GLITCH: A Discrete Gaussian Testing Suite For Lattice-Based Cryptography

James Howe and Máire O'Neill,

Centre for Secure Information Technologies (CSIT), Queen's University Belfast, UK.

@CSIT_QUB / @SAFEcrypto jhowe02@qub.ac.uk

Aims and Objectives

This research aims to provide:

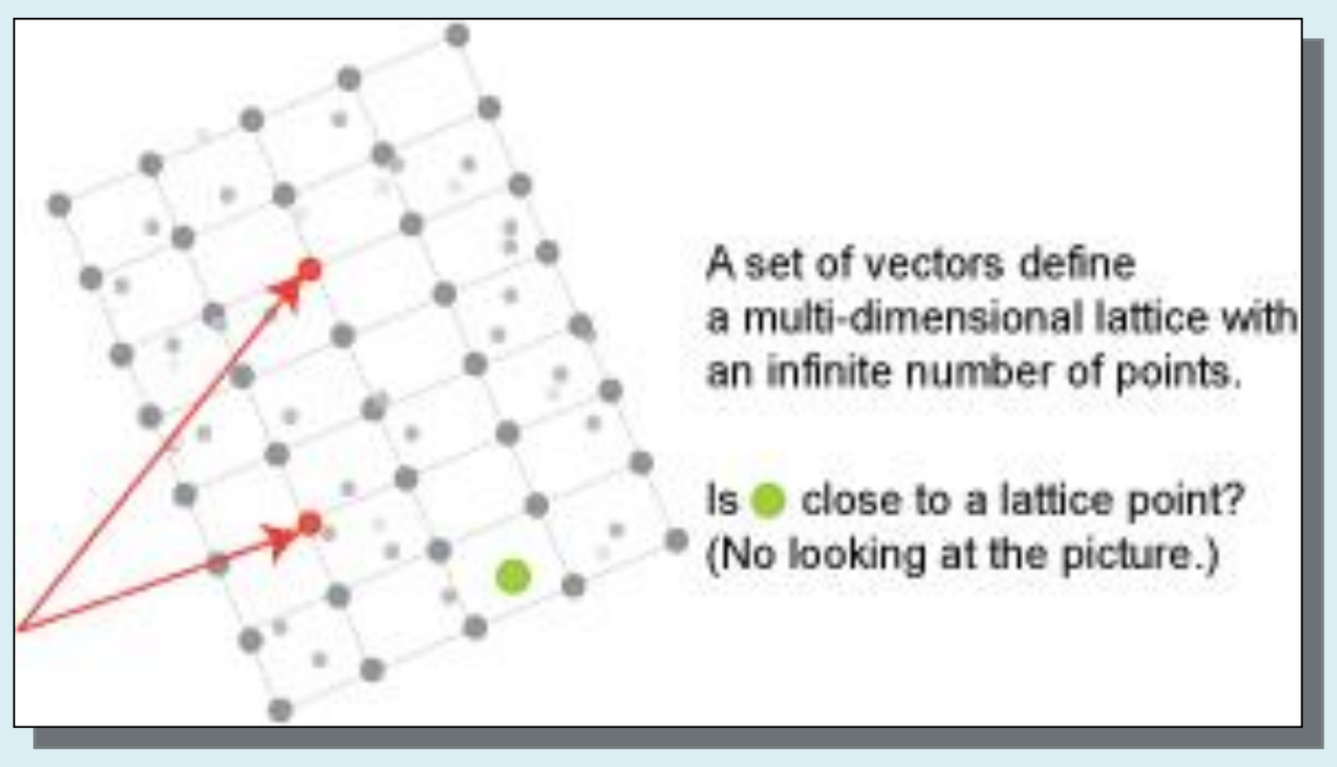
- A generic software-based statistical testing platform for a discrete Gaussian random number generator, a component ubiquitously used with lattice-based cryptography.
- Verification that hardware or software based discrete Gaussian samplers are actually outputting correctly, which could otherwise lead to security issues within lattice-based cryptography.
- Verification that lattice-based cryptoschemes, like BLISS, LPR, or GPV, whose outputs are discrete Gaussian, are correctly distributed.

Lattice-Based Cryptography

Lattice-based cryptography is post-quantum secure, meaning the algorithms will remain secure even after practical quantum computing is a reality.

Advantages of lattice-based crypto:

- Underlying operations can be implemented efficiently.
- Most promising as allows for other constructions/applications beyond encryption/signatures, e.g. IBE, ABE, homomorphic encryption etc.


A set of vectors define a multi-dimensional lattice with an infinite number of points.
Is ● close to a lattice point?
(No looking at the picture.)

The GLITCH Test Suite

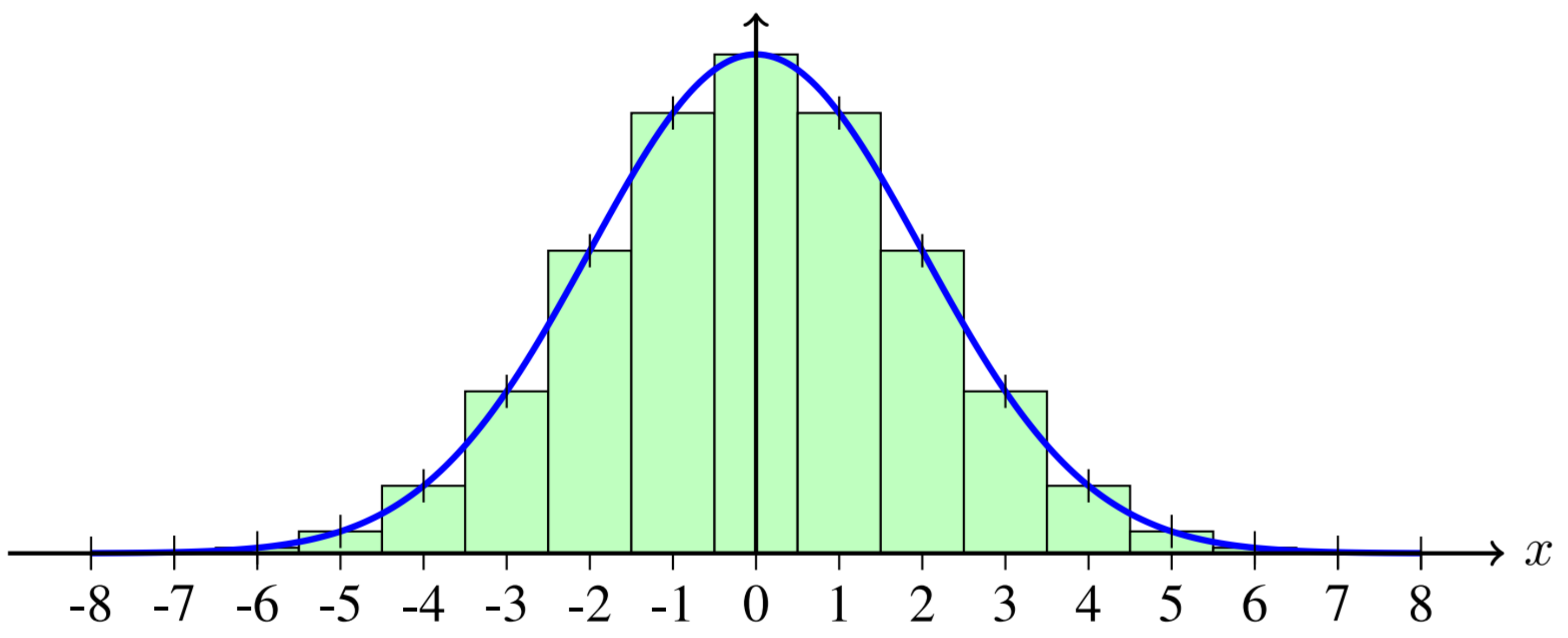
GLITCH takes as input histogram data, thus being able to test any discrete Gaussian sampling design, either in hardware or software.

This paper surveys statistical tests that could be used for this purpose, proposing 11 tests appropriate for use within lattice-based cryptography.

GLITCH includes the testing of;

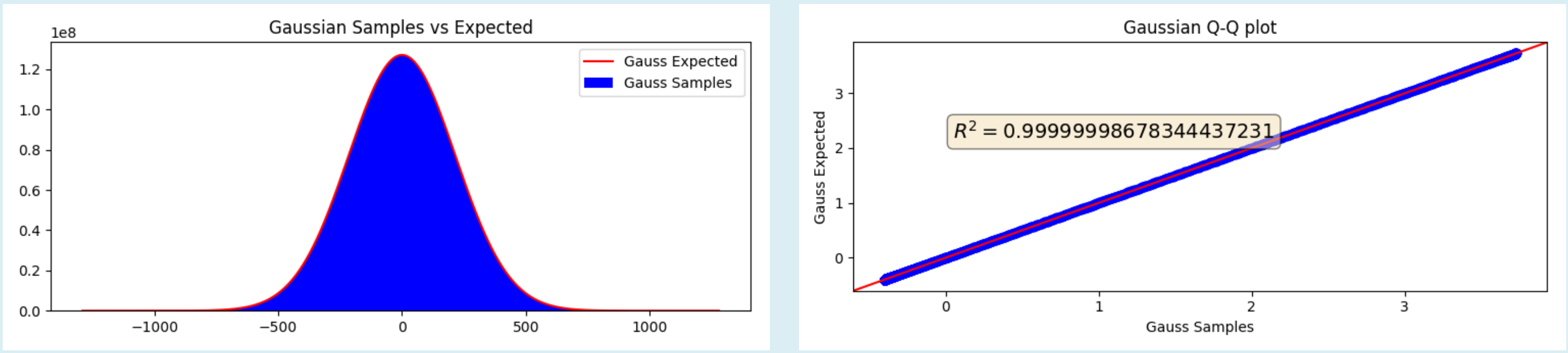
- The mean, standard deviation, tail-cut, and precision parameters.
- The shape of the sample distribution via skewness and kurtosis.
- The normality of the sample distribution via normality tests.
- Graphical representations of the sample data and a QQ-plot.

$$\Pr(X = x) = \rho_\sigma(x)$$

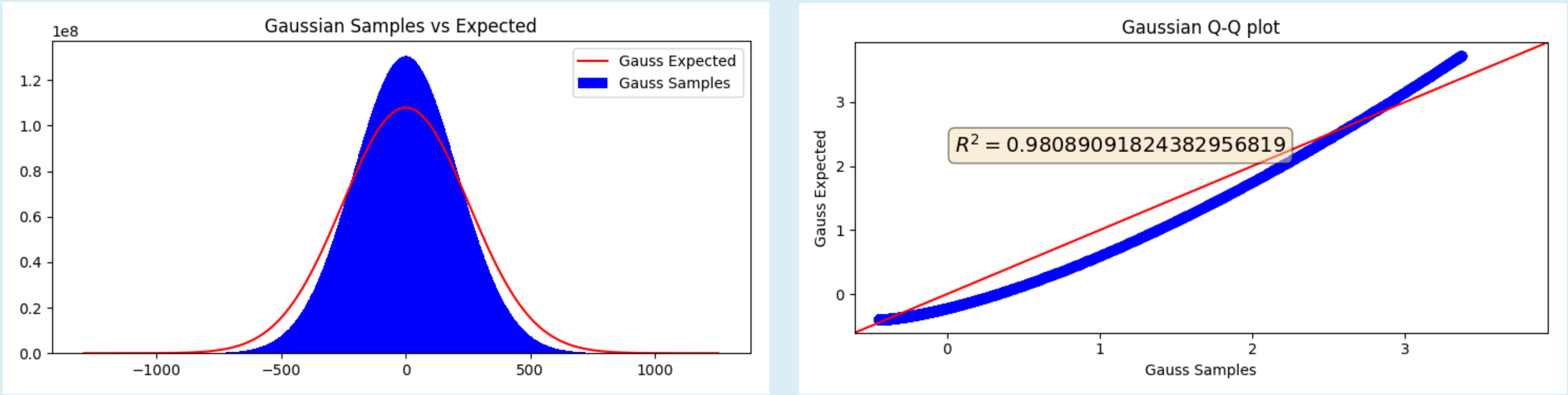


The Discrete Gaussian Distribution

Example results of a correctly operating discrete Gaussian sampler which passes all test:



Example results of an incorrectly operating discrete Gaussian sampler which fails tests:



Conclusions to this research;

- The tests chosen are powerful and operate well on large sample sizes.
- Failure in any of these tests indicates a deviation from the target distribution, which is therefore evidence of an incorrectly performing discrete Gaussian sampler.
- The software for GLITCH is made available online, which also provides sample data for discrete Gaussian samplers; which are able to be tested upon (see: https://github.com/jameshoweee/glitch).

The table below shows the detailed statistical formulae of the proposed GLITCH test suite. Failure in any of these tests indicates a deviation from the target distribution, which is therefore evidence of an incorrectly performing discrete Gaussian sampler.

Test No.	Test Description	Test Formula
Test 1	Sample Mean ($\bar{x}$)	$\bar{x} = (\sum_{i=1}^{N} x_i h_i)/N$
	Standard Error of $\bar{x}$	$\text{SE}_{\bar{x}} = s/\sqrt{N}$
	Confidence Interval of $\bar{x}$	$\bar{x} \pm t_{\alpha/2}\text{SE}_{\bar{x}}$
	Accept Null Hypothesis?	Accept if $\lvert\mu\rvert \in \{0, \dots, \bar{x} + t_{\alpha/2}\text{SE}_{\bar{x}}\}$
Test 2	Sample Standard Deviation (s)	$s = \sqrt{(\sum_{i=1}^{N}(x_i - \bar{\mu}_1)^2 h_i)/N}$
	Standard Error of s	$\text{SE}_s = s/\sqrt{2(N-1)}$
	Confidence Interval of s	$s \pm t_{\alpha/2}\text{SE}_s$
	Accept Null Hypothesis?	Accept if $\lvert\sigma\rvert \in \{0, \dots, s + t_{\alpha/2}\text{SE}_s\}$
Test 3	Sample Tail-Cut ($\bar{\tau}$)	$\bar{\tau} = \max(x_i)/s$
Test 4	Sample Skewness (ω)	$\omega = m_3\sqrt{N(N-1)}/(N-2)$
	Standard Error of ω	$\text{SE}_\omega = \sqrt{\frac{6N(N-1)}{(N-2)(N+1)(N+3)}}$
Test 5	Sample Excess Kurtosis (κ)	$\kappa = (m_4/s^4) - 3$
	Standard Error of κ	$\text{SE}_\kappa = 2\text{SE}_\omega\sqrt{\frac{N^2-1}{(N-3)(N+5)}}$
Test 6	Sample Hyperskewness	$\omega_* = m_5/s^5$
Test 7	Sample Excess Hyperkurtosis	$\kappa_* = m_6/s^6$
Test 8	Jarque-Bera Test For Normality	$\text{JB} = (N/6)(\omega^2 + ((\kappa-3)^2)/4)$
	Accept Null Hypothesis?	Accept if $\text{JB} < \chi^2_\alpha$
Test 9	D'Agostino-Pearson Omnibus Test	$\text{K}^2 = Z_1(\omega)^2 + Z_2(\kappa)^2$
	Accept Null Hypothesis?	Accept if $\text{K}^2 < \chi^2_\alpha$
Test 10	Histogram Plot	-
Test 11	Coefficient of Determination	$R^2 = 1 - (\sum_{i=1} e_i^2 / \sum_{i=1}(y_i - \hat{y})^2)$

www.safecrypto.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644729