Using Neural Net
Launch a Preim
Reduced-Ro

Erica D

Advisor: Kevin Cr

etwork Chains to
mage Attack on
ound SHA-1

a Dong

n Crowthers, PhD

Research Question

Can neural networks be used to conduct a preimage attack?

Hypothesis

Linking together neural networks that are individually trained on data from each round of the cryptographic hash SHA-1 will reduce the complexity each network needs to model, allowing deduction of the preimage.

Knowledge Gap

- Previous work using neuro-cryptanalysis for preimage attacks against modern, non-lightweight hashes has been mostly ineffective (Goncharov, 2019; Liu et al., 2021)
    - Attacked the entire hash with a single neural network
- Failed to take into account the internal structure of the algorithm

Analysis

- Accuracy remained at 0 regardless of any modifications to hyperparameters or training data
- Fundamental issue: some information is lost in each round, so all candidate previous rounds are equally plausible
- Major limitation: lack of computing power resulted in datasets insufficient to train for a modern hash effectively

Conclusion

- Aimed to leverage machine learning advancements for preimage attacks, but all tested neural network architectures were completely ineffective in reversing single rounds
- Future research may explore combining neural network chains with meet-in-the-middle attacks, which have similar strategic paradigms

- Clarified an approach that does not work; research in classical or differential-neural cryptanalysis may be more fruitful

References

Goncharov, S. V. (2019). *Using fuzzy bits and neural networks to partially invert few rounds of some cryptographic hash functions*. arXiv. https://doi.org/10.48550/ARXIV.1901.02438

Greydanus, S. (2017). *Learning the Enigma with recurrent neural networks* (arXiv:1708.07576). arXiv. http://arxiv.org/abs/1708.07576

Liu, G., Lu, J., Li, H., Tang, P., & Qiu, W. (2021). Preimage attacks against lightweight scheme Xoodyak based on deep learning. In K. Arai (Ed.), *Advances in Information and Communication* (Vol. 1364, pp. 637–648). Springer International Publishing. https://doi.org/10.1007/978-3-030-73103-8_45

Sharma, N., & Bhatt, R. (2018). Privacy preservation in WSN for healthcare application. *Procedia Computer Science*, *132*, 1243–1252. https://doi.org/10.1016/j.procs.2018.05.040

So, J. (2020). Deep learning-based cryptanalysis of lightweight block ciphers. *Security and Communication Networks*, *2020*, 1–11. https://doi.org/10.1155/2020/3701067

Acknowledgements

Thank you to Dr. Thomas Peyrin, Joshua DeOliveira, my friends, my parents, everybody who has given me feedback, and Dr. Crowthers for supporting and advising me in my research.

Main Ta

Neither feed-forward neural n
networks, even with restricte
successful in reversing a singl
could not be chained together. T
are not effective for conducting
modern hash s

akeaway

networks nor recurrent neural
ed inputs or fuzzy data, were
gle layer of SHA-1. Hence, they
Therefore, neural network chains
a preimage attack on a reduced
such as SHA-1.

modern hash s

Layer Amount	Learning Rate	Round	Epochs	Batch Size	Loss	Train Accuracy	Test Accuracy	Datase
3	0.001	2	11	32	377.5233	0	0	
3	0.001	2	11	64	377.6703	0	0	
7	0.01	2	11	64	377.4963	0	0	
3	0.001	2	11	64	377.5508	0	0	
3	0.001	16	11	64	405.3415	0	0	
3	0.01	16	11	64	405.2192	0	0	
3	0.01	2	11	64	379.9132	0	0	
3	0.01	3	11	64	428.5194	0	0	
3	0.01	3	50	64	428.6604	0	0	
3	0.01	3	11	64	438.9447	0	0	restricte
3	0.01	3	11	64	399.1621	0	0	1 millio
3	0.01	3	11	64	468.2508	0	0	fuzzy d

Layer Amount	Learning Rate	Round	Epochs	Batch Size	Loss	Train Accuracy	Test Accuracy	Dataset
3	0.01	3	11	64	428.6908	0	0	
3	0.01	3	11	64	439.0123	0	0	restricte
3	0.01	3	11	64	399.1277	0	0	1 million
3	0.01	3	11	64	468.1121	0	0	fuzzy da

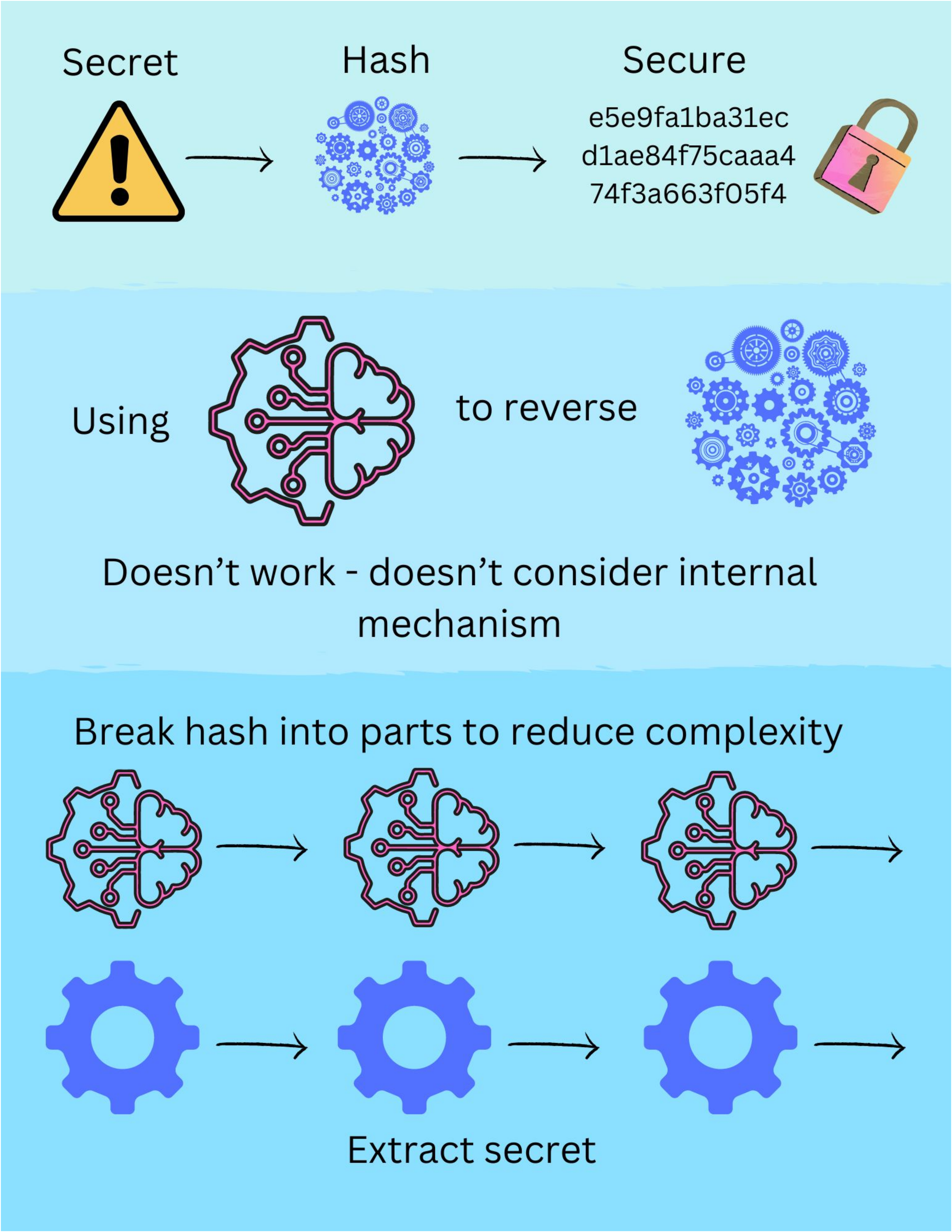
uch as SHA-1.

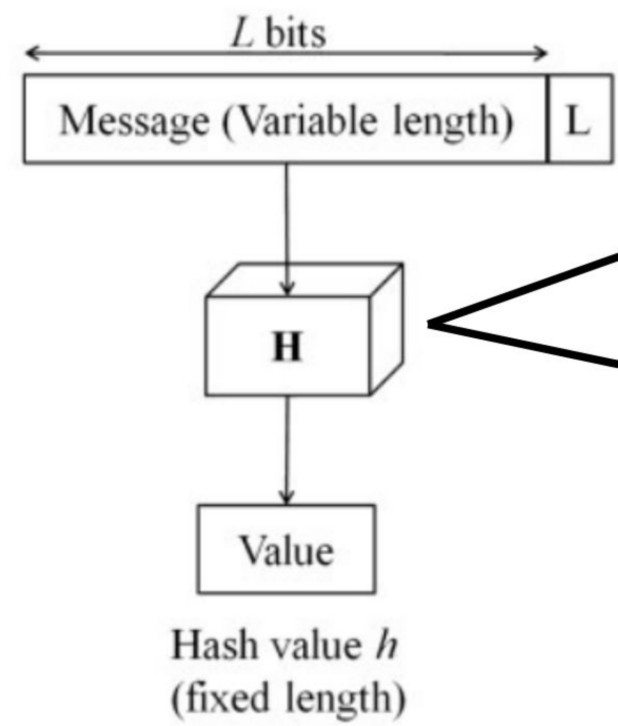
	Bit Accuracy
	0.49
	0.49
	0.49
	0.49
	0.49
	0.49
	0.49
	0.49
	0.49
d input	0.46
dataset	0.51
ta	0.48

Table 1: Accuracies and loss for multilayer feed-forward neural networks with varying hyperparameters and training datasets

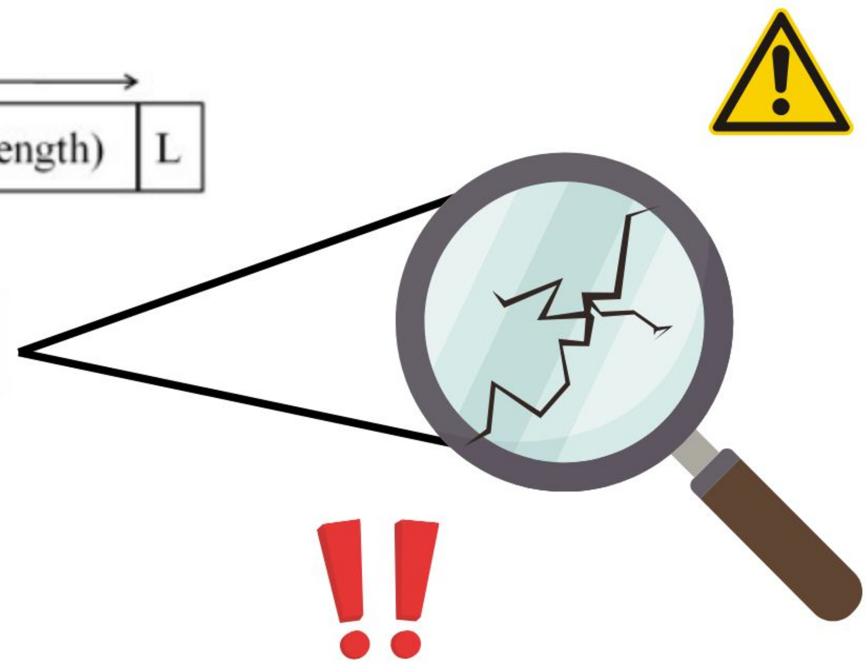
	Bit Accuracy
	0.49
d input	0.46
	0.51
ta	0.48

Table 2: Accuracies and loss for recurrent neural networks with varying hyperparameters and training datasets


Secret
Hash
Secure
e5e9fa1ba31ec
d1ae84f75caaa4
74f3a663f05f4
Using
to reverse
Doesn’t work - doesn’t consider internal mechanism
Break hash into parts to reduce complexity
Extract secret



Structure of a hash function (Sharma & Bhatt, 2018)



Cryptanalysis identifies the issues within these functions.

- **Cryptanalysis:** the process of analyzing systems of information to deduce secret parts of those systems
- Cryptanalysis ensures digital security by identifying weaknesses in critical systems
- Cryptographic hashes: deterministic functions that map the plaintext to the ciphertext approximately randomly
  - Operate in rounds
- Neuro-cryptanalysis can be used for preimage attacks

Proce

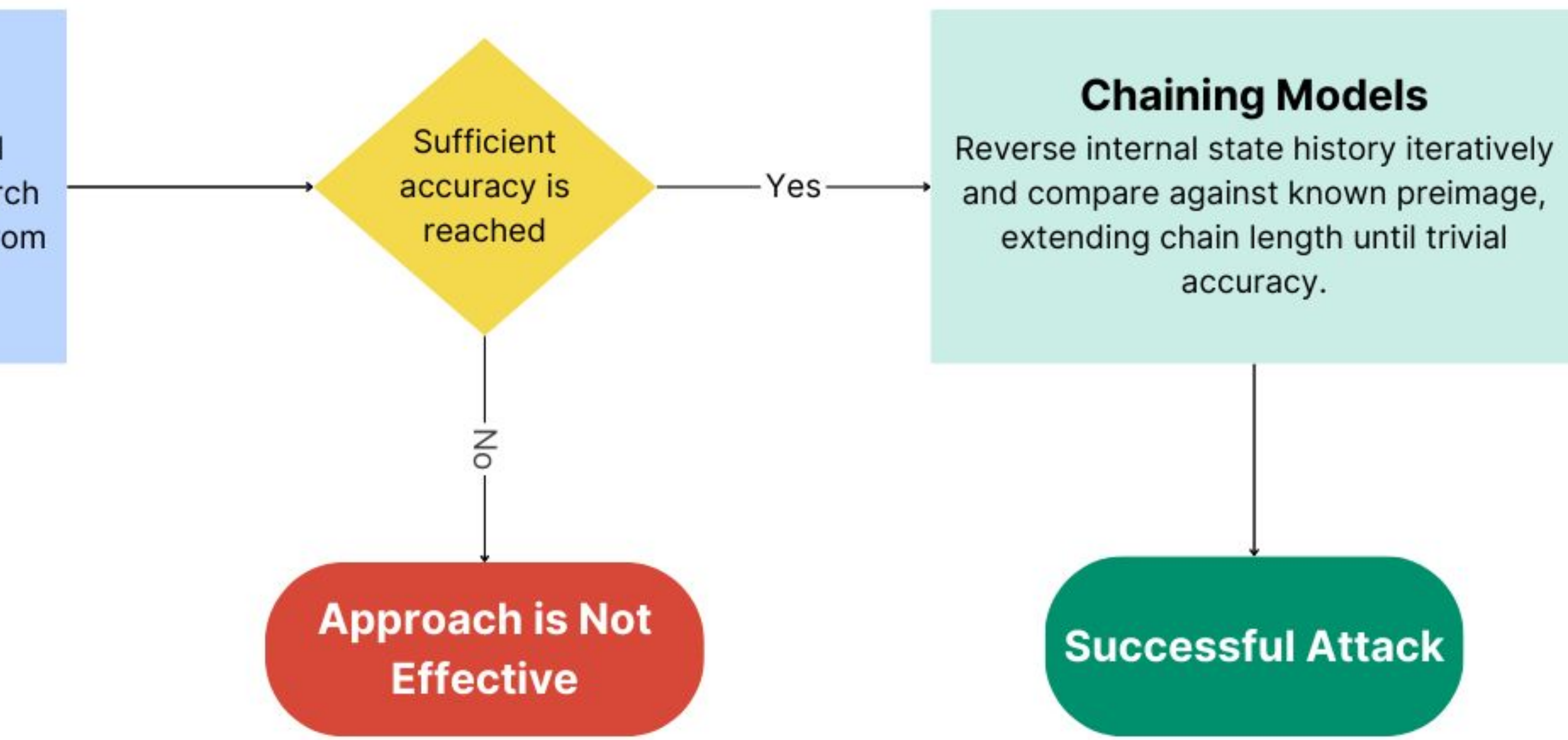
Generate Data

Inputs were randomly generated and hashed with a custom implementation of the SHA-1 hash (both normal and fuzzy) in Java that returns internal states for each round.

Single Layer Learning

Feed-forward and recurrent neural networks were programmed in PyTorch and trained to reverse single layers from the data.

edure



Sufficient accuracy is reached
Yes
No
Chaining Models
Reverse internal state history iteratively and compare against known preimage, extending chain length until trivial accuracy.
Approach is Not Effective
Successful Attack