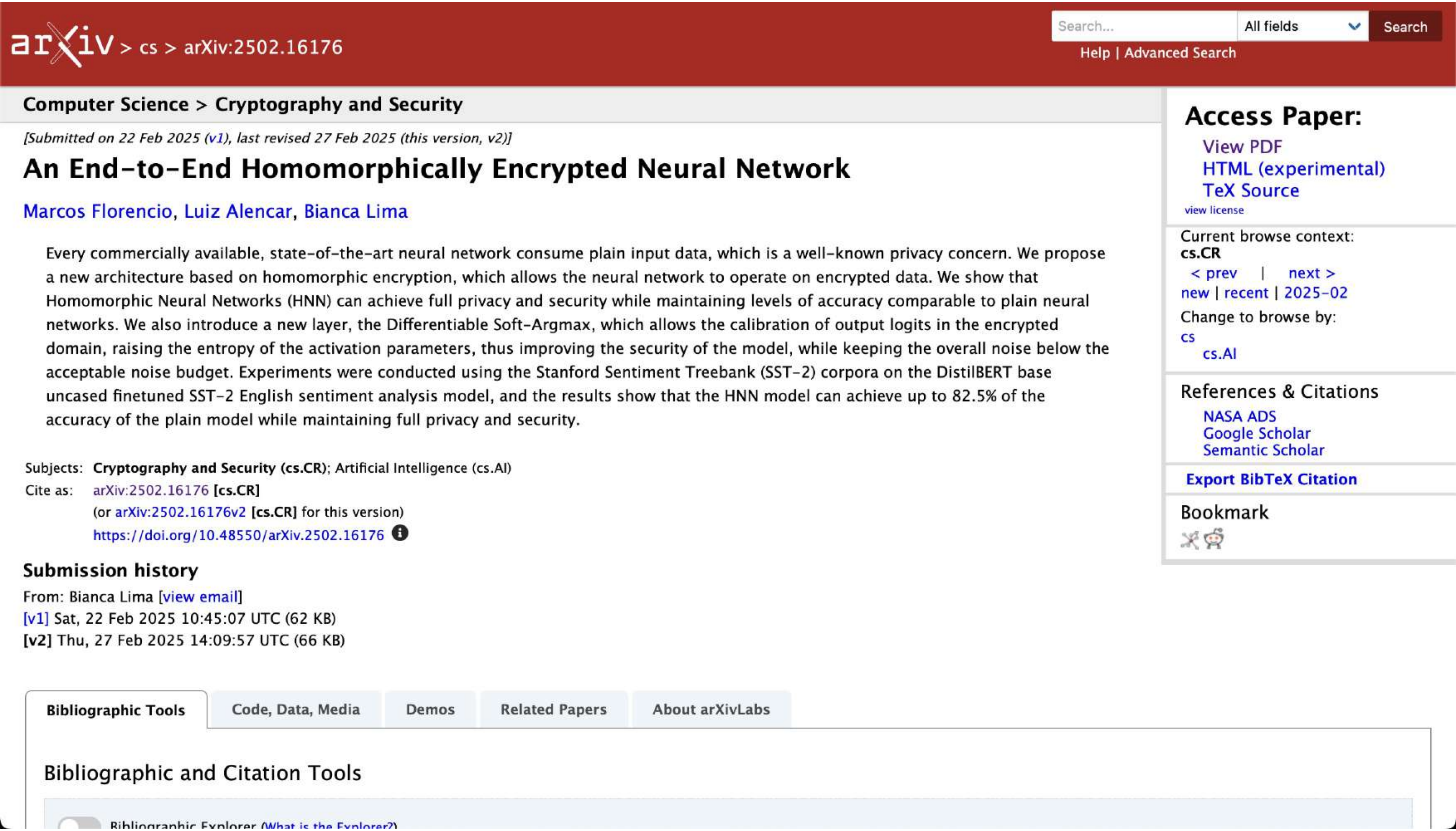

Computer Science > Cryptography and Security

[Submitted on 22 Feb 2025 (v1), last revised 27 Feb 2025 (this version, v2)]

An End-to-End Homomorphically Encrypted Neural Network

Marcos Florencio, Luiz Alencar, Bianca Lima

Every commercially available, state-of-the-art neural network consume plain input data, which is a well-known privacy concern. We propose a new architecture based on homomorphic encryption, which allows the neural network to operate on encrypted data. We show that Homomorphic Neural Networks (HNN) can achieve full privacy and security while maintaining levels of accuracy comparable to plain neural networks. We also introduce a new layer, the Differentiable Soft-Argmax, which allows the calibration of output logits in the encrypted domain, raising the entropy of the activation parameters, thus improving the security of the model, while keeping the overall noise below the acceptable noise budget. Experiments were conducted using the Stanford Sentiment Treebank (SST-2) corpora on the DistilBERT base uncased finetuned SST-2 English sentiment analysis model, and the results show that the HNN model can achieve up to 82.5% of the accuracy of the plain model while maintaining full privacy and security.

Subjects:	**Cryptography and Security (cs.CR)**; Artificial Intelligence (cs.AI)
Cite as:	arXiv:2502.16176 **[cs.CR]**
	(or arXiv:2502.16176v2 **[cs.CR]** for this version)
	https://doi.org/10.48550/arXiv.2502.16176

Submission history

From: Bianca Lima [view email]
[v1] Sat, 22 Feb 2025 10:45:07 UTC (62 KB)
[v2] Thu, 27 Feb 2025 14:09:57 UTC (66 KB)

Bibliographic and Citation Tools

Access Paper: