QKD

Step 1: Distribute Bell pairs (insecure)

Step 2: Bell test: $\forall E: \exists \rho^{ideal} \in S_{ideal}^{t\text{-}error}$:

$$TD(\rho^{ideal}, \rho_{test}) \cdot Pr[success] \le \sqrt{\delta_q}$$

Step 3: Measure the (raw) key

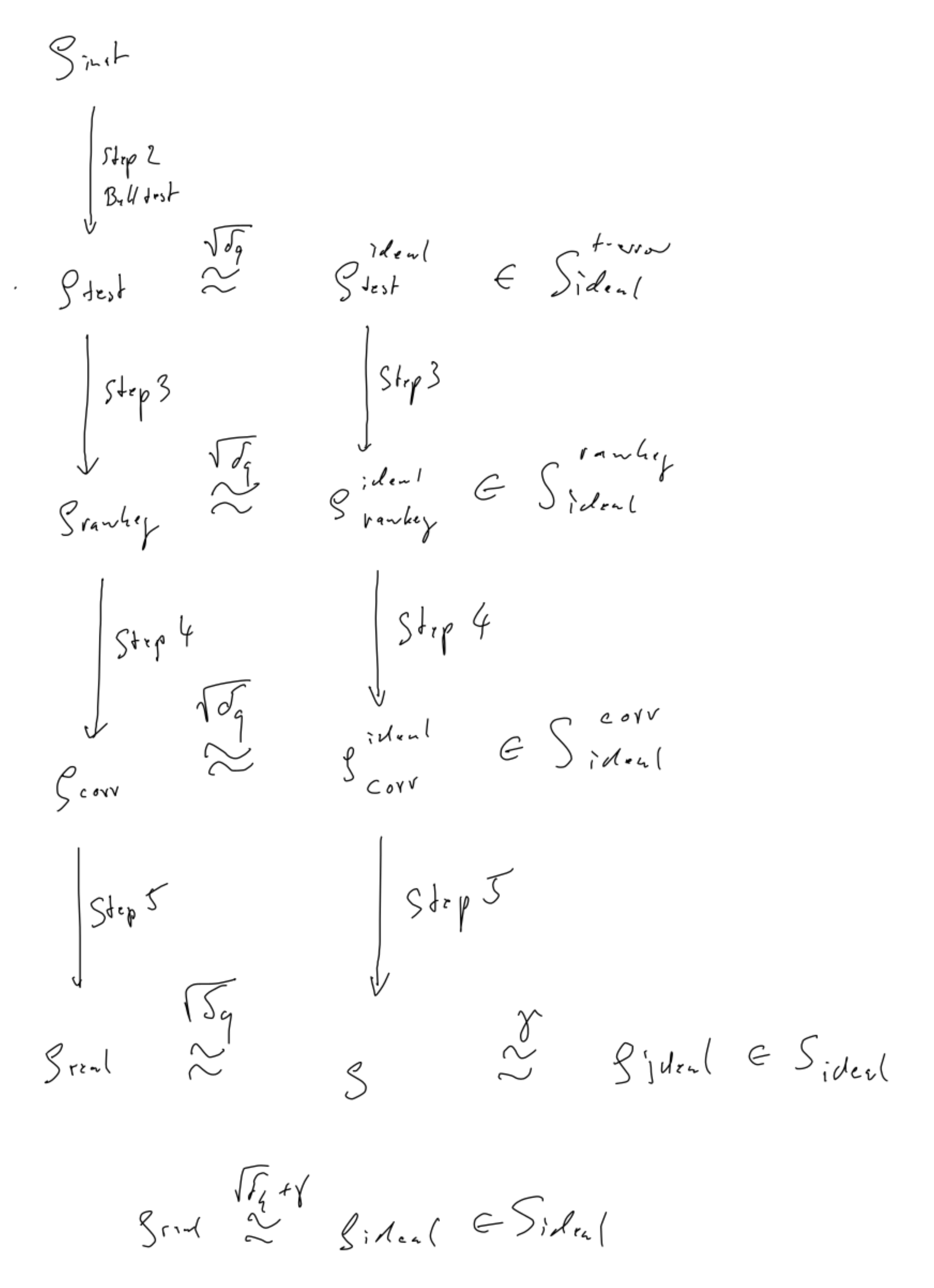
If $\rho_{test} \in S_{ideal}^{t\text{-}error} \Rightarrow \rho_{rawkey} \in S_{ideal}^{rawkey}$

$|K_A| = |K_B| = n = m - q$

$$S_{ideal}^{rawkey} := \{\rho : |K_A \oplus K_B| \le t,\ H_\infty(K_A|E) \ge n - t\log(3n+1)\}$$

$\Rightarrow$ ~~For any ρ_{test}~~ $\forall E$: $\exists \rho_{ideal} \in S_{ideal}^{rawkey}$:

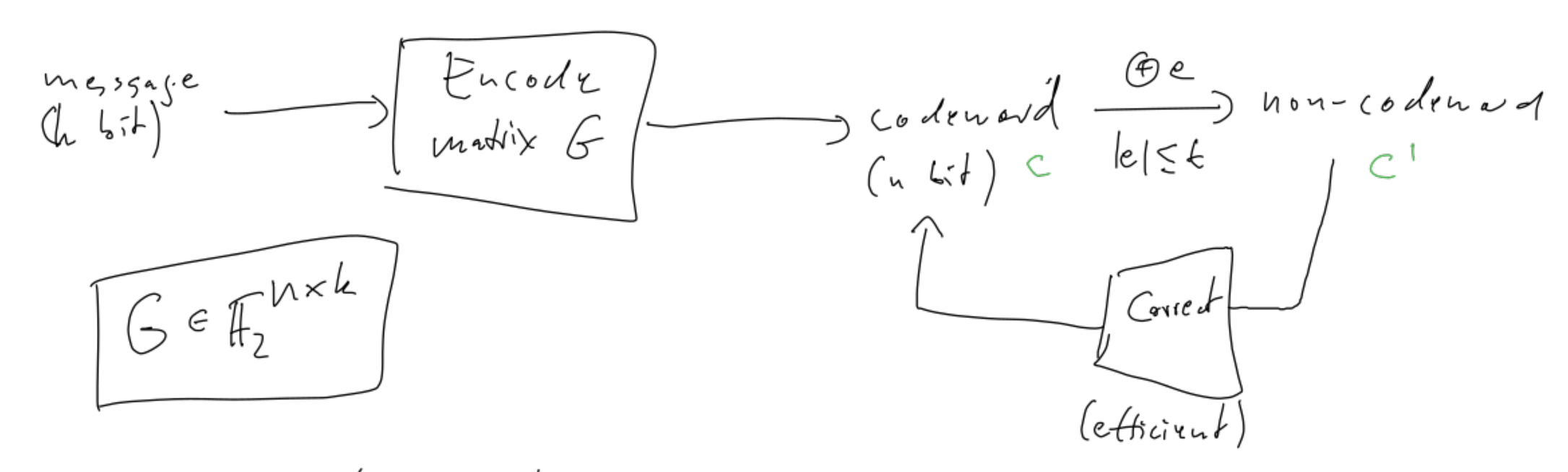
$$TD(\rho_{ideal}, \rho^{rawkey}) \le \sqrt{\delta_q}$$



Step 4 Error correction

Error corr code (linear binary)

$[n,k]$-code correcting t errors



$G \in \mathbb{F}_2^{n \times k}$

Parity check matrix H: $\quad H \in \mathbb{F}_2^{(n-k)\times n}$

$Hc = 0$ iff c is codeword

Syndrome $\sigma = Hc' = H(c \oplus e) = He$

Could error correct by:
- Find e s.t. $He = \sigma$ $(|e| \le t)$
- $c := c' \oplus e$

Crucial fact here:

Given He with $|e| \le t$, can efficiently find the unique e.

Step 4 K_A (A) $\xrightarrow[\text{(auth channel)}]{\sigma = HK_A}$ (B) K_B $\quad |K_A \oplus K_B| \le t$

$K_A' := K_A$

$HK_B \oplus \sigma$
$= HK_A \oplus HK_B$
$= H(\underbrace{K_A \oplus K_B}_{|\cdot| \le t})$
$\rightsquigarrow K_A \oplus K_B$
$\rightsquigarrow K_A$ $\quad$ Set $K_B' := K_A$

$\Rightarrow K_A' = K_B'$ (assuming $\rho_{rawkey} \in S_{ideal}^{rawkey}$)

$E' = E\sigma$

$\Rightarrow H_\infty(K_A'|E')_{corr} = H_\infty(K_A|E\sigma)_{rawkey}$ (depends on)

Lemma (Chain Rule)

$$H_\infty(XY|Z) \le H_\infty(X|YZ) + |Y|$$

[applied with $X = K_A$, $Y = \sigma$, $Z = E$]

$\ge H_\infty(K_A\sigma|E)_{rawkey} - |\sigma|$
$\ge H_\infty(K_A|E)_{rawkey} - |\sigma|$
$\ge n - t\log(3n+1) - (n-k)$
$= k - t\log(3n+1)$

Summary: If $\rho_{rawkey} \in S_{rawkey}^{ideal}$
then $\rho_{corr} \in S_{corr}^{ideal} := \{\rho : K_A = K_B,\ H_\infty(K_A|E) \ge k - t\log(3n+1)\}$

~~A~~ $\Rightarrow \forall E: \exists \rho_{corr}^{ideal} \in S_{corr}^{ideal}$:

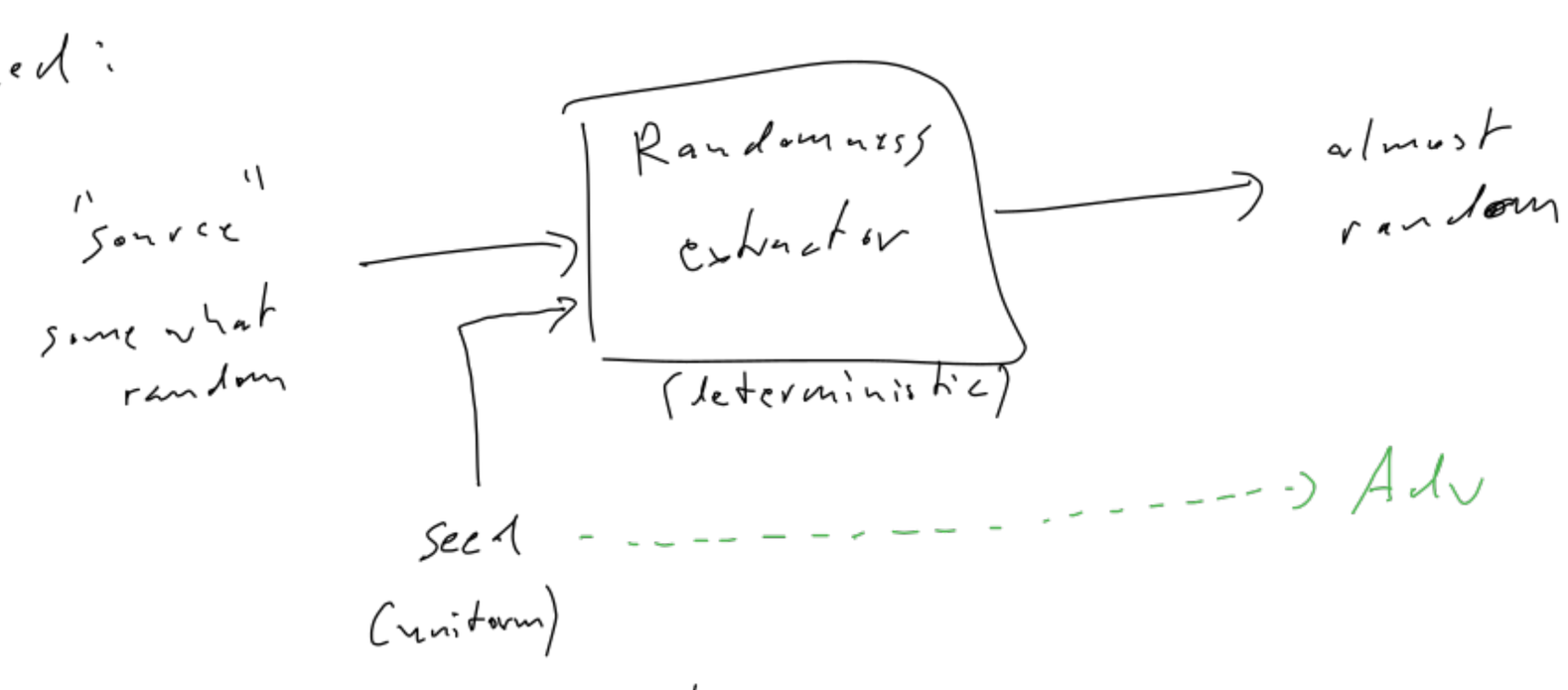
$$TD(\rho_{corr}, \rho_{corr}^{ideal}) \cdot Pr[success] \le \sqrt{\delta_q}$$

Step 5

Have: $H_\infty(K_A|E) \ge k - t\log(3n+1)$

Want: K_A is uniform (or TD-close to it)

Need:

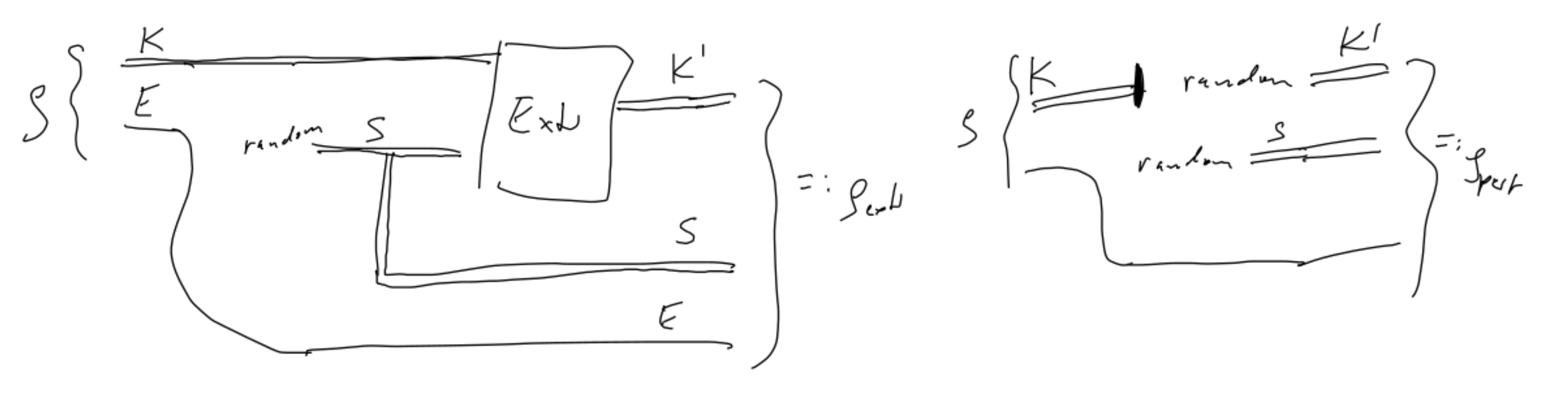


Strong rand extractor:

Output looks random to adv that knows seed!

Def: "Extr" is a strong (k,ε)-quantum rnd extractor iff $\forall \rho$ (with regs K, E (classical)) with $H_\infty(K|E) \ge k$:

$$TD(\rho_{extr}, \rho_{perf}) \le \varepsilon$$



Do such rnd-extr. exist?

Def: A function $F(S, K) \to K'$ is (2-)universal hash func iff ~~...~~ $\forall k_1 \ne k_2$: $Pr[F(s,k_1) = F(s,k_2)] \le \frac{1}{2^{|K'|}}$ for uniform s

Thm (Leftover Hash Lemma, q version)

If F is 2-UHF then
F is strong $(k, 2^{-\frac{1}{2}(k-\ell)})$-q rnd extr
(ℓ := len of F's output, k arb.)

Example of UHF:

$S := \mathbb{F}_2^{\ell \times n}$, $\quad K := \mathbb{F}_2^n$

$F(s,k) = s \cdot k \in \mathbb{F}_2^\ell$ (ℓ bit string)

is UHF $\forall \ell, n$

Step 5 (Privacy amplification) $\quad$ [Let F be strong rnd extr]

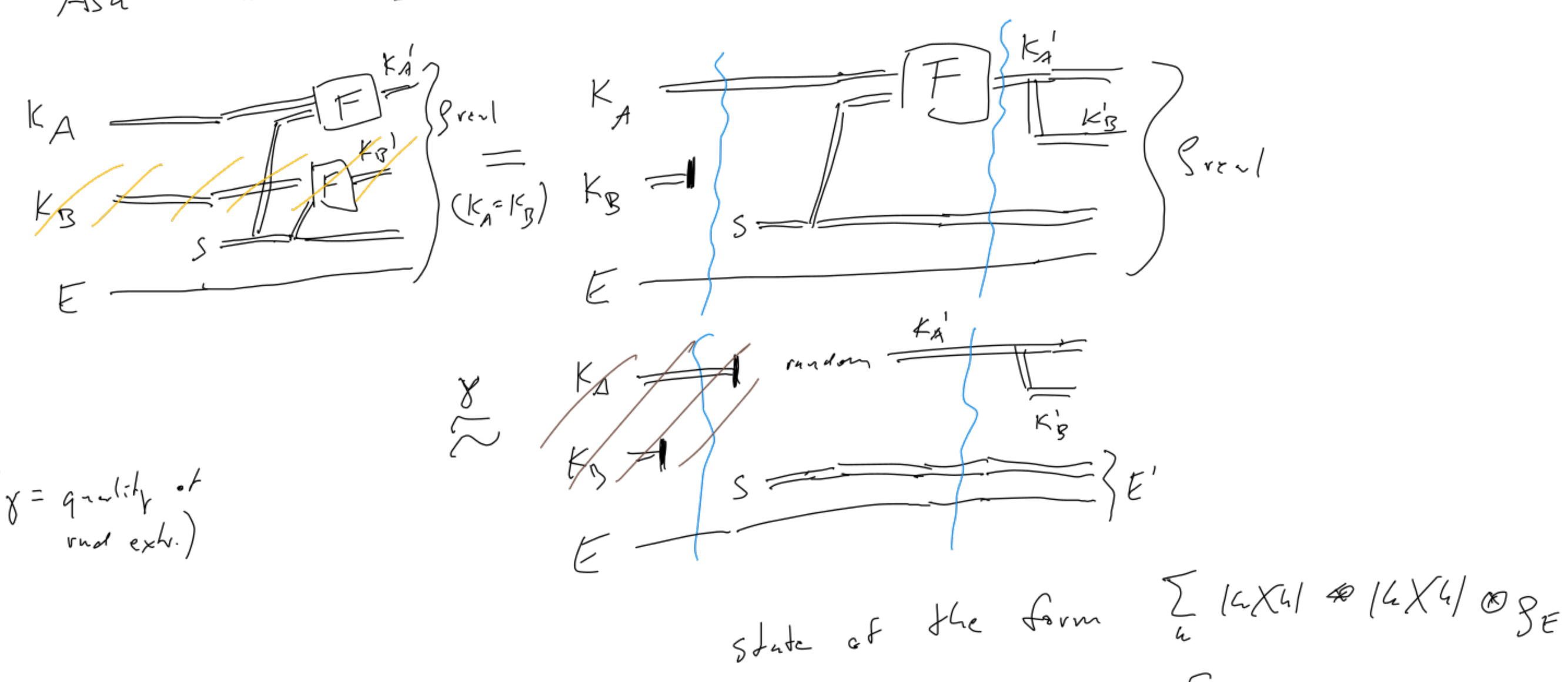
K_A (A) $\xrightarrow{\ s\ }$ (B) K_B $\quad (K_A = K_B)$

$s \xleftarrow{\$}$ seeds S $\quad H_\infty(K_A|E) \ge k - t\log(3n+1)$

$K_A' := F(s, K_A)$ $\quad K_B' := F(s, K_B)$

$\Rightarrow K_A' = K_B'$

Ask: ~~is the result~~ does K_A', K_B' look uniform to E?



(γ = quality of rnd extr.)

state of the form $\sum_k |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \rho_E$ $\in S_{ideal}$

$\Rightarrow$ If $\rho_{corr} \in S_{ideal}^{corr}$
then $\exists \rho_{ideal} \in S_{ideal}$: $TD(\rho_{real}, \rho_{ideal}) \le \gamma$

Final result: $\forall E\ \exists \rho_{ideal} \in S_{ideal}$:

$$TD(\rho_{real}, \rho_{ideal}) \cdot Pr[success] \le \sqrt{\delta_q} + \gamma$$

$$= \left(1 - \frac{t+1}{2m}\right)^{q/2} + 2^{-\frac{1}{2}(k - t\log(3n+1) - \ell)} =: \varepsilon$$

(ℓ = len of final key)

$\Rightarrow$ The proto is an ε-secure QKD