

УДК 004.056.55

Антонюк М.А.¹, Неласа Г.В.²

¹ асп. НУ «Запорізька політехніка»

² канд. техн. наук, проф. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РЕАЛІЗАЦІЇ МАЛОРЕСУРСНОЇ КРИПТОГРАФІЇ

Актуальні питання світу із впровадження технологій, що допоможуть людству постають дуже гостро у час карантинних заходів. Створюється величезна купа пристроїв для виявлення та діагностування стану людей, для моніторингу поточного стану.

Сучасний світ крокує до повної діджиталізації. Цифрові пристрої займають місце цифрового помічника людини полегшуючи та покращуючи його життя. Загалом покращення виникають у момент об'єднання великої кількості розумних пристроїв у єдину систему. На жаль, «інтернет речей» це не лише красива назва, а й повноцінна мережа, де пристрої обмінюються службовою та досить конфіденційною інформацією. «Інтернет речей» диктує свої правила розвитку та поширення пристроїв [1]. Критично важливі дані необхідно захищати, так як це загроза кіберпростору. На жаль, наразі, у більшості пристроїв такої категорії не впроваджено жодного захисту. Зазвичай, всі дані передаються у відкритій формі і єдиний захист, який ці пристрої можуть використовувати – закладений у протоколах передачі даних. На жаль, цього недостатньо. Захист кіберпростору не обмежується лише захистом конфіденційності інформації.

Натомість не важливо від яких типів атак захищатися: починаючи зі збереження конфіденційності, цілісності інформації і закінчуючи порушенням доступу до інформаційних ресурсів. Останній тип нападу може виникати частіше, через поширеність та доступність смарт-пристроїв, так як на них можуть перекладатися деякі функції по ідентифікації користувачів. Наприклад, NFC-чип у смарт-годиннику, як ключ до дверей з NFC-зчитувачем.

Більшість смарт-пристроїв незалежно від їх розміру мають власний захист, але це не відноситься до більшості гаджетів, які входять в категорію “Інтернет речей” (як вже було вказано у прикладі, смарт-годинник), адже у більшості випадків навіть не виникає думки, що якусь шкоду можливо завдати реалізуючи атаку на ці пристрої, або використовувати ці пристрої для обхідної атаки на пристрої з захистом.

Рішення – використовувати криптографію. “Хмари”, сервера, що їх підтримують, мережі, персональні комп’ютери, кишенькові смарт-пристрої – це такі гіганти, на яких вже реалізовані і використовуються алгоритми криптографічного захисту. Оскільки обчислювальна потужність з роками зростала, технологія шифрування стала лише вдосконаленою та безпечнішою. Однак цей прогрес у технології також виявив потенційні обмеження малoresурсних сучасних методів шифрування.

Довжина ключа шифрування є показником сили методу шифрування. Наприклад, оригінальний ключ шифрування DES (Data Encryption Standard) складав 56 біт, тобто він мав 2^{56} можливостей комбінування. Завдяки сучасній обчислювальній потужності 56-розрядний ключ перестав бути захищеним, оскільки він вразливий до злому атакою грубої сили. Сьогодні стандарт сучасних ключів шифрування становить до 4096 бітів у системі RSA. Дешифрування 4096-бітового ключа шифрування практично неможливо з огляду на кількість можливих комбінацій. Однак квантові обчислення загрожують змінити цю безпечну природу.

Квантові обчислення використовують властивості квантової механіки для одночасної обробки великих обсягів даних. Встановлено, що квантові обчислення досягають обчислювальної швидкості в тисячі разів швидше, ніж сучасні суперкомп’ютери. Ця обчислювальна потужність є викликом сучасній технології шифрування. Наприклад, шифрування RSA використовує множення дуже великих простих чисел, щоб створити просте число для його відкритого ключа. Для декодування цього ключа без його приватного ключа потрібно врахувати це просте число, що може зайняти дуже багато часу на сучасних комп’ютерах. Суперкомп’ютеру знадобиться десь від тижня до місяця, щоб врахувати цей ключ.

Звичайно, варто враховувати обмеження, які накладаються від можливостей апаратного та програмного забезпечення смарт пристроїв.

Згідно з результатами досліджень, які проводив NIST (National Institute of Standards and Technology), з порівняння розмірів ключів RSA і ECC, необхідних для отримання однакового рівня захисту, еліптична криптографія може використовувати ключи довжиною у 160 біт аби забезпечити стійкість в 2048 біт RSA або 521 біт щоб забезпечити стійкість в 4096 біт RSA.

Останнім часом набирають популярності квантові комп'ютери. Квантові обчислення можуть використовувати квантові алгоритми для факторизації простого числа RSA за той самий проміжок часу, який потрібен звичайним комп'ютерам для його генерації. Це зробить усі дані, захищені поточним шифруванням із відкритим ключем, вразливими до атак квантових обчислень.

Інші методи шифрування так само вразливі для квантових обчислень. Хоча такі обчислення можуть загрожувати безпеці шифрування в майбутньому, вони у тому вигляді, як зараз існують, все ще дуже обмежені. На даний момент квантові обчислення не є комерційно доступними, не можуть обробляти великі обсяги коду і існують лише як обчислювальні пристрої, а не як комп'ютери. Крім того, квантові обчислення можна буде використовувати на користь шифрування. Так готуються стандарти пост-квантового шифрування на майбутнє.

Саме тому ще є певні причини зі створення можливостей, які дозволять прискорювати виконання вже існуючих алгоритмів. Не лише самі алгоритми можна оптимізувати, але й також оптимізувати виконання необхідної арифметики. Для більш наглядного прикладу необхідно виконувати дослідження на достатньо низькому рівні. А тому мета роботи - дослідити можливості еліптичної криптографії на пристроях з обмеженим об'ємом пам'яті.

Для реалізації авторами було обрано мікроконтролер Arduino. Arduino виступає у ролі найпростішого скалярного процесу, що обробляє один елемент даних за одну інструкцію. На мікроконтролері було реалізовано арифметику еліптичних кривих над простим полем Галуа: додавання точок і множення точки на число. Ця арифметика є базовою для генерації ключів, формування та верифікації електронного цифрового підпису. Мікроконтролер використовується для дослідження швидкості різних типів систем координат: афінна, стандартна проєктивна, система Якобі, система Чудновського-Якобі та змішанні системи Якобі.

Дослідження, що проводяться авторами, в змозі дати відповідь на питання, яка система найшвидша і має більший потенціал з впровадження в системи захисту для смарт-пристроїв. Економія апаратного часу з розрахунку базової арифметики дає зріст швидкодії смарт-пристрою із захистом і буде корисна не лише для пристроїв "Інтернету речей".

Авторами проведено аналіз математичних основ теорії скінченних полів та реалізація логіки мікроконтролеру на основі розглянутих алгоритмів з використанням мови програмування Arduino.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Жуков А. Е. Легковесная криптография [Текст] /А. Е. Жуков // Вопросы кибербезопасности. – 2015. – №1(9). – С. 26–43.