Mircea PLOTEANU,
Republica Moldova

METODE CRIPTOGRAFICE DE PROTEJARE A INFORMAȚIEI: CRIPTOGRAFIA CUANTICĂ – O NOUĂ PERSPECTIVĂ DE SECURITATE A INFORMAȚIILOR

În toată lumea companiile ce activează în sfera Tehnologiilor Informaționale atrag o mare atenție problemei protejării informațiilor, inventând, zi de zi, metode cu o durabilitate mai mare. La orizontul Securității Informațiilor a apărut Criptografia cuantică, care generează noi posibilități în domeniul respectiv.

Dacă e nevoie să apelăm la retorica întrebare i ce a fost la început, computerul sau infracțiunea informațională (de exemplu: accesul neautorizat al informațiilor sau furtul de informații de o confidențialitate strategică), constatăm că, conform datelor istorice şi arheologice, cel mai vechi document cifrat, adică invenția unei metode de criptare a documentelor secrete pentru prevenirea furturilor de informații, a fost găsit în Irak şi datează din sec **XVI a.Cr.** (acum 3600 de ani). Este vorba despre o tăbliță de argilă, pe care, un olar a gravat rețeta sa secretă, prin suprimarea consoanelor şi modificarea ortografiei cuvintelor, actualmente, acestei tablițe i-am spune un "certificat digital al cheii publice". De asemenea, şi grecii antici, locuitorii Spartei, încă din secolul **V a. Cr.** (acum 2500 de ani) au inventat metode de prevenire a furtului de informații (sau de prevenirea a accesului neautorizat la informații suprasecrete), ce țineau de securitatea şi viața unor întregi oraşe-state. Această ştiință a evoluat peste trei milenii, transformându-se, în prezent, acum într-o importantă ştiință de securitate a informațiilor – **criptografia**.[1]

Criptografia, timp de milenii, s-a aflat într-o dezvoltare dinamică, deoarece, de o parte a baricadei se aflau criptologii, specialiştii care se străduiau să inventeze metode de securitate a datelor şi tehnologii avansate ce nu ar permite nimănui să citească scrierile confidențiale, iar de cealaltă parte criptoanaliştii, specialiştii care se străduiau să spargă aceste cifruri secrete şi să citească mesajele confidențiale. La sfârşitul mileniului doi, a apărut o nouă ramură a criptografiei – criptografia cuantică.

Criptarea cuantică este o abordare bazată pe fizica cuantică pentru a realiza comunicații securizate. Spre deosebire metodele de criptografie tradiționale, care folosesc diverse metode matematice pentru a împiedica interceptarea şi decodificarea mesajului, criptarea cuantică se bazează pe legile fizicii în ceea ce priveşte transmiterea informației. Interceptarea poate fi văzută ca o măsurare a unui obiect fizic – în acest caz, purtătorul de informație. Folosind fenomene cuantice, cum ar fi suprapunerea cuantică sau legătura cuantică, se poate proiecta şi implementa un sistem de comunicație care să evite întotdeauna interceptarea. Aceasta este din cauză că măsurătorile asupra unui purtător de natură cuantică îl modifică şi, în acest fel, rămân "urme" ale interceptării.

Istorie. Criptarea cuantică a fost propusă pentru prima oară de Stephen Wiesenr, pe atunci la Universitatea "Columbia" din New York, când, la începutul anilor '70, a introdus un concept de codare cu conjugată cuantică. Lucrarea sa, intitulată "Conjugate Coding", a fost respinsă de Comisia de Teoria Informației a IEEE, dar a fost, în cele din urmă, publicată în 1983 în SIGACT News. El arată cum se poate reține sau transmite două mesaje codate în două "observabile conjugate", cum ar fi polarizarea liniară sau circulară a luminii, astfel, încât oricare dintre ele, dar nu amândouă, pot fi recepționate şi decodificate. El şi-a ilustrat ideea cu un proiect de bancnote care nu pot fi falsificate. Un deceniu mai târziu, pe baza acestei lucrări, Charles H. Bennett, de la Centrul de Cercetare "Thomas J. Watson" al IBM, şi Gilles Brassard, de la Universitatea din Montréal, au propus o metodă de comunicație securizată bazată pe observabilele conjugate ale lui Wiesener. În 1990, în mod independent şi fără să fie la curent cu lucrările precedente, Artur Ekert, pe atunci doctorand la Universitatea din Oxford, a folosit o abordare diferită bazată pe proprietatea de "legătură cuantică".

Schimbul de chei cuantice. O problemă centrală în criptografie este distribuirea cheilor.

[1] Nicolae Ploteanu, Securitatea informațională, Chişinău, Elena V.I. pag. 48

O soluție, aceea a criptografiei cu cheie publică, se bazează pe anumite probleme matematice complexe ca timp de calcul (cum ar fi factorizarea numerelor întregi), în timp ce criptarea cuantică se bazează pe legile mecanicii cuantice. Dispozitivele care folosesc criptarea cuantică utilizează fotoni individuali, şi se bazează fie pe principiul lui Heisenberg sau pe principiul legăturii cuantice. Incertitudine: Actul de a măsura este o parte integrantă a mecanicii cuantice, nu doar un proces extern şi pasiv, ca în cazul fizicii clasice. Este, deci, posibil să se codeze informația în anumite proprietăți ale fotonului, astfel, încât orice efort de a le monitoriza le modifică într-un mod uşor de detectat. Acest efect apare din cauză că, în teoria cuantică, anumite perechi de proprietăți fizice sunt complementare, în sensul că măsurarea uneia dintre aceste proprietăți o modifică pe cealaltă. Acest fenomen este cunoscut ca principiul incertitudinii al lui Heisenberg. Cele două proprietăți complementare, care sunt des folosite în criptarea cuantică, sunt cele două tipuri de polarizare a fotonului, de exemplu, liniară (vertical/orizontal) sau diagonală (la 45 si 135 de grade). Legătura: Este o stare a două sau mai multe particule cuantice (de exemplu, fotoni) în care multe din proprietățile lor fizice sunt puternic corelate. Particulele legate nu pot fi descrise specificând stările individuale ale particulelor, deoarece acestea pot să conțină informație într-un mod care nu poate fi accesat prin experimente făcute asupra vreuneia dintre ele în particular. Acest fenomen se produce indiferent de distanța dintre particule.

Cele două abordări. Pe baza acestor două proprietăți neintuitive ale mecanicii cuantice (incertitudinea şi legătura), au fost inventate două tipuri de protocoale de criptare cuantică. Primul foloseşte polarizarea fotonilor pentru a codifica biții de informație şi se bazează pe natura aleatorie a fizicii cuantice pentru a evita interceptarea mesajului. Al doilea foloseşte fotoni legați pentru a codifica biți, şi se bazează pe faptul că informația apare doar după măsurători făcute de părțile ce comunică.

Mărirea securității. Protocoalele de criptare cuantică au proprietăți la care nu se poate ajunge prin metodele tradiționale de criptare. Cei doi agenți care comunică pot genera şi interschimba chei aleatorii care sunt foarte similare – în condiții ideale ar trebui sa fie identice, dar, în realitate, va exista o anumită rată a erorii. De asemenea, aceste protocoale permit estimarea nivelului de interceptare a comunicației, şi se poate deduce câte din cheile lor aleatorii sunt cunoscute de o terța parte. Aceste rezultate sunt interesante, dar nu suficiente pentru a rezolva problema interschimbării cheilor. Interceptarea chiar a unei mici părți din chei poate avea efecte semnificative: o terță parte poate sa citească o bucată (poate critică) a mesajului secret. Din cauza faptului că erorile şi zgomotul de fond nu pot fi evitate în totaliltate, nu se poate garanta că nicio cheie nu a fost interceptată – erorile de comunicație şi încercările de interceptare nu pot fi deosebite, aşa că se poate presupune că, în cazul cel mai defavorabil, toate erorile se datorează interceptării mesajului. Mărirea securității este o versiune criptografică a corecției de erori, ceea ce permite ca cei doi agenți, care vor să comunice, să aibă la început chei similare despre care o terță parte poate să aibă anumite informații, şi, din aceste chei, să producă unele mai scurte, dar despre care un eventual atacator nu cunoaşte (aproape) nimic. Deşi mărirea (clasică) a securității poate fi folosită pentru oricare din protocoalele Bennett-Brassard sau Ekert, s-a descoperit că encriptarea bazată pe legătura cuantică permite mărirea securității direct la nivel cuantic. Astfel, se măreşte eficiența, şi apar şi alte avantaje. Printre altele, când tehnologia se va fi dezvoltat complet, va permite criptarea cuantică pe distante oricât de mari, folosind relee intermediare.

Bibliografie:

1. N. Ploteanu, Securitatea informațională, Elena VI, Chişinău, 2007, cap.3.
2. www.softpedia.com, Criptografia cuantica testata cu success de cercetătorii de la Universitatea Toronto.