ETH Zurich, Department of Computer Science
SS 2019

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

# Cryptographic Protocols
# Solution to Exercise 5

## 5.1 Consensus: An Example

**a)** The tables look as follows:

**Scenario 1:**

| | $P_1$ | $P_2$ | $P_3$ | $P_4$ |
|---|---|---|---|---|
| Input | – | 1 | 1 | 0 |
| `WeakConsensus` | – | 1 | 1 | $\perp$ |
| `GradedConsensus` | – | $(1,1)$ | $(1,1)$ | $(1,0)$ |
| $\texttt{KingConsensus}_{P_1}$ | – | 1 | 1 | 0 |
| `WeakConsensus` | – | 1 | 1 | $\perp$ |
| `GradedConsensus` | – | $(1,1)$ | $(1,1)$ | $(1,0)$ |
| $\texttt{KingConsensus}_{P_2}$ | – | 1 | 1 | 1 |

**Scenario 2:**

| | $P_1$ | $P_2$ | $P_3$ | $P_4$ |
|---|---|---|---|---|
| Input | – | 1 | 1 | 1 |
| `WeakConsensus` | – | 1 | 1 | 1 |
| `GradedConsensus` | – | $(1,1)$ | $(1,1)$ | $(1,1)$ |
| $\texttt{KingConsensus}_{P_1}$ | – | 1 | 1 | 1 |
| `WeakConsensus` | – | 1 | 1 | 1 |
| `GradedConsensus` | – | $(1,1)$ | $(1,1)$ | $(1,1)$ |
| $\texttt{KingConsensus}_{P_2}$ | – | 1 | 1 | 1 |

**b)** **Scenario 1:** Yes, it is possible the honest players agree on the value 0. A possible strategy achieving this is the following: $P_1$ behaves as an honest player with input 0. It is easy to verify that in that case the output will be 0.

**Scenario 2:** No, it is not possible, as in this scenario we have PRE-AGREEMENT on 1, i.e., all honest players have input 1, in which case the PERSISTENCY ensures that all honest parties output 1.

**c)** If $P_4$ is corrupted, then every honest player has input 1. It follows from the PERSISTENCY that all players output 1.

If $P_4$ is honest, then the PERSISTENCY and the TERMINATION are trivial, and the CONSISTENCY follows from the KING CONSISTENCY property (as the king $P_4$ is honest).

## 5.2 Variations of `GradedConsensus`

**a)** Amélie's suggestion is bad—the resulting protocol does not achieve GRADED CONSENSUS. A concrete counterexample can be obtained in a similar setting as the Exercise 5.1. There, $n = 4$ and $P_1$ is corrupted. $P_2, P_3, P_4$ have inputs $1, 0, 0$, respectively. The strategy of $P_1$ is to send 1 to $P_2$ and 0 to the other parties during the weak consensus step. In the graded consensus step, it sends 1 to parties $P_2$ and $P_3$, and 0 to $P_4$. The following table contains the outputs of the parties after the graded consensus execution:

| | $P_1$ | $P_2$ | $P_3$ | $P_4$ |
|---|---|---|---|---|
| Input | – | 1 | 0 | 0 |
| `WeakConsensus` | – | $\perp$ | 0 | 0 |
| `GradedConsensus` | – | $(1,0)$ | $(1,0)$ | $(0,1)$ |

**b)** Cindy's protocol is well defined, as it is not possible that the conditions (#zeros $> t$) and (#ones $> t$) are satisfied at the same time: the WEAK CONSISTENCY property of WEAK CONSENSUS guarantees that no two honest players $P_i$ and $P_j$ decide on different values $z_i, z_j \in \{0, 1\}$.

Cindy's protocol achieves GRADED CONSENSUS. This can be seen as follows:

GRADED PERSISTENCY: If all honest players have the same input $x$, then every honest player receives the value $x$ (in Step 2) at least $n-t > t$ times and, therefore, decides on $(x, 1)$.

GRADED CONSISTENCY: Let $P_i$ and $P_j$ be honest and $g_i = 1$. Thus, $P_i$ received $y_i$ from at least $n - t$ players, i.e., at least $n - 2t$ honest players sent $y_i$ also to $P_j$. Hence, $P_j$ received $y_i$ at least $n - 2t > t$ times, which means that he decides on $y_j = y_i$.

TERMINATION: Obvious.

**c)** Hans's suggestion is bad—the resulting protocol does not achieve GRADED CONSENSUS. A concrete counterexample can be obtained as follows. The setting contains $n = 7$ parties, and $P_1$,$P_2$ are corrupted. $P_3, P_4, P_5, P_6, P_7$ have inputs $0, 0, 1, 1, 1$, respectively. The strategy of $P_1$ and $P_2$ is to send 1 to $P_6$ and $P_7$, and 0 to the other parties in both steps. The following table contains the outputs of the parties after the graded consensus execution:

| | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ | $P_7$ |
|---|---|---|---|---|---|---|---|
| Input | – | – | 0 | 0 | 1 | 1 | 1 |
| `WeakConsensus` | – | – | $\perp$ | $\perp$ | $\perp$ | 1 | 1 |
| `GradedConsensus` | – | – | $(0, 0)$ | $(0, 0)$ | $(0, 0)$ | $(1, 1)$ | $(1, 1)$ |

### 5.3 Two-Threshold Consensus

**a)** PERSISTENCY: Assume that at most $t_p$ parties are corrupted and honest parties have preagreement on a value $y$. This guarantees that each honest party obtains at least $n - t_p$ times the value $y$. Given that each party decides on $y$ if it obtains at least $n - t$ times the value $y$, we need that $n - t_p \geq n - t$, or $t_p \leq t$.

WEAK CONSISTENCY: Assume that $P_i$ outputs value $y_i \in \{0, 1\}$, hence it received $y_i$ from at least $n - t$ parties, from which at least $n - t - t_c$ are honest. Hence, each $P_j$ has received at least $n - t - t_c$ times the value $y_i$, and $1 - y_i$ at most $t + t_c$ times. So we need that $t + t_c < n - t$, or $2t + t_c < n$.

If we set $t = t_p$, both properties are achievable if $t_c + 2t_p < n$.

**b)** PERSISTENCY: Assume that at most $t_p$ parties are corrupted and honest parties have preagreement on a value $y$. From the PERSISTENCY of WEAK CONSENSUS, we have that every honest party $P_i$ sends $z_i = y$ at Step 2. At Step 3, we need that $n - t_p > t_p$ so that every honest party $P_i$ decides on $y_i = y$. Moreover, we need that every grade is 1, that is, that every honest party $P_i$ receives $y$ at least $n - t$ times. Hence, we need that that $t_p < \frac{n}{2}$, and $n - t_p \geq n - t$, which is $t_p \leq t$.

GRADED CONSISTENCY: Assume that at most $t_c$ parties are corrupted and an honest party $P_i$ outputs value $y_i \in \{0, 1\}$ with grade $g_i = 1$. We need to argue that no other honest party $P_j$ outputs on $1 - y_i$. In this case, $P_i$ received $y = y_i$ at least $n - t$ times. Hence, every other honest party $P_j$ received $y$ at least $n - t - t_c$ times after Step 2. Given the WEAK CONSISTENCY property, after Step 1, every honest party $P_j$ has a value $z_j \in \{y, \perp\}$. Hence, after Step 2 each $P_j$ receives at most $t_c$ values $1 - y$. The requirement we need is that $n - t - t_c > t_c$, or $2t_c + t < n$.

If we set $t = t_p$, both properties are achievable if $2t_c + t_p < n$ and $t_p < \frac{n}{2}$.