Ph.B. Burtyka

UMPHE: A Library for Effective Computing On Encrypted Data

Keywords: fully homomorphic encryption, unilateral matrix polynomials, software library.
The paper describes the design and implementation of a new software library that implements fully homomorphic encryption schemes based on unilateral matrix polynomials. The library is written in C++ using the NTL mathematical library and has multilayer structure. The main focus is on optimizations and batching techniques. The paper presents novel encryption and key generation algorithms for matrix polynomial based cryptosystems and techniques for data movement between the slots of the ciphertext.

Ф.Б. Буртыка

UMPHE: ПРОГРАММНАЯ БИБЛИОТЕКА ДЛЯ ОРГАНИЗАЦИИ ЭФФЕКТИВНЫХ ВЫЧИСЛЕНИЙ НАД ЗАШИФРОВАННЫМИ ДАННЫМИ[1]

Введение

Гомоморфное шифрование позволяет выполнять арифметические операции над зашифрованными данными без необходимости их предварительного расшифрования. Такое шифрование имеет ключевое значение на сегодняшний день в связи с потребностью обеспечения конфиденциальной обработки данных в недоверенных средах, например на облачных серверах. В настоящее время одним из важных вопросов, помимо разработки собственно гомоморфных криптосистем, является разработка библиотеки, поддерживающей весь спектр функций, необходимых программистам для организации полноценной обработки зашифрованных данных. В данной работе предлагается одно из решений этой задачи – библиотека UMPHE (сокращение от “Unilateral Matrix Polynomial Homomorphic Encryption”) [1]. В отличие от известных решений, таких как HELib [2], предлагаемая библиотека основывается на гомоморфном шифровании, использующем так называемые односторонние матричные полиномы [3–5] и являющемся более вычислительно эффективным, чем применяемое в HELib гомоморфное шифрование, основанное на сложных задачах теории решеток.

Библиотека UMPHE состоит из четырех уровней: 1) уровня реализации математических структур (операции с односторонними матричными полиномами); 2) уровня реализации базовых алгоритмов криптосистемы (зашифрования, расшифрования, генерации ключа гомоморфных криптосистем [3–5]), в случае пространства открытых текстов являющегося простым полем F_p; 3) уровня реализации пакетного режима работы криптосистем [5] (в данном режиме в один шифртекст зашифровывается сразу вектор открытых текстов из F_p, что позволяет повысить эффективность гомоморфных вычислений за счет возможности параллельной обработки нескольких наборов данных); 4) уровня виртуальных машинных команд (работа с 32- и 64-разрядными битовыми векторами: операции ADD, SUB, MULT, DIV, CMP, AND, XOR, NOT, SHR, SHL, ROL, ROR).

[1] Данная работа выполнена при финансовой поддержке РФФИ в рамках проектов 15-07-00597А и 16-37-00125 мол_а.

Реализация математических структур

Односторонние матричные полиномы представляются массивом матриц-коэффициентов с элементами из F_p. Умножение, сложение, деление матричных полиномов реализованы с использованием обычных алгоритмов умножения матриц по модулю p из библиотеки NTL [7]. Для вычислений значения матричного полинома в точке и операции композиции с другим односторонним матричным полиномом (совместимым по размерности с исходным) применяется схема Горнера. Реализована процедура построения интерполяционного матричного полинома степени d по заданному набору пар (аргумент, значение) $(\mathbf{X}_i \in \mathrm{F}_p^{n\times n}, \mathbf{Y}_i \in \mathrm{F}_p^{n\times n}), i = \overline{1,d}$.

Реализация процедур генерации ключа, шифрования и расшифрования

Для генерации ключа [3–5] осуществляется генерация случайного набора матриц-коэффициентов, после которой оценивается размерность полученного пространства ключей, и в случае его достаточной размерности в качестве ключа сохраняются базисные векторы. В процессе шифрования происходит генерация случайного вектора матриц-коэффициентов по равномерному распределению, коэффициенты вектора используются для линейного комбинирования базисных векторов пространства ключей. Расшифрование осуществляется с помощью алгоритмов деления односторонних матричных полиномов.

Реализация пакетных операций и перемещение данных между слотами без расшифрования

Слотом с номером i, согласно [2], называется i-й открытый текст, зашифрованный в шифртекст в пакетном режиме. Так же, как и в [2], в UMPHE была реализована операция перемещения открытых текстов между слотами в пакетных шифртекстах. Эта операция нужна для получения возможности более широкого использования пакетной обработки зашифрованных данных, чем просто параллельное вычисление одной и той же функции над несколькими зафиксированными заранее наборами открытых текстов.

Перемещение данных между слотами шифртекстов осуществляется посредством вычисления композиции шифртекстов со специальным образом составленными матричными полиномами.

Реализация условных операций, сравнения и ветвлений

Для реализации операций сравнения (CMP) и ветвления предусмотрено выражение логических операций дизъюнкции и отрицания через полиномы Жегалкина. Процедура CMP использует следующий алгоритм: для двух *N*-разрядных чисел A и B, разряды которых обозначаются A_i и B_i соответственно, зашифрованный предикат равенства вычисляется как $\prod_{i=0}^{N-1} A_i \cdot B_i \oplus (A_i \oplus 1)\cdot(B_i \oplus 1)$. Предикат, проверяющий сравнение на неравенство:

$$("A < B") = (A_{n-1} \oplus 1)B_{n-1} \oplus x_{n-1}(A_{n-2} \oplus 1)B_{n-2} \oplus \ldots \oplus x_{n-1}\ldots x_2(A_1 \oplus 1)B_1 \oplus x_{n-1}\ldots x_1(A_0 \oplus 1)B_0,$$

где $x_i = A_i \cdot B_i \oplus (A_i \oplus 1)\cdot(B_i \oplus 1)$. Ветвление программы организуется с помощью гомоморфного вычисления выражения-переключателя $\overline{condition}\cdot v_0 \oplus condition \cdot v_1$ (см. [6]),

где v_0 ветка программы, вычисляемая при $condition = 0$, а v_1 ветка, вычисляемая при $condition = 1$.

Выводы

Описанная библиотека может быть использована для организации многоразрядных гомоморфных вычислений: целочисленных операций с данными, а также операций с плавающей точкой, и поддерживает любые вычисления с фиксированной разрядностью аргументов и результата, включая, сортировку зашифрованных данных, нахождение максимального/минимального элемента в зашифрованном массиве, другие оптимизационные задачи. Вычисления же с нефиксированной разрядностью результата требуют специальных криптографических протоколов и являются темой для дальнейших исследований и усовершенствований библиотеки.

СПИСОК ЛИТЕРАТУРЫ:

1. Буртыка Ф.Б, UMPHE – реализация гомоморфного шифрования, основанного на использовании односторонних матричных полиномов. [Электронный ресурс] URL:
https://github.com/bbfilipp/UMPHE (дата обращения 03.02.2016)
2. Halevi S., Shoup V. Algorithms in HELib // Advances in Cryptology–CRYPTO 2014. – Springer Berlin Heidelberg, 2014. P. 554–571.
3. Burtyka P. and Makarevich O. Symmetric fully homomorphic encryption using decidable matrix equations // In Proceedings of the 7th International Conference on Security of Information and Networks. Pp. 186–198. ACM, 2014.
4. Буртыка Ф.Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия Южного федерального университета. Технические науки. 2014. Т. 157. № 8. С. 107–122.
5. Буртыка Ф.Б. Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов // Труды Института системного программирования РАН. 2014. Т. 26. № 5. С. 99–115.
6. Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В. Защищенные вычисления и гомоморфное шифрование // Труды Национального суперкомпьютерного форума (НСКФ-2014), ИПС им. АК Айламазяна РАН, г. Переславль-Залесский.
7. ShoupV. Numbertheorylibrary 5.5. 2 (NTL) for C++.

REFERENCES:

1. Burtyka Ph.B, UMPHE – an implementation of homomorphic encryption, based on using unilateral matrix polynomials. URL:https://github.com/bbfilipp/UMPHE (Accessed 03.02.2016)
2. Halevi S., Shoup V. Algorithms in HELib //Advances in Cryptology–CRYPTO 2014. – Springer Berlin Heidelberg, 2014. P. 554-571.
3. Burtyka P. and Makarevich O. Symmetric fully homomorphic encryption using decidable matrix equations // In Proceedings of the 7th International Conference on Security of Information and Networks. Pp. 186–198. ACM, 2014.
4. Burtyka Ph.B. Simmetrichnoe polnost'ju gomomorfnoe shifrovanie s ispol'zovaniem ne-privodimyh matrichnyh polinomov [Symmetric Fully Homomorphic Encryption Using Undecidable Matrix Polynomials].Izvestija Juzhnogo federal'nogo universiteta.Tehnicheskie nauki [Transactions of Southern Federal University. Engineering science]. 2014. Vol. 157. №. 8. Pp. 107–122. (in Russian).
5. Burtyka Ph.B. Paketnoe simmetrichnoe polnost'ju gomomorfnoe shifrovanie na osnove matrichnyh polinomov. [Batch Symmetric Fully Homomorphic Encryption Based on Matrix Polynomials] // Trudy ISP RAN [The Proceedings of ISP RAS]. 2014. № 5. Vol. 26. Pp. 99–115 (in Russian).
6. Babenko L.K., Burtyka Ph. B., Makarevich O.B., Trepacheva A.V. Protected computations and homomorphic encryption // The proceedings of National Supercomputer Forum (NSKF-2014), Pereslavl'-Zalessky.
7. Shoup V. Number theory library 5.5. 2 (NTL) for C++.