www.dergipark.gov.tr
ISSN:2148-3736

El-Cezerî Fen ve Mühendislik Dergisi
Cilt: 9, No: 3, 2022 (1136-1146)

El-Cezerî Journal of Science and Engineering
Vol: 9, No: 3, 2022 (1136-1146)
DOI: 10.31202/ecjse.1129922

ECJSE

Makale / Research Paper

SAAC - Kriptosistemlerin analizi için İstatistiksel Mutlak Çığ-Etkisi Kriter Testi

Burak BAYSAN[1a*], Serhat OZEKES[2b]

[1]Uskudar University, Institute of Addiction and Forensic Sciences, Altunizade Mh. Universite Sk. No:14, 34662 Istanbul, Türkiye
[2]Uskudar University, Department of Computer Engineering, Altunizade Mh. Universite Sk. No:14, 34662 Istanbul, Türkiye
[*]burak.baysan@st.uskudar.edu.tr

Received/Geliş: 13.06.2022 **Accepted/Kabul:** 21.08.2022

Öz: İkilik sayı tabanı (*bit*) dizilerini kullanan kriptosistemler başta farksal saldırılara karşı koyabilmek için giriş ve çıkış değerleri arasında ilişki kurulabilmesini engelleyen katı çığ-etkisi kriterini yerine getirmelidir. Literatür çıkış bitlerinin en az yarısının farklılığına yer vermekteyken, bütün bitlerin değişmesinin ikilik tabandaki tümleyenine ve dolayısıyla istenmeyen bir diğer sonuca neden olacağına yer vermemektedir. Bu çalışma ile önerilen İstatistiksel Mutlak Çığ Kriteri (*SAAC - Statistical Absolute Avalanche Criterion*) testi, bir alt sınırın istatistiksel olarak belirlenmesine ve hipotezlerin kurulmasına imkan vermektedir. SAAC, Mutlak Uzaklık ölçü temelinde tasarlanmıştır. İdeal kriptosistem çıkışları için beklenti değeri ve SAAC'ın varyans değeri hesaplanmıştır. SAAC testleri sayısal sonuçları $\mathbf{n} = \{\mathbf{64}, \mathbf{128}, \mathbf{160}, \mathbf{192}, \mathbf{224}, \mathbf{256}, \mathbf{320}, \mathbf{384}, \mathbf{512}\}$ kriptosistem çıkış uzunlukları için gerçekleştirilmiştir. Deneysel testler için, 256-bit çıkışları olan Blake2s, SHA2, SHA3 ve RIPEMD mesaj özetleme fonksiyonları 10000 deneme ile kullanılmıştır ve SAAC ile Çığ-Etkisi testlerinin sonuçları karşılaştırılmıştır. Sonuçlar maksimum $\%\mathbf{50}$'lik mutlak değerin başarıyla uygulandığını göstermiştir. SAAC testi, şifreleme yöntemleri ve mesaj özetleme fonksiyonları başta olmak üzere kriptosistemlerin analizinde kolaylıkla kullanılabilir bir araçtır.

Anahtar kelimeler: Kripto; kriptanaliz; dağınım; yayınım; çığ-etkisi.

SAAC – Statistical Absolute Avalanche Criterion Test for Analysis of Cryptosystems

Abstract: Cryptosystems using binary radix (bit) arrays must first meet the strict avalanche criterion, which prevents correlation between input and output values to resist differential attacks. While the literature includes the difference of at least half of the output bits, it does not include that changing all the bits will cause the binary complement which is an undesirable result. The Statistical Absolute Avalanche Criterion (SAAC) test proposed in this study allows the statistical determination of a lower limit and the establishment of hypotheses. SAAC was designed based on the Absolute Distance measure. The expected value and variance value of SAAC were calculated for ideal cryptosystem outputs. To calculate the numerical results, SAAC tests were performed for cryptosystem output lengths of $n = \{64,128,160,192,224,256,320,384,512\}$. Some percentiles for the standard normal distribution and critical values of SAAC test were given. For experimental tests, Blake2s, SHA2, SHA3 and RIPEMD hash functions having 256-bit outputs were used with 10000 trials, and results for SAAC and Avalanche-Effect tests were compared. The results showed that maximum of 50% absolute value was successfully applied. The SAAC test is a tool that can be easily used in the analysis of cryptosystems, especially encryption methods and message hash functions.

Keywords: Crypto; cryptanalysis; confusion; diffusion; avalanche-effect.

Bu makaleye atıf yapmak için
Baysan B., Ozekes S., "SAAC - Kriptosistemlerin analizi için istatistiksel mutlak çığ-etkisi kriter testi", El-Cezerî Fen ve Mühendislik Dergisi 2022, 9 (3); 1136-1146.

How to cite this article
Baysan B., Ozekes S., "SAAC – Statistical absolute avalanche criterion test for analysis of cryptosystems", El-Cezerî Journal of Science and Engineering, 2022, 9 (3); 1136-1146.
ORCID: [a]0000-0003-2783-5430, [b]0000-0002-7432-0272

1. Introduction

Cryptology, which has become widespread in individual and corporate fields with the development of communication technologies, is the first scientific method that comes to mind when it comes to information security. Cryptology takes its name from the Greek word “krptós” meaning secret. The field of cryptology has two sub-branches within itself. The first is cryptography, which studies and develops cryptosystems; the second is cryptanalysis, which aims to decrypt confidential data by attacking cryptosystems. Cryptanalysis is used not only by attackers but also by cryptographers to monitor and improve the security of a cryptosystem. Mathematical proofs cannot always be used for the security capabilities of cryptosystems, which is especially common in hash function designs using Boolean functions. In this case, statistical approaches are often preferred by cryptographers. The most important statistical security approaches are the terms of confusion/diffusion, which observe the relationship between the input and output values of the cryptosystem and enter the literature with Shannon's work [1,2]. The substitution of any cryptographic tool is called confusion, and the transformation process is called diffusion [3]. In the common literature, confusion is accepted as the relationship between the key and the output of the cryptosystem, and diffusion as the relationship between the plaintext and the output of the cryptosystem as complex as possible [3]. On the other hand, it is avalanche-effect in a term that focuses on the value at the output, indiscriminately in the key or plaintext input of the cryptosystem, rather than confusion/diffusion. The term avalanche-effect was first used by Horst Feistel [4], but the concept goes back to Shannon's confusion/diffusion terms. The avalanche-effect occurs when a change in cryptosystem input causes significant changes in output. Here, a binary value is expected to change half of the bits in the output. If a cryptosystem does not show a strong avalanche-effect, it shows weak randomness, and an attacker can exploit this weakness to provide a correlation between the input and output values. This may lead to the breaking of part or the whole of the cryptosystem. For this reason, the avalanche-effect is a criterion that cryptosystem designers emphasize. The avalanche-effect can be observed directly in the outputs of the cryptosystem, but also in the internal functions. Here, the strict avalanche criterion (*SAC*) for Substitution Boxes (*S-Box*) has an important place. SAC was first defined by Webster and Tavares as a change of one bit in the input and a change of $1/2$ in the output bits [5].

The definitions given above form the background of the Statistical Absolute Avalanche Criterion test method proposed in this study. On the other hand, there are no studies that will enable the confusion/diffusion, avalanche-effect, and SAC methods, each of which is a continuation of the previous studies, to be brought into a statistical form supported by theorems. The problem here is that different cryptosystems with different bit lengths will have different binomial distributions and therefore different variance values. The fact that this has not been studied causes the baseline of the expected rate of change in cryptosystem output to be uncertain. Another additional problem is that in many cryptosystem studies in the literature, $\geq 1/2$ changes are expected in the output values, not $\sim 1/2$. It is not possible to include all these studies in this article, but the case studies are given in the range of Ref.[6-13]. These studies did not focus on how close an n-bit output is to a change in the ratio of $1/2$, its statistical significance and acceptability. On the other hand, in these studies, it is not observed that the change of bits at a rate of $> 1/2$ is not desirable but undesirable. All bit values consist of 0 and/or 1 value, so changing an entire n-bit output will mean the complement of the previous output. Accordingly, it is clear that will be $x/n < 50\% \Rightarrow 50\% < x/n$ for $n/2 < x$ in an x-bit change.

When the relevant literature up to the date of the study was examined, no new approach and/or method could be found regarding the avalanche-effect. This situation emerged as the biggest problem encountered during the conduct of the study. On the other hand, the necessity and purpose of the study are to fill this gap. In the literature, there are mostly analysis methods based on differential attacks. Such investigations depend on probabilistic and statistical methods but are performed specifically for the cryptosystem. On the other hand, there are many statistical methods designed for

pseudo-random number generators (*PRNG*), but they are not designed to observe the effect of a change in input value on output values. They examine whether the output values obtained by taking an entropy source as input/feed have certain randomness properties.

For the reasons explained above, in this study, it is aimed to determine a statistical limit to 50% variation and to determine different statistical lower limits for cryptosystems with different n-bit length outputs. In this study, the Statistical Absolute Avalanche Criterion (*SAAC*) test method has been proposed to fill this gap in the literature and to use it in future studies.

1.1. Literature

When the studies that have been done up to the date of this study are examined, it is encountered with studies suggesting new cryptosystems that apply the current SAC analysis rather than current studies on avalanche-effect analyses that interest this study. Therefore, the basic literature relevant to this study was included. On the other hand, the main motivation of the study is to fill this gap in the field. The first and most important source of interest to our study is Shannon's (1949) confusion/diffusion of a cryptosystem's key and plaintext inputs as complex effects as possible on the output [1,2]. The term avalanche-effect, which focuses on the effect of any input on the output rather than a key or plaintext input, was introduced to the literature by Feistel in 1973, this term is used to describe how a one-bit value in the input changes half of the bits on the output [4]. Webster and Tavares, in their study for s-box design in 1985, showed SAC that explains a situation similar to avalanche-effect, but SAC is mostly used for s-box studies in the literature [5]. Wu et al. in 2011, by giving a statistical form to the NPCR and UACI randomness tests used for image encryption methods, studied the security test with hypotheses according to the determined lower and upper critical values [14]. But this study is only for the values of pixel placement in a two-dimensional space and therefore only for image encryption. Castro et al. published a randomness test for SAC in 2005, but this study did not limit the case where the rate of change in output was greater than half, and a hypothesis form was not established [15]. In the literature review, it is seen that the current cryptosystem design studies, in which confusion/diffusion and SAC tests are carried out, perform their tests without certain statistical proofs and hypothesis form. Another notable feature is the term confusion/diffusion that is mostly used for hash functions [6-9], and the term SAC that is mostly used for s-box designs [10-13]. There are many test methods in the literature that provide randomness analysis on bit values and sequences, but they are not current studies. Mengdi et al., in their work in 2021, included methods The Frequency (Monobit) Test", "Frequency Test within a Block", "The Runs Test", "Tests for the Longest-Run-of-Ones in a Block", "The Binary Matrix Rank Test", "The Discrete Fourier Transform (Spectral) Test", "The Non-overlapping Template Matching Test", "The Overlapping Template Matching Test", "Maurer's Universal Statistical Test", "The Linear Complexity Test", "The Serial Test", "The Approximate Entropy Test", "The Cumulative Sums (Cusums) Test", "The Random Excursions Test", "The Random Excursions Variant Test", "The Poker Test", "The Runs Distribution Test", "The Binary Derivation Test", "The Autocorrelation Test", "The Disjointness Test", "The Long Run Test", "The Uniform Distribution Test", "The Comparative Test for Multinomial Distributions" ve "The Entropy Estimation Test" and showed which of them were for a subclass limited to PRNGs and which were for the general cryptosystem superclass [16]. Among these studies, "Maurer's Universal Statistical Test" [17], published by Maurer in 1992 and named after him, emerges as a method frequently used by cryptosystem designers. According to the author, "…the correct quality measure for a secret-key source in a cryptographic application…", but very long bit strings are required for this test to be performed. In the literature, there are many standardization studies, methods, and tools that combine randomness testing methods. The best known of these are the National Institute of Standards and Technology's (NIST) tool known as the NIST Test Suite [18], published under the code SP 800-22; China National Standardization Administration's tool standardized with GB/T 32915-2016 of SCA code [19]; PRNG evaluation standard of the German Federal Office for Information Security (Bundesamtfiir Sicherheit in der Informationstechnik, BSI) announced in 2001 AIS 20 [20]

and it's latest development as AIS 31 stands out as [21]. Randomness testing tools can also be used to analyze the reliability of a cryptosystem. The 3D-AES encryption method [22] proposed by Nakahara in 2008 aimed at large-capacity data security and efficiency with a 512-bit key/block length and 22 rounds. However, in the study published by Ariffin and Yusof in 2007, they showed that 3D-AES failed at the 0.001 significance level and was unreliable in the randomness test they performed on different datasets generated with 2 rounds for key avalanche observations [23]. On the other hand, the avalanche-effect test, in its current form, is also the subject of current studies. Madarro-Capó et al., in their study published in 2021 [24], showed that NGG [25], one of the variants of RC4, achieved the worst results in the avalanche test they performed for the RC4 stream encryption method. In 2021, Sanap and More showed that AES achieved more successful results than DES in the SAC test they conducted for AES and DES encryption methods [26].

1.2. Study Outline

Introduction section covers the preliminary information about the study and the relevant literature. In the SAAC section, definitions, theorems, and hypothesis construction for SAAC test are proposed. Numerical Results section includes the hypotheses for the most used cryptosystem output lengths. In the Experimental Test section, SAAC test application for the most used hash functions is given. Finally, section 5 concludes the study.

2. SAAC: Statistical Absolute Avalanche Criterion

Let the inputs of a C cryptosystem be I^1 and I^2, and outputs O^1 and O^2. Here, O^1 and O^2 have n-bit lengths, I^1 and I^2 differ from each other by only one bit.

Definition 1. *Hamming Distance:* It is the number of bits of two x and y vectors that are in the same position but have different values. This is denoted by $hd(x,y) = \sum_{0 \le i < n} x_i \oplus y_i$. When represented $x = (0,0,1,1,0,0,0,1)$ and $y = (0,0,0,0,0,0,1,1)$ the x and y vectors are different from each other in the 2nd, 3th and 6th positions and the hamming distance value is $hd(x,y) = 3$.

Webster and Tavares put in the literature that a change of one bit in the input of a cryptosystem causes a change of $1/2$ in the bits at the output [5], which is a result of $hd(O^1, O^2) = n/2$. However, when the expected value is $e = 0.5$, the resultant value is $x = hd(O^1, O^2)/n$, and $e < x$, it is clear that x deviates from the value of e. There are one best and two worst cases here. $x = 0.5$ is the best case, in which case 50% of the bits of the two output values are changed. $x = 0$ is the first worst case, indicating that both output values have the same bit values at the same locations. $x = 1$ is the second worst case, which means that both output values are different for all bit values at the same location, so O^2 is O^1's complement. Since all bit values consist of two values in the [0,1] range, $x = 1$ means that the outputs O^1 and O^2 are complementary to each other, which is an undesirable result. Then the absolute distance of x from the expected value e has to be observed here, for which a $ad(e,x)$ notation is given by Definition 2.

Definition 2. *Absolute Distance:* e is the expected value, x is the distance value, and $|\cdot|$ is the absolute difference value when an absolute distance function is displayed with $ad(e,x) = e - |(e - x)|$.

For the $ad(e,x)$ given by Definition 2, the e value will be $e = 0.5$ and the x value will be $x = hd(O^1, O^2)/n$. In this way, we can easily find how far the changed bit numbers ratio x of the outputs O^1 and O^2 is from the perfect ratio e. According to these definitions, SAAC is mathematically defined by Eq.1 for a C cryptosystem with an n-bit output.

$$SAAC: S(O^1, O^2) = ad(0.5, hd(O^1, O^2)/n) \quad (1)$$

From the above it is seen that, the SAAC value is in the range of $[0,0.5]$, in which case a lower bound must be set for SAAC. In the following sections, results will be given in the form of an expected value and variance and hypotheses will be formed.

2.1. Ideal Cryptosystem Output

It is vital to establish what an ideal cryptosystem output is before developing the SAAC statistic for it. An ideal cryptosystem output has realistic randomness.

Definition 3. With the integer $i \in [1, n]$, for any n-bit ideal cryptographic output $\mathcal{O}$, the random value $\mathcal{O}_i$ identically and independently (ID) follows a discrete uniformity from 0 to 1 (*the largest possible value of* $\mathcal{O}_i$). In other words, it can be represented as $\forall i \in [1, n], \exists \mathcal{O}_i \sim (ID), \mathbb{U}(0,1)$.

Definition 3 given above is an important definition so that an attacker cannot analyse the O outputs obtained from a C cryptosystem and establish a relationship between the input-output values. Any value at any position of an ideal $\mathcal{O}$ cryptosystem output is an equally similar value to an arbitrary level ℓ in [0,1], i.e. $P[\mathcal{O}(i) = \ell] = 1/2$.

2.2. SAAC Test

In this section, first of all, the expected value and variance value of SAAC are calculated for two ideal cryptosystem outputs, followed by an α-level hypothesis test based on these two values.

Theorem 1. The value at position x of the two ideal cryptosystem outputs given in Definition 3 defines a random variable

$$\mathcal{r} = \begin{cases} 0, & \mathcal{O}_x^1 = \mathcal{O}_x^2 \\ 1, & \mathcal{O}_x^1 \neq \mathcal{O}_x^2 \end{cases}$$

Then this random variable $\mathcal{r}$ follows a Bernoulli Distribution [27] with a parameter $p = 1/2$.
Proof. This can be easily seen using the independence assumption and $\mathbb{U}(0,1)$,

$$\begin{aligned} &P[\mathcal{r} = 0] = P[\mathcal{O}_x^1 = \mathcal{O}_x^2] \\ &= \textstyle\sum_{\ell=0}^{1} P[\, \mathcal{O}_x^1 = \ell \mid \mathcal{O}_x^2 = \ell \,] \times P[\mathcal{O}_x^2 = \ell] \\ &= \textstyle\sum_{\ell=0}^{1} P[\mathcal{O}_x^1 = \ell] \times P[\mathcal{O}_x^2 = \ell] \\ &= 1/2 \end{aligned}$$

As a result, $P[\mathcal{r} = 0] = 1 - P[\mathcal{r} = 1] = 1/2$. *So* $\mathcal{r} \sim \mathbb{B}(1/2)$. ■

Moreover, if the total number of bit values at position x with $hd(\mathcal{O}_x^1, \mathcal{O}_x^2) = 1$ is represented as a random variable R, then R has a Binomial Distribution [28] as in the case of Theorem 2.

Theorem 2. When $p = 1/2$, the random variable $R = \sum_{x=1}^{n} hd(\mathcal{O}_x^1, \mathcal{O}_x^2)$ defined on two ideal cryptosystem outputs follows a Binomial Distribution $\mathbb{B}(n, p)$.
Proof. Using the result of Theorem 1 and the (ID) property between bit values means that

$$P[R = i] = \binom{n}{i} \left(\frac{1}{2}\right)^i \left(\frac{1}{2}\right)^{n-i}$$

clearly shows that it is a $\mathbb{B}(n, p)$ *Binomial Distribution.* ■

According to what was obtained above, the expected and variance values of R are given with Eq.2 and Eq.3.

$$\mu_R = np = \binom{n}{1}\left(\frac{1}{2}\right) = n(1/2) = \frac{n}{2} \tag{2}$$

$$\sigma_R^2 = np(1-p) = \binom{n}{1}\left(\frac{1}{2}\right)\left(\frac{1}{2}\right) = \frac{n}{4} \tag{3}$$

Here, since $S(\mathcal{O}^1, \mathcal{O}^2) = ad(0.5, hd(\mathcal{O}^1, \mathcal{O}^2)/n\ ) = R/n$, it is clear that the random variable R is the scaled version of the SAAC score. Therefore, if the two n-bit outputs $\mathcal{O}^1$ and $\mathcal{O}^2$ are an ideal cryptosystem output then $S(\mathcal{O}^1, \mathcal{O}^2) \sim \mathbb{B}(n, p)$. From here, the definition given by Eq.4 and the expected value and variance given by Eq.5 and Eq.6 are obtained.

$$P\left[S(\mathcal{O}^1, \mathcal{O}^2) = \frac{i}{n}\right] = \binom{n}{i}\left(\frac{1}{2}\right)^i\left(\frac{1}{2}\right)^{n-i} \tag{4}$$

$$\mu_s = \frac{\mu_R}{n} = \frac{n/2}{n} = \frac{1}{2} \tag{5}$$

$$\sigma_S^2 = \frac{\sigma_R^2}{n^2} = \frac{n/4}{n^2} = \frac{n}{4n^2} = \frac{1}{4n} \tag{6}$$

When the definitions given above are used together, the statistical test SAAC given below can be used for the outputs of cryptosystems.

Definition 4. *SAAC Test:* When O^1 and O^2 are two n-bit cryptosystem outputs, hypotheses with α-level significance level for $S(O^1, O^2)$:

$$\begin{cases} \mathcal{H}_0 : S(O^1, O^2) \geq S_\alpha^* \\ \mathcal{H}_1 : S(O^1, O^2) < S_\alpha^* \end{cases}$$

Here, if the critical lower limit value of the SAAC test is $S(O^1, O^2) < S_\alpha^*$, $\mathcal{H}_0$ is rejected, otherwise if $S(O^1, O^2) \geq S_\alpha^*$, $\mathcal{H}_0$ is accepted. The critical value S_α^* is defined by Eq.7 when $\Phi^{-1}(\cdot)$ is the Cumulative Distribution Function (CDF) [29] inverse of the standard normal distribution $\mathbb{N}(0,1)$.

$$S_\alpha^* = \mu_s - \Phi^{-1}(\alpha)\sigma_S = (1/2) - \left(\Phi^{-1}(\alpha)\sqrt{1/4n}\right) \tag{7}$$

3. Numerical Results

In the previous sections, the Probability Density Function (PDF) statistic for expected value, variance and SAAC is shown by Eq.5-7. In this section, SAAC tests were created for $n = \{64,128,160,192,224,256,320,384,512\}$, which are the most used cryptosystem output lengths in the literature. For this purpose, some percentiles for the standard normal distribution, which are frequently used in statistical applications, are given in Table 1. For example, with a significance level of 0.05, it would be $(\alpha = 0.05;\ x = 1.6449)$ or $\Phi^{-1}(0.05) = 1.6449$ for the one-sided hypothesis, and accordingly, if X is $\mathbb{N}(0,1)$, we can easily find that X is exceeds 1.6449 about 5% of the time.

Table 1 Some Percentiles for Standard Normal Distribution

α	0.1	0.05	0.025	0.01	0.005	0.0025	0.001	0.0005
x	1.2816	1.6449	1.9600	2.3263	2.5758	2.8070	3.0902	3.2905

S_α^* critical values of SAAC test are given for $x = \alpha$ values and $n = \{64,128,160,192,224,256,320,384,512\}$ given in Table 2. In Table 2, all values except n are multiplied by 100 to better reflect the decimal places of the numerical results.

Table 2 Numerical Results for SAAC

n	μ_s	σ_S	$S_{0.1}$	$S_{0.05}$	$S_{0.025}$	$S_{0.01}$	$S_{0.005}$	$S_{0.0025}$	$S_{0.001}$	$S_{0.0005}$
64	50.000	6.2500	41.9900	39.7194	37.7500	35.4606	33.9013	32.4563	30.6863	29.4344
128	50.000	4.4194	44.3361	42.7305	41.3379	39.7191	38.6165	37.5947	36.3431	35.4579
160	50.000	3.9528	44.9340	43.4980	42.2524	40.8045	39.8183	38.9044	37.7849	36.9932
192	50.000	3.6084	45.3754	44.0645	42.9275	41.6057	40.7054	39.8711	38.8492	38.1264
224	50.000	3.3408	45.7185	44.5048	43.4521	42.2284	41.3949	40.6225	39.6764	39.0072
256	50.000	3.1250	45.9950	44.8597	43.8750	42.7303	41.9506	41.2281	40.3431	39.7172
320	50.000	2.7951	46.4178	45.4024	44.5216	43.4978	42.8004	42.1542	41.3626	40.8028
384	50.000	2.5516	46.7299	45.8030	44.9990	44.0643	43.4277	42.8378	42.1152	41.6041
512	50.000	2.2097	47.1680	46.3653	45.6690	44.8596	44.3082	43.7973	43.1716	42.7290

For any $S(O^1, O^2)$ test with the values given in Table 2, if the obtained value is less than S_α^*, our null hypothesis will be rejected and (O^1, O^2) cryptosystem outputs fail the SAAC test. It should be noted that the result obtained here is probabilistic, but our probability of fail is only α, which is a very small quantity.

4. Experimental Test

In this section, a sample application of the SAAC test is performed. For the test, Blake2s, SHA2, SHA3 and RIPEMD hash functions are used. These functions have 256-bit output lengths ($n = 256$), They are intended to have a random output feature and are also used in random number generators. Each function has been tested with $N = 10000$ trials. A randomly selected I^1 message was generated in each trial, and the I^2 message was generated by randomly changing one bit of the I^1 message. The outputs of $H(I^1) = O^1$ and $H(I^2) = O^2$ obtained from hash functions were put into both SAAC and conventional Avalanche-Effect (AF) tests. Obtained from tests; SAAC mean value $\overline{\mathrm{X_{SAAC}}} = \sum_{i=1}^{10000} \mathrm{S}(\mathrm{O_i^1},\mathrm{O_i^2})/10000$ and variance value $\widehat{\sigma_{\mathrm{SAAC}}^2} = \sum_{i=1}^{10000} \left(\mathrm{S}(\mathrm{O_i^1},\mathrm{O_i^2}) - \overline{\mathrm{X_{SAAC}}}\right)^2/9999$; Avalanche-Effect mean value $\overline{\mathrm{X_{AF}}} = \left(\sum_{i=1}^{10000} \mathrm{hd}(\mathrm{O_i^1},\mathrm{O_i^2})/\mathrm{n}\right)/10000$ and variance value $\widehat{\sigma_{\mathrm{AF}}^2} = \sum_{i=1}^{10000} \left(\left(\mathrm{hd}(\mathrm{O_i^1},\mathrm{O_i^2})/\mathrm{n}\right) - \overline{\mathrm{X_{AF}}}\right)^2/9999$. In order to better reflect the decimal places of the test results, all values except n are multiplied by 100 and given in Table 3.

The results given in Table 3 showed us that all cryptosystems were successful in the SAAC test. It is also seen with the Max value that 50% absolute value is successfully applied thanks to the $ad(e, x)$ function given by Definition 1 and Eqn.1. On the other hand, when Min values are examined, it has been shown that all cryptosystems tested failed the SAAC test at least in one of the tests repeated $N = 10^4$ times. When the Mod value is examined, it is seen that the most repeated value of all cryptosystems tested is successful for all α-level significance level tests.

Table 3 Experimental Results for SAAC and Avalanche-Effect Tests

	SAAC Test				Avalanche-Effect Test			
Func.	**Blake2s**	**SHA2**	**SHA3**	**RIPEMD**	**Blake2s**	**SHA2**	**SHA3**	**RIPEMD**
n	256	256	256	256	256	256	256	256
Min	37.5000	37.8906	37.8906	37.8906	38.6719	37.8906	38.2813	37.8906
Max	50.0000	50.0000	50.0000	50.0000	62.5000	61.3281	62.1094	62.1094
Mod	49.2188	49.6094	49.2188	49.2188	48.8281	50.3906	49.2188	50.7813
$\overline{X_*}$	47.4554	47.5084	47.4949	47.5091	50.0067	49.9909	49.9635	50.0074
σ_*	1.9007	1.8913	1.9186	1.8920	3.1762	3.1282	3.1553	3.1280

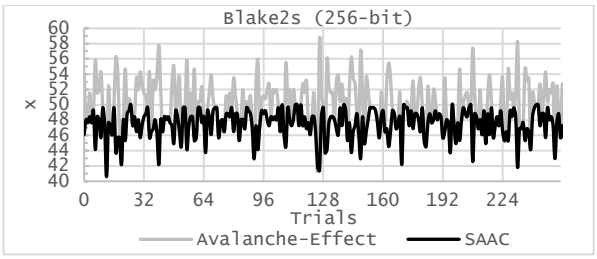

Figure 1. Blake2s

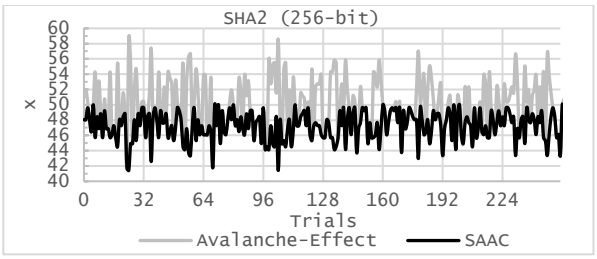

Figure 2. SHA2

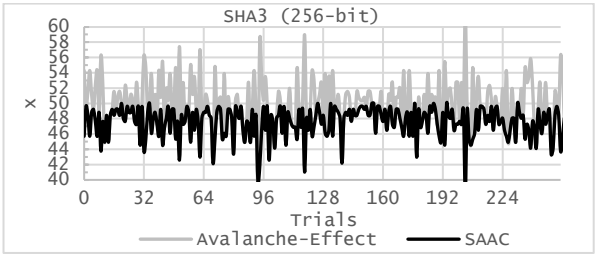

Figure 3. SHA3

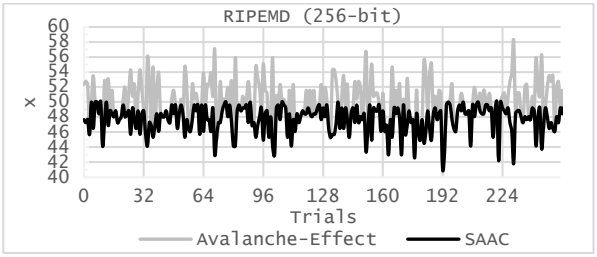

Figure 4. RIPEMD

The graphs of SAAC and Avalanche-Effect test results of $N = 256$ trial is given with Fig.1 for Blake2s, Fig.2 for SHA2, Fig.3 for SHA3, and Fig.4 for RIPEMD. When these graphs are examined, it is seen that the traditional avalanche-effect test usually gives higher values, but the SAAC test gives lower values. This clearly shows us that the traditional avalanche-effect test does not control the deviation from the $e = 0.5$ perfect/expected value, and the SAAC test controls it with $ad(e, x)$. On the other hand, it is seen that the Min, Max, Mod, $\overline{X_*}$ and σ_*^2 values in the Avalanche-Effect Test and SAAC Test sections given in Table 3 for the same (O_i^1, O_i^2) outputs are different. When the $\overline{X_*}$ values are compared, the Avalanche-Effect test giving higher values than the SAAC test shows another simple result. The SAAC test is more demanding than the Avalanche-Effect test.

Table 4 SAAC Test – Pass/Fail Results in Trials

	$S_{0.1}$		$S_{0.05}$		$S_{0.025}$		$S_{0.01}$		$S_{0.005}$		$S_{0.0025}$		$S_{0.001}$		$S_{0.0005}$	
	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail
Blake2s	8023	1977	9054	946	9438	562	9769	231	9054	99	9961	39	9985	15	9994	6
SHA2	8124	1876	9053	947	9455	545	9795	205	9053	118	9946	54	9983	17	9991	9
SHA3	8101	1899	9049	951	9420	580	9751	249	9049	126	9941	59	9973	27	9985	15
RIPEMD	8110	1890	9093	907	9458	542	9795	205	9093	99	9953	47	9971	29	9988	12

The test results performed above and given in Table 3 show that each hash function tested $with\ N = 10000$ trials failed at least once in the SAAC test, with given Min values. With Table 4, the passed and failed numbers in $N = 10000$ trials of hash functions are given for different α-level significance levels given by the Table 2.

The examined hash functions do not always pass the SAAC test, as seen in Table 4. Here it is possible to examine in which position the bit value causes this result for the internal states of the functions. The SAAC test can also be used to test the internal functions of the cryptosystem as a whole, and the iteration of each round. However, a study in this direction is outside the scope and scope of this study. On the other hand, it is clear here that the SAAC test can be used for future cryptanalysis and cryptosystem studies.

5. Conclusion

In this paper, the Statistical Absolute Avalanche Criterion (SAAC) test was proposed in this work. Instead of the conventional Strict Avalanche Criterion (SAC) or other well-known confusion/diffusion assessments, the absolute distance measure, statistical technique, and theorems are investigated for SAAC. According to numerous research on cryptosystems published in the literature, strict avalanche criteria or other well-known confusion/diffusion assessments reveal that a one-bit change in any input value changes at least half of the bits in the output value for security. These studies did not focus on how close an n-bit output is to a change in the ratio of $1/2$, its statistical significance and acceptability. On the other hand, in these studies, it is not observed that the change of bits at a rate of $> 1/2$ is not desirable. In this study, the change of half of the total bits was determined as the expected result and the rate of change was taken as 50% absolute value. An ideal cryptosystem output model was developed for theorems, and it's expected/variance values were included.

Variance lower bound values with multiple α-level significance levels of the SAAC test are given for most used cryptosystems output lengths of $n = \{64,128,160,192,224,256,320,384,512\}$. For the experimental tests, Blake2, SHA2, SHA3 and RIPEMD hash functions having 256-bit outputs were used with 10000 trials, and results for SAAC and Avalanche-Effect tests were compared. The results demonstrated that maximum of 50% absolute value was successfully applied. On the other hand, experimental test results show that the traditional Avalance-Effect test usually produces higher values, and the SAAC test produces lower values. It is more difficult to pass the SAAC test than the Avalanche-Effect test. On the other hand, the SAAC testing of numerous studies in the literature that are claimed to be safe based on the Avalanche-Effect test alone, emerges as an important issue for future studies. As in the experimental results given in this study, researchers can observe the Pass/Fail numbers of the tested cryptosystem in the trials and detect the relationships of the input values that cause the Fail result and observe the weaknesses of the cryptosystem or the internal function of the cryptosystem.

SAAC test is an easily applicable and statistically proven tool that can be used in the analysis of both the output values and the security performance of each round or sub-functions in cryptosystem studies.

References

[1]. Shannon , C.E. "A mathematical theory of communication.," Bell System Technical Journal, no. 27, pp. 379–423, 623–656, 1948.
[2]. Shannon , C.E. "Communication theory of secrecy," Bell System Technical Journal, no. 28, pp. 656-715, 1949.

[3]. Menezes , A.J., van Oorschot, P.C., and Vanstone, S.A., Handbook of Applied Cryptography., 1996.
[4]. Feistel, H. "Cryptography and Computer Privacy," Scientific American, vol. 5, no. 228, 1973.
[5]. Webster, A. F. and Tavares, E. "On the design of S-boxes," Advances in Cryptology - Crypto '85, no. 218, pp. 523–534, 1985.
[6]. Ahmad, M., Khurana, S., Singh, S., and AlSharari, H. "A Simple Secure Hash Function Scheme Using Multiple Chaotic Maps," 3DR EXPRESS, vol. 8, no. 13, pp. 13-18, 2017.
[7]. Li, Y., Ge, G., and Xia, D., "Chaotic hash function based on the dynamic S-Box with variable parameters," Nonlinear Dyn., vol. 84, pp. 2387-2402, 2016.
[8]. Liu, H., Kadir, A., Sun, X., and Li, Y., "Improving the efficiency of quantum hash function by dense coding of coin operators in discrete-time quantum walk," Sci. China-Phys. Mech. Astron., vol. 030312, no. 61, 2018.
[9]. Yang, Y. et al., "Simple hash function using discrete-time quantum walks," Quantum Inf Process, vol. 189, no. 17, 2018. [Online]. https://doi.org/10.1007/s11128-018-1954-2
[10]. Cao, Z., Chen, F., Chen, B., and Zhang, X., "Research on the Balanced Boolean Functions Satisfying Strict Avalanche Criterion," in 2015 International Conference on Computational Science and Computational Intelligence, 2015.
[11]. Alamsyah, "A Novel Construction of Perfect Strict Avalanche Criterion S-box using Simple Irreducible Polynomials," Sci. J. Informatics, vol. 7, no. 1, pp. 10-22, 2020.
[12]. Gupta, C.K. and Sarkar, P., "Construction of Perfect Nonlinear and Maximally Nonlinear Multiple-Output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria," IEEE transactions on information theory, vol. 50, no. 11, 2004.
[13]. Li, L., Liu, J., Guo, Y., and Liu, B., "A new S-box construction method meeting strict avalanche criterion," Journal of Information Security and Applications, no. 66, pp. 2214-2126, 2022.
[14]. Wu, Y., Noonan, J.P., and Agaian, S., "NPCR an UACI Randomness Tests for Image Encryption," Journal of Selected Areas in Telecommunications (JSAT), April 2011.
[15]. Castro, J.C.H., Sierra, J.M., and Seznec, A., "The strict avalanche criterion randomness test," Inform. Process. Lett., no. 68, pp. 1-7, 2005.
[16]. Mendi, Z., Xiaojuan, Z., Zhu, Y. and Miao, S. "Overview of Randomness Test on Cryptographic Algorithms." Journal of Physics: Conference Series 1861, no. 012009, 2021.
[17]. Maurer, M.U. "A Universal Statistical Test for Random Bit Generators." Journal of Cryptography, vol. 5, no. 2, pp. 89-105, 1992.
[18]. Rukhin, A., et al. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications." U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, 2010.
[19]. Dawei, L., Feng, D., and Chen, H. Information security technology binary sequence randomness detection methods. China National Standardization Administration, China Standards Press, 2016.
[20]. Schindler, W. "AIS 20:Functionality classes and evaluation methodology for deterministic random number generators, Version 2.0.", Bundesamt ftir Sicherheit in der Informationstechnik (BSI), pp. 5-11, 1999.
[21]. Killmann, W., and Schindler, W. "AIS 31:A proposal for:Functionality classes and evaluation methodology for true (physical) random number generators, Version 3.1.", Sicherheit in der Informationstechnik (BSI), 2001.
[22]. Nakahara, J. "3D: A three-dimensional block cipher.", in International Conference on Cryptology and Network Security, pp. 252-267, Berlin: Springer, 2008.
[23]. Ariffin, S., and Yusof, N.A.M.. "Randomness analysis on 3D-AES block cipher.", 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 331-335, IEEE, 2017.
[24]. Madarro-Capó, E.J., Legón-Pérez, C.M., Rojas, O. and Sosa-Gómez, G.. "Measuring Avalanche Properties on RC4 Stream Cipher Variants.", Appl. Sci. vol. 11, no. 9646, 2021.
[25]. Paul, G., and Maitra, S. RC4 Stream Cipher and Its Variants. Boca Raton, FL: CRC Press, 2011.

[26]. Sanap, S. D., and More, V. “Performance Analysis of Encryption Techniques Based on Avalanche effect and Strict Avalanche Criterion.”, 2021 3rd International Conference on Signal Processing and Communication (ICPSC). Coimbatore, 2021.
[27]. Weisstein, E., “Bernoulli Distribution” from MathWorld-A Wolfram Web Source. http://mathworld.wolfram.com/BernoulliDistribution.html
[28]. Weisstein, E., “Binomial Distribution” from MathWorld-A Wolfram Web Source. http://mathworld.wolfram.com/BinomialDistribution.html
[29]. Weisstein, E., “Normal Distribution” from MathWorld-A Wolfram Web Source. http://mathworld.wolfram.com/NormalDistribution.html