УДК 004.056.5:512.623

Гущин Б.-Д. І.

ПОБУДОВА ПАКЕТНИХ ПОВНІСТЮ ГОМОМОРФНИХ СХЕМ НА ОСНОВІ МАТРИЧНИХ ПОЛІНОМІВ ДЛЯ ЕФЕКТИВНИХ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

У традиційних криптографічних системах для виконання обчислень над захищеними даними необхідне їх попереднє розшифрування, що створює потенційні ризики компрометації інформації та підвищує вимоги до довіреності середовища виконання. Одним із найбільш перспективних напрямів розв'язання цієї проблеми є застосування повністю гомоморфного шифрування, яке дозволяє виконувати арифметичні та логічні операції безпосередньо над зашифрованими даними. Попри значний прогрес у розвитку повністю гомоморфних схем, їх практичне використання обмежується високою обчислювальною складністю, великими обсягами шифротекстів і значними витратами криптографічних ресурсів [1, 2].

В зв'язку з цим особливого значення набувають пакетні схеми шифрування, які забезпечують одночасову обробку кількох незалежних повідомлень в одному шифротексті за принципом SIMD (Single Instruction Multiple Data). Одним із перспективних підходів до реалізації таких схем є використання матричних поліномів, які дозволяють ефективно організувати структуру шифротексту та оптимізувати виконання гомоморфних операцій.

Метою роботи є дослідження можливостей побудови пакетних повністю гомоморфних схем на основі матричних поліномів для підвищення ефективності криптографічної обробки даних у захищених інформаційно-комунікаційних системах.

Повністю гомоморфне шифрування базується на математичних конструкціях кільцевої алгебри, у межах яких відкриті тексти, ключі та шифротексти описуються

елементами спеціальних алгебраїчних структур. Одним із найефективніших сучасних підходів є використання поліноміальних кілець, у яких операції додавання та множення над шифротекстами відповідають аналогічним операціям над відкритими повідомленнями.

Матричні поліноми розширюють ці можливості шляхом представлення шифротексту у вигляді матриці, елементами якої є поліноми над визначеним кільцем. Така структура дозволяє одночасно кодувати декілька незалежних повідомлень у межах одного криптографічного контейнера.

Перевагою цього підходу є можливість організації пакетної обробки інформації, коли один гомоморфний оператор виконується паралельно над усіма слотами даних. Це суттєво знижує питомі витрати обчислювальних ресурсів на одну операцію.

У пакетних схемах шифрування використовується принцип SIMD, за якого:

- один шифротекст містить множину відкритих текстів;
- операції виконуються одночасно над усіма елементами;
- зменшується кількість необхідних шифротекстів;
- скорочується загальний час гомоморфних обчислень.

Особливо важливою є можливість внутрішньої перестановки слотів без розшифрування, що забезпечує гнучкість побудови складних обчислювальних схем. Практична реалізація такого підходу часто ґрунтується на використанні китайської теореми про залишки, яка забезпечує ефективне розкладання поліноміальних структур на незалежні обчислювальні компоненти, а також на методах інтерполяції матричних поліномів, що дозволяють формувати гнучкі схеми кодування даних у межах одного шифротексту. Додатково застосовується використання множин власних значень матриць, завдяки чому забезпечується оптимізація внутрішньої структури криптографічних перетворень і підвищується ефективність паралельного виконання гомоморфних операцій. Метод матричних поліномів має перевагу в керованості параметрами криптосистеми та забезпечує кращу адаптацію до різних типів навантажень.

Ключовим фактором ефективності є зменшення шуму, що накопичується під час послідовних гомоморфних операцій. Завдяки матричному поданню з’являється можливість більш рівномірного розподілу шумових компонент між слотами, що підвищує глибину допустимих обчислень без необхідності частого bootstrap-перетворення.

Пакетні повністю гомоморфні схеми на основі матричних поліномів можуть застосовуватися: у хмарних обчисленнях, захищених базах даних, системах делегованих обчислень, криптографічному машинному навчанні, сервісах конфіденційної аналітики [3, 4].

Особливо перспективним є їх використання в інфраструктурах, де необхідна паралельна обробка великих масивів конфіденційної інформації.

Проведене дослідження підтверджує, що побудова пакетних повністю гомоморфних схем на основі матричних поліномів є перспективним напрямом розвитку сучасної прикладної криптографії. Використання матричних структур дозволяє підвищити щільність кодування відкритих текстів, оптимізувати виконання гомоморфних операцій і зменшити обчислювальні витрати за рахунок паралельної обробки даних у межах одного шифротексту. Крім того, такий підхід сприяє підвищенню масштабованості криптографічних сервісів, забезпечуючи ефективніше використання обчислювальних ресурсів під час роботи з великими обсягами захищеної інформації. Отримані результати свідчать про доцільність подальших досліджень у напрямі адаптивного вибору параметрів матричних поліномів, оптимізації шумових характеристик та практичної реалізації таких схем на сучасних криптографічних бібліотеках.

Список використаних джерел

1. Гущин Б.-Д. І. Аналіз ефективності повністю гомоморфного шифрування шляхом використання матричних поліномів / Б.-Д. І. Гущин // Проблеми інформатизації: тези

доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла: [у 4 т.]. Т. 2: секції 3, 7 / Ін-т систем управління МНО Азербайджанської республіки, Національний технічний університет "Харківський політехнічний інститут", Харківський національний університет радіоелектроніки [та ін] – Харків : НТУ "ХПІ", 2025. – С. 86-87.

2. Гущин Б.-ДІ Проблемні питання застосування гомоморфного шифрування // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доповідей п’ятнадцятої міжнародної науково-технічної конференції, 24–25 квітня 2025 р.-Баку–Харків–Жиліна, 2025.–Т. 3–С. 114-115.– DOI: https://doi.org/10.32620/ICT. 25. t3.

3. Белей, О. І. (2018) «Гомоморфне шифрування даних у хмарних сховищах методом матричних поліномів», Сучасний стан наукових досліджень та технологій в промисловості, (4 (6), с. 5–14. doi: 10.30837/2522-9818.2018.6.005.

4. Покидько, Д.Ю. "ВИКОРИСТАННЯ МАТРИЧНИХ ПОЛІНОМІВ ДЛЯ ГОМОМОРФНОГО ШИФРУВАННЯ." *Актуальні питання забезпечення кібербезпеки та захисту інформації* (2023): 85.