Quantum Garbled Circuits

Zvika Brakerski
Weizmann

Henry Yuen
Columbia

arxiv.org/abs/2006.01085

European Research Council
Established by the European Commission

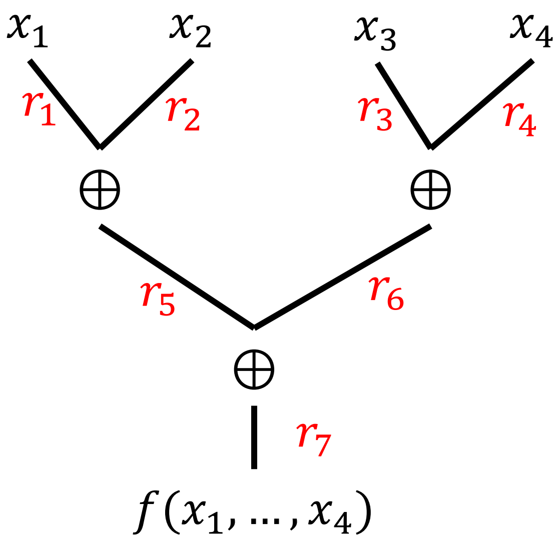
Randomized Encoding (RE) & Garb

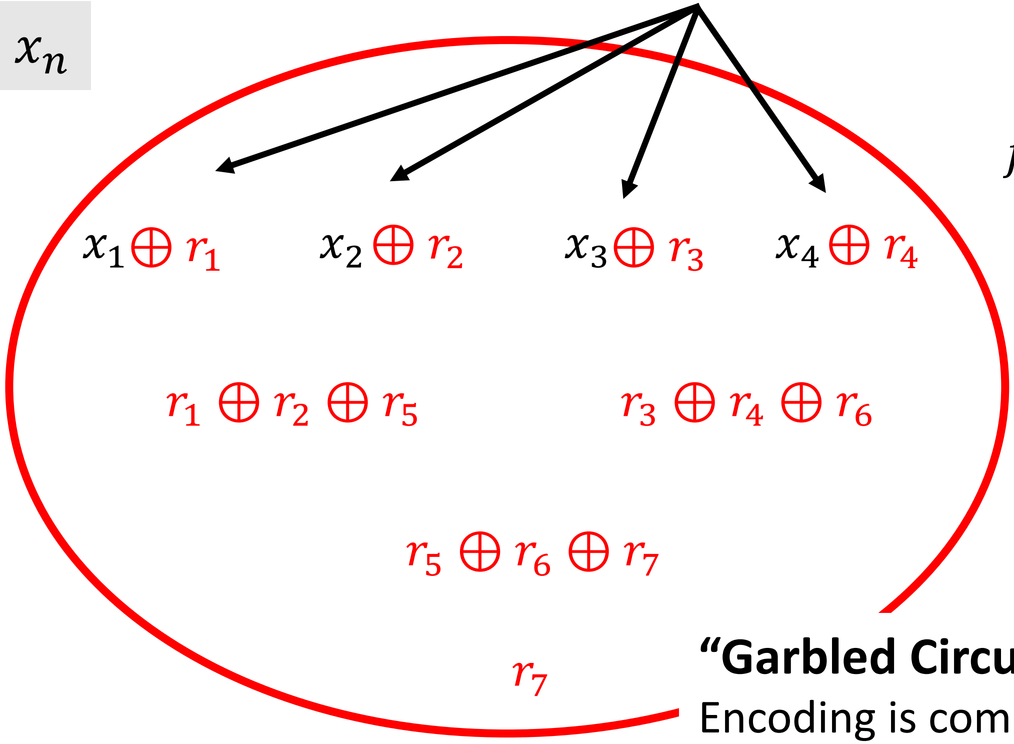
decomposable

each input bit treated separately + offline part

Example: Parity $f(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$

depth $\log n$





$\hat{f}(x_1, \dots, x_4, r_1, \dots, r_7)$

multiple output bits

depth 2

"Garbled Circuit"

Encoding is computed "gate-by-gate"

NAND gate more complicated

[Yao86,BMR90]

$\hat{f}$ is a Randomized Encoding (RE) of f [AIK06]:

- Correctness (decodability): $\hat{f}(x_1, \dots, x_4, r_1, \dots, r_7) \Rightarrow f(x_1, \dots, x_4)$
- Privacy (simulation): $f(x_1, \dots, x_4) \Rightarrow Sample(\hat{f}(x_1, \dots, x_4, U, \dots, U))$

(or stat/comp indistinguishable)

Why?

One of the most useful notions in crypto

The "essence" of f in low complexity

securely compute $\hat{f} \Rightarrow$ securely compute f

Delegation, non-BB constructions, LBs ...

Our Results

- Defining Quantum RE

$\hat{F}$ is a QRE of F: (considering *auxiliary input*)

- Correctness (decodability): $\hat{F}(\boldsymbol{x}, r, \boldsymbol{e}) \Rightarrow F(\boldsymbol{x})$
- Privacy (simulation): $F(\boldsymbol{x}) \Rightarrow Sample(\hat{F}(\boldsymbol{x}, U, \boldsymbol{e}))$ (perfect/stat/comp)

- Construction of quantum garbled circuits (decomposable QRE):

	Perfect Security	Computational Security	
Assumption	- (same)	OWF (same)	(vs. Classical GC [BMR90])
RE Complexity (decoding is linear)	$\mathbf{QNC_f^0}$, size $poly(s, 2^{2^d})$ $\mathbf{NC^0}$, size $poly(s, 2^d)$	$\mathbf{QNC_f^0}$, size $poly(s, \lambda)$ $\mathbf{NC^0}$, size $poly(s, \lambda)$	QCircuit w/ size s & depth d

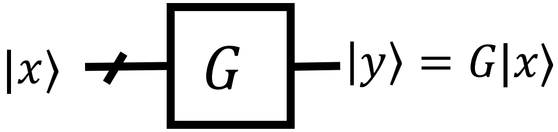
classical input bit $\Rightarrow$ encoded classically

- **Alt. construction:** No shallow encoding, but overall structure is simpler (used in followup [BCKM20]).

- **Application**: ZK "Σ-Protocol" for QMA w/ favorable properties (comp. to [BG20]).

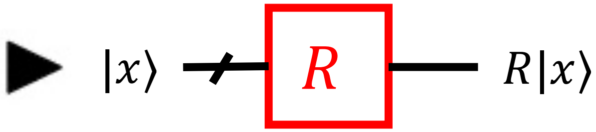
Warmup: The Group Randomizing QRE

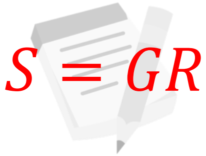
Warmup: Clifford Circuit



$G \in$ Clifford

random Clifford



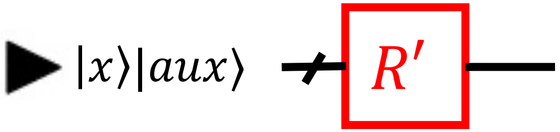


$S = GR^{-1}$

canonical circuit
(classical description)

The Goal (∀ Q circuit):

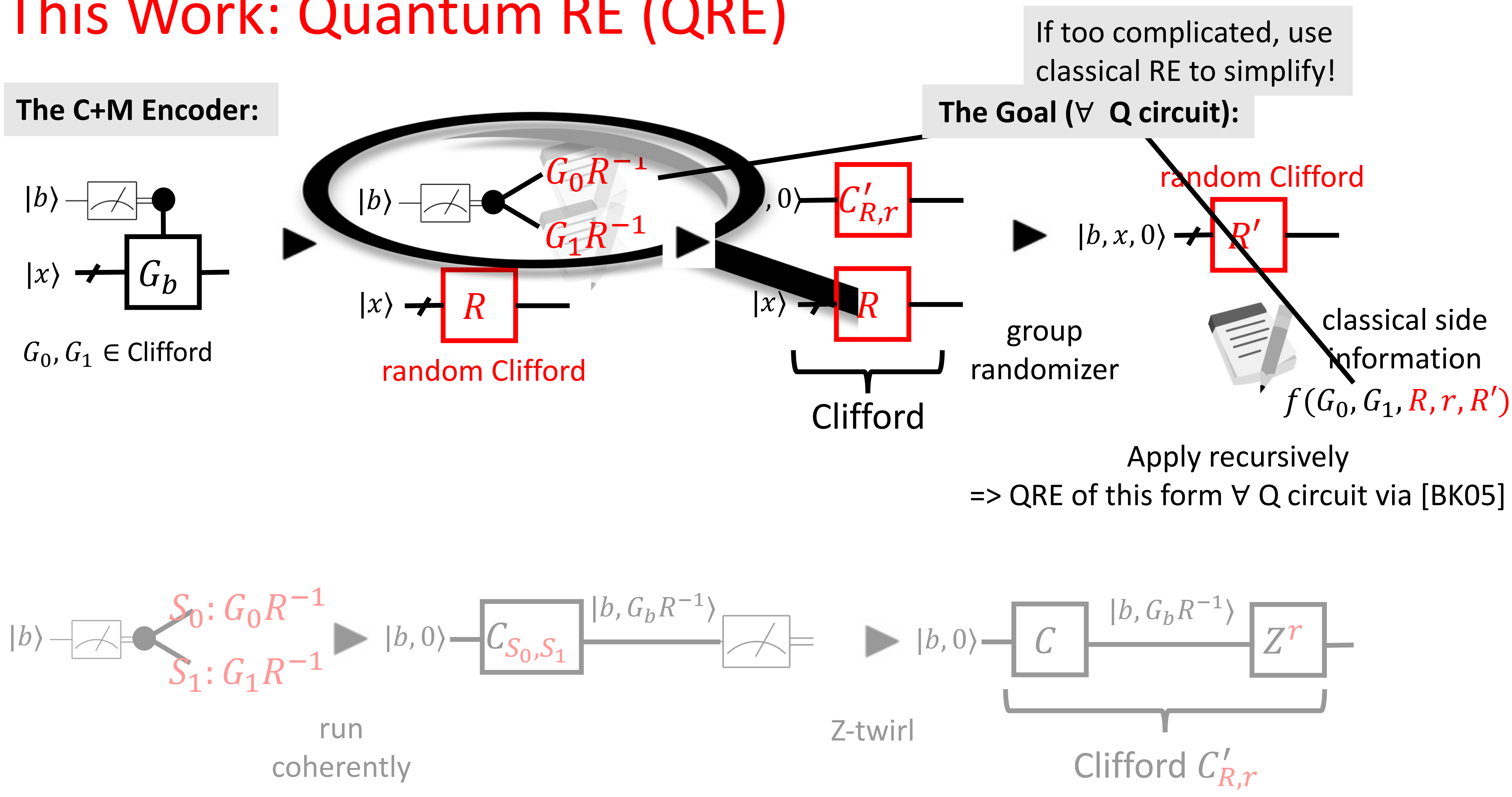
random Clifford



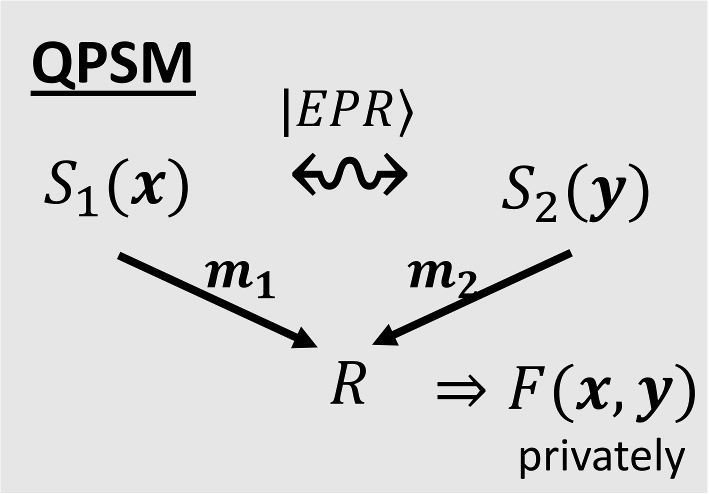
classical side information

Important feature: Hides G

This Work: Quantum RE (QRE)



Other Applications



Potential applications are numerous:

- Import classical
- New quantum applications?

We are unaware of a prior solution, even arbitrarily inefficient

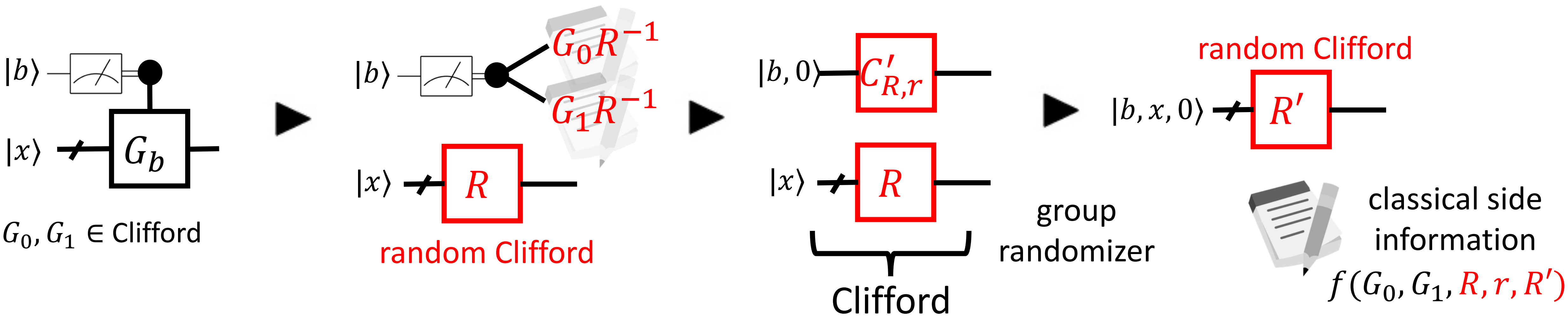
Constant round qMPC?

- Quantum PSM follows by definition.
- Semi-honest 2PC seems straightforward a la Yao.
- Malicious 2PC in 3 rounds recently by [BCKM20].

Functional Encryption and Obfuscation?

- Single-key FE seems straightforward a la [SS10] (but need definition first!).
- Classical RE for Q circuits + Classical obfuscation => Q-Obfuscation. Beware of barriers, e.g. [Morimae20].

...



Thank you

arxiv.org/abs/2006.01085