ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

Reducing the Cost of Machine Learning Attacks for Block ciphers

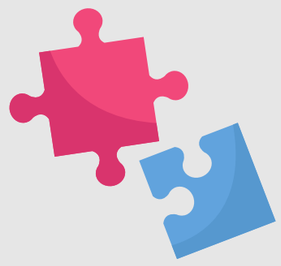
Amirhossein Ebrahimi

Supervised by: Dr. Paolo Plamieri and Prof. Utz Roeadig

PROBLEM STATEMENT

The Sustainable Development Goals (SDGs) cannot be met unless there is a private and secure environment for data transfer. The block ciphers, which are used for encryption, are the most important tool in providing this environment. As a result, assessing their security is critical. AI and machine learning can greatly simplify this evaluation. So, this work is trying to figure out how to make more efficient machines while also lowering the cost of training.

CHALLENGES



- The random environment of block ciphers complicates the training phase.
- The number of features for training will increase for block ciphers with larger inputs.

METHOD

- Choosing the Speck32/64 as our case study due to its lightweight input bandwidth (32 bits)
- We train a Dense layer machine for for differential analysis of Speck
- Then we pick 100 random sets, and inside each set, we randomly choose 16 out of input 32 bits.
- With the random sets we have, we train 100 distinct lightweight machines.
- Based on the *Algorithm*, a score is assigned to each machine.
- we choose the bits with highest score to train a more efficient machine

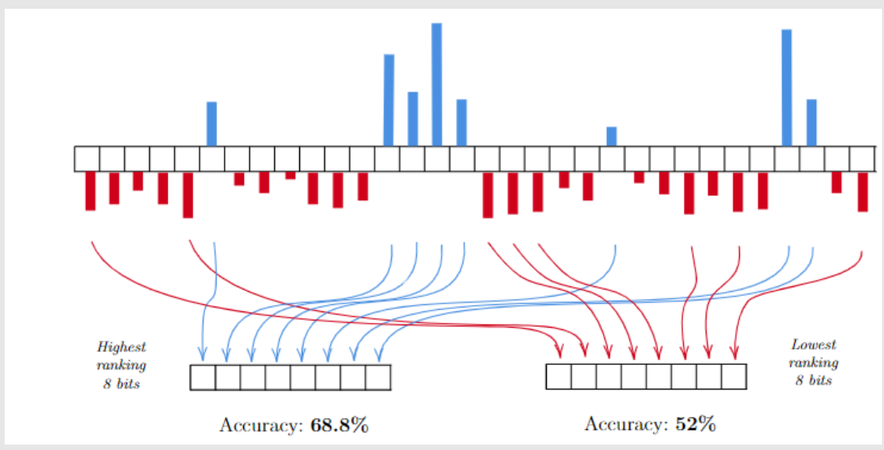
Algorithm : Scores of effectiveness

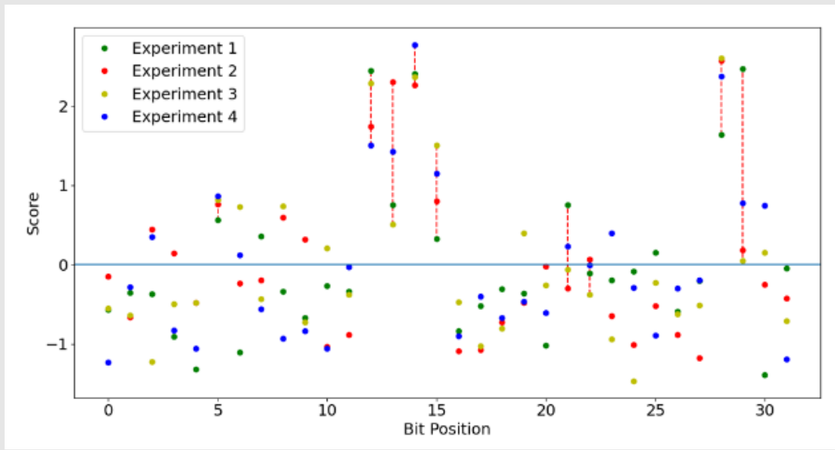
Input: Sequence set of combinations: $\mathcal{C}_B^{16} = [\mathcal{C}_0, \ldots, \mathcal{C}_{99}]$
Output: Sequence set of scores: $S = [s_0, \ldots, s_{31}]$
Training Data: differences of ciphertext pairs of 6-round SPECK32/64 : $\delta = [\delta_0, \ldots, \delta_{31}]$

Initialize Sequence set A with size 100
Initialize $M_{32\times100}$ Matrix
Initialize Sequence set S with size 32
for $\mathcal{C}_i \in \mathcal{C}_B^{16}$ **do**
    /* Training PD-ML distinguishers */
    $D \longleftarrow TrainMachine(\mathrm{C}_i)$
    $A[i] = \mathrm{AccuracyTest}(D)$
    /* Making M matrix */
    for δ_j *in* δ **do**
        if $\delta_j \in \mathcal{C}_i$ **then**
            $M[j][i] = 1$
        else
            $M[j][i] = 0$
    /* Computing the score */
for $0 <= i <= 31$ **do**
    $$S[i] = \frac{\sum_{j=0}^{99} m_{ij} * a_j}{\sum_{j=0}^{99} m_{ij}}$$

RESULTS

By selecting the best 8-bits of the Speck32/64 cipher, we were able to train a machine with an accuracy of 68.8%, as opposed to the worst 8-bits, which had an accuracy of 52%.





Host Institution

UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

Maynooth University National University of Ireland Maynooth

TU DUBLIN Ollscoil Teicneolaíochta Bhaile Átha Cliath Technological University Dublin

Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin