УДК 004.056.55

РЕАЛИЗАЦИЯ ФУНКЦИИ ВЫБОРА В МОДИФИЦИРОВАННОЙ СХЕМЕ SPONGE ПРОЕКТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ

Сисенов Нурбек Маханбетулы, Оспанов Руслан Маратович,
Ергалиева Бану Бахытжановна, Жетписбаева Айнур Турсынкановна

nurbek9291@mail.ru
Научные сотрудники НИИ информационной безопасности и криптологии
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Е.Н. Сейткулов

Введение. Криптографическая хеш-функция относится к основным и базовым криптографическим примитивам, таким как симметричные блочные шифры, поточные шифры, генерация псевдослучайных чисел и т.д. Она является основой для создания эффективных средств криптографической защиты информации для обеспечения информационной безопасности в различных информационных системах. Криптографические хеш-функции используются в огромном количестве приложений, протоколов и схем, например, защита информации с помощью паролей, цифровые подписи, проверка подлинности сообщений, проверка корректности шифротекста, доказательство знания, генераторы псевдослучайных чисел, функции формирования ключей и другие.

В настоящее время наиболее популярной и перспективной схемой построения криптографических хеш-функций является схема “Sponge” (“криптографическая губка”) [1], [2]. По этой схеме был спроектирован алгоритм Keccak [3], ставший победителем конкурса SHA-3. Схема “Sponge” - простая итерационная схема для построения криптографической хеш-функции на основе некотрой внутренней функции f, являющейся преобразованием фиксированной длины или перестановкой, оперирующей с фиксированным числом b битов, составляющих так называемое внутреннее состояние S. Причем b = r + c. Значение r называется битовой скоростью, а значение c — мощностью. Внутреннее состояние S сначала инициализируется некоторым фиксированным значением. Затем, после соответствующего дополнения и разделения сообщения на r-битные фрагменты, просто и итеративно обрабатываются все r-битные фрагменты сообщения, путем побитового сложения их r битам внутреннего состояния, а затем применяя b-битную функцию f. После того, как все блоки сообщений обрабатываются этим процессом «впитывания», последовательно выводятся r битов конечного хеш-значения путем извлечения r битов из внутреннего состояния и последующего применения к нему функции f (процесс «выжимания»).

К настоящему времени уже разработано множество алгоритмов по этой схеме, а также разработаны различные модификации схемы. Модификации используют различные способы дополнения, реализуют множество разных вариантов инициализации состояния, применяют множество различных преобразований и перестановок в качестве внутренних функций. Классическая схема “Sponge” и большинство ее модификаций предполагают в своем составе только одну внутреннюю функцию. Внутренняя функция является основным и важным компонентом схемы “Sponge”, представляющая собой преобразование фиксированной длины или перестановку, оперирующей с фиксированным числом битов, составляющих внутреннее состояние функции.

Выбор внутренней функции из заданного множества. В работе [4] предлагается новая схема “Enhanced Sponge Function (ESF)”, которая предполагает использование двух внутренних функций в отличии от “классической” схемы “Sponge”, в которой используется только одна внутренняя функция. Порядок работы этих двух внутренних функций в составе всей схемы определяется с помощью зависящего от сообщения ключа, сгенерированного псевдослучайным образом. Генерирование ключевого бита выполняется следующим образом: к входному сообщению применяется корректор фон Неймана, затем к полученной в результате последовательности битов применяем XOR корректор, и получаем ключевой бит. С помощью ключевого бита осуществляется выбор одного из двух заданных внутренних функций следующим образом. Первые r бит состояния S последовательно подаются на информационный вход одного 1-2 демультиплексора, на адресный вход которого подается ключевой бит, а остальные c бит состояния S последовательно подаются на информационный вход другого 1-2 демультиплексора, на адресный вход которого также подается ключевой бит; затем к полученным на выходе битам (преобразованному значению

состояния) применяется функция f0, если ключевой бит - 0, или применяется функция f1, если ключевой бит – 1.

В работах [5], [6] предлагается модификация схемы “Sponge”, которая предполагает использование уже множества внутренних функций. Согласно этой схеме над входным сообщением выполняются следующие преобразования из заданного множества внутренних функций выбирается функция f с помощью функции выбора. В случае множества двух функций можно применить способ, изложенный выше [4].

В данной работе рассматривается случай, когда в схеме задается множество трех внутренних функций Fi, i=0,1,2.

Функция выбора определяется следующим образом.

Входное сообщение делится на две части. Если длина m сообщения является четным числом, то делится на две части одинаковой длины, а если не четным, то две части с длинами $\left[\frac{m}{2}\right]+1$ и $\left[\frac{m}{2}\right]$.

Генерируется первый бит выбора. Для этого к первой части входного сообщения применяют корректор фон Неймана, т.е. биты входного сообщения рассматриваются парами: если в паре два одинаковых значения, то пара отбрасывается, если биты разные, то вместо пары записывается только первый бит в этой паре. Затем к результату применяют XOR корректор, т.е. все биты получившейся последовательности складываются по модулю 2. В результате получается первый бит выбора. Аналогичным образом генерируется второй бит выбора, применяя корректор фон Неймана и XOR корректор к второй части входного сообщения.

Первые r бит состояния S последовательно подаются на информационный вход первого 1-2 демультиплексора, на адресный вход которого подается первый бит выбора, а остальные c бит состояния S последовательно подаются на информационный вход второго 1-2 демультиплексора, на адресный вход которого также подается первый бит выбора. Если бит выбора - 0, то полученные на выходе биты первого 1-2 демультиплексора подаются на информационный вход третьего 1-2 демультиплексора, на адресный вход которого подается второй бит выбора, а полученные на выходе второго 1-2 демультиплексора подаются на информационный вход четвертого 1-2 демультиплексора, на адресный вход которого также подается второй бит выбора. Далее к полученным на выходе r+c битам будет применена внутренняя функция F0, если второй бит выбора - 0, или будет применена внутренняя функция F1, если второй бит выбора - 1. Если же первый бит выбора – 1, то к полученным на выходе r+c битам будет применена внутренняя функция F2.

Заключение. В данной работе рассматривается реализация функции выбора внутренней функции из заданного множества для модифицированной схемы “Sponge” проектирования криптографических хеш-функций. Функция выбора построена для случая, когда в схеме задается множество трех внутренних функций Fi, i=0,1,2. Выбор одной из этих трех внутренних функций в составе всей схемы определяется с помощью зависящих от сообщения битов выбора, сгенерированных псевдослучайным образом.

Информация о поддержке. Данная работа выполнена при финансовой поддержке грантового финансирования МЦРИАП, № AP06851124.

Список использованных источников

1. Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche. Sponge Functions. Ecrypt Hash Workshop 2007.
2. Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche Cryptographic sponge functions, Version 0.1, January 14, 2011, https://keccak.team/files/CSF-0.1.pdf
3. Bertoni G., Daemen J, Peeters M., Van Assche G. The Keccak reference. SHA-3 competition (round 3), 2011, https://keccak.team/sponge_duplex.html.

4. Magdy M. Saeb. An Enhanced Sponge Function (ESP). International Journal of Computer Science & Communications Security IJCSCS, July 2012. https://www.researchgate.net/publication/230646378
5. Оспанов Р.М., Сейткулов Е.Н., Арапов Н.К., Ергалиева Б.Б. Модификация схемы построения криптографических хеш-функций SPONGE // Вестник КазНИТУ. -2020. -№ 5 (141). -С.520-525.
6. Оспанов Р.М., Сейткулов Е.Н. Киберщит: О различных реализациях схемы построения криптографических хэш-функций «Sponge» // Материалы Международной научно-практической Web-конференции «Военно-техническое обеспечение деятельности вооруженных сил: мировой опыт и тенденции развития». Нур-Султан: Из-во НУО. -2020. -С.305-308.