ETH Zurich, Department of Computer Science
SS 2020

Prof. Ueli Maurer
Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 13

13.1 Mining Pools

a) One can consider *mining pools*, where miners can jointly share their computing power to find a solution. For that, the mining pool has associated a public key pk, and the miners try to find a nonce satisfying $H(\mathsf{pk}, \mathsf{nonce}) < D$, for some difficulty level D. When a miner finds a solution, it sends the solution to a "manager" of the mining pool (can be a miner as well), who is in charge of submitting the solution and collecting the reward. The manager then shares the reward proportionally towards the miners according to their estimated computational power. In order to do estimate the computational power of each miner, each miner sends *partial* solutions to the manager. That is, for a difficulty level $D' < D$, the miners send partial solutions (nonce satisfying $H(\mathsf{pk}, \mathsf{nonce}) < D'$) to the manager, who uses such partial solutions to estimate the computing power of each miner.

b) Given α, β as fractions of the overall computing power, and a participant P with computing power β in a mining pool with joint computer $\alpha \geq \beta$, the expected revenue for P is $\frac{\beta}{\alpha} \cdot \alpha = \beta$. That is, P receives the same expected revenue as if it were mining alone. However, the risk is smaller because the mining pool receives α of the rewards, and P receives a fraction $\frac{\beta}{\alpha}$ every time the mining pool receives a reward.

c) Let m_1, m_2 be the mining power of the mining pools M_1, M_2, respectively. Moreover, let m be the overall mining power and x be the mining power that M_1 uses to perform the attack on M_2.

The direct revenue for solving solutions in the first mining pool M_1 is $R_1 = \frac{m_1 - x}{m - x}$, since the computing power mining for M_1 is $m_1 - x$, and the total mining computing power is $m - x$ (x of the mining power is not mining solutions). Similarly, the direct revenue for the second mining pool is $\frac{m_2}{m-x}$.

This means that the ratio of revenue per computing power unit in M_2 is $r_2 = \frac{R_2}{m_2 + x}$, since the revenue is distributed among all participants submitting partial solutions for M_2.

Moreover, the ratio in M_1 is $r_1 = \frac{R_1 + x r_2}{m_1}$, because the total revenue for participants in M_1 include the *share* obtained from the x computing power submitting partial solutions in M_2 as well. One can see that r_1 is maximized for some value $0 < x < m_1$ [Eya15].

Finally, the parties that are not in any of the mining pools and do not participate in any pool, obtain a ratio of $\frac{1}{m-x}$.

In conclusion, the parties in M_2 pay for everyone.

d) Let x_1 (resp. x_2) be the amount of computing power that M_1 (resp. M_2) uses to perform the withholding attack on M_2 (resp. M_1).

Following a similar analysis as above, one can compute $R_1 = \frac{m_1 - x_1}{m - x_1 - x_2}$, meaning that $r_1 = \frac{R_1 + x_1 r_2}{m_1 + x_2}$. Moreover, $R_2 = \frac{m_2 - x_2}{m - x_1 - x_2}$, meaning that $r_2 = \frac{R_2 + x_2 r_1}{m_2 + x_1}$.
One can investigate the above system of two equations for r_1 and r_2 as functions of x_1, x_2, m_1, m_2 and m, and arrive to the conclusion that both pools are better off attacking if the other pool doesn't attack (as seen in subtask c)), but if both attack, they end up worse than if none attacks [Eya15].

References

[Eya15] Ittay Eyal. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy*, pages 89–103. IEEE, 2015.