GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
AI-NET-PROTECT
DRESDEN concept

28. VDE ITG Fachtagung Mobilkommunikation
Hochschule Osnabrück \\ 16.05.2024

Attack on Machine Learning based Physical Layer Key Generation scheme

Amelie Wagner, Dawid Franzoso, Stefan Köpsell
Dresden University of Technology (TUD)

Overview

Working on project regarding Physical Layer Security

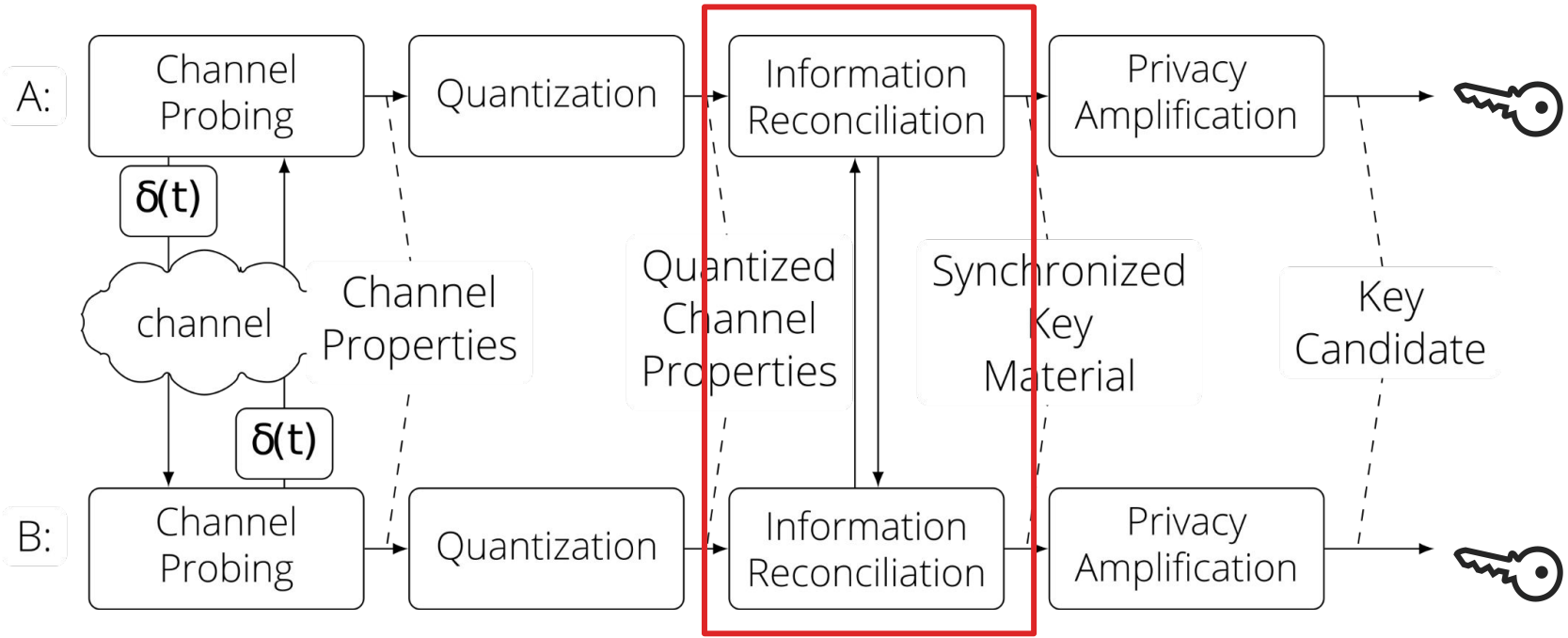
Tried using an existing, already published method:
P. Walther and T. Strufe, *Blind twins: Siamese networks for non-interactive information reconciliation* [0]

Discovery: Method **not working** as expected

Publish our findings (regarding existing method):
Re-Implementation, evaluation of results, code is public[1]

[1] https://dud-scm.inf.tu-dresden.de/dud/ml-based-physical-layer-key-generation

“Classical” Physical Layer Key Generation (PLKG)
Pipeline-Approach



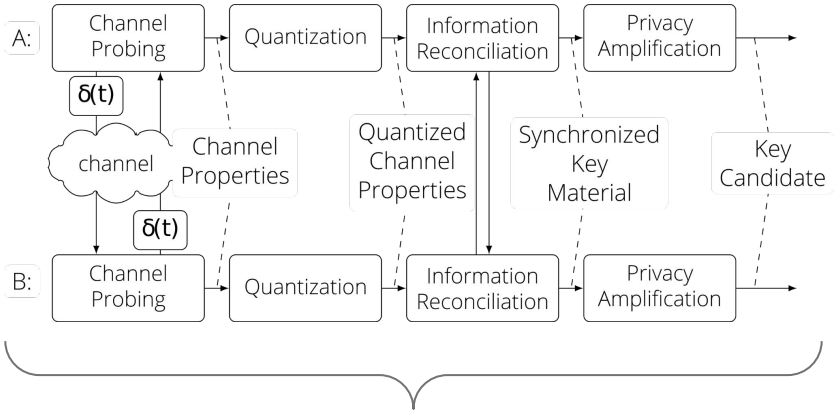
Original Idea
of the method by Walther et al. [0]

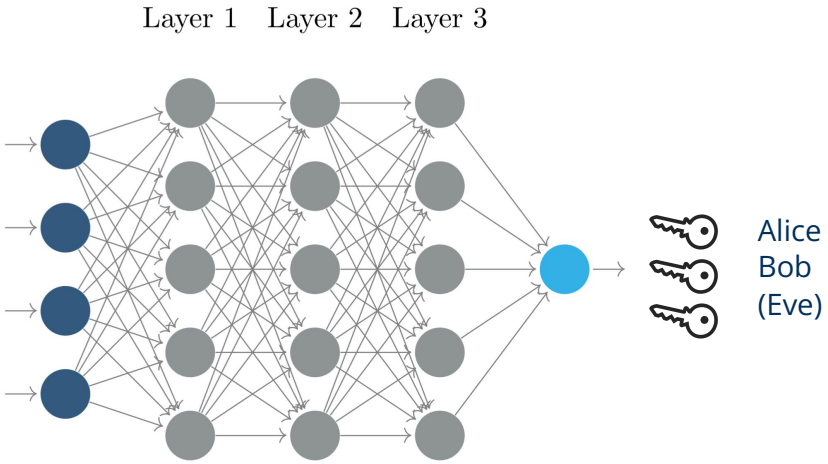
Solve Information Leakage problem:

→ use **one algorithm** for **all steps** of pipeline

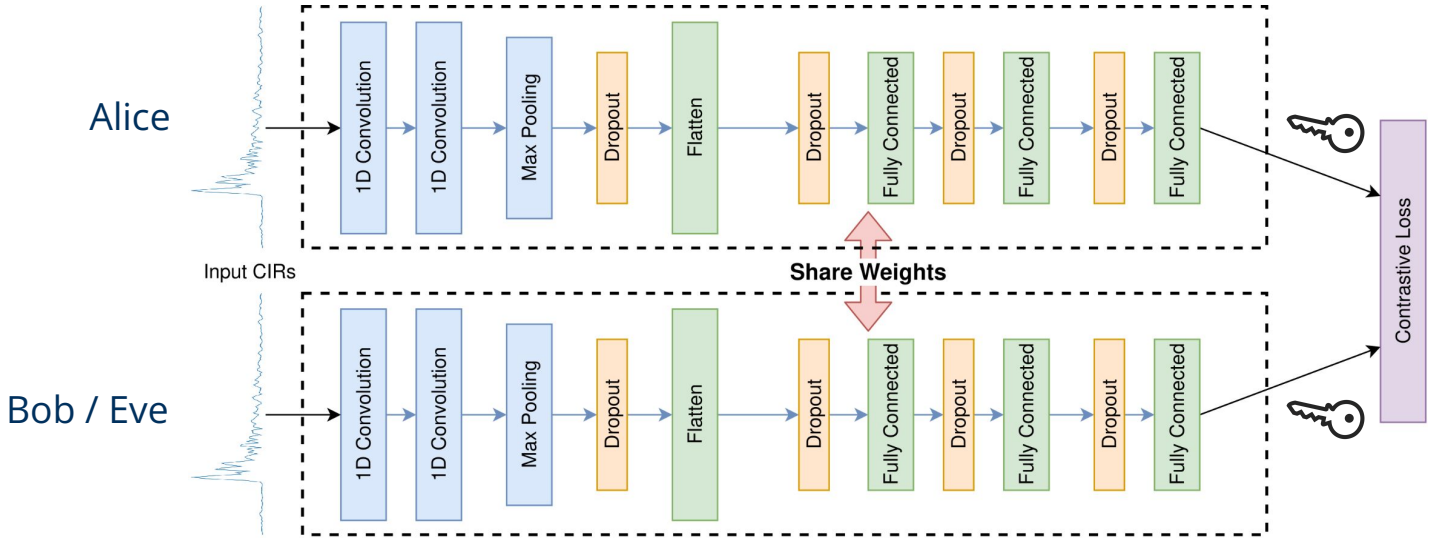
More specifically:
Neuronal Network with

- Input: Channel Impulse Response (CIR) of Alice, Bob, (Eve)
- Output: Keys for Alice, Bob, (Eve)

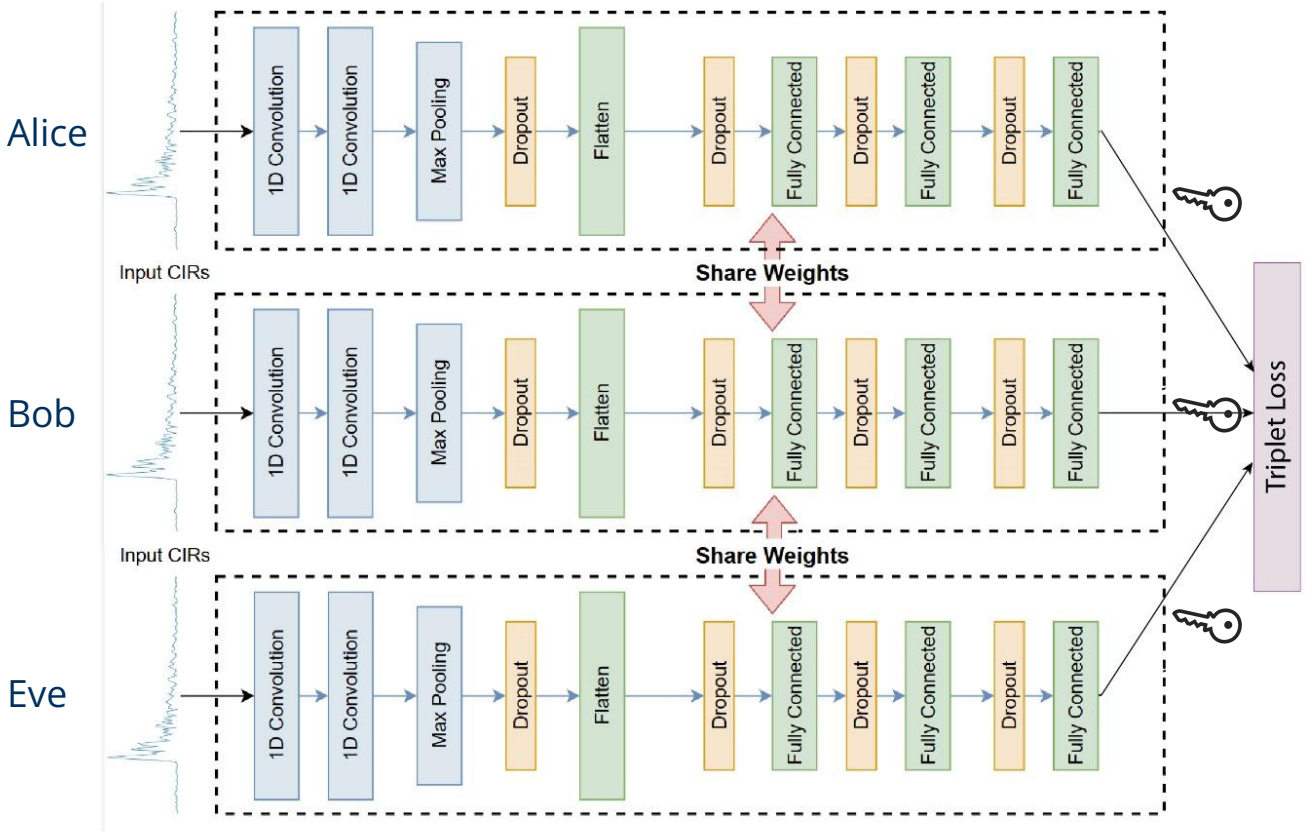




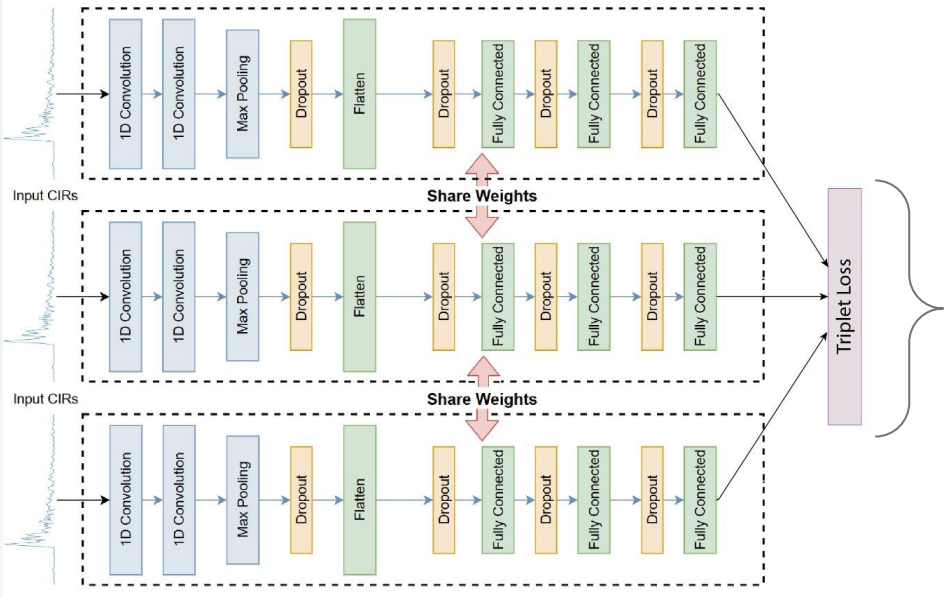
Network Architecture: Siamese Twin Network



Network Architecture: Triplet Network



Network Architecture: Triplet Network
Loss Function



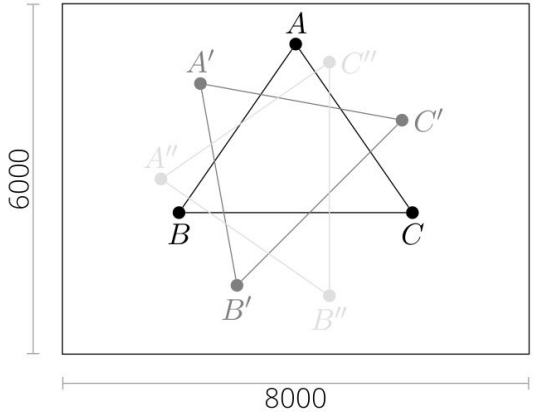
$$L(X_A, X_P, X_N) = \max(D_P - D_N + m, 0)$$

$$D(x, y) = y(1 - x) + (1 - y)x$$

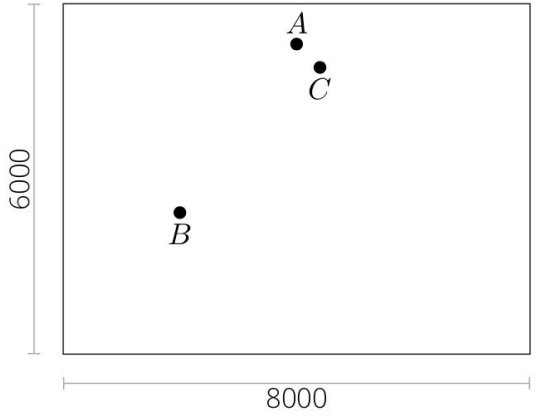
Dataset
used for training original method

Each communication partner:
Sending impulse, others measure signal (Channel Impulse Response)

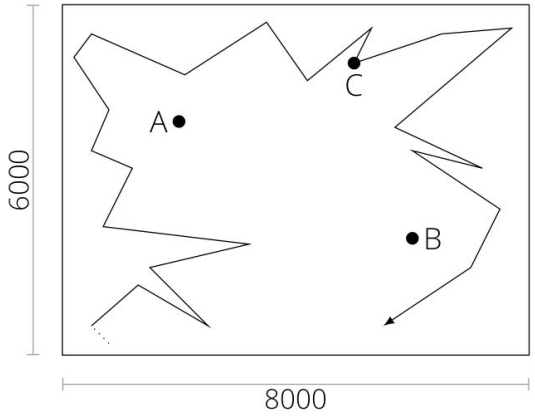
Each scenario:
Static or Dynamic
Same amount of measurements



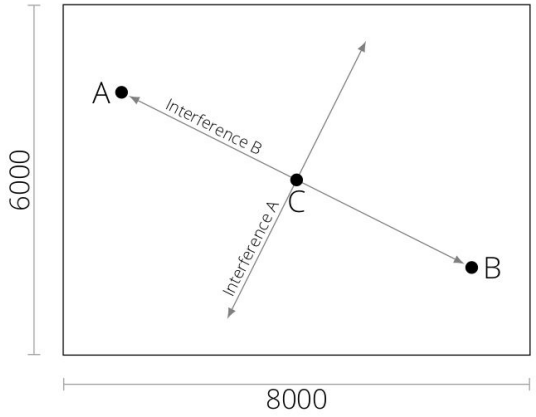
(a) Scenarios: Static A,B,C



(b) Scenario: Static D



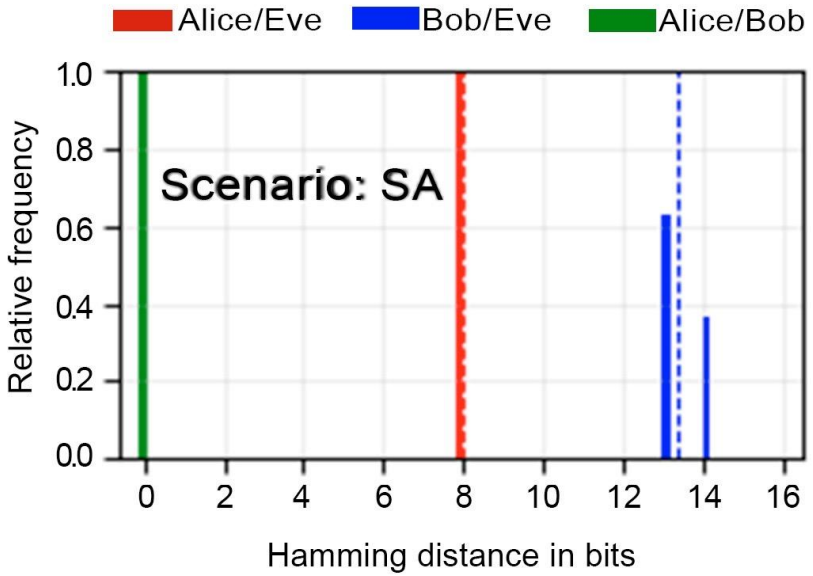
(c) Scenario: Moving Eve

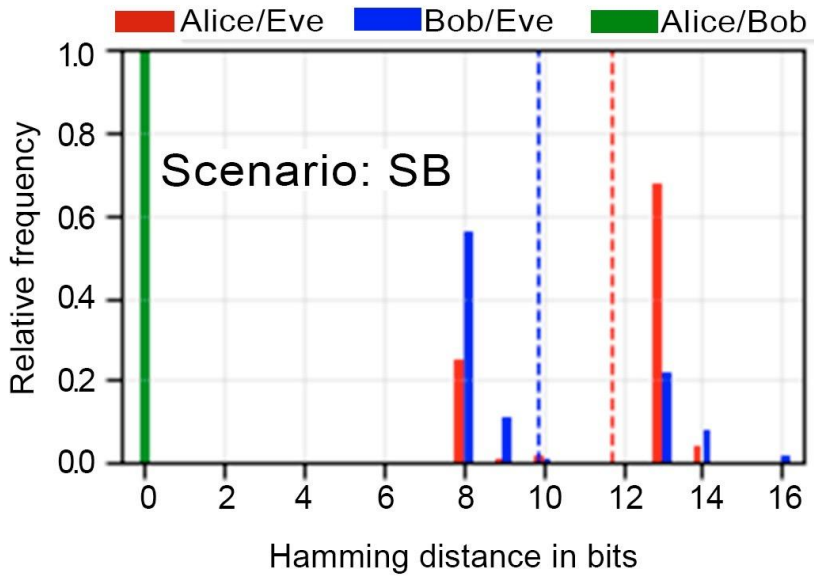


(d) Scenarios: Interference A,B

Original Results - Examples Static Scenarios

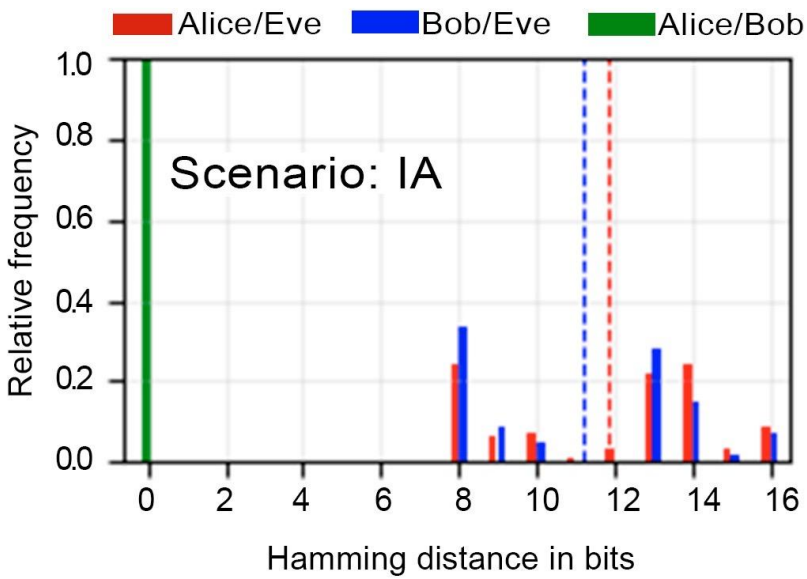
Walther et al. [0]

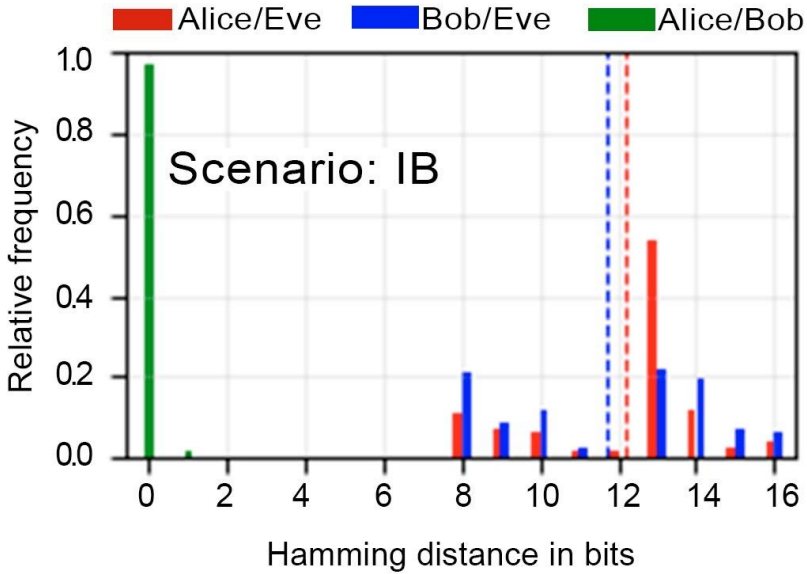




Original Results - Examples Dynamic Scenarios

Walther et al. [0]

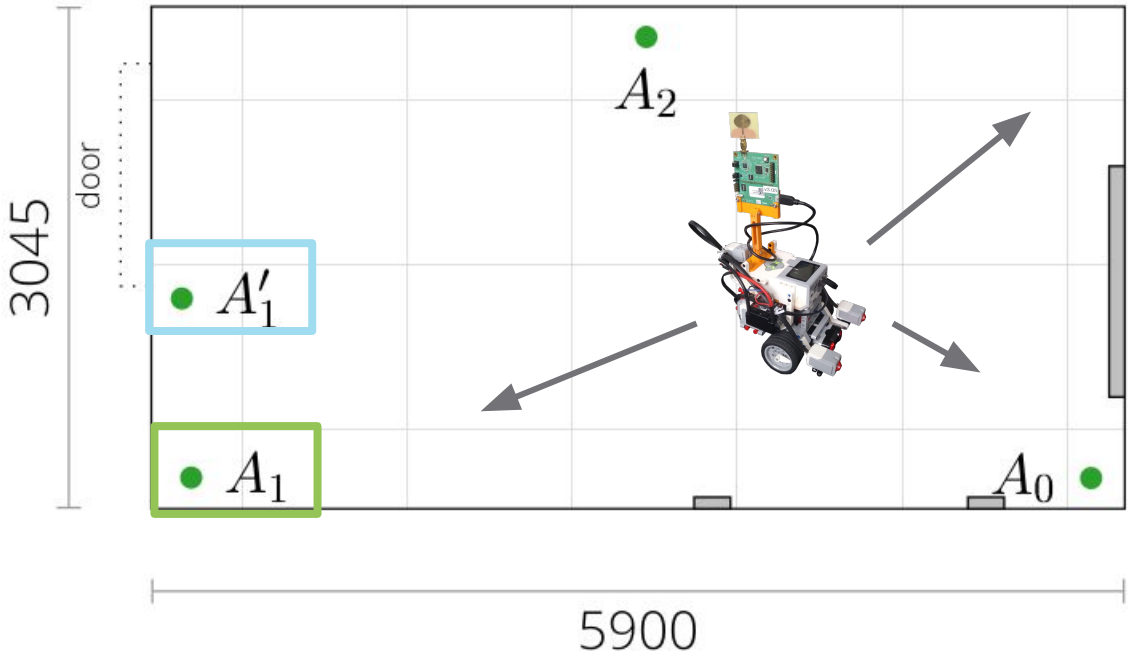




Dataset
used for training “our” model [2]

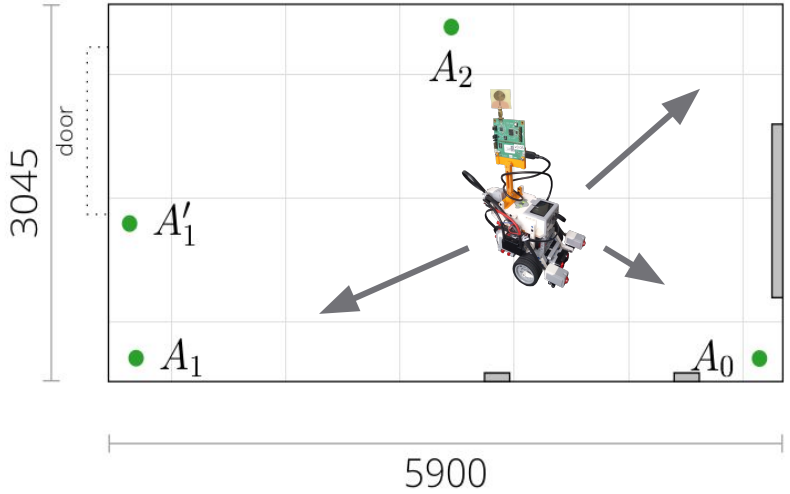
Asymmetric Setting

Symmetric Setting



Dataset
used for training “our” model

Static	Dynamic (+ Robot)
Symmetric-No-Move	Symmetric
Asymmetric-No-Move	Symmetric-Varying-Speed
	Asymmetric
	Asymmetric-Reflector

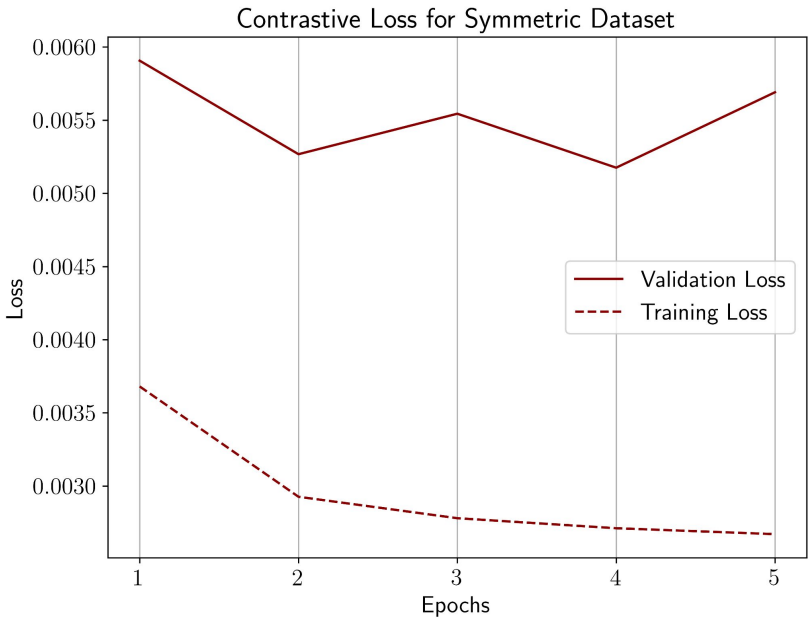


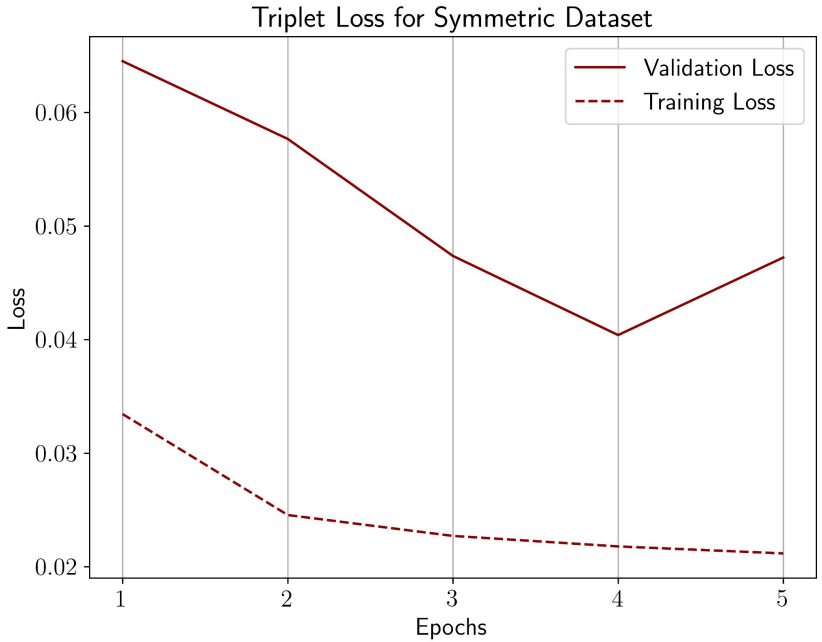
Dataset was evaluated for randomness

Dataset
used for training “our” model

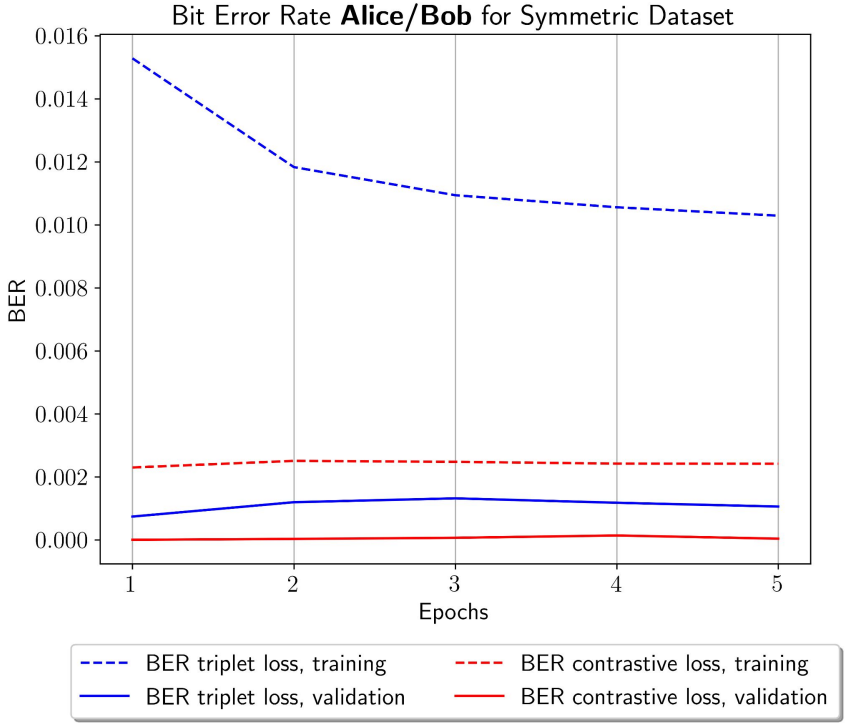
Data Set	Duration	Realizations
symmetric	56 h	845 250
asymmetric	19 h	281 595
reflector	20 h	299 730
var. speed	16 h	237 424
no movement	40 min	5418
total	111 h 40 min	1 669 417

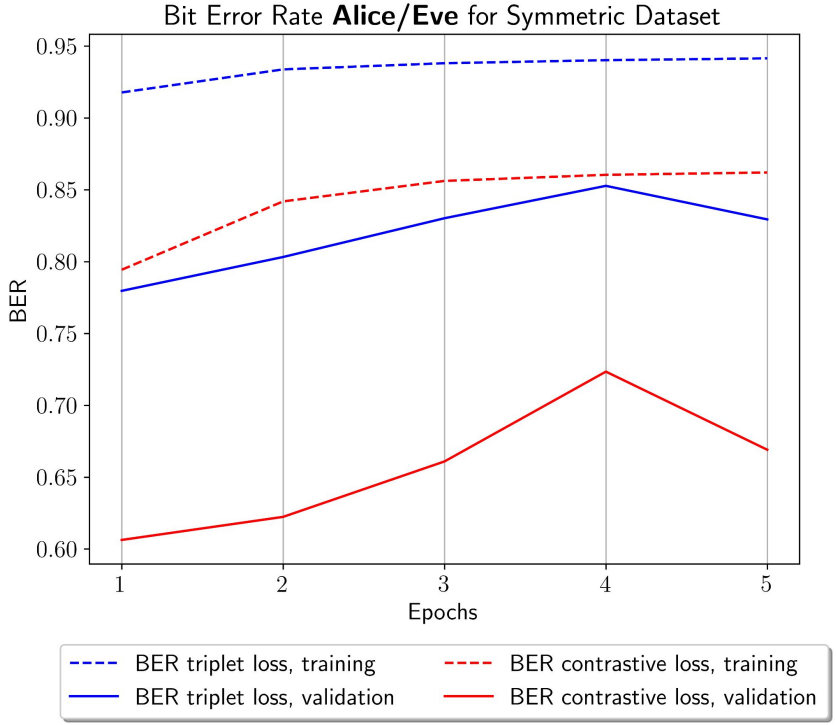
Results - Loss for Siamese + Triplet Network
for the symmetric dataset



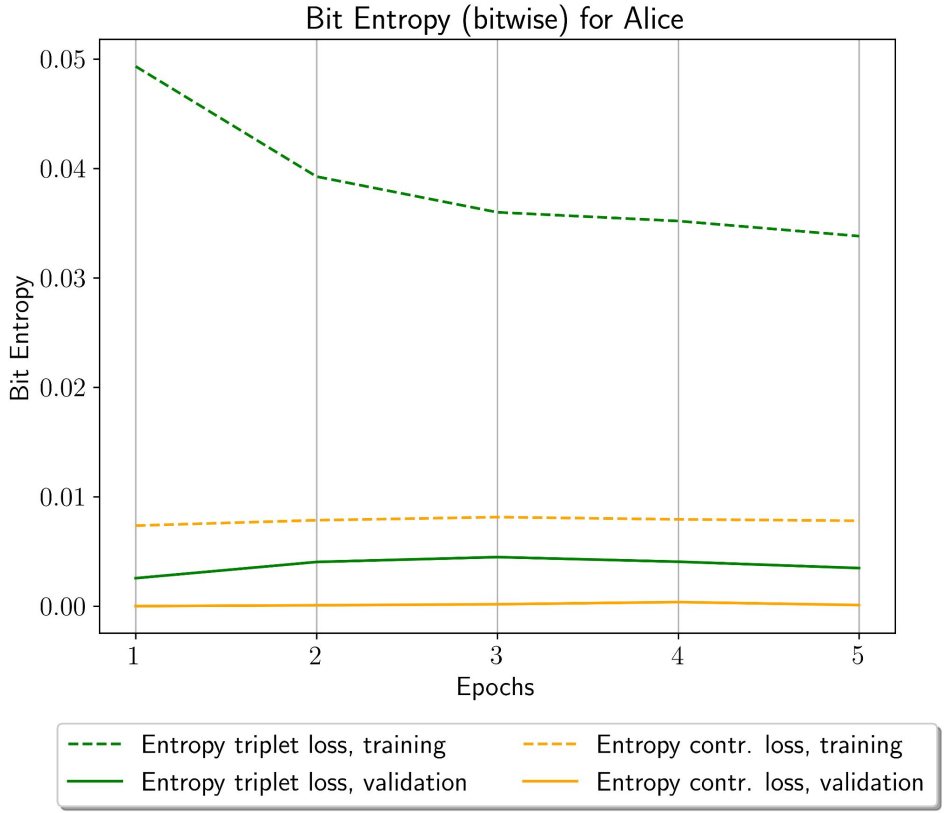


Results - Bit Error Rate (BER)
for **Alice/Bob** and **Alice/Eve** respectively





Results - Bit Entropy (for Alice)



Key Analysis
for the **static** scenarios, **Triplet-Network**

Predicted keys / participant: 1600

Scenario		Most common key(s) (out of 1600 predicted)	#unique keys	Notes
Symmetric-No-Move	**Alice/Bob**	`0011010100100110` (1384x)	12	
	Eve	`1100101111011000` (1278x)	21	Inverse key of Alice/Bob (except for 2 identical bits)
Asymmetric-No-Move	**Alice/Bob**	`0010111110011100` (1473x) `1101000100100011` (120x)	9	Inverse to each other (except of 2 bits)
	Eve	`1101000100100011` (1473x)	14	Identical to (one) key of Alice/Bob

Key Analysis
for the **dynamic** scenarios, **Triplet-Network**

Scenario		Most common keys (out of 1600 predicted)	#unique keys	Notes
Symmetric	**Alice/Bob**	1101000010111101 (1599x) 0010111101000010 (1x)	2	Inverse to each other
	Eve	1101000010111101 (1030x)	16	Identical to Alice/Bob
Symmetric-Varying-Speed	**Alice/Bob**	1011110100010011 (1599x) 0100001011101100 (1x)	2	Inverse to each other (except 1 bit)
	Eve	1011110100010011 (844x) 0100001011101101 (717x)	27	Inverse of each other, identical to Alice/Bob
Asymmetric	**Alice/Bob**	1101001100010001 (1600x)	1	Always same key
	Eve	1101001100010001 (956x)	24	Identical to Alice
Asymmetric-Reflector	**Alice**	0111110100101011 (1600x)	1	Always same key
	Eve	0111110100101011 (1129x)	20	Identical to Alice

Results Key Analysis

Main characteristics of keys: 

- Alice & Bob - always same key(s)
- Keys are practically **static** - only variate in 3-4 bits (out of 16 Bits)
- Keys are **flipped / inverted**

→ network seems to classify in two classes of keys

Conclusion

Our results:

Produced keys have desired Hamming Distance (low BER), but **not** random

- Randomness of keys - probably not evaluated extensively before
- Focus on Hamming Distance

Our theory:

- Key problem in **loss-function** of network:
  Randomness **not** included, only distance between keys

→ Method for solving all steps of PLKG in one step:
unfortunately does not seem to work as intended

→ Extracting randomness with neural network - not a trivial task

Thank you
for your attention.

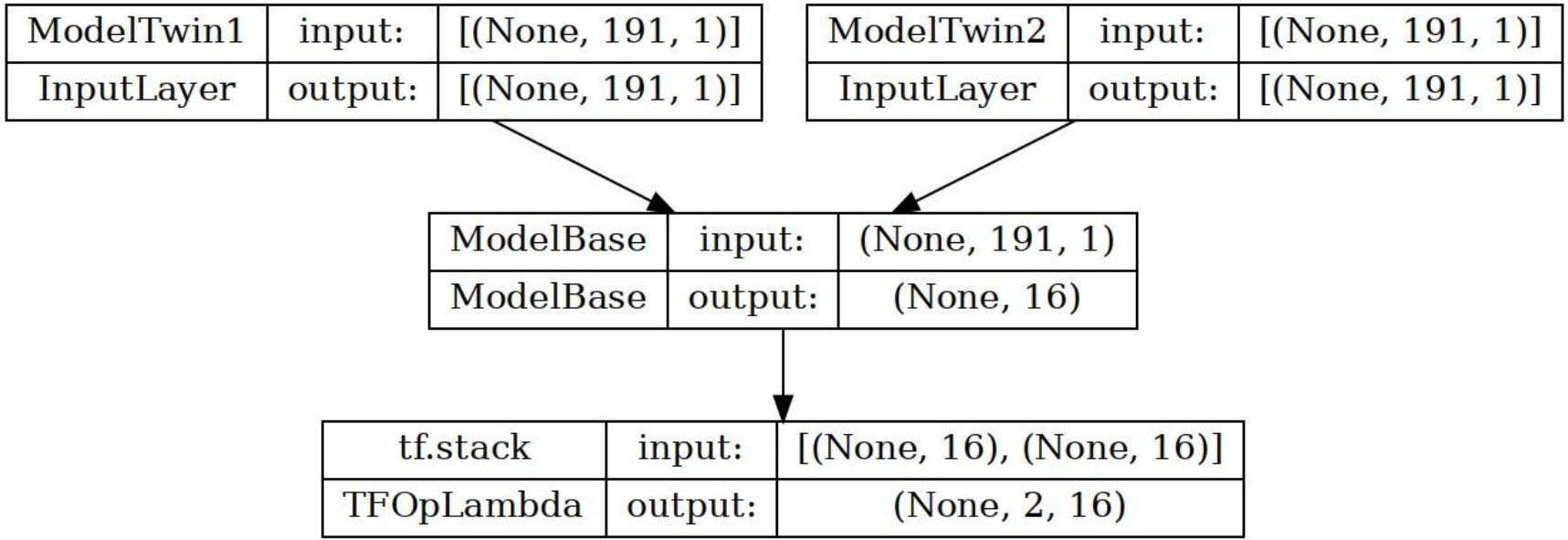
Sources

Original Method:
[0] P. Walther and T. Strufe, “Blind twins: Siamese networks for non-interactive information reconciliation,” in 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, 2020, pp. 1–7

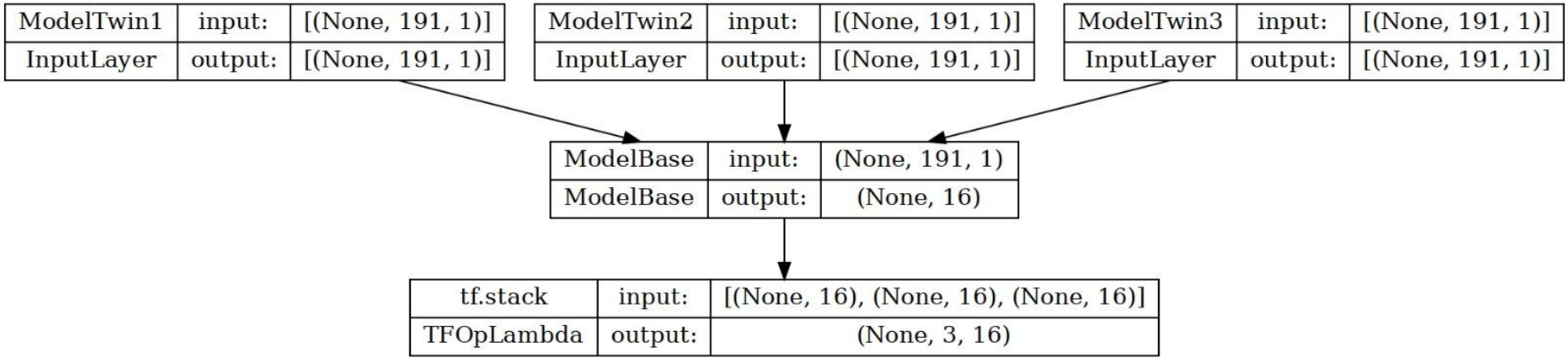
Our Re-Implementation:
[1] “Re-implementation of Siamese and Triplet Network”. Online: https://dud-scm.inf.tu-dresden.de/dud/ml-based-physical-layer-key-generation

Source for Dataset:
[2] P. Walter and R. Knauer and T. Strufe, “Ultra-Wideband Channel State Information and Localization for Physical Layer Security. IEEE Dataport, https://dx.doi.org/10.21227/0wej-bc28. 2021

Backup Slide
Siamese Network



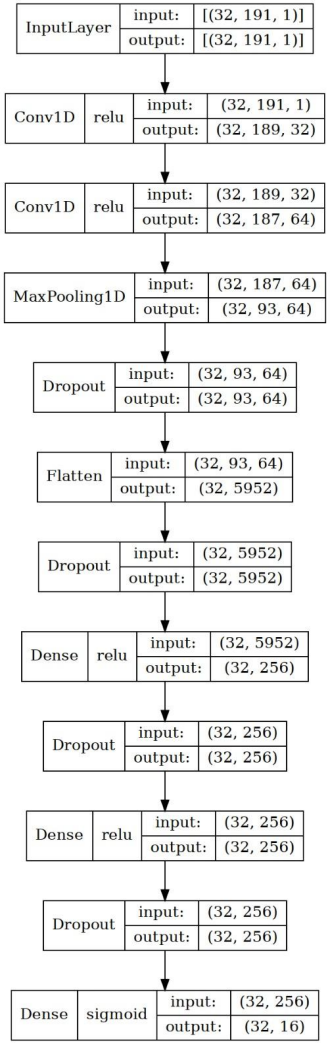
Backup Slide
Triplet Network



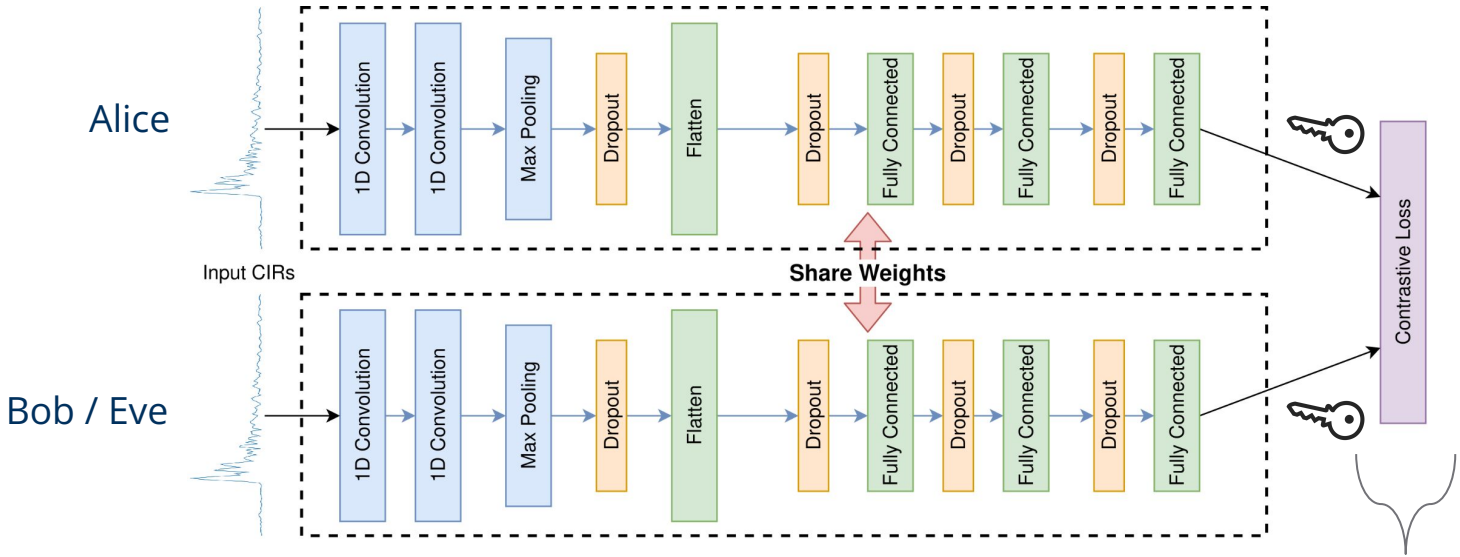
Backup Slide
Siamese / Triplet Neural Network

Architecture of the re-implementation:

- Optimizer: Nesterov Adam (default parameters)
- Batch size: 32
- Slice length / length of one CIR: 191



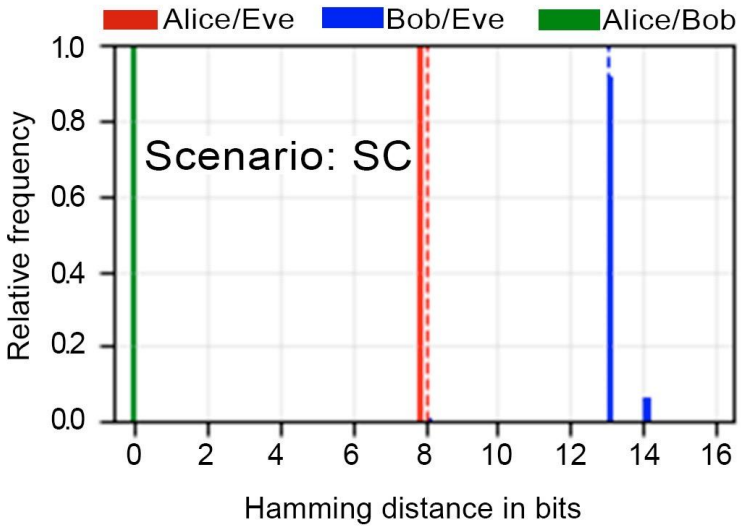
Backup Slide
Network Architecture: Siamese Twin Network

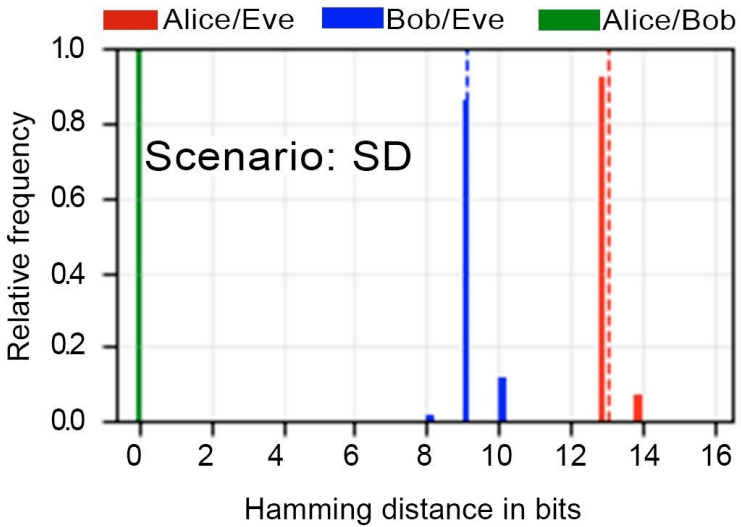


$$L(Y, X_1, X_2) = (1 - Y)\frac{1}{2}D^2 + Y\frac{1}{2}(\max(m - D, 0))^2$$

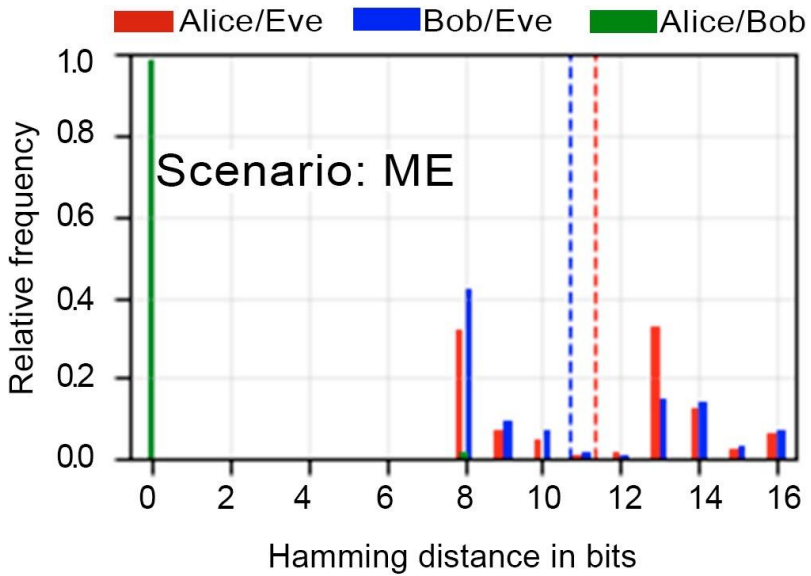
$$D(x, y) = y(1 - x) + (1 - y)x$$

Backup Slide
Original Results - Static Scenarios SC, SD
Walther et al. [0]





Backup Slide
Original Results - Dynamic Scenario ME
Walther et al. [0]



Backup Slide
Original Results - all dataset scenarios
Walther et al. [0]