# BOOMERANG CONNECTIVITY TABLE

A boomerang attack is a cryptanalysis framework that regards a block cipher E as the composition of two sub-ciphers $E_1 \circ E_0$ and builds a particular characteristic for E with probability $p^2 q^2$ by combining differential characteristics for $E_0$ and $E_1$ with probability *p* and *q*, respectively. The Differential Distribution Table (DDT) of an S-box shows how often input difference Δx leads to output difference Δy. It is used in differential cryptanalysis to find high-probability differential characteristics. The Boomerang Connectivity Table (BCT) for an S-box records how often a specific input difference $\Delta_{in}$ combined with a specific output difference $\Delta_{out}$ (delta out) satisfies a *boomerang relation i.e., For an S-box S, its inverse $S^{-1}$, and input difference $\Delta_{in}$, output difference $\Delta_{out}$, the BCT is defined as:*

$$\mathrm{BCT}[\Delta_{\mathrm{in}}, \Delta_{\mathrm{out}}] = |\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \Delta_{\mathrm{out}}) \oplus S^{-1}(S(x \oplus \Delta_{\mathrm{in}}) \oplus \Delta_{\mathrm{out}}) = \Delta_{\mathrm{in}}\}|$$

BCT quantifies how often a differential input-output pair cycles back to the original input difference after applying both the S-box and its inverse. It combines both forward and backward differential behavior, making it more useful for analyzing boomerang distinguishers.

This Project presents the generation of DDT and BCT for AES S-box and TWINE S-box. It gives the frequency count of values in the Differential Distribution Table (DDT) and the Boomerang Connectivity Table (BCT) of both the S-boxes.

aes_sbox.py: contains AES S-box
twine_sbox.py: constains TWINE S-box
bct.py: This program takes the input ffrom the user whether the AES-Sbox or TWINE s-box to be considered for the DDT and BCT geenration. Once the user enters the AES/TWINe, it geernates the DDT and BCT. It counts the frequency of the values in DDT and BCT.

For AES DDT and BCT, the output is stored in aes_ddt.csv and aes_bct.csv.
For TWINE DDT and BCT, the output is stored in twine_ddt.csvand twine_bct.csv respectively.

Input: AES or TWINE
Output: DDT aand BCT of the S-box along with the comparison of frequency of values in DDT and BCT

Boomerang Attack can be performed using the BCT to the Deoxy-BC and SKINNY Cipher (ref: https://eprint.iacr.org/2018/161.pdf)