ИСПОЛЬЗОВАНИЕ ПОСЛЕДОВАТЕЛЬНОЙ И ПАРАЛЛЕЛЬНОЙ КОМПОЗИЦИИ ПРИ ПОСТРОЕНИИ ИТЕРАТИВНЫХ АЛГОРИТМОВ КРИПТОГРАФИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ, ОРИЕНТИРОВАННЫХ НА РЕАЛИЗАЦИЮ С ИСПОЛЬЗОВАНИЕМ СУПЕРКОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Иванов М.А., Васильев Н.П., Ровнягин М.М., Скитев А.А., Спиридонов А.А., Чугунков И.В.

Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)

Жизнь современного общества немыслима без повсеместного использования компьютерных систем (КС), связанных с вводом, хранением, обработкой и выводом информации. Всеобщая компьютеризация, помимо очевидных выгод, несет с собой и многочисленные проблемы, наиболее сложной из которых является проблема информационной безопасности. Высочайшая степень автоматизации, к которой стремится человечество, широкое внедрение дешевых компьютерных систем массового применения и спроса делают их чрезвычайно уязвимыми по отношению к деструктивным воздействиям, ставят современное общество в зависимость от степени безопасности используемых информационных технологий. Важнейшей характеристикой любой КС, независимо от ее сложности и назначения, стала безопасность обрабатываемой в ней информации.

Информационная безопасность давно стала самостоятельным направлением исследований и разработок. Однако, несмотря на это, проблем не становится меньше. Это объясняется появлением всё новых компьютерных технологий (суперкомпьютерных, мобильных и пр.), которые не только создают новые проблемы информационной безопасности, но и представляют, казалось бы, уже решенные вопросы совершенно в новом ракурсе. Кроме того, появление новых компьютерных технологий, новых математических методов дают в руки нарушителей и создателей разрушающих программных воздействий (РПВ) все новые и новые возможности [1]. Главная причина трудоемкости решения задачи обеспечения безопасности информации в современных условиях – всё большее отстранение пользователей от процессов управления и обработки информации и передача его ПО, обладающему некоторой свободой в своих действиях и поэтому очень часто работающему вовсе не так, как предполагает пользователь.

С развитием суперкомпьютерных технологий (СКТ) ситуация принципиально изменилась, причем на первый взгляд в худшую сторону. С появлением суперкомпьютеров стало намного проще решать задачи полного или частично-полного перебора, а именно таковыми являются задачи, связанные с компрометацией систем защиты информации, в частности задачи взлома криптоалгоритмов и криптопротоколов, задачи поиска уязвимостей программных систем. Полный перебор вариантов это универсальный метод решения подобных задач, вероятность его успеха всегда равна единице. Именно с появлением суперкомпьютеров получила широкое распространение простая и эффективная технология фаззинга, суть которой – автоматический поиск уязвимостей атакуемой системы методом грубой силы. Такая атака, основанная на модели «чёрного ящика», хотя и не всегда является наилучшим выбором, практически всегда возможна. Ее основными преимуществами являются доступность, простота и воспроизводимость, которые невозможно получить при использовании других методов [2].

Новый стимул в развитии получают атаки, основанные на использовании криптографии против криптографии. Многие скрытые каналы утечки информации из криптосистем для своего использования требуют именно решения задач частично-полного перебора. С появлением суперкомпьютеров требования к пропускной способности таких каналов существенно снижаются [1, 3, 4]. РПВ, использующие скрытые каналы воздействия на объект, а также приема и передачи информации, уже появились. Совершенствование методов поиска уязвимостей КС, создающих предпосылки для проведения атак, основанных на вставке кода, привело к увеличению фактов обнаружения РПВ, использующих уязвимости нулевого дня (Zero day vulnerabilities). Совершенно очевидно, что в самое ближайшее время будут обнаружены РПВ, которые при функционировании для затруднения своего выявления и нейтрализации приме-

няют СКТ, в частности, гибридные. В результате антивирусы, использующие традиционные реактивные методы защиты, окажутся не в состоянии справиться с новой угрозой. Необходимо опережающее совершенствование методов и средств защиты от РПВ.

Однако не все так плохо. Новый стимул в развитии получает и защищающаяся сторона. Разработка алгоритмов защиты информации, в частности криптоалгоритмов, обладающих высокой степенью параллелизма на уровне элементарных операций и по этой причине эффективно реализуемых с использованием СКТ, позволит избавиться от одного из самых серьезных недостатков современных криптоалгоритмов – низкого быстродействия. Высокая степень параллелизма позволит эффективно решать задачи, связанные с запутыванием программной реализации криптоалгоритмов. Появится возможность практического воплощения идеи У. Маурера, сутью которой является построение самосинхронизирующихся шифров на основе последовательной и параллельной композиции раундовых преобразований [5]. Наконец, появление СКТ создает предпосылки для создания всеобъемлющей методики комплексного анализа защищенности компьютерных систем на всех уровнях – элементная база, архитектура, системное и сетевое ПО, прикладное ПО, иными словами реализации процессного подхода к обеспечению безопасности информации.

Наиболее подходящей для реализации на GPU является двухмерная архитектура Квадрат, предложенная авторами криптоалгоритмов Square и Rijndael, при этом последний в 2001 г. победил в конкурсе на принятие нового Американского стандарта криптозащиты AES (Advanced Encryption Standard). В версии AES-128 все входные и выходные блоки данных, все промежуточные результаты преобразований, все раундовые ключи представляются в виде квадратного массива байтов 4 × 4 (State), таким образом, разрядность всех блоков данных равна 128 битам. В состав раунда входят операции *SubBytes*(*State*) – замены байтов, *ShiftRows*(*State*) – циклического сдвига строк на различное число байтов, *MixColumns*(*State*) – перемешивания столбцов и *AddRoundKey*(*State, K*$_i$) – сложения (XOR) с раундовым ключом [6, 7].

При этом при построении функции шифрования E используется только последовательная композиция раундовых преобразований RF_i: $E = RF_n \bullet RF_{n-1} \bullet \ldots \bullet RF_2 \bullet RF_1$, где n – число раундов; в результате для обеспечения требуемого уровня криптостойкости необходимо выполнение большого числа раундов.

Предлагается строить раундовые преобразования RF_i на основе последовательной и параллельной композиции раундовых функций шифрования, например, аналогичных AES-128. Основная идея данной конструкции – построение последовательностной машины, количество элементов памяти которой превышает разрядность входной памяти. Подобный подход к построению блочных итеративных шифров ранее не применялся, его использование при программной реализации криптографических преобразований стало возможным в связи появлением гибридных СКТ [8–10]. В результате стало возможным в пределах раунда параллельно (иначе говоря, без ущерба для быстродействия) выполнять различные траектории сложных преобразований, а затем на выходе осуществлять параллельную композицию полученных результатов. Таким образом задача инвертирования функции шифрования становится вычислительно неразрешимой при меньшем числе раундов преобразования.

Рассмотрим принципы построения итеративного алгоритма криптографической обработки данных с использованием последовательной и параллельной композиции элементарных преобразований (рис. 1). Внутри каждого раунда по сути происходит формирование N копий входного блока, каждая копия C_{ij} подвергается стохастическому преобразованию $C_{ij} := E_{ij}(C_{ij}, K_{ij})$, где K_{ij} – раундовые подключи i-го раунда, $j = 1, 2, \ldots, N$. Преобразованные значения C_{ij} поступают на входы комбинационной схемы F_i, функцией которой является параллельная композиция различных траекторий раундовых преобразований, результат действия комбинационной схемы $C := F_i(C_{i1}, C_{i2}, \ldots, C_{iN})$ объявляется результатом i-го раунда.

Последовательность преобразований имеет следующий вид:

Формирование по входному блоку M блока C в соответствии с выражением $C := M$.

1-й раунд преобразования. При выполнении первого раунда создается N копий $C_{11}, C_{12}, \ldots, C_{1N}$ входного блока данных C, каждая копия C_{1j} подвергается стохастическому преобразованию, которое записывается в виде $C_{1j} := E_{1j}(C_{1j}, K_{1j})$, где K_{1j} – раундовые подключи первого раунда, преобразованные значения C_{1j} поступают на входы комбинационной схемы F_1, функ-

цией которой является параллельная композиция результатов выполнения различных траекторий раундовых преобразований, результат действия комбинационной схемы $C := F_1(C_{11}, C_{12}, \ldots, C_{1N})$ объявляется результатом первого раунда. Полученное значение поступает на вход второго раунда.

2-й раунд преобразования. При выполнении второго раунда создается N копий $C_{21}, C_{22}, \ldots, C_{2N}$ входного блока данных C, каждая копия C_{2j} подвергается стохастическому преобразованию, которое записывается в виде $C_{2j} := E_{2j}(C_{2j}, K_{2j})$, где K_{2j} – раундовые подключи второго раунда, преобразованные значения C_{2j} поступают на входы комбинационной схемы F_2, результат действия которой $C := F_2(C_{21}, C_{22}, \ldots, C_{2N})$ объявляется результатом второго раунда. Полученное значение поступает на вход третьего раунда.

…

n-й раунд преобразований. При выполнении последнего раунда создается N копий $C_{n1}, C_{n2}, \ldots, C_{nN}$ входного блока данных C, каждая копия C_{nj} подвергается стохастическому преобразованию, которое записывается в виде $C_{nj} := E_{nj}(C_{nj}, K_{nj})$, где K_{nj} – раундовые подключи n-го раунда, преобразованные значения C_{nj} поступают на входы комбинационной схемы F_n, результат действия которой $C := F_n(C_{n1}, C_{n2}, \ldots, C_{nN})$ объявляется результатом n-го раунда. Полученное значение является результатом итеративного криптографического преобразования блока данных M.

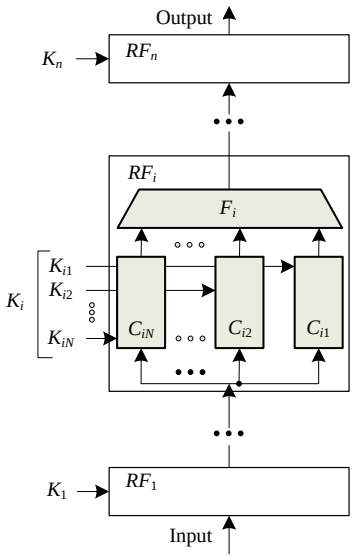

Рис. 1 – Использование параллельной и последовательной композиции при построении итеративного стохастического преобразования

На рис. 2 показан пример построения итеративного алгоритма криптографической обработки данных, где параллельная композиция выполняется с использованием операции сложения по модулю два, а $C_{ij} = MixColumns \bullet MixRows \bullet SubBytes \bullet AddThreadKey$. На рис. 3 показан пример реализации процедуры «разворачивания» ключа, иначе говоря, процесс получения раундовых ключей из исходного ключа K, где RC_{ij} – раундовые константы.

На рис. 4 показаны варианты построения комбинационной схемы F_i.

Рассмотрим пример реализации криптографического преобразования C_{ij}. Все блоки входных данных, все промежуточные результаты, все раундовые подключи K_{ij} имеют разрядность 128 бит и представляются в виде квадратного массива байт 4 × 4. Последовательность операций при выполнении простейшего преобразования C_{ij} имеет следующий вид:

- сложение по модулю два (XOR) входного блока и раундового подключа K_{ij};
- разбиение результата на байты и выполнение для каждого байта операции замены с использованием таблицы H_j размерностью 8 × 256;
- разбиение результата на строки и выполнение для каждой строки операции *MixRow*;
- разбиение результата на столбцы и выполнение для каждого столбца операции *MixColumn*.

Преобразования MixRow и MixColumn суть умножение соответственно строки и столбца на *MDS*-матрицу (Maximum Distance Separable) в поле $GF(2^8)$ [11].

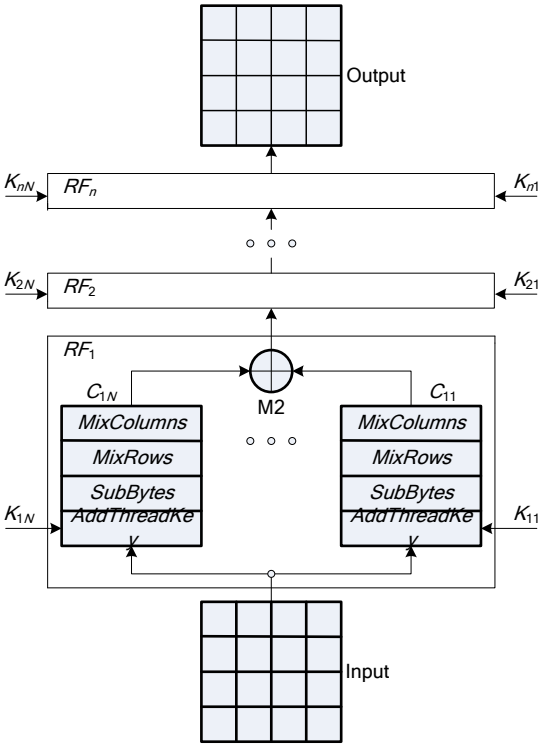

Рис. 2 – Структура итеративного криптографического преобразования

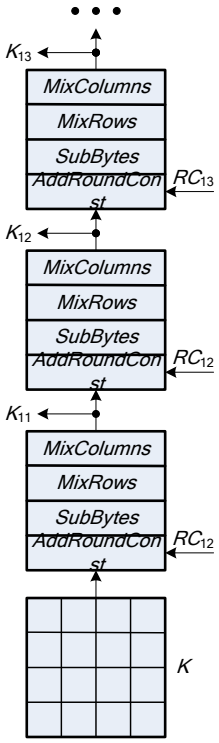

Рис. 3 – Вариант реализации процедуры «разворачивания» ключа

На рис. 5 показан пример построения на основе предложенного способа итеративного криптографического преобразования самосинхронизирующегося поточного шифра, где m_i, c_i – соответственно блоки открытого и шифротекста, S_0, S_i – соответственно начальное и i-е состояния элементов памяти Q ГПСЧ. Схема, показанная на рис. 5,*а* может быть взята за основу при построении криптографической функции хеширования.

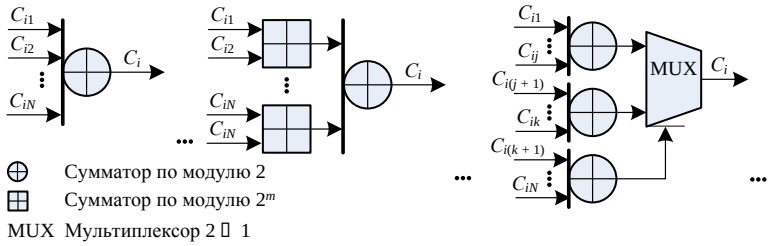

Рис. 4 – Варианты реализации комбинационной схемы F_i

Таким образом, особенностью предлагаемого способа построения итеративного криптографического преобразования является высокая степень параллелизма при выполнении различных траекторий раундовых преобразований, что обеспечивает увеличение быстродействия при его реализации с использованием гибридных СКТ. Для программной реализации наиболее целесообразной представляется технология CUDA (Compute Unified Device Architecture – вычислительная унифицированная архитектура устройств) от компании NVIDIA. Очевидно, что в пределах каждого раунда все траектории преобразований могут быть обработаны параллельно, а применение CUDA позволит существенно упростить процесс разработки ПО.

Аналогично могут быть реализованы и трехмерные итеративные криптоалгоритмы. Рассмотренный принцип построения стохастических преобразований данных может быть использован и при проектировании функции обратной связи или функции выхода многомерных генераторов псевдослучайных чисел [12, 13].

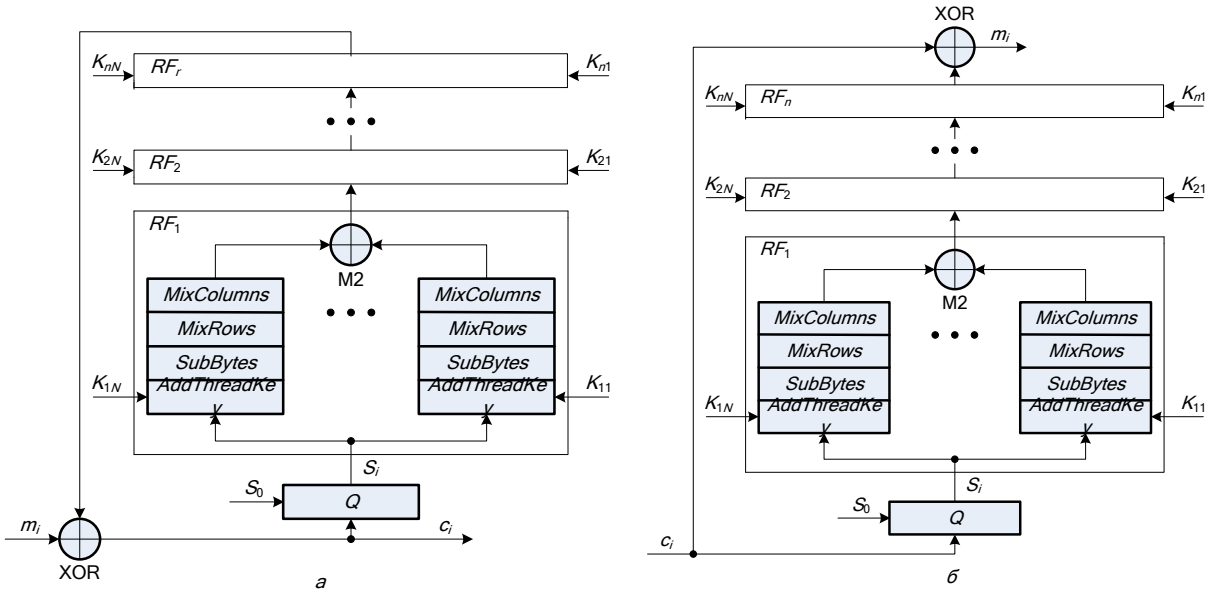

Рис. 5 – Пример построения самосинхронизирующегося поточного шифра:
а – схема зашифрования; *б* – схема расшифрования

Литература

1. Разрушающие программные воздействия / А.Б. Вавренюк, Н.П. Васильев, М.А. Иванов и др. Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011.
2. Kozirsky B.L., Komarov T.I. Fuzzing – a perspective method of searching software vulnerabilities. Proceedings of RES-2013, Moscow, pp. 160-163.
3. Chepik N.A. Kleptographic attacks on ECDSA. Proceedings of RES-2013, Moscow, pp. 163-166.
4. Клептографические атаки на криптосистемы с открытым ключом / З.Р. Гарифуллина, М.А. Иванов, А.В. Ковалев, Н.А. Чепик // Вестник НИЯУ МИФИ, 2012, том 1, № 2.
5. Поточные шифры / А.В. Асосков, М.А. Иванов, А.А. Мирский и др. М.: Кудиц-Образ, 2004.
6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях / Под ред. М.А. Иванова. М.: НИЯУ МИФИ. 2012. [Электронный ресурс] : URL http://library.mephi.ru/Data/book-mephi/Ivanov_Kriptograficheskie_metody_zaschity_informacii_v_kompjuternyh_2012.pdf
7. Daemen J., Rijmen V. AES Proposal: Rijndael. [Электронный ресурс] : URL http://csrc.nist.gov/archive/aes/ rijndael/Rijndael-ammended.pdf
8. Боресков А.В., Харламов А.А. Основы работы с технологией CUDA. М.:ДМК Пресс, 2011.
9. CUDA Toolkit. [Электронный ресурс] : URL http://developer.nvidia.com/cuda-toolkit
10. NVIDIA Parallel Nsight. [Электронный ресурс] : URL http://developer.nvidia.com/nvidia-parallel-nsight
11. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
12. Трехмерный генератор псевдослучайных чисел, ориентированный на реализацию в гибридных вычислительных системах / М.А. Иванов, Н.П. Васильев, А.А. Максутов и др. // Вестник НИЯУ МИФИ, 2012, том 1, № 2.
13. Иванов М.А., Васильев Н.П., Чугунков И.В. Трехмерные алгоритмы стохастического преобразования данных, ориентированные на реализацию с использованием гибридных суперкомпьютерных технологий. [Электронный ресурс] : URL http://2012.nscf.ru/Tesis/Ivanov.pdf

Аннотация

Предлагается новый способ построения итеративных криптиографических алгоритмов обработки данных, основанный на использовании последовательной и параллельной композиции элементарных преобразований. Приводится пример его использования при построении самосинхронизирующегося поточного шифра.

Ключевые слова: итеративный блочный шифр, генератор псевдослучайных чисел, самосинхронизирующийся поточный шифр, AES.

Сведения об авторах

Авторы статьи – преподаватели и аспиранты кафедры Компьютерных систем и технологий факультета Кибернетики и информационной безопасности НИЯУ МИФИ.

Контактная информация: тел. 8-926-558-60-99, email: MAIvanov@mephi.ru, Иванов Михаил Александрович, д.т.н., проф., зав. кафедрой КСиТ НИЯУ МИФИ

USING SEQUENTIAL AND PARALLEL COMPOSITION FOR CRYTOGRAPHIC DATA PROCESSING FOR HETEROGENEOUS SUPERCOMPUTER IMPLEMENTATION

A new method of designing nonlinear iterative data transformation aimed for usage in the field of information security is introduced . The essence of the proposed method is usage of sequential and parallel composition of elementary cryptographic data processing operations.

Keywords: iterative block cipher, pseudorandom number generator, self-synchronized stream cipher, AES.