**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.**

**SHA-3 Стандарт: Хеш-функции на основе перестановок и функции расширенного вывода (XOFs)**

**Аннотация**

Настоящий стандарт определяет семейство функций алгоритма безопасного хеширования (**Secure Hash Algorithm-3, SHA-3**) для двоичных данных. Каждая из функций SHA-3 основана на требованиях, установленных алгоритмом ***KECCAK***, который Национальным институтом стандартов и технологий США (**NIST – National Institute of Standards and Technology**) был выбран в качестве победителя конкурса **SHA-3 Cryptographic Hash Algorithm**. Это стандарт также определяет семейство математических перестановок ***KECCAK-p***, включающих перестановку, лежащую в основе *KECCAK*, для облегчения разработки дополнительных криптографических функций на основе перестановок.

Семейство SHA-3 состоит за четырёх криптографических хеш-функций: SHA3-224, SHA3-256, SHA3-384 и SHA3-512; и двух функций расширенного вывода (**XOFs**): SHAKE128 и SHAKE256.

Хеш-функции являются компонентами многих важных приложений информационной безопасности, в частности: 1) генерация и верификация цифровых подписей; 2) формирование ключа; 3) генерация псевдослучайных битов. Хеш-функции, определенные в настоящем стандарте, дополняют хеш-функцию SHA-1 и семейство хеш-функций SHA-2, определенных в стандарте **FIPS (Federal Information Processing Standards) 180-4, the Secure Hash Standard**.

Функции расширенного вывода отличаются от хеш-функций, но их можно использовать аналогичным образом и гибко адаптировать непосредственно к требованиям конкретных приложений с учетом дополнительных соображений безопасности.

**1. Наименование стандарта:** Стандарт SHA-3: Хеш-функции, основанные на перестановках, и функции расширенного вывода (**FIPS PUB 202**).

**2. Категория стандарта:** Стандарт компьютерной безопасности, криптография.

**3. Объяснение:** Настоящий стандарт (FIPS 202) определяет семейство функций алгоритма криптографического хеширования (SHA-3) для двоичных данных. Каждая из функций SHA-3 базируется на принципах алгоритма *KECCAK*, который NIST выбрало в качестве победителя конкурса SHA-3 Cryptographic Hash Algorithm Competition. Это стандарт также определяет семейство математических перестановок *KECCAK-p*, включающих перестановку, лежащую в основе *KECCAK*. Указанные перестановки могут служить основными компонентами дополнительных криптографических функций, которые могут быть определены в будущем.

Семейство SHA-3 состоит из четырёх криптографических хеш-функций и двух функций расширенного вывода (XOFs). Криптографические хеш-функции: SHA3-224, SHA3-256, SHA3-384 и SHA3-512; функции расширенного вывода: SHAKE128 и SHAKE256.

Данные на входе хеш-функций называются **сообщением** (**message**), a на выходе – **дайджестом** (**digest**) или «хешем» (**hash value**). Сообщение может иметь различную длину, длина дайджеста **фиксирована**. Криптографическая хэш-функция – это хэш-функция, которая обладает специальными свойствами, включающими в себя сопротивление коллизиям (**collision resistance**) и сопротивление прообразу (**preimage resistance**), которые важны для многих приложений в области информационной безопасности. К примеру, криптографическая хеш-функция увеличивает безопасность и эффективность схемы цифровой подписи в том случае, когда вместо сообщения цифровой подписью подписывается дайджест. В этом контексте сопротивление хеш-функции коллизиям обеспечивает уверенность в том, что оригинальное сообщение не могло быть изменено на другое сообщение с тем же значением хеш-функции и, следовательно, с той же подписью. Другое приложение криптографических хеш-функций включает в себя генерацию псевдослучайных чисел (**pseudorandom bit generation**), имитовставки (**message authentication codes**) и функции формирования ключа (**key derivation functions**).

Четыре хеш-функции SHA-3, определенные в настоящем стандарте, дополняют хеш-функции, которые определены в **FIPS 180-4**: семейство SHA-1 и SHA-2. Оба стандарта вместе обеспечивают устойчивость к будущим достижениям в области криптоанализа хеш-функций, поскольку они основаны на принципиально разных принципах проектирования. Помимо разнообразия дизайна, хеш-функции в данном стандарте обеспечивают некоторые дополнительную реализацию и характеристики производительности по сравнению с FIPS 180-4.

Длина выходных данных для XOFs может быть выбрана под требования конкретного приложения. Сами функции расширенного вывода могут быть адаптированы для хеш-функций в связи с дополнительными соображениями безопасности, или использованы во множестве других приложений. Соответствующее использование XOFs будет определено в специальных публикациях NIST.

Перестановки *KECCAC-p* были разработаны для использования в качестве главных компонентов для множества криптографических функций, включая ключевые функции для аутентификации и/или шифрования (**keyed function for authentication and/or encryption**). Шесть функций SHA-3 можно рассматривать как режимы работы (**modes of operation, modes**) перестановки ***KECCAC-p*[1600, 24]**. В будущем дополнительные моды этой перестановки или другие перестановки *KECCAC-p* могут быть определены и одобрены в публикациях FIPS или специальных публикация NIST (**NIST Special Publications**).

**4. Право одобрения (Approving Authority):** Министр торговли (Secretary of Commerce).

**5. Подразделение техподдержки (Maintenance Agency):** Департамент торговли США (U.S. Department of Commerce), Национальный институт стандартов и технологий (NIST), Лаборатория информационной технологии (**Information Technology Laboratory, ITL**).

**6. Применимость (Applicability):** Данный стандарт применим ко всем федеральным департаментам и агентствам (Federal departments and agencies) по защите конфиденциальной несекретной информации, которая подпадает под действие Раздела 10 United States Code Section 2315 (**10 USC 2315**) и не входит в систему национальной безопасности, что определено в Разделе **40 USC 11103(a)(1)**. Данный стандарт или федеральный стандарт обработки информации FIPS 180 должен быть реализован везде, где требуется безопасный алгоритм хеширования для федеральных приложений (Federal applications), в том числе в качестве компонента других криптографических алгоритмов и протоколов. Настоящий Стандарт может быть принят и использоваться неправительственными организациями (non-Federal Government organization).

**7. Спецификации:** Федеральный стандарт обработки информации (FIPS) 202, Стандарт SHA-3: хеш-функции на основе перестановок и функции расширенного вывода.

**8. Реализации:** Федеральные департаменты и агентства должны использовать реализации перестановок *KECCAK-p* только в режимах работы, одобренных FIPS или рекомендованных NIST, таких как SHA-3 функции, указанные в настоящем стандарте. SHA-3 функции могут быть реализованы в программном обеспечении (software), микропрограммном обеспечении (firmware), оборудовании (hardware) или любой их комбинации. Соответствующими настоящему Стандарту считаются только те реализации этих функций, которые проверены Программой валидации криптографических алгоритмов (**Cryptographic Algorithm Validation Program**). Информация о Программе валидации может быть получена по адресу <http://csrc.nist.gov/groups/STM/cavp/index.html>.

**9. График реализации:** Настоящий Стандарт вступает в силу немедленно. Приложения или расширения настоящего Стандарта, которые зависят от выпуска новых или пересмотренных Специальных публикаций NIST, вступают в силу после окончательной публикации поддерживающих Специальных публикаций.

**10. Патенты:** Реализации SHA-3 функций в настоящем Стандарте могут быть защищены иностранными патентами или патентами США.

**11. Экспортный контроль:** Определенные криптографические устройства и технические данные, относящиеся к ним, подлежат федеральному экспортному контролю. Экспорт криптографических модулей реализующих настоящий Стандарт и относящихся к ним технических данных, должен соответствовать федеральным нормам и иметь лицензию Бюро экспортного управления Министерства торговли США (Bureau of Export Administration of the U.S. Department of Commerce). Информация об экспортном регулировании доступна по адресу: <http://www.bis.doc.gov/index.htm>

**12. Квалификация:** Не смотря на то, что настоящий Стандарт определяет математические функции, являющиеся подходящими компонентами для приложений информационной безопасности, соответствие настоящему Стандарту не гарантирует безопасность конкретной реализации. Ответственный орган в каждом агентстве или департаменте должен гарантировать, что общая реализация обеспечивает приемлемый уровень безопасности. Настоящий Стандарт будет пересматриваться каждые пять лет в порядке оценки его адекватности.

**13. Процедура отказа от требования (Waiver Procedure):** Федеральный закон об управлении информационной безопасностью (**FISMA, Federal Information Security Management Act**) не допускает отказов от обязательных требований FIPS, установленных Министром торговли.

**14. Где можно получить копии стандарта:** Настоящая публикация доступна по адресу <http://csrc.nist.gov/publications/>. Другие публикации по компьютерной безопасности, выпущенные NIST, доступны на том же веб-сайте.

**Содержание**

**1. Введение**

**2. Глоссарий**

2.1 Термины и сокращения

2.2 Параметры алгоритма и другие переменные

2.3 Базовые операции и функции

2.4 Специальные функции

**3. *KECCAK-P* перестановки**

3.1 Состояние (State)

3.1.1 Части массива состояний

3.1.2 Конвертация строк в массивы состояний

3.1.3 Конвертация массивов состояний в строки

3.1.4 Соглашение о наименовании массива состояний

3.2 Пошаговое отображение (Step Mapping)

3.2.1 Спецификация ***θ***

3.2.2 Спецификация ***ρ***

3.2.3 Спецификация ***π***

3.2.4 Спецификация *χ*

3.2.5 Спецификация ***ι***

3.3 *KECCAK-p*[*b, nr*]

3.4 Сравнение с *KECCAK-f*

**4. Конструкция «губки» (Sponge Construction)**

**5. *KECCAK***

5.1 Спецификация ***pad10\*1***

5.2 Спецификация *KECCAK[c]*

**6. SHA-3 Спецификация функций**

6.1 SHA-3 хеш-функции

6.2 SHA-3 функции расширенного вывода

6.3 Альтернативные определения SHA-3 функций расширенного вывода

**7. Соответствие стандарту (Conformance)**

**A. Безопасность**

A.1 Резюме

A.2 Дополнительные соображения о функциях расширенного вывода

**B. Примеры**

B.1 Функции преобразования

B.2 Шестнадцатеричная форма для битов дополнения (padding bits)

**C. Идентификаторы объектов**

**D. Использованная литература**

**Рисунки**

Рисунок 1: Части массива состояния, организованные по размерности

Рисунок 2: ***x*,** ***y*** и ***z*** координаты для диаграмм пошагового отображения

Рисунок 3: Иллюстрация ***θ***, примененная к одному биту

Рисунок 4: Иллюстрация ***ρ*** для ***b = 200***

Рисунок 5: Иллюстрация ***π***, примененная к одному биту

Рисунок 6: Иллюстрация *χ*, примененная к одному ряду

Рисунок 7: Конструкция «губки»: ***Z=SPONGE*[*f, pad, r*](*N, d*)**

**Таблицы**

Таблица 1: Ширина *KECCAC-p* перестановки и связанные величины

Таблица 2: Смещение **ρ**

Таблица 3: Размеры входных блоков для *HMAC*

Таблица 4: Надежность (security strengths) SHA-1, SHA-2 и SHA-3 функций

Таблица 5: Иллюстрация ***h2b***

Таблица 6: Шестнадцатеричная форма SHA-3 заполнения для сообщений с

байтовым выравниванием

**ВВЕДЕНИЕ**

Настоящий Стандарт определяет новое семейство функций, которое дополняет семейство хеш-функций SHA-1 и SHA-2, определенных в FIPS 180-4. Это семейство, называемое SHA-3 (Secure Hash Algorithm-3), основано на алгоритме *KECCAK* – победителе конкурса SHA-3 Cryptographic Hash Algorithm Competition. Семейство SHA-3 состоит из четырёх криптографических хеш-функций и двух функций расширенного вывода. Эти шесть функций имеют общую структуру, описанную в [4], а именно, так называемую конструкцию «губки» (***sponge construction***). Функции с данной структурой называются «функциями-губками» (***sponge functions***).

Хеш-функции – это функции над двоичными данными (т.е. битовыми строками), для которых длина выходных данных фиксирована[[1]](#endnote-2). Входные данные хеш-функции называются ***сообщением*** (***message***), а выходные данные – ***дайджестом*** (***digest***) или ***хешем*** (**hash value**).

1. Для многих хеш-функций существует ограничение (очень большое) на длину входных данных. [↑](#endnote-ref-2)