E

1

2.
C
re

following properties:

QUALITY PROTOCOL

1. Verifier first computes the commitments

$$D=D_{n}^{2^{n}} \cdot D_{n-1}^{2^{n-1}} \cdot . . \cdot D_{0}$$

. Finally prover and verifier compute D^{-1} and the prover opens the result to eveal 0.

the prover P puts an integer a into a closed box, where $0 \leq a < q$ for some fixed prime q and gives it to the verifier V .

At this point, V cannot open the box, and P cannot change his mind about a.
However, P may later choose to open a box and reveal the contents to V.

Following Properties

1. From commitment A containing a, resp. B containing b,

V can on his own compute a commitment containing $a+b \bmod q$,

$a-b \bmod q$.

Commitments are in a multiplicative group, denote these commitments by

$A \cdot B$, resp. AB^{-1} .

Implies that V can **multiply** or **add** constants into a commitment. We will let

A^c , cA, cA^{-1} denote commitments to ca, $c+a$, $c-a \bmod q$, as computed

from A.

2. P can convince V in honest verifier zeroknowledge that a given

commitment is a *bit commitment*,

i.e. P knows how to open it to reveal 0 or 1.

3. P can convince V in honest verifier zero knowledge that how to open a set of given **commitments** A, B, C to reveal values a, b, c, for which $c = ab \bmod q$.

In particular, P can show that he knows how to open a **single commitment** A

(by choosing $C = A$ and B a default commitment to 1).

EQ

1. t
C =
wh
bin
2. F
ope

UALITY PROTOCOL

he verifier first computes the commitments
$= C_n^{2^n} \cdot C_{n-1}^{2^{n-1}} \cdot \ldots \cdot C_0$, and $D = D_n^{2^n} \cdot D_{n-1}^{2^{n-1}} \cdot \ldots \cdot D_0$
ich should both be commitments to the number whose
ary representation is $b_n b_{n-1} \ldots b_0$.
Finally prover and verifier compute CD^{-1} and the prover
ens the result to reveal 0 .

assume that a prover P will be generating commitments and sending them to a verifier V

unconditionally binding scheme

One finds that in each **round** of the protocol,
the prover sends the coefficients of some polynomial,
the verifier checks this polynomial, and returns a random element in th
The operations done by the verifier in order to check the polynomials r

Categories

1. Evaluate a po

ne field.
received all fall in one of the following categories: