Identification protocols based on non-crossing and disjoint paths at the hypercube

Guillermo Morales, Israel Buitrón, Feliú Sagols Troncoso

CINVESTAV-México

Conferencia Iberoamericana de Seguridaad de la Información

Abstract

A family of challenge-response identification protocols is proposed. They are based on the construction of Hamiltonian cycles in certain graphs, and in the complexity of finding maximum independent sets in huge graphs.

Tabla de contenido

Purpose of these protocols

In user identification and authentication several challenge-response protocols have been proposed [**?**]. Any *prover* is able to generate instances and corresponding solutions of computationally hard problems: the instances play the role of public keys of him, while the solutions are corresponding private keys. Any *verifier* chooses instances as challenges to the prover, and only the prover is able to submit proof of his knowledge by providing the corresponding solutions.

Our protocol

Here we introduce a challenge-response identification protocol based on the difficulty to solve the Independent Set Problem.

Non-crossing paths

Given a collection of equally length paths in a graph which are pairwise non-crossing (no pair has a common vertex which is internal in at least one of the paths) and disjoint (no edge is shared), it is required to add one path with prescribed endpoints in the graph such that the resulting set of paths remains pairwise disjoint and non-crossing.

Construction of the private and public keys

In the identification protocol, the private key of a prover is a set Π of non-crossing and disjoint paths of the same length in a graph G publicly known, and his/her public key is the collection of endpoints of the paths in Π. The paths are easily constructed from a Hamiltonian cycle of G which is randomly generated by the prover.

Challenges to the prover

The challenges consist of subsets of the public key and the responses are corresponding sets of equally length pairwise disjoint non-crossing paths connecting the challenge pairs. Any intruder aiming to impersonate the prover shall build an acceptable response, i.e., a set of pairwise disjoint non-crossing paths, all having the same given length. This is a rather hard problem.

Difficulties to fake the prover

The difficulties to fake the prover successfully or to disclose the whole secret key is reduced to the hardness of finding an maximum independent set in a graph with a number of vertices growing super polynomially with respect to the size of G. Hence, the impersonation problem is computationally intractable.

Extreme cases

Clearly, two extreme cases arise: if the challenge consists of a very small number of pairs, then an acceptable response may efficiently be forged; on the other side if the challenge consists of the whole public key, then anyone who has received the corresponding response may impersonate the prover. However slight increases of a small number of pairs may render a very hard impersonation problem, preserving in this way the robustness of the proposed method.

Tabla de contenido

We introduce a hard problem related to the construction of non-crossing and disjoint paths with the same length in a graph which must be solved in order to break the our identification protocols.

Non-crossing paths

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

Two-factors and Hamiltonian cycles

A *two-factor* in a graph G is a family $C_1, \ldots, C_k$ of cycles of G such that any vertex in G belongs to one and only one cycle C_i. A two-factor of G consisting of only one cycle is a *Hamiltonian* cycle of G. Let $\mathcal{H}_G$ be the collection of Hamiltonian cycles in G. If $\mathcal{H}_G \neq \emptyset$ then G is called *Hamiltonian*.

Independent sets

Let G be a graph, an *independent* set of G is a subset I of $V(G)$ such that no edge in $E(G)$ contains both end-points in I. A *maximal independent set* of G is an independent set of G that is not a proper subset of another independent set of G. A *maximum independent set* of G is a maximal independent set with the largest cardinality, the so called *independence number* of G, $\alpha(G)$.

The independent set problem is NP-Hard

The Independent Set Problem consists in finding a maximum independent set in a given instance graph G. It is well known that it is an NP-hard problem, difficult even to be approximated [**?**].

From a Hamiltonian cycle is easy to construct non-crossing paths

Any Hamiltonian cycle H in a graph $G = (V, E)$ determines, for each pair of distinct vertices $(u, v) \in V^2$, two paths, one going, let us say, from u to v and the supplementary path from v to u. Let $\pi_H(u, v)$ be the path going from u to v following the order in which the vertices of H are listed. Since H is Hamiltonian, for any two pairs $(u_0, v_0), (u_1, v_1)$ such that u_0, v_0, u_1, v_2 appear in cyclic order in the Hamiltonian cycle the paths $\pi_H(u_0, v_0)$ and $\pi_H(u_1, v_1)$ are non-crossing.

The non-crossing path problem

`NonCrossingPaths`

Instance: A graph $G = (V, E)$. A positive number k, a set $K = \{(i_1, j_1), \ldots, (i_k, j_k)\}$ of k pairwise different pairs of vertices in G, and a positive integer m satisfying $m \cdot k \leq |V(G)|$ and $d_G(i, j) \leq m$ for all $(i, j) \in K$.

Solution: A pairwise non-crossing and disjoint collection of m-length paths $\Pi = \{\pi_1, \ldots, \pi_k\}$ such that π_l has endpoints i_l and j_l, for $l = 1, \ldots, k$.

It is easy to construct instances of NonCrossingPaths having a solution

Given a Hamiltonian cycle H of G it is very simple to complete instances of NonCrossingPaths having as solutions non-crossing and disjoint paths taken from H. For instance, if $H = v_0 v_1 \dots v_{|V(G)|-1}$, and $m \cdot k \leq |V(G)|$, then for

$$\begin{aligned} K = \{ & (v_0, v_m), \\ & (v_{m+1}, v_{2(m+1)-1}), \\ & \vdots, \\ & (v_{(k-1)(m+1)}, v_{k(m+1)-1}) \} \end{aligned}$$

the collection of paths

$$\begin{aligned} \Pi = \{ & v_0 \dots v_m ; \\ & v_{m+1} \dots v_{2(m+1)-1} ; \\ & \vdots \\ & v_{(k-1)(m+1)} \dots v_{k(m+1)-1} \} \end{aligned}$$

But solving NonCrossingPaths is an extremely hard problem

Given an instance of NonCrossingPaths $(G,\ k,$ $K = \{(i_1, j_1), \ldots, (i_k, j_k)\},\ m)$ the *path graph* $P_{m,k,K,G}$ is the graph whose vertices are the m-paths in G connecting pairs at K:

$$\pi = [u_0 \ldots u_m] \in V(P_{m,k,K,G}) \ \Leftrightarrow\ (u_0, u_m) \in K,$$

and the edges are of two types: For any $\pi, \rho \in V(P_{m,k,K,G})$,

- if π, ρ are crossing then $\pi\rho \in E(P_{m,k,K,G})$, and
- if π, ρ have the same extreme points, then $\pi\rho \in E(P_{m,k,K,G})$.

An independent set I of $P_{m,k,K,G}$ yields a set of non-crossing and disjoint paths with ends in K, with no pair of extreme points connected by two paths.

It happens because ...

For any pair $(i_l, j_l) \in K$ let $R(i_l, j_l)$ be the sub graph of $P_{m,k,K,G}$ induced by the set of vertices at $V(P_{m,k,K,G})$ having as extreme points i_l and j_l. Then $R(i_l, j_l)$ is a clique. Those cliques produce a partition of the vertices in $P_{m,k,K,G}$ in k subsets, and any solution of `NonCrossingPaths` should contain exactly one member at each clique, hence it contains at most k paths. Thus, whenever there exists an independent set I^* reaching the upper bound k, such I^* is maximum. This is stated in the following result.

Proposition

The independence number of $P_{m,k,K,G}$ is k and an independent set of $P_{m,k,K,G}$ is maximum if and only if it is a solution of the instance $(G,\ k,\ K = \{(i_1, j_1), \ldots, (i_k, j_k)\},\ m)$ of `NonCrossingPaths`.

Tabla de contenido

Generation of the keys

Let $\mathcal{P}$ be a set of *participants*. Let G be a Hamiltonian graph satisfying the above properties, publicly known. Each participant $p \in \mathcal{P}$ constructs randomly a Hamiltonian cycle $H_p \in \mathcal{H}_G$ and selects as private key a set Π_p of k_p non-crossing and disjoint m_p-paths directly from H for positive values m_p and k_p chosen by the participant p in such a way that $m_p \cdot k_p \leq |V(G)|$. Then, he/she selects as *public key* the tuple (k_p, m_p, K_p), where K_p is the set of pairs of endpoints of the paths in Π_p.

Identification Protocol

A Prover shall prove to a Verifier that he/she knows the private key Π_p of his/her public key (k_p, m_p, K_p).

1. The Verifier selects a subset $L_v \subset K_p$ and sends it to the Prover as a challenge.
2. The Prover replies with the list R_{L_p} of m_p-paths connecting each pair at L_v.
3. The Verifier accepts accordingly to whether R_{L_p} is a collection of pairwise non-crossing and disjoint m_p-paths.

Robustness of the identification protocol

In order that the identification protocol be tampered by an Intruder, a fake private key should be forged, hence the problem `NonCrossingPaths` should be solved.
The robustness of the identification problem lies thus on the Intractability Assumption stated above.
In this proposal we are requiring that the response paths be of equal length just for economy. In this way the length d_p is published as part of the public key. Otherwise, the Prover may choose vertex pairs (u, v) and publish the triples $(u, v, |\pi_{H_p}(u, v)|) \in V(G)^2 \times Z^+$ as his/her public key.

Tabla de contenido

Two building blocks are essential to implement our identification protocol. The first one is the generation of random Hamiltonian cycles in the hypercube to produce the public and private keys. The second one is the criteria to select instances of `NonCrossingPaths` making extremely hard any attack attempt. We address here the random generation of Hamiltonian cycles.

Hamiltonian cycle generation

We need:

Hamiltonian cycle generation

We need:

1. A graph with an exponential number of Hamiltonian cycles.

Hamiltonian cycle generation

We need:

1. A graph with an exponential number of Hamiltonian cycles.
2. A starting Hamiltonian cycle.

Hamiltonian cycle generation

We need:

1. A graph with an exponential number of Hamiltonian cycles.
2. A starting Hamiltonian cycle.
3. A way to travel easily in the space of Hamiltonian cycles of such a graph.

The Hypercube of order n Q_n satisfies these conditions

The Hypercube of order n Q_n satisfies these conditions

1. The number of Hamiltonian cycles is double-exponential

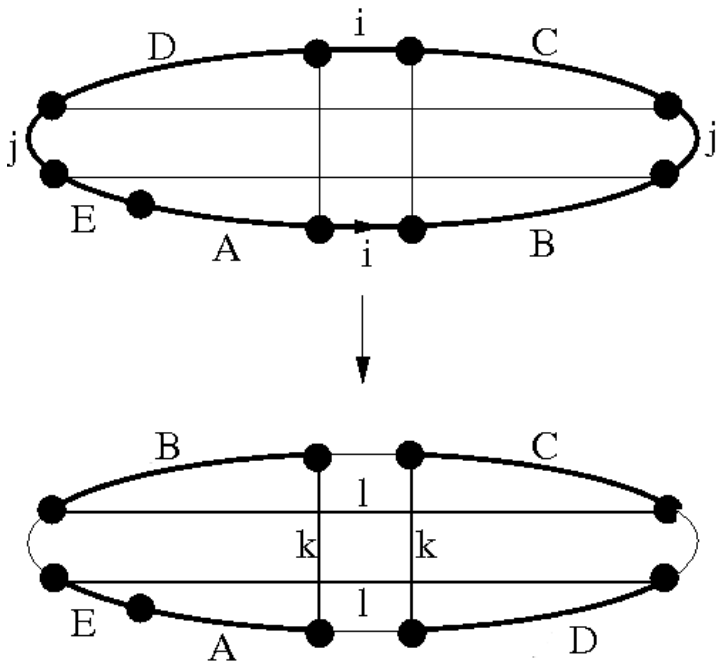
The Hypercube of order n Q_n satisfies these conditions

1. The number of Hamiltonian cycles is double-exponential
2. The Gray code is a good starting Hamiltonian cycle.

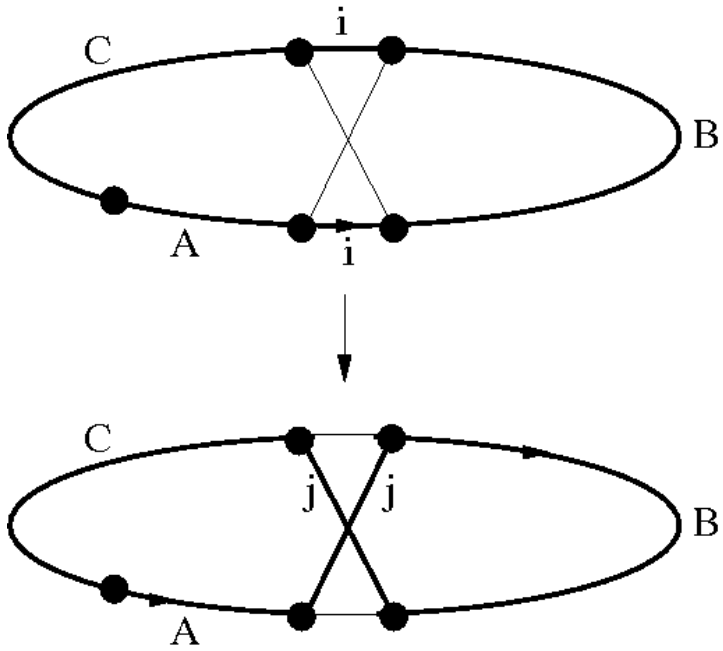
The Hypercube of order n Q_n satisfies these conditions

1. The number of Hamiltonian cycles is double-exponential
2. The Gray code is a good starting Hamiltonian cycle.
3. There are two operations to transform navigate in the set of Hamiltonian cycles of Q_n.

Operation 1



Operation 2



The number of Hamiltonian cycles reachable from the Gray code by using operations 1 and 2

We have proved that the number of Hamiltonian cycles reachable from the gray code is exponential on n. So, a random walk on the graph having as vertices the Hamiltonian cycle of Q_n and were two vertices are adjacent if and only if one is transformed into the other by an Operation 1 o 2 is appropriate to generate the private and public keys of our protocol.

The recommended parameters to make robust our protocol

We have proved too that with parameters $n = 12$, $m = 32$ and $d = 32$ the probability to break our protocol is under $1e^{-60}$. This is the probability to guess an maximum independent set in the corresponding paths graph.