**Mk**

*π2*

**V1**

**V2**

**V3**

**…**

**Vn**

**M2**

**M1**

*π1*

*…*



*Bulletin Board*

**C­1**

**C2**

**C’­1**

**C’2**

Sj

**C­ij-1**

**C2**

**Cmj+1**

**C2**

**C­kj**

**C2**

**Sj+1**

**Sj**

**Proof of knowledge of Paillier plaintext:**

**I know m st. c=gmrn mod n2**

Prover

Verifier

*Pass if*

*grcewn = u*

*Challenge: e random*

*Offer: u🡨gt sn mod n2 where t, s random*

*Response :*

*v🡨x-em*

*w🡨sr-eg(x-em) div n*

*If g1s=y1h1c and g2s=y2h2c then*

*accept*

*else*

*reject*

*Response : s = t+cx mod q*

*Challenge: c 🡨R Zq*

*Offer: y1= g1t, y2= g2t where t 🡨R Zq*

Prover

Verifier

**Chaum-Pedersen Protocol:**

**I know x st. h1=g1x and h2=g2x**

**Schnorr Protocol: I know x st h=gx**

*If gs=yhc then accept,*

*else reject*

*Offer: y=gt where t 🡨R Zq*

*Challenge: c 🡨R Zq*

*Response : s = t+cx mod q*

Verifier

Prover