A0 = MACKA( N || ACK )

A12 = A0  \oplus C0

Root commitment = A20 \oplus E11

E11

A20 = A11  \oplus A12

A20

A12

A11

A12 = A0  \oplus C0

Root commitment = A20 \oplus E11

E11

A20 = A11  \oplus A12

A20

A12

A11

A0 = MACKA( N || NACK )

Aggregation tree