SUCCINCT-VERIFIER AURORA
OR: WHY YOU SHOULD EMBRACE UNIFORMITY

Nick Spooner

from joint work with Eli Ben-Sasson, Alessandro Chiesa,
Tom Gur and Michael Riabzev

To be presented somewhere, at some point, hopefully

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

*not a real conversation

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

We have this cool new zkSNARK!

*not a real conversation

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

We have this cool new zkSNARK!

Nice! How fast is the verifier?

*not a real conversation

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

We have this cool new zkSNARK!

Nice! How fast is the verifier?

Oh, it runs in linear time (which is optimal)

*not a real conversation

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

We have this cool new zkSNARK!

Nice! How fast is the verifier?

Oh, it runs in linear time (which is optimal)

That's way too slow! My circuits are *huge*.

*not a real conversation

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

We have this cool new zkSNARK!

Nice! How fast is the verifier?

Oh, it runs in linear time (which is optimal)

That's way too slow! My circuits are *huge*.

…but it's optimal!!!

*not a real conversation

A REAL, ACTUAL CONVERSATION* WITH A PRACTITIONER

We have this cool new zkSNARK!

Nice! How fast is the verifier?

Oh, it runs in linear time (which is optimal)

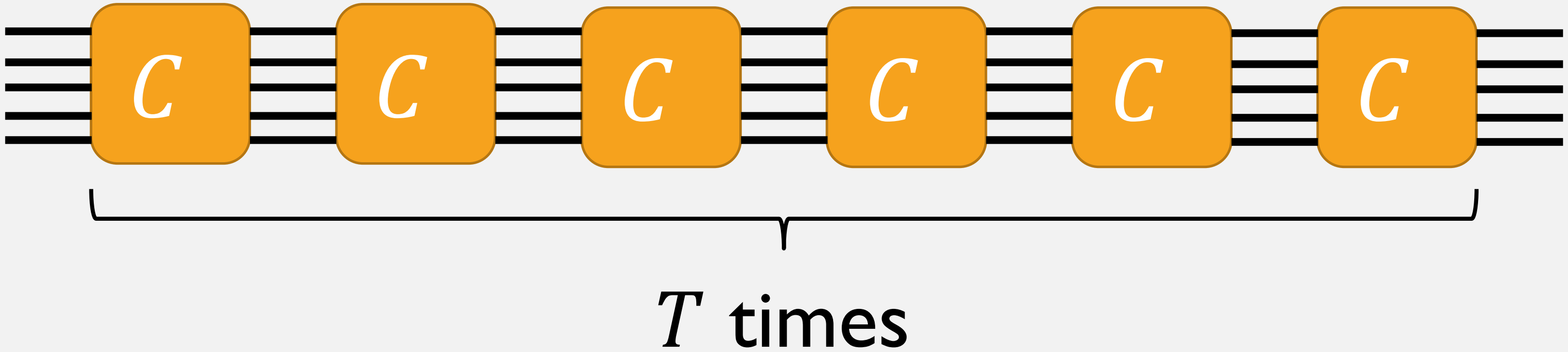
That's way too slow! My circuits are *huge*.

…but it's optimal!!!

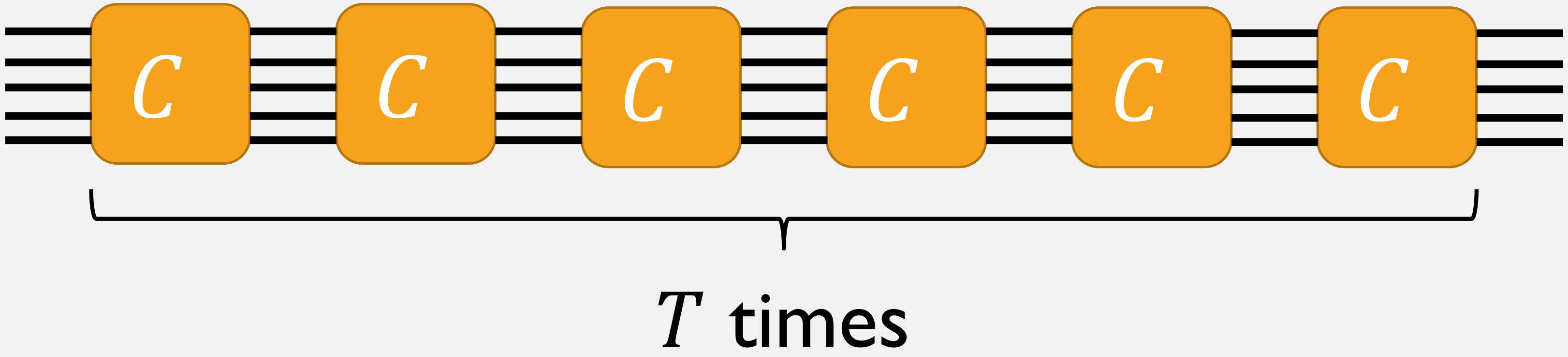
HUGE.

*not a real conversation

ARE HIS CIRCUITS REALLY SO HUGE?

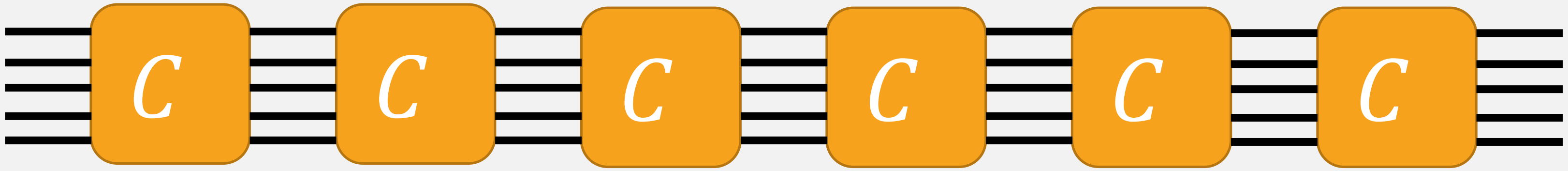


ARE HIS CIRCUITS REALLY SO HUGE?

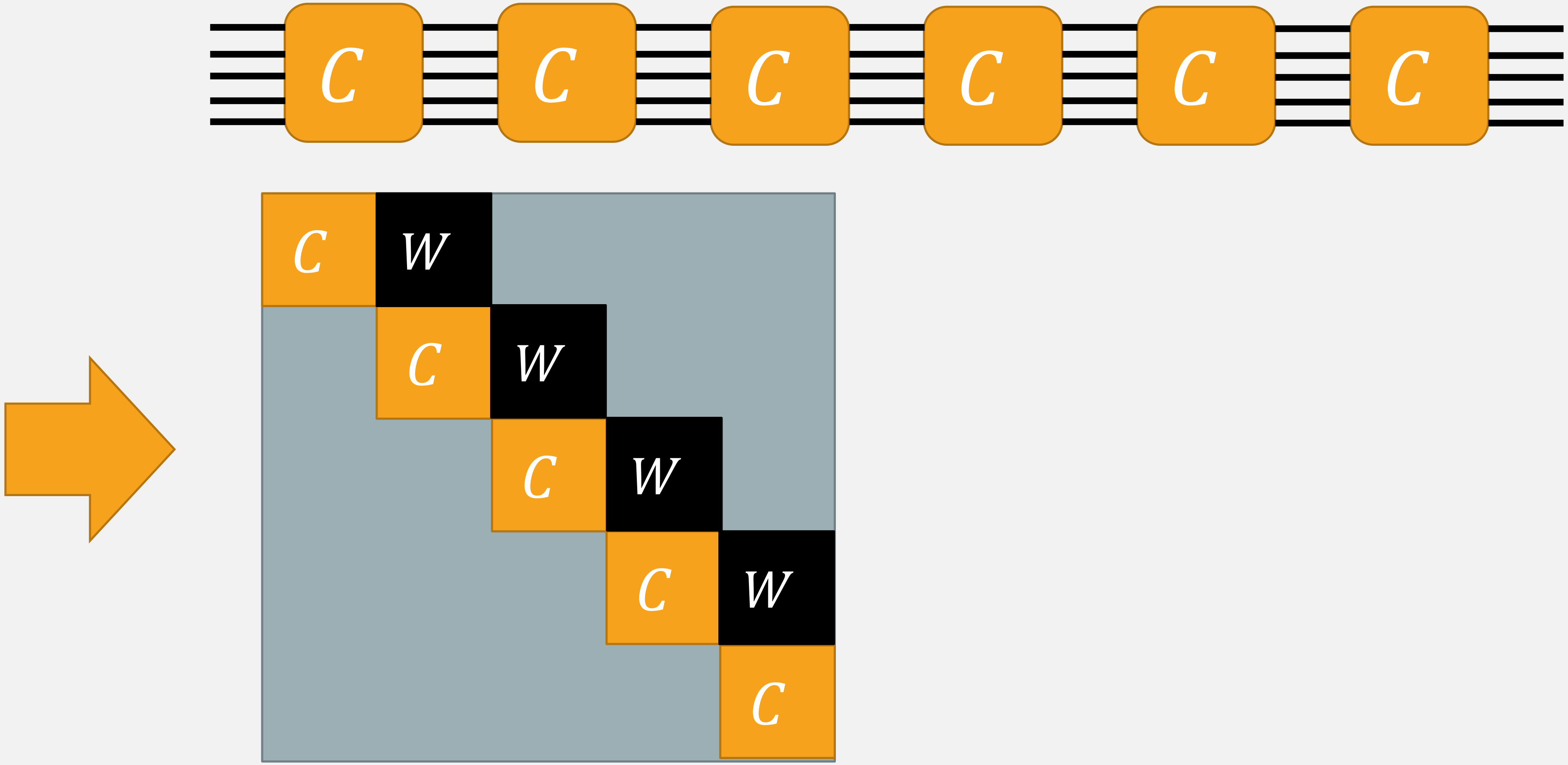


Highly compressible: $|C| + \log T$

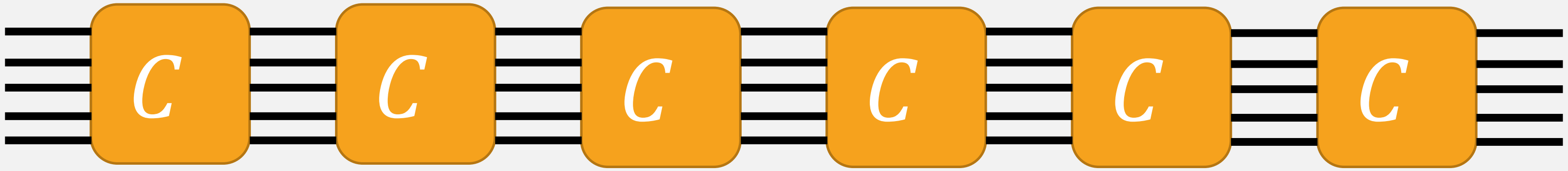
SUCCINCT RICS

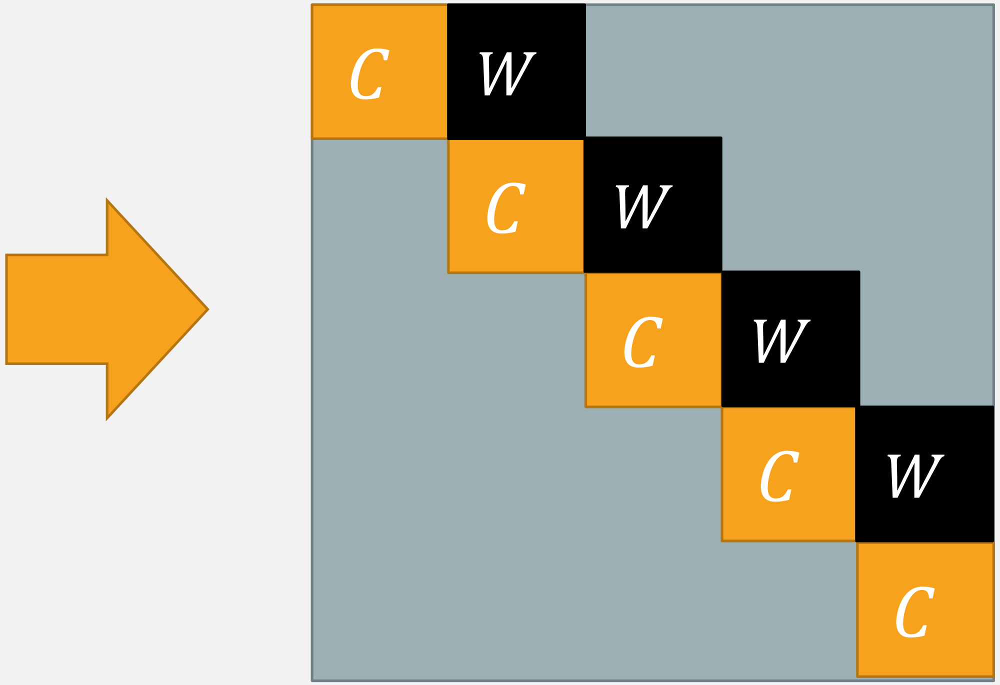


SUCCINCT RICS



SUCCINCT RICS





$$= \boxed{C} \otimes I + \boxed{W} \otimes I^{\rightarrow}$$

SUCCINCT AURORA

Uses algebraic structure to check repeated circuits (& more)

SUCCINCT AURORA

Uses algebraic structure to check repeated circuits (& more)

Verifier runtime is $\mathrm{poly}(|C|, \log T)$