

Ricercatori europei contro gli attacchi alla sicurezza

Il progetto dell'UE per lo sviluppo di una rete assolutamente sicura per la trasmissione di informazione – basato sulla crittografia quantistica – apre una nuova era per la sicurezza.

Vienna, 1° Aprile 2004. La sicurezza della crittografia quantistica si fonda su leggi naturali e non su problemi matematici di difficile soluzione, come i metodi crittografici attualmente in uso. Lo scopo di questo progetto straordinario è quello di rendere la tecnica della crittografia quantistica utilizzabile in ambito commerciale al termine di 4 anni. Fa parte del progetto lo sviluppo di un prototipo per la codifica dell'informazione pronto per il mercato, così come un'efficiente infrastruttura di rete, che permetta l'impiego globale di questo metodo di codifica.

Esperti della fisica quantistica collaborano con specialisti di rete, come anche con corifei nei campi della crittografia, dell'elettronica, delle tecniche di sicurezza e dello sviluppo di software. Esperti di economia integrano questa squadra eterogenea.

“SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography”.

Questo nome criptico significa: sviluppo di una rete globale per comunicazioni sicure basate sulla crittografia. Il primo progetto integrato (IP) del sesto programma tematico della UE sotto la direzione dell'Austria comincia oggi. Il progetto europeo di ricerca e sviluppo è coordinato dal gruppo di tecnologie quantistiche nel campo delle tecnologie dell'informazione ARC Seibersdorf research GmbH.

“Mettiamo a disposizione del mercato gli strumenti, basati sulla tecnologia della fisica quantistica, per difendersi da attività di spionaggio. Lo spionaggio economico è effettuato, tra l'altro, dalla rete di sorveglianza mondiale ECHELON, che ha provocato ingenti danni in passato. Con questo progetto diamo un contributo essenziale all'indipendenza dell'economia europea” dichiara il dott. Christian Monyk, direttore del gruppo di tecnologie quantistiche e promotore del progetto.

Crittografia quantistica come base di una rete di comunicazione altamente sicura

La crittografia quantistica, ovvero la produzione di codici per la codifica dell'informazione attraverso i metodi della meccanica quantistica, offre soluzioni per due problemi dei sistemi di codifica oggi in uso: la produzione di un codice assolutamente casuale e la sua trasmissione. Un ulteriore vantaggio di questo metodo: un' intercettazione può essere scoperta già durante la produzione dei codici, ancora prima della trasmissione dell' informazione. In questo modo si può, nel peggiore dei casi, impedire del tutto la trasmissione dell'informazione. Ma anche nel caso in cui l'informazione è stata codificata con questo metodo, il contenuto dell'intercettazione non può, per principio, più essere trasmesso - un vantaggio essenziale rispetto agli attuali mezzi di codifica.

Attraverso questo progetto vengono poste le basi per una rete di comunicazione altamente sicura, nella quale i risultati quanto meccanici della ricerca di base vengono sviluppati ulteriormente e collegati con le componenti della crittografia, con la tecnologia delle reti e dei computer.

Il progetto ha una durata di 4 anni ed è finanziato dalla UE con 11,4 milioni di euro.

Complessivamente partecipano 41 partner da 12 paesi (Austria, Belgio, Svizzera, Repubblica Ceca, Germania, Danimarca, Francia, Gran Bretagna, Italia, Russia, Svezia, Canada) di cui 3 KMU, 25 università, 5 centri di ricerca e 8 aziende private.

Ricerca di base e applicazioni messe d'accordo

Il progetto è suddiviso in otto parti, di cui ognuna tratta un aspetto essenziale. Dopo una durata di 18 mesi segue una fase di valutazione, in cui i diversi metodi di crittografia quantistica vengono analizzati in base alla possibilità di inserirli nel mercato.

“L'applicabilità nel mercato della crittografia quantistica è meta del progetto, ma anche la ricerca di base, di pari importanza, che dà un contributo essenziale alle future tecnologie”, sostiene il Dott. Christian Monyk.

Il gruppo di tecnologie quantistiche nel campo delle tecnologie dell'informazione ARC Seibersdorf research GmbH è stato fondato nell'anno 2002 allo scopo di favorire l'inserimento nel mercato delle tecnologie della fisica quantistica. Un primo, decisivo passo è stato l'inizio del progetto SECOQC della UE. Il gruppo ha ricevuto nel Dicembre del 2003, per l'organizzazione di questo progetto, il premio degli ARC-Awards per il management della ricerca.

Per ulteriori informazioni:

Mag.^a Julia Petschinka

ARC Seibersdorf research GmbH

Sfera di competenza tecnologie dell'informazione - gruppo di tecnologie quantistiche

Coordinazione del progetto e P.R.

TechGate Vienna

Donau-City Straße 1

1220 Wien

Tel: +43-050550-4161

Cell.: +43-(0)664-8251064

e-mail: Julia.Petschinka@arcs.ac.at