Homomorphic Encryption References

Last updated Tuesday 23 June 2021

Homomorphic Encryption Standardization Webpage

Daniele Micciancio's Lattice Cryptography Links

Pre-FHE Gen I Gen II Gen III Implementations Applications Multi-Key FHE Miscellaneous

Surveys

- Craig Gentry
  Computing Arbitrary Functions of Encrypted Data
  Communications of the ACM

- Vinod Vaikuntanathan
  Computing Blindfolded: New Developments in Fully Homomorphic Encryption
  FOCS 2011 Tutorial (link to local copy)

- Shai Halevi
  Homomorphic Encryption
  Tutorial on the Foundations of Cryptography, Dedicated to Oded Goldreich (linked from Shai's webpage)

Pre-FHE

- Ronald Rivest, Leonard Adleman and Mike Dertouzos
  On Data Banks and Privacy Homomorphisms
  http://people.csail.mit.edu/rivest/RivestAdlemanDertouzos-OnDataBanksAndPrivacyHomomorphisms.pdf

- Shafi Goldwasser and Silvio Micali
  Probabilistic Encryption
  http://groups.csail.mit.edu/cis/pubs/shafi/1984-jcss.pdf

- Taher El Gamal
  A Public-key Cryptosystem and a Signature Scheme based on Discrete Logarithms
  https://link.springer.com/chapter/10.1007/3-540-39568-7_2

- Pascal Paillier
  Public-key Cryptosystems based on Composite Degree Residuosity Classes
  Springer Link

- Ivan Damgard and Mads Jurik
  A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System
  http://www.brics.dk/RS/00/45/

- Dan Boneh, Eu Jin Goh and Kobbi Nissim
  Evaluating 2-DNF Formulas on Ciphertexts
  http://crypto.stanford.edu/~dabo/abstracts/2dnf.html

- Craig Gentry, Shai Halevi and Vinod Vaikuntanathan
  A Simple BGN-Type Cryptosystem from LWE
  https://eprint.iacr.org/2010/182
  Note: This cryptosystem was discovered after Gentry's work on FHE, as a first attempt to base FHE on standard assumptions such as learning with errors (LWE).

Gen I

- Craig Gentry
  A fully homomorphic encryption scheme
  https://crypto.stanford.edu/craig/craig-thesis.pdf

- Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan
  Fully Homomorphic Encryption over the Integers
  https://eprint.iacr.org/2009/616

- Nigel Smart and Frederik Vercauteren
  Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes
  https://eprint.iacr.org/2009/571

- Craig Gentry
  Toward basing fully homomorphic encryption on worst-case hardness
  http://www.iacr.org/archive/crypto2010/62230116/62230116.pdf

- Shai Halevi and Craig Gentry
  Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits
  https://eprint.iacr.org/2011/279
  Note: I would classify this scheme as "somewhere between" the first and second generations, in the sense that it relies on fewer assumptions than the older schemes, yet it still uses ideal lattices.

Gen II

Key Papers:

- Zvika Brakerski and Vinod Vaikuntanathan
  Efficient Fully Homomorphic Encryption from (Standard) LWE
  https://eprint.iacr.org/2011/344

- Zvika Brakerski, Craig Gentry and Vinod Vaikuntanathan
  Fully Homomorphic Encryption without Bootstrapping
  https://eprint.iacr.org/2011/277

- Zvika Brakerski
  Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP
  https://eprint.iacr.org/2012/078

- Craig Gentry, Shai Halevi and Nigel Smart
  Fully Homomorphic Encryption with Polylog Overhead
  https://eprint.iacr.org/2011/566

- Craig Gentry, Shai Halevi and Nigel Smart
  Homomorphic Evaluation of the AES Circuit
  https://eprint.iacr.org/2012/099

Other Works:

- Craig Gentry, Shai Halevi, Chris Peikert and Nigel P. Smart
  Field Switching in BGV-Style Homomorphic Encryption
  http://eprint.iacr.org/2012/240

- Zvika Brakerski, Craig Gentry, and Shai Halevi
  Packed Ciphertexts in LWE-Based Homomorphic Encryption

https://eprint.iacr.org/2012/565

- Adriana Lopez-Alt, Eran Tromer and Vinod Vaikuntanathan
  Multikey Fully Homomorphic Encryption and On-the-Fly Multiparty Computation
  https://eprint.iacr.org/2013/094

- Junfeng Fan and Frederik Vercauteren
  Somewhat Practical Fully Homomorphic Encryption
  https://eprint.iacr.org/2012/144

- Tancrede Lepoint and Michael Naehrig
  A Comparison of the Homomorphic Encryption Schemes FV and YASHE
  https://eprint.iacr.org/2014/062

Gen III

- Craig Gentry, Amit Sahai and Brent Waters
  Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based
  https://eprint.iacr.org/2013/340

- Zvika Brakerski and Vinod Vaikuntanathan
  Lattice-Based FHE as Secure as PKE
  https://eprint.iacr.org/2013/541

- Jacob Alperin-Sheriff and Chris Peikert
  Faster Bootstrapping with Polynomial Error
  https://eprint.iacr.org/2014/094

- Leo Ducas and Daniele Micciancio
  FHEW: Bootstrapping Homomorphic Encryption in less than a second
  https://eprint.iacr.org/2014/816

- Ryo Hiromasa, Masayuki Abe and Tatsuaki Okamoto
  Packing Messages and Optimizing Bootstrapping in GSW-FHE
  Talk Slides and Springer Link

- Ilaria Chillotti and Nicolas Gama and Mariya Georgieva and Malika Izabachène
  Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds
  https://eprint.iacr.org/2016/870

Open Source Implementations

- Shai Halevi and Victor Shoup
  HELib: An Implementation of Homomorphic Encryption
  https://github.com/shaih/HElib

  Algorithms in HELib
  https://eprint.iacr.org/2014/106

  Bootstrapping for HELib
  https://eprint.iacr.org/2014/873

- Hao Chen, Kim Laine and Rachel Player (Microsoft Research)
  SEAL: Simple Encrypted Arithmetic Library
  https://www.microsoft.com/en-us/research/project/homomorphic-encryption/

- Yuriy Polyakov, Kurt Rohloff
  PALISADE

https://palisade-crypto.org/

- Tancrede Lepoint
  NFLLib
  https://github.com/quarkslab/NFLlib

- Leo Ducas and Daniele Micciancio
  FHEW
  https://github.com/lducas/FHEW

- Wei Dai, Yarkin Doroz and Berk Sunar
  cuHE: CUDA Homomorphic Encryption Library
  https://github.com/vernamlab/cuHE

- Daniele Micciancio (based on this paper)
  SWIFFT
  https://github.com/micciancio/SWIFFT
  Note: SWIFFT is a lattice cryptography library that implements (for a specific dimension) power-of-2 cyclotomic using NTT and SSE/AVX parallelism optimizations.

Applications

- Kristin Lauter, Michael Naehrig and Vinod Vaikuntanathan
  Can Homomorphic Encryption be Practical?
  https://eprint.iacr.org/2011/405

- Raphael Bost, Shafi Goldwasser, Raluca Ada Popa and Stephen Tu
  Machine Learning Classification on Encrypted Data
  https://eprint.iacr.org/2014/331

- David Wu and Jacob Haven
  Using Homomorphic Encryption for Large-Scale Statistical Analysis
  https://crypto.stanford.edu/people/dwu4/papers/FHE-SI_Report.pdf

Multi-Key FHE

- Adriana Lopez-Alt, Eran Tromer and Vinod Vaikuntanathan
  Multikey Fully Homomorphic Encryption and On-the-Fly Multiparty Computation
  https://eprint.iacr.org/2013/094

- Michael Clear and Ciarán McGoldrick
  Multi-Identity and Multi-Key Leveled FHE from Learning with Errors
  https://eprint.iacr.org/2014/798

- Pratyay Mukherjee and Daniel Wichs
  Two Round Multiparty Computation via Multi-Key FHE
  https://eprint.iacr.org/2015/345

- Zvika Brakerski and Renen Perlman
  Lattice-Based Fully Dynamic Multi-Key FHE with Short Ciphertexts
  https://eprint.iacr.org/2016/339

- Chris Peikert and Sina Shiehian
  Multi-Key FHE from LWE, Revisited
  https://eprint.iacr.org/2016/196

- Yevgeniy Dodis, Shai Halevi, Ron Rothblum and Daniel Wichs
  Spooky Encryption and Its Applications
  https://eprint.iacr.org/2010/182

Miscellaneous

- Craig Gentry, Shai Halevi and Vinod Vaikuntanathan
  i-Hop Homomorphic Encryption and Rerandomizable Yao Circuits
  https://eprint.iacr.org/2010/145
- Rafail Ostrovsky, Anat Paskin-Cherniavsky and Beni Paskin-Cherniavsky
  Maliciously Circuit-Private FHE
  https://eprint.iacr.org/2013/307
- Leo Ducas and Damien Stehle
  Sanitization of FHE Ciphertexts
  https://eprint.iacr.org/2016/164
- Florian Bourse, Rafael Del Pino, Michele Minelli and Hoeteck Wee
  FHE Circuit Privacy Almost for Free
  https://eprint.iacr.org/2016/381
- Ron Rothblum
  Homomorphic Encryption: From Private Key to Public Key
  https://eccc.weizmann.ac.il/report/2010/146/

Maintained by Vinod Vaikuntanathan