A quantum protocol for the orthogonal vector problem and leakage-resilient computation

Frédéric Dupuis
Masaryk University, Brno, Czech Republic

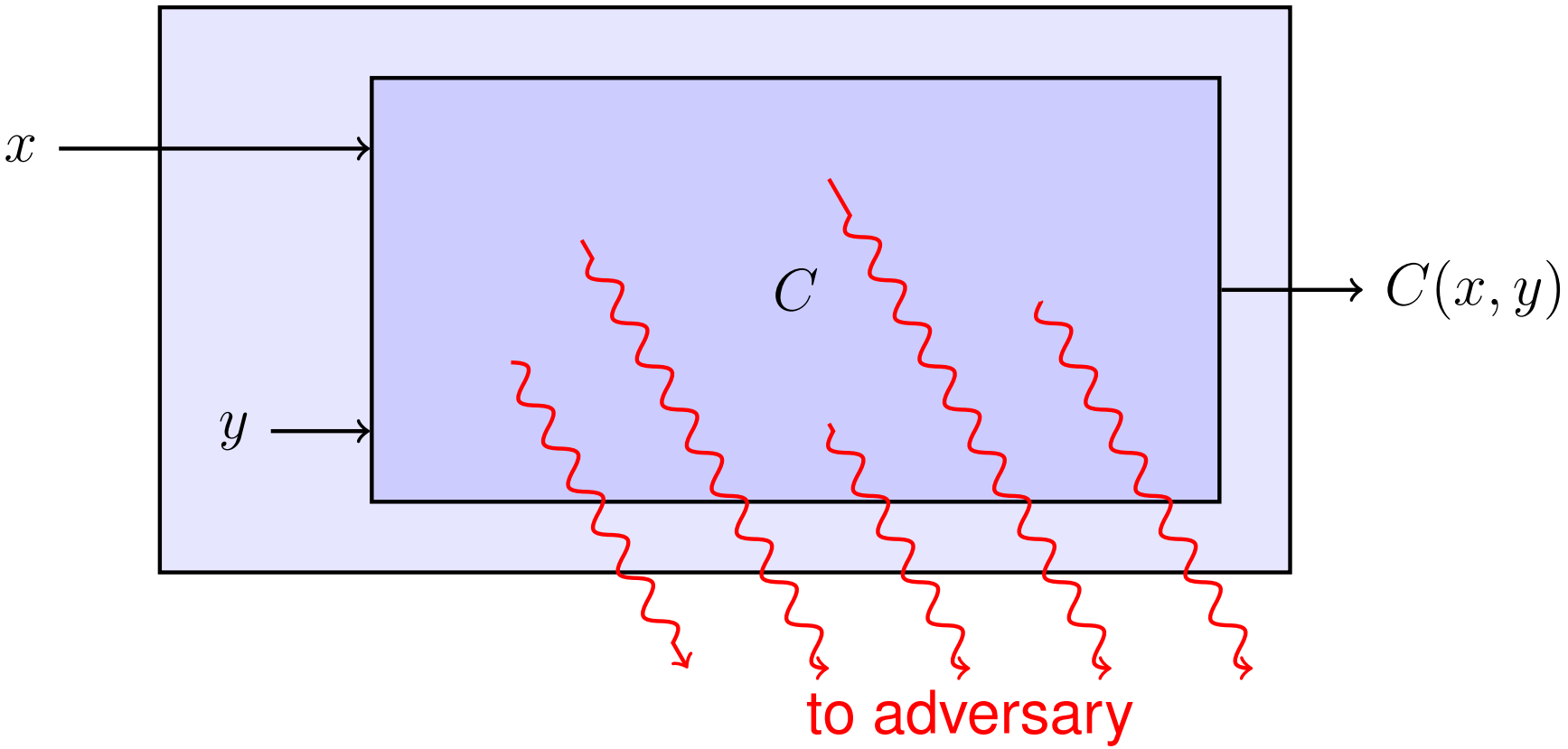
joint work with
Ivan Damgård and Jesper Buus Nielsen
Aarhus University, Aarhus, Denmark

4 September 2014

Introduction

- Leakage resilience: what it is
- The split-state model
- The orthogonal vector problem
- Quantum protocol for the orthogonal vector problem

Leakage resilience



Leakage resilience

How can we model leakage resilience?

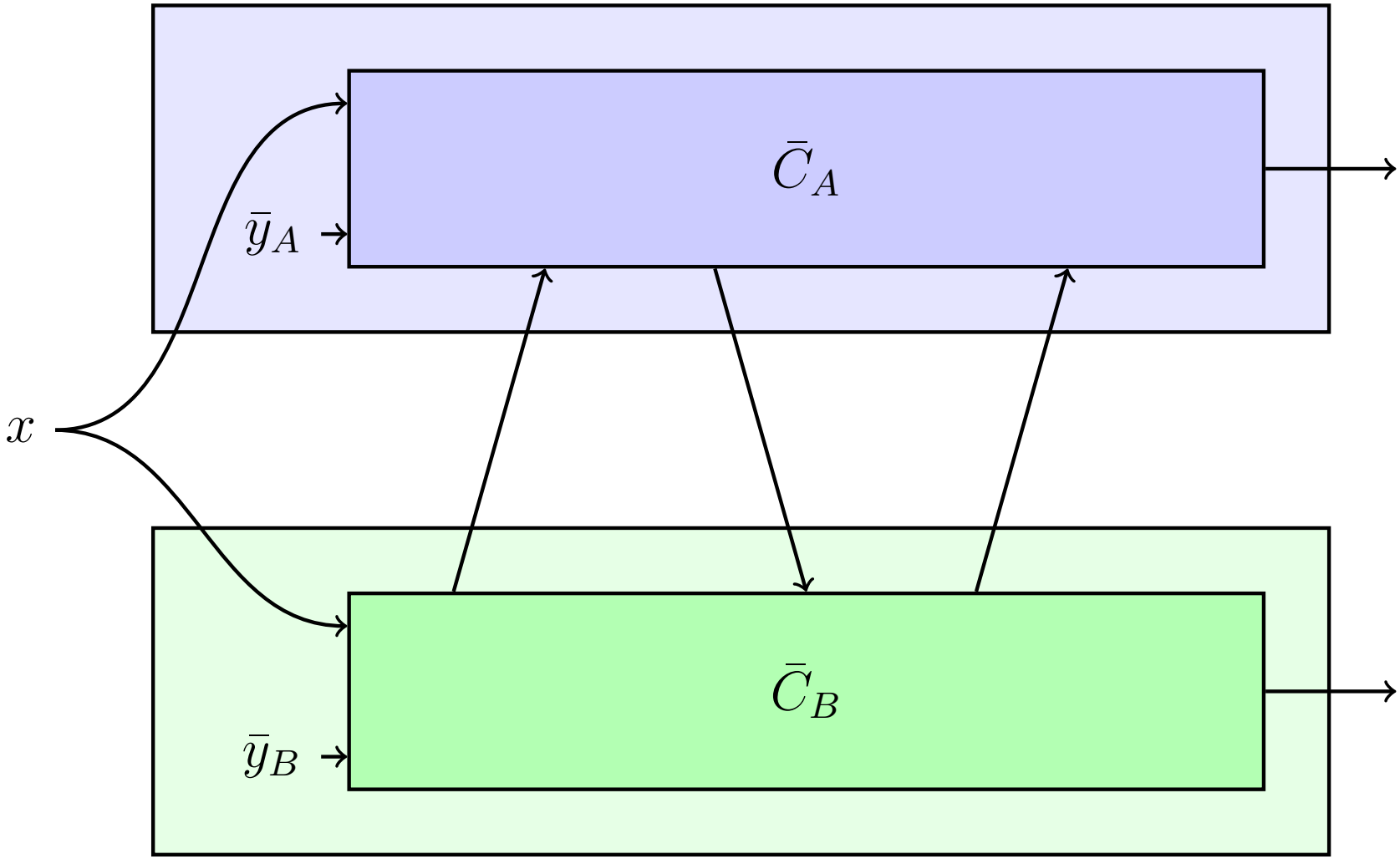
- If everything can leak, there is nothing we can do
- We need to model a more restricted adversary:
  - Leakage from a bounded number of wires [ISW03]
  - Drawback: power consumption attacks, acoustic attacks, etc
  - Bounded number of bits leaked: nothing we can do
  - Only computation leaks: only get leakage from bits currently being processed
  - Leakage is still local in some sense

“Only-computation-leaks” model

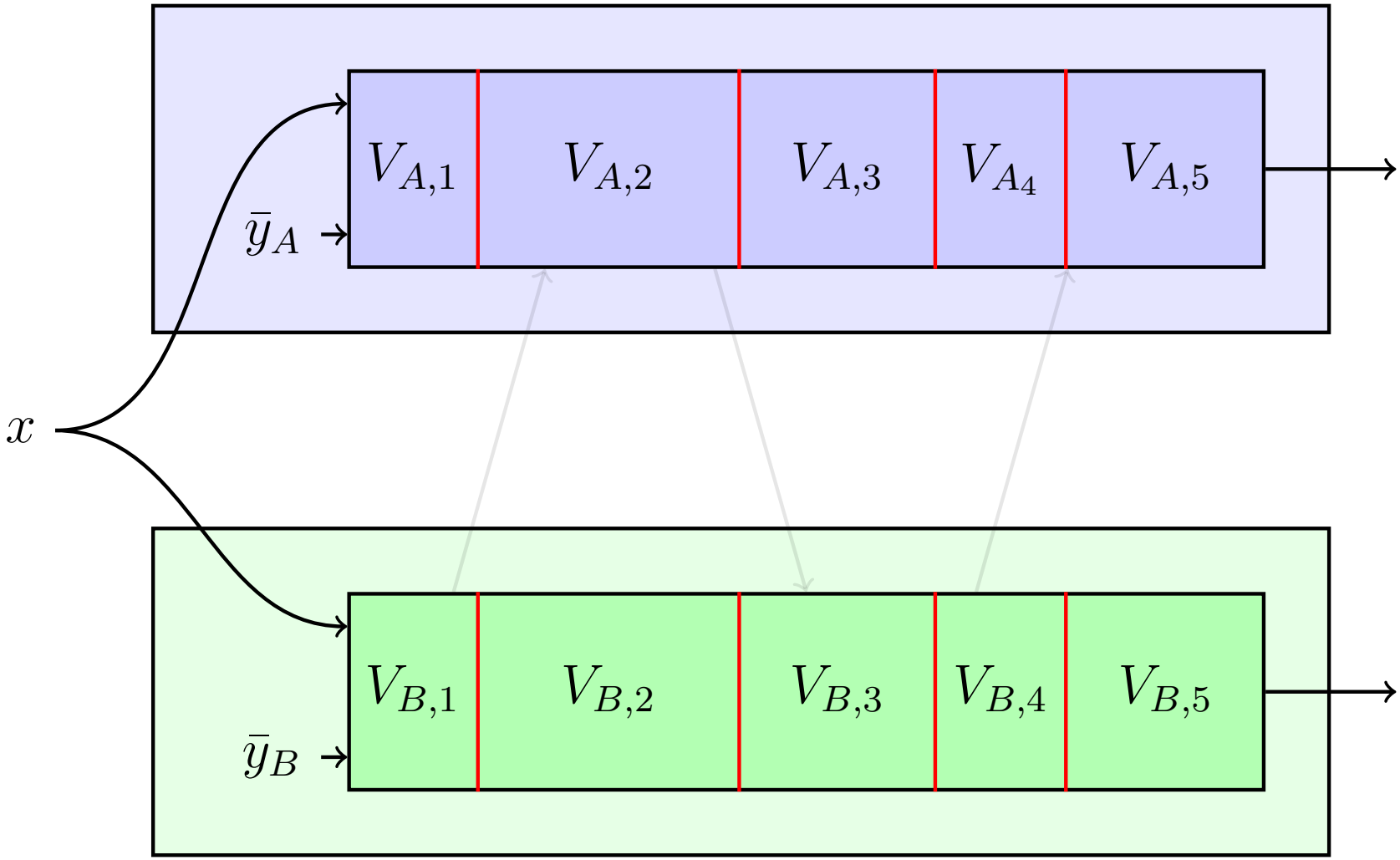
How do we capture this notion?

- Only computation leaks: divide the computation into several steps
- Local leakage: split device into subprocessors
- Data being computed on → messages between subprocessors

“Only-computation-leaks” model

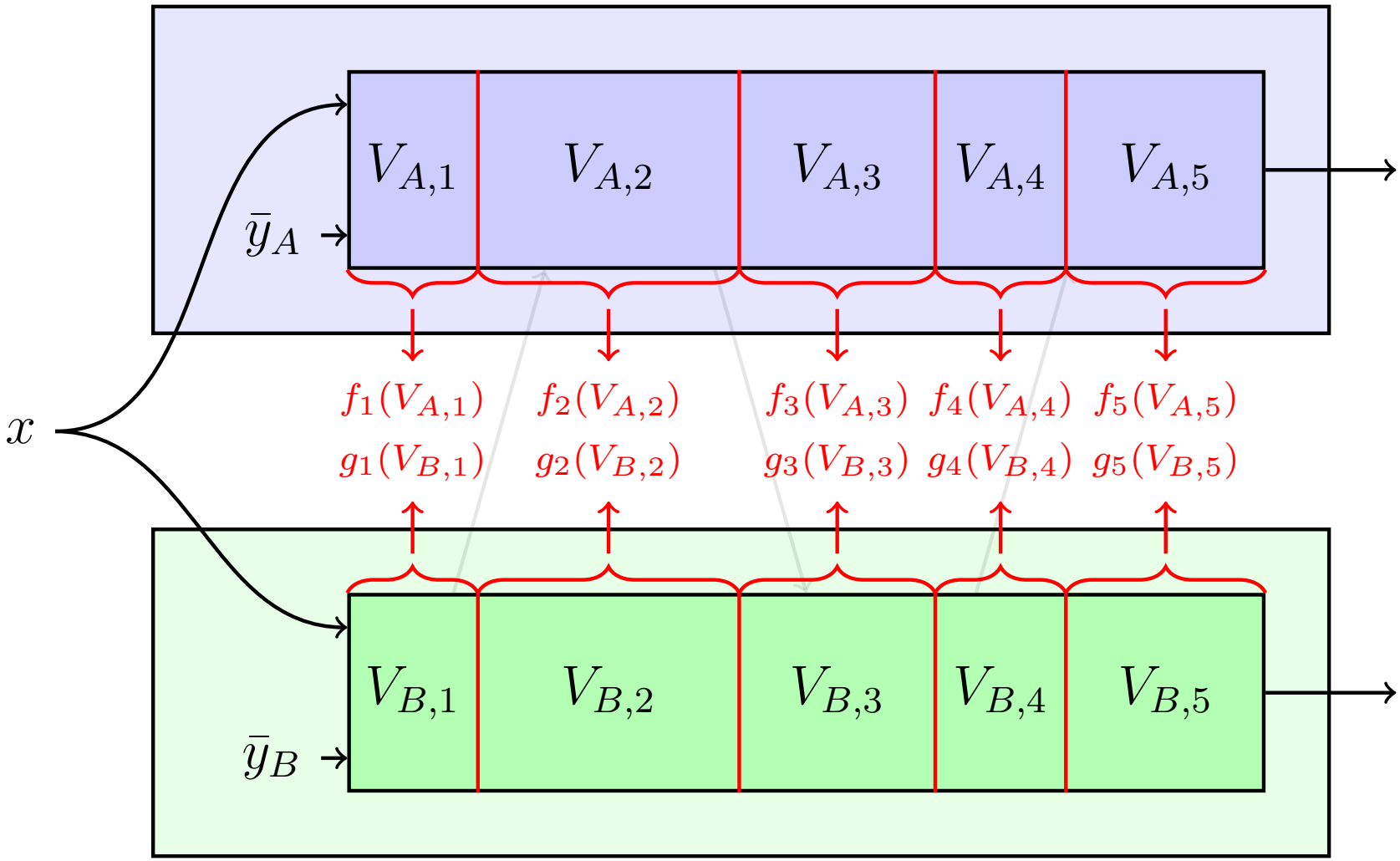


“Only-computation-leaks” model



$V_{A,i}$: New data added to A’s view between point i and $i + 1$.

“Only-computation-leaks” model



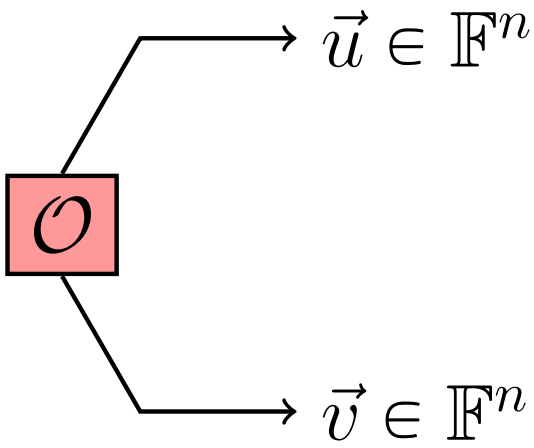
Every $f_i(\cdot)$ is at most λ bits.

“Only-computation-leaks” model

Can we make leakage-resistant circuits in this model?

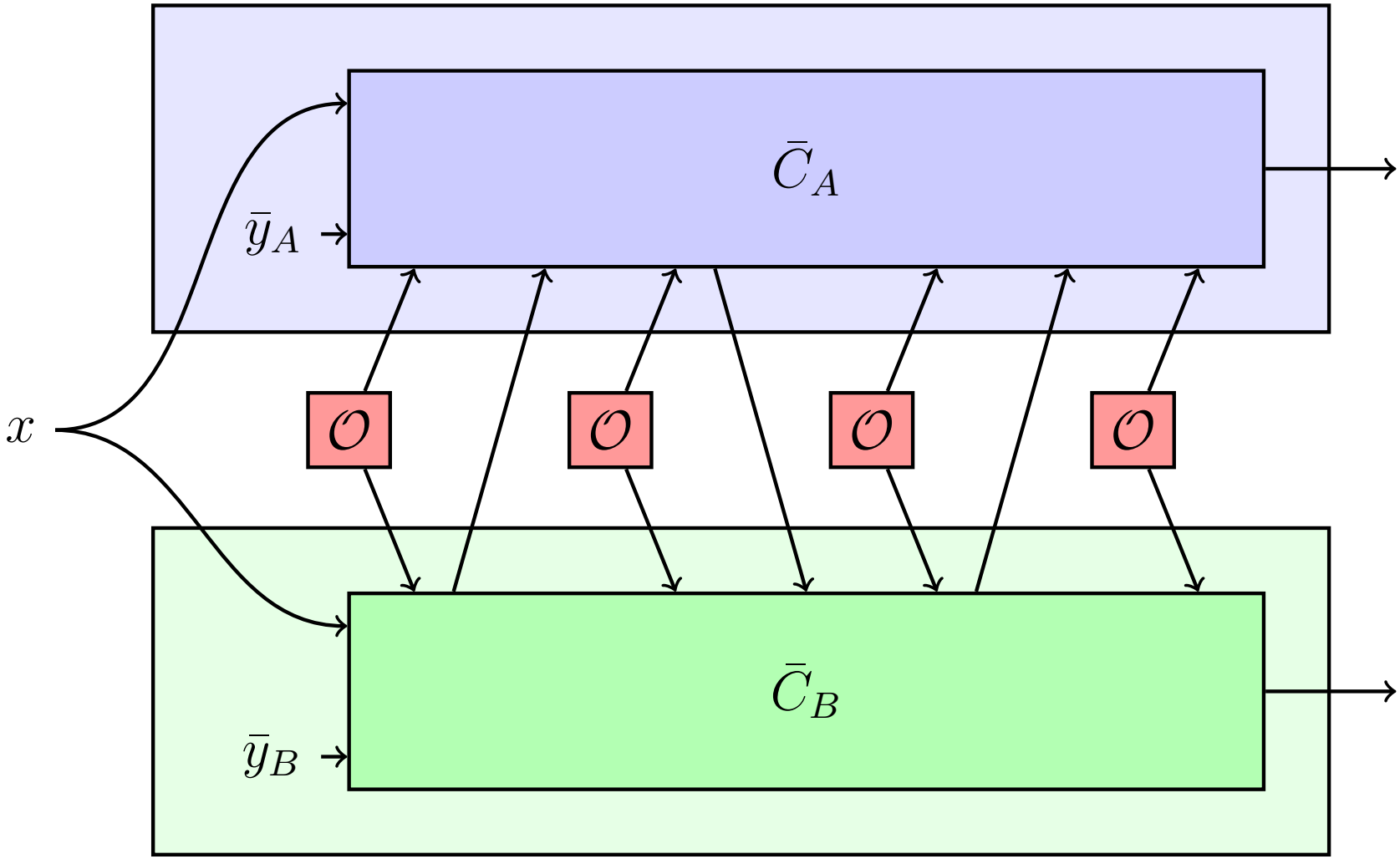
- No: this is still impossible
- Classically, we need extra assumptions to make this true
- [GR12] Need a “ciphertext bank” at the beginning
- [DF12] Need orthogonal vectors from a leak-free component

Leak-free component from [DF12]

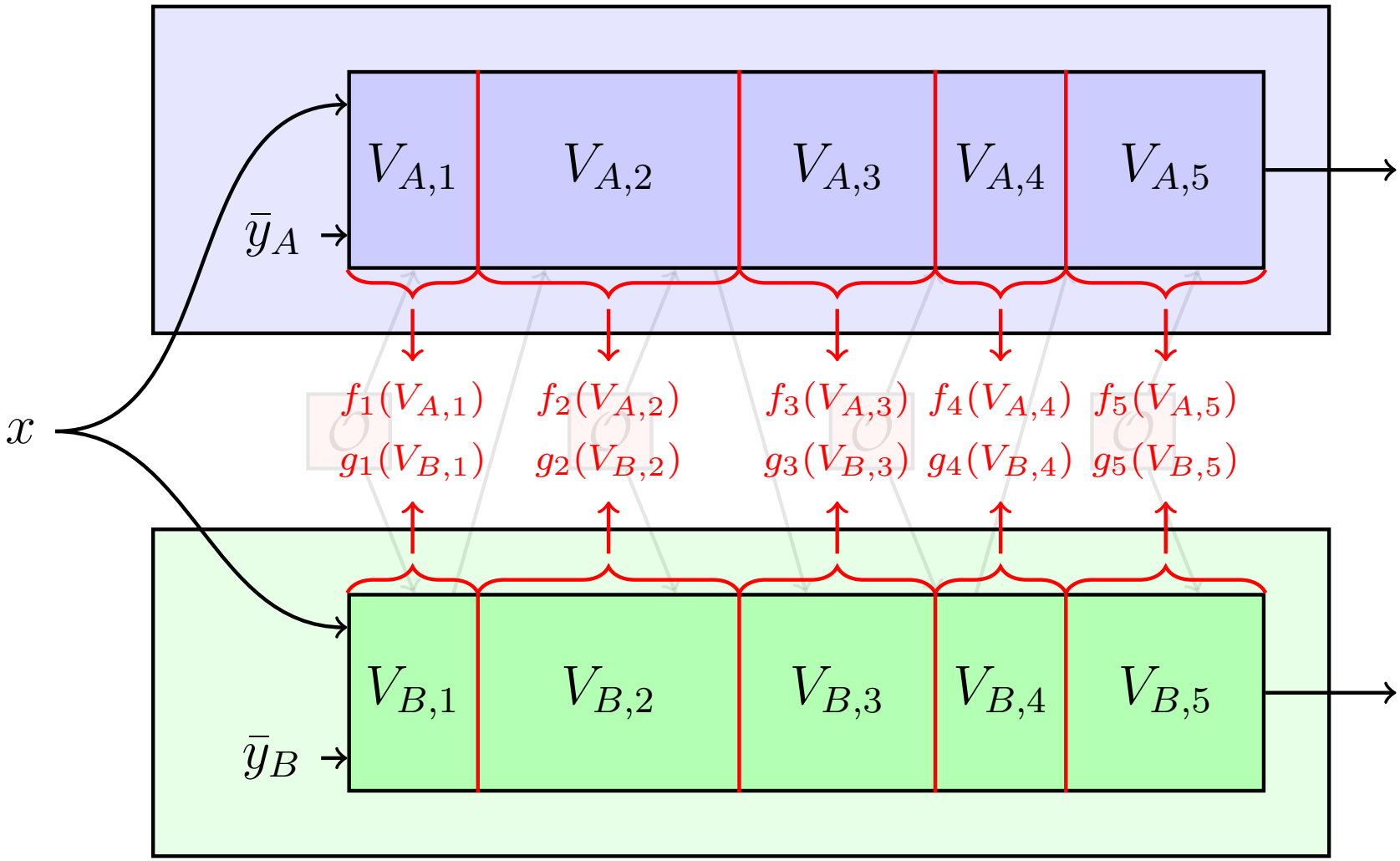


- $\mathbb{F}$: finite field of order 2^k
- Orthogonal: $\langle \vec{u}, \vec{v} \rangle = \sum_i u_i v_i = 0$.
- Uniformly random over all orthogonal vectors.

Split-state model with leak-free components



Split-state model with leak-free components



Every $f_i(\cdot)$ is at most λ bits.

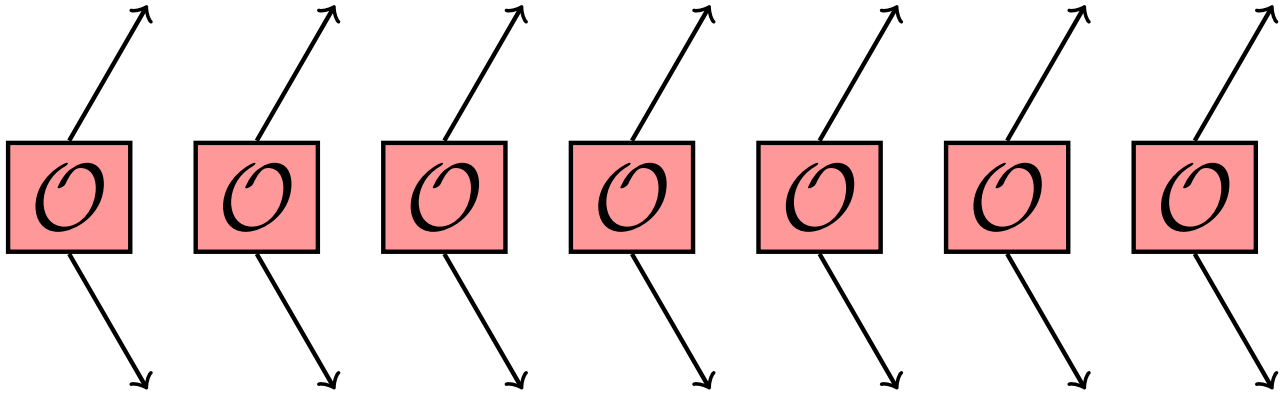
Circuit compiler from [DF12]

How do we compile a circuit in this model?

- Bit $b \to$ pair of random vectors $(\vec{b}_A, \vec{b}_B)$, such that $\langle \vec{b}_A, \vec{b}_B \rangle = b$.
- For every circuit gate, use encoded implementation.
- Each gate requires a new pair $(\vec{u}, \vec{v})$ such that $\langle \vec{u}, \vec{v} \rangle = 0$ to refresh the encoding.

Quantum protocol for orthogonal vectors

So: we need a source of orthogonal vectors:



. . . but without the leakage-free assumption.

Quantum protocol for orthogonal vectors

- Reminiscent of QKD
- We could try to distribute a state

$$|\psi\rangle_{\mathsf{AB}} = \frac{1}{\sqrt{K}} \sum_{\langle \vec{u}, \vec{v} \rangle = 0} |\vec{u}\rangle_{\mathsf{A}} \otimes |\vec{v}\rangle_{\mathsf{B}}$$

- If we can ensure that this is indeed the state we have, then it is automatically private.

Quantum protocol: trivial?

Why don't we just do this:

1. Do regular QKD to get many copies of $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Use entanglement dilution to convert these to $|\psi\rangle$
3. Profit!

This has several drawbacks:

- Involves complicated quantum operations
- What leakage model do we use for those quantum operations?

Quantum protocol for orthogonal vectors

How does this work for QKD?

1. Distribute m copies of the state $|\Phi\rangle_{\mathsf{AB}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. [Test 1] Pick a set S_1, measure both qubits in computational basis, make sure enough bits agree
3. [Test 2] Pick a set S_2, measure in Hadamard basis, make sure enough bits agree
4. Error correction and privacy amplification

Quantum protocol for orthogonal vectors

How about trying something similar?

1. Distribute m copies of the state $|\psi\rangle_{\mathsf{AB}} = \frac{1}{K}\sum_{\langle\vec{u},\vec{v}\rangle=0} |\vec{u}\rangle \otimes |\vec{v}\rangle$.
2. [Test 1] Pick a set S_1, measure both sides in computational basis, make sure the vectors are orthogonal
3. [Test 2] Pick a set S_2, measure in Hadamard basis, and make sure that. . . what?
4. ~~Error correction and privacy amplification~~ Change the classical protocol to tolerate a few errors.

Quantum protocol for orthogonal vectors

What happens when we measure all the qubits of $|\psi\rangle = \frac{1}{K}\sum_{\langle\vec{u},\vec{v}\rangle=0} |\vec{u}\rangle \otimes |\vec{v}\rangle$ in the Hadamard basis?

- With a coherent superposition of all vectors, we would get the all-zero string all the time.
- There are $\frac{1}{|\mathbb{F}|}$ orthogonal vectors $\Rightarrow$ get all-zero strong $\frac{1}{|\mathbb{F}|}$ of the time.
- [Test 2] Pick a set S_2, measure in Hadamard basis, and make sure that at least a fraction $\frac{1}{|\mathbb{F}|} - \delta$ come out as the all-zero string

Quantum protocol for orthogonal vectors

So the protocol looks like:

1. Distribute m copies of the state $|\psi\rangle_{\mathsf{AB}} = \frac{1}{K}\sum_{\langle\vec{u},\vec{v}\rangle=0} |\vec{u}\rangle \otimes |\vec{v}\rangle$.
2. [Test 1] Pick a set S_1, measure both sides in computational basis, make sure the vectors are orthogonal
3. [Test 2] Pick a set S_2, measure in Hadamard basis, and make sure at least a fraction $\frac{1}{|\mathbb{F}|} - \delta$ come out as the all-zero string
4. Run the classical protocol

Quantum protocol for orthogonal vectors

Why does this work?

- Pass Test 1 $\Rightarrow$ state contains mostly orthogonal vectors.
- Pass Test 2 $\Rightarrow$ state contains coherent superposition of at least $\frac{1}{|\mathbb{F}|}$ vectors.
- There are only about $\frac{1}{|\mathbb{F}|}$ orthogonal vectors.

Quantum protocol for orthogonal vectors

The problem: showing this rigorously

- Pass Test 1 $\Rightarrow$ state is in the support of projector Π_1 with mostly only orthogonal vectors
- Pass Test 2 $\Rightarrow$ state is in the support of projector Π_2 with lots of zeros in Hadamard basis
- What we want: state is in the support of projector Π_{good} with $|\psi\rangle$ in most positions
- None of these projectors commute

The solution: a new sampling theorem, based on "postselection" theorem.

Summary of results

- Impossibility of leakage-resilient circuit compilation in classical model without assumptions
- Adapted protocol from [DF12] to tolerate some errors in orthogonal pairs
- Showed a quantum protocol for generating orthogonal pairs with low error rate

Thank you

Thank you!