Two Garbled Circuit Lower Bounds

Lower Bounds for Garbled Circuits from Shannon-Type Information Inequalities

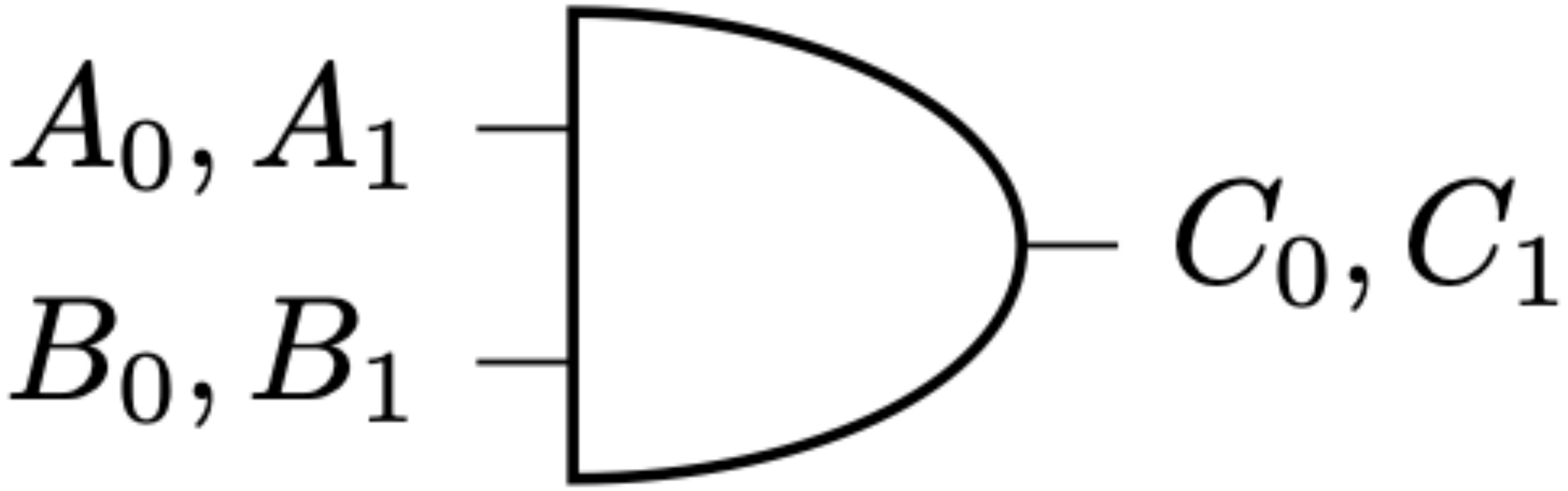
Jake Januzelli + Mike Rosulek + Lawrence Roy

Bitwise Garbling Schemes: A Model with $\frac{3}{2}\kappa$-bit Lower Bound of Ciphertexts

Fei Xu + Honggang Hu + Changhong Xu

Part 1: Background

Yao Garbled Circuits



$$\mathbb{E}_{A_0,B_0}(C_0)$$
$$\mathbb{E}_{A_0,B_1}(C_1)$$
$$\mathbb{E}_{A_1,B_0}(C_0)$$
$$\mathbb{E}_{A_1,B_1}(C_0)$$

Security properties

- Privacy: truth values hidden from evaluator.
- Authenticity: evaluator can only produce correct output.

How big can the gate be?

- Only consider RO/symmetric key constructions.

[BMR90]	4λ	4λ	$\$$
[NPS99]	3λ	3λ	$\$$
[GLNP15]	2λ	λ	$\$$
[ZRE15]	2λ	0	$\mathrm{A}_1 = A_0 \oplus \Delta$
[RR21]	$1.5\ \lambda$	0	$\mathrm{A}_1 = A_0 \oplus \Delta$

Existing lower bounds

Paper	model	Free-XOR AND	non-Free-XOR AND
[ZRE15]	linear model	$\geq 2\lambda$	
[BK24]	linear + general slicing model	$\geq 1.5\lambda$	
[XHX24]	bitwise model	$\geq 1.5\lambda$	$\geq 2\lambda$

Part 2: Our results

Lower Bounds for Garbled Circuits from Shannon-Type Information Inequalities

Speaker: Jake Januzelli (Columbia University)

Joint work with Mike Rosulek (Oregon State University) and Lawrence Roy (Aarhus University)

Our results

- Garbled AND gates w/ Free-XOR labels need $1.5\lambda - negl$ bits.
- Garbled AND gates w/ uncorrelated wire labels need $2\lambda - negl$ bits.
- Garbled XOR gates w/ uncorrelated wire labels need $\lambda - negl$ bits.
- [GLNP15, RR21] are **optimal**.

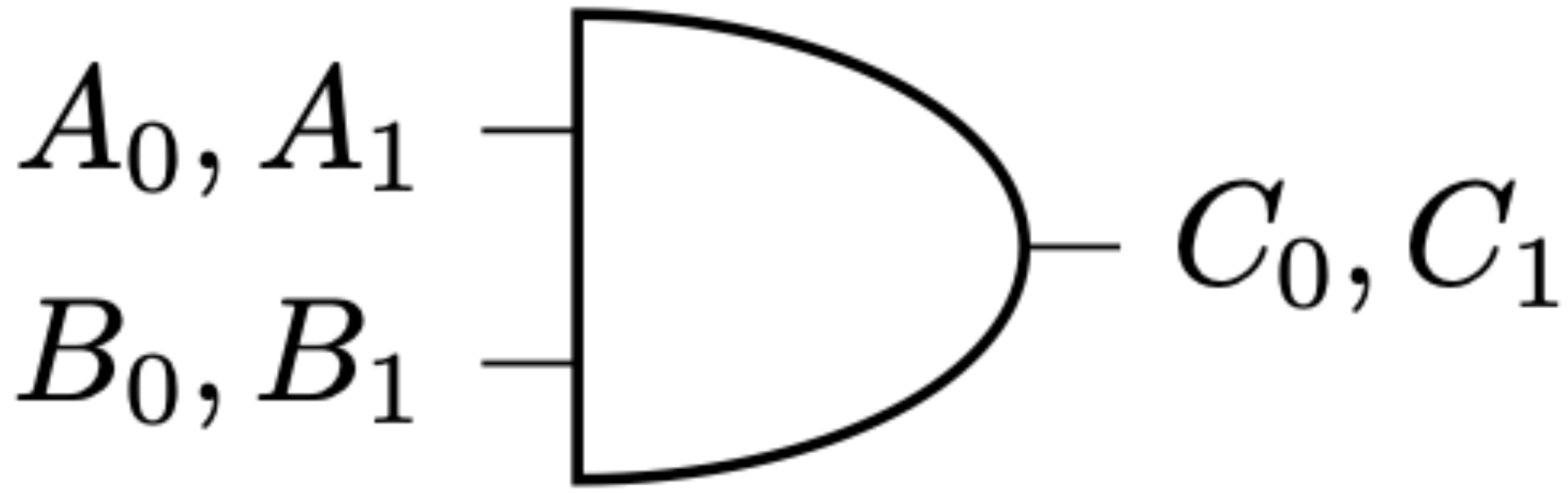
Our assumptions

- **Minicrypt** scheme.
- Unrestricted garbler.
- Evaluator makes only **non-adaptive** random oracle queries $\Rightarrow$ useful for single gates.
- Evaluator makes **coordinated** random oracle queries: for any RO query $Eval$ makes when evaluating on (i, j), $Eval$ knows which other inputs would also make the query.
- The above holds for all known Minicrypt schemes.

Coordinated queries

A_0, B_0	$\mathrm{A}_0, B_0 \oplus \Delta$
$\mathrm{Eval}(0,0)$	$\boxed{\mathrm{Eval}(0,1)}$
$\mathrm{A}_0 \oplus \Delta, B_0$	$\mathrm{A}_0 \oplus \Delta, B_0 \oplus \Delta$
$\boxed{\mathrm{Eval}(1,0)}$	$\mathrm{Eval}(1,1)$

Our (milder) assumptions



- $|A_i| = |B_j| = \lambda, \; \leftarrow \$$
- $(C_0, C_1) \cong (A_0, B_0) \cong (B_0, B_1)$

Security definition (I)

Real:	Ideal:
$\mathcal{C} : (G, C_0, C_1, A_0, A_1, B_0, B_1) \leftarrow \mathsf{Garble}(g)$	$\mathcal{C} : (G, A_i, B_j) \leftarrow \mathsf{Sim}(g)$
$\mathcal{C} \rightarrow \mathcal{A} : (G, A_i, B_j)$	$\mathcal{C} \rightarrow \mathcal{A} : (G, A_i, B_j)$
$\mathcal{A} \leftrightarrow RO$	$\mathcal{A} \leftrightarrow RO$
$\mathcal{A} \rightarrow \mathcal{C} : \sigma$	$\mathcal{A} \rightarrow \mathcal{C} : \sigma$

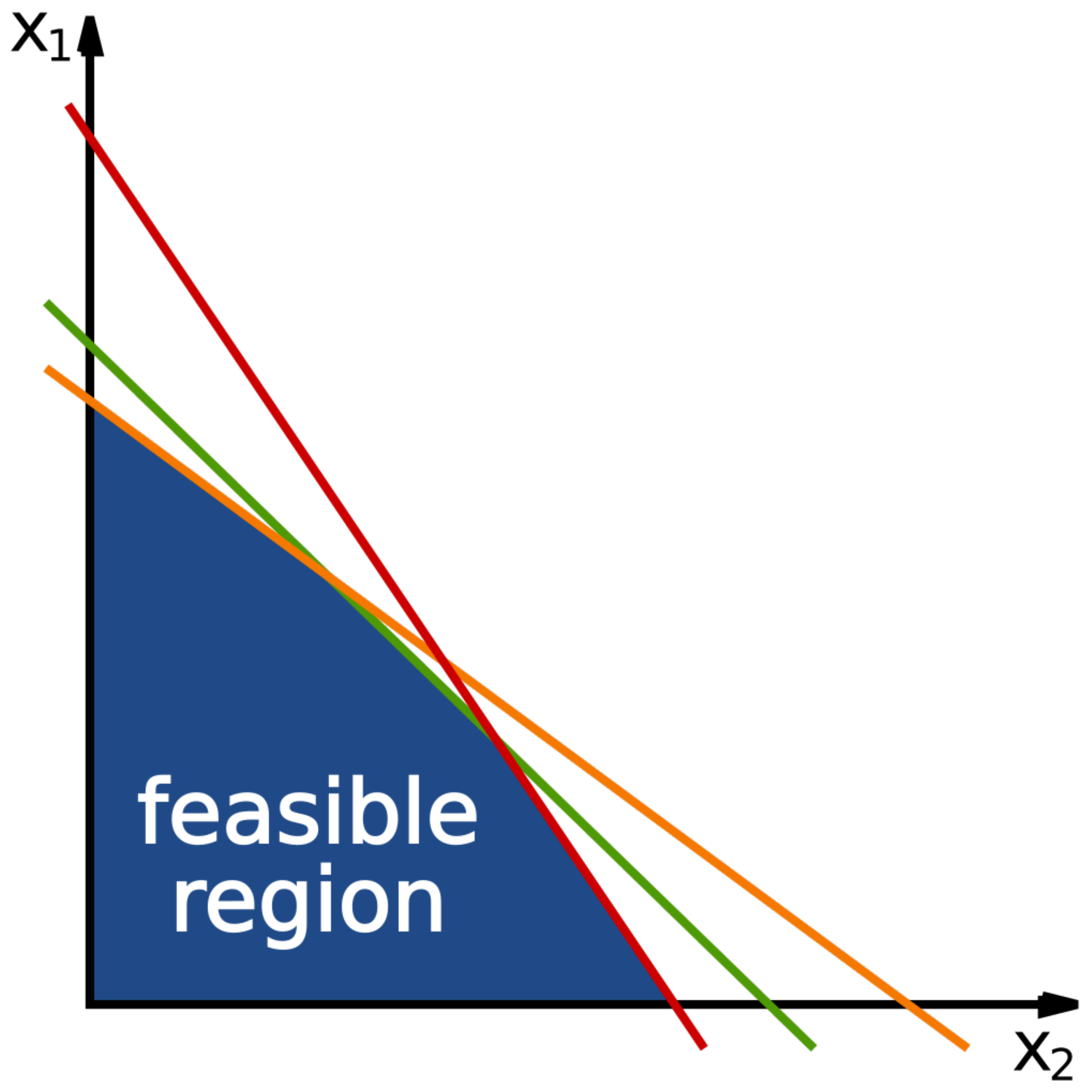
Security definition (II)

<u>Real</u>:
$\mathcal{C}$: $(G, C_0, C_1, A_0, A_1, B_0, B_1) \leftarrow \mathsf{Garble}(g)$
$\mathcal{C} \rightarrow \mathcal{A}$: (G, A_i, B_j)
$\mathcal{A} \leftrightarrow RO$
$*\mathcal{A} \rightarrow \mathcal{C}$: end
$*\mathcal{C} \rightarrow \mathcal{A}$: $(G, C_0, C_1, A_0, A_1, B_0, B_1)$
$\mathcal{A} \rightarrow \mathcal{C}$: σ

<u>Ideal</u>:
$\mathcal{C}$: $(G, A_i, B_j) \leftarrow \mathsf{Sim}(g)$
$\mathcal{C} \rightarrow \mathcal{A}$: (G, A_i, B_j)
$\mathcal{A} \leftrightarrow RO$
$*\mathcal{A} \rightarrow \mathcal{C}$: end
$*(G, C_0, C_1, A_{1-i}, B_{1-j}) \leftarrow \mathcal{C}$
$*\mathcal{C} \rightarrow \mathcal{A}$: $(G, C_0, C_1, A_0, A_1, B_0, B_1)$
$\mathcal{A} \rightarrow \mathcal{C}$: σ

Information theory

- Shannon information inequality: linear combinations of conditional entropies (E.x $\phi(X) - \phi(X \mid Y) \geq 0$).
- Translate correctness + security into Shannon bounds → use LP solver (CITIP).
- "Minimize entropy of garbled gate, subject to [bounds]"



Challenges

- Code modifications to CITIP (multiple distributions, approximate constraints)
- Initial attempts to solve LP take too long.
- Solution: reduce number of variables.

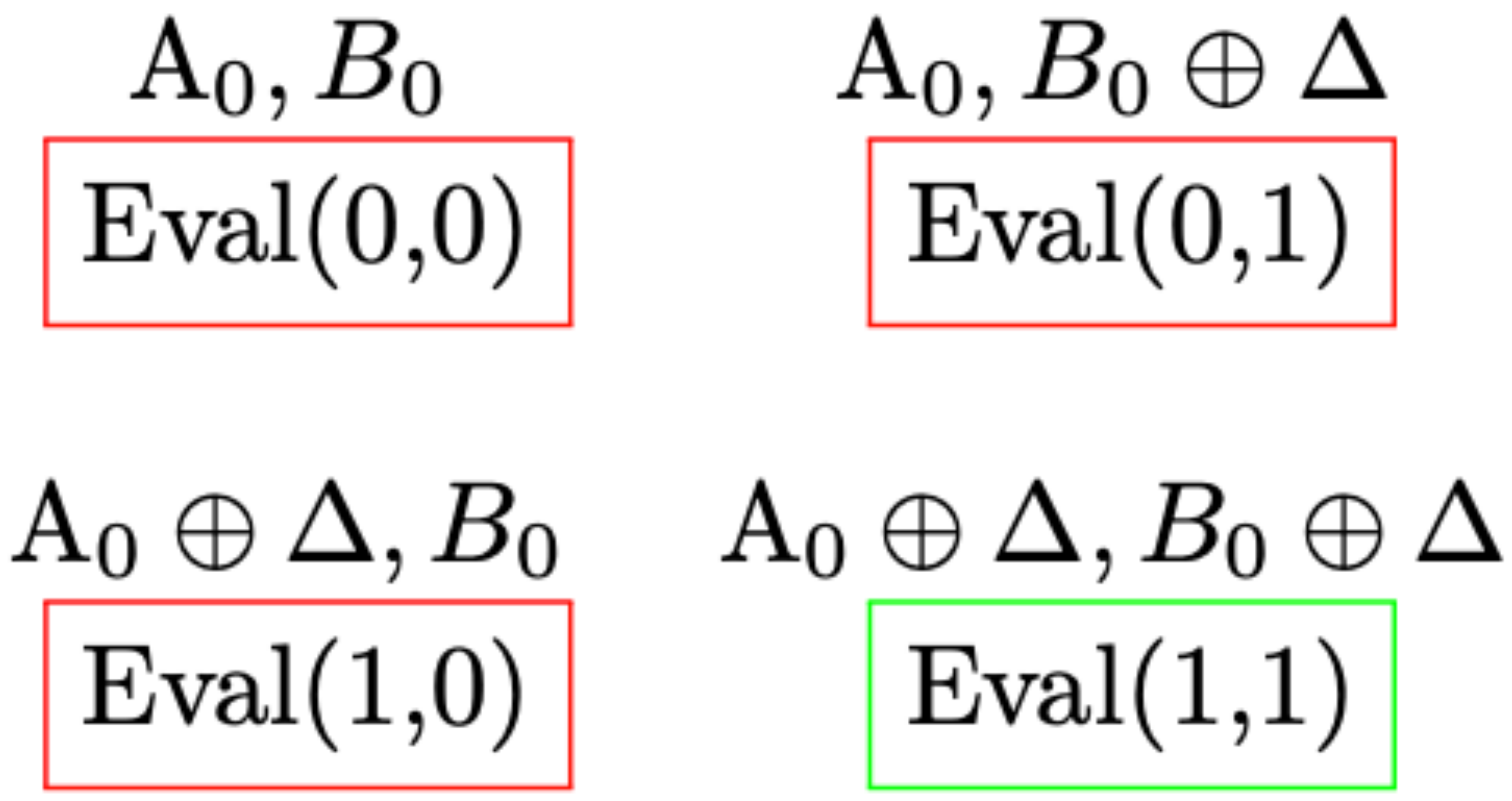
n-way queries

- n-way query: query that can be made with n different input combinations.
- E.g, $A_0 \oplus B_0 \oplus \Delta$ in free-XOR.
- We **show** (don't assume) 2-way queries are the only "useful" queries.

A_0, B_0	$\mathrm{A}_0, B_0 \oplus \Delta$
$\mathrm{Eval}(0,0)$	$\boxed{\mathrm{Eval}(0,1)}$
$\mathrm{A}_0 \oplus \Delta, B_0$	$\mathrm{A}_0 \oplus \Delta, B_0 \oplus \Delta$
$\boxed{\mathrm{Eval}(1,0)}$	$\mathrm{Eval}(1,1)$

n-way queries (II)

- *Lemma:* Any 3-way query is actually 4-way (use non-adaptiveness).
- *Lemma:* 1-way queries can be expressed with 2-ways. E.g $H(A_i, B_j) \cong H(A_i) \oplus H(B_j)$.
- *Lemma:* Only 2-way queries are from Free-XOR.



Conclusion

Paper	model	Free-XOR AND	non-Free-XOR AND
[ZRE15]	linear model	$\geq 2\lambda$	
[BK24]	linear + general slicing model	$\geq 1.5\lambda$	
[FLZ24]	linear + general slicing model	$\geq 1.5\lambda$	
[XHX24]	bitwise model	$\geq 1.5\lambda$	$\geq 2\lambda$
Our work	our model	$\geq 1.5\lambda$	$\geq 2\lambda$

Thank you for your time!