

Cryptography w/ certified deletion

Bartusek, Khurana

922

(rough notes)

Warmup: Secret sharing w/ certified deletion

story: We construct a 2-out-of-2 secret sharing

Setup:

dealer: Alice

wants to share a bit b

b/w two parties

Bob

Charlie

s.t.

(1) (Secret sharing). Individual views of Bob & Charlie,
perfectly hide b
while

• Joint views of Bob & Charlie
can be used to
reconstruct b .

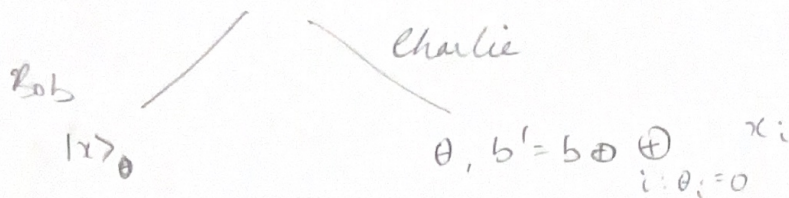
(2) (Certified Deletion). Bob may generate a certificate for Alice
guaranteeing that
 b has been information theoretically
removed from the joint view of Bob & Charlie.

Alice:

Scheme:
[BK22]

$$x \leftarrow \{0,1\}^\lambda$$

$$b \leftarrow \{0,1\}^\lambda$$



Story: Bob holds a quantum state — (a BB84 state in fact)
Charlie holds the basis info &
the bit b masked by the bits x
(of the quantum state) encoded in the
standard basis

To issue a deletion certificate: Bob measures all his qubits in the Hadamard basis, returns x'
Alice checks results match, i.e. $x'_i = x_i$, whenever $\theta_i = 1$.

Claim: This scheme satisfies the two requirements.

Intuition: (1) Secret sharing: Bob has no info about b by def.

Alice holds b padded by random bits

So neither can individually learn b .

But together, clearly, they can.

(2) Certified deletion: If Bob produces a certificate w/o communicating w/ Charlie, then w.p. $1 - \text{negl}$, he must have measured almost all his qubits in Hadamard & in that case, info about x_i on

Exp_b

Challenger

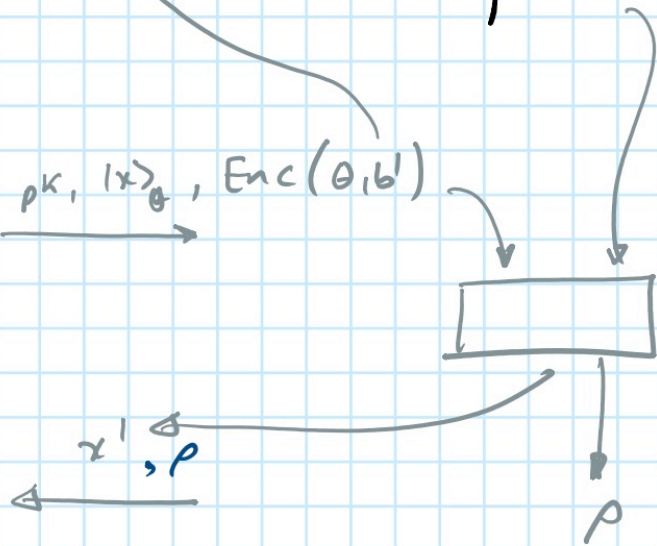
$pk, sk \leftarrow \text{Gen}(1^k)$

$b' = b \oplus \text{parity}_{\theta=0}(x)$

$pk, 1x\rangle_{\theta}, \text{Enc}(\theta, b')$

recall: $b' = b \oplus \text{parity}_{\theta=0}(x)$

Adversary (σ)



if $\exists i, \text{ s.t. } \theta_i = 1, \left[\begin{array}{l} x_i = x_i \end{array} \right]$ then output p

else

output \perp .

Claim: Output of $\text{Exp}_0 \approx_{\text{TD}} \text{Exp}_1$