How To Certifiably Delete Secrets

ENCRYPTION (WITH DELETION)

$\text{Encrypt}_{pk}(b) \longrightarrow ct = \underbrace{|ct_1\rangle, ct_2}_{\text{ciphertext}}, vk$

$\text{Decrypt}_{sk}(|ct\rangle) \longrightarrow b$

ADDITIONALLY

$\text{Delete}(|ct\rangle) \longrightarrow \nu$

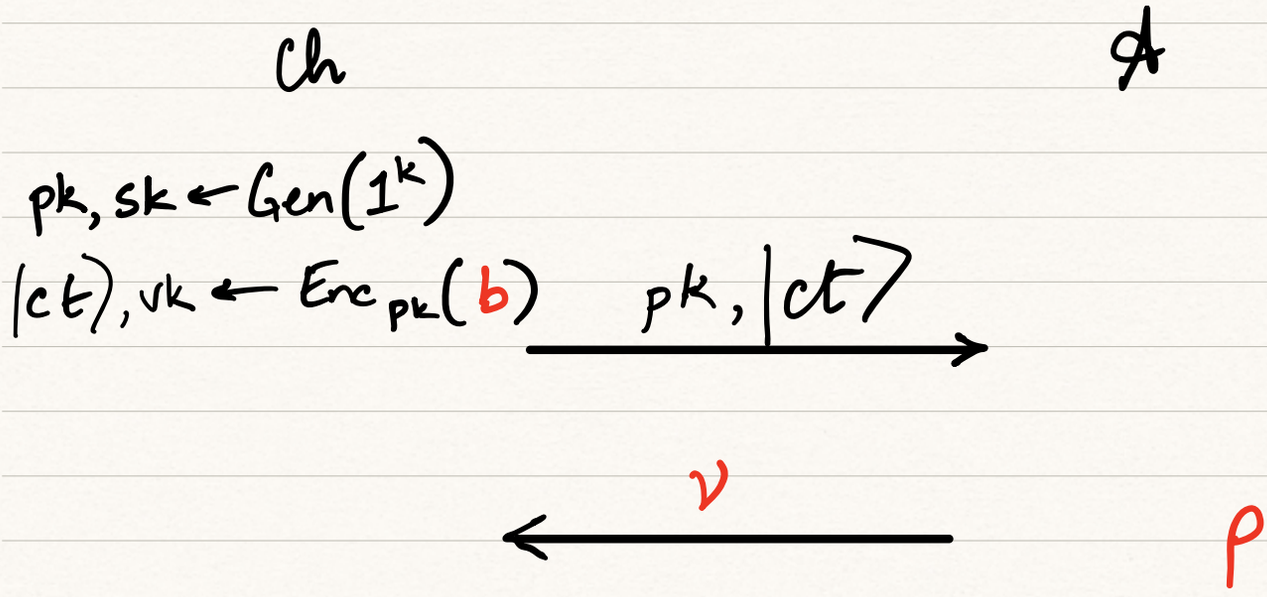
$\text{Ver}(\nu, vk) \longrightarrow \top / \bot$

Certified-Deletion-Security (INFORMAL):

As long as $\mathcal{A}$ is PPT-bounded at the time of generating deletion certificate ν, then verification of ν implies that b is information-theoretically removed from $\mathcal{A}$'s view.

$\text{Expmt}_b(1^k)$

(EVERLASTING)
[Bartusek - Khurana '22]



If ν verifies, output ρ

Else, output $\perp$

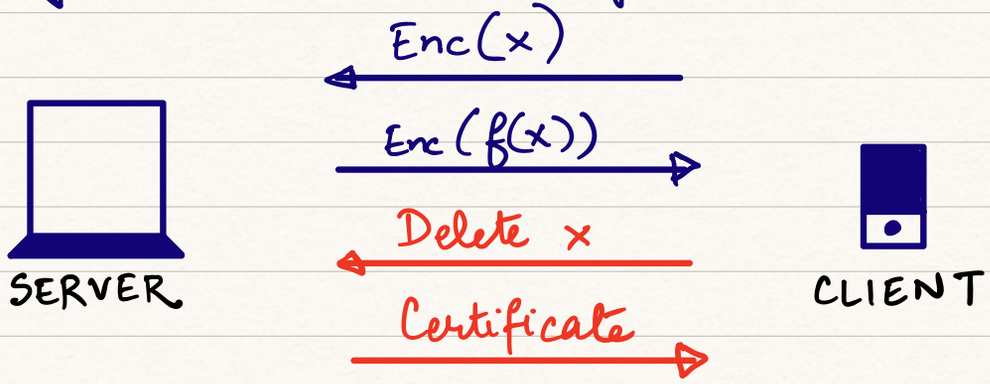
Certified-Deletion-Security (formal)

$$TD(\text{Expmt}_0, \text{Expmt}_1) = \text{negl}(k)$$

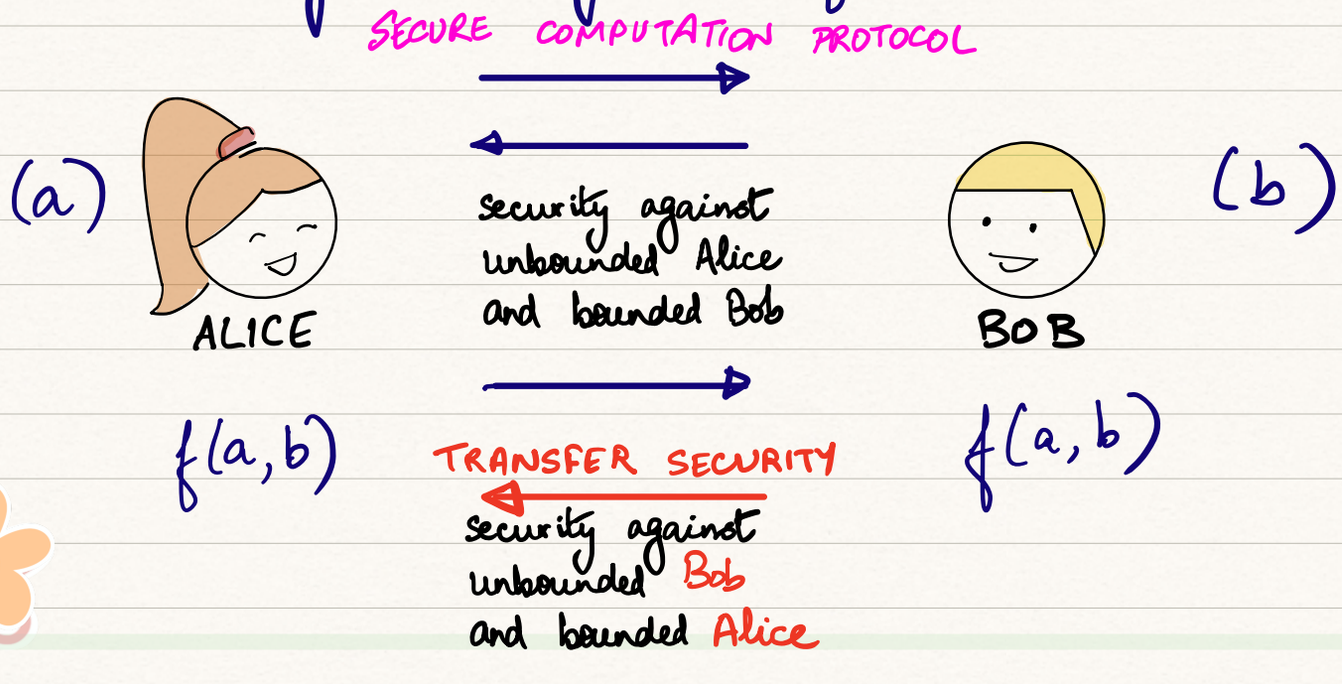
APPLICATIONS

X $\Rightarrow$ X with certified deletion, for X in

* Commitments (applications to ZK)
* Revocable time-lock encryption / puzzles
* Attribute-based encryption (ABE)
* Witness encryption
* Fully homomorphic encryption



* Everlasting Security Transfer



This talk will primarily describe the technique of Bartusek - Khurana '23.

OTHER PRIOR & RELATED WORKS:

Unruh '14: Time-lock puzzles

Broadbent - Islam '20: "Certified Deletion"

One-time pads with certified deletion

Hiroka - Morimae - Nishimaki - Yamakawa '21:

Public-key, attribute-based encryption

(assuming non-committing encryption)

leakage-style definition, ~~FHE~~

Hiroka - Morimae - Nishimaki - Yamakawa' 22:

Certified everlasting zero-knowledge for QMA

statistical soundness, SZK after deletion

Poremba '22:

Proofs of Deletion for Learning with Errors

FHE with CD under conjecture

Hiroka - Morimae - Nishimaki - Yamakawa '22:

Certified everlasting functional Encryption

quantum certificates

BACKGROUND

BB84 / Wiesner states

$|0\rangle$, $|1\rangle$: Computational basis states

+

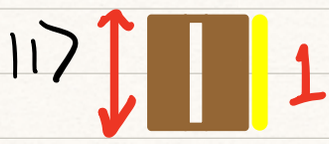
$\propto |0\rangle+|1\rangle$ $\propto |0\rangle-|1\rangle$

$|+\rangle$, $|-\rangle$: Hadamard basis states

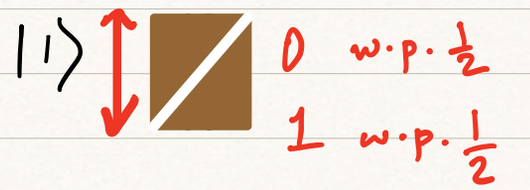
×

$|x\rangle_\theta$: $|x\rangle$ if $\theta=0$, $\frac{|0\rangle+(-1)^x|1\rangle}{\sqrt{2}}$ if $\theta=1$

COMPUTATIONAL BASIS MEASUREMENT



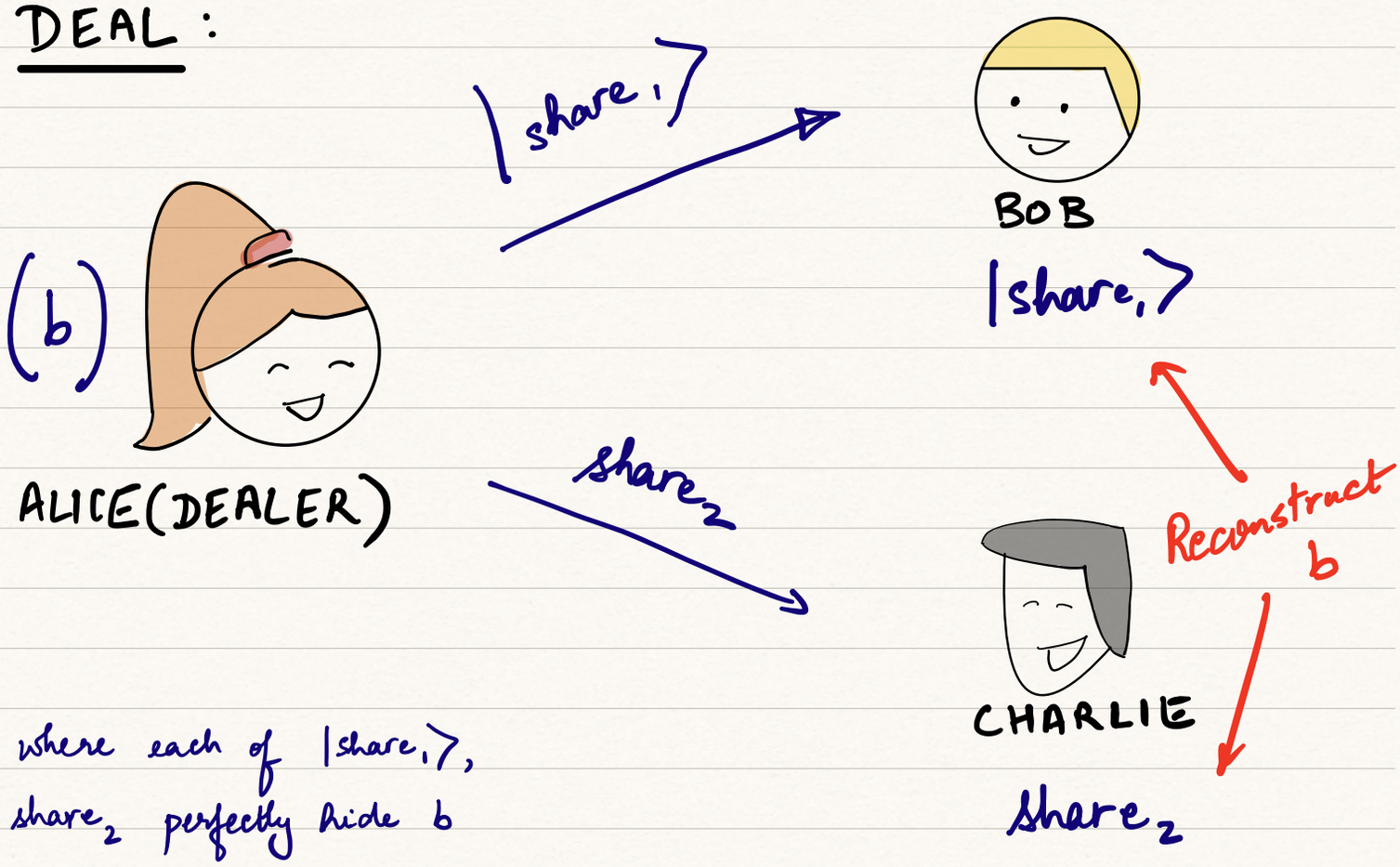
HADAMARD BASIS MEASUREMENT



Before going all the way to encryption,

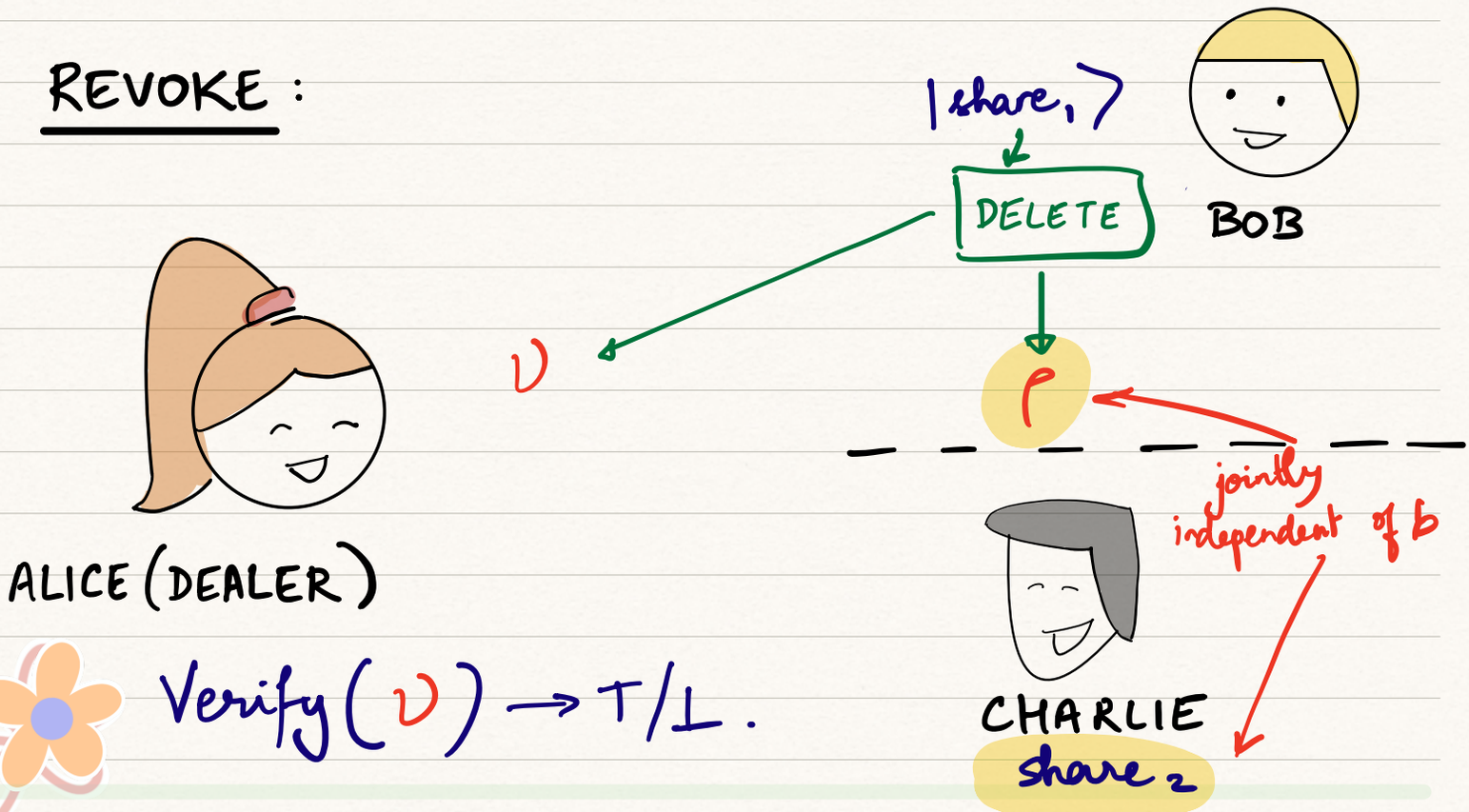
REVOCABLE SECRET - SHARING

DEAL :



where each of $|share_1\rangle$, $share_2$ perfectly hide b

REVOKE :

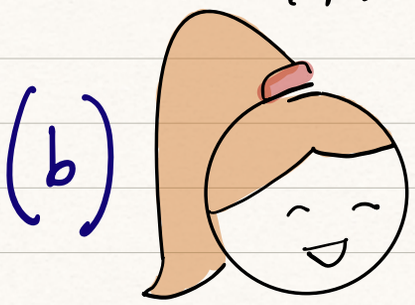


Verify(V) → T/⊥.

REVOCABLE SECRET - SHARING

DEAL :

$x \xleftarrow{\$} \{0,1\}^n$
$\theta \xleftarrow{\$} \{0,1\}^n$



ALICE (DEALER)

$|x\rangle_\theta = \{|x_i\rangle_{\theta_i}\}_{i \in [n]}$

BOB

θ, $b \oplus parity(x)$

CHARLIE

REVOKE :

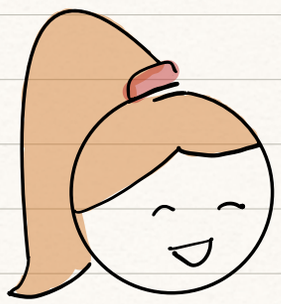
$|x\rangle_\theta$ = 

HADAMARD BASIS MSRMT.

BOB

ν = Measurement outcomes in Had. basis

ρ Deletes x



ALICE (DEALER)

$x_i \ \forall i$ s.t. θ_i = Hadamard

CHARLIE

$(\theta, b \oplus parity(x))$

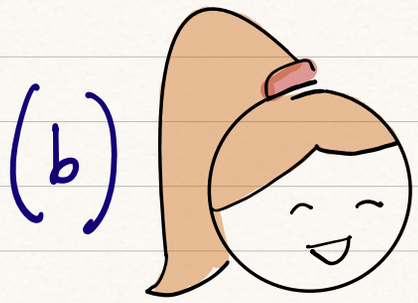
Ver(ν): $\forall i$ s.t. θ_i = Hadamard, $x_i = \nu_i$

ENCRYPTION with certified deletion

can be obtained from secret-sharing by encrypting one share.

ENCRYPT_{pk}

~~DEAL~~:



(b)

ALICE

(x, θ)

$|x\rangle_\theta$ (Bob's share)

$\text{Enc}_{pk}(\theta, b')$ (Charlie's share)

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

DELETE:

Adversary holds $|x\rangle_\theta$, $\text{Enc}(\theta, b')$

Can delete as before. $|x\rangle_\theta$

HADAMARD BASIS MSMT

x'

ρ, $\text{Enc}(\theta, b')$

VERIFY: If $\forall i$ s.t. $\theta_i = H$, $x_i = x_i'$, then $\top$ else $\bot$.

ENCRYPTION (WITH DELETION)

$\text{Encrypt}_{pk}(b) \longrightarrow ct = |ct_1\rangle, ct_2$

$|ct_1\rangle = |x\rangle_\theta$ for $x, \theta \leftarrow \{0,1\}^k$

$ct_2 = \text{Enc}(\theta), \text{Enc}(b \oplus \text{parity}_{\theta=0}(x))$

$\text{Decrypt}_{sk}(ct) \longrightarrow m$

- $ct = |ct_1\rangle, ct_2$. $\text{Dec}_{sk}(ct_2) \rightarrow \theta, b'$
- Measure $|ct_1\rangle$ in basis θ to obtain x
- Output $b = b' \oplus \text{parity}_{\theta=0}(x)$

$\text{Delete}(ct) \longrightarrow \nu$

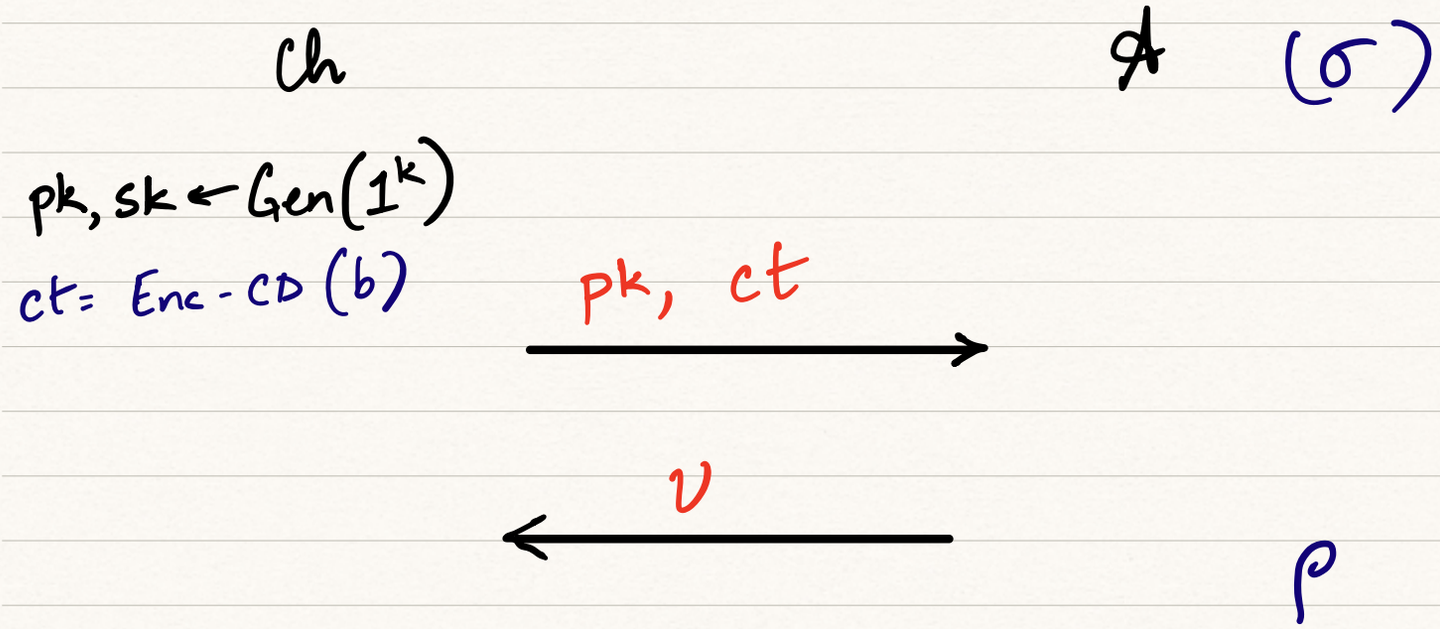
- $ct = |ct_1\rangle, ct_2$.
- Measure $|ct_1\rangle$ in Hadamard basis to output ν

$\text{Ver}(\nu, \overrightarrow{vk}) \longrightarrow T / \perp$ $\quad \overrightarrow{vk} = (x, \theta)$

Output T iff. $\forall\, i$ s.t. $\theta_i = 1$, $x_i = \nu_i$

RECALL: CERTIFIED DELETION SECURITY MEANS:

$\underline{\text{Expmt}_b(1^k)}$



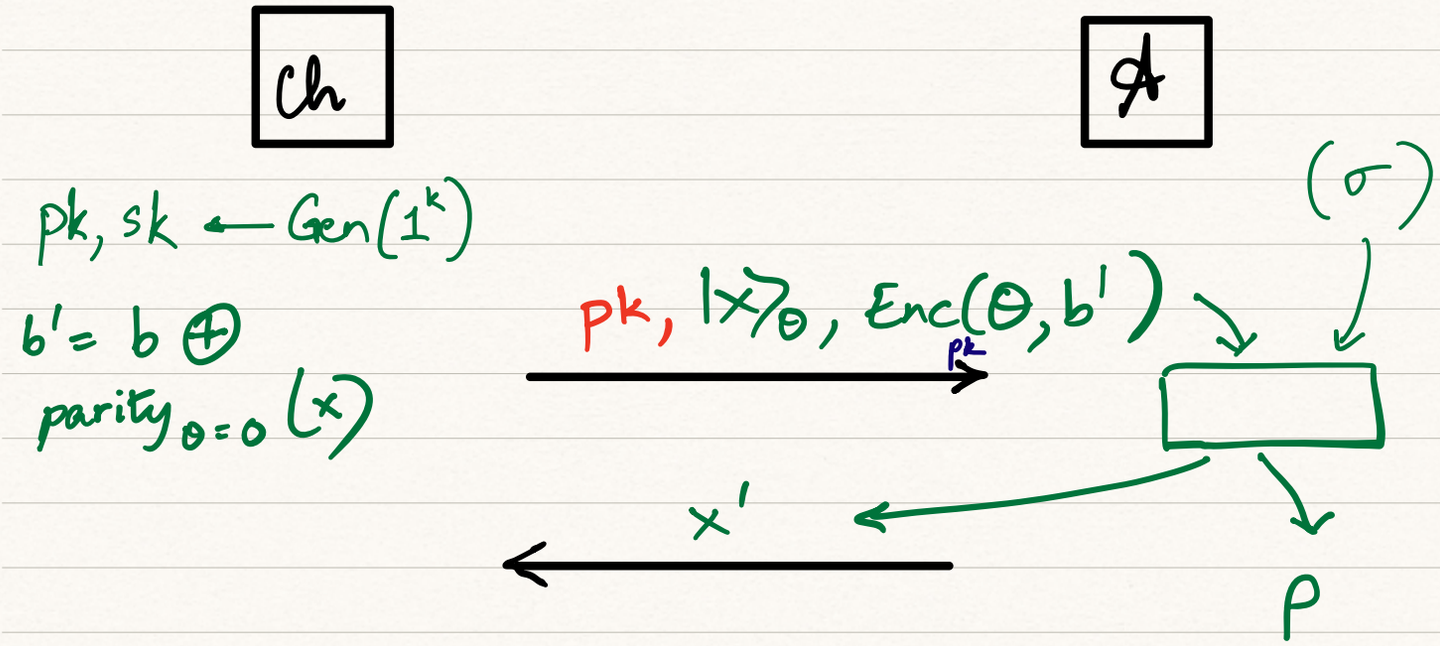
If v verifies, output ρ

Else, output $\perp$

$\underline{\text{Certified-Deletion-Security (formal)}}$

$$TD(\text{Expmt}_0, \text{Expmt}_1) = \text{negl}(k)$$

$\text{Expmt}_b(1^k)$



If $\forall i$ s.t. $\theta_i = 1$, $x_i = x'_i$, output ρ

Else, output $\perp$

Certified-Deletion-Security (formal)

$$TD(\text{Expmt}_0, \text{Expmt}_1) = \text{negl}(k)$$

How should we prove this?

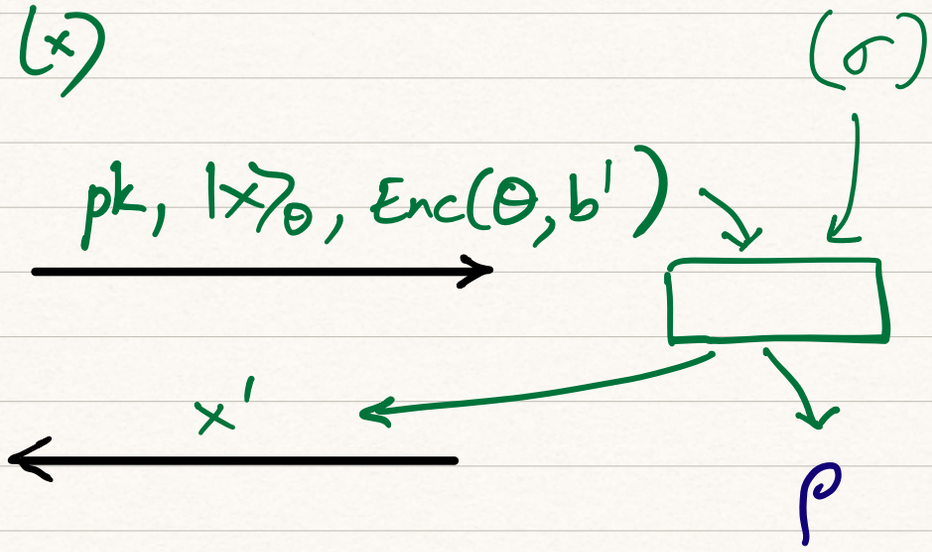
NOTE: b was in A's view before deletion, yet prove it was removed

$\text{Expmt}^{1}_{b}(1^k)$ (defer dependence on b)

$\tilde{b} \xleftarrow{\$} \{0,1\}$

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

$b' = \tilde{b} \oplus parity_{\theta=0}(x)$



If $\tilde{b} = b$,

If $\forall i$ s.t. $\theta_i = 1$, $x_i = x'_i$, output ρ

Else, output $\perp$

If $\tilde{b} \neq b$, output $\perp$.

It suffices to prove that:

$$TD(\text{Expmt}^{1}_{0}, \text{Expmt}^{1}_{1}) = negl(k)$$

[In particular, $TD(\text{Expmt}^{1}_{0}, \text{Expmt}^{1}_{1}) = \frac{TD(\text{Expmt}_0, \text{Expmt}_1)}{2}$

$\text{Expmt}_b^2(1^k)$

(purify the experiment)

Ch | A

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

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ on $\{A_i, B_i\}_{i \in [k]}$

$b' \xleftarrow{\$} \{0,1\}$

(σ)

if unbounded, find θ.

$pk, B, Enc(\theta, b')$ →

x' ←

A_i : Hadamard basis registers. → computational basis ρ

Measure A_i in basis θ_i to get x_i.

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

If $\tilde{b} \neq b$, abort. Else,

If $\forall i$ s.t. $\theta_i = 1$, $x_i = x'_i$, output ρ

Else, output $\perp$

It suffices to prove that:

$$TD(\text{Expmt}_0^2, \text{Expmt}_1^2) = negl(k)$$

$\text{Expmt}_b^3(1^k)$

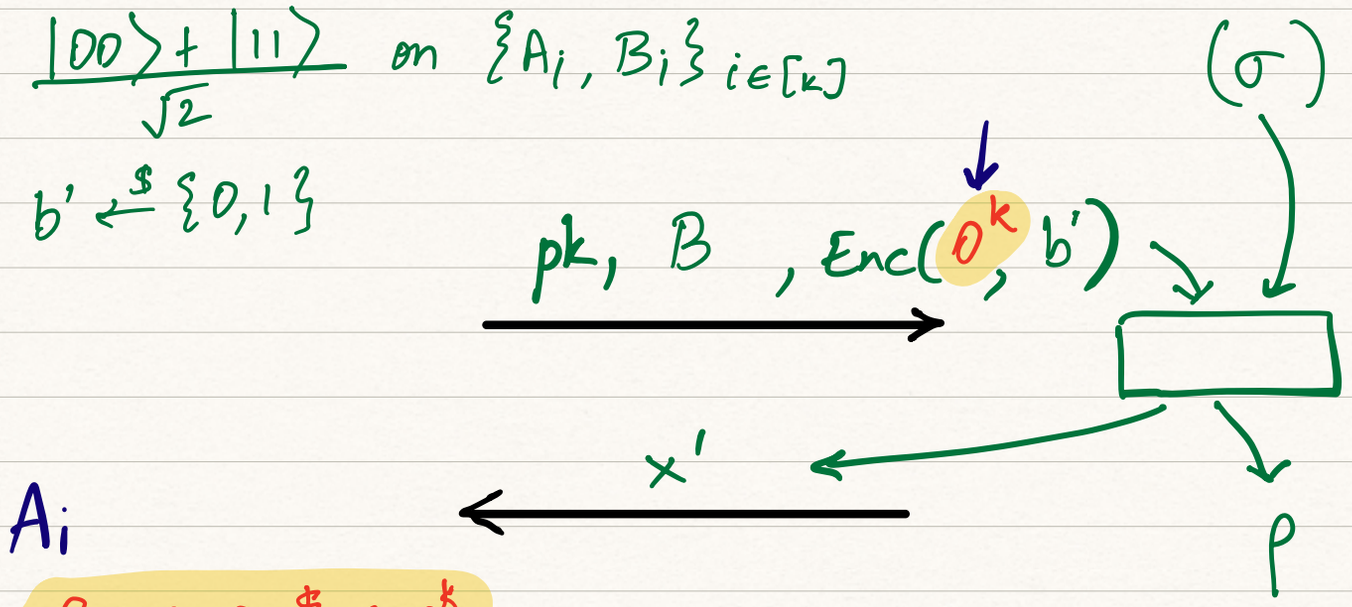
(encrypt garbage | zeroes)

Ch | A

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

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ on $\{A_i, B_i\}_{i \in [k]}$

$b' \xleftarrow{\$} \{0,1\}$



Sample $\theta \xleftarrow{\$} \{0,1\}^k$

Measure A_i in basis θ_i to obtain x_i

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

If $\tilde{b} \neq b$, abort. Else,

If $\forall i$ s.t. $\theta_i = 1$, $x_i = x'_i$, output ρ

Else, output $\perp$

(We will now take a quick detour...)

SAMPLE - AND - ESTIMATE

[Bouman - Fehr 2010]

Challenger

Sample EPR pairs

A_1	A_2	A_3	A_4	...	A_n
B_1	B_2	B_3	B_4		B_n

A_1	A_2	A_3	A_4	...	A_n

Adversary

B_1	B_2	B_3	B_4	...	B_n

Claimed measurements

$+ \quad - \quad + \quad + \quad \ldots$

$x_1' \quad x_2' \quad x_3' \quad x_4' \quad \ldots \quad x_n'$

in Hadamard basis

Sample $S \subset [n]$, $|S| = n/2$.

$\forall\, i \in S$,
measure A_i in Hadamard basis
to obtain x_i
check $x_i = x_i'$

Then w.h.p. $\forall\, i \in \bar{S}$,

A_i is "close to" $|x_i'\rangle_H$

$$\sum_{\Delta(y,x')<cn} |y\rangle\langle y|_H$$

Projection onto
succeeds w.p. $1 - \text{negl}(\kappa)$.

RECALL:

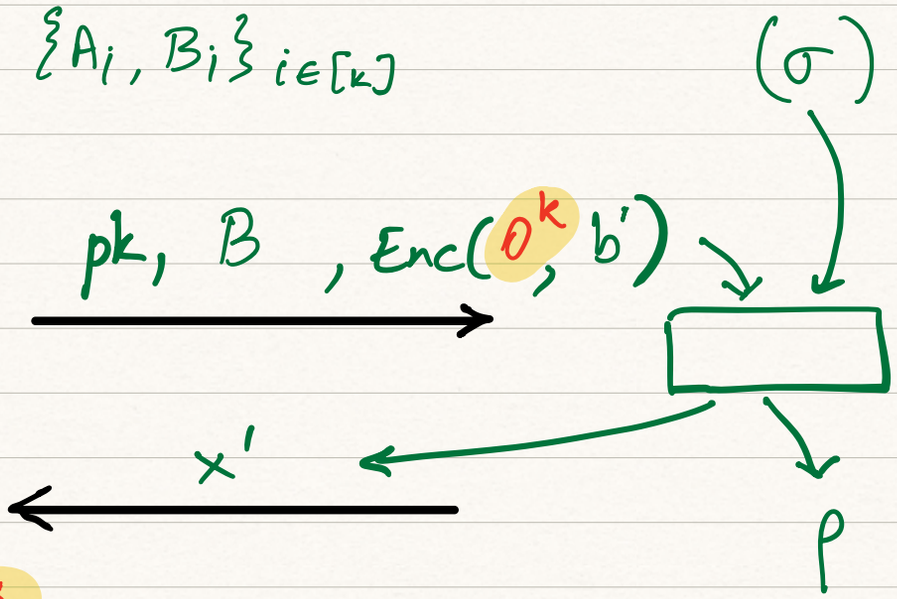
$\text{Expmt}_b^3(1^k)$ (encrypt garbage | zeroes)

Ch | A

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

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ on $\{A_i, B_i\}_{i \in [k]}$

$b' \xleftarrow{\$} \{0,1\}$



Sample $\theta \xleftarrow{\$} \{0,1\}^k$

Measure A_i in basis θ_i to obtain x_i

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

If $\tilde{b} \neq b$, abort. Else,

If $\forall i$ s.t. $\theta_i = 1$, $x_i = x'_i$, output ρ

Else, output $\perp$

We will show:

$$TD(\text{Expmt}_0^3, \text{Expmt}_1^3) = \text{negl}(k)$$

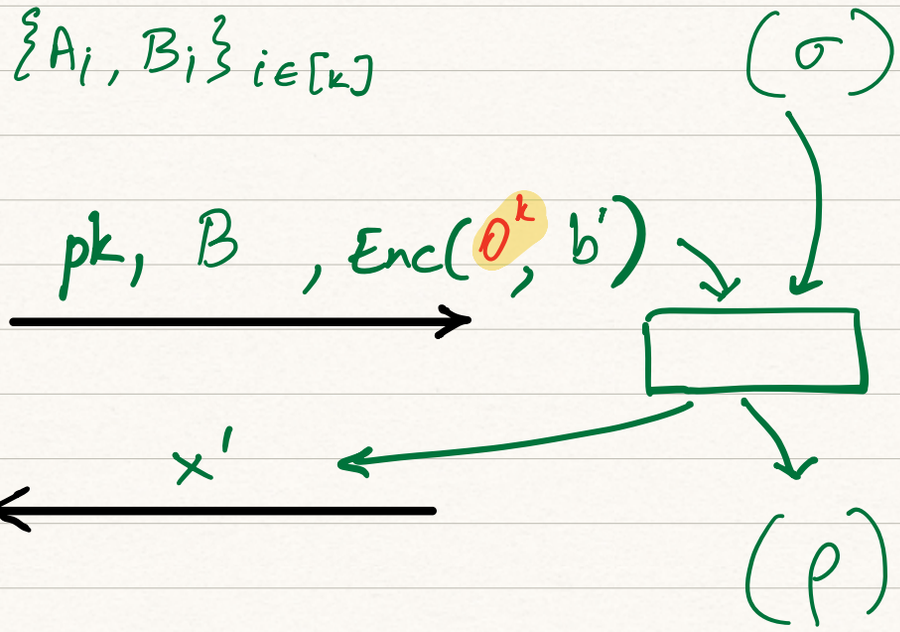
$\text{Expmt}_b^3(1^k)$ (encrypt garbage / zeroes)

Ch | A

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

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ on $\{A_i, B_i\}_{i \in [k]}$

$b' \xleftarrow{\$} \{0,1\}$



Sample $\theta \xleftarrow{\$} \{0,1\}^k$

Measure A_i in basis θ_i to obtain x_i

By the cut-and-choose argument,

if $\forall\, i \in [k]$ s.t. $\theta_i = 1$, $x_i = x_i'$

then $\forall\, i \in [k]$ s.t. $\theta_i = 0$, $A_i \approx |x_i \underset{H}{\times} x_i'|_H$

That is, projection onto $\sum_{\Delta(y,x') < cn} |y \underset{H}{\times} y|_H$ of $\{A_i\}_{i:\theta_i=0}$ succeeds w.p. $1 - \text{negl}(n)$.

RECALL: $\tilde{b} = b' \oplus \underbrace{\text{parity}_{\theta=0}(x)}_{\text{claim: uniformly random when the check passes}}$

LEMMA. (parity is a good extractor)

Given state that is "close" to Hadamard basis state, [Agarwal-Bartusek-Khurana-Kumar '22]

parity of measurements in the computational basis is an independent, uniform bit.

$$\Rightarrow TD(\text{Expmt}_0^3, \text{Expmt}_1^3) = \text{negl}(k)$$

What about $TD(\text{Expmt}_0^2, \text{Expmt}_1^2)$?

By CPA security, the projection in Expmt_b^2 onto $\sum_{\Delta(y,x')<\frac{n}{2}} |y\rangle_H\langle y|_H$ also succeeds w.p. $1-\text{negl}(k)$.

$$\Rightarrow TD(\text{Expmt}_0^2, \text{Expmt}_1^2) = \text{negl}(k).$$

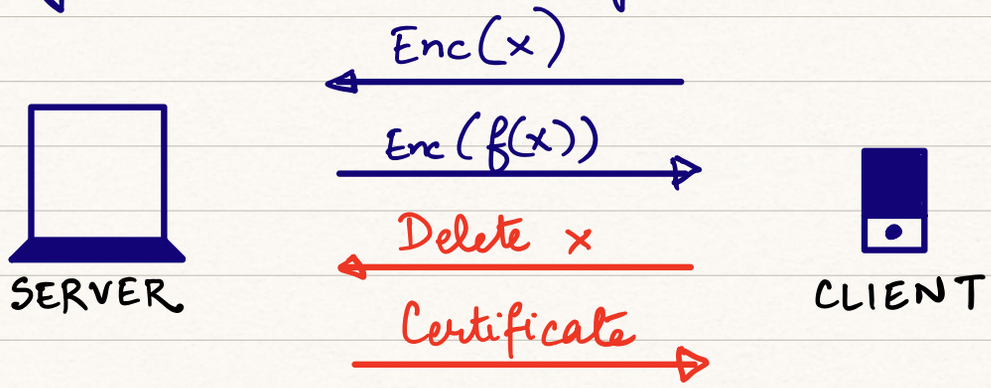
QED

APPLICATIONS

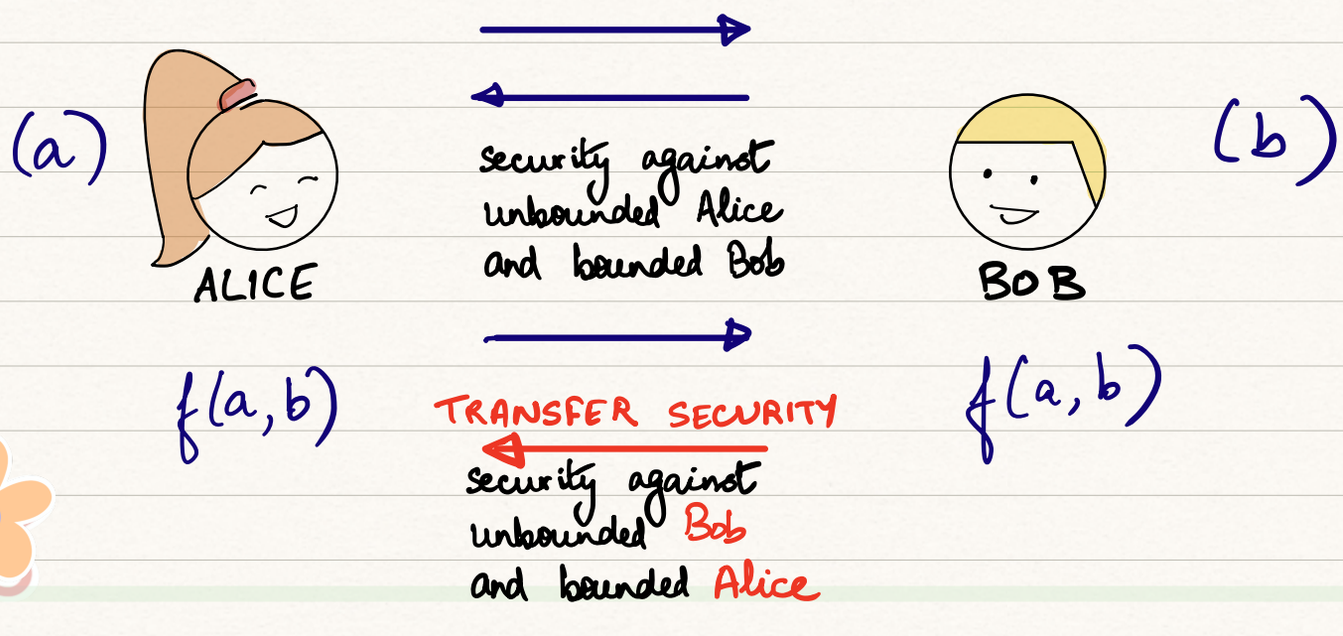
(Quickly recalling)

X $\Rightarrow$ X with certified deletion, for X in

* Commitments (applications to ZK)
* Revocable time-lock encryption / puzzles
* Attribute-based encryption (ABE)
* Witness encryption
* Fully homomorphic encryption



* Everlasting Security Transfer

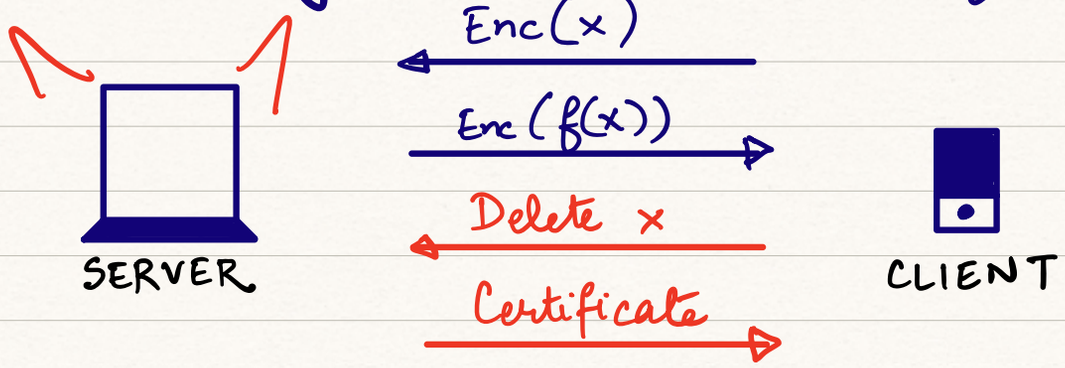


NEW APPLICATIONS

[Bartusek - Garg - Goyal - Khurana - Malavolta - Raizes - Roberts '23, Hiroka - Morimae - Nishimaki - Yamakawa '23]

X with certified deletion, for X in

* CCA - secure encryption
* Maliciously - secure blind delegation



* Obfuscation (differing - inputs)
* Functional encryption
  - deletion of ciphertexts
  - deletion of secret keys

[Other results on key - leasing are related:]

Eg, Agarwal - Kitagawa - Nishimaki - Yamada - Yamakawa, EC '23, Ananth - Poremba - Vaikuntanathan, '23]

KEY DIFFICULTY:

Security given a (partial) decryption oracle.

Consider the previous encryption scheme

$|x\rangle_\theta, Enc(\theta, b')$ where $b' = b \oplus parity_{\theta_i = 0}(x)$

NOT CCA-secure

Adv given

$|x\rangle_\theta, Enc(\theta, b')$

↓ generates

$|0\rangle, |x\rangle_{\theta|_{2..n-1}}, Enc(\theta, b')$

↓

DECRYPTION ORACLE

↓

Acc / reject

Obfuscation / Functional encryption run into similar issues.

SOLUTION: Use subspace-coset states [AC'12, CLLZ'21]

PUBLIC VERIFICATION

[BKP'23, KNY'23, BKMPW'23]

In previous solutions, vk needed to be kept hidden from deletor.

[Recall: $vk = \{x_i\}_{i:\theta_i=1}$]

What if we wanted anyone to be able to verify? (Alternatively, security when vk leaked)

TWO-TO-ONE FUNCTION

Each y has 2 preimages: $(0, x_0)$ and $(1, x_1)$

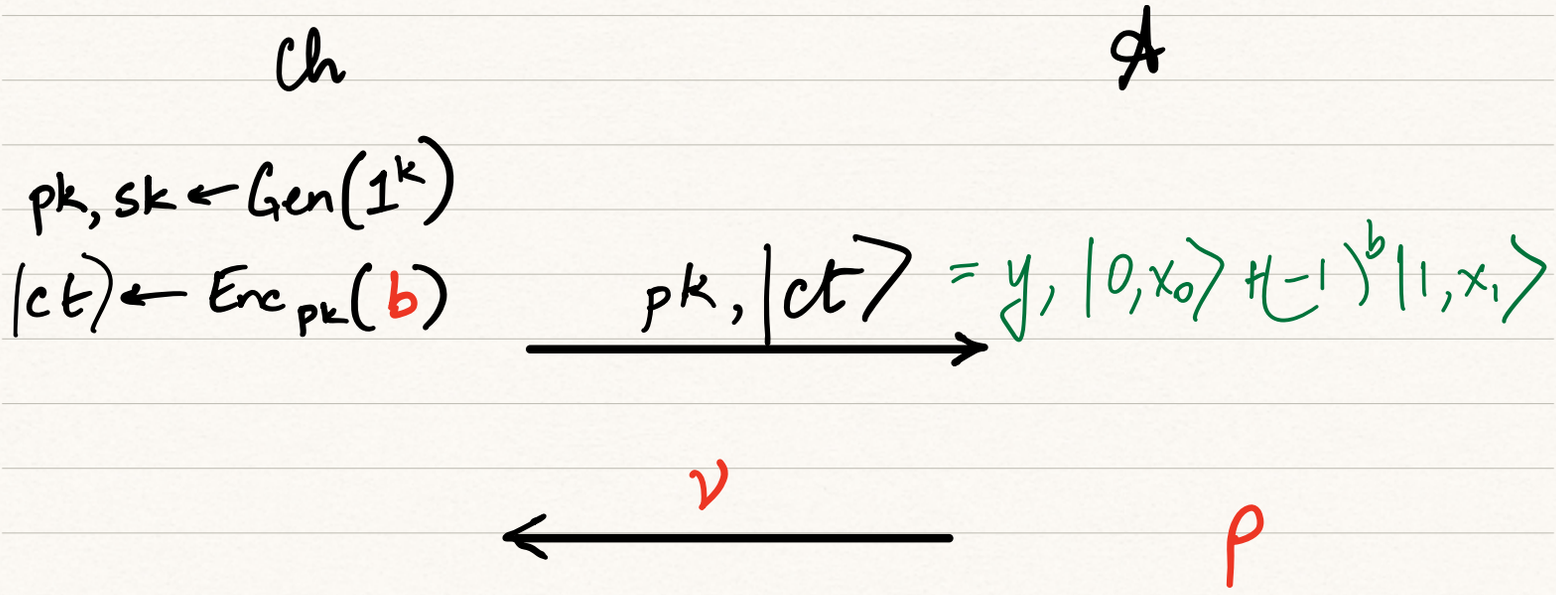
$$\text{Enc}(b) = y, |0, x_0\rangle + (-1)^b |1, x_1\rangle$$

DELETION CERT.: Preimage of y

If f is COLLAPSING,

then everlasting security after deletion.

$\text{Expmt}_b(1^k)$



If ν verifies, output ρ

(i.e., is a preimage of y)

Else, output $\perp$

Certified-Deletion-Security (formal)

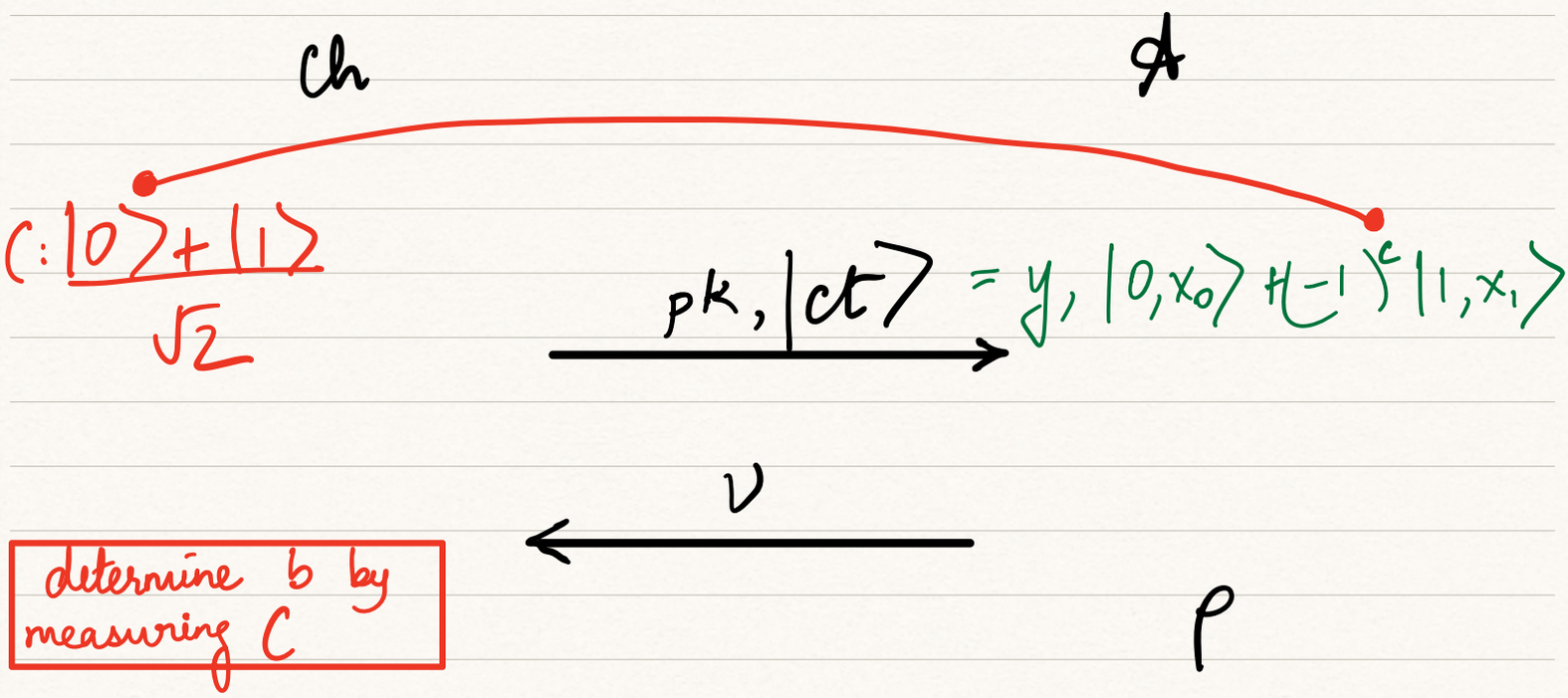
$$TD(\text{Expmt}_0, \text{Expmt}_1) = \text{negl}(k)$$

f is "COLLAPSING" $\Longrightarrow$

$$\forall b, \quad |0,x_0\rangle + (-1)^b |1,x_1\rangle$$

$$\approx_c \begin{cases} |0,x_0\rangle & \text{w.p. } 1/2 \\ |1,x_1\rangle & \text{w.p. } 1/2 \end{cases}$$

$\text{Expmt}_b^1(1^k)$



ρ

If $f(v) = y$, output ρ

Else, output $\perp$

$\text{Expmt}_b^1(1^k)$

Ch $\qquad$ A

$C: \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\qquad$ $|0,x_0\rangle + (-1)^c |1,x_1\rangle$

$A: \frac{|0,x_0\rangle + |1,x_1\rangle}{\sqrt{2}}$

Apply phase kickback to A, controlled on C

$$|0\rangle_C \left(\frac{|0,x_0\rangle + |1,x_1\rangle}{\sqrt{2}}\right)_A + |1\rangle_C \left(\frac{|0,x_0\rangle - |1,x_1\rangle}{\sqrt{2}}\right)_A$$

$\xrightarrow{pk, |ct\rangle = y, C}$

$\xleftarrow{v}$

determine b by measuring C

ρ

If $f(v) = y$, output ρ

Else, output $\perp$

$\text{Expmt}_b^2(1^k)$

Ch $\quad$ $\mathcal{A}$

$C : \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$A : \frac{|0, x_0\rangle + |1, x_1\rangle}{\sqrt{2}}$

Measure A in std. basis

Apply phase kickback to A, controlled on C obtaining

$|+\rangle_C |0, x_0\rangle_A$ w.p. $\frac{1}{2}$, $|-\rangle_C, |1, x_1\rangle_A$ w.p. $\frac{1}{2}$

$\xrightarrow{pk, |ct\rangle = y, C}$

$\xleftarrow{v}$

$\mathcal{P}$

determine b by measuring C

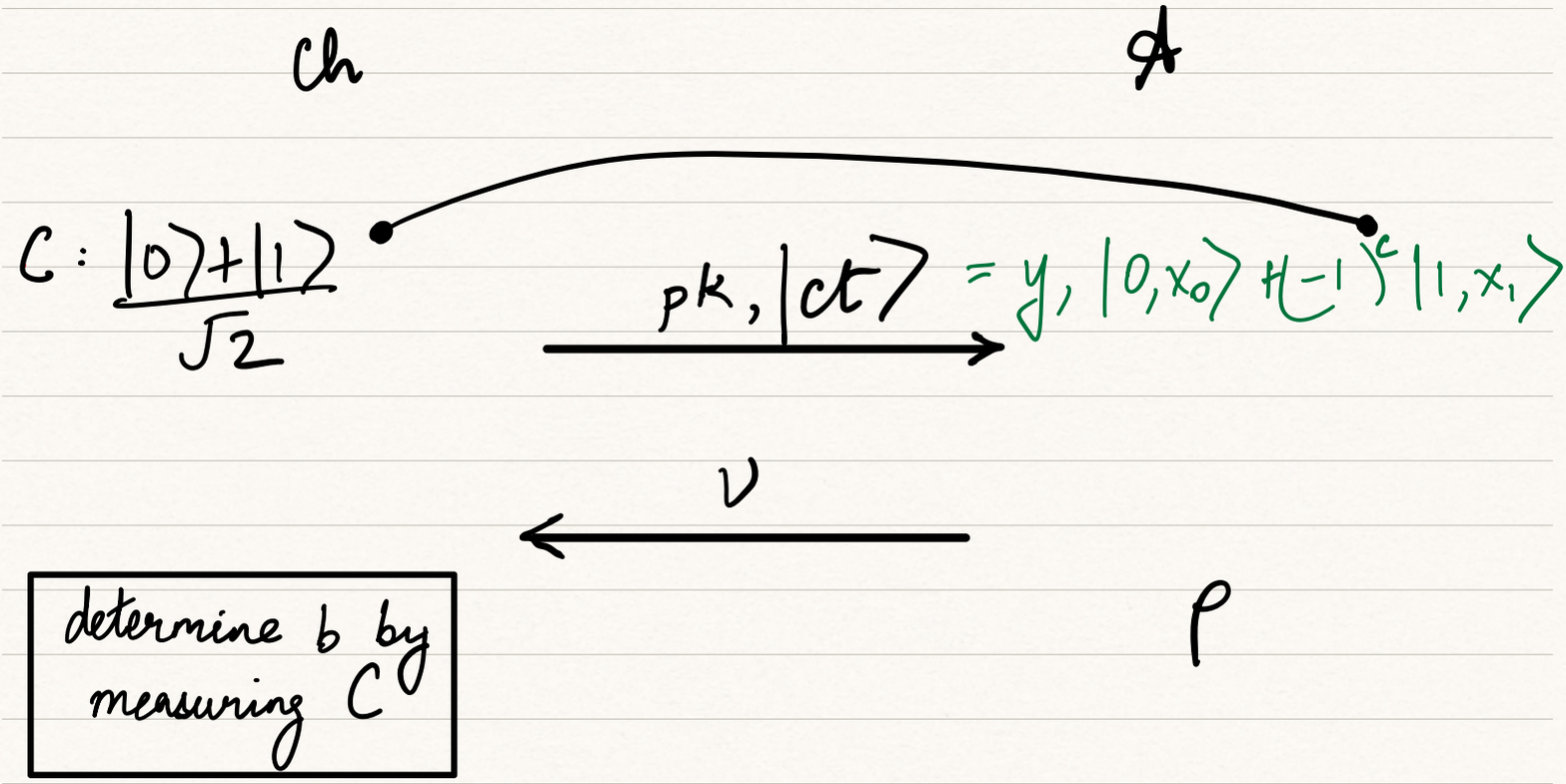
If $f(v) = y$, output ρ

Else, output $\perp$

If v verifies, and is $|1 \ldots\rangle$, $C = |-\rangle$

If v verifies, and is $|0 \ldots\rangle$, $C = |+\rangle$

$\text{Expmt}_b^1(1^k)$



If $f(v) = y$, output ρ

Else, output $\perp$

If v verifies, and is $|1\ldots\rangle$, $C = |-\rangle$

If v verifies, and is $|0\ldots\rangle$, $C = |+\rangle$

Further generalizing this template yields:

1. Proof of "Gaussian collapsing conjecture" [Poremba '22]

$\Rightarrow$ public-key encryption with PVD,
FHE with PVD from LWE / SIS.

2. X $\Rightarrow$ X with PVD
(+ one-way functions)

for X in

* public-key encryption
* attribute-based encryption
* quantum fully homomorphic encryption
* witness encryption
* timed-release encryption