Cryptanalysis is the process of discovering plaintext from ciphertext without knowing any information about the system or the key.

Neural network approach is used for cryptanalysis.

Cryptanalysis is done on two and one rounds of Simon cipher.

The neural network predicts the key used to encrypt a plaintext, given plaintext-ciphertext pairs.

Block size: 32 bits
Key size: 64 bits

Python’s neural network API, Keras, was used to design the neural network.
Google’s TensorFlow was used in the backend.
The GPU version of Keras was used to handle the large volume of dataset for training.

Accuracy is calculated by counting the number of predicted key bits that match with the actual key bits.

Accuracy of the model with two rounds of Simon cipher: 50% to 60%
one round of Simon cipher: 63% to 74%

Huge dataset took a lot of time for training.
Training time increased with an increase in number of epochs.
Took a lot of time to get a right configuration of the neural network.

A design based on fuzzy classifier used along with neural networks yielding probabilities for 0 and 1.
Brute-force search for key using fuzzy classifier.

F. Chollet et al., “Keras,” https://keras.io, 2015.