

## Ricerca. La scoperta dell'ateneo sfrutta la fisica quantistica Camerino «cripta» i dati sensibili

**Mario Savini**  
CAMERINO

Il primo sistema in Italia a prova di hacker per criptare le informazioni da trasmettere e in grado di garantire, sfruttando i principi della fisica quantistica, la sicurezza assoluta dei dati. Si chiama "Criptocam" ed è la recente scoperta del laboratorio di Ottica quantistica del dipartimento di Fisica dell'Università di Camerino che rivoluziona le tecnologie informatiche e telematiche.

Il sistema — sperimentato per ora su 20 chilometri di fibra ottica, ma pronto a essere esteso ai 140 chilometri di cavo disponibile tra Olbia e Civitavec-

chia — annulla i tentativi di intercettazione, rendendo inattuabile la decifrazione di qualsiasi "codice segreto" come quello dei Bancomat o delle carte di credito, grazie all'invio su fibra ottica di un messaggio abbinato a una chiave di lettura random di segnali binari (0 e 1).

L'acronimo fa riferimento alle caratteristiche del progetto (criptaggio dei dati) e alla città da cui parte l'esperimento, Camerino, la cui Università nel 2003 ha ottenuto dal competente Ministero — in seguito a una richiesta del 2001 — un finanziamento di 600mila euro per il progetto Firb "Schemi di crittografia quantistica efficienti in

condizioni reali". «Tutto è partito da qui — precisa il direttore del laboratorio, **Paolo Tombesi**, che ha coordinato il lavoro di quattro ricercatori — arrivando a realizzare, in tempi brevissimi, più di ciò che era stato previsto. Tre anni fa, infatti, il laboratorio non esisteva. È stato eseguito, ad esempio, uno studio degli effetti dei ripetitori quantistici sull'efficienza e la sicurezza dei vari sistemi crittografici.

In particolare, ai due studiosi camerti Stefano Mancini e Marco Lucamarini va il merito di aver inventato il protocollo di comunicazione quantistica deterministica a due-vie "LM05" di Critpocam, che garantisce la

comunicazione segreta tra due parti: A e B, ovvero Alice e Bob (in gergo i due personaggi che si danno informazioni) sono collegati da un canale di fibre ottiche. Con un processo fisico che utilizza fotoni polarizzati, A e B possono ricevere un messaggio in grado di generare una chiave segreta per "leggere" le informazioni, che restano però indecifrabili per terzi. Il lavoro si è basato sull'utilizzo di una fibra ottica lunga 20 chilometri, concessa dalla Pirelli Labs di Milano. «Speriamo di estendere questo sistema a 140 chilometri — conclude Tombesi — ossia la distanza tra Olbia e Civitavecchia, dove mi è stato riferito che c'è un cavo in fibra ottica di Telez. Vogliamo chiedere l'autorizzazione in modo da sviluppare il progetto ed entro un anno e mezzo rendere di concreta applicazione questo metodo sperimentale».