Research Article

A New Type of Graphical Passwords Based on Odd-Elegant Labelled Graphs

Hongyu Wang 1, Jin Xu 1, Mingyuan Ma 1, and Hongyan Zhang 2

1School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
2School of Management Science and Engineering, Shandong Normal University, Jinan 250014, China

Correspondence should be addressed to Hongyu Wang; why5126@pku.edu.cn

Received 11 January 2018; Accepted 1 March 2018; Published 11 April 2018

Academic Editor: Zheng Yan

Copyright © 2018 Hongyu Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Graphical password (GPW) is one of various passwords used in information communication. The QR code, which is widely used in the current world, is one of GPWs. Topsnut-GPWs are new-type GPWs made by topological structures (also, called graphs) and number theory, but the existing GPWs use pictures/images almost. We design new Topsnut-GPWs by means of a graph labelling, called odd-elegant labelling. The new Topsnut-GPWs will be constructed by Topsnut-GPWs having smaller vertex numbers; in other words, they are compound Topsnut-GPWs such that they are more robust to deciphering attacks. Furthermore, the new Topsnut-GPWs can induce some mathematical problems and conjectures.

1. Introduction and Preliminary

1.1. Researching Background. Graphical passwords (GPWs) have been investigated for over 20 years, and many important results can be found in three surveys [1–3]. GPW schemes have been proposed as a possible alternative to text-based schemes. However, the existing GPWs have (i) no mathematical computation; (ii) more storage space; (iii) no individuality; (iv) geometric positions; (v) slow running speed; (vi) vulnerable to attack; and (vii) no transformation from lower safe level to high security. However, QR code is a successful example of GPW applications in mobile devices by fast, relatively reliable and other functions [4, 5]. GPWs may be accepted by users having mobile devices with touch screen [6, 7].

Wang et al. show an idea of “topological structures plus number theory” for designing new-type GPWs (abbreviated as Topsnut-GPWs, [8–10]). All topological structures used in Topsnut-GPWs can be stored in a computer through ordinary algebraic matrices. And Topsnut-GPWs have no requirement of geometric positions for users and allow users to make their individual passwords rather than learning more rules they do not like and so on.

How to quickly build up a large scale of Topsnut-GPWs from those Topsnut-GPWs having smaller vertex numbers? How to construct a one-key versus more-locks (one-lock versus more-keys) for some Topsnut-GPWs? And how to compute Topsnut-GPWs’ space by the basic computing unit 2? Obviously, we need enough graphs and lots of graph coloring/labellings, and we can turn more things into Topsnut-GPWs. Let $G_p^n$ be the number of graphs having $p$ vertices. From [11], we know

<table>
<thead>
<tr>
<th>$p$</th>
<th>$G_p^n$</th>
<th>bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>1787577725145611700547878190848</td>
<td>100</td>
</tr>
<tr>
<td>19</td>
<td>24637809253125004524383007491432768</td>
<td>114</td>
</tr>
<tr>
<td>20</td>
<td>64549012279579984185656463849072749440</td>
<td>129</td>
</tr>
<tr>
<td>21</td>
<td>322027289980898343350224425755283616097664</td>
<td>145</td>
</tr>
<tr>
<td>22</td>
<td>30708464830941444300637568317187105410586657814272</td>
<td>161</td>
</tr>
<tr>
<td>23</td>
<td>55994693996997208059797638081946217981227634858981632</td>
<td>179</td>
</tr>
<tr>
<td>24</td>
<td>195704906302078447922174862416726256004122075267063365754368</td>
<td>197</td>
</tr>
</tbody>
</table>
by selecting the neighbors of each vertex of these four vertices \(v_1, v_{10}, v_{11}, \) and \(v_{20}\). Clearly, such password \(W\) may have longer unit in a large scale of Topsnut-GPW for meeting the need of high level security.

In this article, we will apply a graph labelling called odd-elegant labelling [13]. And we will define some construction operations under odd-elegant labelling for designing our compound Topsnut-GPWs.

1.2. Preliminary. We use standard notation and terminology of graph theory. Graphs mentioned are loopless, with no multiple edges, undirected, connected, and finite, unless otherwise specified. Others can be found in [14]. Here, we will use a \((p, q)\)-graph \(G\) which is one with \(p\) vertices and \(q\) edges; the symbol \([m, n]\) stands for an integer set \(\{m, m + 1, \ldots, n\}\) for integers \(m\) and \(n\) with \(0 \leq m < n\); \([s, t]\) denoting an odd-set \(\{s, s + 2, \ldots, t\}\), where \(s\) and \(t\) both are odd integers with \(1 \leq s < t\); \([k, \ell]\) represents an even-set \(\{k, k + 2, \ldots, \ell\}\), where \(k\) and \(\ell\) both are even integers with respect to 0 \(\leq k < \ell\).

Definition 1 (see [13]). Suppose that a \((p, q)\)-graph \(G\) admits a mapping \(f: V(G) \to [0, 2q - 1]\) such that \(f(u) \neq f(v)\) for distinct vertices \(u, v \in V(G)\), and the label \(f(\text{uv})\) of every edge \(uv \in E(G)\) is defined as \(f(\text{uv}) = f(u) + f(v) \pmod{2q}\) and the set of all edge labels is equal to \([1, 2q - 1]\). One considers \(f\) to be an odd-elegant labelling and \(G\) to be an odd-elegant.

Definition 2 (see [15]). Suppose that a bipartite graph \(G\) receives a labelling \(f\) such that \(\max\{|f(x)| : x \in X\} < \min\{|f(y)| : y \in Y\}\), where \((X, Y)\) is the bipartition of vertex set \(V(G)\) of \(G\). We call \(f\) a set-ordered labelling (So-labelling for short).

As shown in Figure 1, there are four different examples of Definitions 1 and 2.

Definition 3. Let \(G_j\) be a \((p_j, q_j)\)-graph with \(j = 1, 2\). A graph \(G\) obtained by identifying each vertex \(x_{i,1}\) of \(G_1\) with a vertex \(x_{i,2}\) of \(G_2\) into one vertex \(x_i = x_{i,1} \circ x_{i,2}\) with labellings introduced in [12]. As a fact, Topsnut-GPWs can generate alphanumeric passwords with longer units. As an example, we take a path \(v_1v_{10}v_{11}v_{20}\) in Figure 6(d) to produce an alphanumeric password

\[
W = 1^11816141210201^11011517211110^111^110202011^120^111579320^1
\]  

where \(G_p \simeq 2^{\text{bits}}\) for \(p = 18, 19, \ldots, 24\). It means that adding various graph labellings enables us to design tremendous Topsnut-GPWs with huge topological structures and vast of graph coloring/labellings, since there are over 150 graph

Moreover, the \(m\)-identification graph \(G = \circ_m(G_1, G_2)\) defined in Definition 3 has \(p_1 + p_2 - m\) vertices and \(q_1 + q_2\) edges. One can split each identification-vertex \(x_i = x_{i,1} \circ x_{i,2}\) into two vertices \(x_{i,1}\) and \(x_{i,2}\) (called the splitting-vertices) for \(i \in [1, m]\), such that \(G\) is split into two parts \(G_1\) and \(G_2\). For the purpose of convenience, the above procedure of producing an \(m\)-identification graph \(G = \circ_m(G_1, G_2)\) is called an \(m\)-identification operation; conversely, the procedure of splitting \(G = \circ_m(G_1, G_2)\) into two parts \(G_1\) and \(G_2\) is named as the \(m\)-splitting operation.

Definition 4. Let \(G\) be a connected \((p, q)\)-graph with \(i = 1, 2,\) and let \(p = p_1 + p_2 - 2\). If the 2-identification \((p, q)\)-graph \(G = \circ_2(G_1, G_2)\) has a mapping \(f: V(G) \to [0, q - 1]\) holding the following: (i) \(f(x) \neq f(y)\) for each pair of vertices \(x, y \in V(G)\), (ii) \(f\) is an odd-elegant labelling of \(G_i\) with \(i = 1, 2\), and (iii) \(|f(V(G_1)) \cap f(V(G_2))| = 2\) and \(f(V(G_1)) \cup f(V(G_2)) \subseteq [0, q - 1]\), then one calls \(G\) a twin odd-elegant graph (a TOE-graph), \(f\) a TOE-labelling, \(G_1\) a TOE-source graph, \(G_2\) a TOE-associated graph, and \((G_1, G_2)\) a TOE-matching pair.

We illustrate Definition 4 with Figure 2. In other words, a twin odd-elegant graph \(G = \circ_2(G_1, G_2)\) with its TOE-source graph \(G_1\) and TOE-associated graph \(G_2\), where \((G_1, G_2)\) is a TOE-matching pair.

Furthermore, if each \(G_i\) with \(i = 1, 2\) is a connected graph in Definition 4, and the TOE-source \(G_1\) is a bipartite connected graph having its own bipartition \((X_1, Y_1)\) and a labelling \(f\) satisfying Definition 2, we call the 2-identification graph \(G = \circ_2(G_1, G_2)\) a set-ordered twin odd-elegant graph (So-TOE-graph) and \(f\) a set-ordered twin odd-elegant labelling (So-TOE-labelling). Notice that the source graph \(G_1\) is a set-ordered odd-elegant graph by Definitions 1 and 2. In vivid speaking, a source graph and its associated graph

![Figure 1](image-url)
defined in Definition 4 can be called a TOE-lock-model and
a TOE-key-model ([10]), respectively.

1.3. Techniques for Constructing 2-Identification Graphs. The
following three operations, CA-operation, edge-series operation,
and base-pasted operation, will be used in this article.

(O-1) CA-Operation. Suppose each graph \( G_k \) has an odd-
elegant labelling \( f_k \) and \( V(G_k) = \{ x_i^k : i = 1, 2, \ldots, |V(G_k)| \} \)
with \( k \in [1, m] \). Clearly, for \( a \neq b \) with \( a, b \in [1, m] \),
there are vertices \( x_i^a \in V(G_a) \) and \( x_j^b \in V(G_b) \) such that
\( f_a(x_i^a) = f_b(x_j^b) \). For example, some \( G_k \) has a vertex \( x_k^i \) such
that the label \( f_k(x_k^i) = 0 \) with \( k \in [1, m] \). We can combine
those vertices that have the same labels into one vertex, which
gives us a new graph, denoted by \( G = \bigcup_{k=1}^{m} (G_1, G_2, \ldots, G_m) \).
This process is called a CA-operation on \( G_1, G_2, \ldots, G_m \).

(O-2) Edge-Series Operation. Given two groups of disjoint
trees \( G'_1, G'_2, \ldots, G'_r \) with \( r = 1, 2 \) there are vertices \( x_i^r, y_j^r \in V(G'_r) \) with \( k \in [1, m] \). Joining the vertex \( y_j^r \) with the vertex
\( x_j^r \) by an edge for \( j \in [1, m-1] \) produces a tree \( H_r \) (denoted
by \( H_r = e_{j=1}^{m} G'_r \)) with \( r = 1, 2 \); next we let vertex \( u_i \in V(H_r) \)
coincide with one vertex \( v_j \in V(H_r) \) into one vertex
\( a_k = u_i \odot v_j \) with \( s = 1, 2 \). The resulting graph \( \bigcup_{r=1}^{2} \langle H_1, H_2 \rangle \) is
just a 2-identification graph.

(O-3) Base-Pasted Operation. Given two disjoint trees \( T_r \)
(called base-trees) having vertices \( x_i^r, x_2^r, \ldots, x_m^r \) and two
groups of disjoint trees \( G'_1, G'_2, \ldots, G'_m \) with \( r = 1, 2 \), we let a vertex \( u_i \in V(G'_r) \)
coincide with the vertex \( x_i^r \in V(T_r) \) into one vertex \( u_i \odot x_i^r \) for \( k \in [1, m] \) such that the resulting tree \( F_r \) (i.e., \( F_r = T_r \bigcup_{r=1}^{m} G'_r \)) has \( V(F_r) = \bigcup_{r=1}^{m} V(G'_r) \),
\( E(F_r) = \bigcup_{r=1}^{m} E(G'_r) \cup E(T_r) \) for \( r = 1, 2 \). We overlap one
vertex \( w_i^r \in V(F_r) \) with one vertex \( z_i^r \in V(F_r) \) into one vertex
\( b_r = u_i \odot z_i^r \) with \( s = 1,2 \) to build up a 2-identification
graph \( F = \bigcup_{r=1}^{2} \langle F_1, F_2 \rangle \) holding \( V(F_1) \cap V(F_2) = \{ a_1, a_2 \} \) and
\( E(F) = E(F_1) \cup E(F_2) \).

In the following, we give the diagrams with \( m = 2 \) for
degree-series operation and base-pasted operation, shown in
Figures 3 and 4, respectively.

2. Main Results and Their Proofs

Lemma 5. Each star \( K_{1,n} \) is a TOE-source tree of a So-TOE-
tree.

Proof of Lemma 5 is shown in Figure 5. It describes the
construction process of the So-TOE-tree \( \bigcup \langle K_{1,n}, K_{1,n} \rangle \) by
any TOE-source tree \( K_{1,n} \).

Theorem 6. Every set-ordered odd-elegant graph being not a
star is a TOE-source graph of at least two SO-TOE graphs.

Proof. Suppose that \( (p, q) \)-graph \( G_1 \) having vertex biparti-
tion is \( (X,Y) \), where \( X = \{ x_i : i \in [1,s] \}, Y = \{ y_i : j \in [1,t] \}, s + t = p \), and \( \min[s,t] \geq 2 \). By the hypothesis of
the theorem, \( G_1 \) has a set-ordered odd-elegant labelling \( f_1 \)
defined by \( f_1(x_i) + 2 \leq f_1(x_{i+1}), i \in [1,s-1] \); \( f_1(y_i) = f_1(x_i) + 1, f_1(y_i) + 2 \leq f_1(y_{i+1}), i \in [1,t-1] \); \( f_1(y_i) \leq 2q-1 \). Hence,
\( f_1(E(G_1)) = \{ f_1(xy) = f_1(x) + f_1(y) \mod 2q \} : xy \in E(G_1) = \{ 1, 2q-1 \} \). It is not difficult to observe
that \( f_1(V(G_1)) \subset \{ 0, 2, \ldots, f_1(x_1), f_1(y_1), \ldots, 2q-1 \} \); that is,
\( f_1(X)/2 \subset \mathbb{N} \) and \( (f_1(Y)+1)/2 \subset \mathbb{N} \).

Case I. We construct a labelling \( f_2 \) of a new tree \( T_2 \) having \( q+1 \) vertices by the labelling \( f_1 \) such that \( f_2(V(T_2)) = \{ f_1(x_i) + \}
1\} \} \cup \{ f_1(y_1) - 1, 2q-2 \} \}, such that \( f_2(E(T_2)) = \{ f_2(uv) = f_2(u) + f_2(v) \mod 2q \} : uv \in E(T_2) \} = \{ 1, 2q-1 \} \}, where
\( f_2(u) \neq f_2(v) \) for \( u, v \in V(T_2) \). This tree \( T_2 \) can be built up
in the following way: a bipartition \( (U_1, V_1) \) with \( U_1 = \{ u_i :
According to Definition 4, Case 2 with $\nu_i \in \{1, s\}$ and $\nu_j \in \left\{1, t\right\}$, where $s_1 + t_1 = q + 1$, such that $f_2(u_i) = 2i - 1, i \in \left\{1, s\right\}$; $f_2(v_j) = 2(s_1 - 2 + j), j \in \left\{1, t\right\}$. Any edge $u_iv_j \in E(T_2)$ satisfies $f_2(u_iv_j) = f_2(u_i) + f_2(v_j) \pmod{2q}$ with $i \in \left\{1, s\right\}$ and $j \in \left\{1, t\right\}$. We construct the edge set of $T_2$ as $\{(u_i, v_j) : i \in \left\{1, s\right\}, j \in \left\{1, t\right\}\}$ such that the edge labels are $f_2(u_i, v_j) = 2i - 3, f_2(u_i, v_j) = 2j + 2s_1 - 3 \pmod{2q}$ for $i \in \left\{1, s\right\}$ and $j \in \left\{1, t\right\} - 1$. Observe that $f_2(E(T_2)) = \{1, 2q - 1\}^\theta, f_1(y_1) = f_2(v_1), \text{ and } f_1(y_2) = f_2(v_2)$.

Now, we can combine the vertex $y_1$ and $y_2$ of $G_1$ with the vertex $u_1$ and $v_1$ of $T_2$ into one (the identified vertex) $\omega_1$ and $\omega_2$, respectively, so we obtain the desired graph $G = \bigodot G_1, T_2)$. And $G$ has a labelling $f$ defined as $f(x_i) = f_G(x_i), i \in \left\{1, s\right\}$; $f(y_i) = f(y_i), i \in \left\{1, t\right\}; f(u_i) = f_G(u_i), k \in \left\{1, s\right\} - 1, f(v_i) = f(v_i), l \in \left\{1, t\right\} - 1, f(w_i) = f(w_i)$, and $f(w_i) = f_2(v_i)$. Clearly, any pair of two vertices of $G$ are assigned different numbers. According to Definition 4, $G$ is an SO-ToE-graph having the source graph $G_1$. An example that illustrate Case 1 of Theorem 6 are shown by Figures 6(a), 6(b), and 6(d).

Case 2. Similarly to Case 1, we can get the following results: let $f_2(V(T_2')) = \{1, f_1(x_i) - 1\}^\theta \cup \{f_1(y_j) - 1, 2q - 2\} \cup \{0\}, f_2(E(T_2')) = \{1, 2q - 1\}^\theta$, and furthermore $f_2(u) \neq f_2(v)$ for $u, v \in V(T_2')$. This tree $T_2'$ can be built up in the following way: a bipartition $(U_2', V_2')$ with $U_2' = \{u_i : i \in \left\{1, s\right\} - 1\}$ and $V_2' = \{v_j : j \in \left\{1, t\right\} - 1\}$, such that $f_2(u_i) = 2i - 1, i \in \left\{1, s\right\} - 1; f_2(v_j) = 2(s_1 - 2 + j), j \in \left\{1, t\right\}, f_2(v_{j+1}) = 0$. Any edge $u_iv_j \in E(T_2')$ satisfies $f_2(u_iv_j) = f_2(u_i) + f_2(v_j) \pmod{2q}$ with $i \in \left\{1, s\right\} - 1$ and $j \in \left\{1, t\right\} + 1$. We construct the edge set of $T_2'$ as $\{(u_i, v_j) : i \in \left\{2, s\right\}, j \in \left\{1, t\right\}\}$ such that the edge labels are $f_2(u_i, v_j) = 2i - 1, i \in \left\{1, s\right\} - 1$, and $f_2(u_i, v_j) = 2(s_1 - 2 + j) - 3, j \in \left\{1, t\right\}$. Observe that $f_2(E(T_2')) = \{1, 2q - 1\}^\theta, f_1(x_i) = f_2(v_{j+1})$, and $f_1(x_i) = f_2(v_{j+1})$.

Now, we can combine the vertex $x_1$ and $x_2$ of $T_2'$ with the vertex $v_1$ and $v_2$ of $T_2$ into one (the identified vertex) $\omega_1$ and $\omega_2$, so we obtain the desired tree $G' = \bigodot (G_1, T_2)$. And $G'$ has a labelling $f$ defined as $f(x_i) = f_G(x_i), i \in \left\{2, s\right\}; f(y_i) = f(y_i), i \in \left\{1, t\right\}; f(u_i) = f_G(u_i), k \in \left\{1, s\right\} - 1, f(v_i) = f(v_i), l \in \left\{1, t\right\}, f(w_i) = f_1(y_3)$, and $f(w_i) = f_2(v_i)$. Clearly, any pair of two vertices of $G'$ are assigned different numbers. According to Definition 4, $G'$ is a SO-ToE-graph having the source graph $G_1$. An example for illustrating Case 2 of Theorem 6 is given by Figures 6(a), 6(c), and 6(e).

\textbf{Theorem 7.} Suppose that $G_k = \bigodot (G_{k-1}, G_k^1)$ is a SO-ToE-graph, where each $G_k^1$ is a source tree for $k \in \left\{1, m\right\}$. Then $G = \bigodot (G_{k-1}, G_k^1)$ obtained by the edge-series operation has a SO-ToE-labelling.

\textit{Proof.} By the hypothesis of the theorem, every $(p_k^1, q_k^2)$-graph $G_k^1$ has a set-ordered odd-source-elegant (SO-ToE) graph $G_k^1$ and an associated $(p_k^2, q_k^1)$-graph $G_k^2$ for $k \in \left\{1, m\right\}$. Let $V(G_k^1) \cap V(G_k^2) = \{u_k, u_k^2\}$; the vertex set of each graph $G_k^i$ can be partitioned into $(X_k^i, Y_k^i)$ with $r = 1, 2$, where $X_k^i = \{x_{i, k} : i \in \left\{1, s_k^i\right\}\}$, $Y_k^i = \{y_{i, k} : j \in \left\{1, t_k^i\right\}\}$, and $s_k^i + t_k^i = p_k^i$ for $k \in \left\{1, m\right\}$ and $r = 1, 2$. By Definition 4, every $G_k$ has a SO-ToE-labelling $\theta_k$ with $k \in \left\{1, m\right\}$ such that $\theta_k(x_{i, k}) \geq r - 1; \theta_k(x_{i, k}) + 2 \leq \theta_k(x_{i+1, k})$ with $i \in \left\{1, s_k^i\right\}$; $\theta_k(y_{i, k}) \geq r - 1; \theta_k(y_{i, k}) + 2 \leq \theta_k(y_{i+1, k})$ for $i \in \left\{1, t_k^i\right\}$; and $\theta_k(y_{i, k}) \leq 2q_k - r$. 

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{image}
\caption{A scheme of the base-pasted operation.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{image}
\caption{An example of illustrating Lemma 5.}
\end{figure}
Therefore, \( \theta_k(E(G'_k)) = \{ \theta_k(xy) = \theta_k(x) + f'_k(y) \mod 2q \mid xy \in E(G'_k) \} = [1, 2q_k - 1]^{2q} \),
where \( \theta_k(x) \neq \theta_k(y) \) for distinct vertices \( x, y \in V(G'_k) \),
which means \( \theta_k(x_{k+1}^{i}) = \theta_k(y_{k+1}^{i}) = \theta_k(w_k) \) and \( \theta_k(x_{k}^{i}) = \theta_k(x_{k+1}^{i}) \).
Clearly, the labels of other vertices of \( G^1_k \cup G^2_k \) differ from each other.

Firstly, we split \( G_k \) into two parts \( G^1_k \) and \( G^2_k \), that is, doing
a 2-splitting operation on every \( G_k \) with \( k \in [1, m] \). Secondly,
our discussion focuses on \( G^1_k \) and \( G^2_k \) with \( k \in [1, m] \). We
construct a graph by joining the vertex \( y_{k+1}^{i} \) with the vertex
\( x_{k+1}^{i} \) by an edge, where \( k \in [1, m - 1] \) and \( r = 1, 2 \),
called \( H_r \). For the purpose of convenience, we set \( S(a,b) = \sum_{i=0}^{b} \theta_i(x_{i}^{a}) + 2, Q(1, r) = 2 \sum_{i=1}^{r} (q_i + 1), Q_m = 2 \sum_{i=0}^{r} (q_i + m - 1) \).
\( S(1, 0) = 0, \) and \( Q(1, 0) = 0 \). For \( r = 1, 2, i \in [1, s_k], \) and \( j \in [1, t_k] \), we define a new labelling \( f \) as follows:

\[
\text{(T-1) } f(x_{k,i}^{j}) = \theta_k(x_{k,i}^{j}) + S(1, k - 1);
\text{(T-2) } f(y_{k,i}^{j}) = \theta_k(y_{k,i}^{j}) + Q(1, k - 1) + S(k + 1, m);
\text{(T-3) } f(x_{k,i}^{j}, y_{k+1,i}^{j}) = f(x_{k,i}^{j}) + f(y_{k,i}^{j}) \mod Q_m;
\text{(T-4) } f(y_{k+1,i}^{j}, x_{k+1,i}^{j}) = f(x_{k+1,i}^{j}) + f(y_{k,i}^{j}) \mod Q_m.
\]

By the labelling forms (T-1) and (T-2) above, we can verify
\( f(x_{k,i}^{j}, y_{k+1,i}^{j}) \in [0, f(x_{m-s}^{j}, m)^{2q}] \) with \( k \in [1, m] \) and
have the following properties: (i) \( f(x_{k,i}^{j}, y_{k+1,i}^{j}) = [1, S(1, k - 1)]^{2q} \); (ii) \( f(y_{k,i}^{j}, y_{k+1,i}^{j}) = [S(1, m) - 1, Q_m - 1]^{2q} \); and (iii) \( f(y_{k+1,i}^{j}, x_{k+1,i}^{j}) = [S(1, m) - 1, Q_m - 1]^{2q} \).
Computing the labelling forms (T-3) and (T-4) enables us to obtain
\( f(E(H_r)) = [1, Q_m - 1]^{2q} \) for \( r = 1, 2 \). Now, we combine the vertex \( x_{m-s}^{j} \) with the vertex \( y_{1,1}^{j} \) into one
vertex and then combine the vertex \( y_{1,1}^{j} \) with the vertex \( x_{m-s}^{j} \)
in to one vertex. (i.e., do the 2-identification operation). Thus
the labelling \( f \) is a So-TOE-labelling of \( G = \odot_2(H_1, H_2) \);
therefore, \( G \) is a So-TOE-graph too.

See Figures 7, 8 and 9 for understanding Theorem 7.

In experiments, for each arrangement \( G_k^1, G_k^2, \ldots, G_k^m \)
of \( G^1_k, G^2_k, \ldots, G^m_k \), there are many possible constructions of \( G = \odot_2(H_1, H_2) \) for holding Theorem 7 (as shown in Figure 9).

**Theorem 8.** Suppose that \( G_k = \odot_2(G_k^1, G_k^2) \) is a So-TOE-

graph, where each \( G_k^i \) is a source graph for \( k \in [1, p] \). Then
\( G = \odot_2(S_1, S_2) \) obtained by the base-pasted operation has a
So-TOE-labelling if two base-trees \( T_1 \) and \( T_2 \) are set-ordered.

**Proof.** By the hypothesis of the theorem, every \( (p_1^k + p_2^k - 2, 2q) \)-graph \( G_k = \odot_2(G_k^1, G_k^2) \) has a set-ordered odd-elegant
source-\((p_1^k, q)\)-graph \( G_k^1 \) and an associated-\((p_2^k, q)\)-graph \( G_k^2 \)
for \( k \in [1, p] \). Let \( G_k^1 \cap G_k^2 = \{ w_k^1, w_k^2 \} \); the vertex set of
each graph \( G_k^i \) can be partitioned into \((X_k^i, Y_k^i)\) with \( r = 1, 2 \),
where \( X_k^i = \{ x_{k,i}^j: i \in [1, s_k], Y_k^i = \{ y_{k,i}^j: j \in [1, t_k] \} \),
therefore \( s_k \leq t_k \), and \( s_k + t_k = p_k \) for \( k \in [1, p] \) and \( r = 1, 2 \).
Every \( G_k \), by Definition 4, has a So-TOE-labelling \( \pi_k \)
with \( k \in [1, p] \), and \( \pi_k \) has the following properties:
\( \pi_k(x_{k,i}^j) = r - 1; \pi_k(x_{k,i}^j) + 2 \leq \pi_k(x_{k,i+1}^j) \) for \( i \in [1, s_k] \); \( \pi_k(x_{m-s}^{j}) = M - 1 + r; \pi_k(y_{k,i}^j) = \pi_k(x_{k+1,i}^j) - (-1)^r = M - 1 + r - (-1)^r ;
\( \pi_k(y_{k,i+1}^j) + 2 \leq \pi_k(y_{k,i+1}^j) \) with \( i \in [1, s_k] \); \( \pi_k(y_{1,1}^j) = 2q - r \); and
\( \pi_k(x_{k+1,i}^j, y_{k+1,i}^j) = \pi_k(x_{k+1,i}^j) + \pi_k(y_{k,i}^j) \mod (2q) \).

Thus, the properties of each So-TOE-labelling \( \pi_k \)
derive from \( \pi_k(E(G_k^i)) = \pi_k(xy) = \pi_k(x) + f'_k(y) \mod (2q); \ xy \in E(G_k^i) \), and also
\begin{align}
\pi_{k}(E(G^{i}_{k}))
= [\pi_{k}(x^i_1) + \pi_{k}(y^i_1), \pi_{k}(x^i_2') + \pi_{k}(y^i_2')] \mod (2q) = [1, 2q - 1]^\circ,
\end{align}

where \( \pi_{k}(x) \neq \pi_{k}(y) \) if \( x \neq y \) and \( x, y \in V(G_{k}) \). In other words, we have \( \pi_{k}(x^i_{k,j}) = \pi_{k}(y^i_{k,j}) = \pi_{k}(u^i_{k}) \) and \( \pi_{k}(y^i_{k,1}) = \pi_{k}(x^i_{k,1}) = \pi_{k}(u^i_{k}) \). The labels of other vertices of \( G^{i}_{k} \cup G^{j}_{k} \) differ from each other.

Let \( V(T_{r}) = \{ z^{1}_{r}, z^{2}_{r}, \ldots, z^{r}_{r} \} \), such that there exists a set-ordered odd-elegant labelling \( f_{T_{r}}^{\text{oe}}(z^{i}_{r}) < f_{T_{r}}^{\text{oe}}(z^{i+1}_{r}) \) with \( i \in [1, p - 1] \), and the bipartition \( (U_{r}, V_{r}) \) of vertex set of \( T_{r} \) satisfies \( |U_{r}| = |V_{r}| \) for \( |U_{r}| = l \) and \( r = 1, 2 \).

Next, we discuss all graphs \( G^{i}_{k} \) with \( k \in [1, p] \) by the parity of positive integer \( p \) in the following two cases.

**Case I.** For considering the case \( p = 2\beta + 1 \) and \( r = 1, 2 \), we define a new labelling \( f \) with \( i \in [1, \hat{s}_{k}] \) and \( j \in [1, \hat{t}_{k}] \) in the following way:

(C-1) \( f(x^{i}_{2k-1}) = \pi_{2k-1}(x^{i}_{2k-1}) + 2(q + 1)(k - 1) \) with \( k \in [1, \beta + 1] \);

(C-2) \( f(y^{i}_{2k}) = \pi_{2k}(y^{i}_{2k}) + 2(q + 1)(\beta + k) - 2(-1)^{r} \) with \( k \in [1, \beta] \);

(C-3) \( f(y^{i}_{2k-1}) = \pi_{2k-1}(y^{i}_{2k-1}) + 2(q + 1)(\beta + k - 1) \) with \( k \in [1, \beta + 1] \);

(C-4) \( f(y^{i}_{2k}) = \pi_{2k}(y^{i}_{2k}) + 2(q + 1)(k - 1) + 2(-1)^{r} \) with \( k \in [1, \beta] \);

(C-5) \( f(x^{i}_{2k-1}, y^{i}_{2k}) = f(y^{i}_{2k}) + f(x^{i}_{2k-1}) \mod 2p(q + 1) - 2 \).

Based upon the labelling forms (C-1)–(C-4), we compute

\[
\bigcup_{k=1}^{\beta+1} f\left(x^{i}_{2k-1}\right) \cup \bigcup_{k=1}^{\beta} f\left(y^{i}_{2k}\right)
= [0, 2(q + 1)\beta + M]^\circ;
\]
\[
\left( \bigcup_{k=1}^{\beta+1} f\left( Y_{2k-1} \right) \right) \cup \left( \bigcup_{k=1}^{\beta} f\left( X_{2k} \right) \right) \\
= \left[ 2(q+1)\beta + M + 1, 2p(q+1) - 3 \right]^o,
\]

where \( A(x) = M + 1 + 2(q+1)(\beta + 2k - x) \) and \( B(y) = M - 3 + 2(q+1)(\beta + 2k - y) \). By the above deduction, we can know that

\[
\bigcup_{k=1}^{p} f(E(G_r^i)) = \left[ 1, 2p(q+1) - 3 \right]^o \setminus F,
\]

where \( F = [M - 1 + 2(q+1)(\beta + 1 + k), M + 1 + 2(q+1)k : k = 0, 1, 2, \ldots, \beta - 1] \). Next, for each vertex \( z_{ki}^r \in V(T_r) \) with \( k \in [1, p] \) and \( r = 1, 2 \), we set

\[
f(z_{ki}^1) = f(x_{2k-1}^1), \\
f(z_{ki}^2) = f(y_{2\beta+1-k}^1),
\]

where \( \beta = \beta + \beta + 1 \).}

Next, after computing the labelling forms (C-5) with \( k \in [1, p] \), we obtain

\[
f(E(G_{2k-1}^r)) = A(2), B(1))^n, \quad k \in [1, \beta + 1]; \\
f(E(G_{2k}^r)) = A(1), B(0))^n, \quad k \in [1, \beta].
\]

and furthermore the labels of vertices, except \( f(x_{ki}^1) = f(y_{2k-1}^1) \) and \( f(x_{ki}^2) = f(y_{2k}^1) \), differ from each other, and the labels of edges differ from each other.

Next, after computing the labelling forms (C-5) with \( k \in [1, p] \), we obtain

\[
f(E(G_{2k-1}^r)) = A(2), B(1))^n, \quad k \in [1, \beta + 1]; \\
f(E(G_{2k}^r)) = A(1), B(0))^n, \quad k \in [1, \beta].
\]

and furthermore the labels of vertices, except \( f(x_{ki}^1) = f(y_{2k-1}^1) \) and \( f(x_{ki}^2) = f(y_{2k}^1) \), differ from each other, and the labels of edges differ from each other.

Next, after computing the labelling forms (C-5) with \( k \in [1, p] \), we obtain

\[
f(E(G_{2k-1}^r)) = A(2), B(1))^n, \quad k \in [1, \beta + 1]; \\
f(E(G_{2k}^r)) = A(1), B(0))^n, \quad k \in [1, \beta].
\]

According to formula (7), we obtain \( f(z_{ki}^r) = f(z_{ki}^r) + f(z_{ki}^r) \) in \( F \) with \( i \in [1, I], j \in [I + 1, p], k \in [0, 2\beta + 1] \).

and furthermore the labels of vertices, except \( f(x_{ki}^1) = f(y_{2k-1}^1) \) and \( f(x_{ki}^2) = f(y_{2k}^1) \), differ from each other, and the labels of edges differ from each other.

Next, after computing the labelling forms (C-5) with \( k \in [1, p] \), we obtain

\[
f(E(G_{2k-1}^r)) = A(2), B(1))^n, \quad k \in [1, \beta + 1]; \\
f(E(G_{2k}^r)) = A(1), B(0))^n, \quad k \in [1, \beta].
\]

and furthermore the labels of vertices, except \( f(x_{ki}^1) = f(y_{2k-1}^1) \) and \( f(x_{ki}^2) = f(y_{2k}^1) \), differ from each other, and the labels of edges differ from each other.
By Definitions 2 and 4 and formulae (3)–(8), the labelling $f$ is aSo-TOE-labelling of $G = \bigcirc_2(S_1, S_2)$. Hence, $G$ is aSo-TOE-graph. Here, we have proven Case 1. For understanding Case 1, see Figures 10 and 11.

**Case 2.** We, for the case $p = 2\beta$ and $r = 1, 2$, define a new labelling $f$ for $i \in [1, s'_k]$ and $j \in [1, t'_k]$ in the following way:

**L-1** \( f(x'_{2k-1,j}) = \pi_{2k-1}(x'_{2k-1,j}) + 2(q + 1)(k - 1) \) with $k \in [1, \beta]$;

**L-2** \( f(x'_{2k,i}) = \pi_{2k}(x'_{2k,i}) + 2(q + 1)(\beta + k) - M - 4 - (-1)^r \) with $k \in [1, \beta]$;

**L-3** \( f(y'_{2k-1,j}) = \pi_{2k-1}(y'_{2k-1,j}) + 2(q + 1)(\beta + k - 1) - M - 2 \) with $k \in [1, \beta]$;

**L-4** \( f(y'_{2k,i}) = \pi_{2k}(y'_{2k,i}) + 2(q + 1)(k - 1) + 2 + (-1)^r \) with $k \in [1, \beta]$;

**L-5** \( f(x'_{k,j}y'_{k,j}) = f(y'_{k,j}) + f(x'_{k,j}) \mod 2p(q + 1) - 2) \).

From the above labelling forms (L-1)–(L-4), we can compute

\[
\bigcup_{k=1}^{\beta} f(X'_{2k-1}) \cup \bigcup_{k=1}^{\beta} f(Y'_{2k})
\]

\[
= [0, 2(q + 1) \beta - 2]^r;
\]

\[
\bigcup_{k=1}^{\beta} f(Y'_{2k-1}) \cup \bigcup_{k=1}^{\beta} f(X'_{2k})
\]

\[
= [2(q + 1) \beta - 1, 2p(q + 1) - 3]^r,
\]

\( r = 1, \)
= [2(q + 1)\beta - 2, 2p(q + 1) - 4]^{r},
\quad r = 2.
(9)

Therefore, we conclude that \( \bigcup_{r=1}^{2} \bigcup_{k=1}^{p} f(V(G^i_k)) \) = [0, 2p(q + 1) - 3] and
\[
\left[ \bigcup_{r=1}^{2} \bigcup_{k=1}^{p} f(E(G^i_k)) \right] \cup \left[ \bigcup_{r=1}^{2} f(E(T_r)) \right] = [1, 2p(q + 1) - 3]^{r},
\quad r = 1, 2.
(10)
\]
in which the labels of vertices and edges, except \( f(y_{pq}^i) = f(y_{ps}^i) \) and \( f(x_{pq}^i) = f(x_{ps}^i) \), differ from each other, respectively.

Again, by computing the labelling form (L-5) for each \( k \in [1, p] \), we obtain
\[
f(E(G_{2k-1}^i)) = [\alpha(2) \beta(1)]^{r},
\quad \alpha(x) = 2(q+1)(\beta + 2k - x) - 1 \quad \text{and} \quad \beta(x) = 2(q+1)(\beta + 2k - y) - 5.
(11)
\]

Synthesizing the above argument, we get \( \bigcup_{k=1}^{p} f(E(G^i_k)) = [1, 2p(q + 1) - 3]^{r} \setminus F' \), where the set \( F' = [2(q + 1)(\beta + k) - 3 \mod 2p(q + 1) - 2) : k \in [1, 2\beta - 1] \). For each vertex \( z'_k \in T, \) with \( t \in [1, p] \) and \( r = 1, 2 \), we set
\[
f(z'_k) = f(x_{2k-1,1})^r, \quad f(z'_k)^r = f(x_{2\beta+2k-1,1}^r).
(12)
\]
\[
f(z_{l+k}^i) = f(y_{l+k}^i), \quad f(z_{l+k}^i) = f(y_{l+k}^i)^r.
(13)
\]

The above formula (12) enables us to obtain \( f(z'_k z'_j) = f(z'_i) + f(z'_j) \in F' \) with \( i \in [1, l], j \in [l+1, p], \) and \( r = 1, 2 \). Therefore, we have shown
\[
f(E(T_r)) = F'.
(13)
\]

After performing a CA-operation on \( G_k^i \) and \( T_r \), having labelling \( f \) for \( k \in [1, p] \), then we obtain a new graph \( S \), with

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure11.png}
\caption{A So-TOE-graph \( \bigcup(S_1, S_2) \) made by the graphs shown in Figure 10 for understanding the proof of Case 1 of Theorem 8.}
\end{figure}
Conjecture 9. Let each $\circ_2 (G_k, G_k')$ be a TOE-graph for $k \in [1, m]$ with $m \geq 2$. The 2-identification graph $G = \circ_2 (H_1, H_2)$ obtained by the edge-series operation (resp., the base-pasted operation) admits a TOE-labelling $r$.

Conjecture 10. Every simple and connected TOE-graph admits an odd-elegant labelling.

Conjecture 11. Each connected graph is the TOE-source graph of a certain TOE-graph.

A more interesting problem is to design super Topsnut-GPWs such that each super Topsnut-GPW will not be deciphered by attacks of nonquantum computers, since (i) our methods introduced here can construct quickly large scale of Topsnut-GPWs having hundreds vertices; (ii) the space of the Topsnut-GPWs given in Theorem 8 is quite tremendous; (iii) the 2-identification graphs $\circ_2 (H_1, H_2)$ of Theorem 7 and $\circ_2 (S_1, S_2)$ of Theorem 8 are the compound type of Topsnut-GPWs based on smaller scale of Topsnut-GPWs $G_k = \circ_2 (G_k, G_k')$ with $k \in [1, m]$, and they induce the TOE-books $B(H, f)$ and $B(S_1, g)$; it may be guessed that there is no polynomial algorithm for determining the TOE-books; and (iv) no polynomial algorithm was reported for finding all odd-elegant labellings of a given graph.

Thereby, we hope to discover such super Topsnut-GPWs which can be used in the era of quantum information.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.
Acknowledgments

This work was supported by the National Key R&D Program of China (no. 2016YFB0800700) and the National Natural Science Foundation of China (nos. 61572046, 61502012, 61672050, 61672052, 61363060, and 61662066).

References


