Composability of quantum protocols

Applications to Quantum Key Distribution & Quantum Authentication

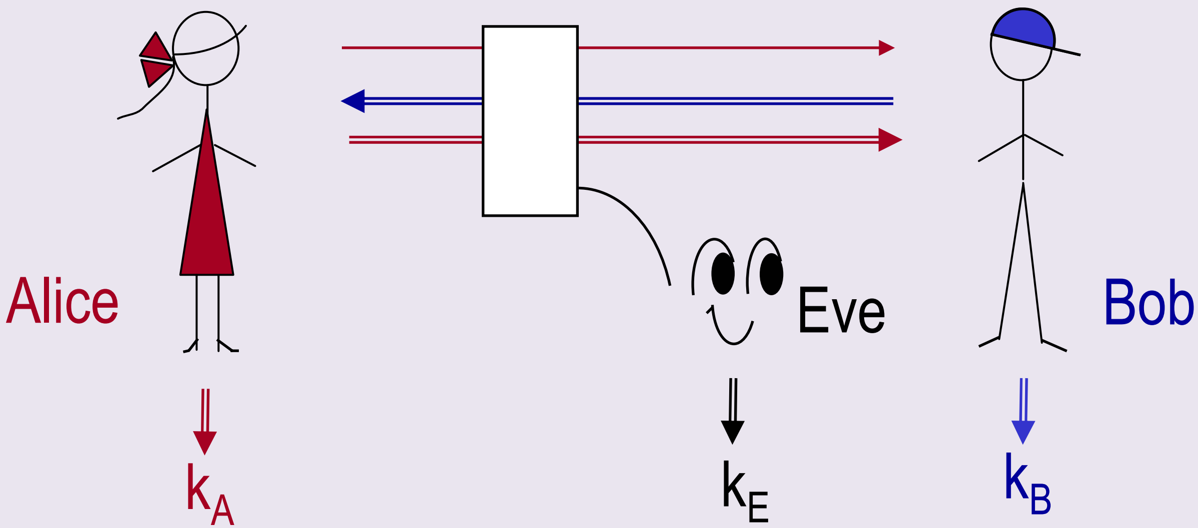
Debbie Leung, Caltech

QIP 2004, Waterloo

Joint work with Ben-Or, Hayden, M. Horedecki, Mayers, Oppenheim

Composability : Motivation

QKD:



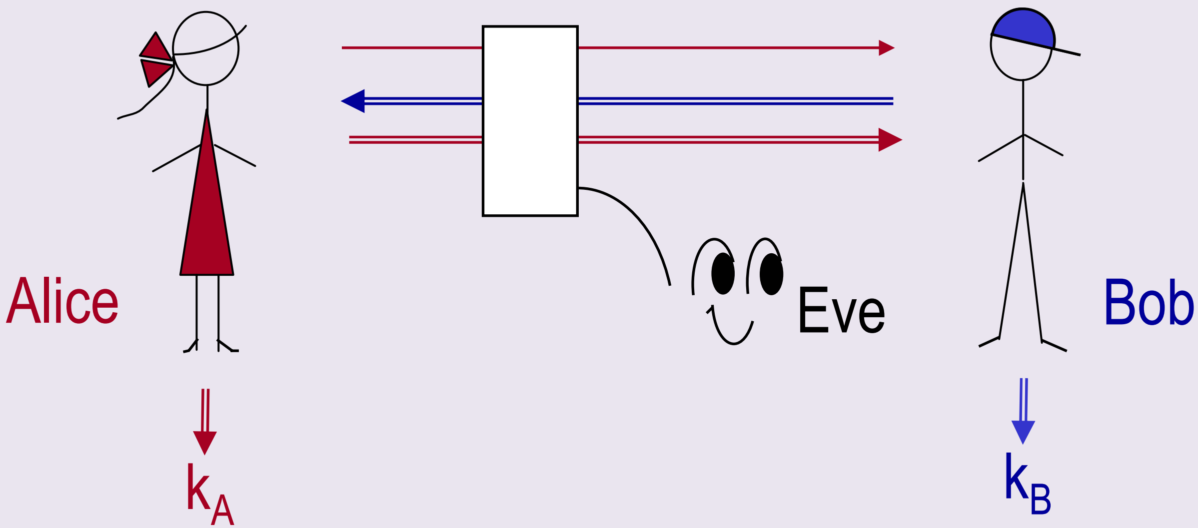
QKD is "unconditionally secure" :

$\forall$Eve's strategy s.t. Pr(success) is non-negligible,

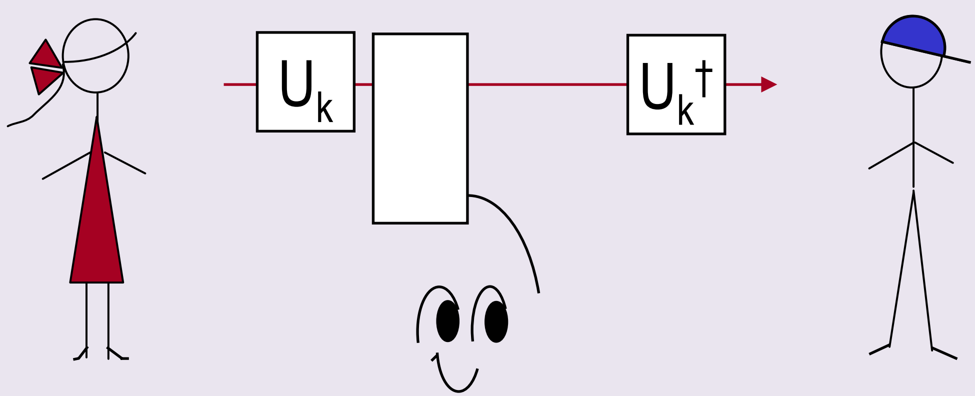
key $k \approx k_A \approx k_B$ & $\mathrm{I}(k_E{:}k) \leq e^{-\alpha n}$.

Composability : Motivation

QKD:



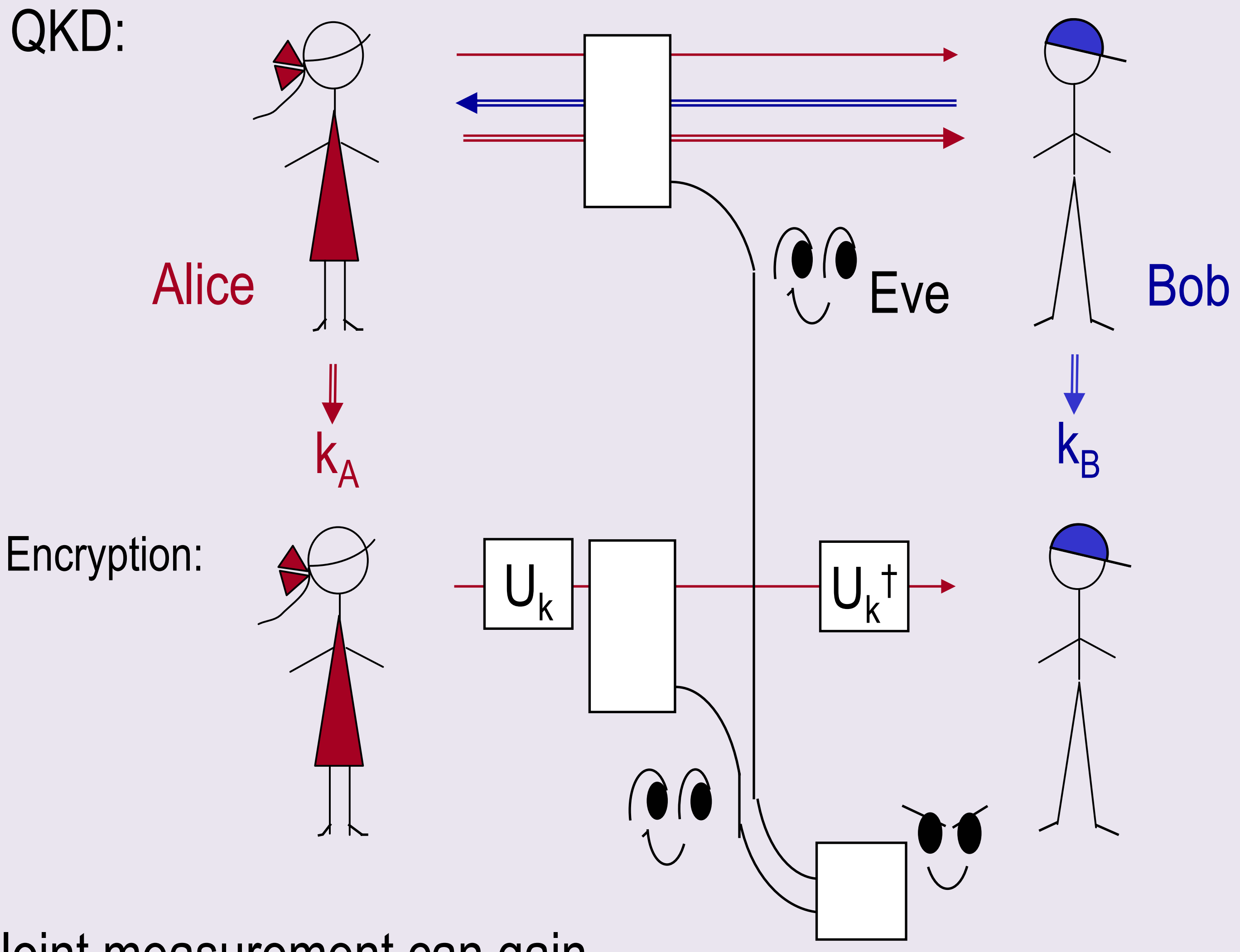
Encryption:



Is “QKD + encryption” secure ???

Criteria $\mathrm{I}(k_E{:}k) \leq e^{-\alpha n}$ applicable only if Eve measures to learn about k.

Composability : Motivation

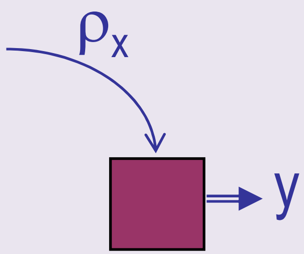


Joint measurement can gain
more info than sum of info obtained from individual measurements

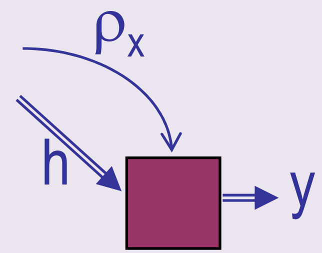
Composability : Motivation (scary story)

Possibility of unlocking information:

DiVincenzo, M. Horedecki, Leung, Smolin, Terhal 0303088, Hayden, Leung, Shor, Winter 0307104



$$I_1 = \max_{\text{meas}} I(X:Y)$$



$$I_2 = \max_{\text{meas}} I(X:Y')$$

Examples are found $I_2 \gg I_1 + \text{size}(h)$.

Unbounded $(I_2 - I_1)$=size(h).

Outline:

- Universal composability theorem in quantum/classical case.
  - Statement & intuition

- Composability of QKD
  - Motivation (key degradation)
  - Usual security criteria implies composable security criteria

- Composability of QAuth
  - Motivation (key recycling)
  - Composability of BCGST02 & related protocols

Reference:

Ben-Or, Mayers 02

(Inheriting much from the classical case, e.g. see Canetti 01.)

Qn:Bennett, Smolin, partial sol'n:Harrow

Ben-Or, M. Horedecki, Leung, Mayers, Oppenheim 02

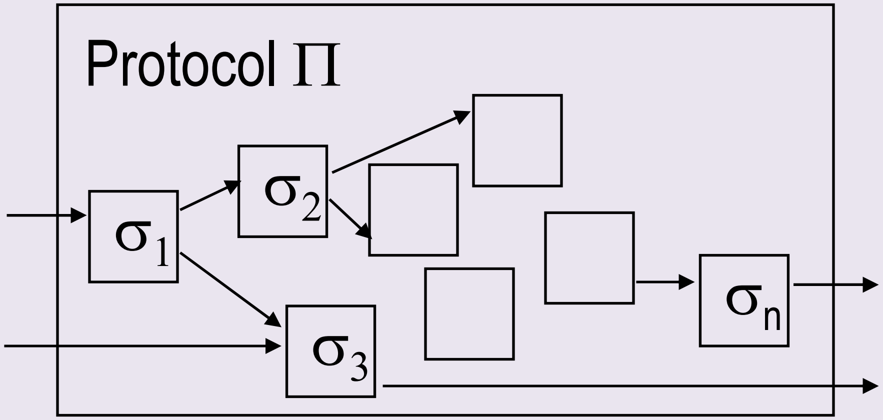
0306161

Partial sol'n by M. Horedecki, Oppenheim

Hayden, Leung, Mayers 03

Universal composable security definition
Universal composability theorem

Composability : general problem



Universal composability theorem:

- When is a subprotocol “secure enough” to be used in a larger protocol?
- When is the main protocol secure, given *“enough security” of all constituent subprotocols*?

Universal: independent of what subprotocols & how they are implemented (imperfectly).

Universal composable security definition

A real protocol "σ" imperfectly realizes an ideal protocol σ^I.

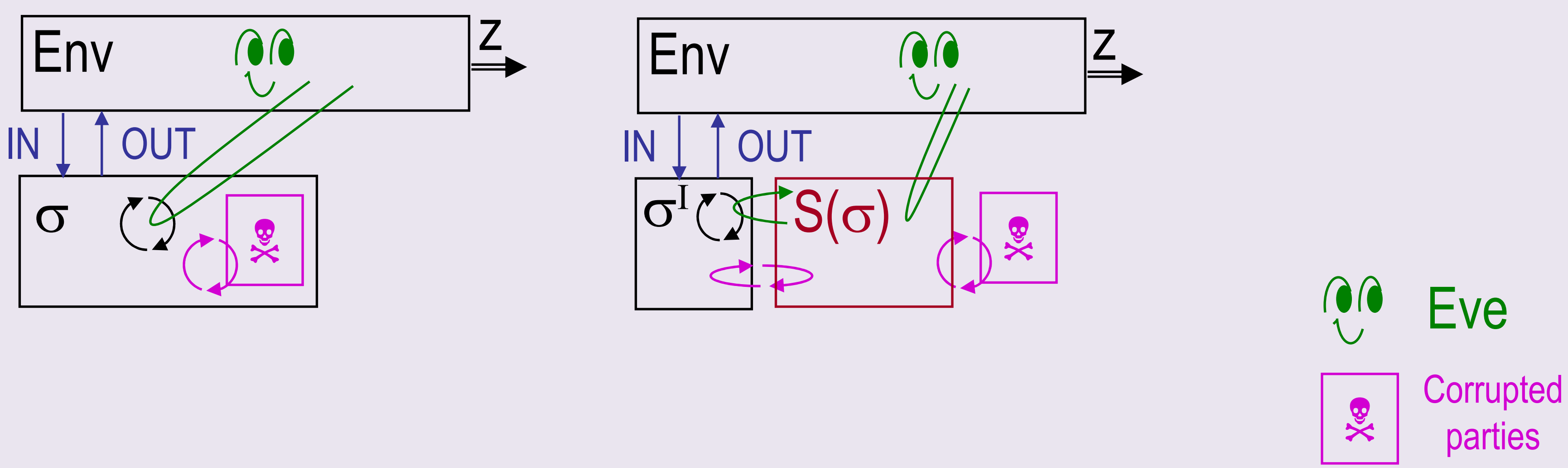
"Env": controls the use of σ (full access to its inputs/outputs), controls all corrupted parties in σ, & eavesdrops on communication in σ.

A "simulator" $S(\sigma)$, depending on the given Env, is added to σ^I .

Env tries to distinguish between "σ" & "$\sigma^I+S(\sigma)$".

Let z be Env's 1-bit answer.

Real vs Ideal



Universal composable security definition

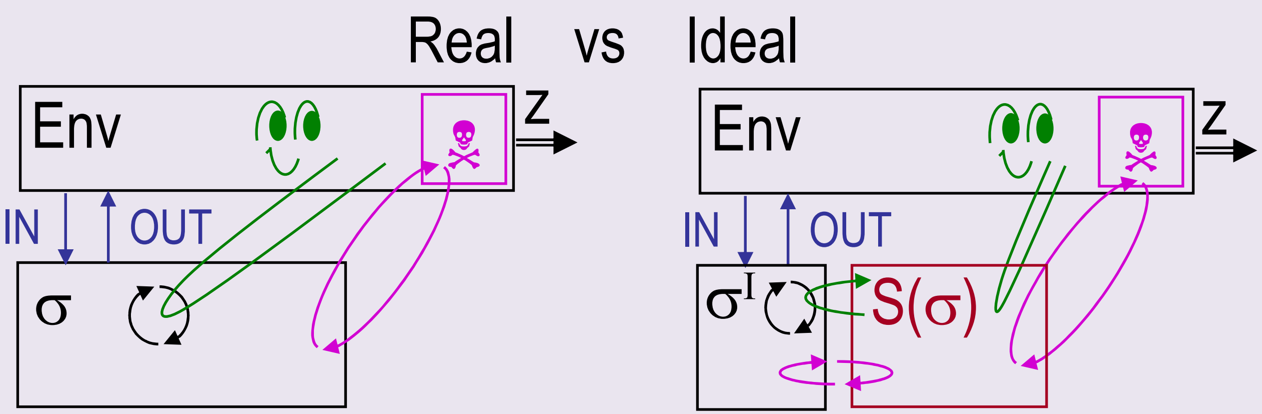
A real protocol “σ” imperfectly realizes an ideal protocol σ^I.

“Env”: controls the use of σ (full access to its inputs/outputs), controls all corrupted parties in σ, & eavesdrops on communication in σ.

A “simulator” S(σ), depending on the given Env, is added to σ^I .

Env tries to distinguish between “σ” & “σ^I+S(σ)”.

Let z be Env’s 1-bit answer.



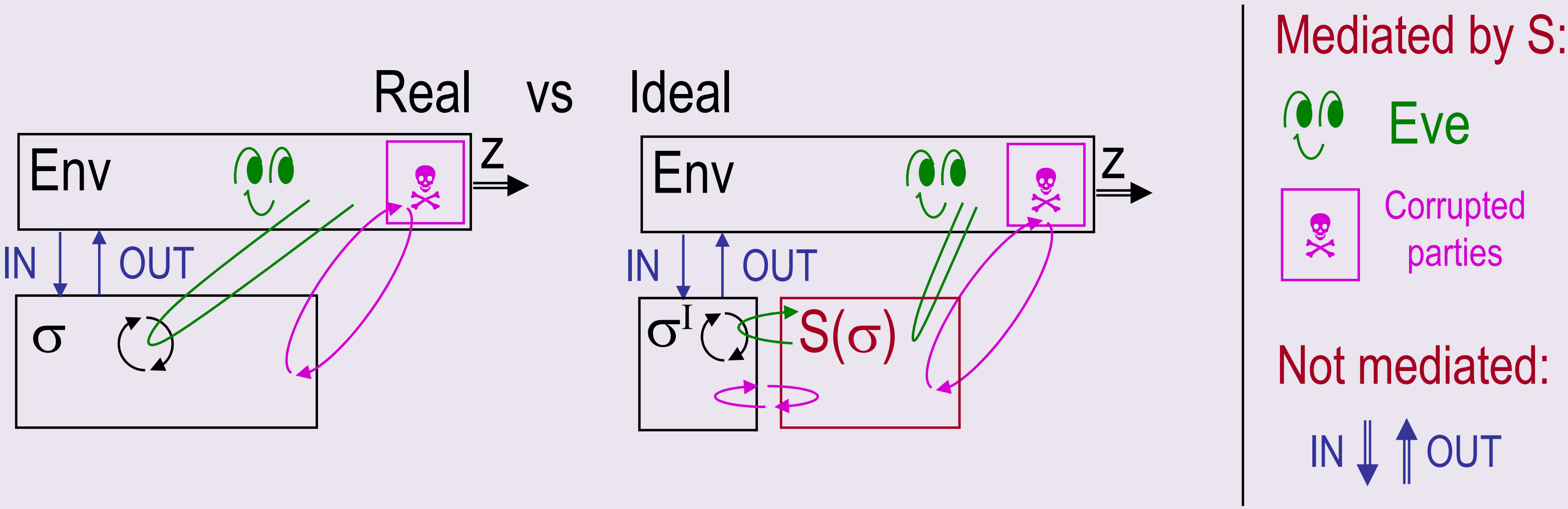
Universal composable security definition

Env tries to distinguish between "σ" & "$\sigma^I+S(\sigma)$", simulator tries to confuse Env.
Let z be Env's 1-bit answer.

Universal composable security definition:

σ ε-s.r.σ^I if $\forall$Env (applications + adversaries + eavesdropping strategies)

$$\exists\, S(\sigma) \text{ s.t. } |\Pr(z=0 \mid \sigma) - \Pr(z=0 \mid \sigma^I+S(\sigma))| \le \varepsilon .$$



Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

(to implement Π^I)

If $\Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I

then $\Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

NB: Security definition crafted to make this hold.

Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^{I})$ ε_1-s.r. Π^{I} and σ ε_2-s.r. σ^{I}

then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^{I} .

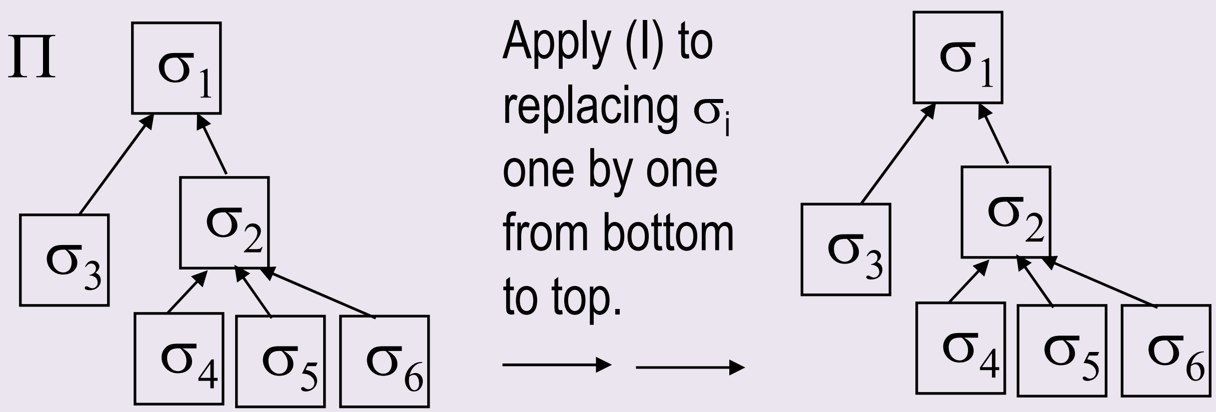
Universal composability theorem (II) (recursive use of (I))

Arbitrarily complicated protocol Π is secure if

(i) no security deadlock (e.g. a tree-like subprotocol structure)

(ii) for each node $\eta(\sigma^{I},\mu^{I},...)$ s.r. η^{I}.

(iii) each subprotocol is secure



Universal composability theorem (I)

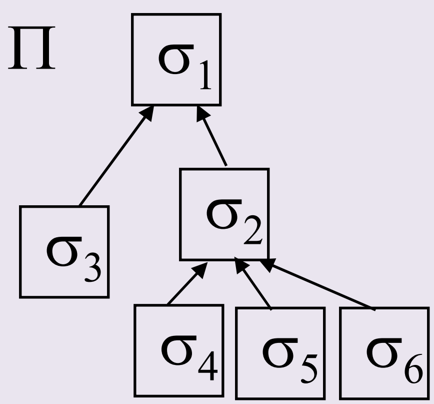
Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I
then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

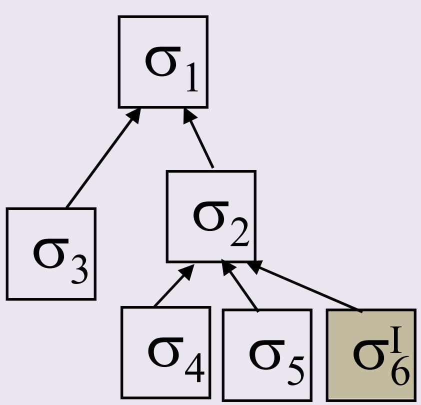
Universal composability theorem (II) (recursive use of (I))

Arbitrarily complicated protocol Π is secure if

(i) no security deadlock (e.g. a tree-like subprotocol structure)
(ii) for each node $\eta(\sigma^I,\mu^I,...)$ s.r. η^I.
(iii) each subprotocol is secure



Apply (I) to replacing σ_i one by one from bottom to top.



Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I

then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

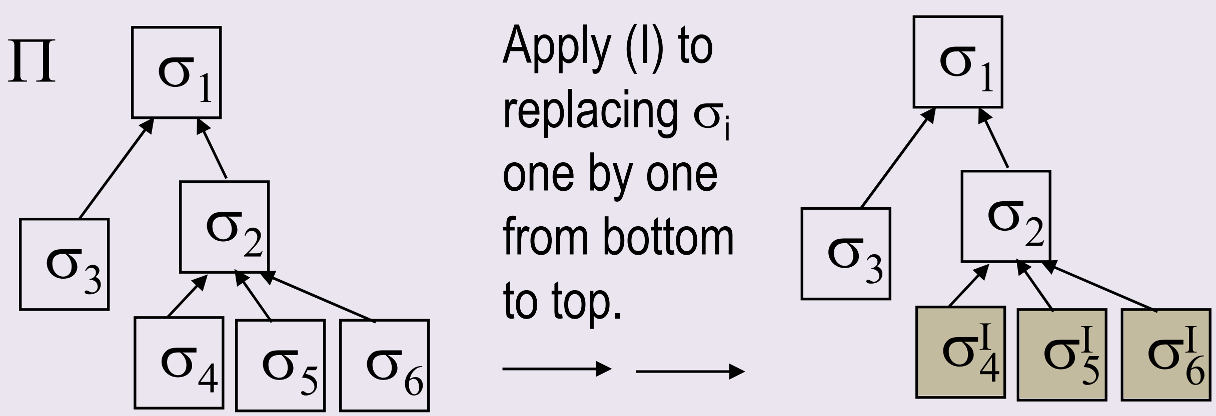
Universal composability theorem (II) (recursive use of (I))

Arbitrarily complicated protocol Π is secure if

(i) no security deadlock (e.g. a tree-like subprotocol structure)

(ii) for each node $\eta(\sigma^I,\mu^I,...)$ s.r. η^I.

(iii) each subprotocol is secure



Universal composability theorem (I)

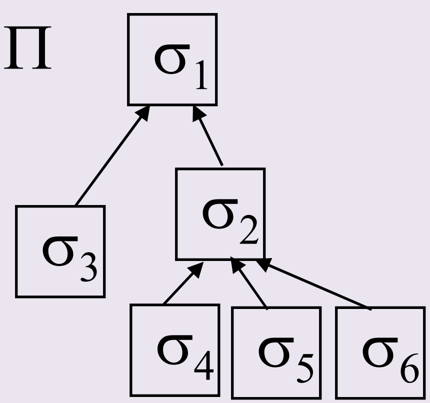
Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I
then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

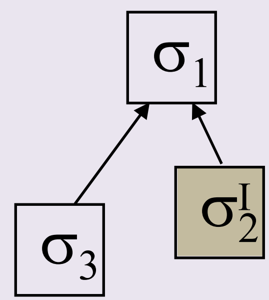
Universal composability theorem (II) (recursive use of (I))

Arbitrarily complicated protocol Π is secure if

(i) no security deadlock (e.g. a tree-like subprotocol structure)
(ii) for each node $\eta(\sigma^I,\mu^I,\ldots)$ s.r. η^I.
(iii) each subprotocol is secure



Apply (I) to replacing σ_i one by one from bottom to top.



Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I

then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

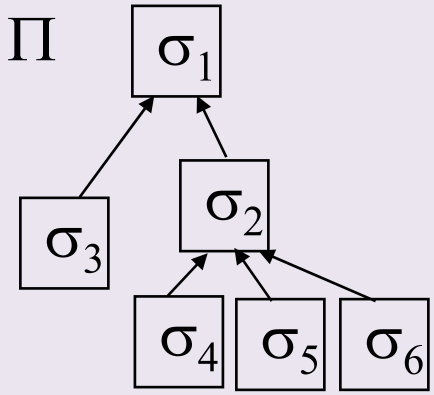
Universal composability theorem (II) (recursive use of (I))

Arbitrarily complicated protocol Π is secure if

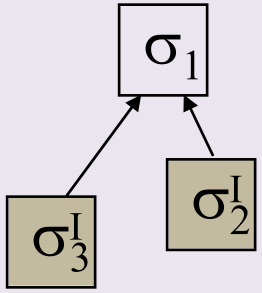
(i) no security deadlock (e.g. a tree-like subprotocol structure)

(ii) for each node $\eta(\sigma^I,\mu^I,...)$ s.r. η^I.

(iii) each subprotocol is secure



Apply (I) to replacing σ_i one by one from bottom to top.



Universal composability theorem (I)

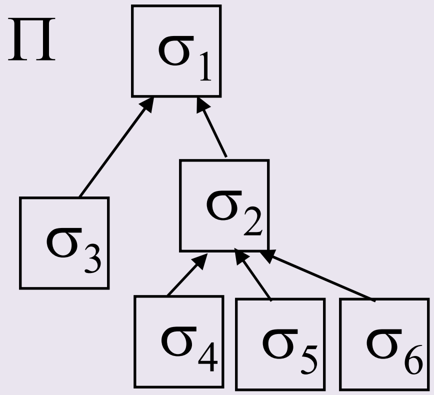
Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I
then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

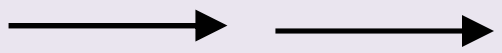
Universal composability theorem (II) (recursive use of (I))

Arbitrarily complicated protocol Π is secure if

(i) no security deadlock (e.g. a tree-like subprotocol structure)
(ii) for each node $\eta(\sigma^I,\mu^I,...)$ s.r. η^I.
(iii) each subprotocol is secure



Apply (I) to replacing σ_i one by one from bottom to top.



Punchline

Universal composable security definition:

σ ε-s.r. σ^I if $\forall$Env (applications + adversaries + eavesdropping strategies)

$\exists$ S(σ) s.t. | Pr(z=0 | σ) – Pr(z=0 | σ^I+S(σ)) | $\leq \varepsilon$.

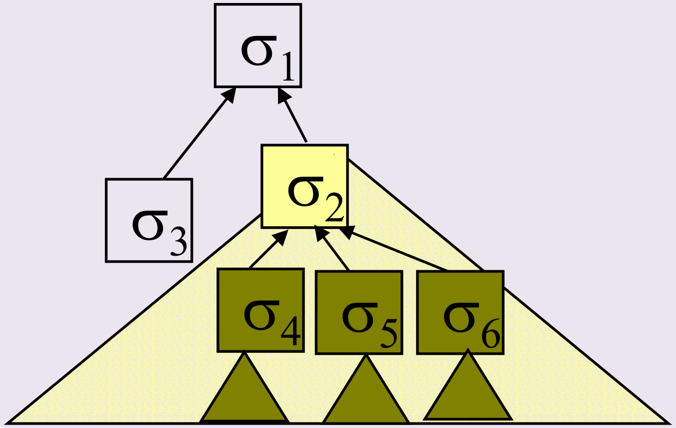
Universal composability theorem:

Π is secure if

(i) no security deadlock

(ii) for each node $\eta(\sigma^I,\mu^I,\ldots)$ s.r. η^I.

(iii) each subprotocol satisfies composable security definition

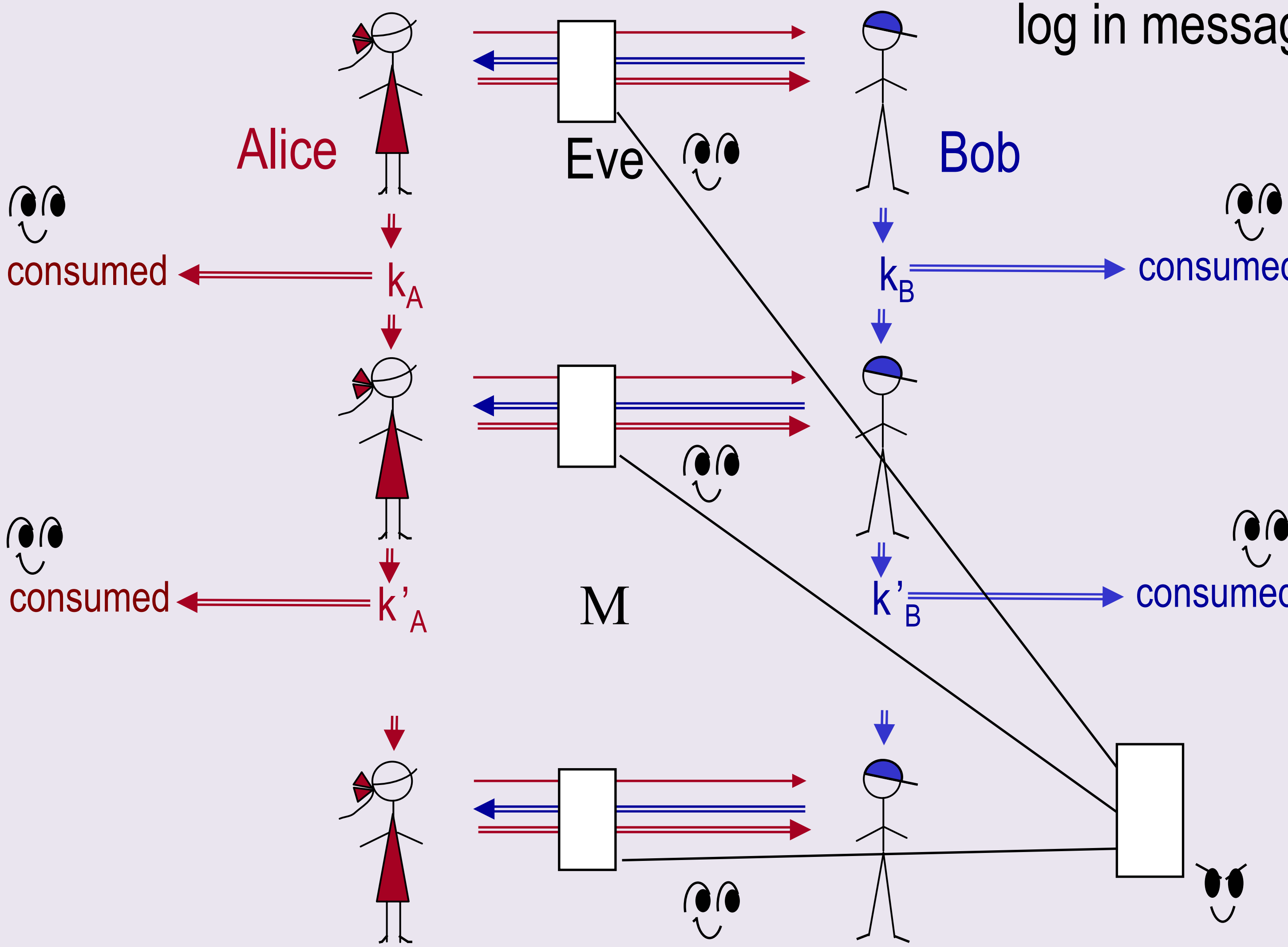


Composability of QKD
(usual security) composable security)

Application 1: Motivation – key degradation of QKD

QKD relies on authentication, authentication relies on sharing a key

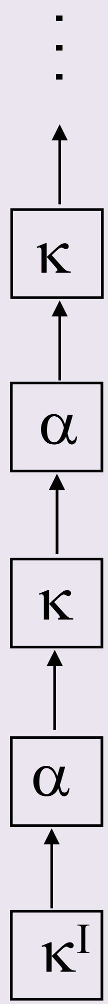
log in message length.



Application 1: Using composability to analyze repeated QKD

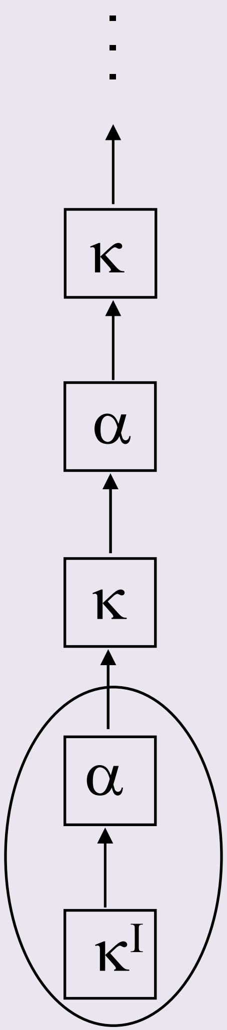
Authentication α Ideal authentication: α^I

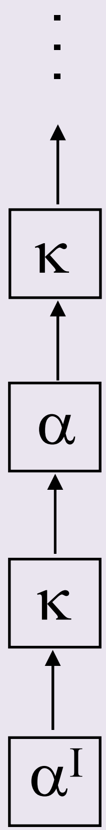
QKD κ Ideal key distribution: κ^I



Application 1: Using composability to analyze repeated QKD

Authentication	α	Ideal authentication: α^I
QKD	κ	Ideal key distribution: κ^I



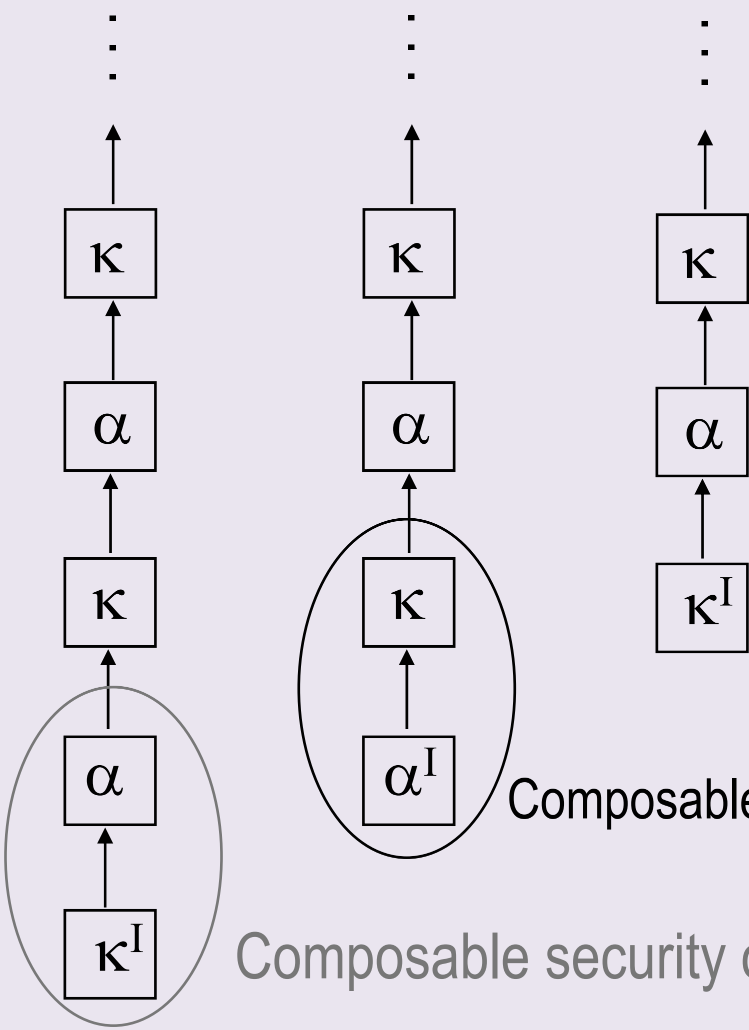


Composable security of auth (using perfect key) known classically

Application 1: Using composability to analyze repeated QKD

Authentication α Ideal authentication: α^I

QKD κ Ideal key distribution: κ^I



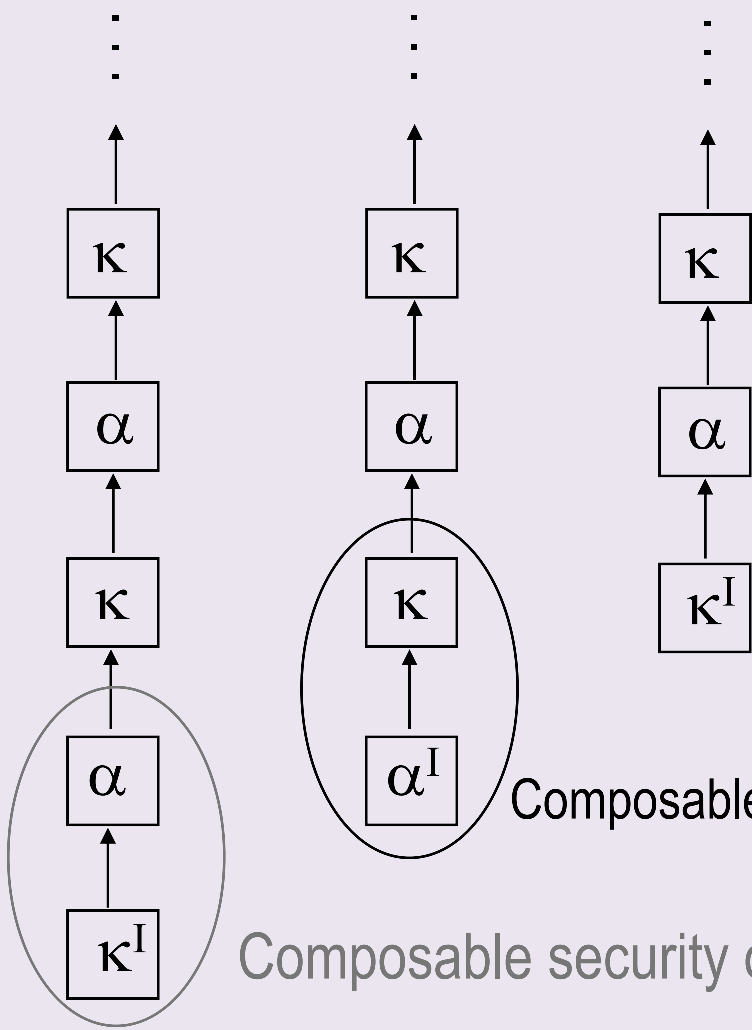
Composable security of QKD (using perfect auth) to be proved

Composable security of auth (using perfect key) known classically

Application 1: Using composability to analyze repeated QKD

Authentication α Ideal authentication: α^I

QKD κ Ideal key distribution: κ^I



In particular, if $\alpha(\kappa^I)$ ε_1-s.r. α^I,

$\kappa(\alpha^I)$ ε_2-s.r. κ^I,

n repeated QKD is $n(\varepsilon_1+\varepsilon_2)$ secure

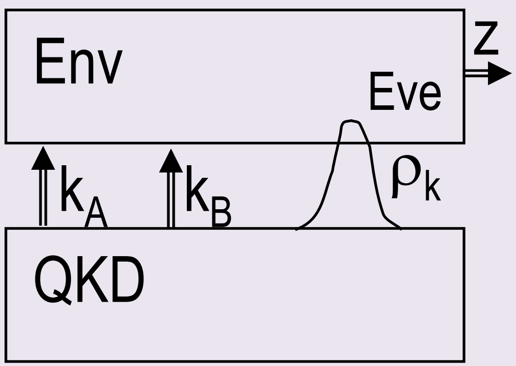
Composable security of QKD (using perfect auth) to be proved

Composable security of auth (using perfect key) known classically

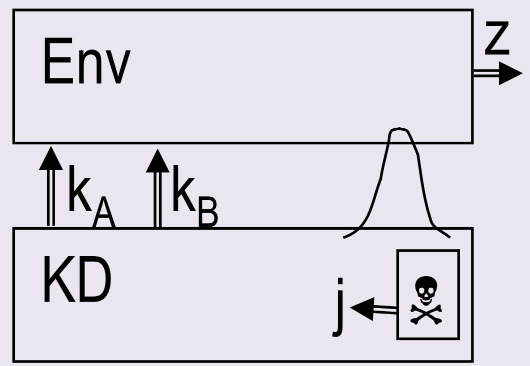
Application 1: Composability of QKD (security of $\kappa(\alpha^I)$)

Auth: α	Ideal auth: α^I
QKD: κ	Ideal KD : κ^I

QKD $\kappa(\alpha^I)$



Ideal KD : κ^I

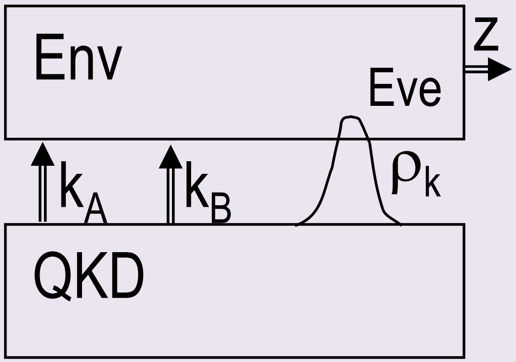


Real vs Ideal

Auth: α	Ideal auth: α^I
QKD: κ	Ideal KD : κ^I

Application 1: Composability of QKD (security of $\kappa(\alpha^I)$)

QKD $\kappa(\alpha^I)$



If QKD fails, $k_A = k_B = F$

else, $k_A \approx k_B = k \in \{0,1\}^{\otimes m}$

$p_k \approx 2^{-m}(1-p_F)$

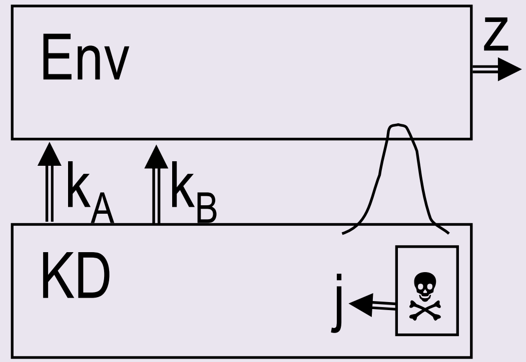
Env sees:

$$\rho_{QKD} = \Sigma_k \, p_k \, |k\rangle\langle k| \otimes \rho_k + p_F \, |F\rangle\langle F| \otimes \rho_F$$

Eve (Env) determines

p_k , ρ_k , p_F , ρ_F

Ideal KD : κ^I



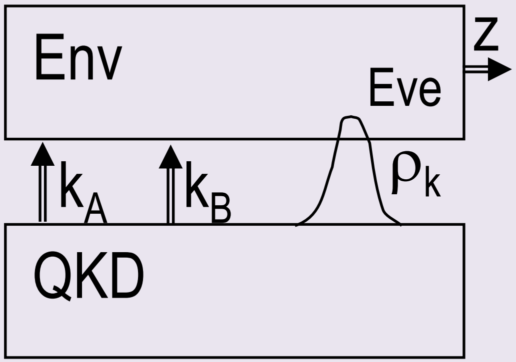
If $j=1$, $k_A = k_B = F$,

else $j=0$, $k_A = k_B = k \in_R \{0,1\}^{\otimes m}$

$p_k = 2^{-m}(1-p_{j=1})$

Application 1: Composability of QKD (security of $\kappa(\alpha^I)$)

QKD $\kappa(\alpha^I)$



If QKD fails, $k_A = k_B = F$

else, $k_A \approx k_B = k \in \{0,1\}^{\otimes m}$

$p_k \approx 2^{-m}(1-p_F)$

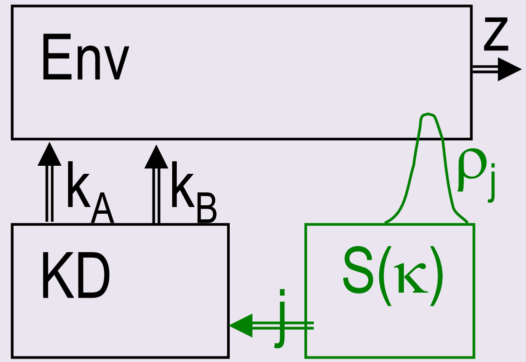
Env sees:

$$\rho_{QKD} = \Sigma_k \, p_k \, |k\rangle\langle k| \otimes \rho_k + p_F \, |F\rangle\langle F| \otimes \rho_F$$

Eve (env) determines

p_k , ρ_k , p_F , ρ_F

Ideal KD : κ^I



Given the Env, we construct simulator $S(\kappa)$, with known p_k , ρ_k , p_F , ρ_F .

If $j=1$, $k_A = k_B = F$, $\rho_j = \rho_F$

else $j=0$, $k_A = k_B = k \in_R \{0,1\}^{\otimes m}$

$p_k = 2^{-m}(1-p_F)$

$\rho_{j=0} = \rho = (1-p_F)^{-1} \, \Sigma_k \, p_k \, \rho_k$

Env sees:

$$\rho_{\kappa^I} = \Sigma_k \, p_k \, |k\rangle\langle k| \otimes \rho + p_F \, |F\rangle\langle F| \otimes \rho_F$$

Auth: α	Ideal auth: α^{I}
QKD: κ	Ideal KD : κ^{I}

Application 1: Composability of QKD (security of $\kappa(\alpha^{\mathrm{I}})$)

Claim: QKD $\kappa(\alpha^{\mathrm{I}})$ ε-s.r. κ^{I} where $\varepsilon = 2^m\, \mathrm{I}_{eve}$

Proof: $|\, \Pr(z=0 \,|\, \mathrm{QKD}) - \Pr(z=0 \,|\, \kappa^{\mathrm{I}}+S(\kappa(\alpha^{\mathrm{I}})))\, |$

$\leq \mathrm{I}_{acc}\,(\{\, \rho_{QKD}\,,\, \rho_{\kappa^{\mathrm{I}}} \}_{equiprobable}\,)$

$\leq 2^{\,m}\, \mathrm{I}(k_E{:}k|\, j)$

Mechanical
"subtle-ss" calculation

where $\mathrm{I}_{acc}\,(\{p_x,\xi_x\,\}) = \max \mathrm{I}(X{:}Y)$
y=outcome of meas ξ_x

$\rho_{QKD} = \Sigma_k\, p_k\, |k\rangle\langle k| \otimes \rho_k + p_F\, |F\rangle\langle F| \otimes \rho_F$

$\rho_{\kappa^{\mathrm{I}}} = \Sigma_k\, p_k\, |k\rangle\langle k| \otimes \rho + p_F\, |F\rangle\langle F| \otimes \rho_F$

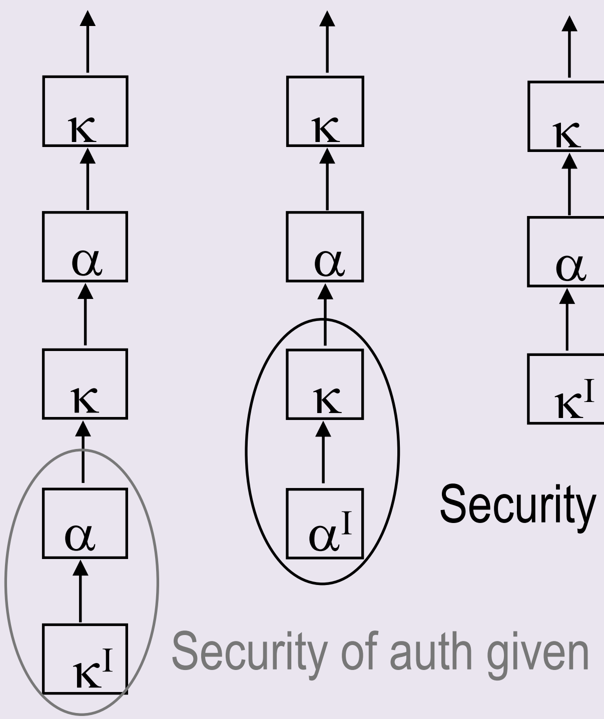
$\mathrm{I}(k_E{:}k|\, j) \approx 2^{-\alpha n}$, n = message size.

NB In many *known* QKD protocols, can bound $\mathrm{I}_{acc}(\{\, \rho_{QKD}\,,\, \rho_{\kappa^{\mathrm{I}}} \}_{equiprob}\,)$ directly (i.e. analyze composable security directly, not in terms of the usual security definition) without 2^m factor.

Punchline

Auth: α Ideal auth: α^I
QKD: κ Ideal KD : κ^I

1. QKD does provide a key that can be safely used in both quantum & classical applications designed to use a perfect key !!!
2. Insecurity of QKD increases only linearly with # repetitions.



If $\alpha(\kappa^I)$ ε_1-s.r. α^I,
$\kappa(\alpha^I)$ ε_2-s.r. κ^I,
n repeated QKD is $n(\varepsilon_1+\varepsilon_2)$ secure

Security of QKD given perfect auth

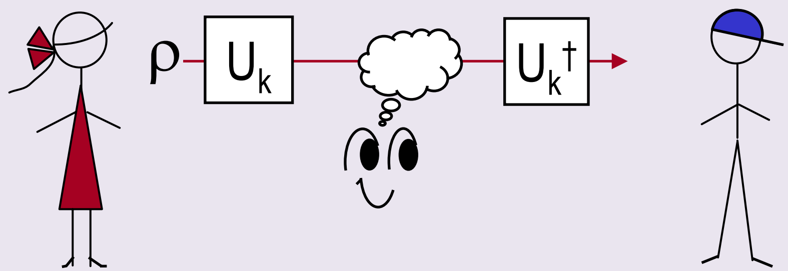
Security of auth given a perfect key

Composability of “Quantum Auth with key recycling”

Application 2: Motivation – key recycling using quantum authentication

Q_{enc} : Quantum encryption (Ambainis, deWolf, Mosca, Tapp 0003101, Boykin, Roychowdhury 0003059)

Encrypts a quantum message by a shared classical key k.



$\forall\rho$, $\Sigma_k\, p_k\, (U_k\, \rho\, U_k^\dagger) = I/2^m$ (e.g. U_k= m-qubit Pauli's)

QA : Quantum-message auth (Barnum, Crepeau, Gottesman, Smith, Tapp 0205128)

Ensure vanishing probability of accepting a fabricated or tampered quantum message, using a classical key.

Application 2: Motivation – key recycling using quantum authentication

Q_{enc} : Encrypts a quantum message by a shared classical key k.
QA : Ensure vanishing prob of accepting a fabricated/tamper quantum message using classical key.

Eavesdropping a quantum state disturbs it.

When performing Q_{enc} , if we further apply QA to the cipher-text, accepting the message in QA *strongly suggests* no eavesdropping, begging possibility to recycle the key – but hard to prove.

Will focus on key recycling of BCGST02.

QA always requires Q_{enc} (BCGST 0205128).

2 pts of view:
"Adding QA to Q_{enc} for key recycling" ≈ *"recycling encryption key in QA."*

Will prove composable security of reuse the encryption key in QA with privacy amplification when QA accepts the message ! ☺

Application 2: Composability of “QA (BCGST02) with key reusing”

1. Review BCGST02 (& scenario).
2. Show composable security of BCGST02 is equiv to that of TQA, another authentication protocol based on teleportation.

   (Similar equivalence for the usual security was used in BCGST02).
3. Prove composable security of TQA.

Bonus material:

1. Quantum authentication of pure states for half the price.
2. On the lower bound of key size of quantum authentication

Application 2: Scenario for QA & key recycling

What is available to Alice & Bob in BCGST02:

1. Classical key
2. Insecure quantum channel
3. Forward classical channel (from Alice to Bob) (WLOG authenticated)
4. No back communication – noninteractive
   - 2-way classical comm + quantum comm $\Rightarrow$ QKD
   - applications to authenticate quantum storage

Here we allow a little back classical comm – necessary in key recycling – to inform Alice whether the key is successfully recycled or not.

OK Θstill rule out QKD & applies to quantum storage.

Application 2: Review of BCGST02

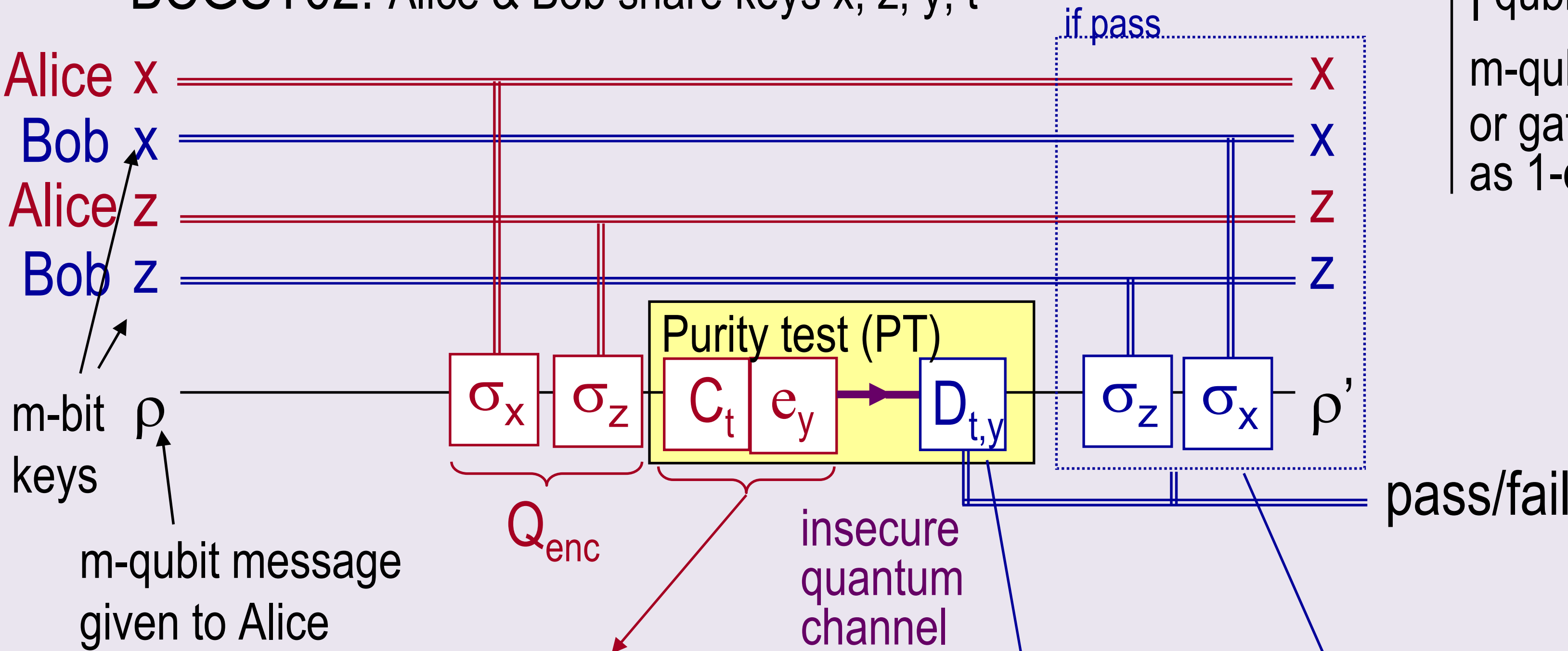
BCGST02: Alice & Bob share keys x, z, y, t

$\rightarrow$ time

$=$ bits

| qubits

m-qubit states or gates drawn as 1-qubit



Encode with q. code C_t , obtain (m+s)-qubit state, add syndrome y. [t,y≈s-bit, s<<m.].

Decode & meas syndrome y ' according to C_t .

If y ≠ y ', outputs "fail", and $|0\rangle\langle 0|$

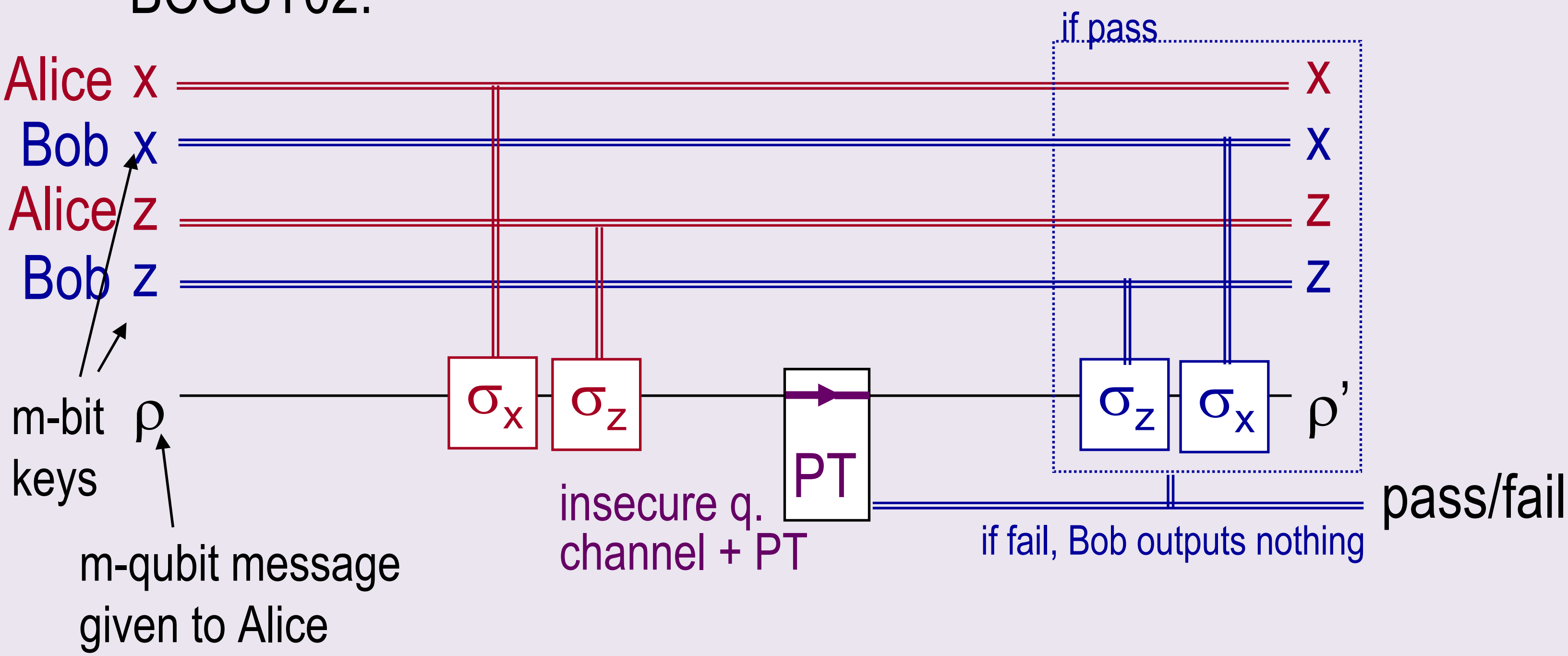
If y = y ', outputs "pass"

If pass PT, decode & output

$$\rho_{out} = \rho' \otimes |pass\rangle\langle pass| + |0\rangle\langle 0| \otimes |fail\rangle\langle fail|$$

Application 2: Review of BCGST02

BCGST02:

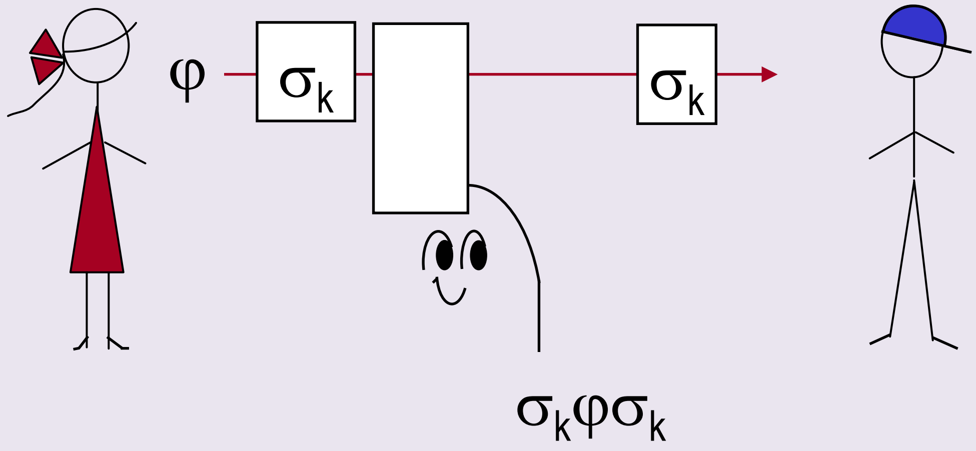


$$\rho_{out} = \rho' \otimes |pass\rangle\langle pass| + |0\rangle\langle 0| \otimes |fail\rangle\langle fail|$$

Security (pure ρ for simplicity):

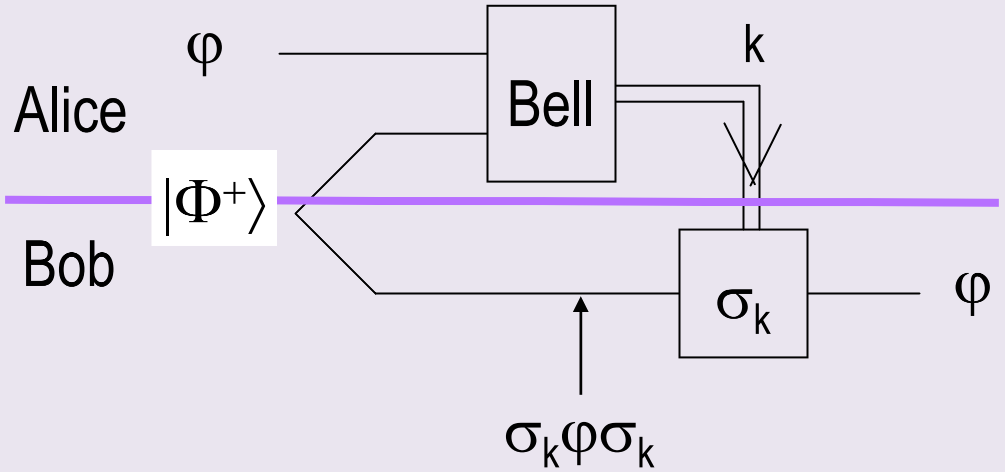
$$\mathrm{Tr}\,[\,\rho_{out}\ \ (\rho \otimes |pass\rangle\langle pass| + \mathrm{I} \otimes |fail\rangle\langle fail|)\,] \geq 1-\varepsilon\ ,\quad \varepsilon = 2^{-(s-1)}\,(m+s)\,/\,s\ .$$

Q_{enc}

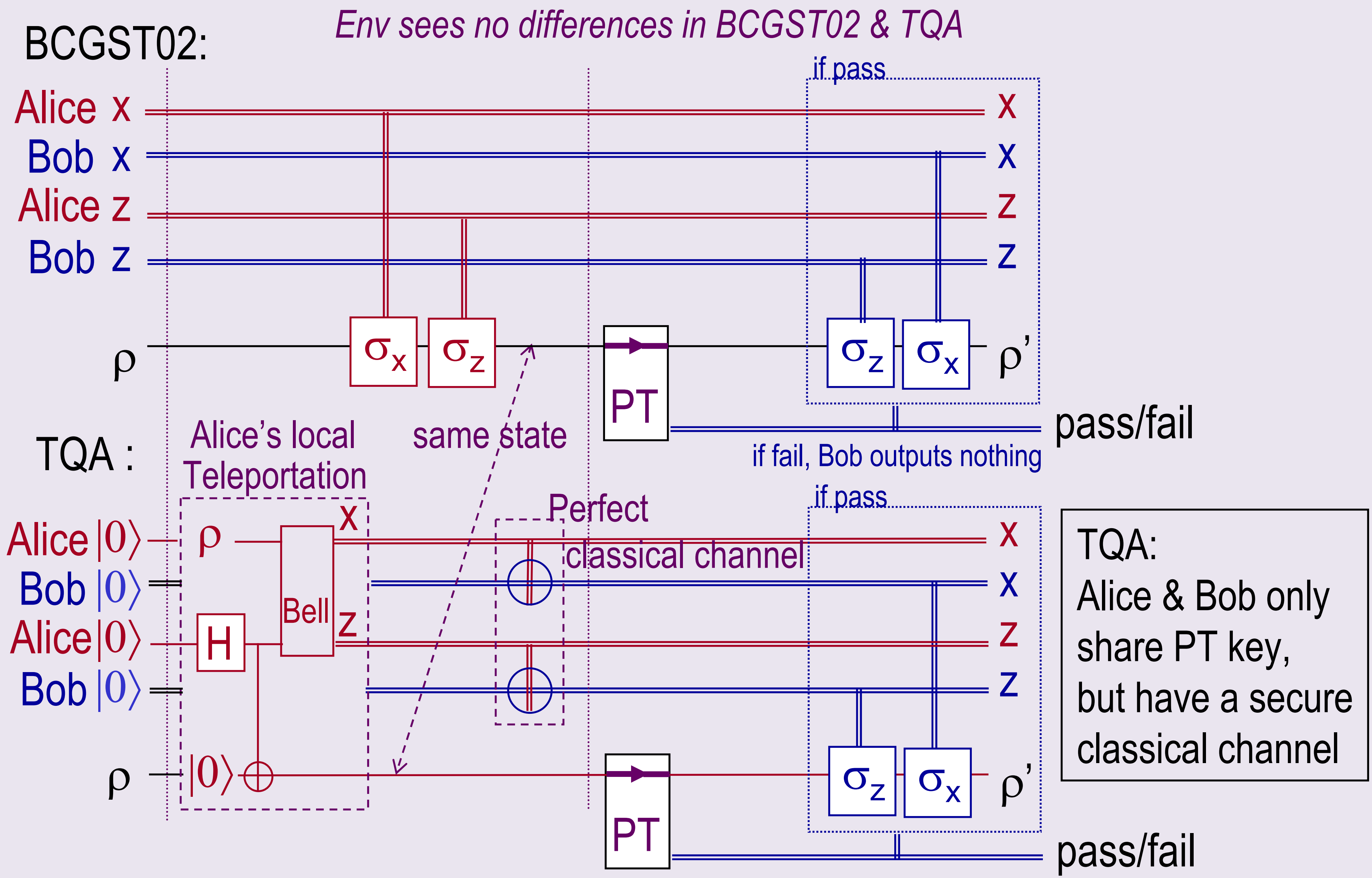


Teleportation

BBCJPW 93

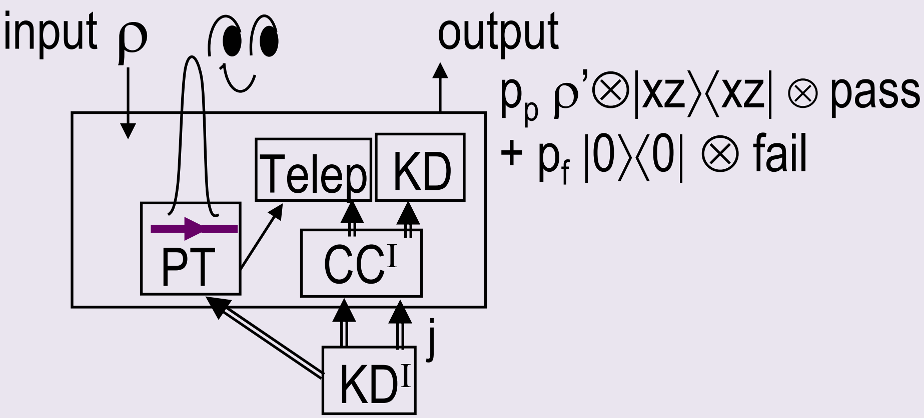


Application 2: Reduction to teleportation with imperfect EPR pairs

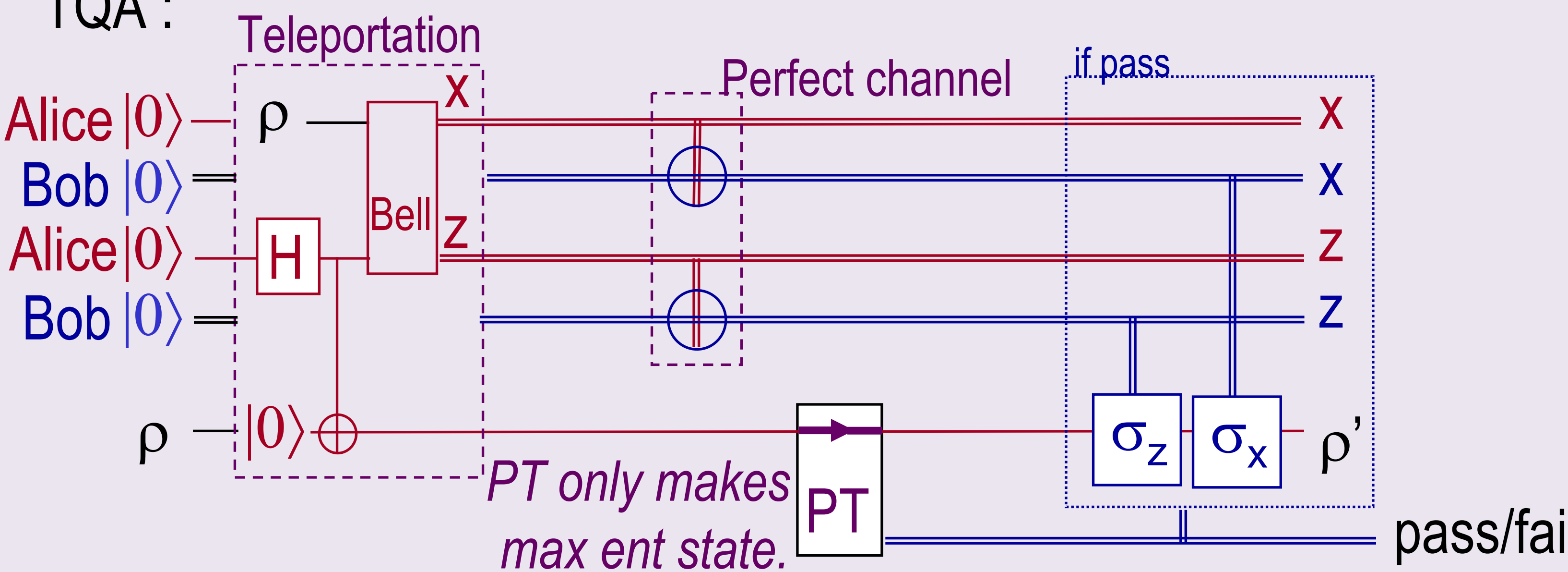


Application 2: Reduction to teleportation with imperfect EPR pairs

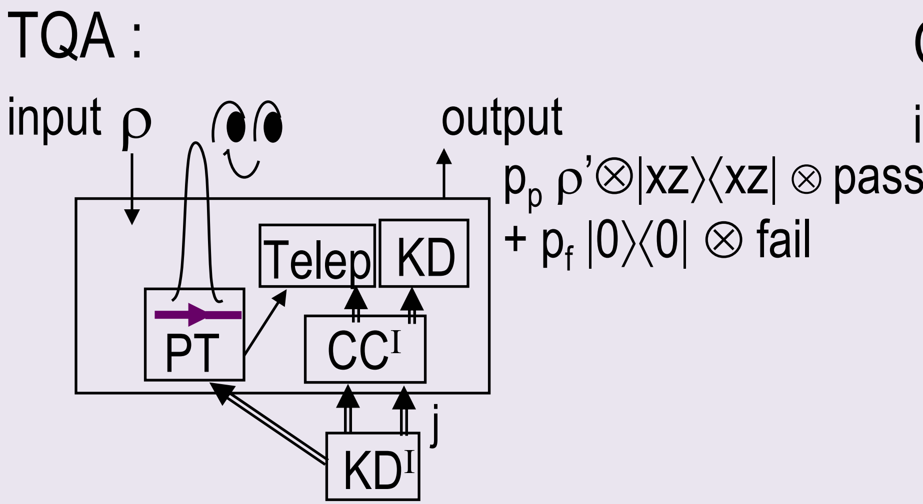
TQA :

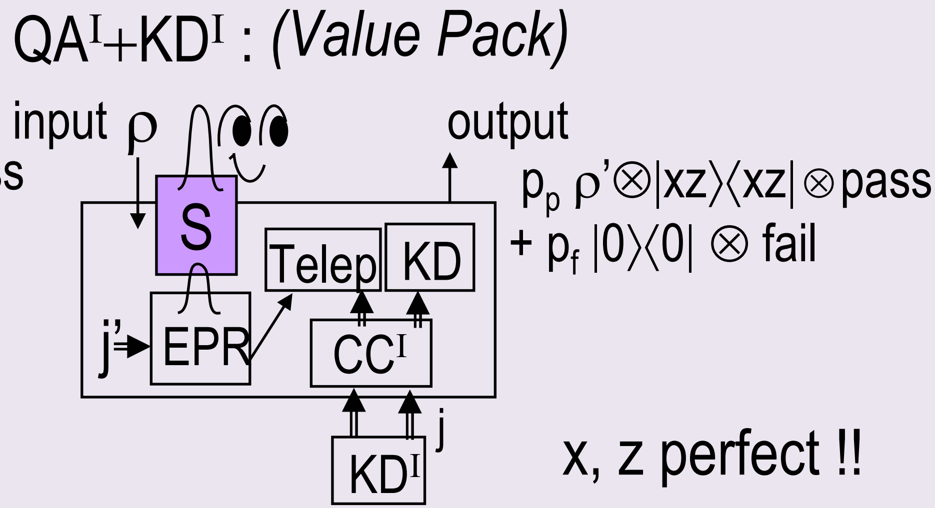


TQA :

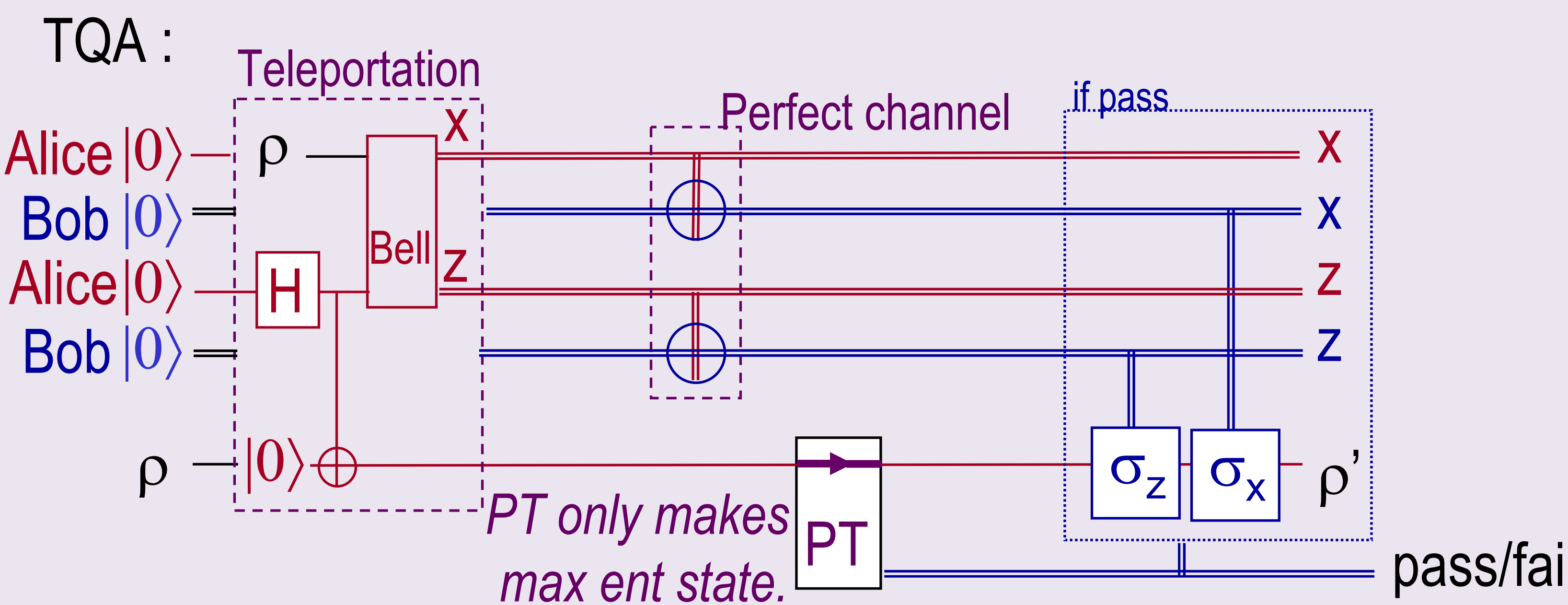


Application 2: Teleportation with imperfect vs perfect EPR pairs





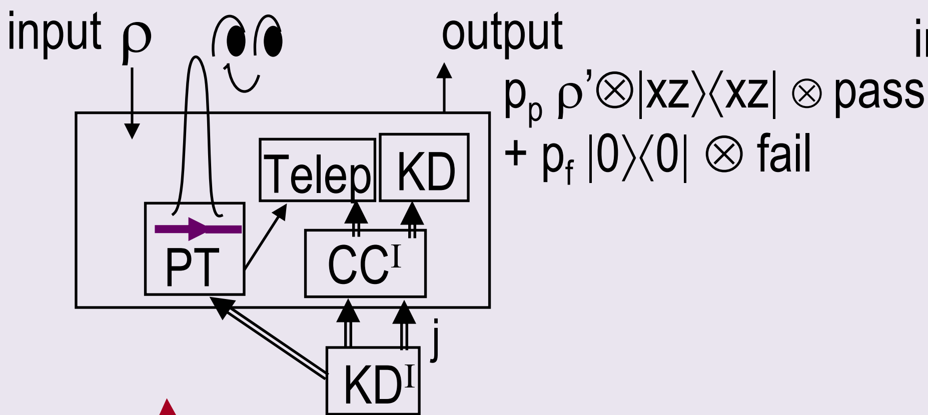
x, z perfect !!



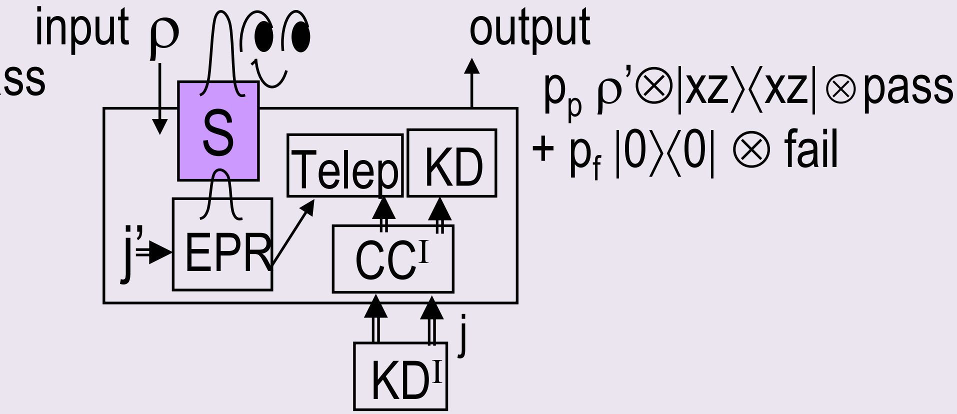
$$| \Pr(z=0|TQA) - \Pr(z=0|QA^I+KD^I) | \le | \Pr(z=0|PT) - \Pr(z=0|EPR) | \le \varepsilon^{1/4}$$

Compos of PT

TQA :

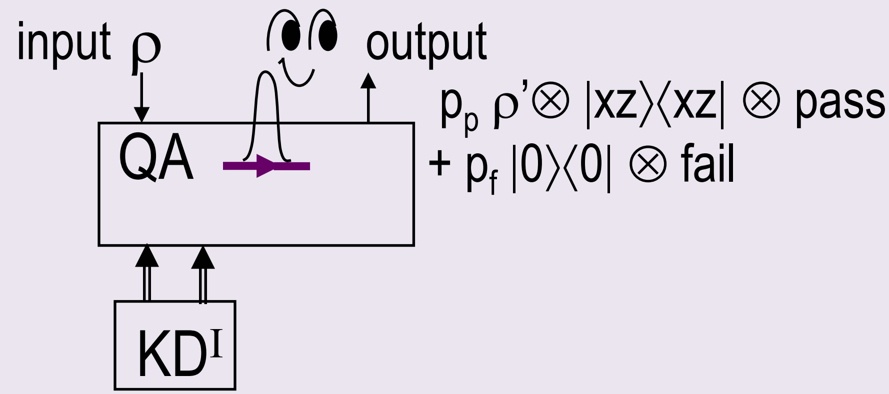


Ideal QA^I+KD^I :



Real

BCGST02:



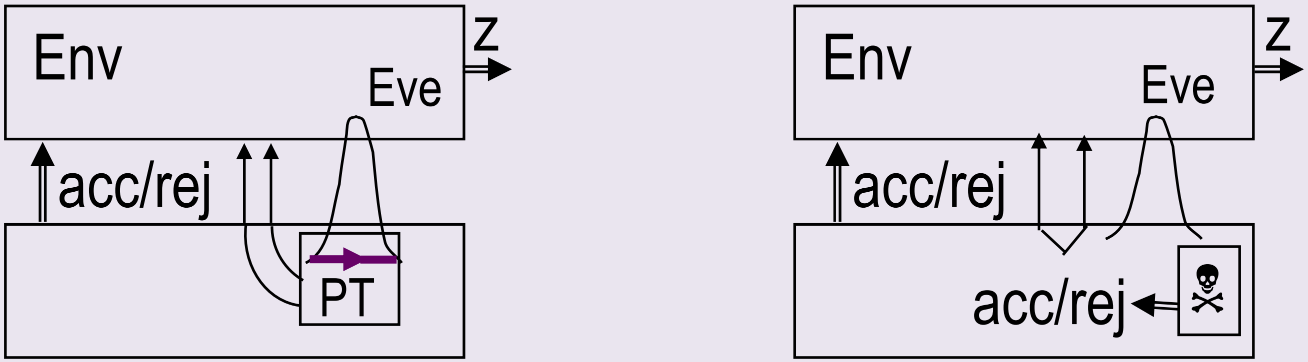
$\Pr(z=0|TQA)$
$= \Pr(z=0|BCGST02)$

Real

Application 2: Composability of PT

EPR from PT

Ideal EPR : Φ



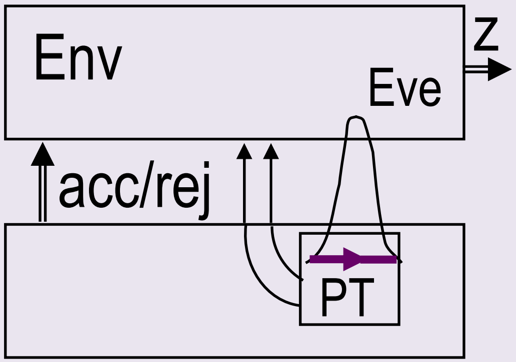
$$\eta^{PT} = p_{acc}\, \rho^{ABE} \otimes \text{acc} + p_{rej}\, |0\rangle\langle 0|^{AB}\, \rho^{E} \otimes \text{fail}$$

$$\mathrm{Tr}\,[\, \mathcal{P}\ \mathrm{tr}_E(\eta^{PT})\,] \geq 1-\varepsilon$$

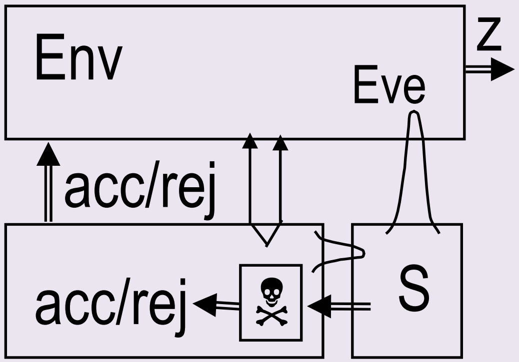
for $\mathcal{P} = \Phi^{AB} \otimes \text{acc} + I^{AB} \otimes \text{fail}$

Application 2: Composability of PT

EPR from PT



Ideal EPR : Φ



$$\eta^{PT} = p_{acc}\, \rho^{ABE} \otimes \text{acc} + p_{rej}\, |0\rangle\langle 0|^{AB}\, \rho^{E} \otimes \text{fail}$$

$$\eta^{EPR} = p_{acc}\, \Phi^{AB}\, \rho^{E} \otimes \text{acc} + p_{rej}\, |0\rangle\langle 0|^{AB}\, \rho^{E} \otimes \text{fail}$$

$$\left.\begin{array}{l} \mathrm{Tr}\,[\, \mathcal{P}\ \mathrm{tr}_E(\eta^{PT})\,] \geq 1-\varepsilon \\ \text{for } \mathcal{P} = \Phi^{AB} \otimes \text{acc} + I^{AB} \otimes \text{fail} \end{array}\right\}$$

$$|\, \Pr(z=0|PT) - \Pr(z=0|EPR)\, | \leq \mathrm{Tr}|\, \eta^{PT} - \eta^{EPR}\, | \leq \varepsilon^{1/4}$$

Bonus materials: Lower bounds for QA & pure state authentication

Q_{enc} : $\forall \rho$, $\Sigma_k \, p_k \, (U_k \, \rho \, U_k^\dagger) = I/2^m$
key size $\geq$ 2m bits (ADMT00, BR00)

QA implies Q_{enc} : (BCGST02)
key size $\geq$ 2m bits

NB Encryption key (2m bits) >> PT key (2s bits, s $\approx$ log(1 / ε))
The main cost of QA, the encryption key is only “catalytic.”

Approx Pure state

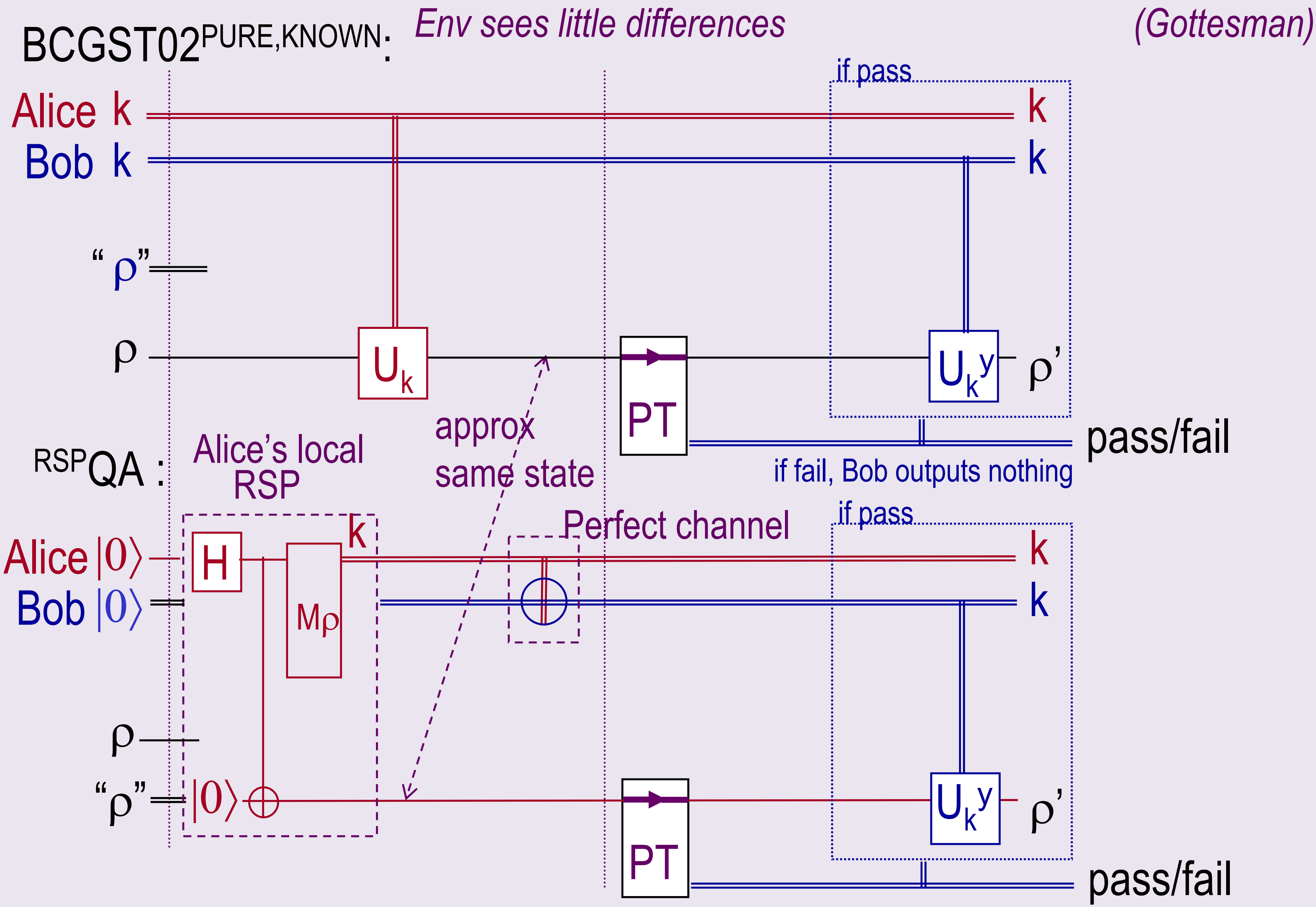
APQ_{enc} : $\forall |\varphi\rangle \, \| \, (1/n) \, \Sigma_k \, U_k \, |\varphi\rangle\langle\varphi| \, U_k^\dagger - I/2^m \, \|_\infty \leq \varepsilon/2^m$
key size $\approx$ m + o(m) bits (Hayden, Leung, Shor, Winter 0307104)

$APQ_{enc} \leftrightarrow$ Remote state preparation

$Q_{enc} \leftrightarrow$ Teleportation

Can we replace Q_{enc} in BCGST02 by APQ_{enc} securely?

Application 2: Reduction to teleportation with imperfect EPR pairs



Conclusion

Composability – gives a prescription for organizing our security proofs into components, each simple and well-defined.

To achieve composable security, we find out what will make the proof work – it is a systematic method to select secure variations.

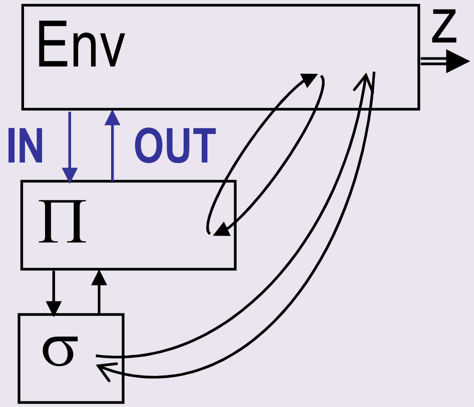
QKD & BCGST02 work better than we thought.
How do the difficulties disappear? (We have j

Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I
then $\Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

Proof:

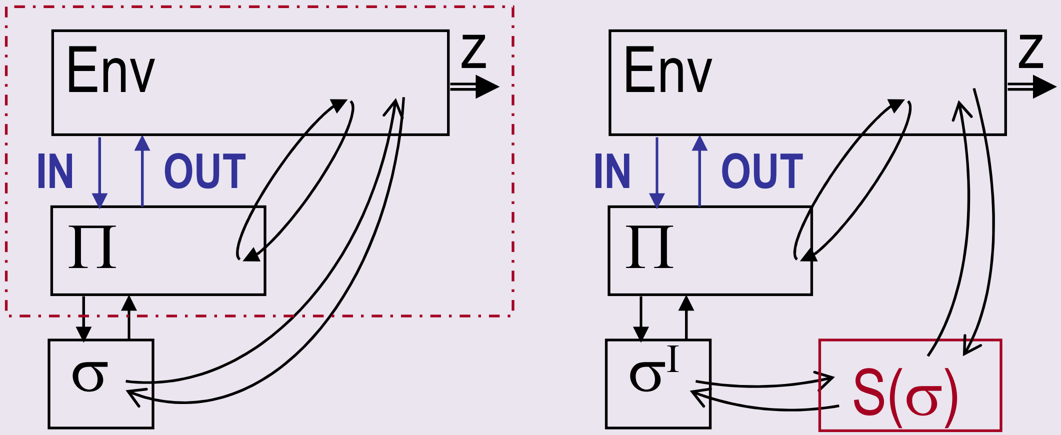


Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I
then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

Proof:



σ ε_2-s.r. σ^I

$$\underbrace{\Pr(z=0 \mid \Pi(\sigma)) \qquad\qquad \Pr(z=0 \mid \Pi(\sigma^I))}_{\text{differ by } \leq \varepsilon_2}$$

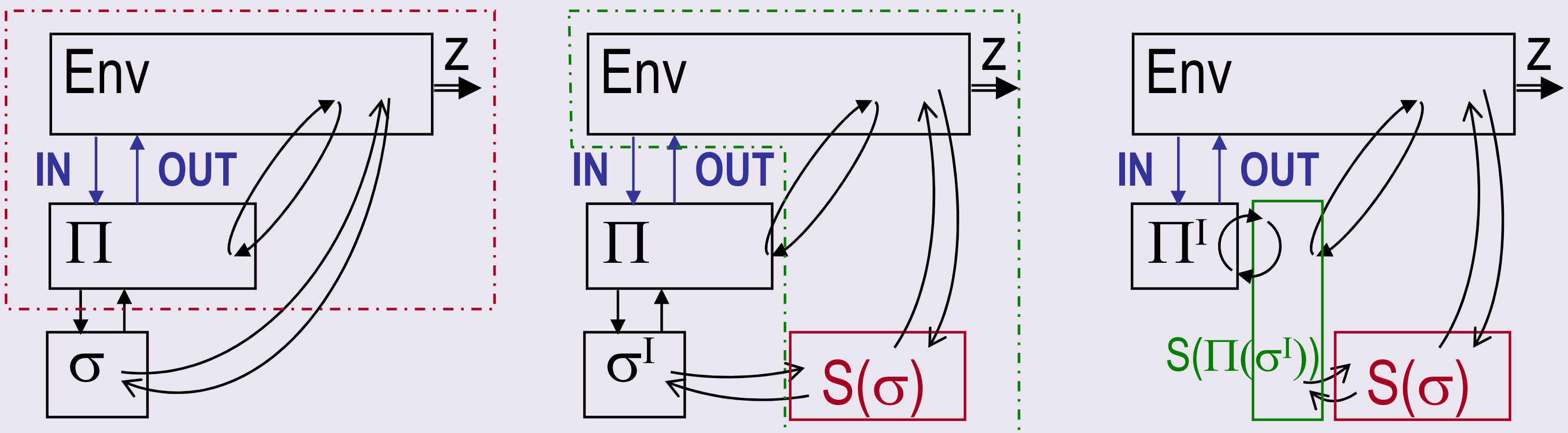
Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I

then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

Proof:



σ ε_2-s.r. σ^I $\qquad$ $\Pi(\sigma^I)$ ε_1-s.r. Π^I

$\Pr(z=0 \mid \Pi(\sigma))$ $\qquad$ $\Pr(z=0 \mid \Pi(\sigma^I))$ $\qquad$ $\Pr(z=0 \mid \Pi^I)$

differ by $\leq \varepsilon_2$ $\qquad$ differ by $\leq \varepsilon_1$

Universal composability theorem (I)

Let $\Pi(\sigma)$ be a real protocol that uses a real subprotocol σ.

If $\quad \Pi(\sigma^I)$ ε_1-s.r. Π^I and σ ε_2-s.r. σ^I

then $\quad \Pi(\sigma)$ $(\varepsilon_1+\varepsilon_2)$-s.r. Π^I .

Proof: