PIR + FHE: CHIP'N'DALE OF PRIVACY

A survey on PIR and FHE

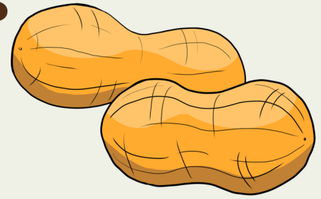
Presented By Luiza Soezima

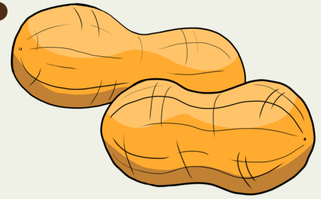
TEAM

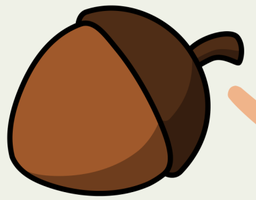
LUIZA

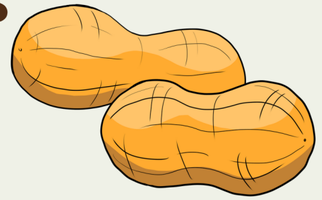
SOFIA

PRIVATE INFORMATION RETRIEVAL



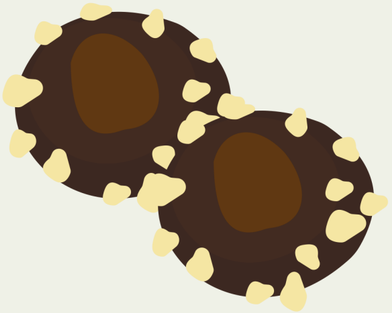


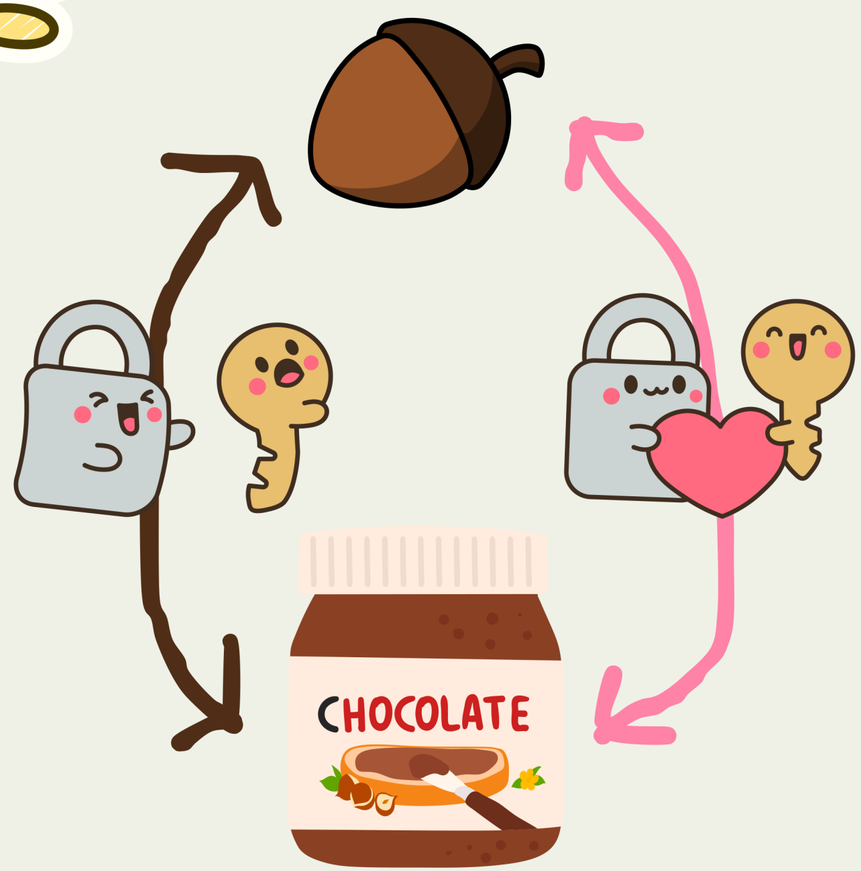


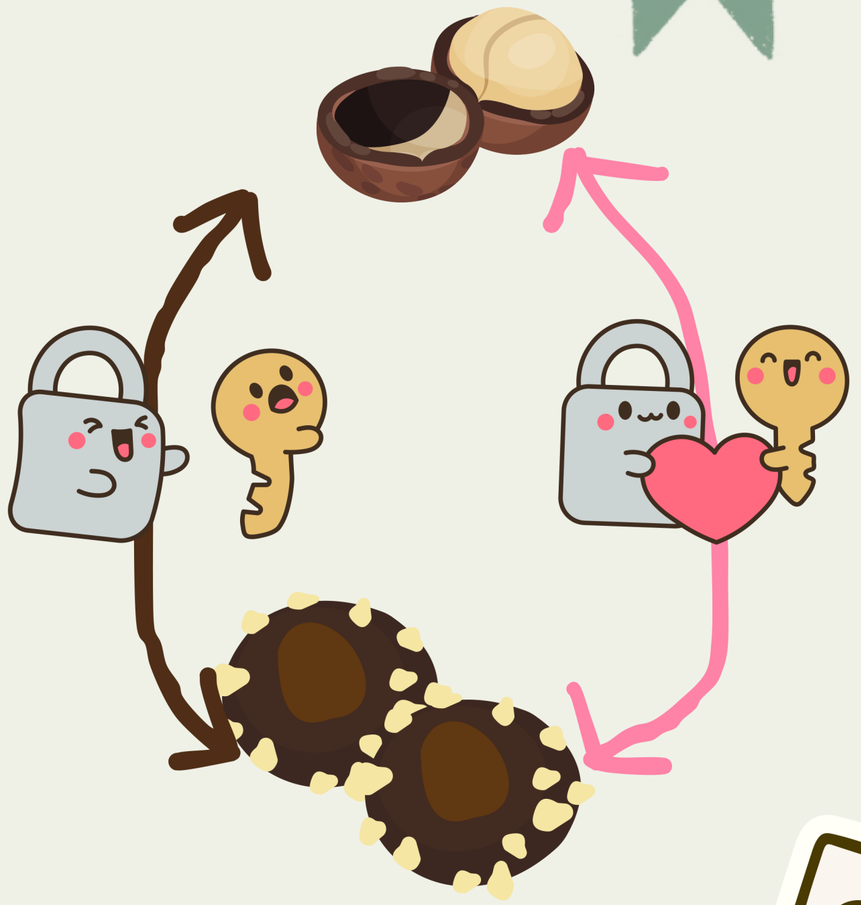


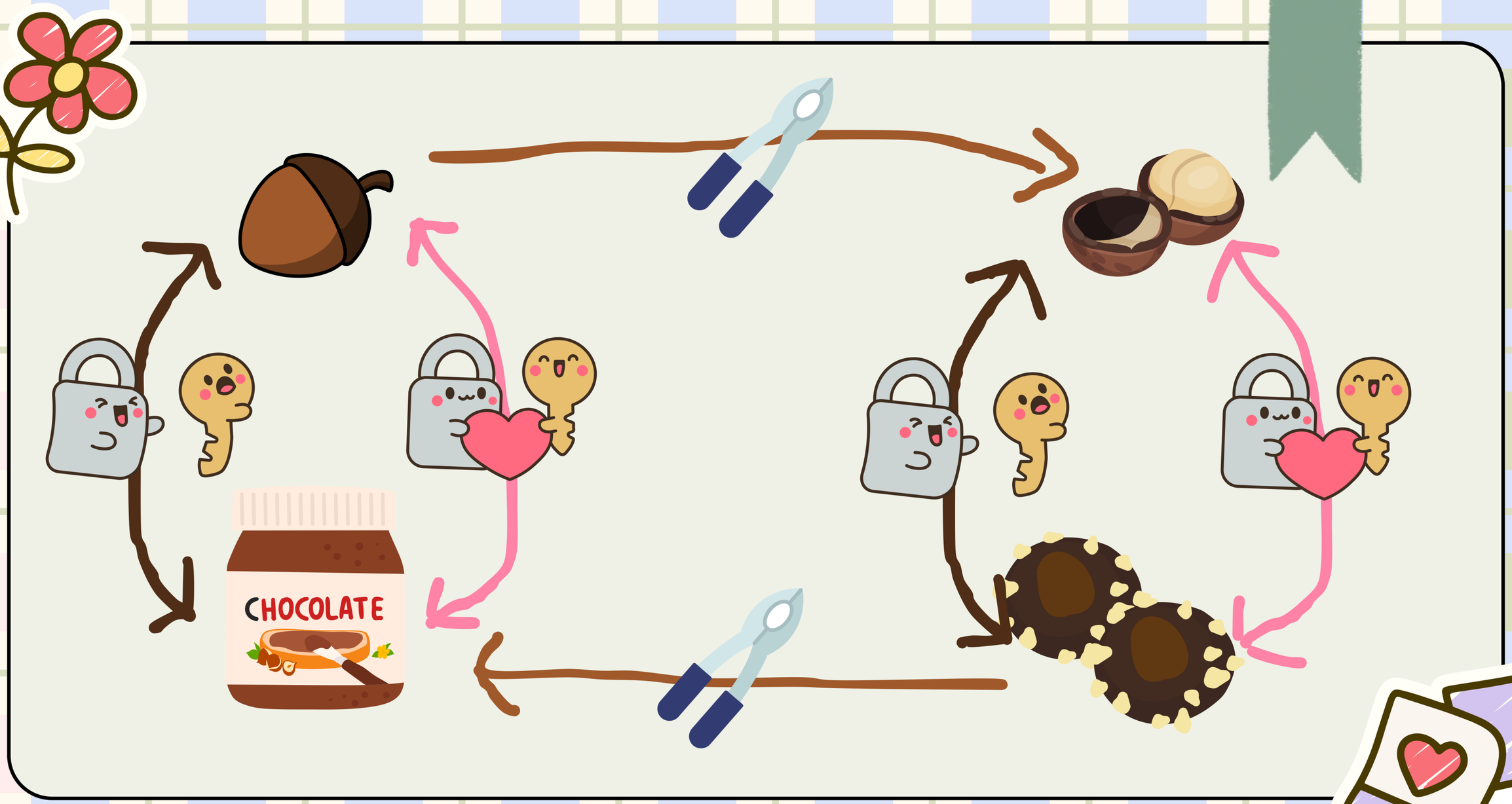
FULLY HOMOMORPHIC ENCRYPTION


CHOCOLATE




CHOCOLATE




CHOCOLATE

OVERVIEW

Currently there isn't any SoK in FHE+PIR.

The litature is very sparse on the implementations, costs and theory used. Therefore causing constant rereading and rework by reviewing implementations.

EXISTING WORK

These are the main works that focus in FHE-based PIR. They may vary in a few details:

- Amount of servers
- Stateful or Stateless
- Efficiency
- Computation

SealPIR

S. Angel, H. Chen, K. Laine, and S. T. V. Setty. PIR with compressed queries and amortized query processing. In 2018 IEEE Symposium on Security and Privacy, pages 962–979. IEEE Computer Society Press, May 2018.

XPIR

C. Aguilar Melchor, J. Barrier, L. Fousse, and M.-O. Killijian. XPIR: Private information retrieval for everyone. PoPETs, 2016(2):155–174, Apr. 2016

OnionPIR

M. H. Mughees, H. Chen, and L. Ren. Onionpir: Response efficient single-server pir. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21, page 2292–2306, New York, NY, USA, 2021. Association for Computing Machinery.

SHECS-PIR

J. Park and M. Tibouchi. SHECS-PIR: Somewhat homomorphic encryption-based compact and scalable private information retrieval. In L. Chen, N. Li, K. Liang, and S. A. Schneider, editors, ESORICS 2020, Part II, volume 12309 of LNCS, pages 86–106. Springer, Heidelberg, Sept. 2020

SPIRAL

S. J. Menon and D. J. Wu. SPIRAL: fast, high-rate single-server PIR via FHE composition. In 43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022, pages 930–947. IEEE, 2022.

FrodoPIR

Alex Davidson, Gon¸calo Pestana, and Sof´ıa Celi. Frodopir: Simple, scalable, single-server private information retrieval. Cryptology ePrint Archive, Paper 2022/981, 2022.

ChalametPIR

Sofía Celi and Alex Davidson. Call me by my name: Simple, practical private information retrieval for keyword queries. Cryptology ePrint Archive, Paper 2024/092, 2024

SECURITY ASSUMPTIONS

These are the current implementations we wish to underline and their implementation base.

Protocol	Security assumptions
SealPIR	LWE
XPIR	RLWE
OnionPIR	RLWE
SHECS-PIR	LWE
SPIRAL	RLWE
ChalametPIR	LWE
FrodoPIR	LWE

WORK IN PROGRESS

A comprehensive Systematization of Knowledge (SoK) helps synthesizes existing research, identifies gaps, and highlights new directions for investigation.

WORK IN PROGRESS

In this work we aim to approach the existing schemes that implements PIR protocols using FHE, with security being derived from LWE or RLWE.

THANK YOU!
GRACIAS!
OBRIGADA!