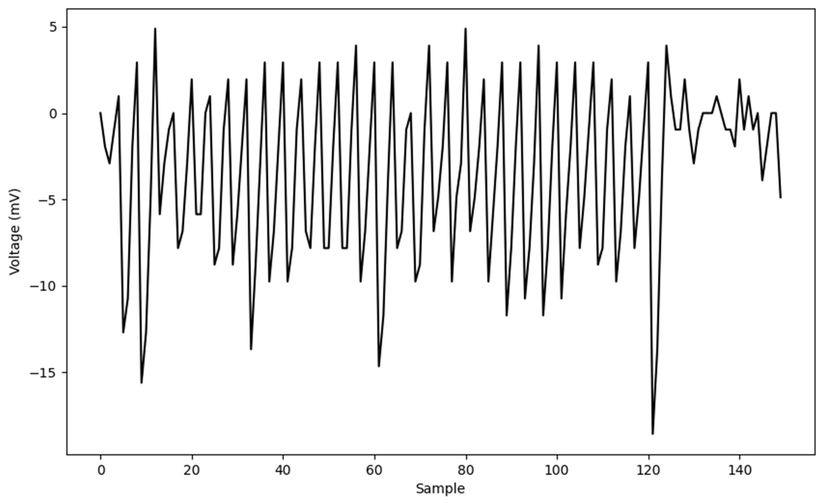
Efficient Deep Learning-based Side-Channel Attack on DIZY Stream Cipher

George Attia[+*], Shekoufeh Neisarian[+*], Martin Schmid[*+], Elif Bilge Kavun[+~]
+ {george.attia, shekoufeh.neisarian, martin.schmid, elif.kavun}@barkhauseninstitut.org
∗ {attia01, neisar01, schmi516}@ads.uni-passau.de
~ elif_bilge.kavun@tu-dresden.de

Introduction & Motivation

- Side-Channel Attacks **(SCAs)** exploit physical leakages, like power consumption during cipher execution
- **DL-based** SCAs outperform traditional methods like CPA by modeling complex leakage patterns
- Previous research predominantly targets block ciphers such as AES
- **Lightweight stream ciphers** remain understudied

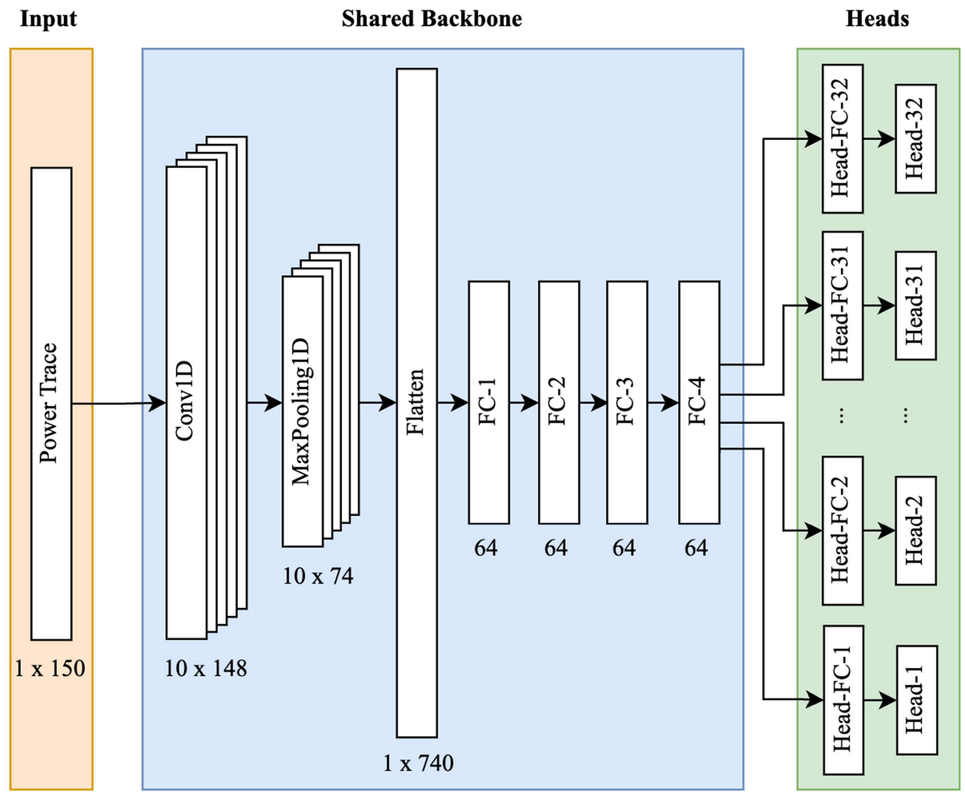


Sample Power Trace from DIZY Hardware

- We evaluate the feasibility of DL-based SCAs on "*lightweight*" **DIZY** stream cipher [1]
- Using power traces captured from a hardware implementation [2], we assess DIZY's vulnerability to SCA, focusing on its 128-bit variant
- This study investigates the security of lightweight stream ciphers against advanced SCAs

Implementation

- SCA is formulated as an ML classification problem
- Given a set of power traces, a Neural Network (NN) predicts a specific internal state of DIZY
- Predicted internal states can then be used to infer information about the secret key used
- Given an ML classifier with an accuracy slightly better than a random classifier, guessing entropy of the secret key gradually decreases with an increasing number of traces



Visual Representation of the Multi-Head CNN Model

- Most studies focus on specific internal state bytes
- We implement a CNN targeting whole 160-bit internal state output from the S-box used in the first round through a multi-head model that predicts each 5-bit S-box output group of the internal state
- Our architecture has benefits over separate networks training
  - Efficient model training
  - Better generalization of the leakage patterns using a unified learned internal representation in the DL model

Results & Evaluation

- We trained 4 CNN models to test the success of our SCA
- Proposed multi-head models were tested against traditional separate networks models with following results:
  - Fewer power traces are required for the multi-head model to converge towards the correct key bits (for both fixed-key and variable-key datasets)
  - More key bit groups are converging towards the correct key bits with the multi-head model
  - The multi-head model is parameter-efficient compared to the separate networks model

Overview of Our Side-Channel Attack Results

Dataset	Model Architecture	Training Time (s)	# of Parameters	Converging Grps.	# of Power Traces
Fixed-key	Separate Networks	**1689**	414,336	3/32	2267
	Multi-Head	8046	**209,960**	**11/32**	**782**
Variable-key	Separate Networks	**4221**	414,336	4/32	1163
	Multi-Head	14824	**209,960**	**9/32**	**567**

References

[1] Çağdaş Gül et al., "A New Construction Method for Keystream Generators", *IEEE Transactions on Information Forensics and Security 18*, pp. 3735–3744, 2023.

[2] Martin Schmid et al., "Robust and Energy-efficient Hardware Architectures for DIZY Stream Cipher", *IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 461–465, 2024.