Galambos Máté

Gábor Dénes Főiskola, mérnök-informatikus szak, III. évfolyam

Konzulens: Dr. Bacsárdi László

Tudományos munkatárs

ADATSOROK KVANTUM-NYOMKÖVETÉSE – EGY ÚJ ALKALMAZÁS

Számtalanszor előfordul, hogy valakinek vagy valaminek ismernünk kell a helyét – ugyanakkor fennáll a veszélye annak, hogy az illető hazudik arról, hol tartózkodik. A kvantum-nyomkövetés ebben a helyzetben segíthet minket; segítségével egy válaszadásra alkalmas eszköz térbeli helyét lehet ellenőrizni.

A protokoll alapja két fizikai törvény: egyrészt a kvantuminformáció nem másolható (ez az úgynevezett no-cloning vagy másolhatatlansági tétel), másrészt a fénynél gyorsabb információtovábbítás lehetetlen.

Az eljárást nagyjából tíz évvel ezelőtt fedezték fel, így még gyerekcipőben jár, és számos megválaszolatlan kérdés kapcsolódik hozzá. Jelen dolgozatomban ezek közül a kérdések közül vizsgálok meg néhányat.

Fontos megjegyezni, hogy a kvantum-nyomkövetés sem azt nem garantálja, hogy illetéktelen személy ne jusson be a kérdéses helyre (ezt másképp kell biztosítani), sem a kommunikációs partner kilétéről nem árul el semmit. Ez ellentétben áll az intuíciónkkal, ami félreértésekre adhat okot. A gyakorlatban inkább egy mozgásban lévő partnerről szeretnénk megállapítani, hol tartózkodik: például jelent már meg olyan cikk a szakirodalomban, ami önvezető autók helyét próbálta kvantum-nyomkövetéssel ellenőrizni. A valóságban azonban nem garantálhatjuk, hogy ami az adott helyen van, valóban autó.

Jelen dolgozatomban ezt a hiányosságot szeretném legalább részben orvosolni: olyan a kvantum-nyomkövetésre épülő protokollt mutatok be, amivel ha nem is fizikai objektumokat, de legalább adatsorokat nyomon követhetünk.

GÁBOR DÉNES FŐISKOLA

1119 Budapest, Fejér Lipót u. 70.
Tel: 36-1-203-0283

ABSTRACT

Máté Galambos

Dennis Gábor College, Computer Engineering, 3rd year

Consultant: Dr. László Bacsárdi
Research Fellow

QUANTUM TAGGING A DATASET–A NEW APPLICATION

We would often like to know the position of someone or something–even if there is a possibility that this person is lying about his or her location. Quantum tagging could help in these situations: with this procedure we can verify the location of a special communication device.

The protocol is based on two physical laws: a) unknown quantum information cannot be copied (this is known as the no-cloning theorem) and b) faster than light signaling is not possible.

Quantum tagging was first discussed in the scientific literature about ten years ago; naturally it is still a developing field with many open questions. In my present work I examine some of these questions.

It is worth knowing however that quantum tagging does not prohibit unauthorized personnel to enter the verified site (it is often assumed that something outside the protocol guarantees this), nor does it authenticate who or what our communication partner is. This contradicts our intuition–it would be more useful if we could verify the position of a moving communication partner. For example: some authors suggested quantum tagging self-driving cars. Unfortunately the protocol–as we know it today–does not guarantee that it is indeed a car whose position we verified.

In my present work I address this shortcoming, at least partially: I introduce a modified protocol that can verify the location of a dataset if not a physical object.