СТАН СТВОРЕННЯ ТА ЗАСТОСУВАННЯ МЕТОДІВ ГЕНЕРУВАННЯ ЗСП

Фролов О.С.
Науковий керівник – д.т.н., проф. Бондаренко М.Ф.
Харьківский національний університет радіоелектроніки
(61166, Харьків, пр. Леніна,14, каф. БІТ, тел. (057) 702-14-25),
факс (057) 702-11-13

Qualified work contains the analysis of algorithms of generation general system parameters to the cryptography systems realized in group of points of elliptic curves. The comparative analysis of resistance of unsymmetrical systems realized in rings, fields and groups of points of elliptic curves is resulted. And also resistance of various algorithms of a digital signature attack of a selective fake. The advanced method of definition about random generated curve is developed.

На сьогоднішній день широке застосування знайшли асиметричні криптоперетворення типу ЕЦП на НШ з використанням математичного апарату групи точок еліптичних кривих. Обов'язковою умовою забезпечення стійкості в групі точок еліптичних кривих є використання загальносистемних параметрів(ЗСП) зі спеціальними властивостями.

Стійкість криптоперетворень в групі точок еліптичних кривих у значній мірі залежить від порядку точки еліптичної кривої, наприклад він може бути не менше ніж 2^{160}. В ДСТУ 4145 представленні значення загальносистемних параметрів, але їх величини обмежені порядком точки 2^{431}. В ряді науково-технічних статей в тому числі за участю автора запропонована математична модель та практичний метод побудування загальносистемних параметрів над полем 2^m що базується на методі САТО, але цей метод також має недоліки при порядку 2^{768}. Вирішення вказаних задач досягненно розв'язком таких задач:

1. Досліджень існуючих методів. Визнач їх обмежень та проблемних питань генерування ЗСП для порядків точок еліптичної кривої від 2^{571} до 2^{1024};
2. Розроблення або удосконалення методу побудування ЗСП по критерію зменшення складності при збереження стійкості;
3. Розробка та оптимізація програмно-апаратної моделі засобів генерування ЗСП;
4. розроблення пропозиції та системи ген загальних параметрів в указаному діапазоні порядку тонкі для ДСТУ 4145-2002.

За результатами досліджень розроблено математичну та програмну модель, з використанням яких побудовані ЗСП, які задовольняють вимогам.