Universal composable security of quantum message authentication with key recycling

w/ Patrick Hayden & Dominic Mayers

:CRC, CFI, ORF, NSERC, CIFAR

Gilbert, MacWilliams, Sloane 74, Wegman, Carter 81,
Stinson 91, Gemmell, Naor 98, ...

Message authentication

- Two communicating parties (sender Alice and receiver Bob)

- Goal: ensure message received is "authentic"
  i.e. neither forged nor altered by an adversary

e.g. In QKD, should authenticate the classical messages between Alice and Bob.

Gilbert, MacWilliams, Sloane 74, Wegman, Carter 81,
Stinson 91, Gemmell, Naor 98, ...

Message authentication

- Two communicating parties (sender Alice and receiver Bob)

- Goal: ensure message received is "authentic"
  i.e. neither forged nor altered by an adversary

- Independent of message encryption

- Requires a key of size sublinear in message size for information theoretic security

- Does not ensure Bob receives the correct message
  Only ensures an altered message is rejected with high prob

Barnum, Crepeau, Gottesman, Smith, Tapp 2002

Quantum message authentication

- Two communicating parties (sender Alice and receiver Bob)
- Goal: ensure message received is "authentic"
  i.e. neither forged nor altered by an adversary
- ~~Independent of message encryption~~ (requires encryption[‡])
- Requires a key of size linear in message size for information theoretic security (Ambainis, Mosca, Tapp, deWolf 00)
- Does not ensure Bob receives the correct message
  Only ensures an altered message is rejected with high prob

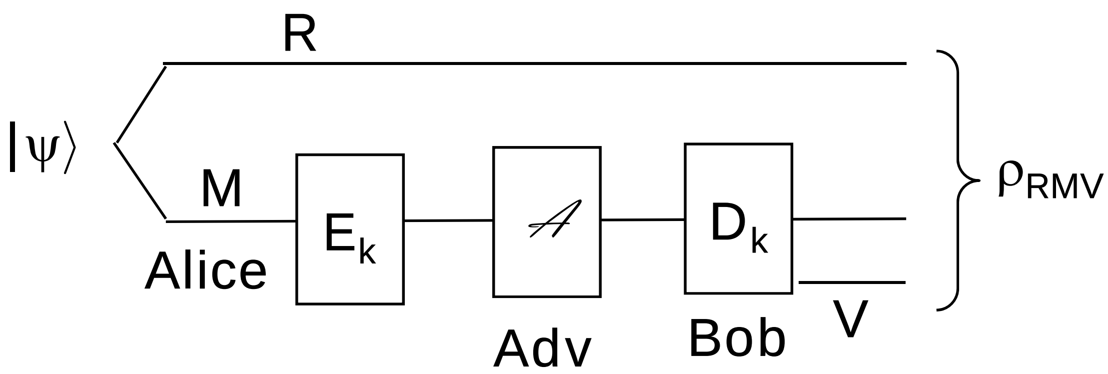
---

‡ If Adv can distinguish $\rho_{|0\rangle}$, $\rho_{|1\rangle}$, a logical Z can go undetected.

Barnum, Crepeau, Gottesman, Smith, Tapp 2002

Quantum message authentication

General noninteractive protocol:



Output $\rho_{RMV} = \sum_k p_k \, I_R \otimes (D_k \mathscr{A} E_k)_M \, (|\psi\rangle\langle\psi|_{RM})$

(Intuitive) Security definition:

Completeness (if $\mathscr{A}$ trival): $\rho_{RMV} = |\psi\rangle\langle\psi|_{RM} \otimes |acc\rangle\langle acc|_V$

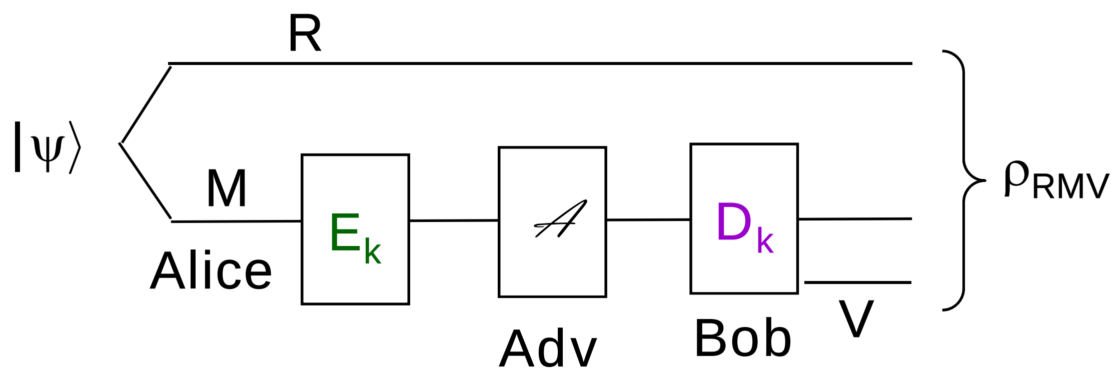
Soundness (for $\mathscr{A}$ arbitrary): $\mathrm{Tr}\,[\rho_{RMV} \times (I - |\psi\rangle\langle\psi|)_{RM} \otimes |acc\rangle\langle acc|_V] \leq \varepsilon$

(in)security parameter

Barnum, Crepeau, Gottesman, Smith, Tapp 2002

Quantum message authentication

The BCGST02 noninteractive protocol (for m-qubit message):



E_k (Alice): encrypts message

encodes encrypted message with random quantum error detecting code + random error syndrome

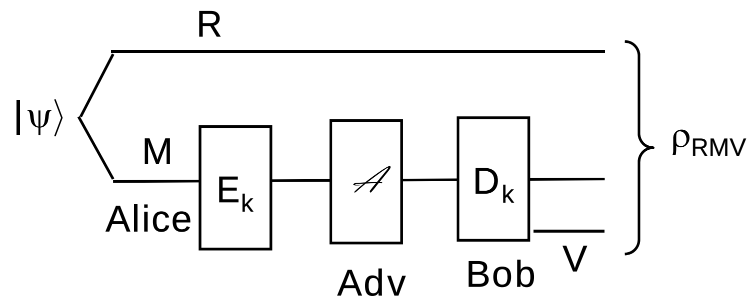
D_k (Bob): decodes. If syndrome correct, accepts and decrypts

Can achieve insecurity parameter ε with:

2m enc key	+	log $(4m/\varepsilon)$ secret syndrome	+	log $(4m/\varepsilon)$ secret code	bits of key

expensive

Idea – key recycling



Adv can only gain information about the key k
from the transmitted state, which is inevitably altered

It's "unlike" "Bob accepts and k compromised"

Recycle the key if Bob accepts ??

Don't take this for granted!

Need to prove the JOINT security of Q-M-Auth and some "protocol-TBD-in-futyre" that reuses the key, against any joint quantum attack …

Natural (and safest) approach:

Prove universal composable (UC) security for the recycled key
(Canetti 00, Ben-Or Mayers 04, Unruh 04, 09)
in the "Adv-bounded-by-QM-only" model.

Recall: once a protocol σ is proven secure in the UC framework (with respect to an idea functionality $\mathcal{F}$), we can replace $\mathcal{F}$ by σ anywhere while preserving security.

e.g. if a QKD protocol using ideal authenticated classical channel is secure, one using a real UC secure classical channel is secure.

Since security of recycled key relies on security of authentication, we consider the UC-security of authentication+key recycling as a combined protocol.

Our contributions (I)

We take the BCGST02 protocol, add a step that if Bob accepts, then reuse the 2m-bit encryption key (in the future) [QA+KG]

We prove UC security for QA+KG. Thus:

(1) key recycling is UC secure, so authentication of quantum messages can consume only sublinear amount of key

---

Recall: BCGST02 achieves insecurity parameter ε with

2m	+	log (4m/ε)	+	log (4m/ε)	bits of key
enc key		secret syndrome		secret code	

Our contributions (I)

We take the BCGST02 protocol, add a step that if Bob accepts, then reuse the 2m-bit encryption key (in the future) [QA+KG]

We prove UC security for QA+KG. Thus:

(1) key recycling is UC secure, so authentication of quantum messages can consume only sublinear amount of key

(2) protocol by BCGST02 is UC secure

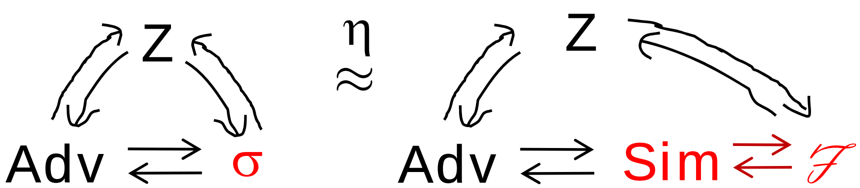
(3) quantum encryption can be made UC secure & consuming sublinear amount of key, by adding secret error detecting codes are used (our initial motivation).

Proof sketch (I):

Universal composability:

UC security definition

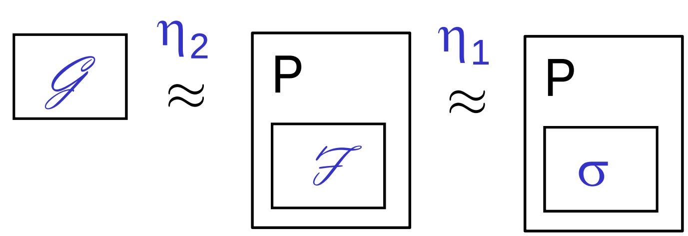
σ η-s.r. $\mathscr{F}$ iff
$\forall$Adv $\exists$Sim $\forall$Z (output 1-bit Γ)
$|\Pr[\Gamma=1 | \sigma+\text{Adv}+\text{Z}]$
$- \Pr[\Gamma=1 | \mathscr{F}+\text{Sim}+\text{Z}] | \leq \eta$



σ as good as $\mathscr{F}$ (indistinguishable from $\mathscr{F}$) for all Adv & Z

Operational consequence

If σ η_1-s.r.-$\mathscr{F}$ & $P^{\mathscr{F}}$ η_2-s.r.-$\mathscr{G}$
then, P^{σ} $(\eta_1+\eta_2)$-s.r.-$\mathscr{G}$

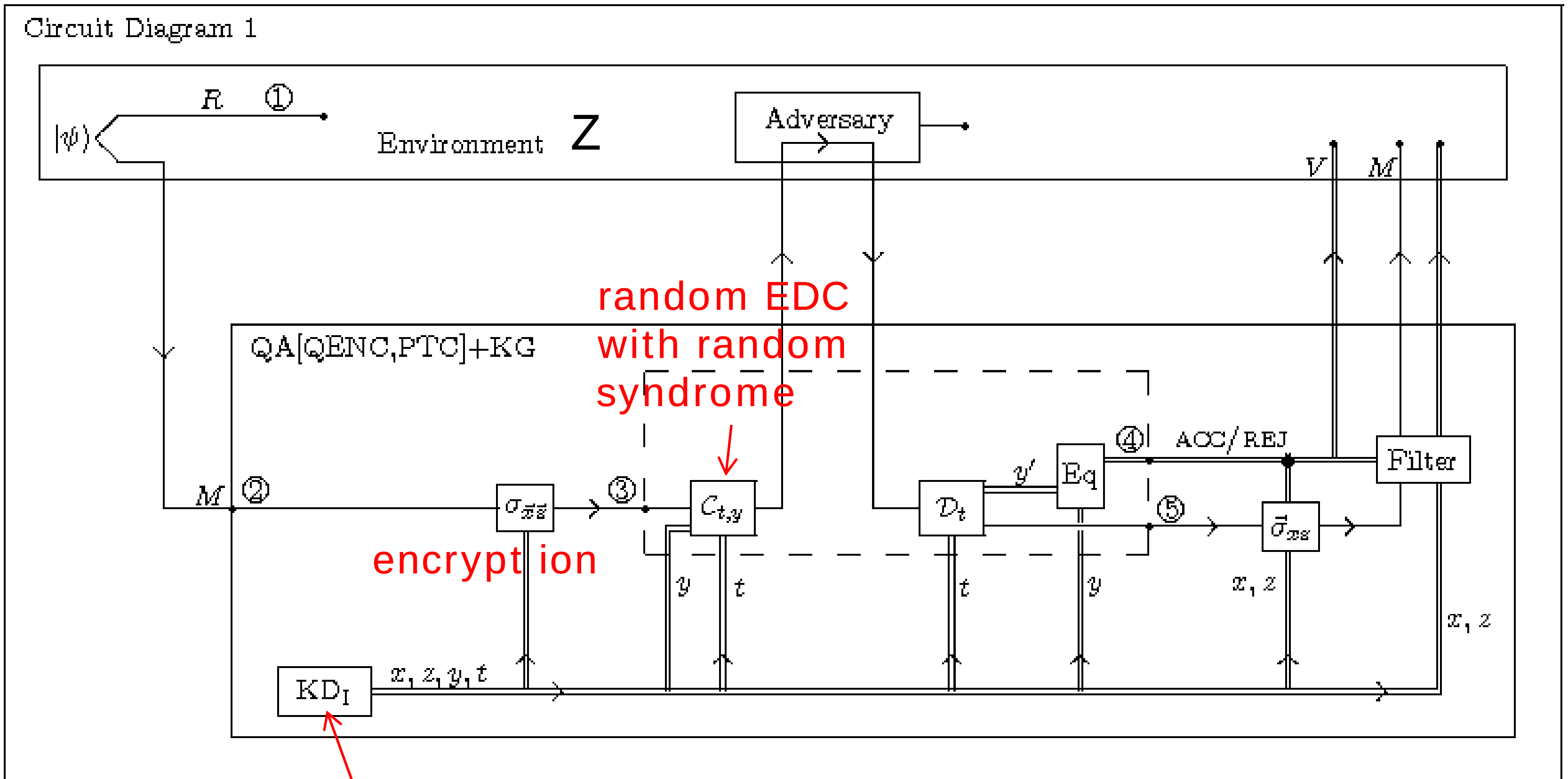


Can replace $\mathscr{F}$ by σ while preserving security.

1st of 3 circuits

Proof sketch (II):

QA+KG (BCGST02 w/ key recycling):



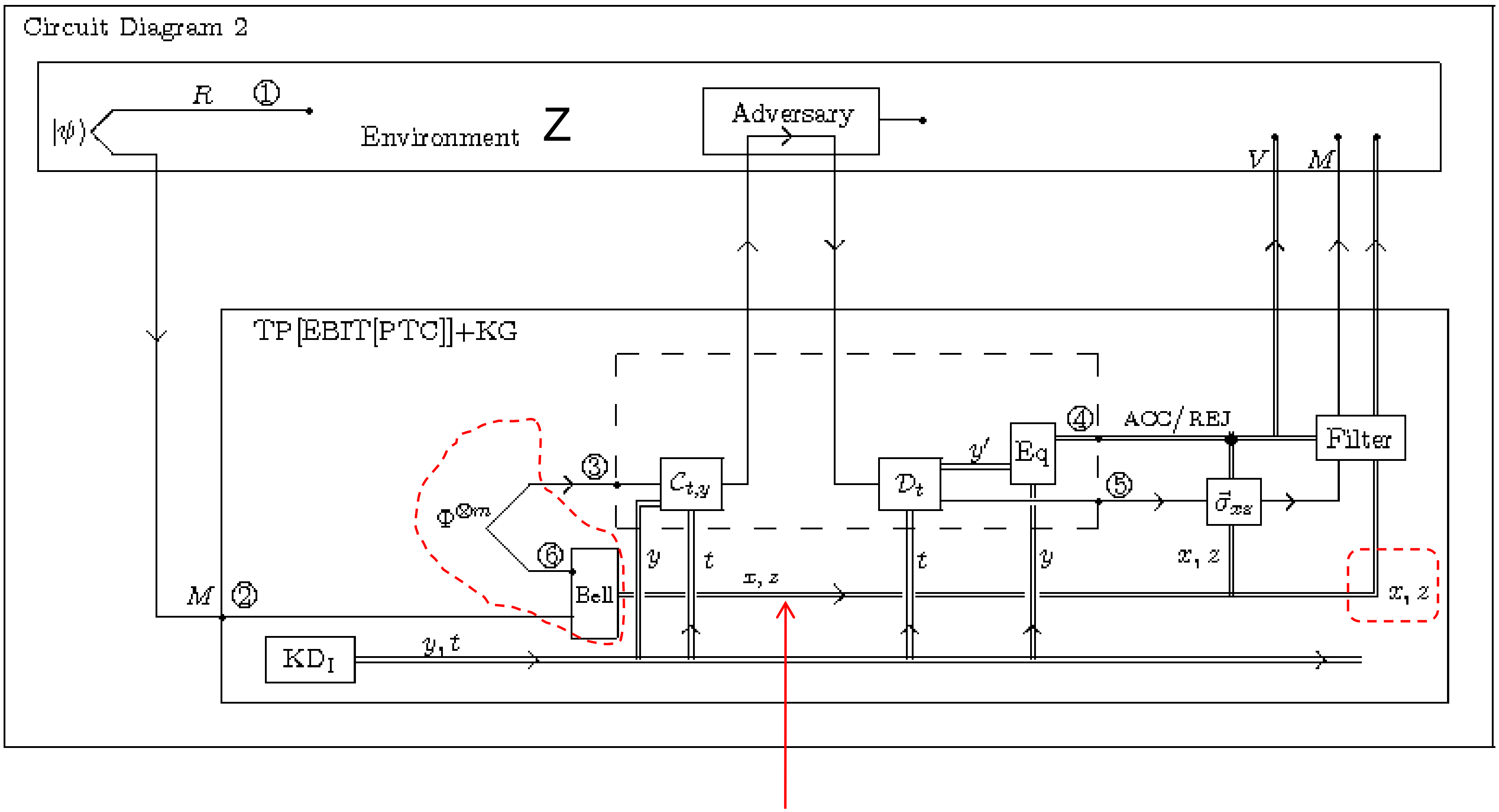
random EDC with random syndrome

encryption

perfect key generating box

Proof sketch (II):

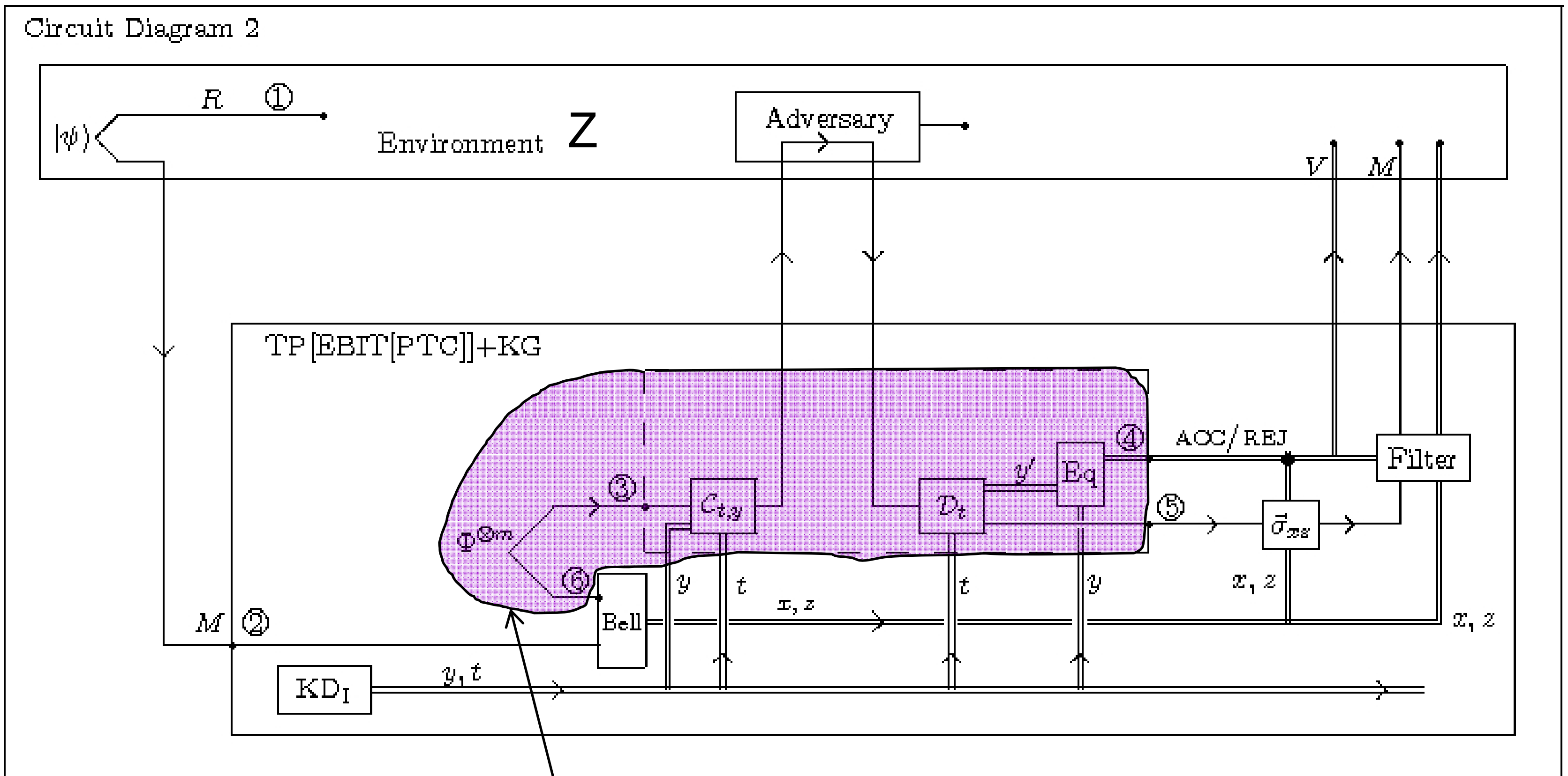
TQA+KG: a protocol indistinguishable from the previous:



perfect, hidden channel

Proof sketch (II):

TQA+KG: a protocol indistinguishable from the previous:



generate entanglement
with insecure channel
and with acc/rej flag

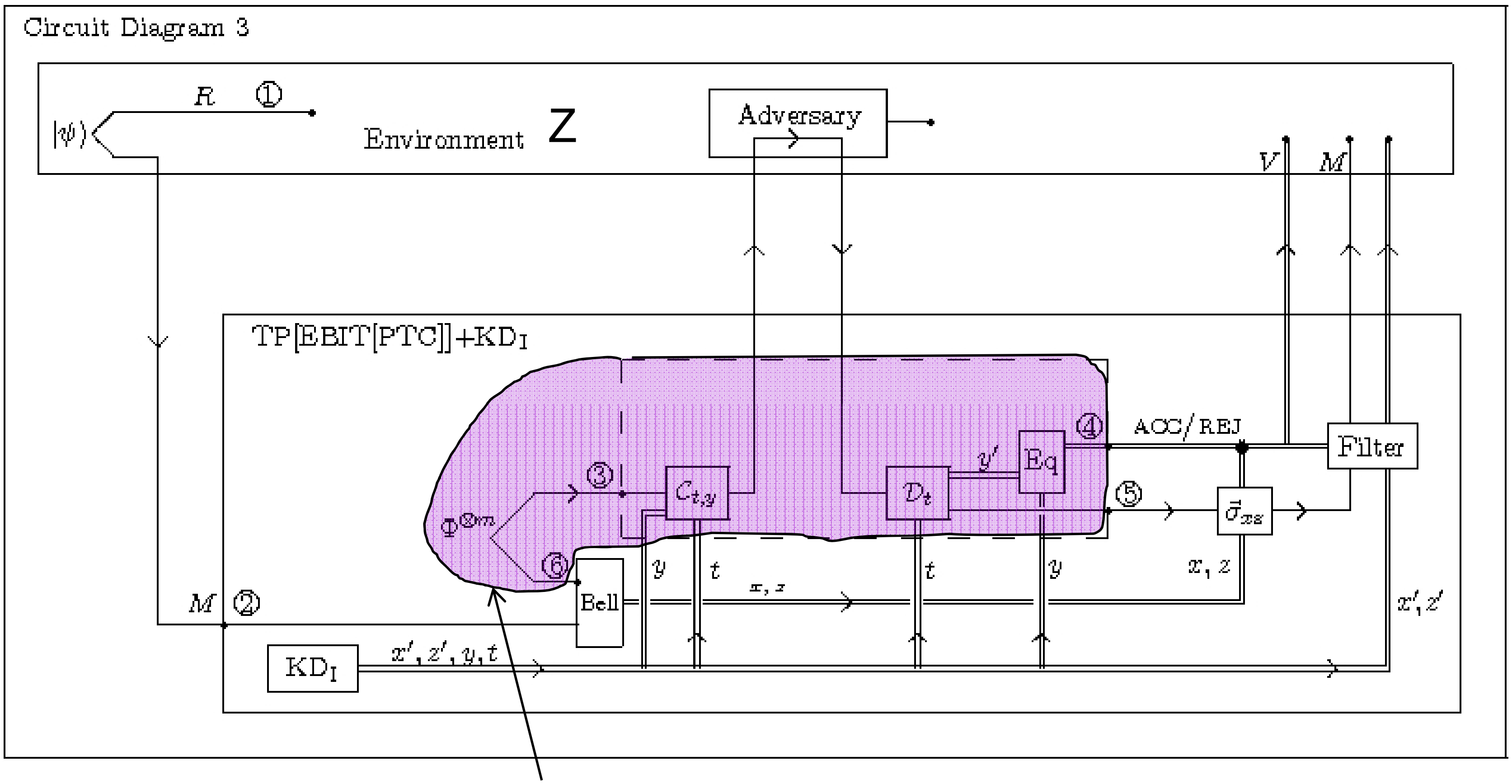
then teleport M
(whether acc/rej)

Proof sketch (II):

3rd of 3 circuits

TQA+KD$_I$: this one has ideal key instead

if insecure entanglement is replaced by perfect ebits, 3rd circuit ≈ 2nd.



generate entanglement with insecure channel and with acc/rej flag

then teleport M (whether acc/rej)

Proof sketch (II):

1st circuit | 2nd circuit | 3rd circuit

BCGST02+KG = TQA+KG | TQA+KD_I output ideal key

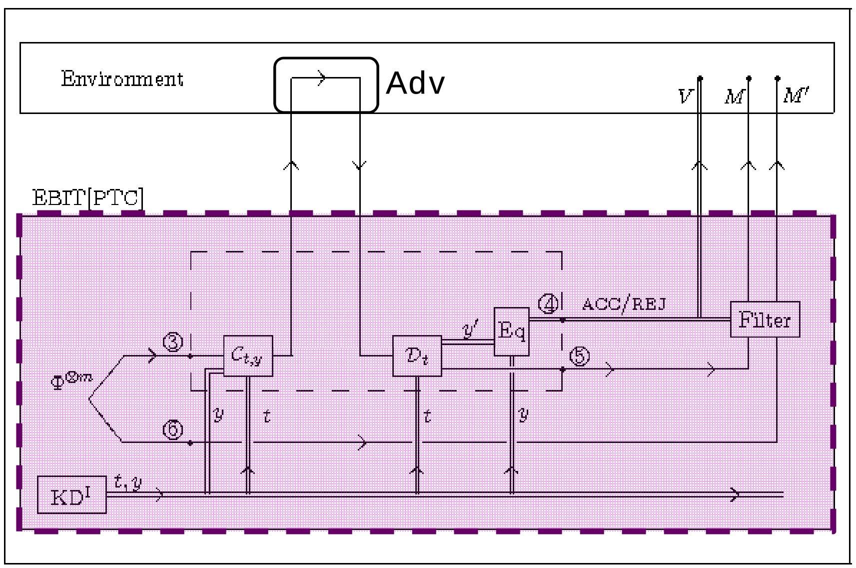
if "ideal entanglement" is used in both,
then they're both indistinguishable from
"ideal channel + ideal key generation"

We prove (directly) UC-security for the purple entanglement generation protocol, with parameter $2\epsilon^{1/3}$ (ϵ relates to key size).

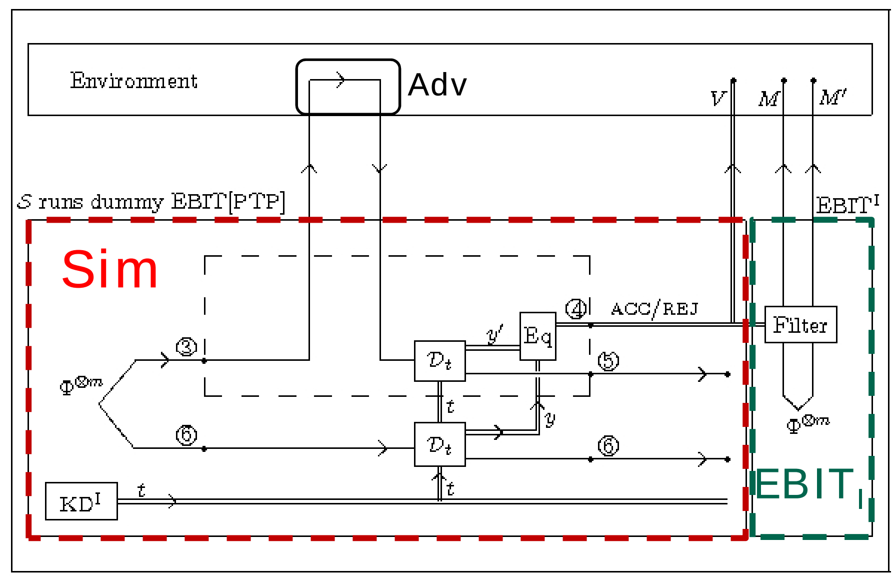
Proof sketch (II):

The "ideal entanglement" $EBIT_I$:
- no input
- interacts with an Adv which says "acc" or "rej"
- output the acc/rej in V to Bob, and MM' to Alice and Bob
  If V=acc, MM' max entangled, if V=rej, MM' max mixed.

The purple box (ebit generation):



$2\varepsilon^{1/3}$
$\approx$



Teleportation using $EBIT_I$ gives a secure erasure channel C_I.

Proof sketch (II):

1st circuit | 2nd circuit | 3rd circuit

BCGST02 + KG = TQA + KG   TQA + KD_I

$\approx 2\varepsilon^{1/3}$ $2\varepsilon^{1/3} \approx$

result

$C_I + KD_I$

Contributions (II)

(4) We defined UC secure ebits and show the “purple” part of BCGST02 produces it.

(5) We showed BCGST02 realizes a UC secure erasure channel.

(6) Can adapt to quantum message authentication via noisy channels (detail to be written up, w/ Anne Broadbent)

(7) UC security implies that BCGST02 is secure against Adv attacking reference R and the protected M jointly!

Other methods, credits, & open problems

- Horodecki and Oppenheim 05: similar intuition to recycle key but security was only proved for a limited adversary.

- No free lunch – though much discounted. Half of our proof structure similar to BCGST02 (surprise?) but knowing what to prove allow us to claim more with less work.

- Key recycling here requires 1 bit of back communication (so that Alice knows acc/rej) before the key is actually reused.

- Alternative: use QKD to generate lots of key for auth, & don't recycle. This takes much less initial key, but twice the quantum comm and rounds of back communication.

- Open problems – Authenticate operations? Partial recycling when message is rejected? Upper/lower bounds of key for classical message authentication in QKD?