УДК 681.3.06
Чура Б. – ст. гр. КСМс-52
Тернопільська академія народного господарства

АПАРАТНА РЕАЛІЗАЦІЯ КРИПТОАЛГОРИТМІВ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ КРИПТОГРАФІЇ ЕЛІПТИЧНИХ КРИВИХ

Науковий керівник: аспірант Якименко І.З.

Інформаційні ресурси в сучасних умовах являються одним із найважливіших результатів діяльності людського суспільства. Саме тому проблема захисту інформації на сьогоднішній день є дуже актуальною. Багато відомих причини призвели до виникнення цілої гами методів і засобів захисту інформації. Одним із підходів, щодо вирішення задач захисту інформації є застосування асиметричних криптоалгоритмів. Передове місце серед таких криптосистем займають еліптичні криві (ЕК).

Безпека криптосистем на основі еліптичних кривих, як правило, заснована на складності рішення задачі дискретного логарифмування в групі точок на еліптичній кривій над скінченим полем. Особливий інтерес до криптографії еліптичних кривих обумовлений такими перевагами – швидкодія та невелика довжина ключа. Усе це свідчить про високий рівень криптостійкості алгоритмів на ЕК. Правда, вони ніколи широко не використовувалися на практиці і не залучали до себе такої пильної уваги наукової громадськості як, наприклад, RSA. Зараз ситуація міняється, а отже системи з використанням ЕК реалізовуються як програмно так і апаратно.

Перевага апаратного шифрування над програмним обумовлено декількома причинами. По-перше, апаратне шифрування має більшу швидкість. Криптографічні алгоритми складаються з величезного числа складних операцій, виконуваних над бітами відкритого тексту. Сучасні універсальні комп’ютери погано пристосовані для ефективного виконання цих операцій, а спеціалізоване устаткування вміє робити їх набагато швидше. По-друге, апаратуру легше фізично захистити від проникнення ззовні. Програма, виконувана на персональному комп’ютері, практично беззахисна. Озброївшись відладчиком, зловмисник може внести в неї зміни, і ніхто нічого не помітить. І по-третє, апаратура шифрування більш проста в установці. Дуже часте шифрування потрібно там, де додаткове комп’ютерне устаткування є зовсім зайвим. Телефони, факсимільні апарати і модеми значно дешевше обладнати пристроями апаратного шифрування, чим вбудовувати в них мікрокомп’ютери з відповідним програмним забезпеченням. Навіть у комп’ютерах установка спеціалізованого шифрувального устаткування створює менше проблем, чим модернізація системного програмного забезпечення з метою додавання в нього функцій шифрування даних. Щоб домогтися цього за допомогою програмних засобів, шифрування повинне бути сховане глибоко в надра операційної системи. Але навіть будь-який непрофесіонал зможе приєднати шифрувальний блок з однієї сторони до персонального комп’ютера і до зовнішнього модему з іншої.

Основними арифметичними операціями в еліптичних кривих є додавання і скалярне множення точок. З використанням САПР VHDL мною ведуться розробки апаратної реалізації множення точки на скаляр та додавання точок на ЕК, а також дослідження часових та продуктивних параметрів системи. В перспективі планується апаратна реалізація повноцінної криптосистеми на основі еліптичних кривих.