A WIP collection of resources for learning about HE and FHE. The first two sections of the document are dedicated for planning the reading list for FHE kindergarten, section “Basement” contains the resources that were not sorted yet.

partial, somewhat HE & pre-FHE:

- Introduction to HE
- Ronald Rivest, Leonard Adleman and Mike Dertouzos: On Data banks and privacy Homomorphisms
- Taher El Gamal: A Public-key Cryptosystem and a Signature Scheme based on Discrete Logarithms
- Pascal Paillier: Public-key Cryptosystems based on Composite Degree Residuosity Classes
- Ivan Damgard and Mads Jurik: A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-Key System
- Dan Boneh, Eu Jin Goh and Kobbi Nissim: Evaluating 2-DNF Formulas on Ciphertexts
- Craig Gentry, Shai Halevi and Vinod Vaikuntanathan: A Simple BGN-type Cryptosystem from LWE

FHE:

- Introduction to FHE
- [

: Introduction to FHE w/ Pascal Paillier](https://www.youtube.com/watch?v=umqz7kKWxyw)

Basement

- Awesome HE
- [Homomorphic Encryption References

](https://people.csail.mit.edu/vinodv/FHE/FHE-refs.html)

- Zama
- Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based (no relinerarization)
- Blyss
- FHE
- Nigel Smart - Computing on Encrypted Data (Lattices + FHE)
- Gentry’s essay (details on FHE + jewelry analogy)
- Silverberg (mathematical background behind FHE)
- Halevi’s survey: extensive introduction to FHE
- DGHV paper
- DGHV implementation (with description)
- Gentry’s FHE paper
- Survey on FHE

Blogposts

- Ingonyama: Solving LLP privacy with FHE
- Zama: Towards Encrypted Large Language Models with FHE