ETH Zurich, Department of Computer Science
SS 2018

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

Cryptographic Protocols
Solution to Exercise 11

11.1 Consensus: An Example

a) The tables looks a 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-property ensures that they all output the value 1.

c) If P_4 is corrupted, then every honest player has input 1. It follows from the persistency property that at the end all players output 1.

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

11.2 Variations of `GradedConsensus`

a) Amélie's suggestion is bad—the resulting protocol does not achieve GRADED CONSENSUS, as shown by the following counterexample: Let P_i and P_j be two honest players. Assume that P_i receives exactly $n-t$ zeros, in which case he will decide on $y_i = 0$ and $g_i = 1$. As t out of these $n-t$ players might be corrupted, it is possible that P_j receives less than $n-t$ zeros, in which case he decides for $y_j = 1$ (and $g_j = 0$). But this violates graded consistency.

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 `WeakConsensus` 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. Similarly to Amélies suggestion, it is possible that an honest player P_i decides on y_i with grade $g_i = 1$, while another player P_j decides on $y_j \neq y_i$: Assume that P_i receives exactly $k = \lfloor n/2 \rfloor + 1$ zeros, in which case he decides on $y_i = 0$ with grade $g_i = 1$. As t of these zeros might come from corrupted players, it is possible that P_j receives only $k - t$ zeros and t ones, and, as $k - t < t$, P_j will decide on $y_j = 1$.

11.3 Broadcast of Long Messages

a) If the sender P_s is honest, the same value x is sent to every party in Step 1. In Step 2, every honest party P_i sends $x_i = x$. This means that every party P_i receives x from at least $n - t$ parties. Hence, in Step 3 every honest P_i broadcasts a 1-bit. This implies $|\mathcal{M}| \geq n - t$. Because the majority of parties in $\mathcal{M}$ are honest ($N - t > t$), every honest P_i outputs value $y_i = x$ in Step 4.

b) Assume that $x_i \neq x_j$. Since $P_i \in \mathcal{M}$, he received x_i from at least $N - t$ parties. Hence, P_j received x_i from at least $N - 2t$ parties. This means, P_j received x_j from at most $2t < N - t$ parties, and hence, $P_j \notin \mathcal{M}$, which is a contradiction.

c) If $|\mathcal{M}| < n - t$, all honest parties output $\perp$.

Now consider the case $|\mathcal{M}| \geq N - t$. There are at least $N - 2t > t$ honest parties in $\mathcal{M}$ (there is a majority of honest parties in $\mathcal{M}$). We know from b) that $x_i = x_j$ for any honest $P_i, P_j \in \mathcal{M}$. Let us denote that value y. We have that every honest player P_i outputs the same value $y_i = y$, which corresponds to the value that is received most often from parties in $\mathcal{M}$.