Problems related to combinatorial configurations with applications to P2P-user private information retrieval

Maria Bras-Amorós, Klara Stokes, Marcus Greferath

***Abstract*— We explain the applications that combinatorial configurations have to peer-to-peer user-private information retrieval and we analyze some problems that arise from these applications. In particular we deal with the existence of combinatorial configurations, the characterization of optimal configurations for peer-to-peer user-private information retrieval and the existence of configurations preventing collusion attacks of dishonest users.**

I. Introduction

In the previous years some effort has been done for finding systems guaranteeing private information retrieval (PIR) in front of a data base or a search engine [2]. The aim is that the server owning the information to be retrieved should not learn what the queries are. A major problem is the need for the cooperation of the server, which in most of the scenarios is not likely to occur.

Instead of hiding the queries we can try to hide the profile of the users. This is what we call user-private information retrieval (UPIR). One can define UPIR systems that do not need the cooperation of the server by means of a peer-to-peer community [5], [6], [16]. Indeed, a peer as a user can submit queries on behalf of other peers and get the answers to her/his own queries through other peers. In [5], [6] users are distributed among different private communication spaces using combinatorial configurations [10] (also called (r, k)-partial linear spaces). This implies that all users share the same number of communication spaces, each of these communication space is shared by the same number of users and, most important, no two users share more than one communication space.

In this contribution we will evaluate three problems related to P2P-UPIR and we will give some solutions. In Section II we deal with the first problem that one has when trying to use the protocol in [5], [6]. It consists not only of being able to find combinatorial configurations but also to see whether these objects can exist for large communities of users. In Section III we will deal with the problem of characterizing what are the optimal configurations for P2P-UPIR as for guaranteeing maximum privacy and minimum storage. Finally in Section IV we study the existence of configurations that prevent from collusion attacks.

II. On the existence of combinatorial configurations

In the literature a combinatorial configuration [10] (or a partial linear space [3]) is defined as a particular case of a so-called incidence structure. Here, for simplicity, we chose to define it as a particular case of bipartite graph. Since incidence structures and bipartite graphs are essentially the same, our choice to use bipartite graphs does not introduce any ambiguity. We define a (v, b, r, k)-combinatorial configuration as a connected bipartite graph with v vertices on one side, each of them of degree r, and b vertices on the other side, each of them of degree k, and with no cycle of length 4.

There are many results on the existence of combinatorial configurations. For instance in Gropp's papers [7], [8], [9], [10] and in Grünbaum's book [11]. Gropp states in his references that the next two conditions are necessary for the existence of a (v, b, r, k)-configuration:

P1 $vr = bk$
P2 $v \geq r(k-1)+1$

In particular, for $k = 3$ he proves that P1 and P2 are also sufficient. The next theorem by Gropp guarantees the existence of large configurations and, in fact, the existence of any configuration satisfying the necessary conditions with *sufficiently large* v (and so b). Its limitation is the restriction on the choice of the parameters r, k.

Theorem 1 (Gropp)**.** *For given k and r with $r = tk$ there is a v_0 depending on k, t such that there is a (v, b, r, k)-configuration for all $v \geq v_0$ satisfying P1 and P2.*

In this section we will generalize this result by showing that for any fixed $k \geq 2$ and for *any* fixed $r \geq 2$, the set of tuples (v, b) for which a (v, b, r, k)-combinatorial configuration exists is in bijection with a numerical semigroup. This implies that, for a fixed number k of users per communication space and a fixed number r of communication spaces per user, there exists a community size v_0 such that there will exist configurations with parameters k, r for any community size v larger than v_0, provided that k divides vr. The proof is based on [1] and is constructive.

A. The submonoid of (r, k)-configurable tuples

Definition 1. *We say that the tuple (v, b, r, k) is configurable if a (v, b, r, k) configuration exists.*

It is immediate to prove that if (v, b, r, k) is configurable then $vr = bk$ and consequently there exists d such that $v = d\frac{k}{\gcd(r,k)}$ and $b = d\frac{r}{\gcd(r,k)}$. So, to each configurable tuple (v, b, r, k) we can assign an integer d and two different

This work was partly supported by the Spanish Government through projects TIN2009-11689 "RIPUP" and CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia under grant 2009 SGR 1135.

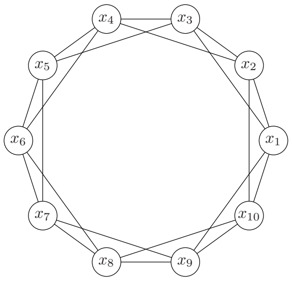

Fig. 1. Construction of a connected 4-regular graph with 10 vertices

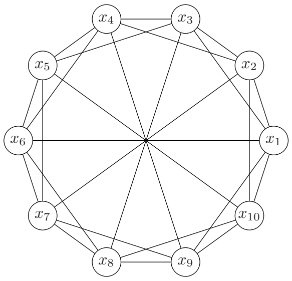

Fig. 2. Construction of a connected 5-regular graph with 10 vertices

configurable tuples (v, b, r, k) will have different integers d. Let us call $D_{r,k}$ the set of all possible integers d corresponding to configurable tuples (v, b, r, k). That is,

$$D_{r,k} = \{d \in \mathbb{N}_0 : (d\frac{k}{\gcd(r,k)}, d\frac{r}{\gcd(r,k)}, r, k) \text{ is configurable}\}.$$

Our aim is to study $D_{r,k}$. We will consider the empty graph to be also a configuration and consequently $0 \in D_{r,k}$ for all pair r, k. Obviously $D_{r,k} = D_{k,r}$ and $D_{1,k} = \{0, k\}$. We will prove that if $r, k > 1$ then $D_{r,k}$ is a numerical semigroup, that is, a subset of $\mathbb{N}_0$ containing 0, closed under addition and with a finite complement in $\mathbb{N}_0$. A general reference on numerical semigroups is [12]. If $a_1, \dots, a_l$ are coprime then the set $\{n_1a_1 + \dots + n_la_l : n_1, \dots, n_l \in \mathbb{N}_0\}$ is a numerical semigroup and it is called the semigroup generated by $a_1, \dots, a_n$ and denoted by $\langle a_1, \dots, a_l\rangle$.

In the next section we will give a complete description of $D_{2,k}$ and in the following one we will study the case $r \geq 3$.

B. The case $r = 2$

There is a natural bijection between $(v, b, 2, k)$-configurations and k-regular connected graphs with b vertices and v edges. Two vertices in the graph share an edge if and only if the corresponding nodes in the configuration share a neighbor and viceversa.

Lemma 1. *Let k be an even positive integer. A connected k-regular graph with b vertices exists if and only if $b \geq k+1$.*

Proof: By definition, any k-regular graph must have a number of vertices at least $k + 1$.

Conversely, suppose $b \geq k + 1$. Consider a set of vertices $x_1, \dots, x_b$. Put an edge between x_i and x_j, with $i \leq j$, if $j - i \leq k/2$ or $i + b - j \leq k/2$. This gives a connected k-regular graph with b vertices.

The construction in this last proof is illustrated in Figure 1.

Corollary 1. *If k is an even positive integer then*

$$D_{2,k} = \langle k + 1, k + 2, \dots, 2k + 1\rangle.$$

Lemma 2. *Let k be an odd positive integer. A connected k-regular graph with b vertices exists if and only if b is even and $b \geq k + 1$.*

Proof: By definition, any k-regular graph must have a number of vertices at least $k + 1$. Now, since the number of edges is $kb/2$ this means that kb must be even and since k is odd b must be even.

Conversely, suppose b is even and $b \geq k + 1$. Consider a set of vertices $x_1, \dots, x_b$. Put an edge between x_i and x_j, with $i \leq j$, if $j - i \leq (k - 1)/2$ or $i + b - j \leq (k - 1)/2$. Put also edges between x_i and $x_{i+b/2}$ for i from 1 to $b/2$. This gives a connected k-regular graph with b vertices.

The construction in this last proof is illutrated in Figure 2.

Corollary 2. *If k is an odd positive integer then*

$$D_{2,k} = \left\langle \frac{k+1}{2}, \frac{k+1}{2} + 1, \frac{k+1}{2} + 2, \dots, k \right\rangle.$$

C. The case $r \geq 3$, $k \geq 3$

1) The set $D_{r,k}$ is non-trivial:
We need the next result by Sachs [13].

Lemma 3. *For any integer $n \geq 3$ and any $\gamma \geq 2$ there exists an n-regular graph with girth at least γ.*

Now we are ready to prove that $D_{r,k}$ is non-trivial.

Lemma 4. *For any pair of integers r, k, there exists at least one non-zero integer in $D_{r,k}$ for all r, k.*

Proof: The cases in which $r \leq 2$ or $k \leq 2$ have been proved in the previous sections. So, we can assume that $r \geq 3$ and $k \geq 3$. Consider the complete bipartite graph $K_{r,k}$. From basic graph theory we know that we can take a subset of $r + k - 1$ edges in $K_{r,k}$ such that they connect all $r + k$ vertices and no cycle is formed (i.e., a generating tree). Let A be the set of the $rk - r - k + 1$ remaining edges of $K_{r,k}$.

Let $n = rk - r - k + 1$ be the number of edges in A. Notice that since r and k are at least 3 then $n \geq 3$. Consider an n-regular graph G with girth at least 5 as in Lemma 3 and consider as many copies of $K_{r,k}$ as vertices in G. Associate each copy of $K_{r,k}$ to a different vertex in G. For each edge e in G, take the copies of the graphs $K_{r,k}$ corresponding to the ends of e and swap one edge xy in A in the first copy and one edge $x'y'$ in A in the second copy for xy' and $x'y$ (here we abused notation using the same letter A for different copies of it). This can be done in a way such that every time we take one edge in A corresponding to a given copy of $K_{r,k}$, the edge is different.

It is easy to check that we obtain a non-trivial (r, k)-biregular bipartite graph with girth at least 5.

2) The set $D_{r,k}$ is a numerical semigroup:

Lemma 5. *Suppose we have a (v,b,r,k)-configuration with $r,k \geq 2$. There exist three edges in the configuration such that the six ends are all different.*

Proof: Since no cycle of length 4 exists and $r,k \geq 2$, there exists a path with four edges with the five ends being different. Three of these ends will be on one partition of the graph while the other two will be in the other partition. Take the vertex at the end of the path. It must be one of the three in the same partition. Since its degree is at least 2, then it will have one neighbor not in the path. So, by adding the edge from the end of the path to this additional vertex, we obtain a new path with 5 edges with all its vertices being different. By taking the first, third, and fifth edges of this new path we obtain the result.

This lemma tells us that the vertices $\{x_1,\dots,x_v\}$, $\{y_1,\dots,y_b\}$ in a (v,b,r,k)-configuration with $r \geq 3$ can be arranged in a way such that the edges x_1y_1, x_2y_2 and x_vy_b belong to the configuration.

Suppose we have a (v,b,r,k)-configuration with vertices $\{x_1,\dots,x_v\}$, $\{y_1,\dots,y_b\}$ and a (v',b',r,k)-configuration with vertices $\{x'_1,\dots,x'_v\}$, $\{y'_1,\dots,y'_b\}$. Consider the graph with vertices $\{x_1,\dots,x_v\} \cup \{x'_1,\dots,x'_v\}$, $\{y_1,\dots,y_b\} \cup \{y'_1,\dots,y'_b\}$ and all the edges in the original configurations. Swap the edges x_vy_b and $x'_1y'_1$ for $x_vy'_1$ and x'_1y_b. This gives a $(v+v',b+b',r,k)$ configuration [6]. An example of this construction is illustrated in Figure 3. This construction proves the next lemma.

Lemma 6. *If (v,b,r,k) and (v',b',r,k) are configurable tuples, so is $(v+v',b+b',r,k)$.*

Lemma 7. *$D_{r,k}$ satisfies*

- $0 \in D_{r,k}$
- *If $d,d' \in D_{r,k}$ then $d+d' \in D_{r,k}$.*

Proof: It is obvious that $0 \in D_{r,k}$ and, by Lemma 6, if $d,d' \in D_{r,k}$ then $d+d' \in D_{r,k}$.

In order to have a numerical semigroup it remains to see that the number of elements in $\mathbb{N}_0 \setminus D_{r,k}$ is finite. This will be proved in the next theorem. In the proof of the theorem it is used that two coprime integers generate a numerical semigroup and so, if a subset containing 0 and closed under addition contains two coprime integers then it is a numerical semigroup.

Theorem 2. *$D_{r,k}$ is a numerical semigroup.*

Proof: Because of the results in the previous sections we can assume that r and g are at least 3.

By Lemma 4 and since $D_{r,k} \subseteq \mathbb{N}$, there is a minimal non-zero element m in $D_{r,k}$. Let us call $v = mk/\gcd(r,k)$ and $b = mr/\gcd(r,k)$. Select a (v,b,r,k) configuration. Take $s = rk/\gcd(r,k)$ copies of this configuration. Let us call the vertices of the ith copy $x_1^{(i)},\dots,x_v^{(i)}$, $y_1^{(i)},\dots,y_b^{(i)}$. By Lemma 5 we can assume that $x_1^{(i)}y_1^{(i)}$, $x_2^{(i)}y_2^{(i)}$ and $x_v^{(i)}y_b^{(i)}$ belong to the ith copy. Consider $k/\gcd(r,k)$ further vertices $x'_1,\dots,x'_{k/\gcd(r,k)}$ and $r/\gcd(r,k)$ further vertices $y'_1,\dots,y'_{r/\gcd(r,k)}$. For all $i < s$ swap the edges $x_v^{(i)}y_b^{(i)}$ and $x_1^{(i+1)}y_1^{(i+1)}$ for $x_v^{(i)}y_1^{(i+1)}$ and $x_1^{(i+1)}y_b^{(i)}$. Remove the edges $x_2^{(i)}y_2^{(i)}$ for all $i \leq s$. Add the edges

$$x'_1y_2^{(1)}, x'_1y_2^{(2)}, \dots, x'_1y_2^{(r)},$$
$$x'_2y_2^{(r+1)}, x'_2y_2^{(r+2)}, \dots, x'_2y_2^{(2r)},$$
$$\vdots$$
$$x'_{k/\gcd(r,k)}y_2^{(s-r+1)}, \dots, x'_{k/\gcd(r,k)}y_2^{(s)}$$

and

$$x_2^{(1)}y'_1, x_2^{(2)}y'_1, \dots, x_2^{(k)}y'_1,$$
$$x_2^{(k+1)}y'_2, x_2^{(k+2)}y'_2, \dots, x_2^{(2k)}y'_2,$$
$$\vdots$$
$$x_2^{(s-k+1)}y'_{r/\gcd(r,k)}, \dots, x_2^{(s)}y'_{r/\gcd(r,k)}.$$

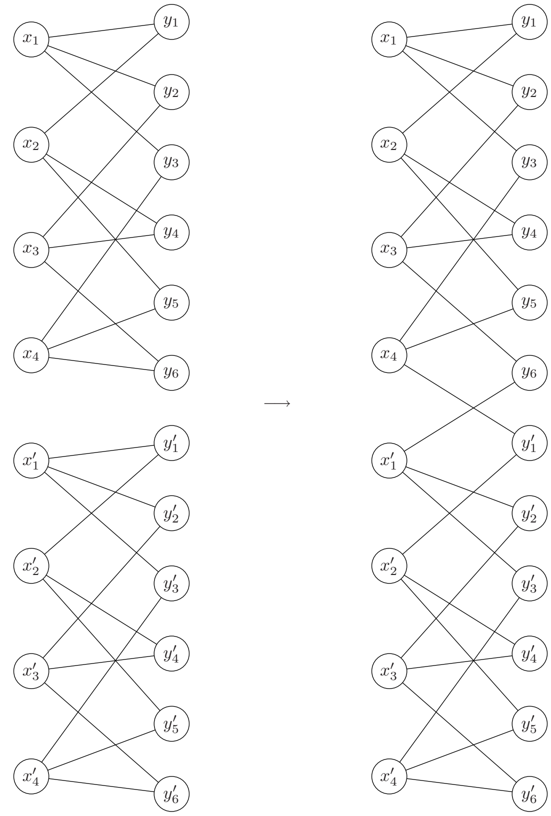

Fig. 3. Construction of a $(v+v',b+b',r,k)$ configuration from a (v,b,r,k) configuration and a (v',b',r,k) configuration.

This construction is illustrated in Figure 4. It is easy to check that this is a new configuration with parameters $(sv + k/\gcd(r,k), sb + r/\gcd(r,k), r, k) = (smk/\gcd(r,k) + k/\gcd(r,k), smr/\gcd(r,k) + r/\gcd(r,k), r, k) = ((sm+1)k/\gcd(r,k), (sm+1)r/\gcd(r,k), r, k)$ and so $sm+1 \in D_{r,k}$.

Since m and $sm+1$ are coprime, they generate a numerical semigroup and this semigroup is contained in $D_{r,k}$. So the

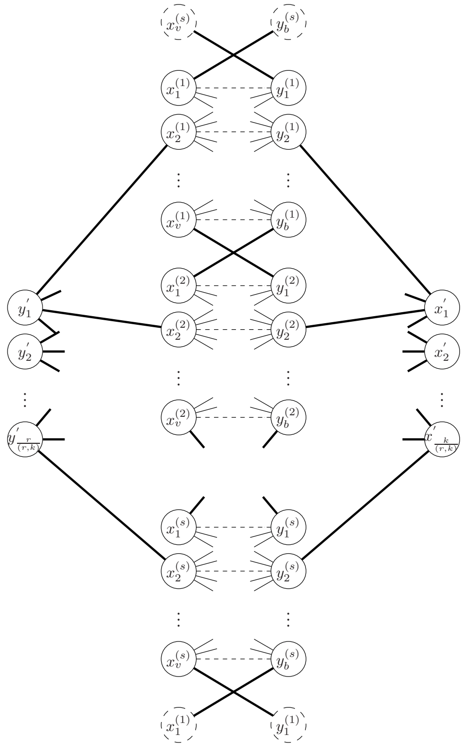

Fig. 4. Construction in the proof of Theorem 2. Dashed edges are replaced by bold faced edges.

complement of $D_{r,k}$ in $\mathbb{N}_0$ is finite and $D_{r,k}$ is a numerical semigroup.

As a consequence of the fact that the necessary conditions P1, P2 are also sufficient for $k = 3$ it is easy to deduce that $D_{r,k} = \{0\} \cup (\frac{2r+1}{3} \gcd(3, r) + \mathbb{N}_0)$. The computation of examples for $r, k > 3$ is computationally very hard.

The main conclusion of this section is that for fixed r and k there exist configurations for all parameters b, v large enough provided that $vr = bk$. In [1] there are some bounds for the minimum values b_0, v_0 such that for all $b \geq b_0$, $v \geq v_0$ satisfying $vr = bk$, a (v, b, r, k)-configuration exists.

Another important fact is that our proofs are all constructive and so we can derive algorithms for constructing large configurations.

III. The optimal configurations for P2P-UPIR are the finite projective planes

We will show here that the optimal configurations for P2P-UPIR are exactly the finite projective planes. The proof is based on the proof in [14]. We consider the P2P-UPIR protocol of [5], [6] defined on a combinatorial configuration with v users, b communication spaces, and with k users per communication space and r communication spaces per user.

It is proved in [5], [6] that in the P2P UPIR system, the privacy of the users against the database is an increasing function of $r(k-1)$. But by the necessary condition P2, we have that $r(k-1) \leq v-1$. Hence, the optimal configurations for the P2P UPIR, considering the privacy against the database, are those for which

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

These configurations exist, as is shown in the following example with $v = 9$, $b = 12$, $r = 4$ and $k = 3$, where the adjacency list of the users and the communication spaces are given.

u_1 :	c_1	c_2	c_3	c_4
u_2 :	c_1	c_5	c_6	c_7
u_3 :	c_1	c_8	c_9	c_{10}
u_4 :	c_2	c_5	c_8	c_{11}
u_5 :	c_2	c_6	c_9	c_{12}
u_6 :	c_3	c_5	c_{10}	c_{12}
u_7 :	c_3	c_7	c_9	c_{11}
u_8 :	c_4	c_6	c_{10}	c_{11}
u_9 :	c_4	c_7	c_8	c_{12}

c_1 :	u_1	u_2	u_3
c_2 :	u_1	u_4	u_5
c_3 :	u_1	u_6	u_7
c_4 :	u_1	u_8	u_9
c_5 :	u_2	u_4	u_6
c_6 :	u_2	u_5	u_8
c_7 :	u_2	u_7	u_9
c_8 :	u_3	u_4	u_9
c_9 :	u_3	u_5	u_7
c_{10} :	u_3	u_6	u_8
c_{11} :	u_4	u_7	u_8
c_{12} :	u_5	u_6	u_9

In the following lemma we see what relation r and k should keep for these configurations.

Lemma 8. *Given a configuration with $r(k-1) = v-1$, we always have $k \leq r$.*

Proof: Suppose as before that the user u_1 is assigned the communication spaces $c_1, \ldots, c_r$. From the condition $r(k-1) = v-1$ we get that $u_2, \ldots, u_v$ are assigned to one and only one of the communication spaces $c_1, \ldots, c_r$. We also suppose, without loss of generality, that u_2 is assigned the communication spaces c_1 and c_j with $j > r$. Then each of the other $k-1$ users assigned to the space c_j, should be assigned to another space between c_2 and c_r. Therefore $k-1 \leq r-1$ and the result follows.

In our scenario, it is preferable if the number of memory sectors, as well as the number of cryptographic keys is small, that is if b is small. But $b = v\frac{r}{k}$, so we are interested in the configurations for which

$$r = k. \tag{2}$$

In this case we also have that $v = b$ and therefore we are dealing with symmetric configurations. We put $n = v = b$ and $d = r = k$. From the condition (1) we deduce that $n = d^2 - d + 1$ and we also have that every pair of users share one and only one communication space while every pair of communication spaces is assigned simultaneously to one and only one user. In the area of finite geometry these configurations are called finite projective planes [15]. The order q of the finite projective plane corresponds to the value of $d-1$. Hence the number of users (and memory sectors) in the configuration, i.e. the number of points (and lines) in the finite projective plane is $n = d^2 - d + 1 = q^2 + q + 1$.

We conclude that the optimal configurations for the peer to peer user private information retrieval are, indeed, the finite projective planes. It is known that finite projective planes of order q exist whenever q is a power of a prime number, but when q is an integer in general the existence is not guaranteed. Actually there is not a single known example of a finite projective plane where q is not a power of a prime. In [15] it is specified that the existence of finite projective planes of arbitrary orders is one of the most difficult questions within finite geometry.

IV. Triangle-free configurations for collusion-free P2P-UPIR

One problem that the UPIR system could have is that two dishonest users connected to an honest user through two different communication spaces, could communicate themselves through a third communication space and infer some joint information. This can be avoided by simply avoiding circuits of length 6 in the bipartite graph representing the combinatorial configuration. The combinatorial configurations with girth larger than 6 are the so-called triangle-free configurations or $(0,1)$-geometries [3], [4], [15].

Definition 2. *We say that the tuple (v,b,r,k) is triangle-free configurable if a (v,b,r,k) triangle-free configuration exists.*

We also define

$$D^{\triangle}_{r,k} = \{d \in \mathbb{N}_0 : (d\tfrac{k}{\gcd(r,k)}, d\tfrac{r}{\gcd(r,k)}, r, k) \text{ is triangle-free configurable}\}.$$

Using the existence of regular graphs of girth at least 7 and any degree (Lemma 3) we can demonstrate the existence of triangle-free configurations of each given parameters $r \geq 3, k \geq 3$, by a proof paralleling that of Lemma 4. For the particular case $r = 2$, for any $k \geq 2$ the hypercube graph Q_k is k-regular and has girth 4. So, it corresponds to a $(2,k)$-configuration with girth 8. In fact, if $k \geq 3$ then Sachs' result (Lemma 3) already guarantees the existence of k-regular graphs of girth 4.

We can compose triangle-free configurations as we composed general configurations before and deduce that $D^{\triangle}_{r,k}$ is a non-trivial submonoid of the non-negative integers.

For the particular case $r = 2$, $k = 2$, the triangle-free configurations are exactly all cycles with an even number of edges larger than or equal to 8. So, $D^{\triangle}_{2,2} = \langle 4,5,6,7 \rangle$.

Now, in order to provide a version of Theorem 2 for triangle-free configurations, we need to reformulate Lemma 5 as follows.

Lemma 9. *Suppose we have a (v,b,r,k)-triangle-free configuration with $r \geq 3$ or $k \geq 3$. Then there exist three edges x_1y_1, x_2y_2, x_3y_3 in the configuration such that the six ends are all different and such that x_iy_j is not in the configuration if $i \neq j$.*

Proof: We can assume that $r \geq 3$ without loss of generality. Since no cycle of length 6 exists and $r \geq 2, k \geq 2$, there exists a path with six edges starting and ending at different vertices of degree r, and with the seven ends being different. Take the vertex at the end of the path. It will have $r - 1 \geq 2$ neighbors not in the path. From those neighbors not in the path at least one will furthermore be not connected to the first vertex in the path. So, by adding the edge from the end of the path to this additional vertex, we obtain a new path with 7 edges with all its vertices being different and with the first and last vertices not being connected. By taking the first, fourth, and seventh edges of this new path we obtain the result.

Now we can state the main result of this section.

Theorem 3. *$D^{\triangle}_{r,k}$ is a numerical semigroup.*

The proof of this theorem has been ommitted since it is the same proof as for Theorem 2, except that now Lemma 9 plays the role of Lemma 5.

As in Section II the main conclusion of this section is that for fixed r and k there exist triangle-free configurations for all parameters b, v large enough provided that $vr = bk$. Also, since our proofs are all constructive, we can derive algorithms for constructing large triangle-free configurations. These configurations have the nice property that they prevent from collusion attacks.

References

[1] M. Bras-Amorós and K. Stokes. On the existence of combinatorial configurations. arXiv:0907.4230v2, 2009.

[2] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. *Journal of the ACM*, 45:965–981, 1998.

[3] F. De Clerck, J. A. Thas, and H. Van Maldeghem. Generalized polygons and semipartial geometries, 1996. EIDMA minicourse.

[4] F. De Clerck and H. Van Maldeghem. On linear representations of (α, β)-geometries. *Eur. J. Comb.*, 15(1):3–11, 1994.

[5] J. Domingo-Ferrer and M. Bras-Amorós. Peer-to-peer private information retrieval. In J. Domingo-Ferrer and Y. Saygin, editors, *Privacy in Statistical Databases*, volume 5262 of *Lecture Notes in Computer Science*, pages 315–323. Springer, 2008.

[6] J. Domingo-Ferrer, M. Bras-Amorós, Q. Wu, and J. Manjón. User-private information retrieval based on a peer-to-peer community. *Data Knowl. Eng.*, 68(11):1237–1252, 2009.

[7] Harald Gropp. Non-symmetric configurations with deficiencies 1 and 2. *Annals of Discrete Mathematics*, 52:227–239, 1992.

[8] Harald Gropp. Nonsymmetric configurations with natural index. *Discrete Math.*, 124(1-3):87–98, 1994. Graphs and combinatorics (Qawra, 1990).

[9] Harald Gropp. Existence and enumeration of configurations. *Bayreuth. Math. Schr.*, (74):123–129, 2005.

[10] Harald Gropp. *Handbook Of Combinatorial Designs (Charles J. Colbourn and Jeffrey H. Dinitz ed.)*, chapter Configurations, pages 353–355. Chapman and Hall/CRC, Kenneth H. Rosen, 2007.

[11] Branko Grünbaum. *Configurations of points and lines*, volume 103 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.

[12] J. C. Rosales and P. A. García-Sánchez. *Numerical semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.

[13] H. Sachs. Regular graphs with given girth and restricted circuits. *J. London Math. Soc.*, 38:423–429, 1963.

[14] K. Stokes and M. Bras-Amorós. Optimal configurations for peer-to-peer user-private information retrieval. *Computers and Mathematics with Applications*, 59(4):1568–1577, 2010.

[15] L. Storme. *Handbook Of Combinatorial Designs (Charles J. Colbourn and Jeffrey H. Dinitz ed.)*, chapter Finite Geometry, pages 702–729. Chapman and Hall/CRC, Kenneth H. Rosen, 2007.

[16] A. Viejo and J. Castellà-Roca. Using social networks to distort users' profiles generated by web search engines. *Computer Networks*, to appear.