Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 107 (2017) 15 – 20

Procedia Computer Science

International Congress of Information and Communication Technology (ICICT 2017)

Twin Odd-Graceful Trees Towards Information Security

Hongyu Wang[a], Jin Xu[a], Bing Yao[b, *]

[a] School of Electronics Engineering and Computer Science, Peking University, 100871, CHINA
[b] College of Mathematics and Statistics, Northwest Normal University, Lanzhou, 730070, CHINA
* Corresponding authors: yybb918@163.com

Abstract. We design cryptographical graphs for information security by the following principles: (1) be used conveniently in usually; (2) with strong security, that is, it is difficult to be broken; (3) there are enough graphs and labellings for making desired keys and locks. For answering the above problems, we prove the series cryptographical graphs have good properties, and show the guarantee for constructing large scale of cryptographical trees from smaller cryptographical trees. The methods used for constructing the desired cryptographical graphs can be transformed into efficient algorithms.

Keywords: Graph labelling; odd-graceful labelling; information network; tree; algorithm; security.

1. Introduction and definitions

The methods of graph theory have been applied in researching complex networks successfully for a long time ([13, 14, 15]). Three physical scientists Newman (Ref. [20]), Barabási (with his doctor Albert proposed *BA models* in their most popular article *Emergence of scaling in random networks*) and Watts (with Strogatz distributed *Small-world models* in their excellent article *Collective dynamics of 'small-world' networks*) (Ref. [4, 5, 18]) pointed that *pure* and *applied graph theories* can be applied to studying complex networks, and suggested the researching networks toward design and engineering (Ref. [11,13]).

In network information, Alice wants to send a encrypted file to her friends in the following possible ways: this file can be opened by her friends by one unique key; or each of her friends has a private key differing from others' keys to open this file; or Alice makes the copies of the file such that each copy has a lock to be secured, and send them to her friends. The authors (Ref. [9, 10]) are motivated from this story, and consider a general problem: *m keys open n locks with integers m*, *n*≥1. They have designed the so-called *cryptographical graphs* by the thought of "topological structure plus number theory". Doubtless, the research of cryptographical graphs is producing new graph labellings for graph theory itself.

It is not difficult to see that the cryptographical graphs should have the following principles: (1) be used conveniently in usually; (2) with strong security, that is, it is difficult to be broken; (3) there are enough graphs and

Peer-review under responsibility of the scientific committee of the 7th International Congress of Information and Communication Technology
doi:10.1016/j.procs.2017.03.050

labellings for making desired keys and locks. Wang and her coauthors use graphs of orders not large and dozens of graph labellings (Ref. [2]) for realizing their idea. As known, there are 63,042,253 tress of orders ≤24 and 31,455,590,793,615,400,000 graphs of orders ≤15 (Ref. [3]). More and more new graph labellings have been discovered in the field of researching information (Ref. [11, 12, 16, 19]). On the other hands, some graph labellings have been realized on trees and graphs of smaller orders, for example, Deo, Nikoloski and Suraweera (Ref. [1]) have shown the graceful labellings of trees of orders ≤ 29 by associated computer, and Sheppard (Ref. [7]) has shown that a graceful graph having q edges may have $(1\cdot 2\cdot\cdots\cdot q)/2$ different graceful labellings. Clearly, we have more sources materials for making new cryptographical graphs.

One discovered many conjectures on trees (Ref. [2, 17]): GTC: *Each tree is graceful* (Ref. [6]), Elegant GTC, SGTC, OGTC, Elegant odd-GTC, Super edge-magic total labelling tree conjecture, etc. Solving these conjectures are NP-hard, except Xu's computer that differs from Turing-type computer (Ref. [8]).

In Section 2, we prove the series cryptographical graphs have good properties, and provide the guarantee for constructing large size of cryptographical trees from smaller cryptographical trees. The methods used for constructing the desired cryptographical graphs can be transformed into efficient algorithms.

All graphs mentioned are called to be *simple* if they have not multiple edges and loops, and are undirected and finite. We use notation and terminology of graph theory hereafter. A (α,β) -graph G is a simple graph having α vertices and β edges. The first notation $[m, n]$ indicates an integer set $\{m, m+1,\ldots, n\}$ with integers $n>m\geq 0$; the second symbol $[r, s]^o$ stands for an odd-integer set $\{r, r+2,\ldots, s\}$ with odd numbers r, s holding $s-2\geq r\geq 1$; and the third symbol $[a, b]^e$ denotes an even-integer set $\{a, a+2,\ldots,b\}$ with even numbers a, b holding $b-2\geq a\geq 0$. We reformulate several definitions used in this article; the fourth notation $|S|$ is the number of elements of a set S.

Definition 1. [2, 16, 19] If a (α,β)-graph G has a labelling $f: V(G)\rightarrow[0,2\beta-1]$ such that $f(u)\neq f(v)$ for distinct u, $v\in V(G)$, and the edge label set $\{f(uv): uv\in E(G)\}=[1, 2\beta-1]^o$ with $f(uv)=|f(u)-f(v)|$, then f is called an ***odd-graceful labelling*** (og-labelling) of G. Moreover, if G is a bipartite graph with vertex set bipartition (S, L) holding $\max\{f(x): x\in S\}<\min\{f(y): y\in L\}$ ($f_{\max}(S)<f_{\min}(L)$ for short) true, then f is called a ***set-ordered odd-graceful labelling*** (so-og-labelling) of G.

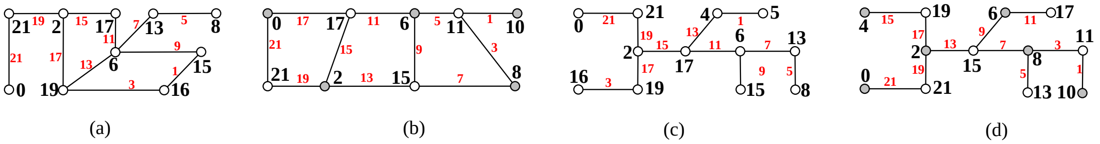

Fig. 1. (a) An og-graph; (b) A so-og-graph; (c) An odd-graceful tree; (d) A so-og-tree.

If a (α,β)-graph G has two subgraphs K and L such that $V(K)\cap V(L)=\{w\}$ and $E(G)=E(K)\cap E(L)$, we denote G as $G=K\diamond L$, called a ***vertex-identified graph*** (vi-graph for short). Moreover, we call G a uniformly vertex-identified graph (uniformly vi-(α,β)-graph) if $\beta=2|E(K)|=2|E(L)|$.

Definition 2. Let a uniformly vi-(p,q)-graph $G=K\diamond L$ have a labelling $f: V(G)\rightarrow[0, q]$ such that (i) $f(x)\neq f(y)$ for any pair of vertices $x,y\in V(G)$; (ii) f is an odd-graceful labelling of K; (iii) the set edge label $f(E(L))=\{f(uv)=|f(u)-f(v)|: uv\in E(L)\}=[1, q-1]^o$. Then G is called a ***twin odd-graceful vi-(p,q)-graph, f a twin odd-graceful labelling*** of G, and K a ***source graph***, and L an ***associated graph*** of K.

Furthermore, in Definition 2, if f is a so-og-labelling of K, and L is a bipartite graph having bipartition (U,V) such that $\max\{f(u): u\in U\}<\min\{f(v): v\in V\}$. Then we call G a ***set-ordered twin odd-graceful*** (so-t-og) ***vi-(p,q)-graph***, f a ***set-ordered twin odd-graceful labelling*** (so-t-og labelling) of G.

Now, we introduce an algorithm, called *KL-construction*, for building large scale of vi-trees.

KL-construction: For $k\in[1, m]$ and r=1,2, each uniformly vi-graph $G_k=G^1_k\diamond G^2_k$ holds $V(G^1_k)\cap V(G^2_k)=\{w_k\}$; and there are vertices $x^r_k, y^r_k\in V(G^r_k)$ such that a graph H_r obtained by joining y^r_j with x^r_{j+1} for $j\in[1,m-1]$ has $V(H_r)=\bigcup^m_{k=1}V(G^r_k)$, $E(H_r)=\bigcup^m_{k=1}E(G^r_k)\cup\{y^r_jx^r_{j+1}: j\in[1, m-1]\}$. Construct a uniformly vi-graph $H=H_1\diamond H_2$ holding $V(H_1)\cap V(H_2)=\{w_m\}$ and $E(H)=E(H_1)\cup E(H_2)$, and call $H=H_1\diamond H_2$ a KL-construction graph. For the purpose of