Riley Wong (they/them) • Principal, Emergent Research

Devcon 2024

Applications of Multi-Party Fully Homomorphic Encryption (MP-FHE) for Vulnerable Communities

How can cryptographic and privacy-preserving systems be built by and with vulnerable communities **most in need of privacy protections?**

How can cryptographic and privacy-preserving systems can enable **collective agency and consent?**

What is MP-FHE?

(Secure) Multi-Party Computation (MPC)

- Cryptographic framework that allows ***multiple parties*** to contribute data towards a ***joint computation*** while keeping their data ***private*** from each other

- May involve:
  - Garbled circuits
  - Verifiable secret sharing, e.g. Shamir's
  - SPDZ

- Pros:
  - Collective
  - Privacy-preserving
  - Opportunities for ***consent mechanisms*** with mathematical guarantees

- Cons:
  - Some protocols require multiple "rounds" of computation (back-and-forth)
  - Scales exponentially with parties

Fully Homomorphic Encryption (FHE)

- Cryptographic framework that allows for computations ***on encrypted data***
  - data stays encrypted at all times
  - third parties can run the computation and return outputs without ever seeing the data

- Pros:
  - Data security throughout the process, including computation as well as data in transit
  - Computations can be outsourced

- Cons:
  - 1,000 - 1,000,000x slower than equivalent plaintext operation

Multi-Party Fully Homomorphic Encryption (MP-FHE)

- Compute on ***encrypted data*** from ***multiple parties***
  - Ring-Learning-with-Errors (RLWE)

- Pros:
  - "Best of both worlds": Data security for multiple parties, including data in transit
- Cons:
  - Still in development, experimental
  - Very slow, not always practical for use cases, especially as the number of parties scales upward

What are useful, real-world applications of MP-FHE?

MP-FHE Applications

- Ideal for situations where:
  - Consequence, penalty, stigma, or retaliation for individuals
  - Meanwhile, ***collective power in numbers***

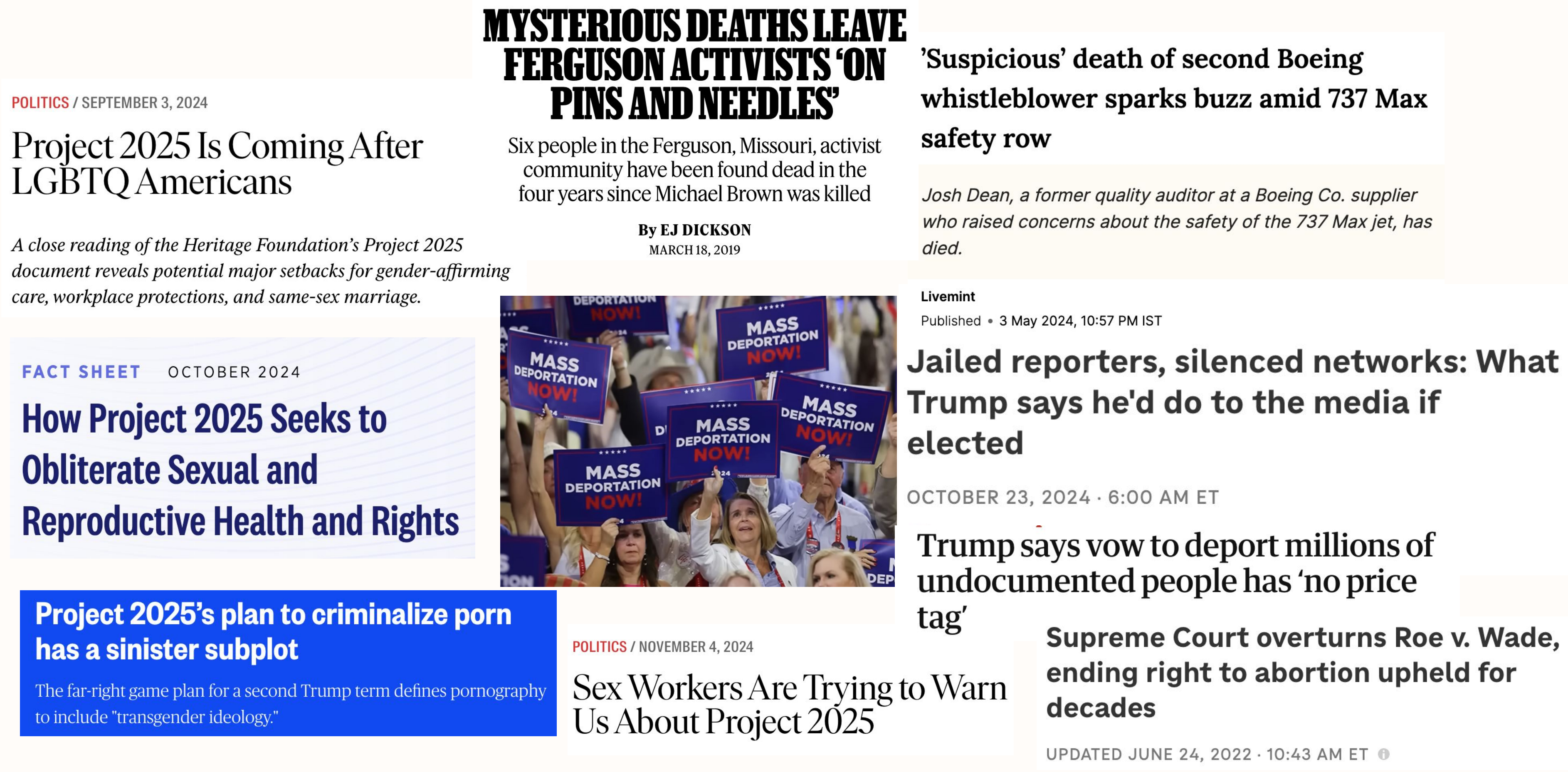
- Also ideal for coordinating “prisoner’s dilemma”-style situations

- ***Collective consent mechanisms*** for community governance

MP-FHE Applications

- Coordination
  - Labor organizing: can only succeed if threshold is met, otherwise potential risk or penalty
    - Unions
    - Protests
    - Strike pledges
  - Data strikes
    - Commitments to: delete accounts or data, mass unfollow, data poisoning, etc. (anti-surveillance)

- MP-FHE statistics for vulnerable communities:
  - Sex workers
  - Undocumented migrants
  - Abortion seekers
  - Transgender healthcare
  - Whistleblowers
  - Community organizers



POLITICS / SEPTEMBER 3, 2024

Project 2025 Is Coming After LGBTQ Americans

A close reading of the Heritage Foundation's Project 2025 document reveals potential major setbacks for gender-affirming care, workplace protections, and same-sex marriage.

FACT SHEET OCTOBER 2024

How Project 2025 Seeks to Obliterate Sexual and Reproductive Health and Rights

Project 2025's plan to criminalize porn has a sinister subplot

The far-right game plan for a second Trump term defines pornography to include "transgender ideology."

MYSTERIOUS DEATHS LEAVE FERGUSON ACTIVISTS 'ON PINS AND NEEDLES'

Six people in the Ferguson, Missouri, activist community have been found dead in the four years since Michael Brown was killed

By EJ DICKSON

MARCH 18, 2019

POLITICS / NOVEMBER 4, 2024

Sex Workers Are Trying to Warn Us About Project 2025

'Suspicious' death of second Boeing whistleblower sparks buzz amid 737 Max safety row

Josh Dean, a former quality auditor at a Boeing Co. supplier who raised concerns about the safety of the 737 Max jet, has died.

Livemint

Published • 3 May 2024, 10:57 PM IST

Jailed reporters, silenced networks: What Trump says he'd do to the media if elected

OCTOBER 23, 2024 · 6:00 AM ET

Trump says vow to deport millions of undocumented people has 'no price tag'

Supreme Court overturns Roe v. Wade, ending right to abortion upheld for decades

UPDATED JUNE 24, 2022 · 10:43 AM ET

How can privacy-preserving tools be designed in collaboration with communities **most in need of privacy protections?**

Participatory Co-Design

- designing ***by and with communities***
- identifying the specific needs, wants, challenges, and priorities for vulnerable populations in an intersectional, holistic, and interdependent way
- acknowledging that the process of building and implementing technology is inherently political

At what point can technical tools for privacy and cryptography help vulnerable communities, and at what point are the remaining challenges ***outside the scope of technology*?**

What ***cultural, social, legal***, and other infrastructural barriers exist, and how can they be addressed in tandem?

MP-FHE for Reporting Abuse

Community Tools: Reporting Abuse

- > ***1 in 3*** women have experienced rape, physical violence, or stalking by an intimate partner in their lifetime
- reporting abuse, intimate partner violence, and sexual assault comes with ***risks***:
  - possible retaliation or escalation of harm from the abuser
  - risks to physical and emotional safety
  - social stigma, victim blaming, not being believed
- vast majority of sexual assault (70%) and domestic violence cases (95%) are never reported
  - campus assaults: “over 90% of cases are committed by repeat offenders, who offend an average [of] 6 times before they graduate”

- Prior Work: Callisto Vault
  - Callisto: A cryptographic approach to detecting serial perpetrators of sexual misconduct
  - “encrypted platform designed to empower survivors of sexual assault”
  - Uses Shamir’s Secret Sharing, oblivious pseudo-random functions, symmetric encryption, and public key encryption
  - Paper from 2018

System Design

Sample flow for a cryptographic system using MP-FHE and ZK-email:

1. With ZK-email, submitter uses ***privacy-preserving verification*** tool s.t. identity is private.
2. Submitter submits a unique identifier of the perpetrator, such as through an institutional or community ***directory***, so that matches can be made with precision.
3. Using MP-FHE, system can ***match*** when multiple people have reported the same perpetrator. (Directory makes this match a simple integer equivalence check.)
4. Submitters can opt-in to be contacted by other survivors and make ***collective decision*** for next steps. Can also set thresholds for matching.

Technical Resources

- ZK-Email for privacy-preserving identity verification
- Phantom Zone: MP-FHE library, able to perform integer equivalence
  - haunted: boilerplate and backend for Phantom Zone.
- lattigo: lattice-based multiparty homomorphic encryption library in Go
- Both PZ and lattigo use Ring-Learning-With-Errors (RLWE)

- mpz: multi-party computation libraries written in Rust, from PSE
- awesome-mpc: compilation of libraries and tools for secure multi-party computation
- awesome-fhe: compilation of libraries and tools for fully homomorphic encryption (not necessarily multi-party)

Thank you!

emergentresearch.net/mpfhe-reporting

emergentresearch.net
riley@emergentresearch.net
Telegram: @rrriley / Signal: @ryw.42