

MULTI-BLOCK CHAINING-BASED AUTHENTICATION MODE¹

Huang Yuhua^{**} Hu Aiqun^{*} Zhong Ziguo^{*}

^{*}(Research Center of Information Security, Southeast University, Nanjing 210096, China)

^{**}(College of Info. Science & Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 210016, China)

Abstract A fast authentication mode based on Multi-Block Chaining (MBC) is put forward; and its security is proved. The MBC mode is for new generation block cipher algorithms. Its speed is about 13% faster than that of the authentication modes in common use (for example, cipher block chaining-message authentication code mode). The dependence test results meet the requirement. The MBC mode is complete; its degree of avalanche effect is about 0.9993; its degree of strict avalanche criterion is 0.992 or so. The frequency test results indicate that the output generated by the MBC mode has uniformity. The binary matrix rank test results imply that it is linear independent among disjoint sub-matrices of the output. Maurer's universal statistical test results show that the output could be significantly compressed without loss of information. Run test, spectral test, non-overlapping template matching test, overlapping template matching test, Lempel-Ziv compression test, linear complexity test, serial test, approximate entropy test, cumulative sums test, random excursions test and random excursions variant test results fulfill the requirements of all. Therefore the MBC mode has good pseudo-randomness. Thus the security of MBC mode is verified by the way of statistical evaluation.

Key words Block cipher algorithm; Authentication mode; Statistical evaluation; Pseudo-randomness

I. Introduction

The block cipher algorithm is one of the encryption algorithms in common use. It only defines a function turning a block of plaintext into a block of cipher-text. Usually the length of message to be encrypted and authenticated is much more than a block. Thus a block cipher mode is necessary^[1]. Operation modes of block cipher algorithm include encryption mode, authentication mode and authenticated encryption mode. Only authentication modes would be studied in this paper.

The Cipher Block Chaining-Message Authentication Code (CBC-MAC) mode^[2] is a standard authentication mode in most common use for block cipher algorithms. Most of authentication modes are modified modes on CBC-MAC, for example, the eXtended CBC-MAC (XCBC-MAC) mode^[3] and the Randomized MAC (RMAC) mode^[4]. The latter was recommended by National Institute of Standard & Technology (NIST) of USA.

Among those existing authentication modes, the Parallelizable MAC (PMAC) mode^[5] is a parallelizable authentication mode, which has distinctive idea. Other authentication modes do not go beyond

the thinking of CBC-MAC mode. Therefore the thought of multi-block might be the only way to design securer and faster authentication modes.

Generally the block size of new generation block cipher algorithm is no less than 128 bits, while the key length is variable, for instance, AES (Rijndael)^[6], RC6 and Camellia, etc. The fast authentication mode to be presented in this paper is for these block cipher algorithms.

Usually authentication modes have 3 input parameters: plaintext (message) P , secret key K and Initialization Vector (IV). Generally IV is a counter or an unrepeated pseudo-random number, which is for anti-replaying^[2]. On current conditions, a 64-bit counter is enough^[7]. A 48-bit counter will be adopted in IEEE 802.11i Wireless Local Area Network (WLAN)^[8]. For the sake of universality, a 64-bit counter would be employed in this document.

II. Authentication Mode Based on Multi-Block Chaining (MBC)

Here after^[4] $E_K(P)$ represents the encipher function of the block cipher algorithm under the key K applied to the plaintext block P ; T the block size; k the key length in bytes for the block cipher, denoted by an 8-bit number; m the bit length of the MAC; n the number of data blocks in the padded plaintext; L the byte length of unpadded plaintext, denoted by a 56-bit number; $P||Y$ the concatenation of two bit strings P and Y ; $P\oplus Y$ the bitwise eXclusive-OR (XOR) of two bit strings P and Y of the same length; $MSB_m(Y)$ the bit string consisting of the m left-most bits of the bit string Y ; τ the byte length of the last block of unpadded plaintext; P_i the i -th block in the partition of the padded plaintext;

¹ Manuscript received date: September 13, 2004; revised date: December 14, 2004.

Supported by the National Hi-Tech Research & Development Plan of China (863 Project) (No.2003AA143040) and Jiangsu Provincial Key Laboratory of Network & Information Security (No.BM2003201).

Communication author: Huang Yuhua, born in 1975, male, Ph.D. candidate. Research Center of Information Security, Southeast University, Nanjing 210096, China. hyuhua2k@163.com.

$P[i]$ the i -th byte of the padded plaintext; and $P+Y$ the byte-wise sum (mod 256) of two bit strings P and Y of the same length.

1. Authentication mode based on Triple-Block Chaining (TBC)

The authentication mode on the basis of TBC may be denoted by $\text{MAC} = \text{TBC}(\text{IV}, K, P)$. Its arithmetic operations are performed as follows.

(1) Padding: $Y_{-1} = \text{IV} \parallel k \parallel L$; (It might be agilely processed according to the actual case).

If L can be divided exactly by T (48 bytes), the plaintext padding is not necessary; otherwise for $i=1$ to $T-\tau$, $P[L+i]=P[i]$ (periodic padding).

This padding way of the beginning and the end echoing each other might have some significance to the security of recurrence authentication algorithms.

(2) Partition: The padded plaintext is partitioned into n big blocks by 384 bits; each big block is divided into 3 small blocks by 128 bits.

(3) Generating unrepeated & secret pseudo random number: $Y_0 = E_K(Y_{-1})$;

(4) Recurrence: $Y_1 = E_{(P_1+Y_0)\parallel(P_2+Y_{-1})}(P_3 \oplus Y_0)$;
if $n > 1$ { for $i = 2$ to n

$$Y_i = E_{(P_{3i-2} \oplus Y_{i-3}) \parallel (P_{3i-1} \oplus Y_{i-2})}(P_{3i} \oplus Y_{i-1});$$

$\text{MAC} = \text{MSB}_m[E_K(Y_n)]$.

On account of that the key length of new generation block cipher algorithm is variable, the last block of plaintext may be flexibly processed to speed up in some degree.

The TBC mode is applicable to any block cipher algorithm whose key length is twice of block size, for example, IDEA^[2] and SHACAL2, etc (the initialization step needs to be modified).

2. Authentication mode based on 2.5-Block Chaining (eBC)

(1) Padding: $Y_{-1} = \text{IV} \parallel k \parallel L$; $T = 40B$; for $i = 1$ to $T - \tau$, $P[L+i] = P[i]$;

(2) Partition: The padded plaintext is partitioned into n big blocks by 320 bits; each big block is divided into 2.5 small blocks by 128 bits (the bit length of P_{3i-2} is 64).

(3) Generating unrepeated pseudo-random number: $Y_0 = E_K(Y_{-1})$;

(4) Recurrence:

$$Y_1 = E_{[P_1 + \text{MSB}_{64}(Y_0)] \parallel (P_2 \oplus Y_{-1})}(P_3 \oplus Y_0);$$

if $n > 1$ { for $i = 2$ to n

$$Y_i = E_{[P_{3i-2} \oplus \text{MSB}_{64}(Y_{i-3})] \parallel (P_{3i-1} \oplus Y_{i-2})}(P_{3i} \oplus Y_{i-1});$$

$\text{MAC} = \text{MSB}_m[E_K(Y_n)]$.

It might be elastically processed to design a similar authentication mode for any specific block cipher algorithm in terms of its block size b and key

length k (Let block length of authentication mode $T = b + k$).

III. Proof on Security of MBC Mode

The method of proof is described in Ref.[9]. Assume that the basic block cipher algorithm E is secure. In order to simplify the proof, we assume that the CBC-MAC mode is secure. Let $\text{Perm}(m)$ denote the set of all permutations on m -bit field $\{0,1\}^m$. Let A be an adversary (a probabilistic algorithm) with access to an oracle, and suppose that A always outputs a bit. Define^[5]

$$\text{Adv}_E^{\text{prp}}(A) = \Pr[K \xleftarrow{R} \kappa : A^{E_K(\cdot)} = 1] \\ - \Pr[\pi \xleftarrow{R} \text{Perm}(m) : A^{\pi(\cdot)} = 1]$$

The above description is the probability that adversary A outputs 1 when given an oracle for $E_K(\cdot)$, minus the probability that A outputs 1 when given an oracle for $\pi(\cdot)$, where K is selected randomly from κ and π from $\text{Perm}(m)$.

Let $\text{Adv}_{\text{MBC}}^{\text{auth}}(A) = \Pr[K \xleftarrow{R} \kappa : A^{E_K(\cdot)} \text{ forges}]$. We emphasize that the nonce used in the forgery attempt may coincide with the nonce used in one of the adversary's queries.

Lemma 1 Security of Pseudo-Random Function (PRF) families

Function family $F : \{0,1\}^T \rightarrow \{0,1\}^m$ is said to be a secure PRF family if for any distinguisher who makes at most q oracle queries and runs in time at most t , and it is the case that

$$\text{Adv}_F^{\text{prf}}(q, t) \leq (1 + \dots + q) / 2^m = q(q+1) / 2^{m+1},$$

where $T \geq m$.

The proof of Lemma 1 can be found in Ref.[5].

$V_T(\sigma_1, \sigma_2)$ measures the probability of running into trouble when the adversary asks some two particular oracle queries of the specified lengths, where the trouble means that a block-cipher input associated to the first message coincides with a block cipher input associated to the second message.

Lemma 2 CBC collision bound

Assume that the output length is m -bit. Let M_1, M_2 be distinct strings having σ_1, σ_2 blocks, then $V_T(\sigma_1, \sigma_2) \leq (\sigma_1 + \sigma_2) / 2^m$

The proof of Lemma 2 can be seen in Ref.[10].

Theorem 1 Fix TBC parameters $m = T/3$. Let A be an adversary that asks q queries and then makes its forgery attempt. Suppose that q queries have aggregate length of σ blocks. Then

$$\text{Adv}_{\text{TBC}}^{\text{auth}}(q, t) \leq \text{Adv}_E^{\text{prp}}(q', t') + \frac{2q^2\sigma^2 + q^2 + 1}{2^m}$$

where $q' = \sigma q, t' = t + O(\sigma q t)$.

Proof: The block size $T > m$, so $\text{Adv}_F^{\text{prf}}(q, t) \leq$

$(1 + \dots + q)/2^m = q(q+1)/2^{m+1}$. The birthday probability^[11] $\Pr(m, q) \leq C_q^2/2^m$, where $C_q^2 = q(q-1)/2 < q^2/2$. Then

$$\begin{aligned} \text{Adv}_{\text{TBC}}^{\text{auth}}(q, t) &= \text{Adv}_E^{\text{prp}}(q', t') + C_q^2 V_T(\sigma_1, \sigma_2) \\ &\quad + C_q^2/2^m + \text{Adv}_F^{\text{prf}}(q, t) + 1/2^m \\ &\leq \text{Adv}_E^{\text{prp}}(q', t') + \frac{q^2}{2} \frac{4\sigma^2}{2^m} + \frac{q(q-1)}{2^{m+1}} \\ &\quad + \frac{q(q+1)}{2^{m+1}} + \frac{1}{2^m} \\ &= \text{Adv}_E^{\text{prp}}(q', t') + \frac{2q^2\sigma^2 + q^2 + 1}{2^m} \end{aligned}$$

Q.E.D.

On condition that the queries are the same, the number of blocks σ of MBC mode is less than that of authentication modes in common use, that is, the bound of MBC mode is less than that of common used authentication modes. It means that the security of MBC mode might be higher than that of traditional authentication modes. For multi-block of plaintexts are nonlinearly processed at one time, the local diffusion and confusion characteristics of MBC mode are better than those of general authentication modes.

IV. Speed of MBC Mode

Assume that the AES algorithm is adopted. On condition that the size of CPU is 2.4GHz, the speed of XOR operation is about 1444Mbps; the encryption speed of AES-128 (the key length k is 128-bit) or AES-192 is 200Mbps or so; the speed of AES-256 is about 170Mbps. The speed of AES-128 without key schedule is 433Mbps or so. Each block of plaintext needs XOR with former recurrence results in the CBC-MAC mode. Therefore the speed of CBC-MAC mode is about $1/(1/1444+1/433)=333$ Mbps; the speed of eBC mode is $1/(1/1444+1/500)=370$ Mbps or so for 2.5 blocks of plaintexts are processed at one time; the speed of TBC mode is about $1/(1/1444+1/510)=377$ Mbps for 3 blocks of plaintexts are processed simultaneously. Thus the speed of TBC is about 13% faster than that of authentication modes in common use. Tab.1 displays the speed test results of two authentication modes in C while the key length is 128-bit.

Tab.1 Speed of authentication modes (Mbps)

Plaintext-length(B)	CBC-MAC	TBC
48	191.0448	183.7321
96	240.7524	244.5860
240	286.5672	309.6774
480	304.7619	342.8571
720	311.3514	353.3742
1200	318.9369	360.9022
2400	322.6891	374.2690

V. Statistical Evaluation of MBC Mode

The definition of dependence test (includes the degree of completeness d_c , the degree of avalanche effect d_a , and the degree of strict avalanche criterion d_{sa}) used by statistical evaluation may be found in Ref.[12].

Definitions of frequency test, run test, binary matrix rank test, spectral test, non-overlapping template matching test, overlapping template matching test, Maurer's universal statistical test, Lempel-Ziv compression test, serial test, approximate entropy test, cumulative sums test, random excursions test and random excursions variant test are described in Ref.[13]. The definition of linear complexity test may be seen in Refs.[14,15]. The AES algorithm is adopted for all tests.

1. Dependence test

The output length of MBC mode is 128-bit; the number of inputs is 10000 in this paper. The more the number of inputs, the better the observed results.

The dependence test results showed that the degree of completeness $d_c = 1$.

(1) Dependence test of MBC algorithm in block mode: The block size of TBC algorithm is 384-bit; the one of eBC algorithm is 320-bit. For TBC-256 (the key length k is 256-bit), when a single input bit is complemented respectively, the proportions r_j that the number of changed output bits is j (from r_{37} to r_{90}) are as follows: 0.000001, 0.000001, 0.000004, 0.000006, 0.000017, 0.000033, 0.000062, 0.000120, 0.000241, 0.000438, 0.000752, 0.001260, 0.002076, 0.003332, 0.005035, 0.007457, 0.010675, 0.014812, 0.019951, 0.025980, 0.032866, 0.040269, 0.047774, 0.055054, 0.061083, 0.066128, 0.069264, 0.070499, 0.069365, 0.066276, 0.061367, 0.054845, 0.047724, 0.040163, 0.032894, 0.026074, 0.019881, 0.014770, 0.010690, 0.007459, 0.005000, 0.003288, 0.002068, 0.001275, 0.000747, 0.000430, 0.000237, 0.000125, 0.000066, 0.000033, 0.000017, 0.000008, 0.000003, 0.000002.

Other test results are displayed in Tab.2.

(2) Different input sizes for the dependence test Assume that the input size of a function F is variable and $n < N$. If F satisfies that $d_c = 1$, $d_a \approx 1$, and $d_{sa} \approx 1$ while the input length is N -bit, F usually satisfies that $d_c = 1$, $d_a \approx 1$, and $d_{sa} \approx 1$ while the input size is n -bit. The plaintext length was 1024-bit in this test. The test results meet all the demands. Due to space constraints, they were not presented.

Tab.2 Dependence test results of MBC algorithm in block mode

Modes	w (bit)	Average of w (bit)	Probability that output bit changes	Average of Pr	d_a	d_{sa}
TBC-256	$36 < w < 93$	63.998596	$0.4766 \leq Pr \leq 0.5209$	0.499989	0.999259	0.992028
TBC-192	$35 < w < 93$	63.996784	$0.4791 \leq Pr \leq 0.5228$	0.499975	0.999282	0.992020
TBC-128	$34 < w < 93$	64.001602	$0.4792 \leq Pr \leq 0.5239$	0.500013	0.999316	0.992063
eBC-256	$35 < w < 93$	64.002930	$0.4762 \leq Pr \leq 0.5211$	0.500023	0.999298	0.992014
eBC-192	$35 < w < 93$	64.000130	$0.4773 \leq Pr \leq 0.5215$	0.500001	0.999271	0.992006
eBC-128	$34 < w < 93$	63.997105	$0.4784 \leq Pr \leq 0.5207$	0.499977	0.999275	0.991995

Note: w is the number of changed output bits.

Tab.3 Test results of MBC algorithm in OFB mode

		TBC-256	TBC-192	TBC-128	eBC-256	eBC-192	eBC-128	Threshold
Frequency (monobit)	S	0.091875	0.466250	0.248125	0.338125	0.273750	0.953125	2.5758
	Pv	0.9268	0.6410	0.8040	0.7353	0.7843	0.3405	0.01
Frequency (block)	S	79.090586	98.716641	110.863320	107.966055	85.061641	92.458711	135.807
	Pv	>0.9	>0.1	>0.1	>0.1	>0.1	>0.1	0.01
Frequency (template)	S	7.675838	9.984037	12.100125	18.991675	7.797600	13.580713	30.578
	Pv	>0.9	>0.7	>0.5	>0.1	>0.9	>0.1	0.01
Runs (monobit)	S	0.335625	0.380000	1.903750	0.891875	0.910625	0.217756	2.5758
	Pv	0.7372	0.7039	0.0569	0.3725	0.3625	0.8276	0.01
Run of ones in a block	S	0.647921	0.416464	7.496126	0.955943	0.004629	4.278423	11.345
	Pv	>0.7	>0.9	>0.05	>0.7	>0.995	>0.1	0.01
Binary matrix rank	S	1.865233	1.743171	0.251117	1.156167	0.257071	0.019594	9.210
	Pv	>0.3	>0.3	>0.7	>0.5	>0.7	>0.99	0.01
Spectral	S	0.000000	1.282473	0.128247	0.448866	0.769484	0.192371	2.5758
	Pv	1	0.1997	0.8980	0.6535	0.4416	0.8475	0.01
Non-overlapping	S	32.555062	26.276914	43.313901	50.006574	30.840163	23.539157	52.191
	Pv	>0.3	>0.7	>0.05	>0.01	>0.3	>0.7	0.01
Overlapping template	S	3.849840	3.952834	8.120815	3.171335	7.970328	5.097526	15.086
	Pv	>0.5	>0.5	>0.1	>0.5	>0.1	>0.3	0.01
Universal Maurer	S	1.022406	0.022204	0.126501	0.976344	0.408940	0.728450	2.5758
	Pv	0.3066	0.9823	0.8993	0.3289	0.6826	0.4663	0.01
Lempel-Ziv compression	S	69628	69638	69615	69625	69637	69637	69561
	Pv	0.99999	$1 \cdot 10^{-9}$	0.9997	0.99999	$1 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	0.01
Linear complexity	S	1.110	9.229	7.740	3.829	7.946	2.103	16.812
	Pv	>0.975	>0.1	>0.1	0.69	>0.1	>0.9	0.01
Serial ($\nabla^2 \psi_m^2$)	S	2.880	3.456	4.480	3.328	1.856	2.752	13.277
	Pv	>0.5	>0.3	>0.3	>0.5	>0.7	>0.5	0.01
Serial ($\nabla^2 \psi_m^2$)	S	1.984	1.216	1.472	1.152	1.408	0.512	9.210
	Pv	>0.3	>0.5	>0.3	>0.5	>0.3	>0.7	0.01
Approximate entropy	S	2.851587	3.458592	4.555569	3.324505	1.826164	2.716947	13.277
	Pv	>0.5	>0.3	>0.3	>0.5	>0.7	>0.5	0.01
Cumulative (forward)	S	1803	1441	1109	1464	1034	925	2841
	Pv	0.1496	0.3088	0.5442	0.2959	0.6094	0.7091	0.01
Cumulative (backward)	S	1417	2022	1130	1284	1262	925	2841
	Pv	0.3228	0.0914	0.5266	0.4087	0.4243	0.7091	0.01

Note: S is the statistic used by each test suite respectively.

2. Statistical evaluation of MBC algorithm in OFB & CTR mode

The MBC algorithm is tested in OFB and CTR mode respectively. Due to space constraints, only the test results in OFB mode is presented. They are showed in Tab.3. All tests are started with their default inputs. It is required the level of acceptance $PV > 0.01$ ^[13].

The frequency test results indicate that the output generated by the MBC mode has uniformity. The binary matrix rank test results imply that it is linear independent among disjoint sub-matrices of the output. Maurer's universal statistical test results show that the output is not significantly compressed. Run test, spectral test, non-overlapping template matching test, overlapping template matching test, Lempel-Ziv compression test, linear complexity test, serial test, approximate entropy test, and cumulative sums test results fulfill all the requirements. Random excursions and random excursions variant test results accord with all the demands. Due to space constraints, they were not presented. Therefore the MBC mode has good pseudo-randomness. Thus the security of MBC mode is verified by way of statistical evaluation.

VI. Conclusions

A fast authentication mode based on MBC is proposed in this paper; and its security is proved. The speed of MBC mode is faster than that of authentication modes in common use (for example, CBC-MAC mode). The dependence test results meet the demands. The MBC mode is complete; it exhibit the avalanche effect; and satisfies the strict avalanche criterion. The frequency test results indicate that the output sequence generated by MBC mode has uniformity. The binary matrix rank test results imply that it is linear independent among disjoint sub-matrices of the output. Maurer's universal statistical test results show that the output is not significantly compressed without loss of information. Run test, spectral test, non-overlapping template matching test, overlapping template matching test, Lempel-Ziv compression test, linear complexity test, serial test, approximate entropy test, cumulative sums test, random excursions test, and random excursions variant test results fulfill all the requirements. Therefore the output generated by the MBC mode has good pseudo-randomness. Judged by way of statistical evaluation, the MBC mode is secure.

References

- [1] Geng Jia. Study on cryptography in wireless local area networks. Master thesis, Nanjing, Department of Radio Engineering, Southeast University, 2002, (in Chinese).
- [2] Wang Yumin, Liu Jianwei. Security of Communication Networks—Theory & Technology. Xi'an, Xidian University Press, 1999, 172–174, (in Chinese).
- [3] J. Black, P. Rogaway. A suggestion for handling arbitrary-length messages with the CBC MAC. [Http://csrc.nist.gov/CryptoToolkit/modes/proposed-modes/xcbc-mac/xcbc-mac-spec.pdf](http://csrc.nist.gov/CryptoToolkit/modes/proposed-modes/xcbc-mac/xcbc-mac-spec.pdf), 2001.
- [4] M. Dworkin. DRAFT recommendation for block cipher modes of operation: The RMAC authentication mode. NIST special publication 800-38B. [Http://csrc.ncsl.nist.gov/publications/drafts/draft800-38B-110402.pdf](http://csrc.ncsl.nist.gov/publications/drafts/draft800-38B-110402.pdf), 2002.
- [5] P. Rogaway, J. Black. PMAC (Proposal to NIST for a parallelizable message authentication code). [Http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/pmac/pmac-spec.pdf](http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/pmac/pmac-spec.pdf), 2001-04-01.
- [6] NIST FIPS Publication 197. Specification for the advanced encryption standard(AES). [Http://csrc.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf](http://csrc.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf), 2001-11-26.
- [7] Huang Yuhua, Hu Aiqun, Song Yubo. On algorithms of re-keying in network & their implementation. *Computer Engineering & Applications*, **39**(2003)35, 27–29, (in Chinese).
- [8] T. Moore. Suggested changes to RSN for IEEE 802.11. Microsoft, USA: Technical Report, IEEE 802.11-02/298r4. [Http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm](http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm), 2002-09-02.
- [9] M. Bellare, A. Desai, E. Jorjani, *et al.* A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. Proceedings of the 38th Symposium on Foundations of Computer Science, Los Alamitos, USA, 1997, 394–403.
- [10] J. Black, P. Rogaway. CBC MACs for arbitrary-length messages: The three-key constructions. Advances in Cryptology—Crypto'2000, LNCS 1880, Germany, Springer-Verlag, 2000, 197–215.
- [11] M. Bellare, J. Kilian, P. Rogaway. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, **61**(2000)3, 362–399.
- [12] P. Serf. The degrees of completeness, of avalanche effect, and of strict avalanche criterion for mars, rc6, rijndael, serpent, and twofish with reduced number of rounds. Siemens, Germany, Technical Report NES/DOC/SAG/WP3/003/1. [Http://www.cosic.esat.kule-ven.ac.be/nessie/reports/phase1/sagwp3-003.pdf](http://www.cosic.esat.kule-ven.ac.be/nessie/reports/phase1/sagwp3-003.pdf), 2000, 2–3.
- [13] A. Rukhin, J. Soto, J. Nechvatal, *et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22, <http://csrc.nist.gov/rng/SP800-22b.pdf>, 2001, 14–46.
- [14] A. Menezes, P. Oorschot, S. Vanstone. Handbook of Applied Cryptography. USA, CRC Press, 1996, 200–201.
- [15] Feng Dengguo. Cryptanalysis. Beijing, Tsinghua University Press, 2000, 58–59, (in Chinese).