UDC 003.26

Mironkin V.O.
MIEM NRU HSE, Moscow

Urusov M.I.
MIEM NRU HSE, Moscow

Utkina K.A.
MIEM NRU HSE, Moscow

On some properties of Sponge construction

In this paper we consider the basic modes of Sponge construction. We describe some ways of building collision and the second preimage of the keyed Sponge construction and ways of determination of the key. The probability of generating the specified output of the Sponge construction is estimated.

Introduction

The structure of cryptographic hash functions [9] has been described in doctoral thesis by Ralph Merkle in 1979, which based on the principle of splitting the input message into blocks of the same size and sequential processing an unilateral compression function that converts an input fixed-length message into a shorter output message (Fig. 1).

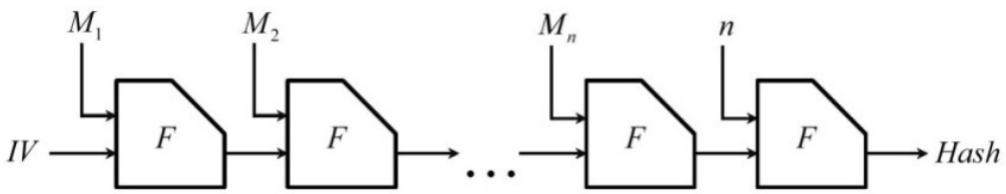


Fig. 1. Merkle-Damgard's scheme

Despite the popularity of Merkle-Damgard's scheme, a number of works has shown the disadvantages of this design associated with multiple collisions [1], the padding of the message to the desired length and the finding the second preimage [4]. Therefore it was proposed to use the compression function in the form of a separate structural block. It was decided to construct a keyless entry function F_{Sp} called Sponge construction [2].

Currently, the analysis of Sponge construction is one of the most urgent tasks of modern cryptography, because it allows to generate almost all of cryptographic mechanisms (see Fig. 2) such as a message authentication code, a generator of equiprobable sequences and keys for passwords, etc.

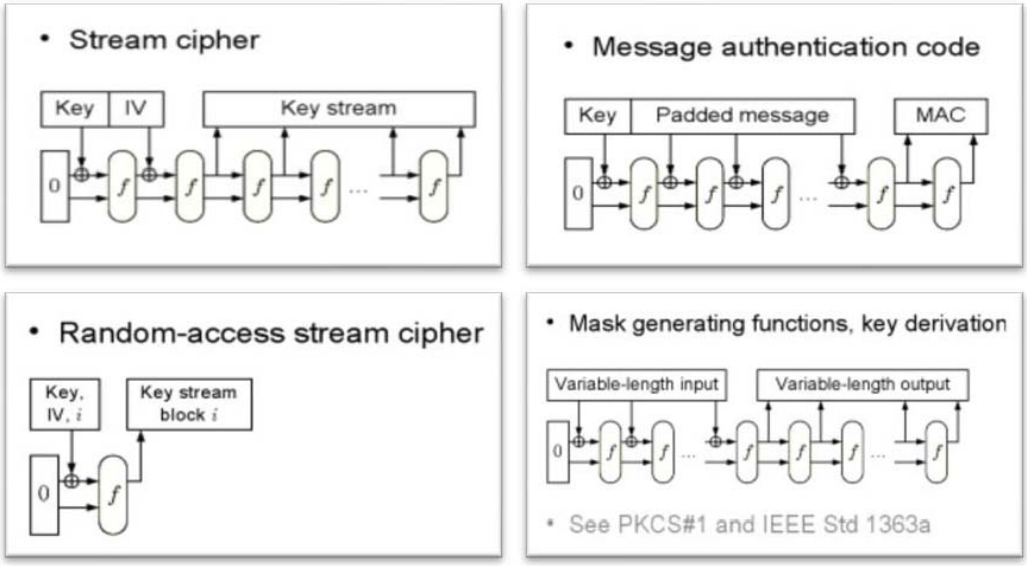


Fig. 2. Usage of Sponge construction

In recent years a number of works in analysis of Sponge construction is increasing [1, 3, 8, 10, 11]. To date, proposed a number of exotic attacks on Sponge constructions such as the attacks on the elongation of the message, the attacks on partial collisions with the selected prefix, etc.

However, the approaches to cryptanalysis Sponge construction based on usage of structural features of transformation graph is not fully investigated.

In this paper we study the properties of keyed hash functions and encryption algorithms based on F_{Sp}, and suggest some methods for constructing collisions for F_{Sp}.

1. The main modes of Sponge construction

In this section the operating modes of hashing and encryption algorithms based on Sponge is submitted.

1.1. Sponge construction as a hash function

The basis of the work of Sponge is the transformation of a fixed set of $b = r + c$ bits. The final length of the output sequence is formed by cutting of the first l bits of the original output string. In the beginning b bits are initialized by zero values. The input message is padded and divided into blocks of r bits long. A further process consists of two phases:

- ***Absorbing phase*:** each block of input message is summarized with part of the r bit of b-bit internal state of the Sponge by operation XOR. The substitution f is applied to b-bit state between these operations.
- ***Squeezing phase*:** the substitution f is applied successively to the block formed in the absorbing phase. Accumulated blocks forming the output message Z. [2]

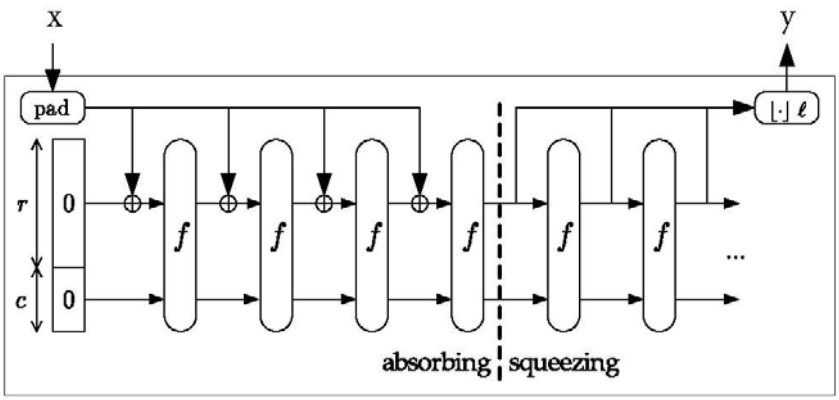


Fig. 3. The functioning of Sponge-construction

1.2. The keyed Sponge construction

The keyed Sponge constructions, which use the key $K \in \{0,1\}^k$ are divided into two classes:

- Sponge construction F_{OKSp} with outer key (the outer-keyed Sponge), where a string $K \| x$ goes to the input of Sponge.

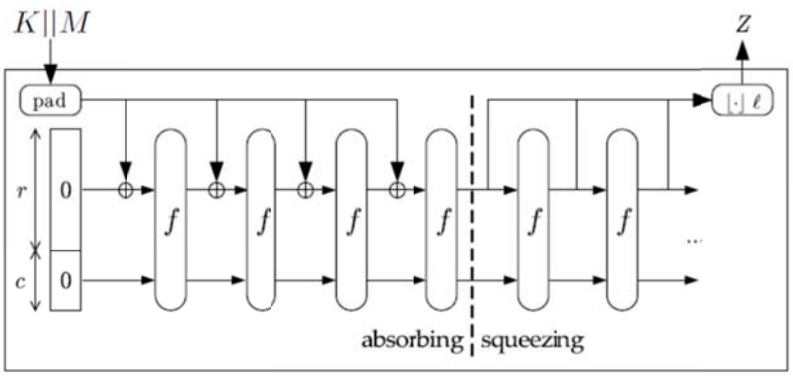


Fig. 4. The functioning of the outer-keyed Sponge construction

- Sponge construction F_{IKSp} with inner key (the inner-keyed Sponge), where internal state is generated as follows: $s_i = f(s_{i-1} \oplus x_{i-1})$, where $s_0 = (0^{b-k} \| K)$.

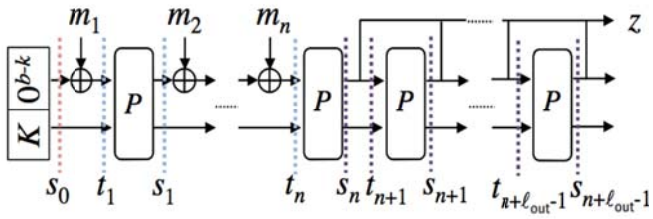


Fig. 5. The functioning of the inner-keyed Sponge-construction

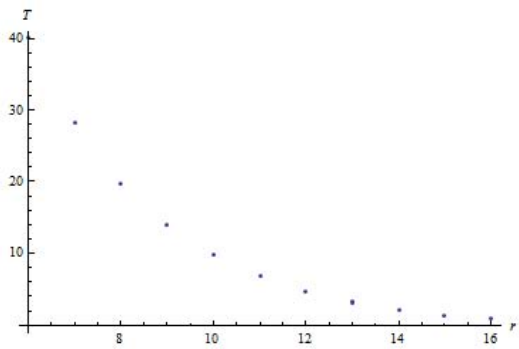
1.3. Collisions of the keyed Sponge construction

In this section we research Sponge construction with outer key. Let $|K| = r$, then the following result is true.

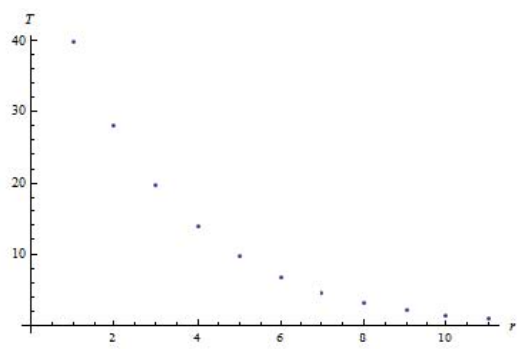
Proposition 1. *If internal state of F_{OKSp} lies on k-cycle of graph of the substitution f after the procedure of absorbing, then for an arbitrary input vector $x' = K \| x = K \| x_0 \| x_1 \| ... \| x_{m-1}$ the second preimage has the form:*

$$K \| 0^{rkp} \| x_0 \| ... \| x_{m-1}.$$

Similarly, the main results for Sponge construction with outer key are formulated with the replacement of x to $K \| x$ according to the article [6]. Herewith the average complexity of finding collisions equals to $T = \sum_{k=0}^{2^c-1} \prod_{i=0}^{k-1} \left(1 - \frac{(i-1)2^r - i}{2^b - i}\right)$ [6]. The dependence T_{av} on r is illustrated on graphs 1, 2.



Graph. 1. Dependence T_{av} on r with $b = 16$



Graph. 2. Dependence T_{av} on r with $b = 32$

It should be noted that the key length and, consequently, length of its possible additions are the main characteristics of Sponge F_{OKSp} influenced the security.

If the key K length t exceeds r, then part of the key length $t - r$ has no influence the functioning of the Sponge. At the same the power the keyed set is reduced from 2^t to 2^r. In the case when the key length is less than 2^r, a way of key padding becomes crucial. For example, when we add zero bits to keys $(a_1,...,a_{t-2},0)$ and $(a_1,...,a_{t-2})$, they become equivalent, that allows to build the collision. Also such padding allows to build the collision due to the movement on the cycle of substitution f. Thus, it is reasonable to use padding of the vector of the form $(1,0,...0,1)$ [5].

1.4. Stream encryption

Using the secret key with the open the initialization vector (*IV*) for Sponge construction allows to forming blocks required for a stream encryption. For example we can use XOR for forming encryption blocks of open text and sponge output.

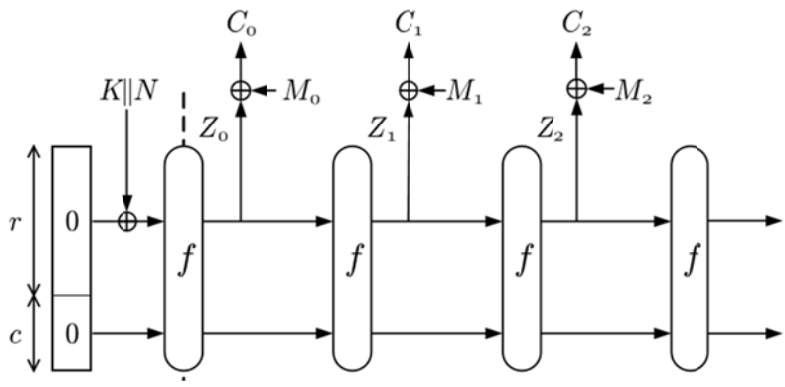


Fig. 6. The scheme of stream encryption mode of Sponge construction

However, such mode is inauthentic. It means that we can replace the message without knowing the key. In order to fix this, we must add blocks of open text with Sponge function input by XOR. Thus, this mode forms the MAC (Tag) [3].

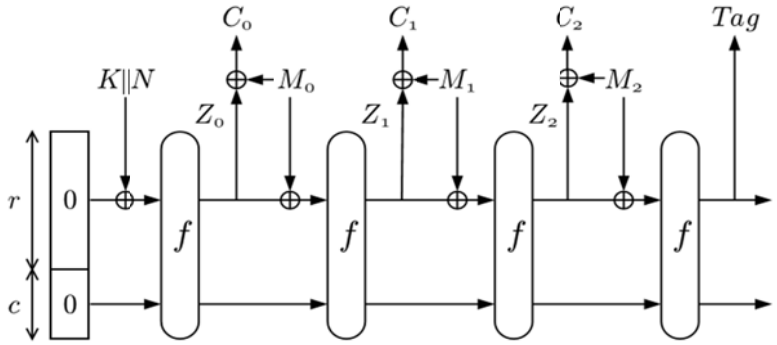


Fig. 7. Encryption with MAC generation

Let's consider the issue of a key recovery from the internal state of Sponge construction in the case of simple XOR without generating MAC.

Remark 1. *The knowledge of any inner state of Sponge construction allows to uniquely recover the previous one if only there isn't any external impact, because each substitution uniquely determines the inverse function.*

Let $K' = K \,||\, IV$ (a secret key, concatenated with an initializer vector).

In the case $|K'| < r$ *absorbing* stage takes only one step. It is possible to calculate value $Z_0 = C_0 \oplus X_0$ because we suppose that message M is known. For each of the variants for an unknown suffix with $b - r$ length we solve the equation:

$$f\left(K' \oplus \vec{0}\right) = Z_0' \Leftrightarrow K' \oplus \vec{0} = f^{-1}\left(Z_0'\right). \tag{1}$$

The resulting solutions contain value K' determined key K. If there is more than one solutions of equation (1), then solutions forming the class of the equivalent keys with the representative K, which can be used in constructing collisions for F_{OKSp}.

Remark 2. *If* $|K'| \geq r$ *and* $|K| < r$ *or* $|K| > r$ *and* $\left\lceil \frac{|K|}{r} \right\rceil = m$, *then the recovery requires a compiling multiple relations of type* (1).

1.5. Rotational properties

Recently researches focused on rotational properties of different encryption patterns e.g. [8, 10]. Let's recall a number of definitions.

Definition 1. *For an arbitrary* $X \in V_n$ *rotation pair with parameter* r *call a pair of the strings* $\left(X, \overrightarrow{X}_r\right)$.

Definition 2. *Let's sat that the operation* $*$ *maintains a rotation for* t *rotation pairs* $\left(X_1, \overrightarrow{(X_1)}_r\right), \ldots, \left(X_t, \overrightarrow{(X_t)}_r\right)$, *if* $\overrightarrow{(X_1 * \ldots * X_t)}_r = \overrightarrow{(X_1)}_r * \ldots * \overrightarrow{(X_t)}_r$.

Let M – block of an open text, Y – block of gamma, C – block of an encrypted text, $\overrightarrow{M}_r, \overrightarrow{Y}_r, \overrightarrow{C}_r$ - the corresponding rotations. In paper [7] the probability $P(\oplus)$ of the event $\left\{\overrightarrow{M}_r \oplus \overrightarrow{Y}_r = \overrightarrow{M \oplus Y}_r\right\}$ is estimated. Using the equality $M \oplus Y = C$ we obtain the relation

$$\overrightarrow{M} \oplus \overrightarrow{Y} = \overrightarrow{(M \oplus Y)} = \overrightarrow{C}.$$

Therefore, $P(\oplus)$ can be used for estimating probability of output $\overrightarrow{C}_r$ when the input is $\overrightarrow{M}_r, \overrightarrow{Y}_r$. Thus, using the output of the Sponge construction we can get information about blocks of gamma and message.

Conclusions

Using of a secret key makes Sponge construction more resistant to the attacks based on the structural collisions. However, an important point of Sponge construction creating is choice of key padding algorithm. It should also be noted that rotational properties allow to build statistics tests for identification of not equiprobable output sequences.

References

1. *Bernstein D. J.* Second preimages for 6 rounds of Keccak. NIST hash forum mailing list, November 27, 2010.
2. *Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.* Cryptographic sponge functions.
3. *Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.* On the security of the keyed sponge construction.
4. *Bertoni G., Daemen J., Peeters M., Van Assche G.* Sponge Functions, http://noekeon.org.
5. *Bertoni G., Daemen J., Peeters M., Van Assche G.* The Keccak reference, http: // noekeon.org.
6. *Dali F.A., Marshalko G.B., Mironkin V.O.* On collisions of Sponge constructions. - CRCNAA 2017.
7. *Daum M.* Cryptanalysis of Hash Functions of the MD4-Family. PhD thesis, Ruhr-Universitat Bochum, 2005.
8. *Khovratovich D., Nikolin I.* Rotational cryptanalysis of ARX. Fast Software encryption 2010 (S. Hong, T. Iwata, eds.) LNCS Vol. 6147, Springer, Heildelberg, 2010, pp. 333-346.
9. *Merkle R.C.* Secrecy, authentication, and public key systems, PhD thesis, UMI Research Press, 1982.
10. *Morawiecki P., Pieprzyk J., Srebrny M.* Rotational cryptanalysis of round-reduced Keccak. Cryptology ePrint Archive Report 2012/546, 2012.
11. *Perrin L., Khovratovich D.* Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64. Eprint.iacr.org/2014/223, 2014.