On the splitting the current PSI paper into two papers:

* What is new in VOPA?

1. It’s secure
2. It’s in coefficient form
3. It uses a polynomial of particular/new structure
4. It uses the beacon or coin tossing protocol

* What is new in ZSPA? Not clear yet, I need to do literature review
* What is new in Arbiter protocol: Everything is new, and the Arbiter can be semi-honest
* What is new in the main multi-party fair PSI protocol?

1. Compared to eurocrypt’19 paper it is secure and does not leak any information
2. It’s fair and multi-party

* What is the main differences between the multi-party fair PSI and Eurocrypt’19?

1. It uses polynomials in coefficient forms
2. Uses the observation (i.e. the polynomial divisibility) for additional verification
3. Constructed a polynomial of particular structure in VOPA

To achieve efficiency, we use:

1. Hash tables
2. Merkel tree

* What tools used to make the protocol fair:

1. Smart contract
2. Deposit paradigm