Libsnark Exercise: Basic FinTech Gadgets

Chan Nam Ngo
channam.ngo@unitn.it
University of Trento, Trento, Italy

November 26, 2018

Zero-Knowledge Proof can be used for maintaining integrity in FinTech systems. Randomnesses for commitments are omitted for the sake of gadgets description. Students will implement the following gadgets. Consider also the following question: "Can the below two gadgets use the same implementation but with different usage?"

Table 1: Maintaining Interity with Relations 1

Purpose	**Statement**	**Witness**	**Conditions**
P_i updates correctly	$[c_i], [a_i], [c'_i], [a'_i], v, p$	c_i, a_i, c'_i, a'_i	$c'_i = c_i - v \cdot p$ and $a'_i = a_i + v$
P_j updates correctly	$[c_j], [a_j], [c'_j], [a'_j], v, p$	c_j, a_j, c'_j, a'_j	$c'_j = c_j + v \cdot p$ and $a'_j = a_j - v$

Let us assume that a sell offer indicates negative amount while a buy offer indicates positive amount. Students will implement the following gadget which combines the two "Can make a buy offer" and "Can make a sell offer" gadgets as one.

Table 2: Maintaining Interity with Relations 2

Statement	**Witness**	**Conditions**
$[c_i], [a_i], v, p$	c_i, a_i	$((v < 0) \wedge (v < a_i)) \vee ((v > 0) \wedge (c_i \geq v \cdot p))$

Sometimes in FinTech we can also encounter a gadget that implements a state machine. For instance the status flag of a trader in Futures Trading.

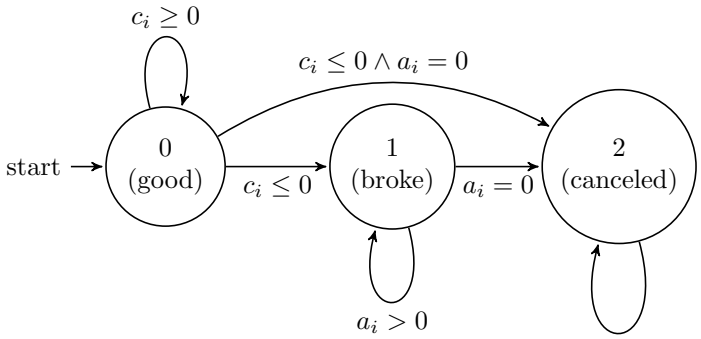

Table 3: Maintaining Interity with Relations 3

Statement	**Witness**	**Conditions**
$[c_i], [a_i], [f_i], [f_i']$	c_i, a_i, f_i, f_i'	See below.

The condition is as follows.

$$
\begin{aligned}
& f_i = 0 \wedge f_i' = 0 \wedge c_i \geq 0 \\
& \qquad \vee \\
& f_i = 0 \wedge f_i' = 1 \wedge c_i \leq 0 \\
& \qquad \vee \\
& f_i = 0 \wedge f_i' = 2 \wedge c_i \leq 0 \wedge a_i = 0 \\
& \qquad \vee \\
& f_i = 1 \wedge f_1' = 1 \wedge a_i > 0 \\
& \qquad \vee \\
& f_i = 1 \wedge f_i' = 2 \wedge a_i = 0 \\
& \qquad \vee \\
& f_i = 2 \wedge f_i' = 2
\end{aligned}
$$