Random keys for classified cryptographic systems

Mariusz Borowski

Military Communication Institute
22A Warszawska Str., 05-130 Zegrze, Poland
m.borowski@wil.waw.pl

Abstract. Assured security is the desirable feature of modern cryptography. A one-time pad cipher may be used to ensure perfect (unconditional) security. There are many ciphers and other cryptographic transformations, which are not perfect, but ensure conditional security adequate to needs. All cryptosystems require keys and other crypto materials. A hardware generator is the best source of random bit sequences used in production of keys for special cryptosystems. MIT has developed a generator, which can produce binary random sequences with the potential output rate of 100 Mbit/s. It gives us the capability to build an efficient key generation equipment for cryptosystems rely on the OTP cipher, as well as for cryptosystems based on symmetric or asymmetric transformations, where many of relatively short keys are needed.

Keywords: perfect security, the OTP cipher, key generation

1 Introduction

Classified information, as defined by the Polish law: "Protection of classified information act", is divided into four clauses: *top secret*, *secret*, *confidential* and *restricted*. Diplomacy, military top commands and some special government agencies need perfect (unconditional) security for stored and exchanging between them *top secret* information. Other government and military institutions classify stored and exchanged information as *secret*, *confidential* and *restricted*, if such information should be protected.

Security of top secret information is not limited by time. Interception of some plaintext by hostile state or organization can prove destructive in two months as wall as in a hundred years, then requirement of usage the perfect cipher is obvious. It is important to recall that messages that were encrypted in the 1950's with 'state of the art' not perfect cipher machines, and were kept archived by the adversary (which actually happened) are now generally broken within a few seconds, minutes or some hours at the most. On the other hand the messages that were sent 60 years ago with any realization of perfect ciphering will stay unbreakable for ever if the keys have been destroyed.

Methods of realization the perfect ciphering has changed by decades from a pencil-and-paper version to a today's PC computer system equipped with modern software and provided other then confidentiality cryptographic services [11]. It is interesting that all the methods have the same perfect security. Obviously perfect security is not for free. The perfect cipher requires random keys as long as the plaintext, a data management system and a robust, trusted key distribution system. Development of secret communications causes growing demand for cryptographic keys, especially in systems which use symmetric ciphers with private keys. One of the basic problem in key generation systems is an efficient source of random bit sequences.

In Military Communication Institute (MCI), from the nineties we have been developing hardware random number generators and key generation systems for cryptographic systems based on perfect and no perfect ciphers utilized one-time, private and public keys. We observe continuous growth of demand for random bits in key generation systems. We started from random generators with a bit rate 115 kbit/s, then we constructed 1 Mbit/s and 8 Mbit/s random generators to meet requirements. Now we have possibility to hardware generation of binary random sequences with the potential bit rate 100 Mbit/s. It will eliminate the restriction connected with availability of very long one-time keys for perfect ciphering and many short keys for non perfect ciphering.

2 One-Time Pad

The one-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where a plaintext is combined with a random key. The one-time pad was developed in 1917 by Gilbert Vernam for use on telex machines. We can only talk about OTP, if four important rules are followed. When rules are applied correctly, the one-time pad can be prove unbreakable. However, if only one of these rules is disregarded, the cipher is no longer unbreakable.

1. The key is as long as the plaintext.
2. The key is truly random.
3. There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers).
4. The keys are used only once, and both sender and receiver must destroy their key after use.

Electro-mechanical OTP cipher machines were manufactured from the fifties to the seventies and widely used in diplomacy and army on the highest levels of command. Wide usage of microprocessor, personal computers, magnetic data storage made possible to replace electro-mechanical crypto machines in the nineties. Newly designed OTP cipher machines should ensure unconditional information confidentiality by the OTP cipher usage. Moreover, it should provide additional cryptographic services:

- integrity of messages;
- cryptographic confidentiality of one-time keys;
- integrity of one-time keys;
- authentication of correspondent machines;
- authentication of the key generation station;
- authentication of operators;
- an automatic key generation according to the plan of secure connections
- compression of data to be ciphered;
- electronic accountability;
- electromagnetic emanation protection.

Many OTP secret connections enhance demands for keys and this cause problems with generation. Now we take up a challenge of extend the key generation system for OTP machines [1], [10] constructed in our Institute over ten years ago. Hardware generation of binary random sequences with the a potential bit rate of 100 Mbit/s eliminates the restriction connected with availability of many very long one-time keys for perfect ciphering. Large amount and size of one-time keys also force a change of carriers used for transferring keys from generation system to ciphering devices.

3 Hardware random generator with an output rate of 100 Mbit/s

Binary random sequences have numerous applications in many fields of science and security (military) usage. Due to the lack of trusted sources of truly random sequences Military Communication Institute researched, implemented and developed a family of hardware random bit generators, first in the nineties. The devices can generate random sequences with an output rate 115.2 kbit/s (SGCL-1) up to 8 Mbit/s (SGCL-1MB). Both were certified [8] by the Polish national security authority according to the "The protection of classified information act" and can be used in cryptographic systems up to top secret level [10]. We implemented these generators in many cryptographic systems designed for generation of keys. In the Figure 1, the overall structure of the electronic device is presented.

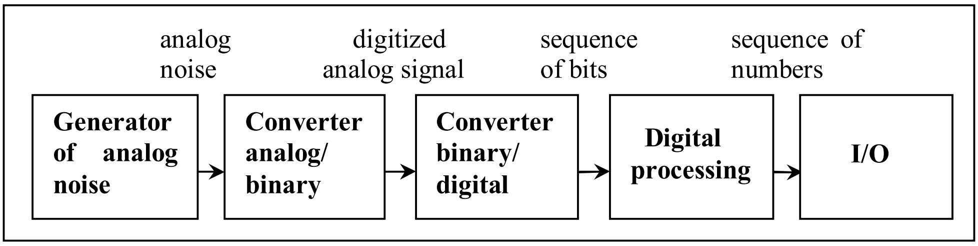

Fig. 1. Electronic device of random generation

In 2012 MIT started the project of 100 Mbit/s hardware generator. The theoretical goal of the project is to developing mathematical and technical methods of generation, giving rise to the physical structure of the generator, implementing the hardware generation of binary random sequences with the potential throughput (amount of data per unit time) 100 Mbit/s, supported by a mathematical proof of their randomness, which guarantees a set of sequences with required probabilistic characteristics and parameters, confirmed by statistical research [1]. The generator (a practical part of the project), will be allowed to be used in cryptographic systems up to top secret level. It will also be able to be used in any scientific and technical applications.

As a scientific tool the SGCL-100M generator will be used in advanced researches in the field of probability theory, the theory of stochastic signals and information theory. Assumptions of such high bit-rate output of the generator is caused by the fact, that in most modern applications very large samples of random sequences are needed, reaching gigabytes on one calculation or simulation. At the rate 100 Mbit/s a sample of 1 GB size is generated in approximately 90 seconds.

OTP cipher machines use one-time keys as long as a plaintext (and only once) so key accessibility is critical [1]. Possibility for hardware generation of binary random sequences with the potential bit rate 100 Mbit/s eliminates restrictions connected with availability of very long one-time keys for OTP cipher. The SGCL-100M will be able to generate continuously the one-time keys with a bit rate 100 Mbit/s. The keys can be recorded by a data management system for OTP cipher machines to mass storage. The generator will be able to produce a little more than 1 TB one-time keys per day and act as a practically "infinite" source of one-time keys.

The prototype of the generator and the necessary documentation will be forwarded to the certification. The generator will have to possess a "certificate of type" up to top secret level issued by the national security authority. The data management system for OTP cipher machines is a perfect place to use the SGCL-100M generator.

3.1 Outline of hardware generation of binary random sequences

Military Communication Institute has already an outline of theory of hardware generation of binary random sequences, which involves generation of many binary (little) imperfectly random component sequences and their post-processing using an XOR sum to the form of perfectly random output sequences, then their superposition into one sequence.

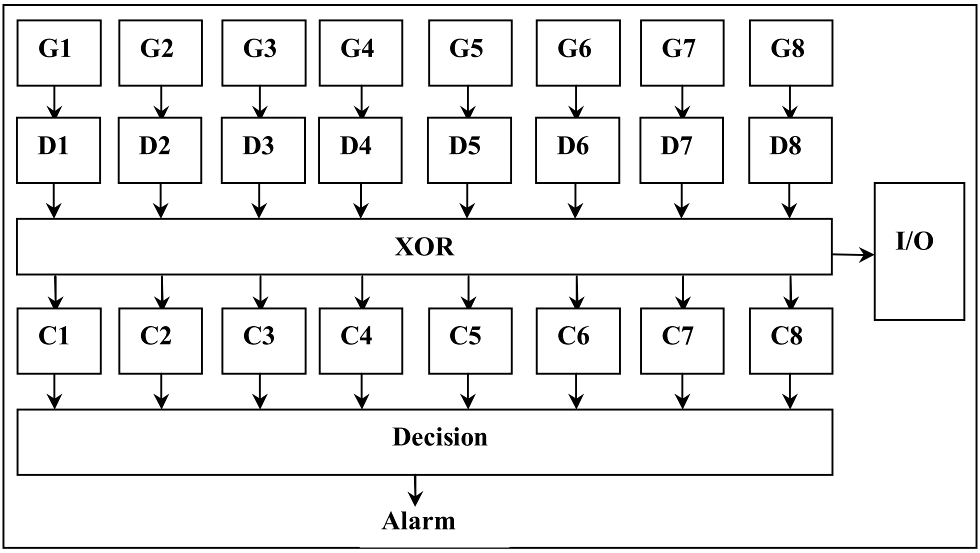

Fig. 2. Schedule of electronic realization of the SGCL-1MB generator

Outline of the electronic realization of the SGCL-1MB generator is presented in Fig. 2. Gn denotes imperfectly random generators (the source of noise and comparators). Dn denotes digital converters (flip-flops) and Cn denotes tests of randomness. The XOR sum produces an output stream of bits and almost eliminates lack of balance between '0' and '1' coming from eight generators G. MIT has published reviewed monograph [5]. The monograph describes the problem of generation of sequences of 8 Mbit/s rate.

The essence of the SGCL-1MB generator work is based on following principles:

- Source random sequences are passed from exits of D*n* flip-flops on K*n* inspector controllers testing entropies of all sequences in the real time.
- The entropy of every of these sequences is obviously not isolated and depends from the so-called randomness errors of the sequence on which set the relative bias of „0" and „1" number, $s = |n(0) - 1/2| = |n(1) - 1/2|$ (in the compartment from $s = 10^{-3}$ to $s = 10^{-2}$) and correlations between next bits in the sequence, results from sampling of the Poisson signal. It is easily to estimate [3], that entropy of sequences about such bed randomness parameters contains in the compartment from $H = 1 - 3.7 \cdot 10^{-4}$ to $H = 1 - 3.7 \cdot 10^{-6}$, what makes up very weak values but well-known and fully controlled, just thanks to the possibility of continuous measurement of the „0" and „1" number bias and the frequencies of pass in the Poisson signal.
- The creation of the output sequence follows in the arrangement of the digital processing of source sequences, subjected the parallel operation XOR, what minimizes the randomness errors of the output sequence. On the basis generated so far and the examined tests of above 1 TB sequences which came from about thirty various generators of this type, there are no bases to rejection of the hypothesis about the randomness of sequences produced by our constructed generator.

- In the case, when any randomness errors of any source sequences grows up unacceptably ($s > 10^{-2}$ or $K > 10^{-2}$), reducing the admissible entropy of the given sequence, and as the consequence of the output sequence, the decision circuit raises the alarm and the generator switches off.

An introduction to the further work will be dedicated the analysis and synthesis of the mathematical basis of the theory of perfect and imperfect binary random sequences and impaction of requirements for generated sequences. Important area will devoted to the analysis of selecting a source of randomness, conducted on the basis of analytical investigations and results of the author's experience. Theoretical support of the analysis is the theory of analog and binary stochastic noise signals. As a result of these studies, conditions for selection of potential sources of randomness will be indicated, leading to a physical source of randomness in the form of avalanche diodes batteries, which generate Poisson signals with controlled randomness. The target theory of generation, however, there will be formulated on the basis of the author's approach, using the original theory, based on integrated considerations, resulting from the above experiences. Experimental support for the scientific tools will be resulted from the experiments and statistical measurements.

Proof of randomness of generated sequences will be based on the analysis and synthesis of Poisson signals, modeled as a stochastic, binary Markov chains. The methodology of the proof will be based on probabilistic-signal risk analysis of imperfectly random sequences generation [3]. In addition to assessing the quality of sequences in the above sense, the security analysis of the generator operation will be made from the viewpoint of electromagnetic compatibility and electromagnetic leakage of information.

Theoretical part of the work also requires to formalize the mathematical description and to show what properties and parameters will have generated sequences. Then, the prototypes of generators will be constructed, which will be used for the practical verification of the theory.

3.2 Realization of the SGCL-100M generator

Technical design problems connected with the SGCL-100M generator are encountered on two levels - the electronics and the programming. The electronic board of the generator will consist of 48 generators, which must be calibrated to generation state consistent with the Poisson signal theory. The stability of the properties and parameters of such a signal as a function of time and climate-mechanical exposures must be tested. The electronic system will also consist of a programmable chip, in which all post-processing operations will be performed, including formatting of the sequence before its sending. Transmission of the sequence from the generator to a computer will take place through a standard 100Base-TX Ethernet. As handling of this interface with full throughput is a very difficult task, the dedicated Ethernet interface controller will be used and it will be controlled by RISC microprocessor that will perform the data transfer between the programmable chip and a controller in Direct Memory Access mode. In practice, only such solution allows to achieve full throughput of 100 Mbit/s. Outline of the electronics is presented in Fig. 3.

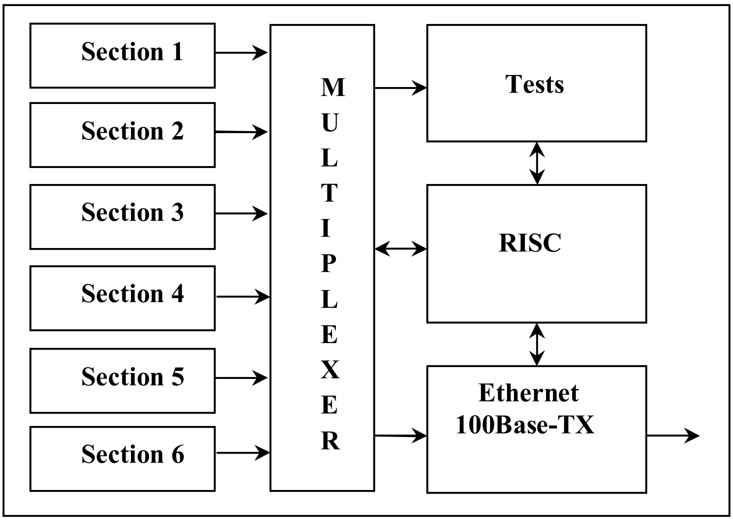

Fig. 3. Outline of 100Mbit/s random bit generator

The essence of the 100Mbit/s generator work is based on following principles:

- Every section is a copy of the technical solutions of the SGCL-1MB generator in the draft layout sense.
- Every section is a 16.384 Mbit/s random sequence source. This value results from duplication of the testing frequency of Poisson signals. Such testing does not enlarge the randomness errors above established $s < 10^{-2}$ and $K < 10^{-2}$, because we used selected avalanche diodes (the raised frequency of changes crossing $2\lambda = 70$ MHz).
- The construction contains six sections, clocked by the same 16.384 MHz clock tact synchronically, what lets to get $6 \cdot 16.384$ Mbit/s = 98.304 Mbit/s.
- A multiplexation can be made on any principle, but optimum algorithm takes six synchronic bits from all six generator sections in parallel and then formats them in frame boxes. Notice, that different, than the systematic algorithm of taking bits will not let on obtainment of a full 98.304 Mbit/s output. There are excluded any algorithms of multiplexation controlled by the values of bits from generated sequences or the usage many times the same bits from any sequences.
- The standard Ethernet 100Base-TX is the optimum interface to send the 98.304 Mbit/s output stream. The interface enables an efficient 100 Mbit/s random sequences transmission from the generator to a computer.

The generator is a very complex hardware object requiring the software. The software is generally required by two circuits – a programmable chip (a program in AHDL, a VHDL language in the corporate version of Altera) and RISC microprocessor (programs in C/C++ with "inserts" in the assembler). The both softwares must be optimized due to the efficiency of data transfer, to avoid a conflict with the essential functions of a random sequence generation. The correctness of theoretical assumptions and the correctness of technical solutions - including software - will be confirmed experimentally by statistical testing of generators at all stages of the development [10].

3.3 Our statistical tests

The 100 Mbit/s random generator can pass the tests for randomness of the NIST Statistical Test Suite and the MCI battery test [10], [6]:

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 observed frequencies with the expected ones. For the whole sequence the hypothesis testing in a classical manner is used, where the hypothesis H0 that the variable is random is verified using calculated statistics with significance level p=0.05. Classes of tests' results for 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.1.

Table.1. 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.2. It shows that percentages of classes are similar to the expected appearances of classes for random sequences (see Table.1). The obtained results confirm that the generator has very good statistical quality.

Table.2. Percentages of classes for 10 GB sequences from the reseedable pseudo random bit generator

Sequence	**A+B+C**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
N.1	95.05	80.20	9.70	5.15	2,97	1.32	0.25	0.38	0.04
N.2	94.98	79.96	10.05	4.97	2.53	1.47	0.47	0.44	0.11
N.3	94.72	79.83	10.22	4,67	2.74	1.55	0.48	0.45	0.06
N.4	95.28	79.93	10.31	5.04	2.39	1.45	0.47	0.34	0.07
N.5	95.09	80.26	9.68	5.15	2,95	1.30	0.24	0.39	0.02

The generator is very efficient and can produce binary pseudo-random sequences with the potential throughput (amount of data per unit time) higher than 150 Mbit/s in the 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.

4 Data management for OTP crypto machines

Data management systems have been subject to big changes over the time of cryptographic systems development. At the beginning they were simple elements – key generators – producing only keys in open (not encrypted) form. The other operation connected with data processing (i.e. protecting, storing) were carried out a person. Such kind of the key management system was used by the OTP cipher machines in the seventieth.

In the next stages tasks of system development generators were widened to recording results, protection (ciphering), and authentication. Such extended systems are called generation systems. As a result of a rising number of cryptographic devices and development of computer systems, generation systems were equipped with mechanisms of planning secure connections and an element responsible for distribution. Only such systems can be called cryptographic data management systems. These complex management systems has been built since the middle of the nineties. They raised efficiency of data processing and security. The data management systems are intended to deliver correct and reliable key data to proper cryptographic devices. OTP cipher machines demand a data management system [7]. The system consists of: a secure connecting planning station and a key generation station. OTP cipher machines can work in two modes: ”in a direction way” and “in a circular way” These two modes of operation should be introduced by the secure connecting planning station.

4.1 Planning secure connections

The main aim of a planning secure connection station is to implement only really necessary connections in an OTP cipher machines net. The OTP cipher machine uses one-time keys and time of generating keys is an important factor of a key generating process. “In a direction way” mode needs generation of unique keys for each direction therefore an automatic making connection “each to each” is disabled in the planning station. “In a circular way” mode needs only generation of unique keys for a whole circular. The information about the OTP cipher machine planned networks includes the number of OTP cipher machines, types of directions, number of one-time keys. Then the information goes to the key generation station. The planning station should be built with the use of a hardened, electromagnetic emanation leakage resistant computer set.

4.2 Generation of one-time keys

The key generation station generates keys on the basis of the information obtained from the planning secure connections station. The keys are generated for all algorithms used by the OTP cipher machine. Of course the longest time is needed for generating one-time keys. One-time keys are automatically generated, ciphered and signed by the key generation station. Cryptographic keys do not leave the station unprotected: ciphered one-time keys are copied on carriers and symmetric and asymmetric keys needed to fulfill additional cryptographic services of OTP cipher machines are transferred to temper-resistant smart cryptographic modules.

The quality of generated keys depends on a random number generator. The key generation station uses a hardware random bit generator. Basic characteristics and parameter of the generator:

- good statistical quality of generated binary random streams confirmed by appropriate statistical tests [9], [6], [2];
- user-friendly utilization and maintenance of generated bit streams quality;
- alarm activation while statistical defects are detected [10].

The random bit generator will have a “certificate of type” issued by the national security authority. The certificate must determinate that the generator is suitable for generating data for usage in cryptosystems up to top secret level.

4.3 One-time pads in today's world

In the PC computer era, modern algorithms such as symmetric block ciphers and asymmetric public key algorithms replaced one-time pads because of practical considerations and key distribution solutions. Modern crypto algorithms provide practical (not proved) security and privacy, essential to our economy and everyday life. However, top commands of the arm forces and some special military and government institutions need ever lasting absolute security and privacy, and in practice that's only possible with one-time encryption.

Some experts argue that the distribution of large quantities of one-time pads or keys is impractical. This was indeed the limitation in the era of paper tapes on reels and paper pads. However, today’s electronics, as the SGCL-100M generator will be able to act as practically “infinite” source of one-time keys. Current data storage technology such as USB sticks, DVD’s, external hard disks, solid-state drives or dedicated carriers enable the physical transport of enormous quantities of truly random keys. Actual sensitive communications are often limited to a small number of important users. In such cases, one-on-one communications with the associated key distribution, possibly in configuration with a star topology, is no longer a practical problem, especially considering the security benefits. By using a so-called sneakernet (transferring data on removable media by physically couriering), you can reach a throughput of one-time keys that is greater than what a network can process on encrypted data. In other words, it could take a few hours to drive a terabyte of key material, stored on an external drive, but it will take days or even weeks to consume that amount of keys on a broadband network. A terabyte sized key can easily encrypt e-mail traffic of special (military or diplomacy users) for a year, including attachments. Therefore, one-time key encryption is still well-suited in specific circumstances where absolute security is preferable to practical considerations, regardless the cost of secure physical transport of keys by couriering.

5 Generation of keys for non perfect cryptosystems

Modern communication systems, which store, process and transmit classified information, consist of several hundred or even several thousand cryptographic devices, which require huge amounts of cryptographic data. The generation of cryptographic data entails the performance of large amount of time-consuming calculations and does not only relate to the problem of generating cryptographic keys, but also to their appropriate protection against errors, disclosure, labeling and storage.

The currently applied systems and tools for generating cryptographic data are not very efficient for large communication systems, where symmetric keys are used. For every secure information relation, appropriate cryptographic data should be assumed, e.g. if there is n=100 devices, at least $\frac{1}{2} \cdot n \cdot (n - 1)$, i.e. nearly five thousand cryptographic data for the “each to each” information relation model should be prepared. The planning, generation and distribution of cryptographic data for such a large network is a technically complicated system.

The cryptographic key generation subsystem for special networks consists of one or several combined computer stations. These stations perform various functions within a system.

A station for special network planning and cryptographic data distribution is to implement necessary connections in a secure network. Proper functioning of a secret data information system requires designing of a network made up of encryption devices and software as well as providing cryptographic data to every device and user (keys, passwords). This operation is carried out regularly at certain time intervals (every few/several months). When planning, the need to immediately generate data in particular emergency situations should be taken into account. Once generated, the cryptographic data should be combined into sets and distributed to loading stands or directly to the devices. The data ought to be delivered in a safe manner, so as to preclude its disclosure and unauthorized modification.

A cryptographic key generation station serves the cryptographic data generation for every cryptographic device operating within a secure communication network. The data is secured within the distribution period. The cryptographic key generation station is most often built based on a personal computer with attached external devices such as the hardware random sequence generator, order station and data preparation for distribution in the system. The cryptographic data generation station should generate data necessary for the operation of various cryptographic algorithms such as stream and block ciphers, message signing and different passwords for cryptographic devices and systems.

Development of secret communications causes growing demand for cryptographic keys, especially in systems which use symmetric ciphers with private keys. One of the basic problem in key generation systems is an efficient source of random bit sequences. Currently used in key generation systems random generators with an output bit rate from 115 kbit/s to 8 Mbit/s will be not sufficient in the future. Now we are capable of the hardware generating binary random sequences with the potential 100 Mbit/s bit rate. It will eliminate the restriction connected with availability of large amount of keys for non perfect ciphering.

6 Conclusions

All cryptographic systems require keys and other crypto materials. These cryptographic keys should fulfill many conditions and randomness is the most obvious. The SGCL-100M generator shown in Figure 3 and described in chapter 3 of the article will be able to produce a little more than 2^{40} random bytes per day and act as a practically "infinite" source of a random material for any keys producing. The generator will have a "certificate of type" issued by the national security authority. The certificate must determinate that the generator is suitable for generating data for usage in cryptosystems up to *top secret* level. A data management system for classified communication systems is a perfect place to use the SGCL-100M generator. Capability to one-time keys generation or generating random keys for non perfect cryptosystems will be no limitation any longer.

As a scientific tool the SGCL-100M generator will be able to use in advanced researches in many fields of science and technology. The most important ones are cryptography, theory of stochastic signals, information theory, statistics, numerical computation, stochastic simulations using the Monte Carlo method, and many others. Since the generator is a quite complex and costly device 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.

References

[1] Borowski, M., Wicik, R,: A one-time cipher machine for Polish Army. Military Communication Conference, Prague, 2008

[2] Gliwa, R., Leśniewicz, M., Wicik, R.: Testing of hardware-based random bit generators utilized in cryptography. National Telecommunication Symposium, Bydgoszcz, 2002

[3] Komorowski, P., Leśniewicz, M.: Sprzętowy generator binarnych ciągów losowych o wyjściowej przepływności 1 MB/s. A hardware binary genertaor with output throughput 1 MB/s. X Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2006

[4] Leśniewicz, M.: Sprzętowa generacja ciągów losowych z przepływnością 100 Mbit/s. Hardware generation of binary sequences with throughput 100 Mbit/s. Przegląd Telekomunikacyjny nr 11/2011

[5] Leśniewicz M.: Sprzętowa generacja losowych ciągów binarnych. Hardware generation of binary random sequences. WAT, Warszawa 2009, ISBN 978-83-61486-31-2.

[6] Menezes A.J,, van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. CRC Press, 1997

[7] D. Rijmenants', Cipher Machines and Cryptology, Historical and Technical Information about Crypto Machines, Cryptology and Free Software Simulations, http://users.telenet.be/d.rijmenants/index.htm

[8] Register of certified cryptographic equipment, http://www.skw.gov.pl/BezpIT/certyfikacja_lista.htm

[9] Schindler, W., Killmann, W.: Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. Workshop on Cryptographic Hardware and Embedded Systems CHES, 2002, Springer-Verlag Berlin Heidelberg 2003.

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

[11] http://www.cryptomuseum.com/crypto/otp.htm