

QUANTI E SEGRETI

Stefano Mancini

Scuola di Scienze e Tecnologie, Università di Camerino
Istituto Nazionale di Fisica Nucleare, Sezione di Perugia

Le comunicazioni segrete hanno da sempre segnato la storia dell'uomo con un continuo rincorrersi tra code-makers e code-breakers. Esse si sono sviluppate nel corso dei secoli come "arte" fino a divenire "scienza" grazie al paradigma della sicurezza dimostrabile. Il problema delle comunicazioni segrete verrà quindi affrontato da un punto di vista matematico rivisitando le soluzioni che caratterizzano la crittografia moderna. Poi, allargando gli orizzonti alla fisica quantistica, si analizzeranno nuove prospettive per il futuro: code-breakers che potrebbero beneficiare delle potenzialità di calcolo di computers quantistici e code-makers che potrebbero beneficiare della sicurezza assoluta di codici quantistici.