1,\ldots,x_n) = x_1+\cdots+x_n$, is an $(n,1,n-1,q)$-resilient function. (It is used above to determine the key K_{ij} when two nodes have n subkeys in common). It can be shown that $l \leq n-t$ in any resilient function. A construction of resilient functions with $l = n-t$ can be found in [4], more precisely, if q is a prime power such that $q \geq n-1$, then there exists a $(n,n-t,t,q)$-resilient function. For each pair $a = (P_i,P_j)$ of points of $\mathcal{K}$ and for each set $\{Q_1,\ldots,Q_w\} \subset \mathcal{P} - \{P_i,P_j\}$, denote by C_a the number of subkeys in $(P_i) \cap (P_j)$ and by D_a the number of subkeys of $(P_i) \cap (P_j)$ which contain at least one point Q_i. Define $l = \min\{C_a - D_a\}$ as a varies in the set of pairs of $\mathcal{P}$.

Let q be a prime power with $q \geq max\{C_a\} - 1$ as a varies in the set of pairs of $\mathcal{P}$. Then there exists a (C_a, l, D_a, q)-resilient function f_a and the key K_{ij} is thus an element of $[GF(q)]^l$: precisely $f_a(x_1, \ldots, x_{C_a})$ denoting by x_i a common subkey of the pair $a = (P_i, P_j)$. Now the information rate and the total information rate are respectively $\dfrac{l}{max\{(P) : P \in \mathcal{P}\}}$ and $\dfrac{l}{|\mathcal{B}|}$, [16, Theorem 3.5]. The value l improves the efficiency of the KDP and we have chosen l as large as possible.

Let now go back to $\mathcal{M}'_J$ and $\mathcal{K}_4(s, u, t)$. In the first case we obtain $C_a = p2^{m-1}$ and $D_a = (p-1)2^{m-1}$ for each pair a. Let q be a prime power with $q \geq 2^{m-1}p - 1$ and let f be a $(p2^{m-1}, 2^{m-1}, (p-1)2^{m-1}, q)$-resilient function. Each subkey is an element of $GF(q)$ and then it can be represented by an r-bit string with $2^r \geq q$. Recall that the length of each subkey must be $\lceil \dfrac{n}{2^{m-1} - 1} \rceil$, where n denotes the length of each key. Therefore we must take n in such a way that $\lceil \dfrac{n}{2^{m-1} - 1} \rceil \geq r$. An easy calculation shows that it is possible to take n in such a way that $\lceil \dfrac{n}{2^{m-1} - 1} \rceil = r$. This leads to the storages: $\overline{\rho} = p(2^m - 1)2^{m-1}r$ and $\beta = p(2^m - 1)2^{m-1}2^m r$. With r the smallest value satisfying the relation $2^r \geq q$. The information and total information rates are: $\dfrac{1}{p(2^m - 1)}$ and $\dfrac{1}{p2^m(2^m - 1)}$ respectively. In $\mathcal{K}_4(s, u, t)$ we obtain $C_a = p(2^m + 1)$ and $D_a = (p-1)(2^m + 1)$. Let $\bar{q}$ be a prime power with $\bar{q} \geq (2^m + 1)p - 1$ and let $\bar{f}$ be a $(p(2^m + 1), 2^m + 1, (p-1)(2^m + 1), \bar{q})$-resilient function. Each subkey is an element of $GF(\bar{q})$ and then it can be represented by a $\bar{r}$-bit string with $2^{\bar{r}} \geq \bar{q}$. As before, denoting by $\bar{n}$ the length of each key, we must take $\bar{n}$ in such a way that $\lceil \dfrac{\bar{n}}{2^m} \rceil \geq \bar{r}$. It is possible to take $\bar{n}$ with $\lceil \dfrac{\bar{n}}{2^m} \rceil = \bar{r}$. This leads to the storages: $\overline{\rho} = p(2^m + 1)2^m \bar{r}$ and $\beta = p(2^m + 1)2^{2m}\bar{r}$. With $\bar{r}$ the smallest value satisfying the relation $2^{\bar{r}} \geq \bar{q}$. The information and total information rates are : $\dfrac{1}{p2^m}$ and $\dfrac{1}{p2^{2m}}$ respectively.

The efficiency of $\mathcal{M}'_J$ is better than the efficiency of $\mathcal{K}_4(s, u, t)$. Furthermore $\bar{q} \geq q$ which implies $\bar{r} \geq r$ so that the storages of $\mathcal{M}'_J$ are better (smaller) than the storages of $\mathcal{K}_4(s, u, t)$.

References

[1] C.H. Bennett, G. Brassard and J.M. Robert, *Privacy amplification by public discussion*, SIAM J. Comput. **17** (1988), 210–229.

[2] R.C. Bose, *On the applications of the properties of Galois fields to the construction of hyper-Graeco-Latin squares*, Sankhyā **3** (1938), 323–338.

[3] B. Chore, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky, *The bit extraction problem or t-resilient functions*, Proc. 26th IEEE Symposium on Foundations of Computer Science (1985), 396–407.

[4] K. Gopalakrishnan, *A study of correlation-immune, resilient and related cryptographic functions*, PhD Thesis, University of Nebraska-Lincoln, 1994.

[5] J.W.P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford 1979-XII.

[6] C.M. O'Keefe, *Key distribution patterns using Minkowski planes*, Designs Codes and Cryptography **5** (1995), 261–267.

[7] C.M. O'Keefe, *A comparison of key distribution patterns constructed from circle geometries*, Advances in Cryptology, AUSCRYPT '92, Springer-Verlag, Berlin. Lecture Notes in Computer Science **718** (1992), 517–527.

[8] C.J. Mitchell and F.C. Piper, *Key storage in secure networks*, Discrete Applied Math. **21** (1988), 215–228.

[9] M. Meschiari and P. Quattrocchi, *Una classificazione delle strutture di incidenza associate a insiemi di sostituzioni strettamente* 3*-transitivi finiti*, Atti Sem. Mat. Fis. Univ. Modena **24** (1975), 123–141.

[10] K.A.S. Quinn, *Combinatorial structures with applications to information theory*, PhD thesis, RHBNC, University of London, (1991).

[11] K.A.S. Quinn, *Some construction for key distribution patterns*, Designs, Codes and Cryptography **4** (1994), 177–191.

[12] P. Quattrocchi, *Sugli insiemi di permutazioni strettamente* 3*-transitivi finiti*, Atti Sem. Mat. Fis. Univ. Modena **24** (1975), 279–289.

[13] P. Quattrocchi, *Insiemi planari di permutazioni*, Atti Sem. Mat. Fis. Univ. Modena **36** (1988), 141–151.

[14] P. Quattrocchi and G. Rinaldi, *Finite tangent-circle structures*, Research and Lecture Notes in Mathematics, Combinatorics '88, Mediterranean Press **2** (1988), 349–357.

[15] G. Rinaldi, *Key Distribution Patterns using tangent circle structures*, Designs, Codes and Cryptography, **31** (2004), 289–300.

[16] D.R. Stinson, *On some methods for unconditionally secure key distribution and broadcast encryption*, Designs Codes and Cryptography **12** (1997), 215–243.

[17] D. Welsh, *Codes and Cryptography*, Oxford University Press (1988).

(Received 13 May 2003)