

ჰიბრიდული ბიო-ციფრული კრიპტოსისტემა: DNA-XOR დაშიფრვის ალგორითმის სიმულაცია და ანალიზი

ლუკა ხანჯალაძე, ილია მახარაძე, საბა სიდამონიძე

luka.khanjaladze233@ens.tsu.edu.ge

კომპიუტერული მეცნიერების დეპარტამენტი, ზუსტ და საბუნებისმეტყველო მეცნიერებათა
ფაკულტეტი, თბილისის სახელმწიფო უნივერსიტეტი, თბილისი უნივერსიტეტის ქ.11

კვანტური გამოთვლების ეპოქის მოახლოებასთან ერთად, ტრადიციული კრიპტოგრაფიული სტანდარტები, როგორცაა RSA და AES, მოძველებისა და გატეხვის რეალური საფრთხის წინაშე დგანან, რადგან ისინი ეყრდნობიან ისეთ მათემატიკურ ამოცანებს, რომელთა გადაჭრაც კვანტურ ალგორითმებს მარტივად შეუძლიათ. პროექტი წარმოადგენს „ჰიბრიდული ბიო-ციფრული კრიპტოსისტემის“ შემუშავებასა და სიმულაციას, რომელიც იყენებს DNA-XOR არქიტექტურას პოსტ-კვანტური უსაფრთხოების მისაღწევად. ნაშრომში განხილული მთავარი გამოწვევა დნმ-კოდირების არსებული მეთოდების მოწყვლადობაა. ადრეული მიდგომები ეყრდნობოდა მარტივ ჩანაცვლებას (მაგალითად, ბინარული 00-ის ასახვა ადენინზე), რაც ინარჩუნებს ღია ტექსტის სტატისტიკურ კანონზომიერებებს და სისტემას დაუცველს ხდის სიხშირული ანალიზის მიმართ. ამ პრობლემის გადასაჭრელად, შმოთავაზებულია დაშიფრვის მრავალსაფეხურიანი ალგორითმი, რომელიც აერთიანებს ციფრული ლოგიკის სისწრაფესა და მოლეკულური ბიოლოგიის სირთულეს. წარმოდგენილი მეთოდი იყენებს ქაოსურ პირად გასაღებს ბულის "DNA-XOR" ოპერაციის შესასრულებლად, რასაც მოჰყვება ბიოლოგიური მანიპულაციის ტექნიკები: ჯაჭვის კომპლემენტაცია და მიმდევრობის რევერსი (შებრუნება). პროექტი მოიცავს პროგრამული სიმულაციის შექმნას აღნიშნული ლოგიკის ვალიდაციისა და უსაფრთხოების აუდიტისთვის. მოსალოდნელი შედეგები აჩვენებს, რომ ეს ჰიბრიდული მიდგომა ქმნის „შიფრ-დნმ-ს“, რომელიც ქიმიურად სტაბილურია, თუმცა სტატისტიკურად არ განსხვავდება ბიოლოგიური „ხმაურისგან“ (შემთხვევითი მიმდევრობისგან). ბიოლოგიურ გარემოში ციფრული კვალის წაშლით, სისტემა აღწევს „ინფორმაციულ-თეორიულ უსაფრთხოებას“, რაც მას შეუვალს ხდის Brute Force შეტევებისა და თანამედროვე კრიპტოანალიზისთვის.