DIVERSIFICAREA STRUCTURILOR DE DATE IN VEDEREA APLICARTI EFICIENTE A ALGORITMILOR DE CRIPTARE

LUMINITA SCRIPCARIU si PETRUT DUMA

Imbunatairea algoritmilor de criptare are, in general, ca scop, scaderea sanse1or de deducere a informatiilor utile prin atacuri criptografice. Cresterea lungimii cheii de criptare si a dimensiunii blocului de date pe care se aplica algoritmul de criptare este limitata ca grad de complexitate si timp admis pentru procesul de criptare. Se propune un non mod de proiectare a structurii spatiului de criptare, cu mai multe dimensiuni, precum si o distributie a datelor aleatorizata, pe mai multe containere care sa permita eliminarea efectelor corelatiilor existente intre simbolurile invecinate sau relative apropiate din secventa de intrare. In plus, prin combinarea datelor cu zgomot alb se realizeaza diversiunea necesara inducerii in eroare a eventualilor atacatori. Metoda propusa permite cresterea dimensiunii blocului de intrare, a lungimii cheii de criptare, precum si reducerea drastica a sanselor oricarui tip de atac criptografic.