Byzantine Agreement Using Authentication

```
If I am P and own input is 1
    value :=1
    broadcast "P has 1"
else
    value := 0

In each round r ϵ 1...$f+1$:

If value = 0 and accepted r messages "P has 1" in total including a message
from P itself
    value := 1
    broadcast "P has 1" plus the r accepted messages that caused the
    local value to be set to 1

After f+1 rounds:

Decide value
```

In total r+1 authenticated "P has 1" messages

Randomized Algorithm

```
$x$ := own input; $r$ = 0
Broadcast proposal($x$, $r$)

In each round $r$ = 1,2,....:

Wait for $n-f$ proposals
If at least $n-2f$ proposals have some value $y$
      $x$ := $y$; decide on $y$
else if at least $n-4f$ proposals have some value $y$
      $x$ := $y$;
else
      choose $x$ randomly with P[$x$=0] = P[$x$=1] = ½
Broadcast proposal($x$, $r$)
If decided on a value → stop
```