UltraPlonkova: Minimising Parallel Plonkish Constraints Using Transformers

Joint work with Lúcás Meier

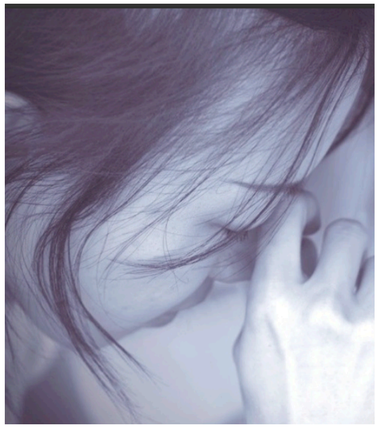
JPA - Eurocrypt 2023 rump session

Prior art

- [KST21] **Nova:** SNARK-less incremental proof system, O(|F|) proof size
  - Used by the Lurk ZK language! (https://lurk-lang.org/)
- [KS22] **SuperNova**: Generalization for arbitrary instruction sets
- [KS23] **HyperNova**: Custom constraints (CCS) + minimal MSM count

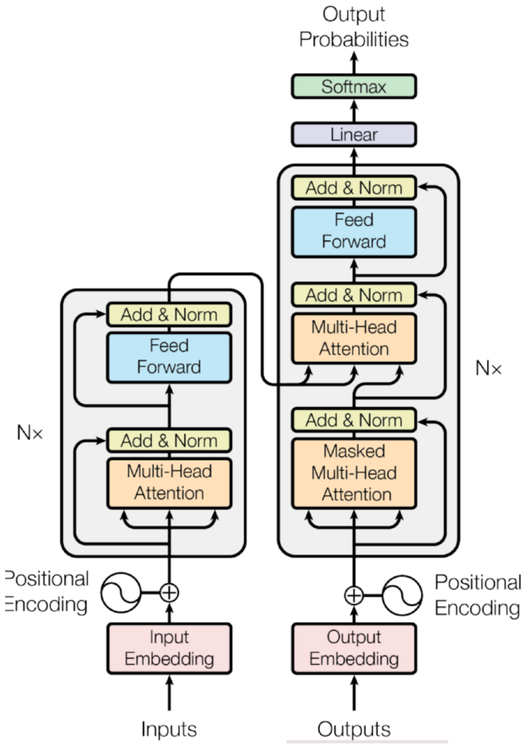
Open problems:

- Automated constraint generation from expressive DSLs
- Efficient parallelisation of proof generation
- Leverage the effect of AI and quantum



From Hyper to Ultra

- Combines ideas from **HyperPlonk** and **Supernova**
- Uses **Transformers** models to create building blocks:
  - Parallel AI custom gates
  - Post-quantum sublineartime zkSNARKS



	Fast	*Simple*	*Secure*
UltraPlonkova	✅	✅	✅
Previous protocols	❌	❌	✅
Even older protocols	❌	❌	❌


INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH