Split-State Non-Malleable Codes and Secret Sharing Schemes for Quantum Messages

Rahul Jain

Centre for Quantum Technologies,
School of Computing,
National University of Singapore.

Joint work with Naresh Goud Boddu, Vipul Goyal, and João Ribeiro

December 1, 2024

Outline

Introduction

Non-Malleable Codes (NMCs) [DPW10]

- NMCs encode a message M in a manner such that tampering the codeword results in the decoder either outputting the original message M or a message that is unrelated/independent of M.

- $M \to \mathsf{Enc}(M) \to f(\mathsf{Enc}(M)) \to \mathsf{Dec}(f(\mathsf{Enc}(M))) = M'$.

- $\forall M$, we need $M' \approx_\epsilon p_f M + (1 - p_f)\mathcal{D}_f$, where $p_f, \mathcal{D}_f$ depend only on f (chosen by adversary from family $f \in \mathcal{F}$).

- NMCs can be thought of as a relaxation of error detecting codes.

Non-Malleable Codes (NMCs) [DPW10]

- NMCs encode a message M in a manner such that tampering the codeword results in the decoder either outputting the original message M or a message that is unrelated/independent of M.
- $M \to \mathsf{Enc}(M) \to f(\mathsf{Enc}(M)) \to \mathsf{Dec}(f(\mathsf{Enc}(M))) = M'$.
- $\forall M$, we need $M' \approx_\epsilon p_f M + (1 - p_f)\mathcal{D}_f$, where $p_f, \mathcal{D}_f$ depend only on f (chosen by adversary from family $f \in \mathcal{F}$).
- NMCs can be thought of as a relaxation of error detecting codes.

Non-Malleable Codes (NMCs) [DPW10]

- NMCs encode a message M in a manner such that tampering the codeword results in the decoder either outputting the original message M or a message that is unrelated/independent of M.
- $M \rightarrow \mathsf{Enc}(M) \rightarrow f(\mathsf{Enc}(M)) \rightarrow \mathsf{Dec}(f(\mathsf{Enc}(M))) = M'$.
- $\forall M$, we need $M' \approx_{\epsilon} p_f M + (1 - p_f)\mathcal{D}_f$, where $p_f, \mathcal{D}_f$ depend only on f (chosen by adversary from family $f \in \mathcal{F}$).
- NMCs can be thought of as a relaxation of error detecting codes.

Non-Malleable Codes (NMCs) [DPW10]

- NMCs encode a message M in a manner such that tampering the codeword results in the decoder either outputting the original message M or a message that is unrelated/independent of M.
- $M \to \mathsf{Enc}(M) \to f(\mathsf{Enc}(M)) \to \mathsf{Dec}(f(\mathsf{Enc}(M))) = M'$.
- $\forall M$, we need $M' \approx_\epsilon p_f M + (1 - p_f)\mathcal{D}_f$, where $p_f, \mathcal{D}_f$ depend only on f (chosen by adversary from family $f \in \mathcal{F}$).
- NMCs can be thought of as a relaxation of error detecting codes.

Split-state model

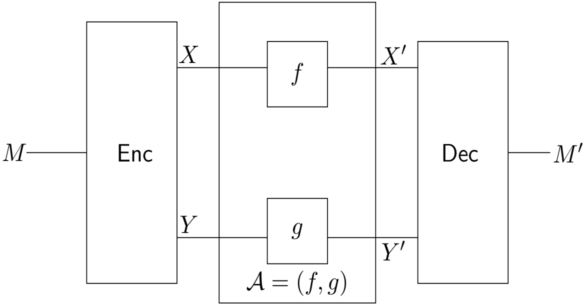


Figure: Split-state model.

Rate of the NMC : $\frac{|M|}{|X|+|Y|}$.

Non-Malleable Randomness Encoder (NMRE) [KOS18]

- "NMRE" can be thought of as a further relaxation of non-malleable codes in the following sense:
  - NMREs output a random message along with its corresponding non-malleable encoding.

Non-Malleable Randomness Encoder (NMRE) [KOS18]

- "NMRE" can be thought of as a further relaxation of non-malleable codes in the following sense:
  - NMREs output a random message along with its corresponding non-malleable encoding.

NMRE in the split-state model

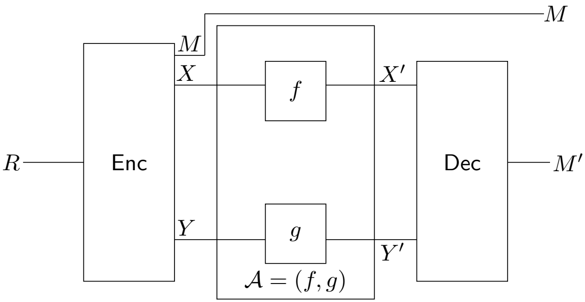


Figure: NMRE in the split-state model.

Rate of the NMRE : $\frac{|M|}{|X|+|Y|}$.

Quantum split-state adversary model [ABJ22]

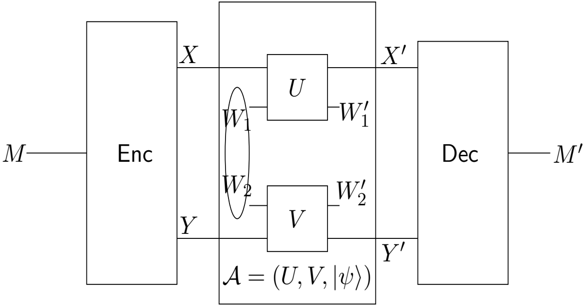


Figure: Quantum split-state adversary model.

Quantum secure NMRE [BBJ23]

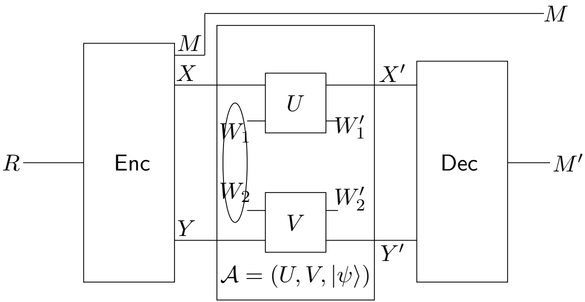


Figure: Quantum secure NMRE.

- NMRE security : $MM' \approx_\varepsilon p_\mathcal{A} MM + (1 - p_\mathcal{A}) M \otimes M'_\mathcal{A}$.

Theorem

There exists a rate $1/2$, 2-split quantum secure NMRE.

Prior work - NMCs in the split-state model

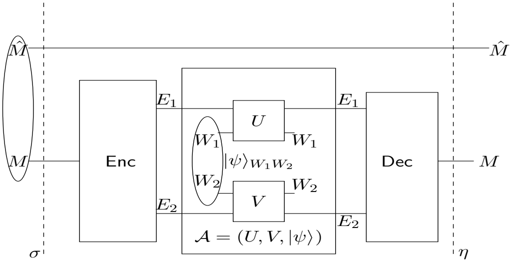
Work by	Rate	Splits	Messages	Adversary
CZ19	$\Omega(1)$	10	classical	classical
KOS18	$1/3$	3	classical	classical
CGL15	$\Omega\left(\frac{1}{\text{poly}(n)}\right)$	2	classical	classical
Li17	$\Omega\left(\frac{1}{\log n}\right)$	2	classical	classical
Li19	$\Omega\left(\frac{\log\log n}{\log n}\right)$	2	classical	classical
AO20	$\Omega(1)$	2	classical	classical
Li23	$\Omega(1)$	2	classical	classical
AKOOS22	$1/3$	2	classical	classical
ABJ22	$\Omega\left(\frac{1}{\text{poly}(n)}\right)$	2	classical	**quantum**

Applications - NMCs

- In construction of non-malleable secret sharing [GK18a, GK18b, ADN+19].
- In construction of non-malleable commitment schemes [GPR16].
- In secure message transmission and non-malleable signatures [SV19].

Results and few technical details

Definition: Quantum NMCs.



- NMC security: $\forall \sigma_M$, we need $\eta_{M\hat{M}} \approx p_{\mathcal{A}}\sigma_{M\hat{M}} + (1-p_{\mathcal{A}})\gamma_M^{\mathcal{A}} \otimes \sigma_{\hat{M}}$.

Quantum NMC with shared key [AM17]

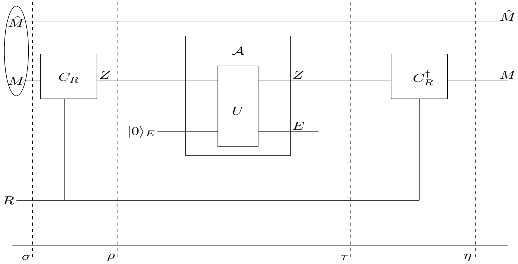


Figure: Quantum NMC with shared key.

- Here, $\{C_r\}_{r \leftarrow R}$ denotes a family of 2-design unitaries.
- Quantum NMC definition from [AM17] is based on mutual information.

3-split quantum NMC

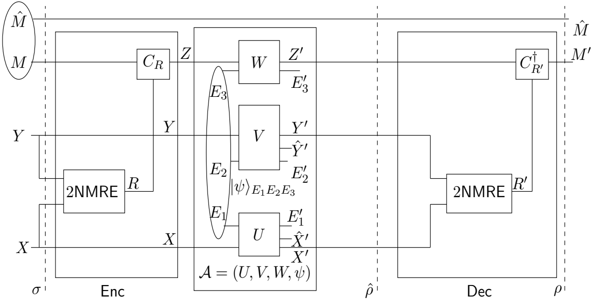


Figure: Rate $1/11$, 3-split quantum NMC.

3-split quantum NMC - High level overview

- Use 2-splits to protect the key R.
- Use the 3rd split to protect the message using 2-design unitaries.
- 1. $R = R'$, security follows from 2-design unitary properties (Pauli mixing and decoupling property).
  2. $RR' = U_R \otimes R'$, security follows from the decoupling property of 2-design unitaries.

3-split quantum NMC - High level overview

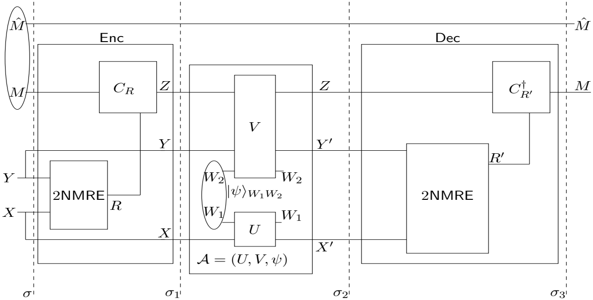
- Use 2-splits to protect the key R.
- Use the 3rd split to protect the message using 2-design unitaries.
- 1. $R = R'$, security follows from 2-design unitary properties (Pauli mixing and decoupling property).
  2. $RR' = U_R \otimes R'$, security follows from the decoupling property of 2-design unitaries.

3-split quantum NMC - High level overview

- Use 2-splits to protect the key R.
- Use the 3rd split to protect the message using 2-design unitaries.
- 1. $R = R'$, security follows from 2-design unitary properties (Pauli mixing and decoupling property).
  2. $RR' = U_R \otimes R'$, security follows from the decoupling property of 2-design unitaries.

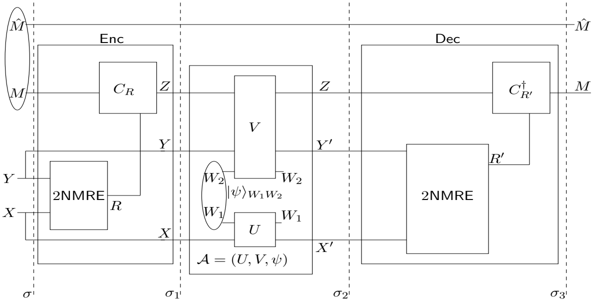
From 3-split to 2-split quantum NMC

- We combine 2-splits as shown below.



From 3-split to 2-split quantum NMC

- Problem: register Z carries information on register R. This implies NMRE security no longer holds.



- Register Z carries no information on R if the input message σ_M is uniform.
- Additionally need - augmented property of 2NMRE.

2-split quantum NMC

Theorem

There exists a rate $1/11$, 2-split quantum NMC for uniform input message.

- Quantum NMC for uniform input message can be thought of as protecting half of maximally entangled state against split-state tamperings.

2-split quantum NMC

Theorem

There exists a rate $1/11$, 2-split quantum NMC for uniform input message.

- Quantum NMC for uniform input message can be thought of as protecting half of maximally entangled state against split-state tamperings.

Threshold non-malleable secret sharing (NMSS) [GK18a]

- Let M be a classical message and $(\mathrm{Share}, \mathrm{Rec})$ be a t-out-of-p secret sharing scheme.
- Let $\mathrm{Share}(M) = (S_1, \ldots, S_p)$.
- Let adversary Adv tamper $(S_1, \ldots, S_p) \rightarrow (S'_1, \ldots, S'_p)$.
- Let $T = \{1, 2, \ldots, t\}$ be an authorized set to reconstruct the message and $M' = \mathrm{Rec}(S'_1, \ldots, S'_t)$.
- **Non-malleable security:** $MM' \approx p_{\mathsf{Adv}} MM + (1 - p_{\mathsf{Adv}}) M \otimes M'_{\mathsf{Adv}}$.

From 2-split NMC to threshold NMSS [GK18a]

Construction from [GK18a] needs the following:

- a 2-split NMC $(\mathrm{2nmShare}, \mathrm{2nmRec})$.
- additionally:
  - a t-out-of-p secret sharing scheme $(\mathrm{Share}, \mathrm{Rec})$.
  - a 2-out-of-p leakage resilient secret sharing scheme $(\mathrm{lrShare}, \mathrm{lrRec})$.

From 2-split NMC to threshold NMSS [GK18a]

Construction from [GK18a] needs the following:

- a 2-split NMC $(\mathrm{2nmShare}, \mathrm{2nmRec})$.
- additionally:
  - a t-out-of-p secret sharing scheme $(\mathrm{Share}, \mathrm{Rec})$.
  - a 2-out-of-p leakage resilient secret sharing scheme $(\mathrm{lrShare}, \mathrm{lrRec})$.

From 2-split NMC to threshold NMSS [GK18a]

Construction from [GK18a] needs the following:

- a 2-split NMC $(\mathrm{2nmShare}, \mathrm{2nmRec})$.
- additionally:
  - a t-out-of-p secret sharing scheme $(\mathrm{Share}, \mathrm{Rec})$.
  - a 2-out-of-p leakage resilient secret sharing scheme $(\mathrm{lrShare}, \mathrm{lrRec})$.

From 2-split NMC to threshold NMSS [GK18a]

Candidate threshold NMSS scheme from [GK18a]:

1. Compute the split-state encoding $(L, R) = \mathrm{2nmShare}(M)$;
2. Apply Share to L to obtain p shares stored in $L_1, \ldots, L_p$;
3. Apply $\mathrm{lrShare}$ to R to obtain p shares stored in registers $R_1, \ldots, R_p$;
4. Form the i-th final share $S_i = (L_i, R_i)$.

From 2-split NMC to threshold NMSS [GK18a]

Candidate threshold NMSS scheme from [GK18a]:

1. Compute the split-state encoding $(L, R) = \mathrm{2nmShare}(M)$;
2. Apply Share to L to obtain p shares stored in $L_1, \ldots, L_p$;
3. Apply $\mathrm{lrShare}$ to R to obtain p shares stored in registers $R_1, \ldots, R_p$;
4. Form the i-th final share $S_i = (L_i, R_i)$.

Reduction from threshold NMSS to 2-split NMC [GK18a]

- Tampering of $R \to R'$ must be performed independent of L.
  - R' depends on $R'_1 R'_2$ which further depend on $L_1 L_2$. But note $L_1 L_2$ information theoretically hides L.

- Tampering of $L \to L'$ must be performed independent of R.
  - L' depends on $L'_1 L'_2 \ldots L'_t$ which further depend on $R_1 R_2 \ldots R_t$. Considering, L'_i as a leakage on R_i, $\mathrm{lrShare}$ property implies now L' is independent of R.

- Overall, they identify random variables $LL'ERR'$ such that
  - $L \otimes E \otimes R$
  - $L'L \leftrightarrow E \leftrightarrow RR'$

Analogous reduction for quantum messages

- Tampering $R \to R'$ is independent of L.
  - Analogous to the classical setting.
- Tampering $L \to L'$ is independent of R.
  - Realizing this argument in the quantum setting requires **"augmented"** leakage-resilient secret sharing scheme.
- We cannot identify registers $LL'ERR'$ such that
  - $L \otimes E \otimes R$
  - $L'L \leftrightarrow E \leftrightarrow RR'$

Theorem

*Using 2-split quantum NMC, quantum secret sharing scheme and **augmented** leakage resilient secret sharing scheme (instead of classical schemes) in the GK18a threshold NMSS scheme gives us the threshold quantum NMSS scheme.*

Difficulty in the quantum setting

- $\{X \otimes E \otimes Y\}$ and adversary modifies $(E, X) \to (E, X, X')$ and $(E, Y) \to (E, Y, Y')$.
  1. When adversary is classical, we have $XX' \leftrightarrow E \leftrightarrow YY'$.
  2. When adversary is quantum, above Markov chain may not be true.

Conclusion and open questions

Improved NMCs

Constant rate 2-split NMCs

- Can we design (worst-case) split-state NMCs for quantum messages with a constant rate? This is open even for classical messages against quantum adversaries with shared entanglement.

Constant rate NMSS schemes

Can we construct (worst-case) split-state NMSS schemes for quantum messages with a constant rate?

NMSS schemes against joint tamperings

- Can we design NMSS schemes for quantum messages that are secure against joint tampering of shares?

Final slide

That's all from my end! Any questions ?