HA2

1

Correct. [1]. *(1.0)*

2

Think it's correct, couldn't find any reference to explicit secret sharing. But first answer is really just references to slides without explaining so I will deduct 0.2 points. *(0.8)*

3

Correct[2]. *(1.0)*

4

This seems reasonable. Don't want to disclose votes unnecessarily[3]. *(1.0)*

5

Correct, accurate with the lecture notes[4]. *(1.0)*

6

Correct, good explanation[5]. *(1.0)*

7

Correct. The votes will be summed without knowing what's inside so it's important that it's only -1 or 1[7]. *(1.0)*

8

Correct[**?**]. *(1.0)*

References

[1] `https://en.wikipedia.org/wiki/Zero-knowledge_proof#Definition`

[2] `https://en.wikipedia.org/wiki/Computational_hardness_assumption`

[3] Lecture Notes for Advanced Web Security 2017. Part 3 - Electronic Voting. Martin Hell, Section 4.1, Page 9

[4] Lecture Notes for Advanced Web Security 2017. Part 3 - Electronic Voting. Martin Hell, Section 4.2, Page 10

[5] Lecture Notes for Advanced Web Security 2017. Part 3 - Electronic Voting. Martin Hell, Section 4.3.1, Page 13

[6] Lecture Notes for Advanced Web Security 2017. Part 3 - Electronic Voting. Martin Hell, Section 4.3.2, Page 15

[7] Lecture Notes for Advanced Web Security 2017. Part 3 - Electronic Voting. Martin Hell, Section 4.1, Page 3