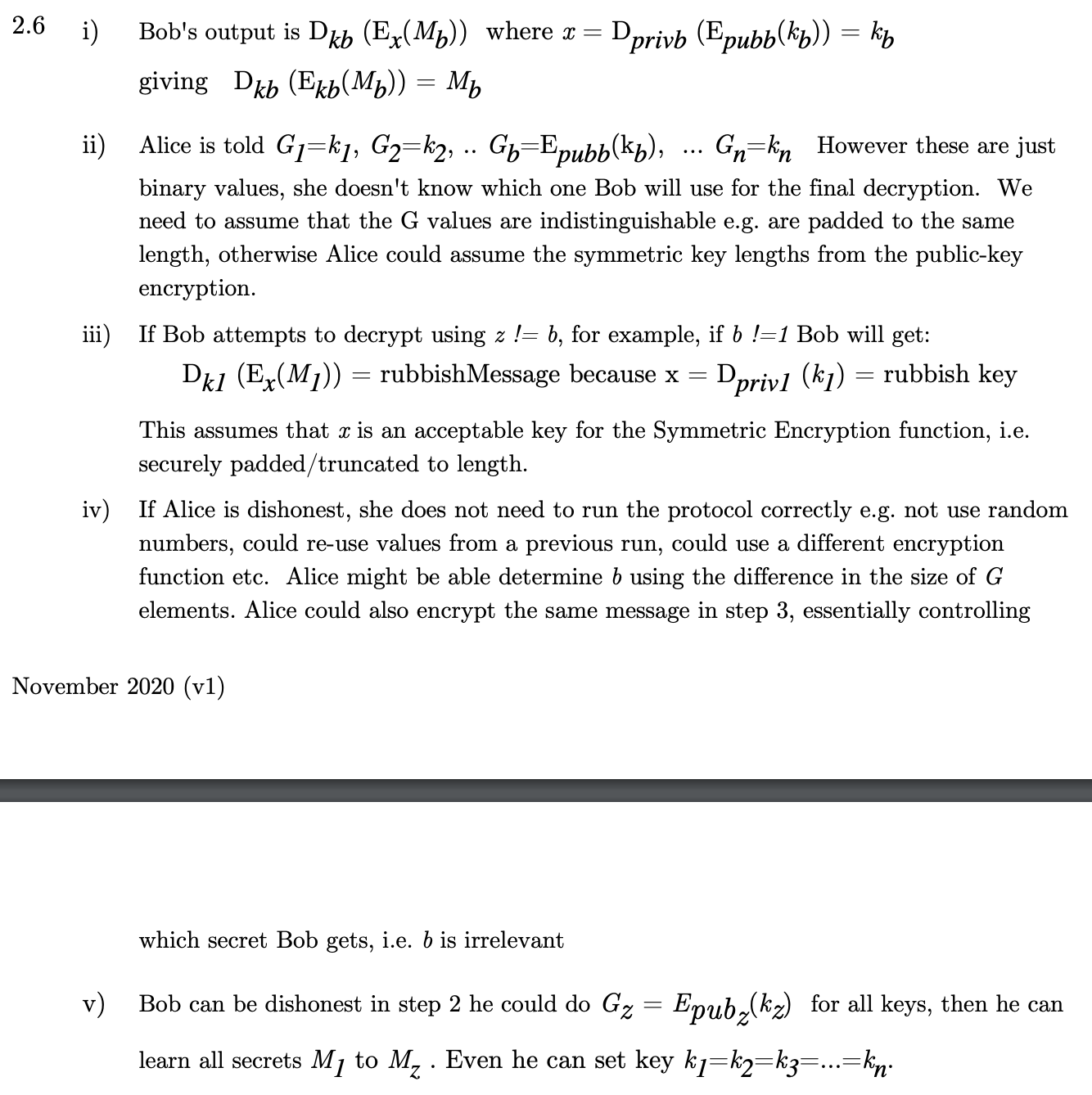
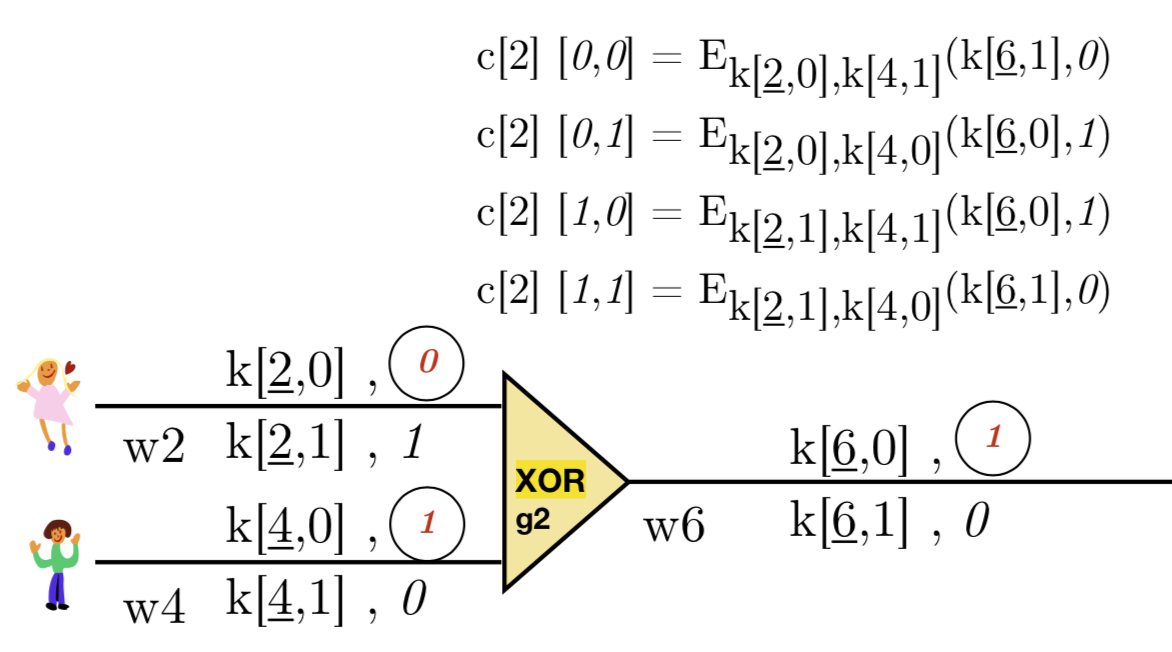
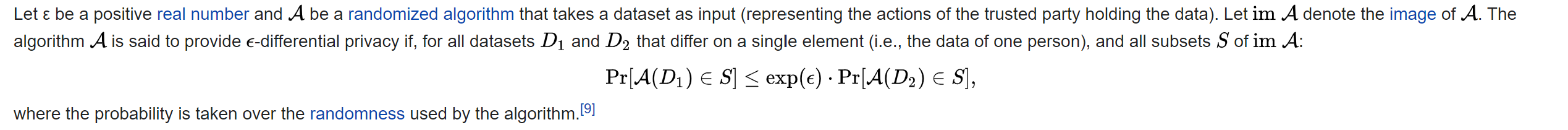
1. 1. It solves the problem of figuring out which of two parties is richer without disclosing either party’s actual wealth value. Not sure how to extend for equality.

Suggestion: To extend for equality we could adjust the algorithm so A only increments the value corresponding to it’s own worth.

We could also run the algorithm twice, where they swap roles, and then if a<=b and b<=a then a = b

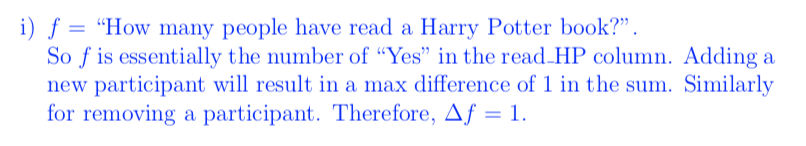
* 1. 
  2. The encrypted truth table is called garbled table. This is done such that one can decrypt the garbled table only if they have the correct two input labels.

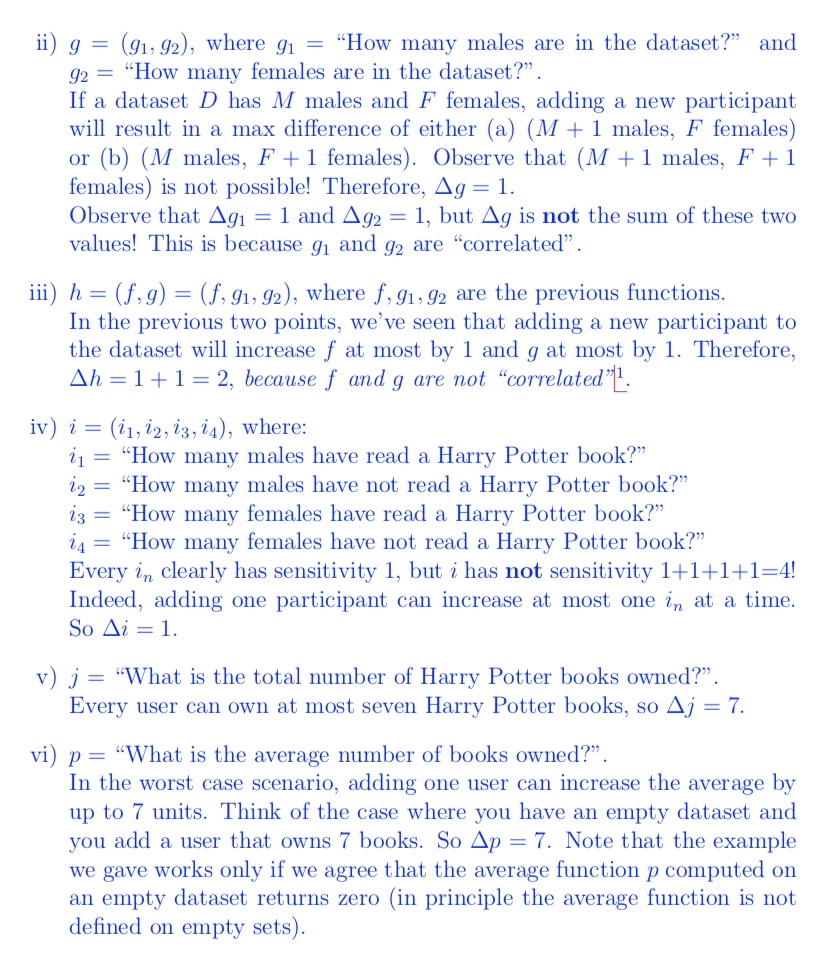


* 1. 
  2. Epsilon is a positive real number. The higher the value of epsilon used to more the probabilities can differ and the more information can potentially leak. We can think of epsilon as a privacy budget; giving the result of two ε-DP queries is the same as one 2ε-DP mechanism. ε ranges from 0 to 1.
  3. i) If the survey results say men are 50% more likely to smoke than women, then if you’re a man, the adversary knows you’re 50% more likely to smoke compared to a woman

ii) If everyone in a school took the survey, and you go to that school, then by definition they can reliably determine you took the survey







* 1. Just add Laplace noise?

f = set of datasets --> [0,100]  
f(D) = |D\_{grad=1}|/|D| \* 100 + lap(1/epsilon)

1. We didn’t learn about bitcoins