ИСПОЛЬЗОВАНИЕ ФЛЕШ-ПАМЯТИ В КАЧЕСТВЕ ИСТОЧНИКА СЛУЧАЙНОСТИ ДЛЯ РЕАЛИЗАЦИИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Заливако С. С., Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: zalivako@bsuir.by, ivaniuk@bsuir.by

В работе рассмотрены сущетвующие реализации физически неклонируемых функций (ФНФ) на основе флеш-памяти. Экспериментально показано, что операции чтения без применения кодов коррекции ошибок могут быть использованы при реализации ФНФ. Предложенный подход позволяет избежать использования операций частичной записи, однако требует предварительного сбора статистики о массиве элементов флеш-памяти.

Введение

В настоящее время физически неклонируемые функции (ФНФ) используются в качестве альтернативы классической аппаратной криптографии [1]. В силу небольших аппаратурных затрат в сравнении с алгоритмами хеширования и шифрования, ФНФ применяются при реализации протоколов аутентификации компактных устройств с низким энергопотреблением (например, устройства Интернета вещей). Аппаратные реализации ФНФ, как правило, основываются на источниках случайности, имеющих физическую природу и, как следствие, уникальность(например, задержка распространения сигнала, частота работы элементов цифровых устройств, пороговые напряжения транзисторов, нестабильность начального состояния элементов памяти и т.п.).

Особенностью организации NAND флеш-памяти является обязательное наличие кодов коррекции ошибок с большой корректирующей способностью (например, код с малой плотностью проверок на четность, LDPC-код). Данная особенность обусловлено крайне низкой надежностью элементов памяти, которые зачастую при повторном чтении могут менять хранимые значения на противоположные. С другой стороны, нестабильные значения бит памяти, а также их позиции являются уникальными и могут быть использованы при реализации ФНФ на основе флеш-памяти [2].

I. Существующие реализации ФНФ на основе флеш-памяти

Реализация ФНФ на основе флеш-памяти, как правило, основана на операции частичного программирования (частичной записи) [3]. Алгоритм извлечения случайности состоит в том, чтобы последовательно записывать стертую страницу и в процессе каждой записи сохранять номера бит, которые меняют свое значение. Операция частичной записи не требует повторного стирания, поскольку интерфейс массива флеш-памяти (Open NAND Flash Interface, ONFI) поддерживает операцию прерывания. Таким образом, ответ ФНФ генерируется как результат непредсказуемого влияния операции частичного программирования на элементы памяти. Недостатком предложенного подхода является использование внутренних команд флеш-памяти, а также в 10-15 раз большая длительность операции записи по сравнению с операцией чтения.

В связи с указанными недостатками предлагается использовать операции чтения без применения кодов коррекции ошибок для извлечения уникальности из массива флеш-памяти. При чтении страницы объемом 4 Кб в порядка 100-150 битах возникают ошибки. Позиции бит, а также частота возникаемых ошибок являются уникальными как для страницы или блока памяти, так и для каждого отдельного идентичного устройства флеш-памяти.

II. Экспериментальное исследование блока флеш-памяти

Блок – это минимальная единица стирания флеш-памяти. Как правило, современные устройства флеш-памяти содержат от 100 до 1000 страниц в блоке. Данный эксперимент был проведен на плате быстрого прототипирования контроллеров флеш-памяти Cosmos OpenSSD с TLC (Triple Level Cell) памятью производства SK hynix.

Алгоритм эксперимента состоит из 4 шагов: выбор случайного блока, стирание выбранного блока, запись нулей во все страницы блока без использования кодов коррекции ошибок, чтение каждой из страниц по 100 раз. В качестве уникальной характеристики каждой из страниц используется среднее число страниц, полученное при чтении.

Для проведения эксперимента был выбран блок с адресом 0x2F0. Как показано на рисунке 1 число единиц при чтении значительно отличается для различных страниц. Следовательно, аналогично ФНФ на основе кольцевых генераторов, сравнение числа единиц при чтении позволяет генерировать уникальные ответы ФНФ.

Как показано на рисунке 2 на примере страниц 0, 212, 444 и 576 с увеличением числа чтений среднее число единиц на странице стабилизируется. Более того, различия между страницами по среднему соответствуют различиям между страницами при однократном чтении. Следовательно, различия в среднем значении единиц при чтении влияют на стабильность генерируемых бит: чем больше отличие в среднем между страницами, тем стабильнее будет ответ ФНФ.

Следовательно, набор из всех страниц блока является источником случайности для реализации ФНФ.

Заключение

Было проведено экспериментальное исследование TLC флеш-памяти производства SK hynix с помощью платы быстрого прототипирования контроллеров Cosmos OpenSSD. Результат эксперимента показал, что количество единиц, полученное при чтении без использования кодов коррекции ошибок, является уникальным для каждой из страниц в блоке памяти. Предложенный подход позволяет избежать операций частичной записи и генерировать ответы ФНФ с помощью операций чтения. Недостатком предложенного подхода является сбор статистики о среднем числе единиц, полученных при чтении.

Список литературы

1. Zalivaka, S. S. Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography / S. S. Zalivaka, L. Zhang, V. P. Klybik, A. A. Ivaniuk, C. H. Chang // Secure System Design and Trustable Computing / ed. by C.H. Chang, M. Potkonjak. – New York : Springer, 2016. – P. 39–81.
2. Extracting Robust Keys from NAND Flash Physical Unclonable Functions / J. Shie [et al.] // Proc. of Int. Conf. on Inf. Secur. (ISC'2015), Sep. 2015. – Frankfurt, Germany – P. 437–454.
3. Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints / Y. Wang [et al.] // Proc. IEEE Int. Symp. on Secur. and Priv. (SP'2012), May. 2012. – San Francisco, USA – P. 33–47.

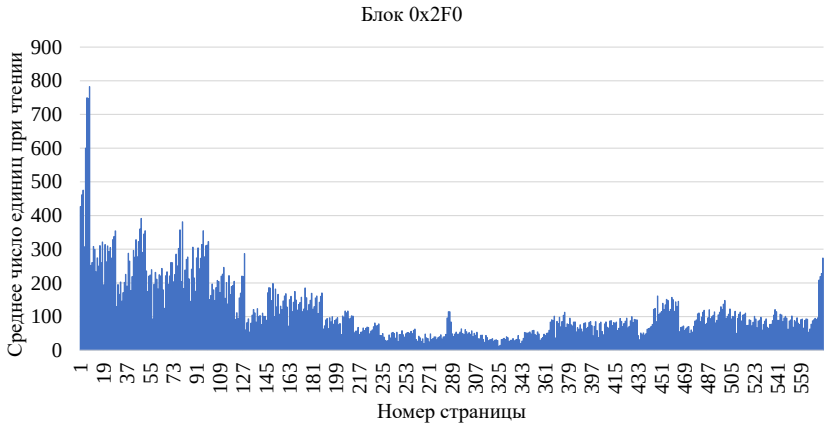

Рис. 1 – Среднее число единиц, полученное при чтении, в засимости от номера страницы с блоке

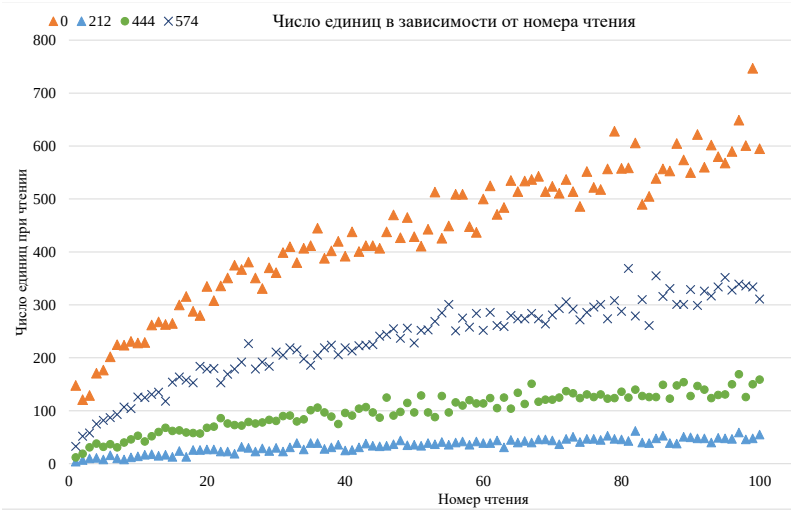

Рис. 2 – Число единиц в зависимости от номера чтения для разных страниц