УДК 004.056, 004.8
М.В. Онай, к.т.н., доцент, А.І. Северін
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна

МОДИФІКОВАНИЙ ПІДХІД ДЛЯ ПОБУДОВИ МАТРИЦІ МІЖБАЗИСНИХ ПЕРЕТВОРЕННЬ У $GF(p^m)$

M.V. Onai, PhD, Assoc. Prof., A.I. Severin

MODIFIED APPROACH FOR CONSTRUCTING THE CHANGE-OF-BASIS MATRIX IN $GF(p^m)$

Питання збереження приватності даних є важливим у сучасних інформаційних системах, зокрема при побудові систем аналізу даних та штучного інтелекту. Прикладами таких методів захисту таких даних є гомоморфне шифрування (наприклад, з використанням схеми Ель-Гамаля) і безпечні багатосторонні обчислення [1], що використовують арифметику скінчених полів (полів Галуа – $GF(p)$). У зв'язку з цим, задача розроблення нових методів виконання операцій над елементами полів Галуа, які мають низьку обчислювальну складність є актуальною.

Проведено порівняльний аналіз процесів виконання базових операцій (додавання, множення, обчислення мультиплікативного оберненого елемента, ділення, піднесення до степеня, операції Фробеніуса) над елементами скінченних полів типу $GF(p^m)$ у поліноміальному та нормальному базисах. Проаналізовано процес перетворення елементів з одного базису в інший. Досліджено способи перетворення між базисами в залежності від різних вхідних даних, зокрема параметрів p і m. Запропоновано модифікований підхід для побудови матриці перетворення між базисами [2], який полягає в обчисленні елемента нормального базису t^{p^i} за допомогою рекурентної формули $\alpha_{i+1} = t^{p^{i+1}} = t^{p^i \cdot p} = \prod_{j=1}^{p} t^{p^i} = (\alpha_i)^p$, замість класичних підходів: ділення на незвідний поліном та підстановок з незвідного поліному. Це дозволяє зменшити кількість виділеної пам'яті й пришвидшити виконання алгоритму.

Існуючі та запропоновані алгоритми були реалізовані мовою програмування C# в середовищі розробки Visual Studio 2015. Для проведення експериментальних досліджень розроблено програмне забезпечення, яке дозволяє виконувати обчислення з використанням поліноміального та нормального представлення елементів $GF(p^m)$, задавати різні вхідні параметри p і m, а також отримувати різні набори тестових даних залежно від нормальних поліномів $GF(p^m)$.

Отримані експериментальні результати методів і алгоритмів виконання операцій над елементами $GF(2^m)$ у заданих базисах показали, що запропонований підхід для побудови матриці перетворення дає збільшення швидкості у понад 5 разів для параметра $m > 12$.

Література

1. Block, A. R., Maji, H. K., & Nguyen, H. H. (2018). Secure Computation with Constant Communication Overhead using Multiplication Embeddings. doi:10.1007/978-3-030-05378-9_20.

2. Dychka, I. A., Legeza, V. P., Onai, M. V., & Severin, A. I. (2020). MODIFIED CHANGE-OF-BASIS CONVERSION METHOD IN $GF(2^m)$. Radio Electronics, Computer Science, Control, (2), 117–128. https://doi.org/10.15588/1607-3274-2020-2-12.