Annales UMCS Informatica AI XIV, 1 (2014) 37–48
DOI: 10.2478/umcsinfo-2014-0002

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Cryptographic Applications of the Duplex Construction

Mariusz Borowski[1]*

[1] *Cryptology Division, Military Communication Institute*

Abstract – Assured security is the desirable feature of modern cryptography. Most of modern cryptography primitives have no provably secure constructions. Their safety is defined on the basis of well-known in the given time cryptanalytic attacks. The duplex construction equipped with one ideal permutation and appropriate security parameters is suitable for building provably secure cryptographic primitives. The constructions can be used for unclassified information of different sensitivity levels protection. Some of them can secure classified information up to the "TOP SECRET" level. The applications based on the duplex construction can be used for key wrapping, authenticated encryption and can work as a pseudo-random bit sequence generator. They are not covered by any known intellectual property.

1 Introduction

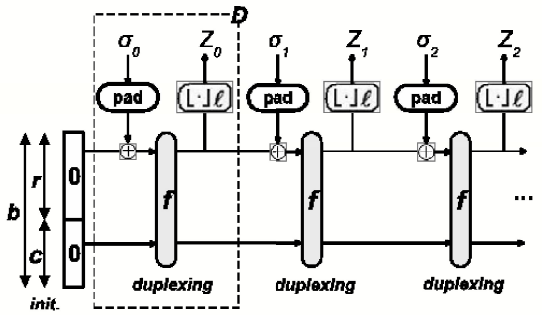
Assured security is the desirable feature of modern cryptography. Sponge constructions equipped with only one ideal permutation and appropriate security parameters can be used to provably secure cryptographic primitives building [**4**], [**8**]. Because of their arbitrarily long input and output sizes, the constructions allow building various primitives such as a hash function, a stream cipher or a message authentication code (MAC). Another set of applications takes advantage of the duplex construction which is closely related to the sponge construction. Security of the duplex construction can be shown to be equivalent to the sponge one. The duplex construction permits the alternation of input and output blocks at the same rate as the sponge construction. This allows to implement an efficient reseedable pseudo random bit sequence generation and one pass authenticated encryption scheme free from patent limitations. Sections 2 and 3 show known facts connected with the duplex construction and security of the duplex

*m.borowski@wil.waw.pl

and sponge constructions in a coherent and rather simple and compact way. Original results are presented in Section 4. Security of authenticated encryption schemes defined for block ciphers and schemes based on the duplex construction is reviewed in Section 4.1. Section 4.2 shows comparison of some key wrapping schemes. The assessment proves that cryptographic schemes based on the duplex construction can be used for protection of the classified information up to the "TOP SECRET" level and unclassified information of different sensitivity levels. Section 4.3 briefly presents the design and evaluation of a cheap but very fast pseudo-random sequences generator based on the duplex construction and a slow random bit generator developed by Military Communication Institute. Finally, Section 5 concludes the paper.

2 The Duplex Construction

The duplex construction (Fig. 1), like the sponge construction [**4**], [**8**], uses a fixed length transformation or permutation f operating on a fixed number b of bits, a padding rule "pad" to build a cryptographic scheme. The duplex construction operates on a state of $b = r + c$ bits. The value b is called the width, the value r is called the bitrate and the value c the capacity. Different values for a bitrate and a capacity give the trade-off between speed and security. The higher bitrate gives the faster cryptographic function that is less secure. It is important that the last c bits of the b-bit state are never directly affected by the input blocks and are never output during the output producing. The capacity c, the most important security parameter, determines the attainable security level of the constructions, as proven in chapter 3. The duplex construction results in an object that accepts calls that take an input string and return an output string that depends on all inputs received so far. An instance of the duplex construction is called a *duplex object* and is denoted by D.



Rysunek 1. The duplex construction

A duplex object D has a state of b bits. Upon initialization all the bits of the state are set to zero. From then on one can send to it D.duplexing (σ, ℓ) calls, with σ as an input string and the requested number of bits. The maximum number of bits ℓ one

can request is r and the input string should be short enough such that after padding it results in a single r-bit block.

3 Security of the Sponge and Duplex Constructions

A fundamental property of the duplex construction (called the duplexing-sponge lemma) is that the output of a call to a duplex object can be obtained by evaluating a sponge function with the same parameters to the input (r and c) constructed from all previous inputs to the duplex object [**6**]. The lemma states that the output of a duplexing call is the output of a sponge function with an input $\sigma_0 \parallel pad_0 \parallel \sigma_1 \parallel pad_1 \parallel \cdots \parallel \sigma_i \parallel pad_i$ and from this input that exact sequence $\sigma_0, \sigma_1, \ldots, \sigma_i$. As such, the duplex construction is as secure as the sponge construction with the same parameters. In particular, the duplex construction inherits its upper bound on the random oracle differentiating advantage, where the input to the random oracle is the sequence of inputs to the duplexing calls since the initialization. The cryptanalytic attacks on the sponge and duplex constructions can be divided into two types. The first type shows a non-random behaviour, weakness in an internal permutation or a random transformation. Such attack leads to built distinguishers on such functions (permutations or transformations). The second type is the attack on the core security properties of the whole cryptographic function based on the sponge construction (a preimage attack and a collision attack). An attack on a sponge function is a generic attack if it does not exploit specific properties of f (an internal permutation or a random transformation). Guido Bertoni, Joan Deamen, Michael Peeters, Gilles Van Assche in [**5**] showed the sponge type hash function Keccak, that was selected by NIST as the winner of the SHA-3 competition in October 2012. The constructors adopted the sponge construction and built an underlying permutation f that should not have any structural distinguishers. The capacity c determines the claimed level of security, and one can trade claimed security for speed by increasing the capacity c and decreasing the bitrate r accordingly, or vice-versa. Keccak is a member of the sponge function family [**4**],[**5**]. The sponge type hash function Keccak is proven indifferentiable from a random oracle up to bound:

$$\Theta((Kq)^2/2^{c=2n})$$

if the underlying permutation is assumed to be ideal [**5**]. The indifferentiability bound shows an optimal collision resistance bound for Keccak,

$$Adv^{col}_{Keccak} = \Theta(q^2/2^n) \tag{1}$$

as well optimal preimage and second preimage resistance:

$$Adv^{prev}_{Keccak} = Adv^{sec}_{Keccak} = \Theta(q/2^n) \tag{2}$$

The most successful result (in terms of a number of rounds) on the sponge type Keccak's permutation is the zero-sum distinguisher [**14**], [**3**], [**20**]. However, the complexity of the distinguishers is very high. For example, the zero-sum distinguisher for all 24 rounds of Keccak has the complexity of 2^{1579} (instead of the theoretical complexity 2^{1600}) [**14**]. The results do not lead to any attacks on the Keccak hash function. The second type generic attacks have the complexity bounded up to 8 rounds [**20**], [**11**], [**13**], [**21**], [**11**]. The design of the ideal permutation is the key matter for the sponge and duplex constructions. The Keccak-f permutation [**5**] or "Keccak-f like" permutations [**4**], [**17**] can be used in cryptographic applications based on the constructions.

4 Applications Based on the Duplex Construction

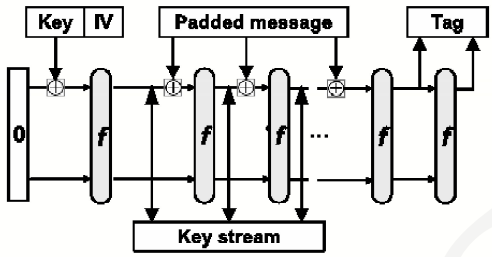
The duplex construction can be applied to [**7**],[**8**]:

- one pass authenticated encryption;
- key wrapping;
- reseedable pseudo-random bit sequence generation.

4.1 One Pass Authenticated Encryption

Authenticated Encryption (AE) has been extensively studied in the last ten years. Block cipher modes are a popular way to provide simultaneously both integrity and confidentiality. Authenticated encryption schemes are defined for block ciphers with a block length of 128 bits. The length of an authenticating tag is bounded by a used block cipher in the schemes. The maximal length of the tag in block cipher AE schemes is 128 bits. One pass authenticated encryption schemes based on the block ciphers (e.g., OCB, IAPM, IACBC) are very efficient but they are patent encumbered. Two pass authenticated encryption schemes based on the block ciphers (e.g., GCM, CWC, INK) are free from patent limitations. The AE based on the duplex construction is not covered by any known intellectual property. Some of the sponge-based AE schemes can achieve a significantly higher security bound than the classical $\frac{2c}{2}$ bound [**16**]. Some of them can be parallelized [**19**], [**7**]. The AE scheme shown in Fig. 2 uses the duplex construction and it is one pass. Upon initialization it loads the key (K). From then on one can send request to it for wrapping or unwrapping data. The key stream blocks used for encryption and the tags (T) depend on the key (K) and the data sent in all previous requests. Key stream sequences give no information on tags and vice versa as they are obtained by call to different duplex instances.

Authenticated encryption is an example of a duplex function turned into a keyed function by including a secret key in the input. If the duplex function behaves like a random oracle, the keyed duplex function conducts as a random function to anyone not knowing the key but having access to the duplex function. Let us consider security of a duplex function used in conjunction with a key, for example in the case of our AE



Rysunek 2. One pass authenticated encryption (*DuplexAE*)

scheme (Fig. 2). The dependences also set for key wrapping and reseedable pseudo-random sequence generators. It was shown in [**6**] that the advantage in distinguishing a keyed duplex function from a random oracle is upper bounded by:

$$max((\frac{M^2}{2} + 2 \cdot M \cdot N) \cdot 2^{-c}, N \cdot 2^{-|K|})$$

where M is the data complexity, i.e. the amount of access to the keyed scheme, N is the number of queries to the underlying transformation (or permutation), and $|K|$ is the length of the key. In the typical case if $M << 2^{\frac{c}{2}}$ time complexity is much smaller and it carries out about

$$min(\frac{2^{c-1}}{M}, 2^{|K|})$$

The key is related to the capacity with the following dependence:

$$|K| + 1 + log_2 M \leq c \tag{3}$$

This allows decreasing the capacity c (and thus the permutation width) for a given security level or achieving a higher security level for a given capacity. The shown bound for keyed applications allows usage of very fast lightweight duplex constructions, especially on the platforms with limited resources.

The one pass AE scheme based on the duplex construction satisfies the security requirements of key recovery (probability of finding the key with trying N keys K is not above $N \cdot 2^{-|K|}|$), tag forgery ($2^{-|T|}$ and plaintext recovery ($N \cdot 2^{-|K|}$) if the used sponge is secure.

The authenticated encryption based on the duplex construction has some advantages:

- it is one pass and requires only one fixed-length permutation;
- it supports the alternation of strings that require authenticated encryption and strings that only require authentication;
- it has a strong security bound against generic attacks with a simple proof, that relies on the bound of the random oracle differentiating advantage of the sponge construction and on the sponge-duplexing lemma;

- it is flexible as the bitrate r can be freely chosen as long as the capacity c is larger than the required security bound;
- the length of the authenticating tag is bounded by $\frac{c}{2}$, considerably more than in a block cipher AE case.

Table.1 summarizes the features of some AE schemes defined for block ciphers and the AE scheme built from the duplex constructions. Security of authentication and encryption is higher for the AE scheme built from the duplex construction. The possibility of the parameter choice is also higher for the scheme. The AE scheme based on the duplex construction can be used for protection classified information up to the "TOP SECRET" level and unclassified information of different sensitivity levels.

Tablica 1. Comparison of some authenticated encryption schemes

AE scheme	**Year**	**Operating mode**	**Security of A (max)**	**Security of E (max)**	**Transformation**
OCB	2001	1. A+E	2^{128}	(2^{128} to 2^{255})	e.g., AES
GCM	2007	1.E 2.A	2^{128}	(2^{128} to 2^{255})	e.g., AES
INK [**13**]	2009	1.A 2.E	2^{128}	(2^{128} to 2^{255})	e.g., AES
DuplexAE	2010	1. A+E	$2^{\frac{c}{2}}$ (2^{160} to 2^{512})	$\min(2^{c-60}, 2^{\lvert K\rvert})$ (2^{160} to 2^{512})	Duplex [r={1152, 1088, 832, 576}, c={448, 512, 768, 1024}]

4.2 Key Wrapping

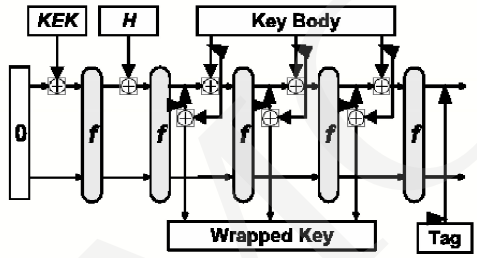
Key wrapping is the example of the practical use of authenticated encryption. It can provide assurance of the confidentiality and the integrity of data, especially cryptographic keys or other specialized data. In a key wrapping scheme a payload key of arbitrary length is wrapped with a key-encrypting key. Key wrapping is very important in the key management systems [**9**]. It helps to protect the secrecy and integrity of cryptographic keys in transport or storage. Key wrap schemes are typically built of approved symmetric key block ciphers [**1**], [**2**]. Security concerns [**2**], [**16**] and absence of security proofs connected with the design of the ANS X9.102 block cipher key wrap schemes (e.g., TDKW, AESKW) caused the development of the SIV (the Synthetic Initialization Vector mode) scheme [**22**] also based on block ciphers. This scheme was standardized as the new AES mode in RFC 5297. All the schemes are not covered by any known intellectual property.

Key wrapping based on the duplex construction is the example of assured cryptography free from security concerns discussed above [**16**], [**8**]. The practical use of one pass authenticated encryption shown in Fig. 2 is the *DuplexKW* key wrapping scheme (Fig.3).

In such scheme a payload key of arbitrary length is wrapped with a key-encrypting key (*KEK*). If each key is associated to a unique identifier in the cryptosystem it is

sufficient to include the identifier of the payload key in the header and two different payload keys will be enciphered with different streams.

The inputs to the key wrapping process are the *KEK*, the identifier H and the plaintext (the payload key) of an arbitrary length to be wrapped. After key wrapping the wrapped key and the tag as an authentication code will be generated. The inputs to the unwrapping process are the *KEK*, the identifier H and the ciphertext consisting of previously wrapped key data and the tag. During the unwrapping process the wrapped key is deciphered and its integrity is checked. If the tag is invalid an error message will be generated.



Rysunek 3. *DuplexKW* key wrapping

Table 2 summarizes the features of some key wrap schemes based on block ciphers and the key wrap scheme (Fig.3) built of the duplex constructions. It can be seen that the security of authentication offered by the schemes based on block ciphers is not sufficient at present.

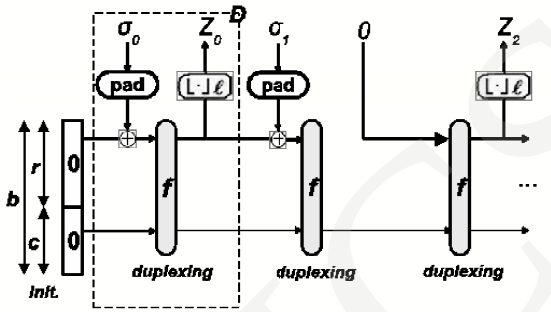
Tablica 2. Comparison of some authenticated encryption schemes

KW scheme	**Year**	**Operating mode**	**Security of A (max)**	**Security of E (max)**	**Transformation**
TDKW	2001	1. A+E	2^{48}	2^{112}	Triple DES
AESKW	2001	1.E 2.A	2^{63}	(2^{128} to 2^{255})	AES
SIV	2008	1.A 2.E	2^{128}	(2^{128} to 2^{255})	e.g., AES
DuplexKW	2010	1. A+E	(2^{160} to 2^{512})	$\min(2^{c-60}, 2^{\lvert K\rvert})$ (2^{160} to 2^{512})	Duplex [r={1152, 1088, 832, 576}, c={448, 512, 768, 1024}]

The key wrap scheme based on the duplex construction offers high flexibility in the choice of the duplex transformation parameters. It is possible to determine the claimed level of security by the appropriate parameters choice. The scheme can be used for protection classified information up to the "TOP SECRET" level and unclassified information of different sensitivity levels.

4.3 A Reseedable Pseudo-random Bit Sequence Generator

The duplex construction can be readily used as a reseedable pseudo-random bit sequence generator shown in Fig. 4. Seeding material can be fed via σ inputs in it D.duplexing () call and the responses can be used as pseudo-random bits.



Rysunek 4. Reseedable pseudo-random bit sequence generator

The only limitation of this is that the user must split his seeding material in strings of at most $\rho < (r-1)$ bits and at most r bits can be requested in a single call. Binary random sequences have numerous applications in many fields of science and technology. Military Communication Institute (MCI) developed a family of hardware random bit generators, the first in the nineties. The generators can generate random sequences with an output rate $115.2kbit/s$, $8Mbit/s$ up to $100Mbit/s$ and they were certified by the Polish national security authority according to "The Protection of Classified Information Act" and can be used in cryptographic systems up to "TOP SECRET" level [**9**], [**10**]. As a scientific tool the SGCL-100M generator (the generator with an output rate $100Mbit/s$) produced by MCI can be used in advanced research in many fields of science and technology. Since the generator is a quite complex and costly device [**18**] with a very high output rate it can be assumed that it could be used as a source for random sequence servers in R&D centers.

In 2012 MCI decided to build a cheap but very fast pseudo-random sequences generator based on the duplex construction and our old and slow random bit generator as a source of seeding material. The generator applies a sponge function f to the sequences of values $seed + 1, seed + 2, seed + 3, \ldots$. The output sequence is $f(seed + 1), f(seed + 2), \ldots$. Because of the property of forward security, it is necessary to keep only a few bits of the output values $f(seed + i)$ in order to remove possible correlation between the successive values. The reseedable pseudo random bit sequence generator, based on "a Keccak-f like" permutation and a slow hardware random bit generator can pass the tests for randomness of the NIST Statistical Test Suite and the MCI battery test [**24**], [**23**].

The MCI battery test consists of:

- frequency test,
- serial test,
- two bit test,
- 8 bit poker test,
- 16 bit poker test,
- runs tests (for max 22 consecutive zeros or ones)
- autocorrelation tests (for shifted sequences by 1, 2, ..., 8 bits).

The tests calculate suitable statistics for binary sequences and use the chi-squared and the standard normal distribution to compare the observed frequencies with the expected ones. For the whole sequence the hypothesis testing in a classical manner is used, where the hypothesis H_0 that the variable is random is verified using calculated statistics with the significance level $p = 0.05$. Classes of tests results for the subsequences are used to assign percentages of calculated statistics. The calculated statistics are split into eight classes according to the range of a significance level. The class A defines a group of the best statistics and the class H defines the worst case in terms of randomness, but all cases are possible with appropriate probabilities as it is listed in Table. 3.

Tablica 3. Classes and their expected percentages of appearance

Classes	A+B+C	A	B	C	D	E	F	G	H
%	95	80	10	5	2.5	1.5	0.5	0.4	0.1

Many 1GB sequences obtained from our reseedable pseudo random bit sequence generator were tested using the MCI battery test. The results for fours sequences are listed in Table.4. It shows that percentages of classes are similar to the expected appearances of classes for random sequences (see Table.3). The obtained results confirm that the generator has a very good statistical quality.

Tablica 4. Classes and their expected percentages of appearance

Sequence	A+B+C	A	B	C	D	E	F	G	H
N.1	94.72	79.83	10.22	4,67	2.74	1.55	0.48	0.45	0.06
N.2	94.98	79.96	10.05	4.97	2.53	1.47	0.47	0.44	0.11
N.3	95.09	80.26	9.68	5.15	2,95	1.30	0.24	0.39	0.02
N.4	95.28	79.93	10.31	5.04	2.39	1.45	0.47	0.34	0.07

The generator is very efficient and can produce binary pseudo-random sequences with the potential throughput (amount of data per unit time) higher than $150Mbit/s$ in a relatively cheap way. It will be able to produce a little more than $1.5T$ bytes per day and act as a practically "infinite" source of pseudo-random sequences with very good statistical properties.

5 Conclusions

Assured security is the desirable feature of modern cryptography. Applications based on the duplex construction can be used for protection of classified and unclassified information. The primitives are provably secure. The creation of the ideal permutation or the random transformation is the key matter for the sponge and duplex construction. Guido Bertoni with his team showed how such safe permutations can be built. The effectiveness of the method was confirmed by the third-party cryptanalysis.

Applications of the duplex construction showed in the paper can be used for key wrapping, authenticated encryption and work as a pseudo-random bit sequence generator. The duplex construction is very flexible and other applications can be readily built. It is possible to first fix the capacity c such that $\frac{c}{2}$ is at least the desired security level and then choose the remaining parameters. It is very important that for the duplex construction there are no generic attacks with complexity of the order below $2^{\frac{c}{2}}$.

The keyed duplex functions are used for key wrapping and one pass authenticated encryption schemes free from patent limitations. They are very efficient because enciphering and authenticating together require only a single call to the underlying permutation per block. The schemes are based on one appropriate permutation instead of a block cipher. Usage of the key in the applications allows decreasing the capacity (and thus the permutation width) for a given security level or achieving a higher security level for a given capacity. The bound for keyed applications permits usage of very fast lightweight sponges, especially on the platforms with limited resources [**7**],[**8**].

Literatura

[1] AES Key Wrap Specification. NIST (2001).
[2] ANS X9.102 Wrapping of Keys and Associated Data (2004).
[3] Aumasson J. P., Meier W., Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi, CHES (2009), http://131002.net/data/papers/AM09.pdf.
[4] Bertoni G., Deamen J., Peeters M., van Assche G., Cryptographic sponge functions (2011), http://sponge.noekeon.org.
[5] Bertoni G., Deamen J., Peeters M., van Assche G., The Keccak reference Version 3.0, STMicroelectronics (2011), http://sponge.noekeon.org.
[6] Bertoni G., Deamen J., Peeters M., van Assche G., On the security of keyed sponge constructions, Symetric Key Encryption Workshop (2011).
[7] Bertoni G., Deamen J., Peeters M., van Assche G.:,Duplexing the sponge: single-pass authenticated encryption and other applications, SAC (2011), http://eprint.iacr.org/2011/499.pdf.
[8] Borowski M., The sponge construction as a source of secure cryptographic primitives, Military Communication Conference, France (2013).
[9] Borowski M., Leśniewicz M., Wicik R., Grzonkowski M., Generation of random keys for cryptographic systems, Annales UMCS Informatica AI XII, 3 (2012).
[10] Borowski M., Wicik R., A one-time cipher machine for Polish Army, Military Communication Conference, Prague (2008).

[11] Dinur I., Morawiecki P., Pieprzyk J., Srebrny M., Straus M., Practical complexity cube attack on round-reduced Keccak sponge function, http://eprint.iacr.org/2014/259.pdf.

[12] Dinur I., Dunkelman O., Shamir A., New attacks on Keccak-224 and Keccak-256, FSE 2012, LNCS 6147, Springer-Verlag (2012): 462–461.

[13] Dinur I., Dunkelman O., Shamir A., Self-differential cryptanalysis of up to 5 rounds of SHA-3, http://eprint.iacr.org/2012/672.pdf.

[14] Duan M., Lai X., Improved zero-sum distinguisher for full round Keccak-f permutation, http://eprint.iacr.org/2011/023.pdf (2011).

[15] Gliwa R., Uwierzytelnione szyfrowanie w specjanych sieciach telekomunikacyjnych, Ph. D. thesis, Military Technical Academy, Warsaw (2013).

[16] Jovanovic P., Luykx A., Mennink B., Beyond 2c/2 security in sponge-based authenticated encryption modes, http://eprint.iacr.org/2014/373.pdf.

[17] Khovratovich D., Key wrapping with fixed permutation, http://eprint.iacr.org/2013/145.pdf.

[18] Leśniewicz M., Sprzętowa generacja losowych ciągów binarnych, Hardware generation of binary random sequences, WAT, Warszawa (2009).

[19] Morawiecki P., Pieprzyk J., Parallel authenticated encryption with the duplex construction, http://eprint.iacr.org/2013/867.pdf.

[20] Morawiecki P., Pieprzyk J., Srebrny M., Rotational cryptanalysis of round-reduced Keccak, FSE (2013).

[21] Naya-Plasenica J.M., Rock A., Meier W., Practical analysis of reduced-round Keccak. INDOCRYPT 2011, LNCS 7107, Springer-Verlag (2011): 236–254.

[22] Rogaway P., Shrimpton T., The SIV Mode of Operation for Deterministic Authenticated-Encryption (Key Wrap) and Misuse-Resistant Nonce-Based Authenticated Encryption (2007).

[23] Schindler W., Killmann W., Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications, Workshop on Cryptographic Hardware and Embedded Systems CHES, Springer-Verlag Berlin Heidelberg (2003).

[24] Wicik R., Borowski M., Randomness testing of some random and pseudorandom sequences, Military Communication Conference, Prague (2009).