0.1 Protocol BA' (= Dolev-Strong')

Nested Signatures When a user X digitally signs the digital signature of another user Y, $SIG_Y(m)$, the resulting string $SIG_X(SIG_Y(m))$ is a *level-2 nested signature*, by signers X and Y, of value m. Generalizing, if $X_k, \ldots, X_1$ are distinct users, then $s = SIG_{X_k}(\cdots(SIG_{X_1}(m)\cdots)$ is a *level-k nested signature*, by signers $X_1, \ldots, X_k$, of value m. Due to the retrievability property of digital signatures, anyone receiving s easily computes m. To highlight the first signer of s, we may refer to s as a (k, X_1)-*signature* of m.

A Classical Protocol in Our Notation. Except for the notation adopted and for the fact that messages are propagated in our network model, rather than sent to all players in a synchronous network, BA' coincides with the mentioned BA protocol of Dolev and Strong. Accordingly, the protocol is a slightly more specialized BA protocol, but perfectly adequate in our Algorand application. Namely, it makes use of digital signatures, and the initial value v_X of a player X is not an arbitrary value, but the value he has actually received from a distinguished player, *the leader*, ℓ. More precisely, prior to the start of the protocol, ℓ is supposed to have propagated $SIG_\ell(v)$.

Accordingly, "Step 0" is not technically part of BA'. (In our Algorand application, if BA' is indeed the chosen BA protocol, Step 0 has already been executed by the round-r leader, when protocol ROUND(r) calls the execution of the chosen BA protocol.)

Remark As for protocol ROUND(r), in describing BA' we omit to include, in each message m, a full specification of the "context" in which m is sent.[1]

For each player X, the set S_X is initially (reset to be) empty.

Protocol BA'

COMMUNICATION STEP 0. *For some value v, leader ℓ propagates $SIG_\ell(v)$.*

COMMUNICATION STEP i **(for $i = 1$ to $t+1$).** *For each player X:*

- *For each value $x \notin S_X$ for which, in Step $i-1$, he receives a (i, ℓ)-signature of x, by signers other than himself, X arbitrarily chooses one such signature, s, and propagates $SIG_X(s)$.*
- *For each (i, ℓ)-signature of a value x received in Step $i-1$, $S_X := S_X \cup \{x\}$.*

COMPUTATION STEP $t+2$. *For each player X:*

- *If S_X contains exactly one value, $S_X = \{x\}$, then X sets $OUT_X = x$.*
- *Else, X sets $OUT_X = \perp$.*