СУЧАСНІ АЛГЕБРАЇЧНІ КРИПТОСИСТЕМИ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ

"Дослідження сучасних алгебраїчних криптосистем"

1. Мета роботи

Дослідження особливостей реалізації сучасних алгебраїчних криптосистем на прикладі учасників першого раунду процесу стандартизації постквантової криптографії (NIST PQC).

2. Порядок і рекомендації щодо виконання роботи

Комп'ютерний практикум виконується бригадами, до складу яких входить один або двоє студентів.

3. Завдання на комп'ютерний практикум

Розробити програмну реалізацію обраного криптографічного алгоритму. Реалізація повинна містити всі можливі варіанти алгоритму.

Коректність реалізації підтвердити за допомогою тестів, які використовують за наявності офіційні тестові вектори або офіційну реалізацію. Знайти схожі алгоритми та провести порівняльний аналіз швидкодії за різних умов та використання модифікацій складових частин.

Навести повний теоретичний опис алгоритму з усіма деталями та відомими результатами досліджень. Провести теоретичний порівняльний аналіз обраного алгоритму зі схожими алгоритмами та дослідити можливість перенесення відомих атак на обраний алгоритм.

4. Криптографічні алгоритми:

Учасники першого раунду процесу стандартизації постквантової криптографії (NIST PQC) https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions.

5. Оформлення результатів роботи та звіту

Результатом роботи є всі тексти програм, скомпільовані виконувані файли (які мають запускатися на чистій ОС; якщо є потреба, можна використовувати контейнери), необхідна документація щодо використання програми з прикладами застосування та звіт.

Звіт до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт, за такими винятками:

– дозволяється використовувати шрифт Times New Roman 12pt та одинарний інтервал між рядками;

– дозволяється не починати нові розділи з окремої сторінки;

– дозволяється не включати анотацію, перелік термінів та позначень і перелік використаних джерел;

– не обов'язково оформлювати зміст.

Звіт має містити:

– мету проведення комп'ютерного практикуму;

– постановку задачі;

– хід виконання роботи, опис труднощів, що виникали, та шляхів їх подолання;

– детальний опис обраного криптографічного алгоритму та його складових частин;

– результати порівняльного аналізу швидкодії обраного алгоритму зі схожими алгоритмами (або модифікаціями алгоритму за допомогою заміни складових частин);

– огляд наявних результатів досліджень обраного алгоритму;

– результати порівняльного аналізу стійкості обраного алгоритму зі схожими алгоритмами з обґрунтуванням можливості застосування відомих атак;

– опис власних тестів, які проводилися з метою перевірки коректності реалізованої програми;

– детальний опис особливостей реалізації та приклади застосування;
– результати аналізу постквантової стійкості за наявними результатами аналізу;
– висновки до роботи.

Тексти програм не включати у звіт.

Комп'ютерний практикум вважається повністю виконаним після надіслання всіх текстів програм, скомпільованих виконуваних файлів, необхідної документації щодо використання програм з прикладами застосування, звіту та після захисту роботи. Дата захисту роботи назначається виключно після надсилання всіх необхідних матеріалів та їх перевірки за допомогою тестування коректності та швидкодії (включаючи перевірку на плагіат).

6. Оцінювання комп'ютерного практикуму

За виконання комп'ютерного практикуму кожен учасник бригади може одержати до 30 рейтингових балів; зокрема, оцінюються такі позиції:

– реалізація програми — до 10 балів (в залежності від правильності та швидкодії, за не проходження простих тестів можна отримати від'ємні бали, як і за використання чужої реалізації);
– оформлення звіту — до 4 балів;
– теоретичний аналіз алгоритму та результати проведеного порівняльного аналізу — до 10 балів;
– своєчасне поетапне виконання роботи — до 6 балів (детальніше далі);
– несвоєчасне виконання роботи — (-1) бал за кожен день пропуску.

Захист роботи передбачає питання по програмній реалізації та щодо проведеного аналізу, а також має на меті перевірити особистий вклад кожного з учасників бригади.

Виконання комп'ютерного практикуму містить два проміжних етапи:

15.11.2024 (3 бали) оформлений повний теоретичний опис алгоритму та реалізації основних алгебраїчних операцій, які використовує обраний алгоритм;

15.12.2024 (3 бали) реалізація алгоритму та результати проходження тестових даних.