2014 11th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)
Ciudad del Carmen, Campeche. Mexico September 29–October 3, 2014

Complexity of Independent Set Problem over m-path graphs

Israel Buitron-Damaso
Computer Science Departament
CINVESTAV-IPN
Mexico City, Mexico
Email: ibuitron@computacion.cs.cinvestav.mx

Feliú Sagols Troncoso
Mathematics Departament
CINVESTAV-IPN
Mexico City, Mexico
Email: fsagols@math.cinvestav.mx

Guillermo Morales-Luna
Computer Science Departament
CINVESTAV-IPN
Mexico City, Mexico
Email: gmorales@cs.cinvestav.mx

***Abstract*—Some authentication protocols are based on NP-complete problems as the Independent Set Problem. However, this problem can be solved within polynomial-time algorithms over certain particular graph classes.**

We have found experimentally that the complexity of the Independent Set Problem provides a satisfactory confidence in order to be used on zero knowledge authentication protocols whose platform spaces are the introduced m-path graphs.

I. Introduction

A family of challenge-response identification protocols is proposed based on the construction of Hamiltonian cycles on certain graphs and in the difficulty to find maximum independent sets in those rather big graphs.

In this protocol, a prover must prove to a verifier that he/she possesses a secret digital identity. Both, the prover and the verifier, have as common knowledge a graph G. The secret possessed by the prover is a set Π of pairwise non-crossing and disjoint subpaths in G all of length $m \in \mathbb{Z}^+$.

Let us propose the following:

Identification protocol

The prover chooses a Hamiltonian cycle H of G and constructs a set of pairwise disjoint subpaths within H, say

$$\begin{aligned}\Pi \;=\; & \{p_1 = [v_{1,1}, \ldots, v_{m,1}],\\ & \vdots\\ & p_k = [v_{1,k}, \ldots, v_{m,k}]\},\end{aligned}$$

where $m, k \in \mathbb{N}$ are appropriate security parameters and the prover makes public the pairs of extreme vertices $V = \{(v_{1,1}, v_{m,1}), \ldots, (v_{1,k}, v_{m,k})\}$.
Then, the verifier challenges the prover with a set $U \subset V$ and the prover must respond with a set of pairwise non-crossing paths connecting each pair at U, all of length m.

The protocol is robust because the paths at the response are in correspondence with an independent set at a certain huge graph, thus finding such set directly poses a computationally intractable problem.

The aim of this paper is to illustrate the computational difficulties for an intruder to forge a fake successful identification interactive test. The paper is structured as follows: in section II we introduce a brief idea about the Independent Set Search Problem applied to our protocol and we recall the so called Berge graphs. In section III we show details of our experiments focused to prove that m-path graphs are not Berge graphs. In section IV we show our experimental results and finally in section V we state the conclusion of these experiments, as well as some comments on the complexity of the search problem.

II. Problems in graphs

A. Independent Set Problem

A *graph* is a pair $G = (V, E)$ where $V(G)$ is a finite and non-empty set of *vertices* and the set of *edges* $E(G)$ is a subset of

$$V^{(2)} = \{A \subset V |\ \text{card}(A) = 2\},$$

the cardinalities of $V(G)$ and $E(G)$ are respectively, the *order* and the *size* of the graph G.

A *subgraph* H of G is a graph such that $V(H) \subset V(G)$ and $E(H) \subset E(G)$. If $U \subset V(G)$ then the *induced subgraph* G_U by U is the graph such that $V(G_U) = U$ whose set of edges is determined by the following rule:

> two vertices u, v in U' are joined by an edge in $E(G_U)$ if and only if $uv \in E(G)$.

If $e = v_1v_2 \in E(G)$, then v_1 is *adjacent* to v_2 and the vertices v_1 and v_2 are *incident* to the edge e.

The *complete graph* K_n of order n is the graph having n vertices which are pirwise adjacent. A *clique* in G is a complete induced subgraph of G.

A *path* in G with *initial vertex* v_0 and *ending vertex* v_m is a sequence of vertices

$$\pi = v_0v_1 \ldots v_m$$

such that $\forall i = 0, \ldots, m-1$, $v_iv_{i+1} \in E(G)$ and those edges are pairwise different, m is a positive integer. The vertices v_0 and v_m are the *endpoints* of π. The length $|\pi|$ of the path π is m, hence π is said to be an *m-path*. The internal vertices of π are $v_1, \ldots, v_{m-1}$. If $v_0 = v_m$ then π is a *cycle*.

The *distance* $d_G(u, v)$ between two vertices u, v in the graph G is the length of the shortest path connecting u and v. Two paths which are not cycles π_1, π_2 are *non-crossing* if there is no a common vertex in π_1 and π_2 which is internal in at least

978-1-4799-6230-3/14/$31.00