Abstract

Using $(0,1)$-geometries for collusion-free P2P-user private information retrieval

Maria Bras-Amorós, Klara Stokes, Marcus Greferath

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 owing the information to be retrieved should not learn what are the queries. A major problem is the need for the cooperation of the server which in most of the scenarions is not likely to occur.

Instead of hiding the queries we can try and 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 [4, 5, 10]. 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 [4, 5] users are distributed among different private communication spaces using combinatorial configurations [6] (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.

It is proved in [8] that the optimal configurations for this scenario are exactly the projective planes. However, this means that the number of users and communication spaces as well as the number of communication spaces per user are very inflexible. Some results have been developed on the existence and construction of combinatorial configurations for any pair (r,k), where r and k are respectively the number of communication spaces per user and the number of users per communication space [1]. In particular it is proved in the latter that (r,k)-configurable tuples have the structure of a numerical semigroup.

One problem that the UPIR system could have is that two dishonest users connected to a 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 $(0,1)$-geometries [3, 9].

Using the existence of regular graphs of girth 8 and any degree [7] we can demonstrate the existence of $(0,1)$-geometries of each given degrees r,k. Composing $(0,1)$-geometries we deduce that the set of tuples representing the parameters of $(0,1)$-geometries of degrees r,k constitute a submonoid of the non-negative integers and with a particular construction, parallel to that in [1], we prove that this set of tuples is in fact a numerical semigroup.

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] 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.

[5] 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.

[6] H. 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.

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

[8] K. Stokes and M. Bras-Amorós. Optimal configurations for peer-to-peer user-private information retrieval. *Computers and Mathematics with Applications*, to appear.

[9] 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.

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