Smart PSI:

Would the smart PSI have enough contribution if it’s put in a separate paper?

What contributions it would have?

1. We have to add at least two modifications to the fair PSI protocol:
   1. element encoding e||H(e)
   2. element encryption s=Enc(e)
   3. uses collusion counter contracts
   4. uses the commitment of the polynomials
   5. it requires an arbiter potentially semi-honest
   6. uses smart contract for verification
   7. reduces the rolle of the arbiter