

# Quantum Assisted Secure Multiparty Computation

Manuel Batalha dos Santos

Thesis defense  
16 January 2025



# Outline

# Outline

- Motivation and outcomes

# Outline

- Motivation and outcomes
- Quantum and classical oblivious transfer

# Outline

- Motivation and outcomes
- Quantum and classical oblivious transfer
- Private phylogenetic trees

# Outline

- Motivation and outcomes
- Quantum and classical oblivious transfer
- Private phylogenetic trees
- Quantum oblivious linear evaluation

# Motivation

SMC

# Motivation

SMC

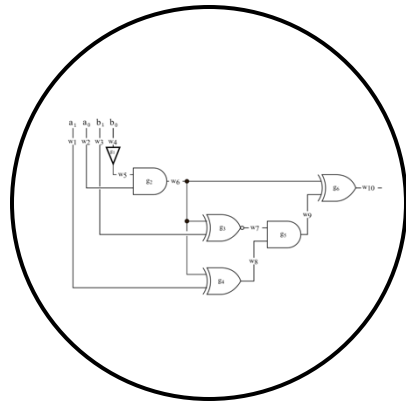




# Motivation

SMC

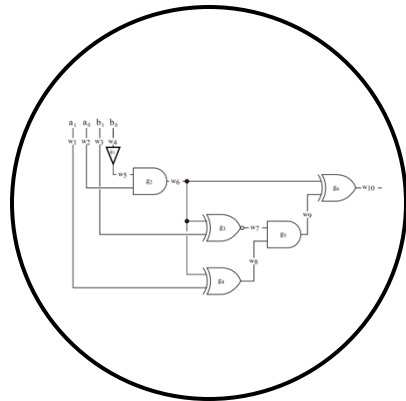
Boolean



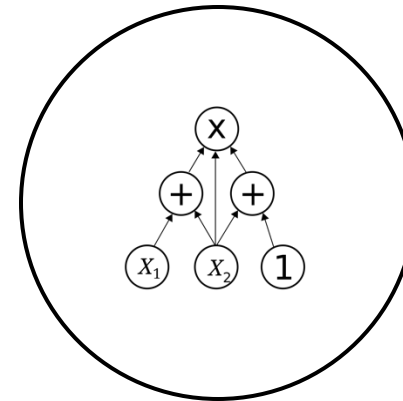
# Motivation

SMC

Boolean



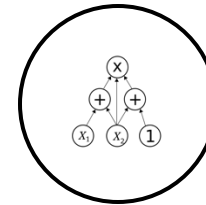
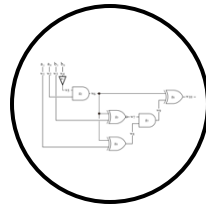
Arithmetic



# Motivation

SMC

Circuit

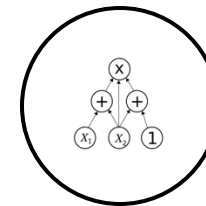
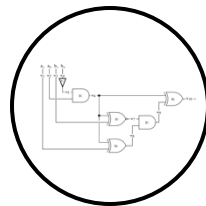


# Motivation

SMC

Primitive

Circuit



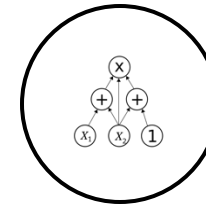
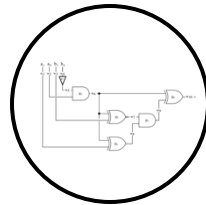
# Motivation

SMC

Primitive

Oblivious  
Transfer

Circuit



# Motivation

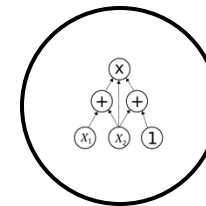
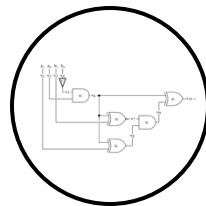
SMC

Primitive

Oblivious  
Transfer

Oblivious  
Linear  
Evaluation

Circuit



# Motivation

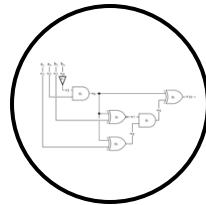
## SMC

Classic

Oblivious  
Transfer

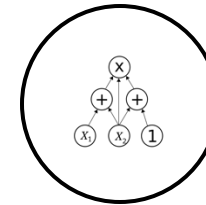
Primitive

Circuit



Classic

Oblivious  
Linear  
Evaluation



# Motivation

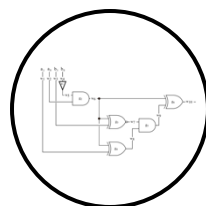
SMC

# Quantum

## Classic

## Primitive

## Oblivious Transfer

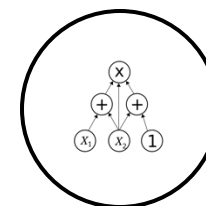


## Circuit

# Quantum

## Classic

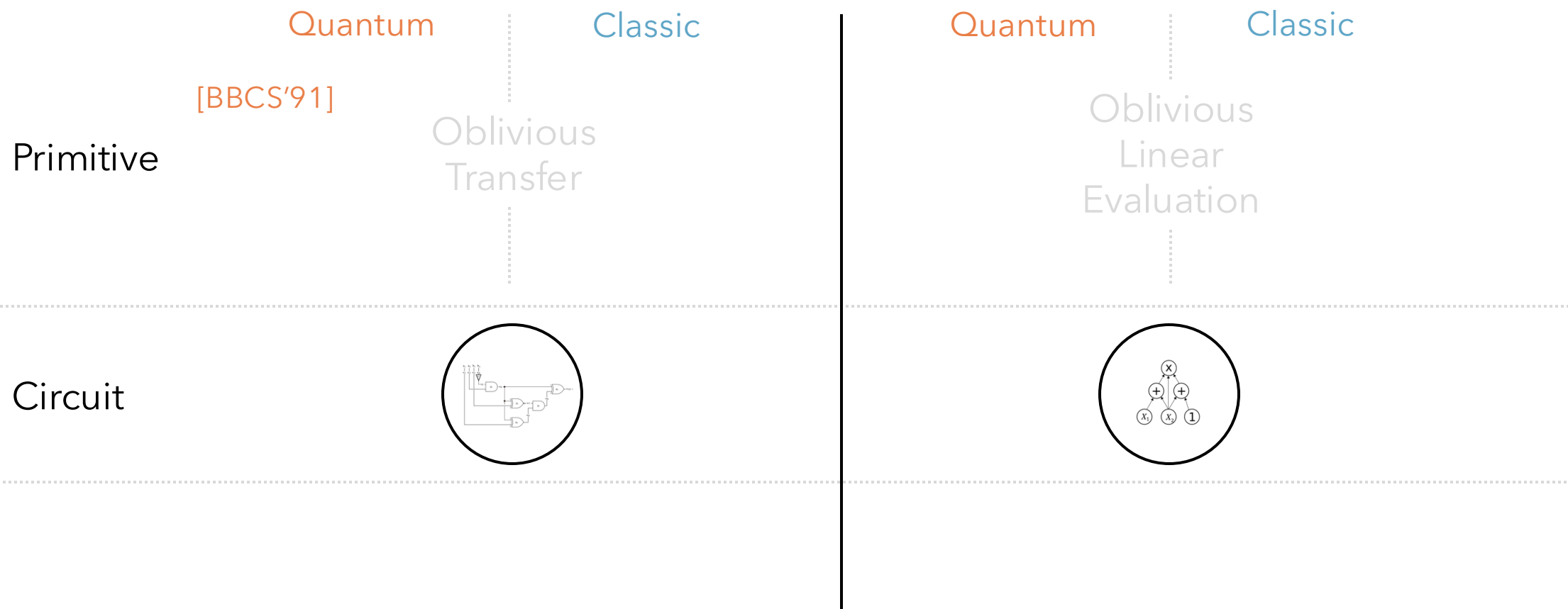
# Oblivious Linear Evaluation





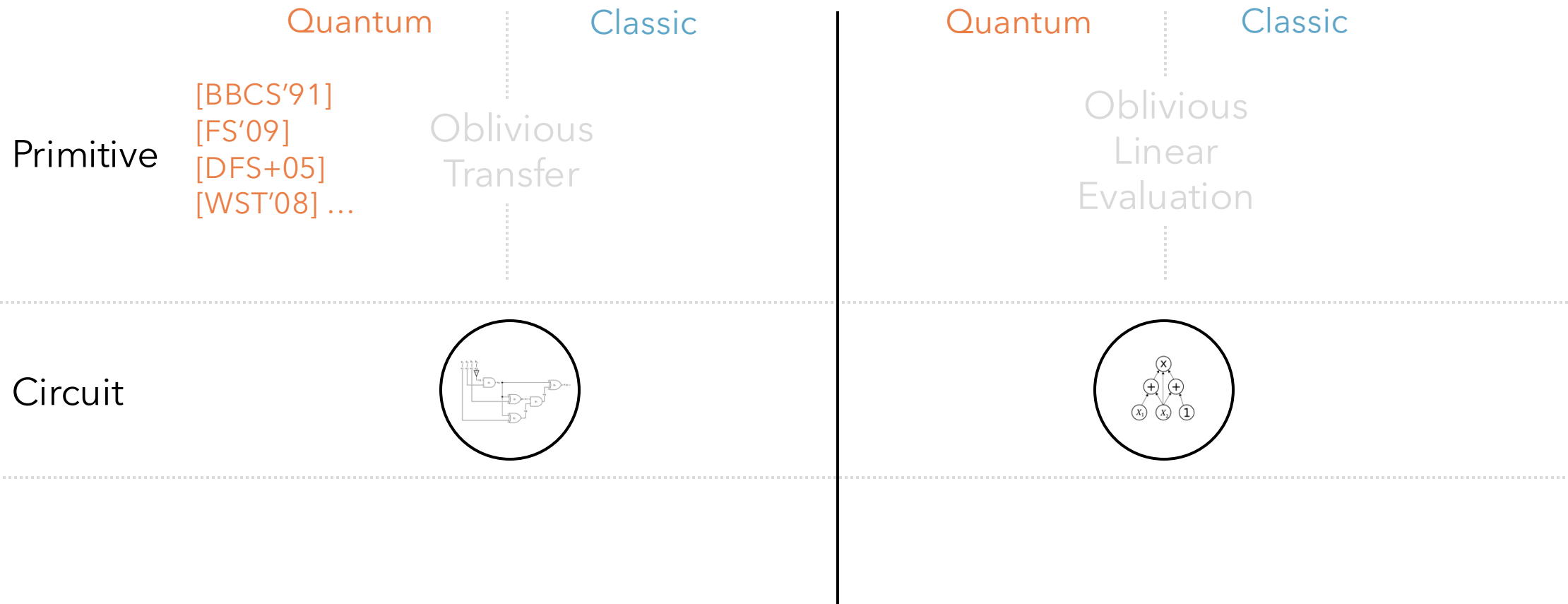
# Motivation

## SMC



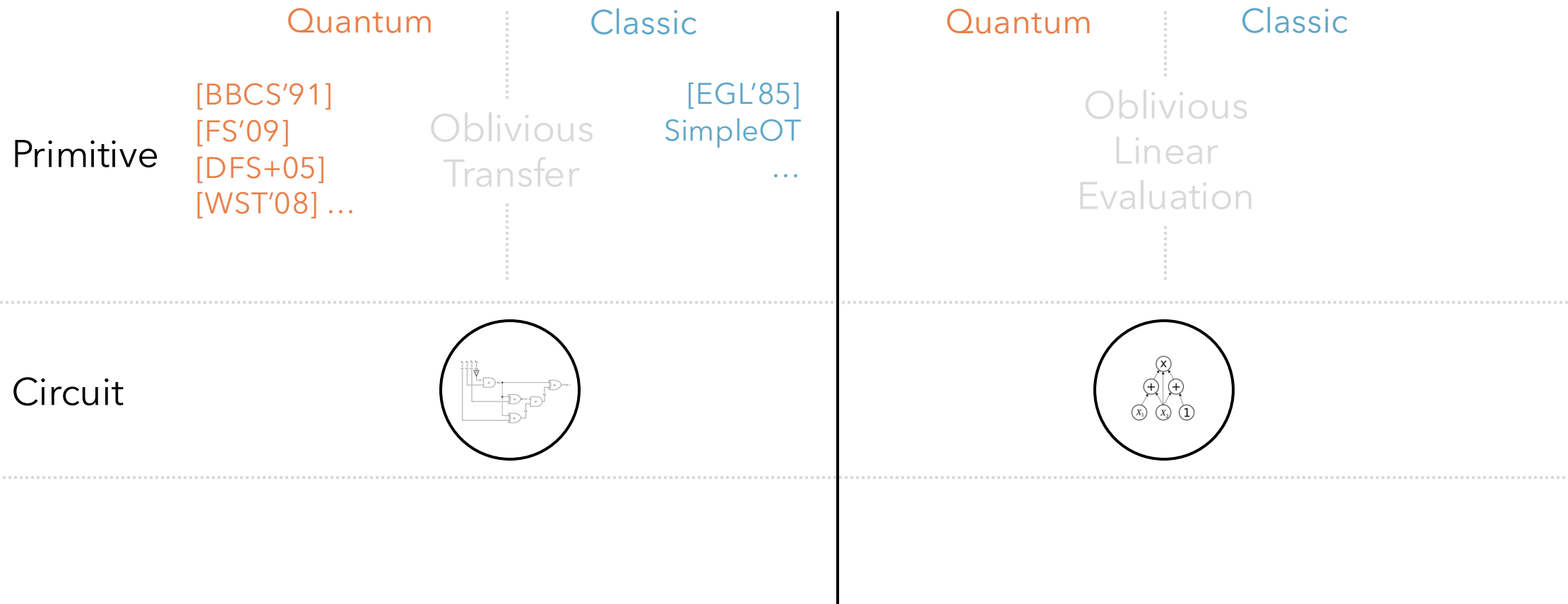
# Motivation

## SMC



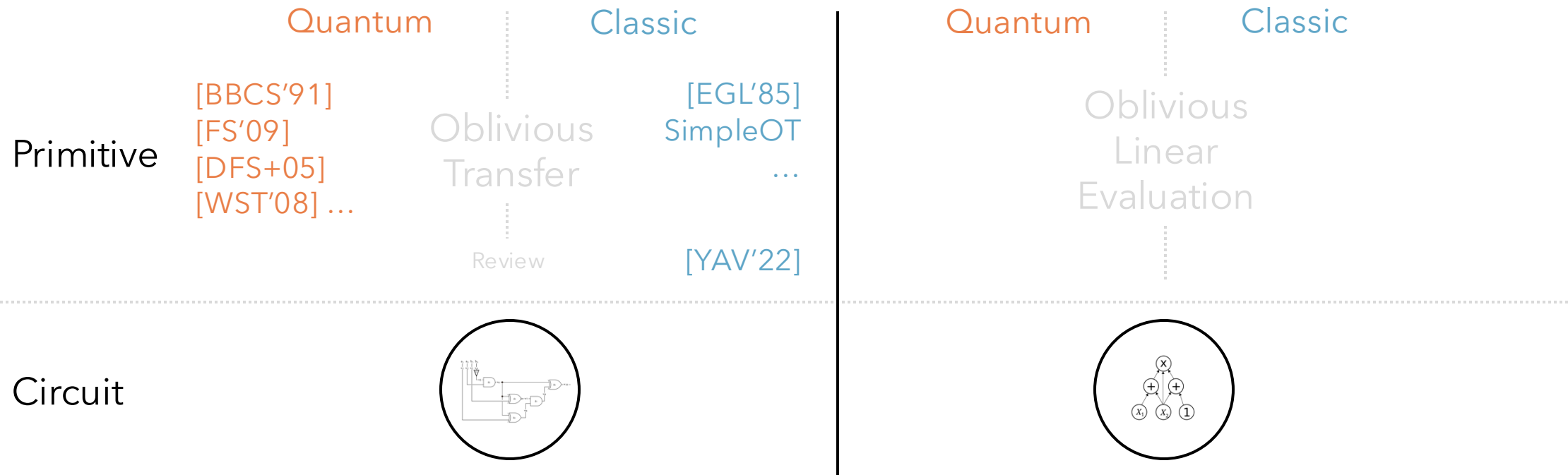
# Motivation

## SMC



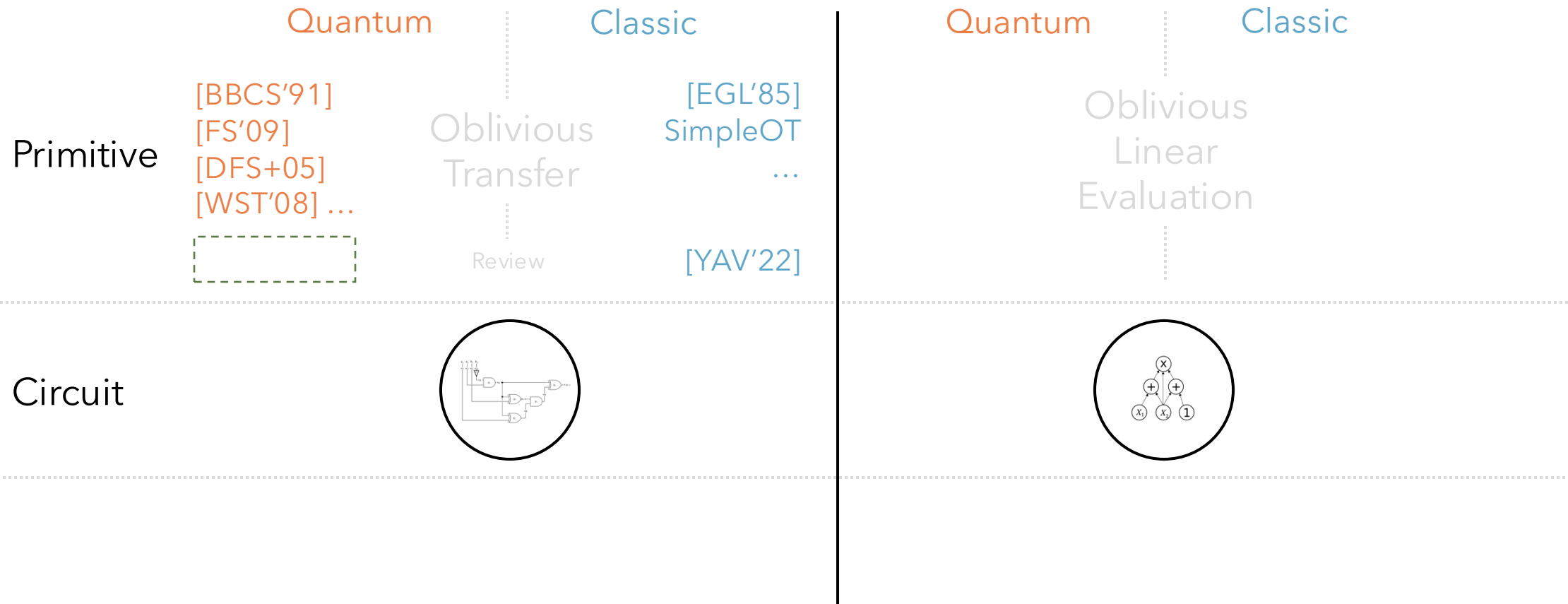
# Motivation

## SMC

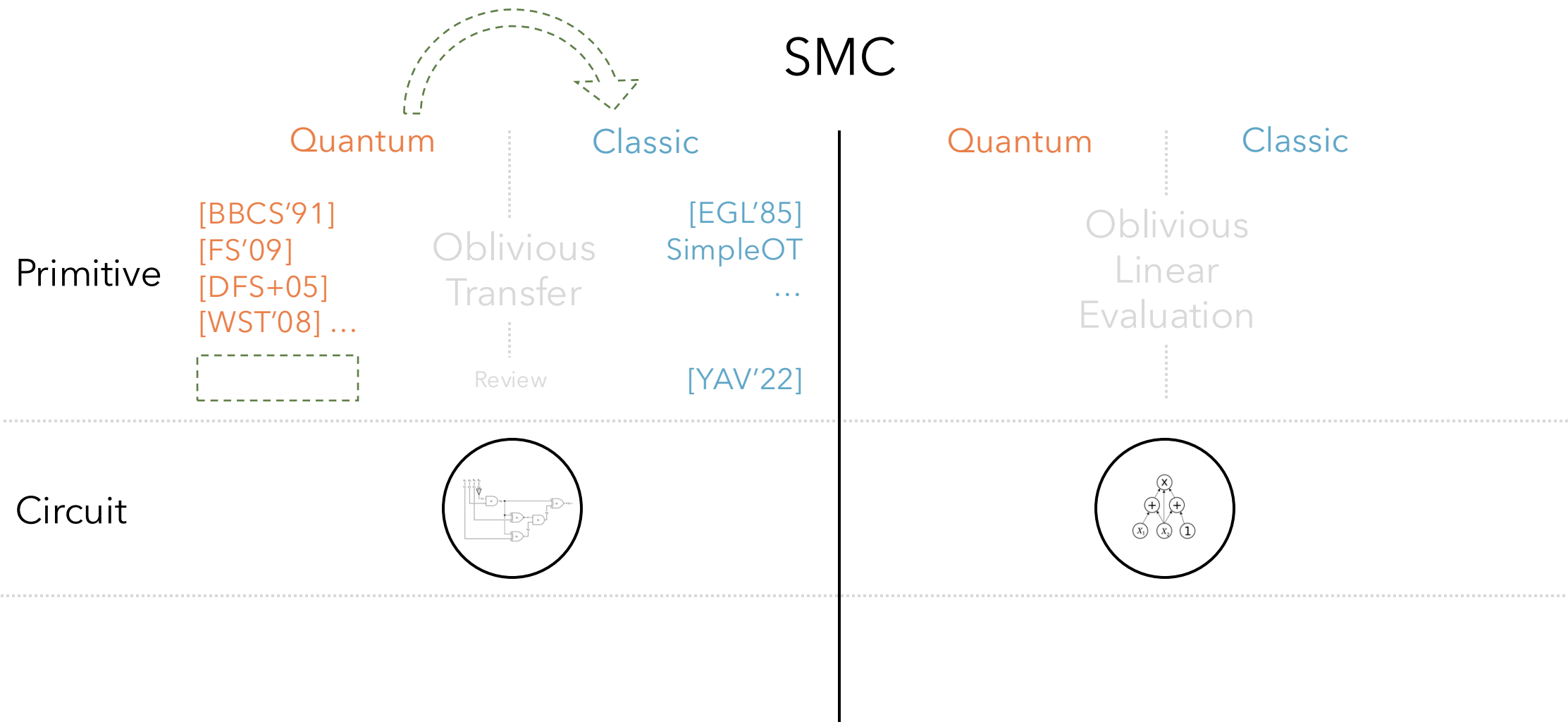


# Motivation

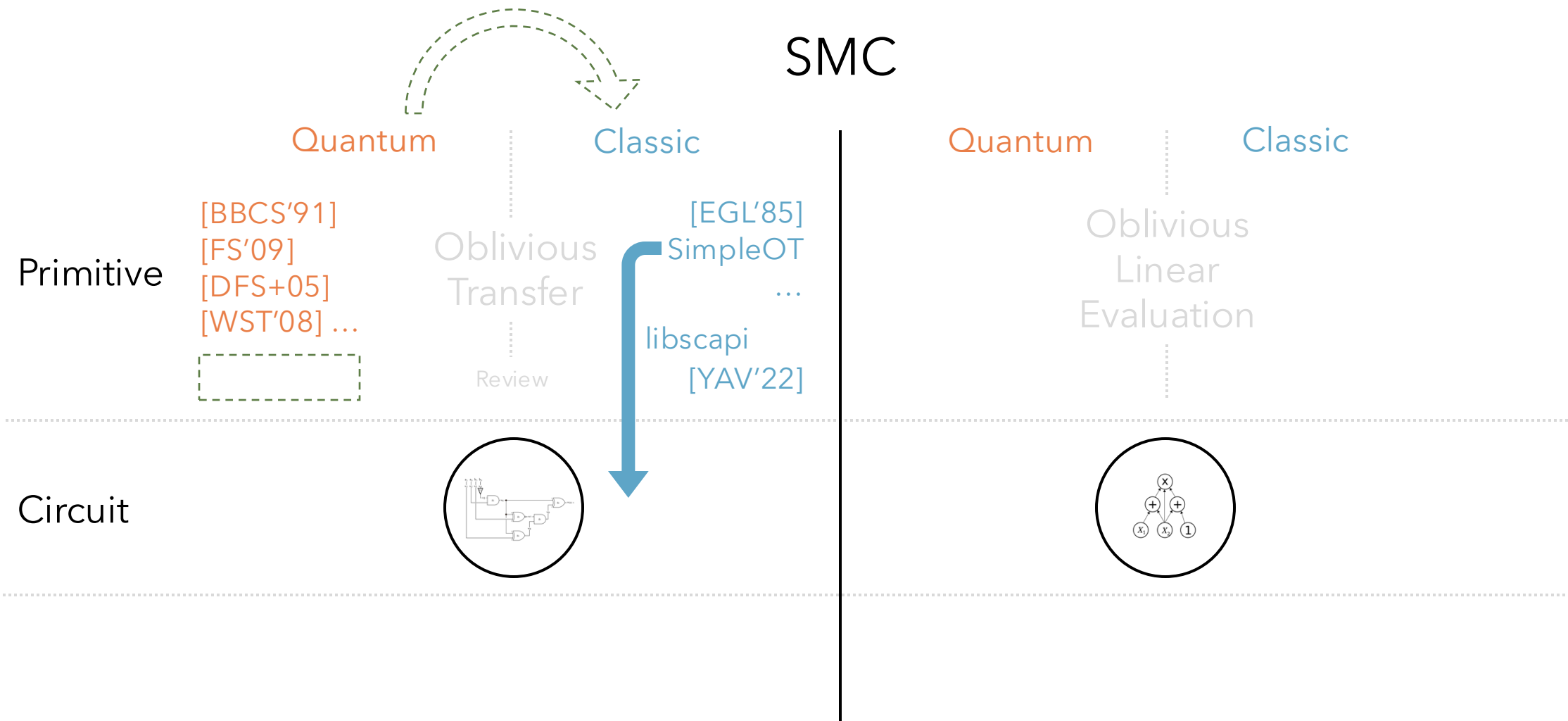
## SMC



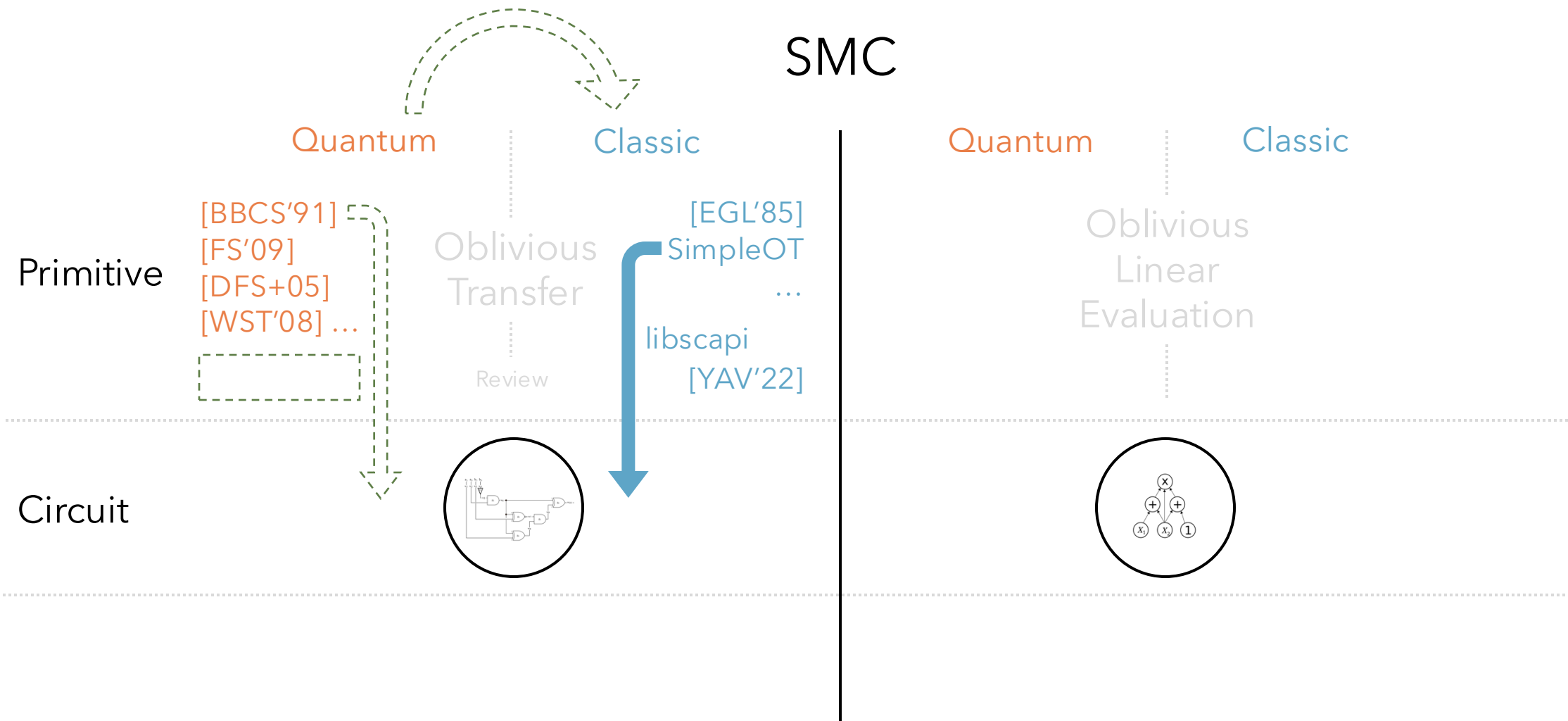
# Motivation



# Motivation

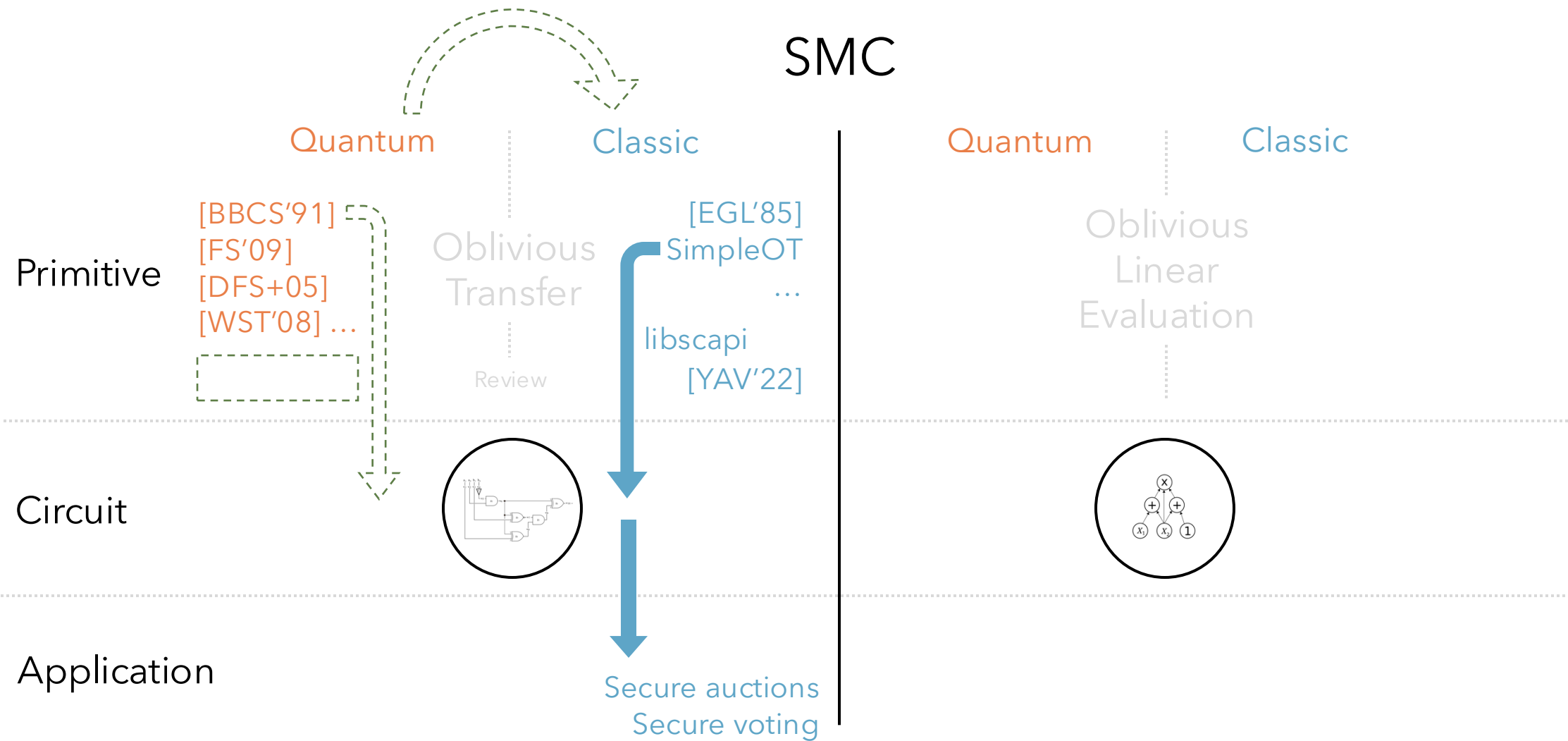


# Motivation

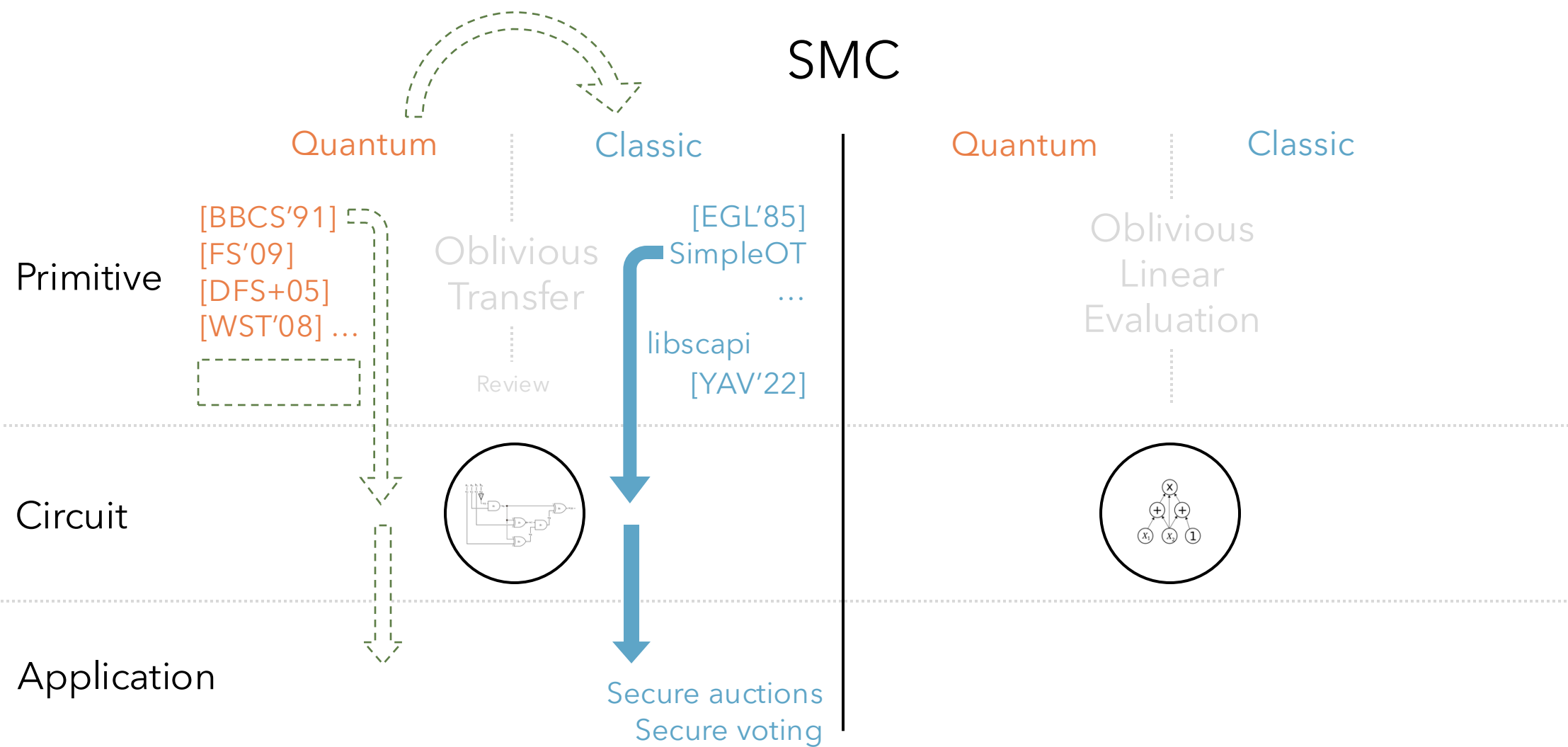




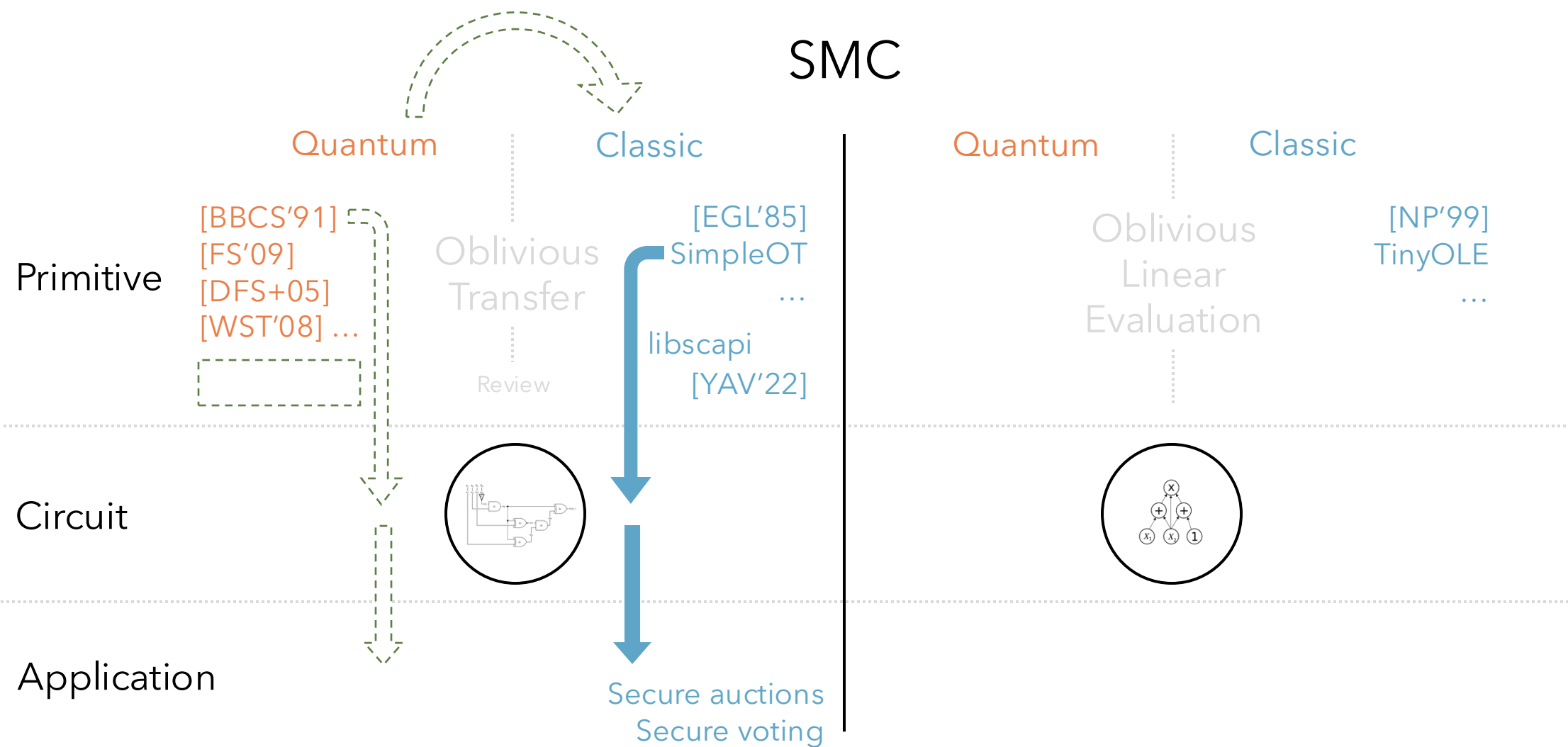
# Motivation



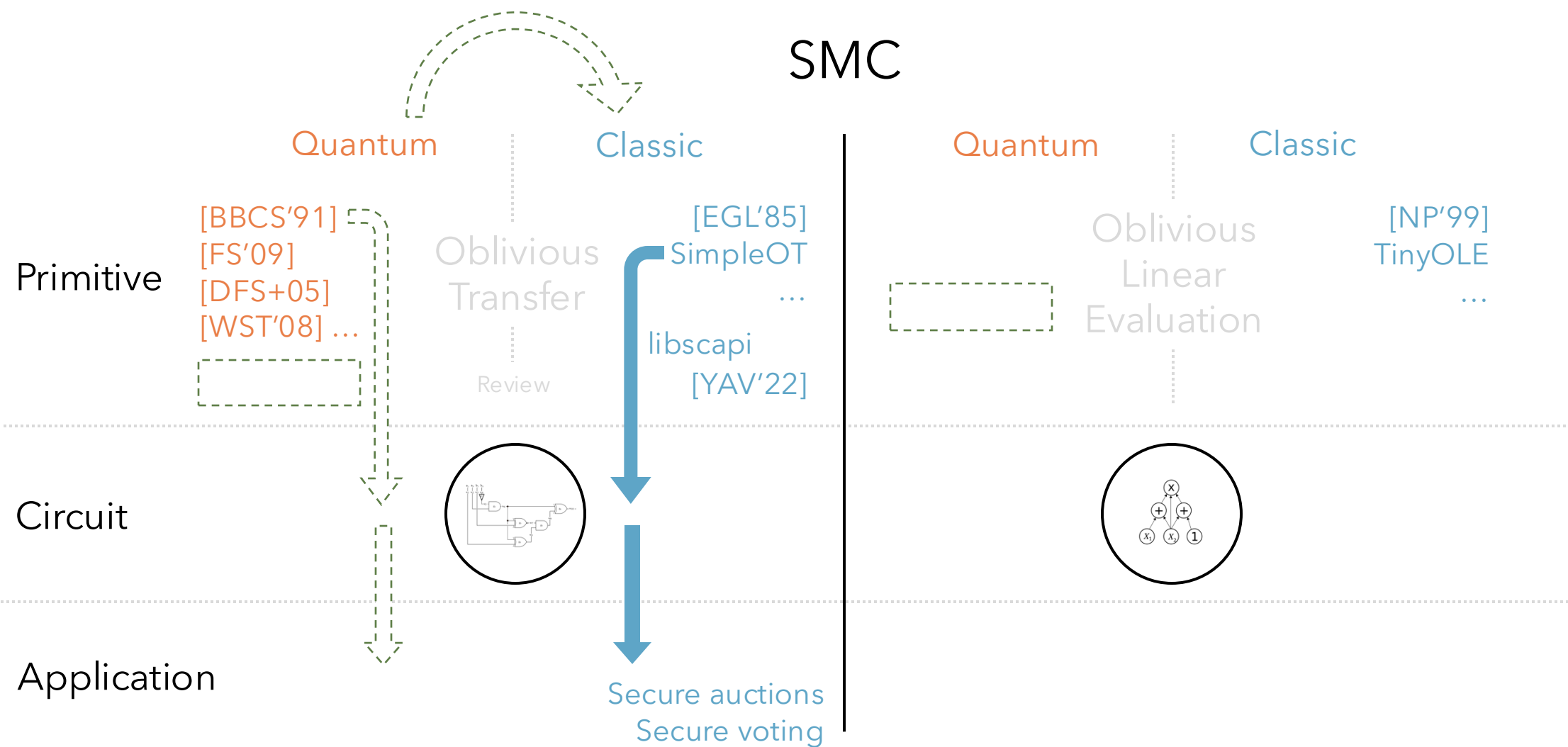
# Motivation



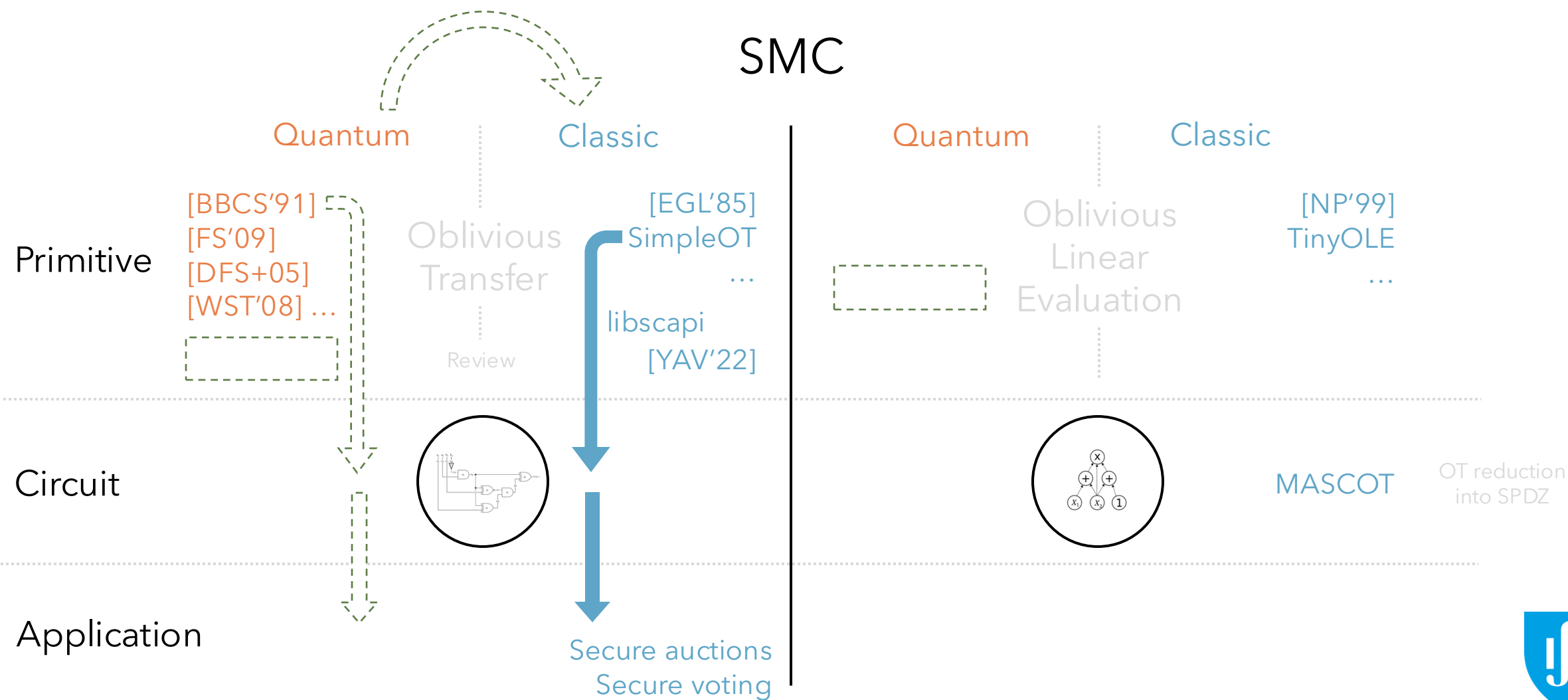
# Motivation



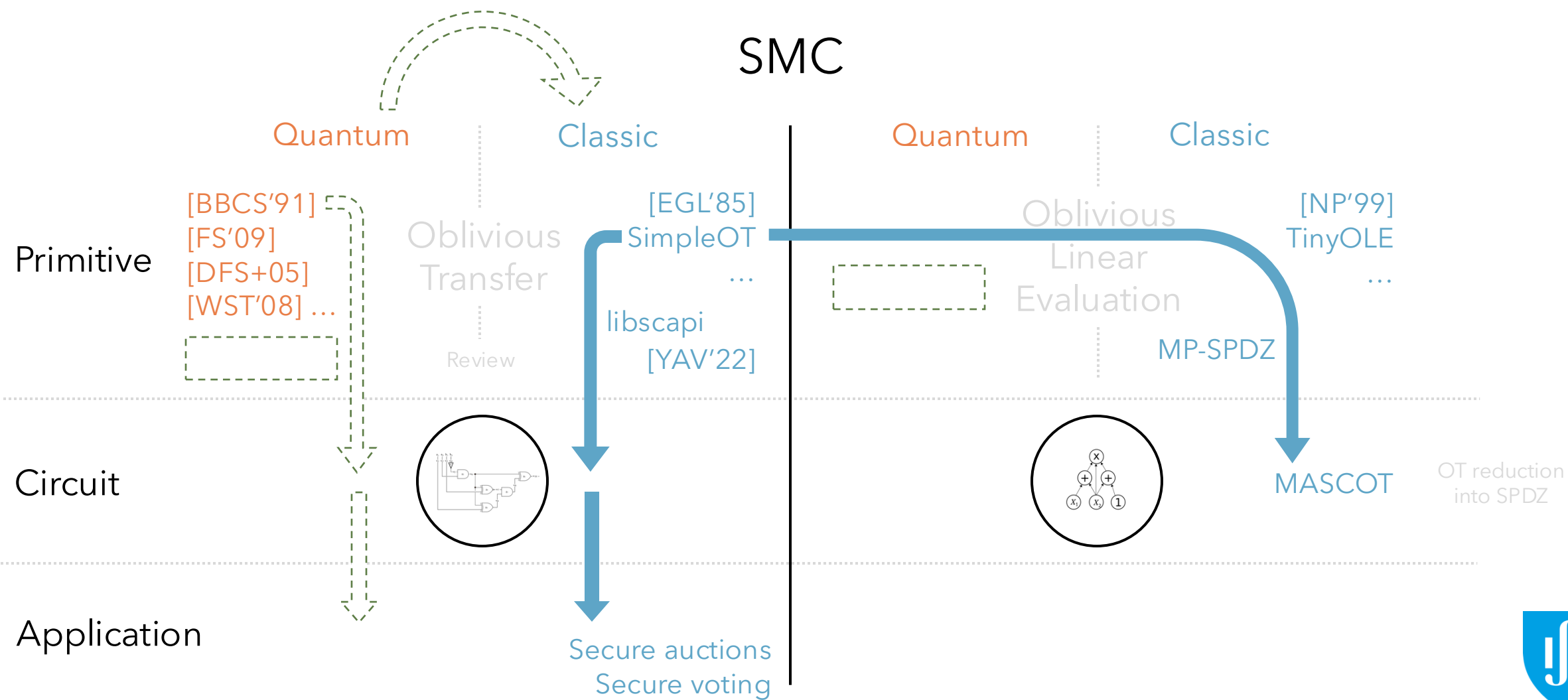
# Motivation



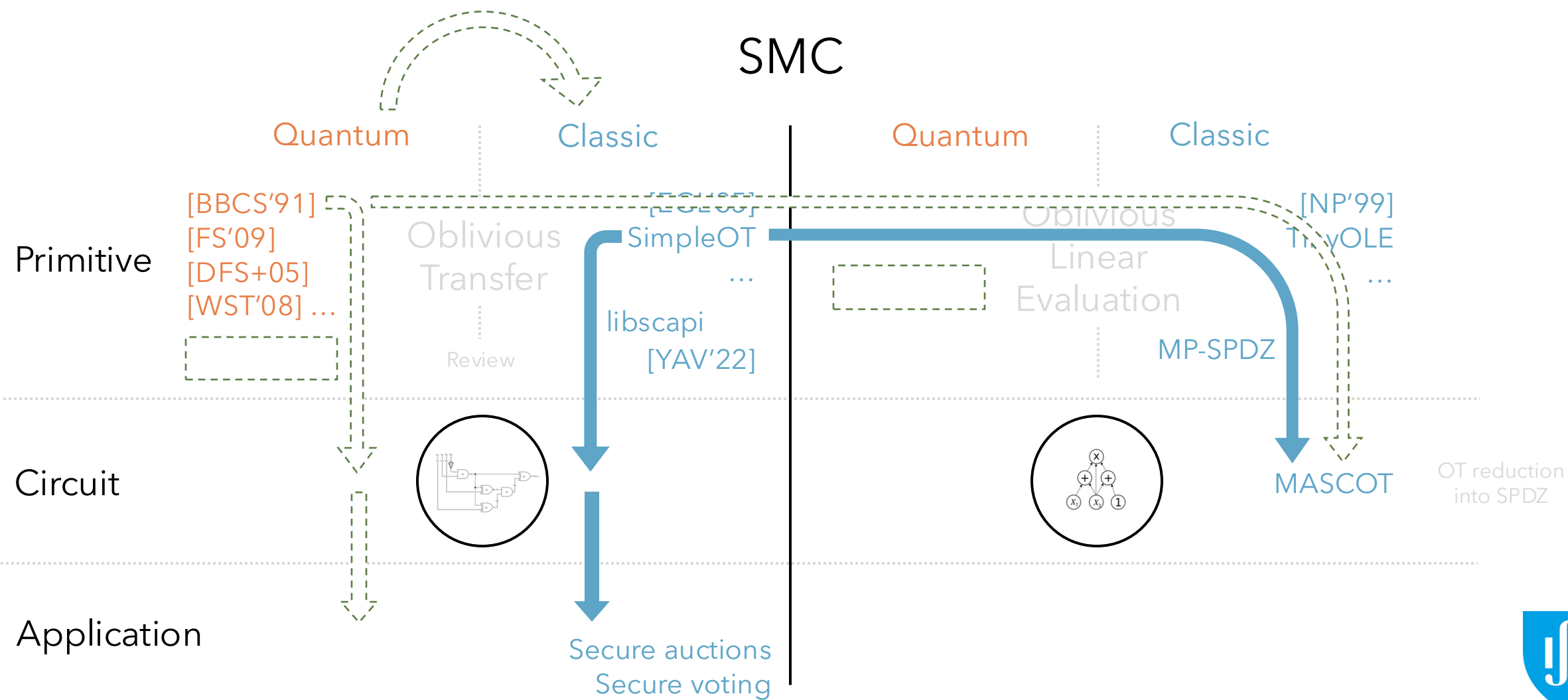
# Motivation



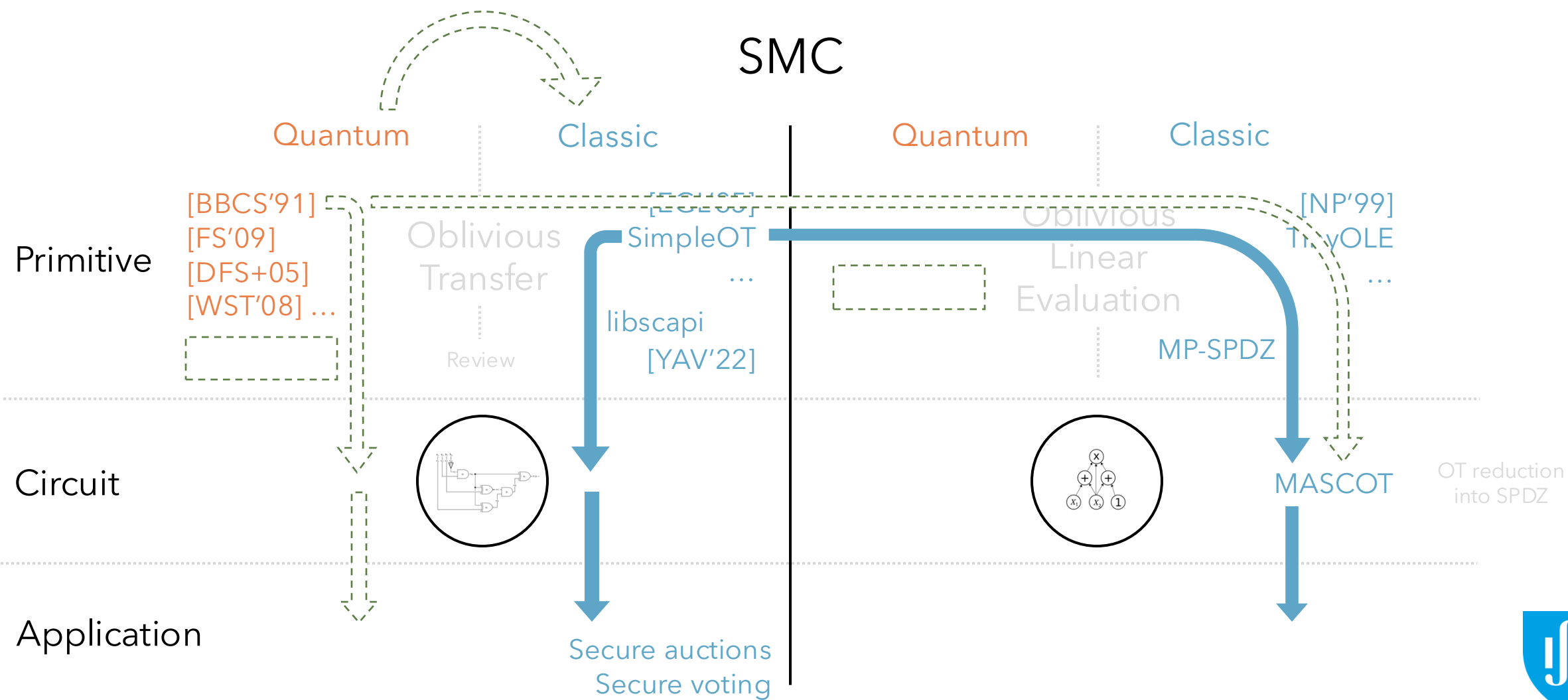
# Motivation



# Motivation

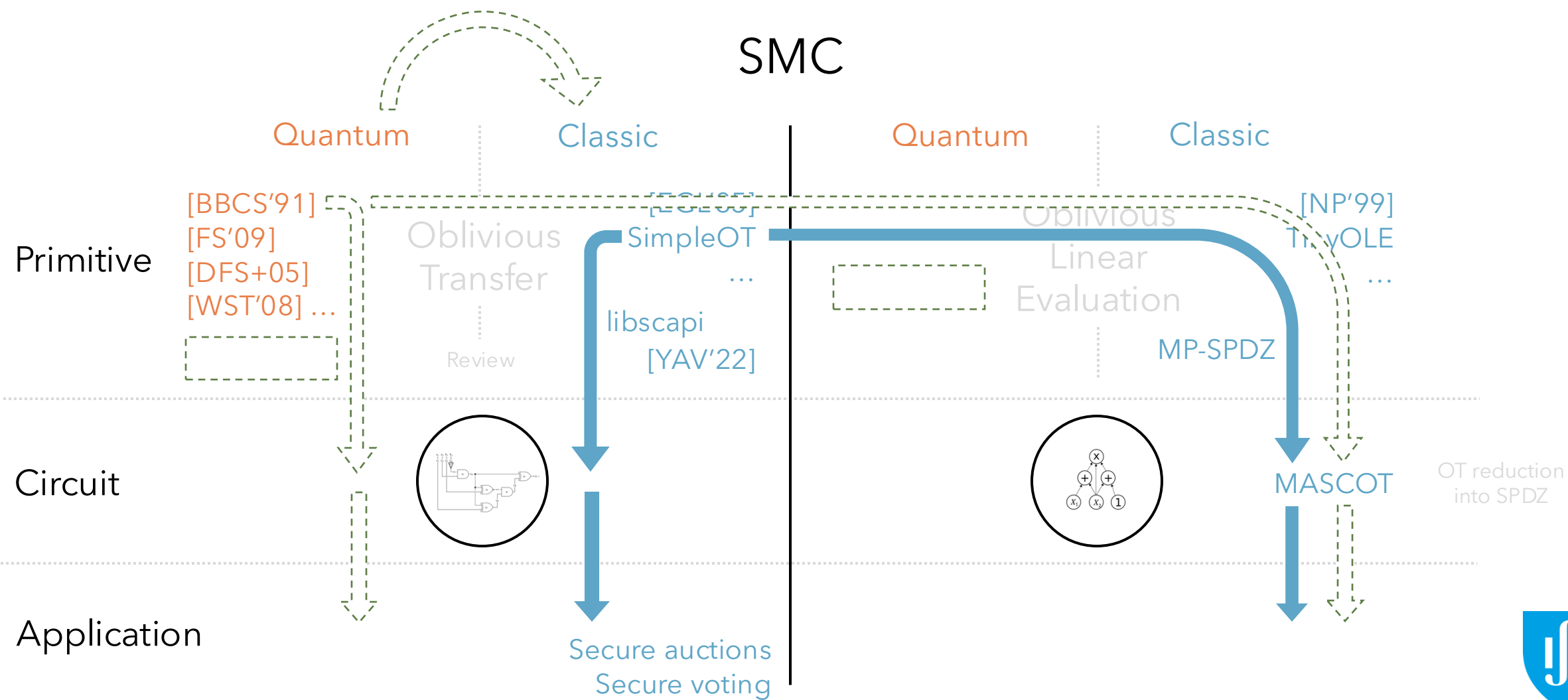


# Motivation

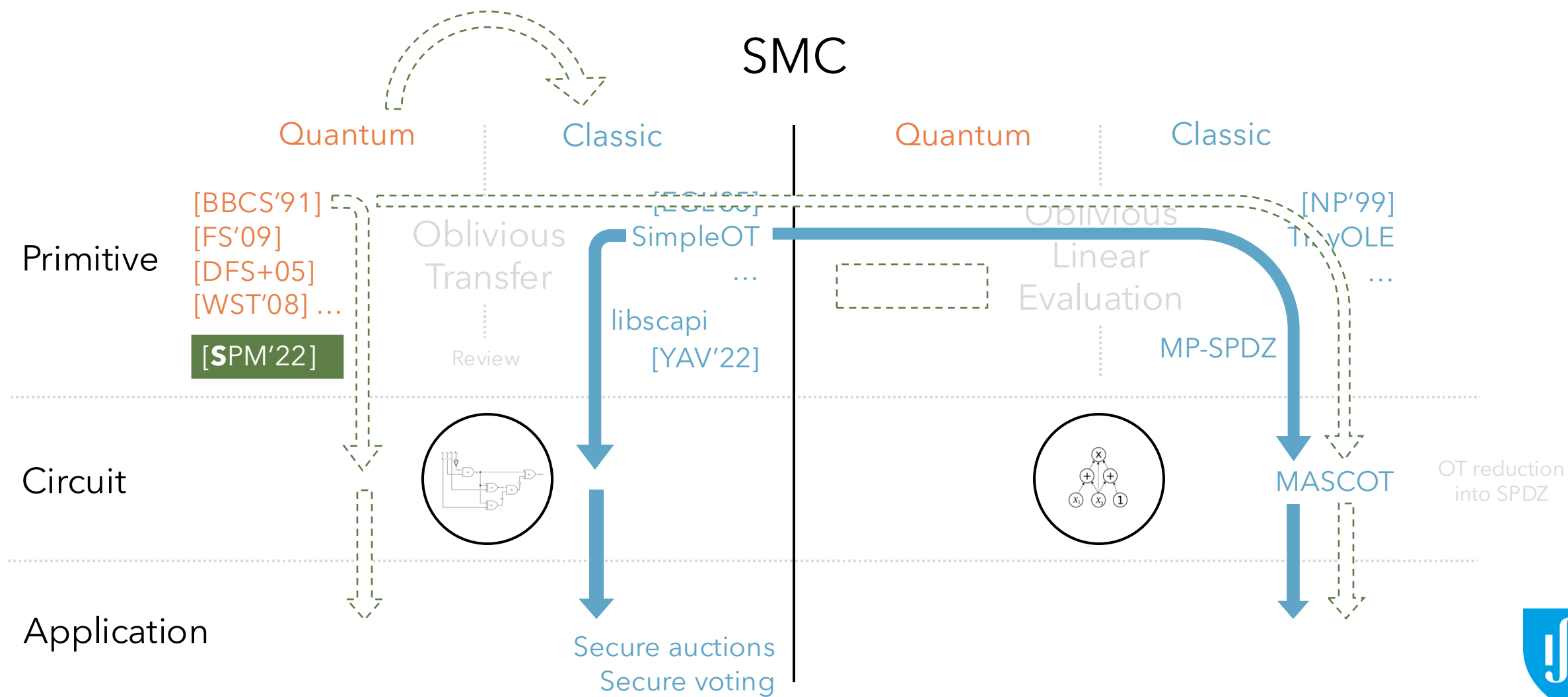




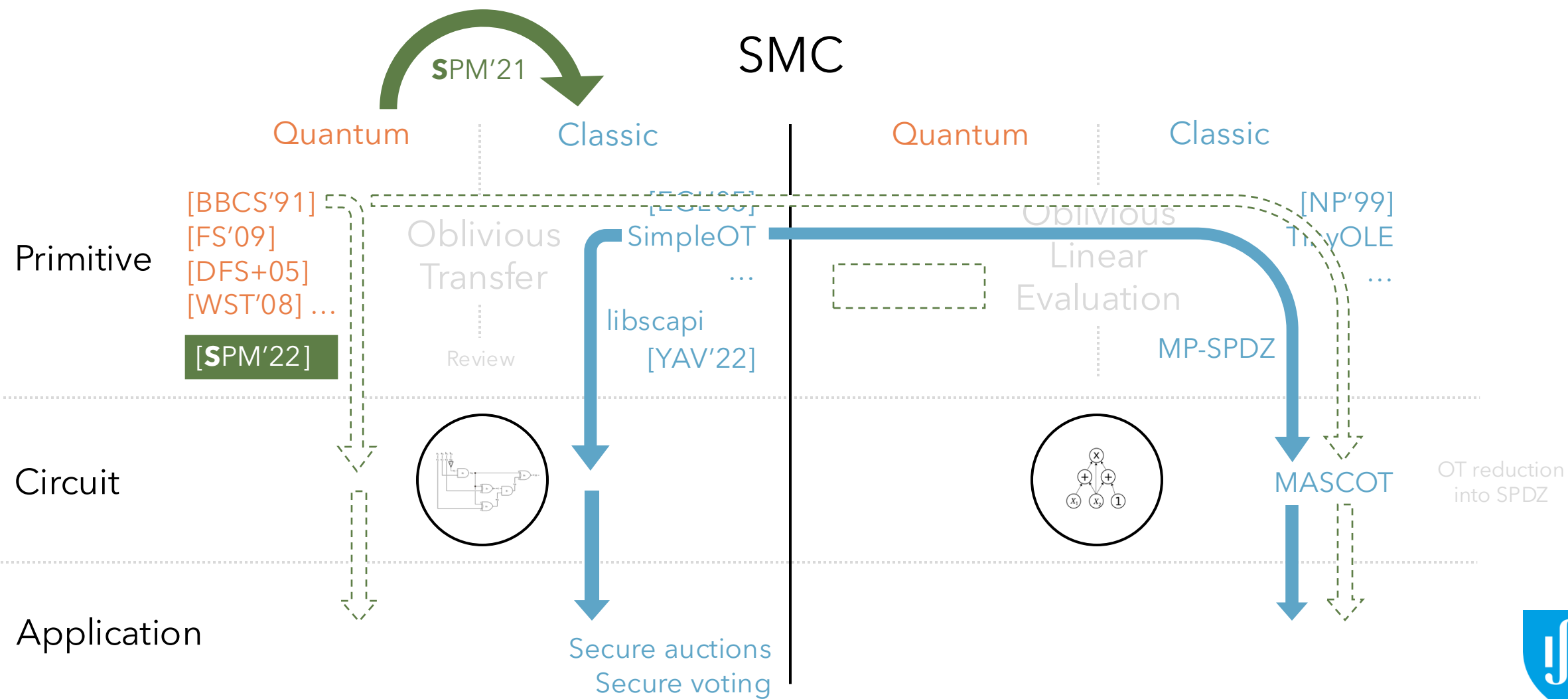
# Motivation



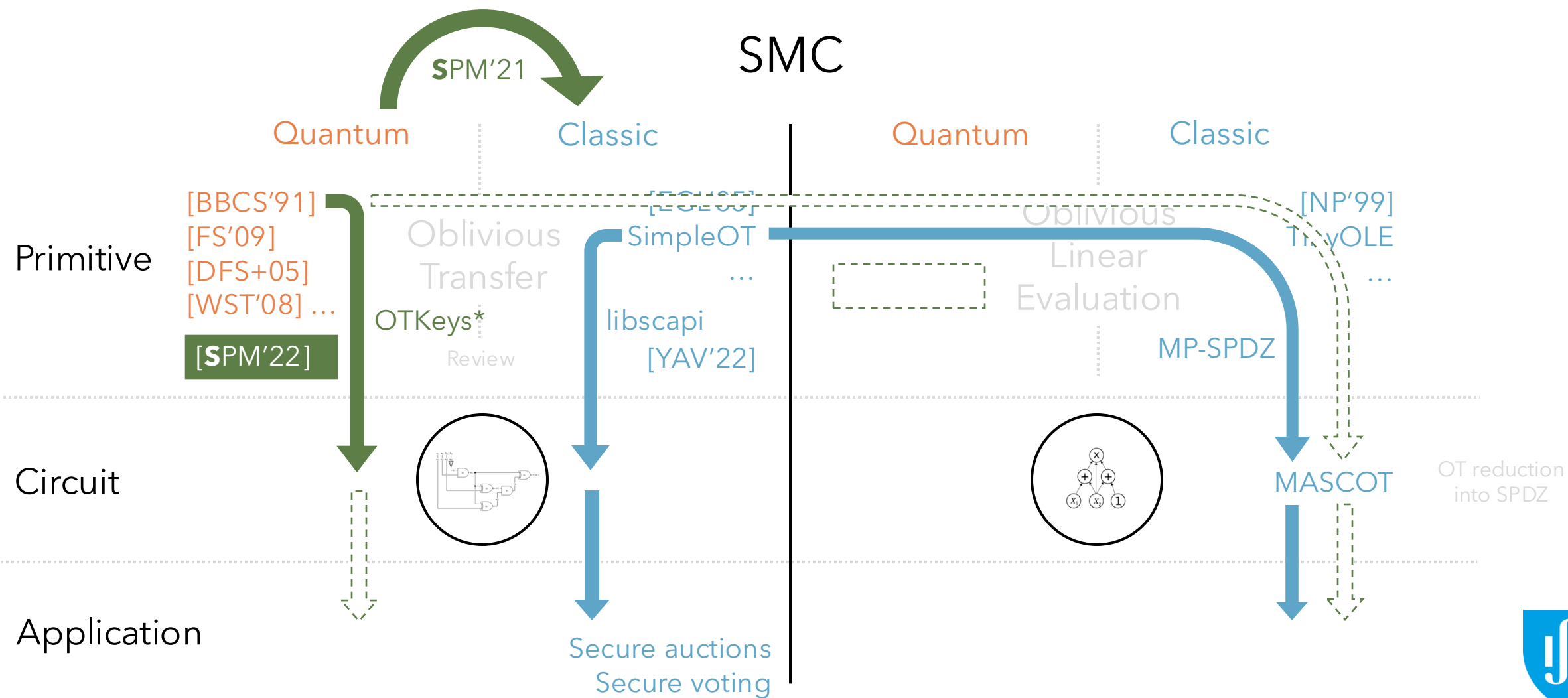
# Outcomes



# Outcomes



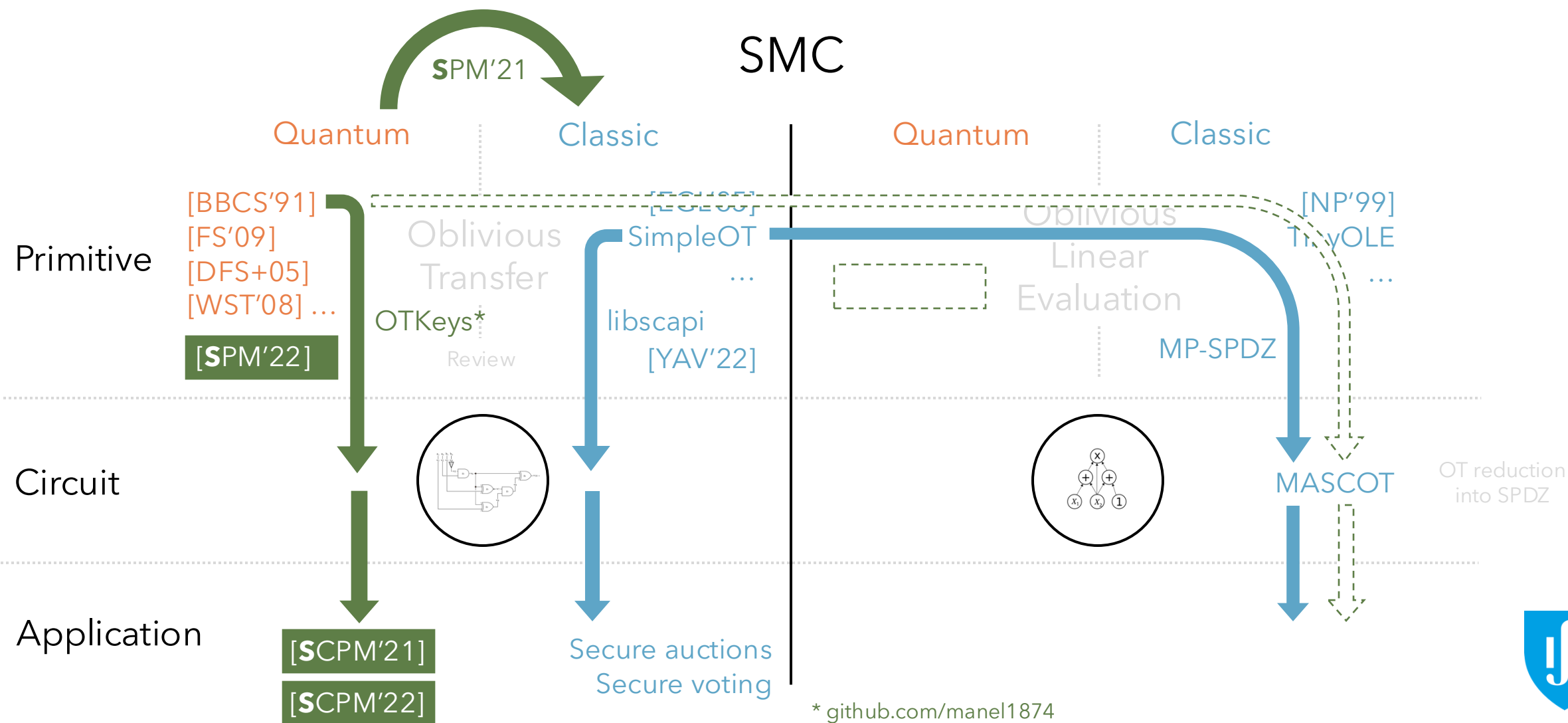
# Outcomes



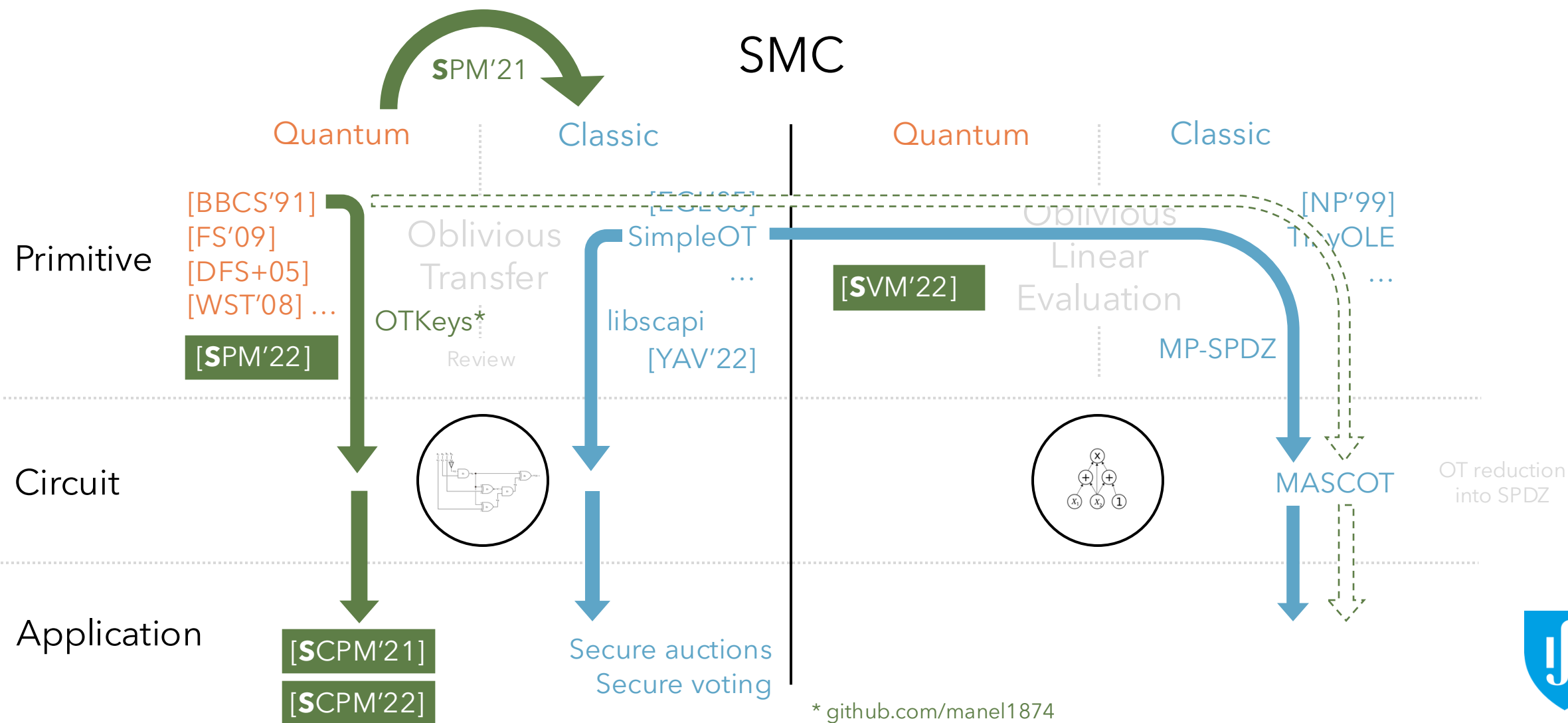
\* [github.com/manel1874](https://github.com/manel1874)



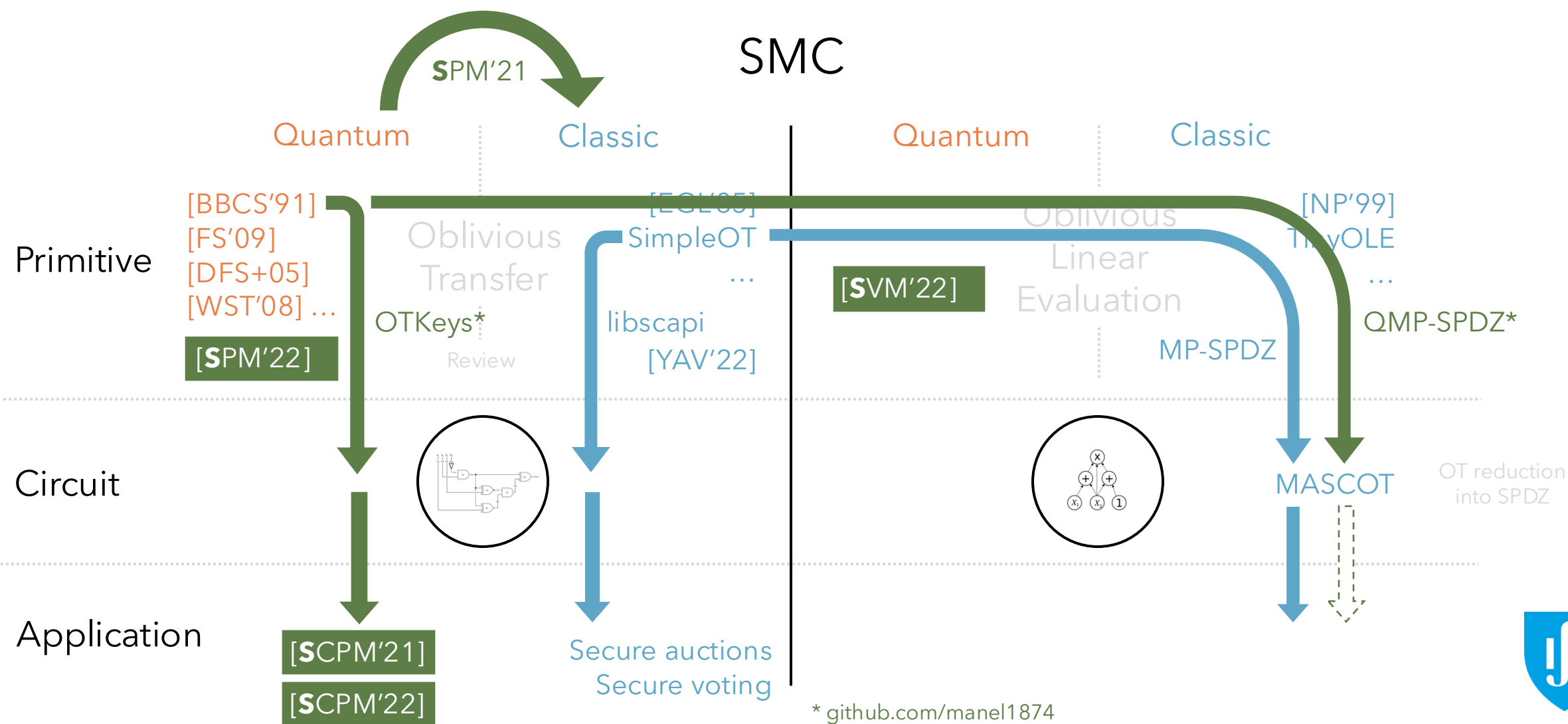
# Outcomes



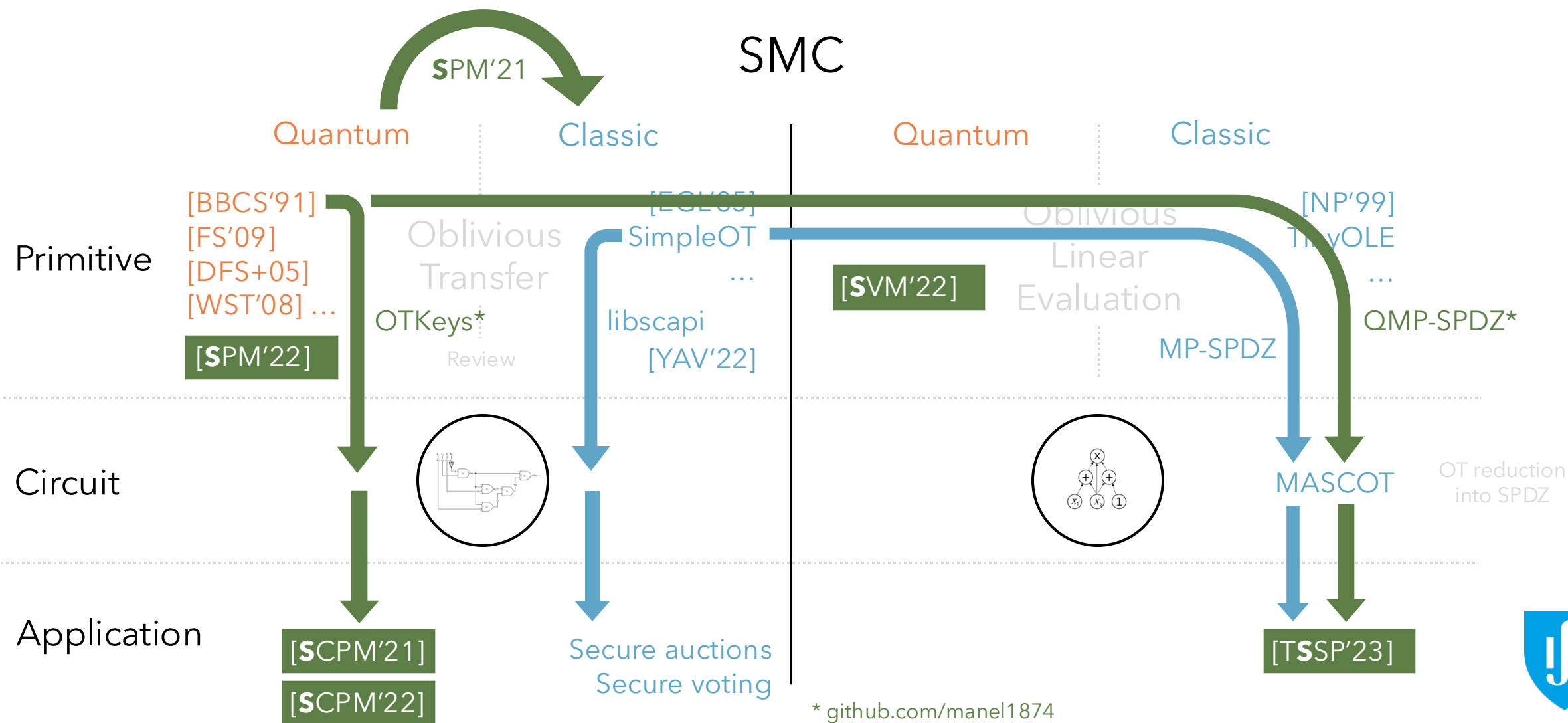
# Outcomes



# Outcomes

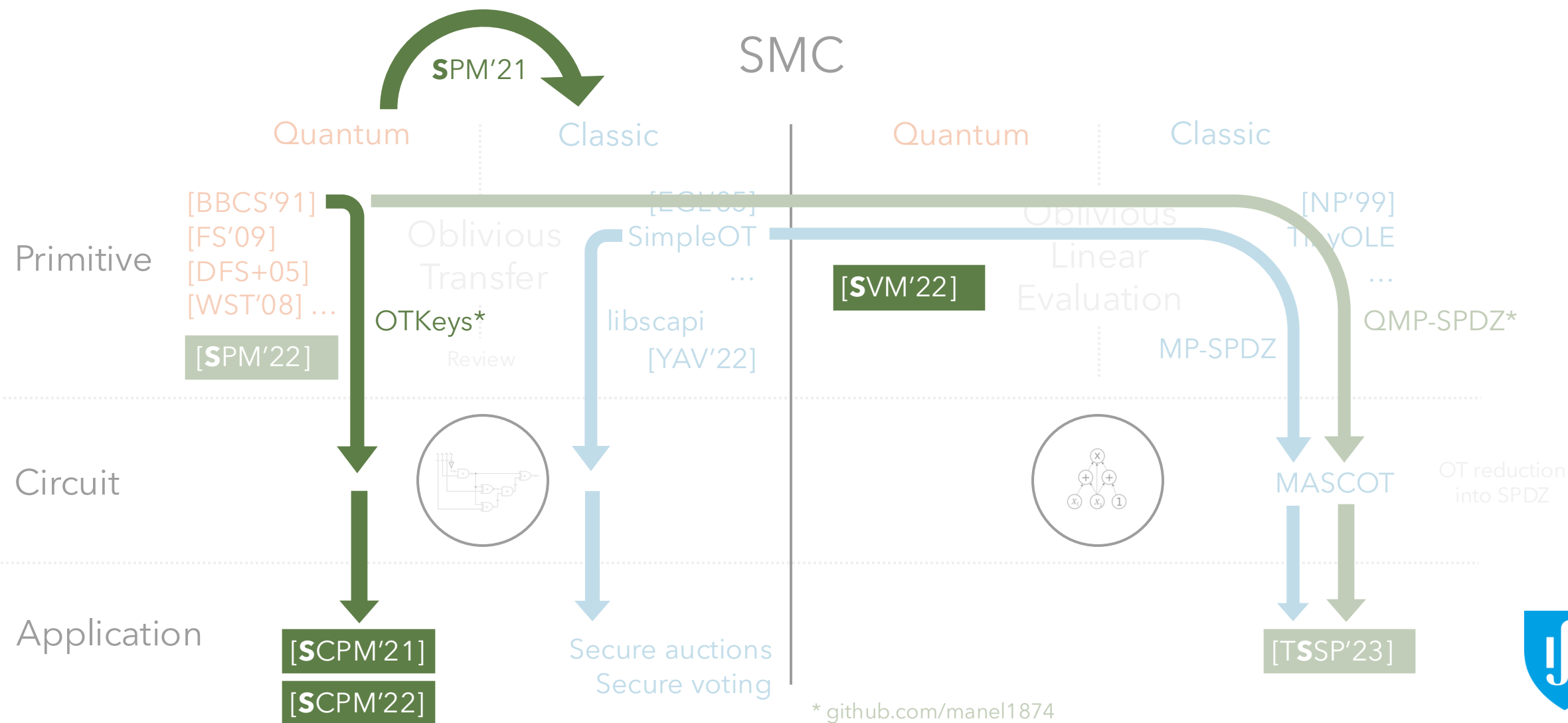


# Outcomes

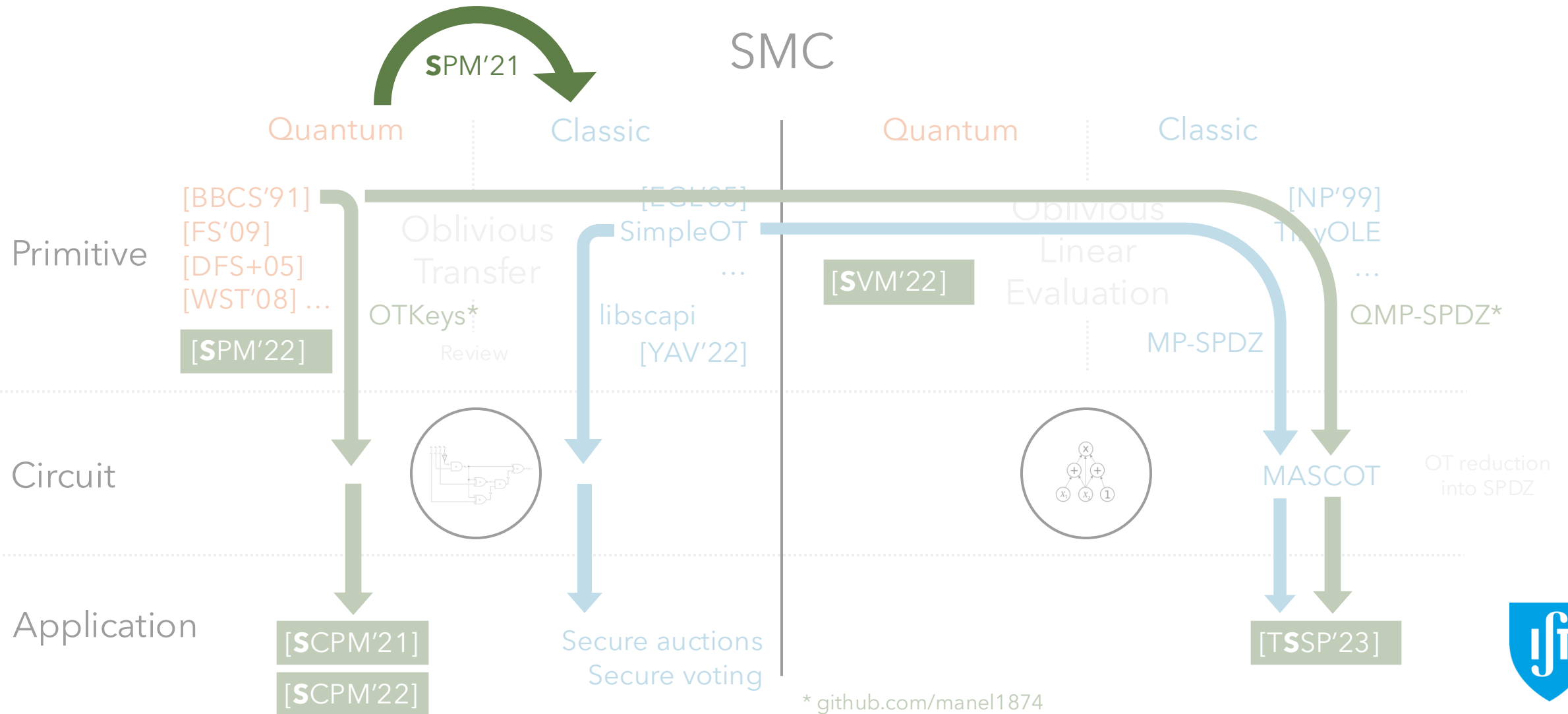




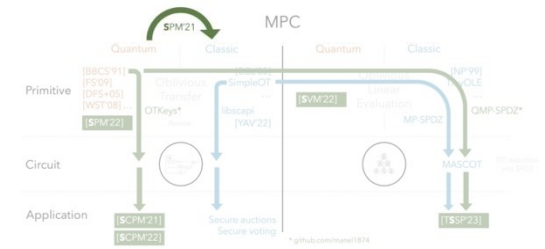
# Outcomes



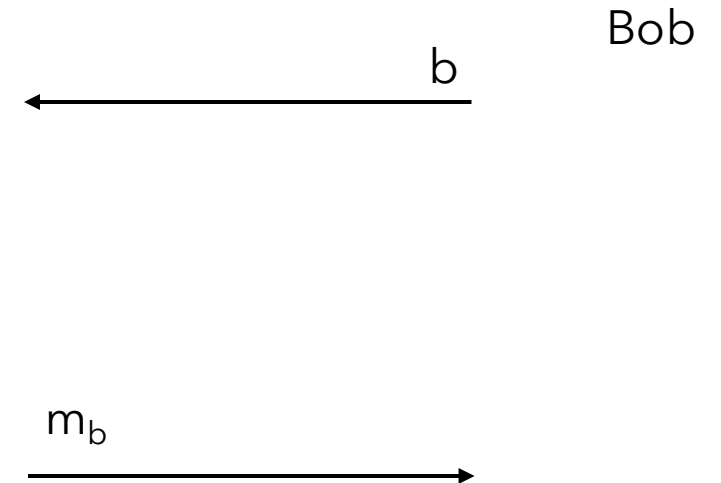
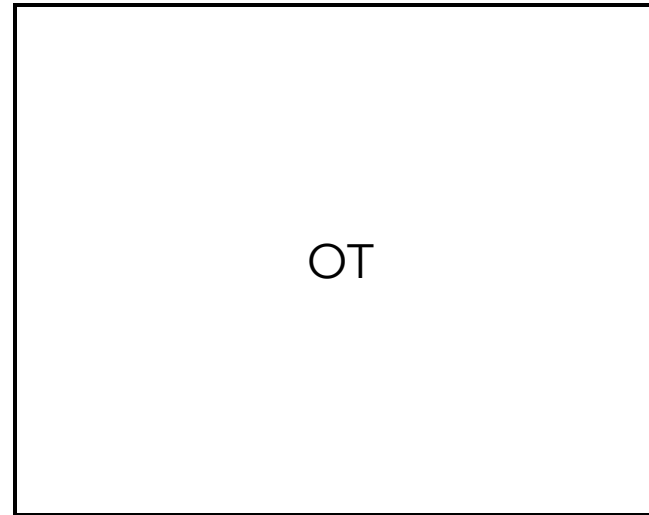
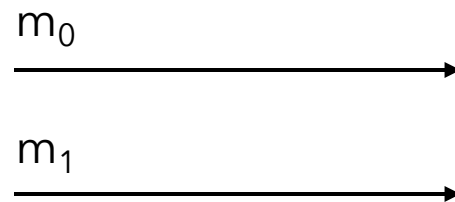
# Quantum and classical OT



# Oblivious Transfer



Alice



The diagram illustrates the evolution of MPC protocols across three rows: Primitive, Circuit, and Application. The diagram is divided into Quantum and Classic phases.

- Primitive:**
  - Quantum:** BB84<sup>[91]</sup>, PSW<sup>[9]</sup>, DPS<sup>[45]</sup>, NIST88<sup>[1]</sup>, SPM22<sup>[22]</sup>.
  - Classic:** Oblivious Transfer, SimpleOT<sup>[1]</sup>, Tlscape<sup>[18]</sup>, Tlscape<sup>[18]</sup>, Tlscape<sup>[18]</sup>.
- Circuit:**
  - Quantum:** A quantum circuit diagram showing a T gate and a CNOT gate.
  - Classic:** A classical circuit diagram showing a T gate and a CNOT gate.
- Application:**
  - Quantum:** SCFM21<sup>[21]</sup>, Secure auctions, Secure voting.
  - Classic:** TSP23<sup>[23]</sup>, MAScot<sup>[20]</sup>, TSP23<sup>[23]</sup>.

A green arrow labeled SPM21 points from the Quantum phase to the Classic phase in the Primitive row.

- [BBCS'91]
- [DFS+05]
- [WST'08]
- [FS'09]
- ...

- [EGL'85]
- [BM'89]
- [NP'01]
- SimpleOT
- ...

No previous work

# How can we compare?

The diagram illustrates the evolution of MPC protocols across three rows: Primitive, Circuit, and Application. The diagram is divided into Quantum and Classic phases.

- Primitive:**
  - Quantum:** [BBC<sup>+</sup>91], [PSW99], [DPS+05], [MST08], [SPM22]
  - Classic:** [Oblivious Transfer], [OTkeys\*], [SimpleOT], [Ibscp1], [WAV22], [SVM22], [Linear Evaluation], [MP-SPDZ], [NMP99], [NIOLE], [QMP-SPDZ\*]
- Circuit:**
  - Quantum:** (Circuit diagram)
  - Classic:** [MASCOT]
- Application:**
  - Quantum:** [SCPM21]
  - Classic:** [Secure auctions], [Secure voting], [TSP23]

A green arrow labeled SPM21 points from the Quantum phase to the Classic phase in the Primitive row.

\* github.com/mayne1874

## Classic

- [EGL'85]
- [BM'89]
- [NP'01]
- SimpleOT
- ...

No previous work

# How can we compare?

Comparable structure?  
Corresponding phases with same technology?  
Any practical insight?

The diagram illustrates the evolution of MPC protocols across three rows: Primitive, Circuit, and Application. The diagram is divided into Quantum and Classic phases.

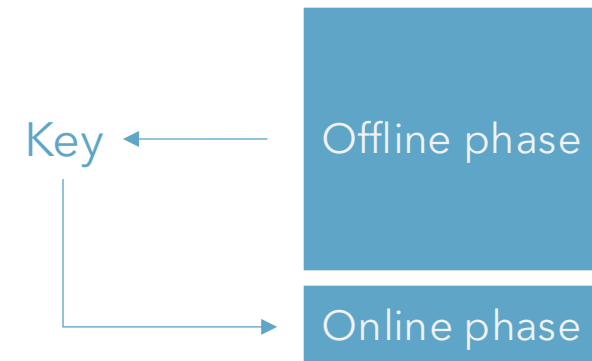
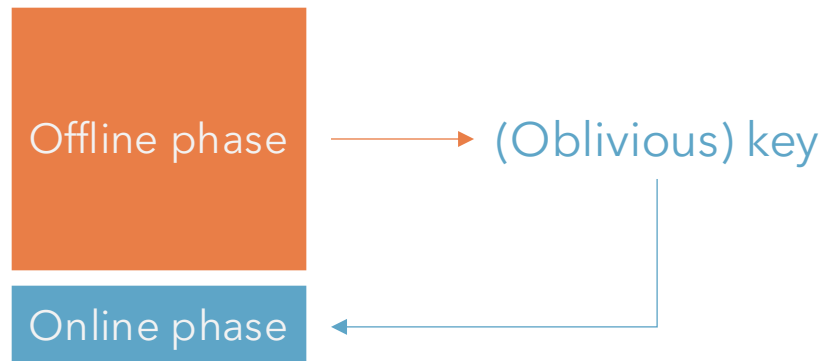
- Primitive:**
  - Quantum:** [BBC<sup>+</sup>91], [PSW99], [DPS+05], [MST08], [SPM22]
  - Classic:** [Oblivious Transfer], [OTkeys\*], [SimpleOT], [Ibscp], [WAV22], [SVM22], [Linear Evaluation], [MP-SPDZ], [NM<sup>+</sup>99], [NCOLE], [OMP-SPDZ\*]
- Circuit:**
  - Quantum:** (Circuit diagram)
  - Classic:** [MASCOT]
- Application:**
  - Quantum:** [SCPM21]
  - Classic:** [Secure auctions], [Secure voting], [TSP23]

A green arrow labeled SPM21 points from the Quantum phase to the Classic phase in the Primitive row.

\* github.com/mayne1874

Classic

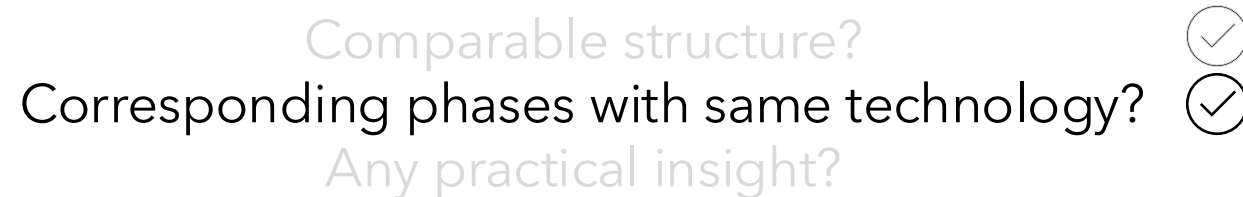
Base OT      OT Extension



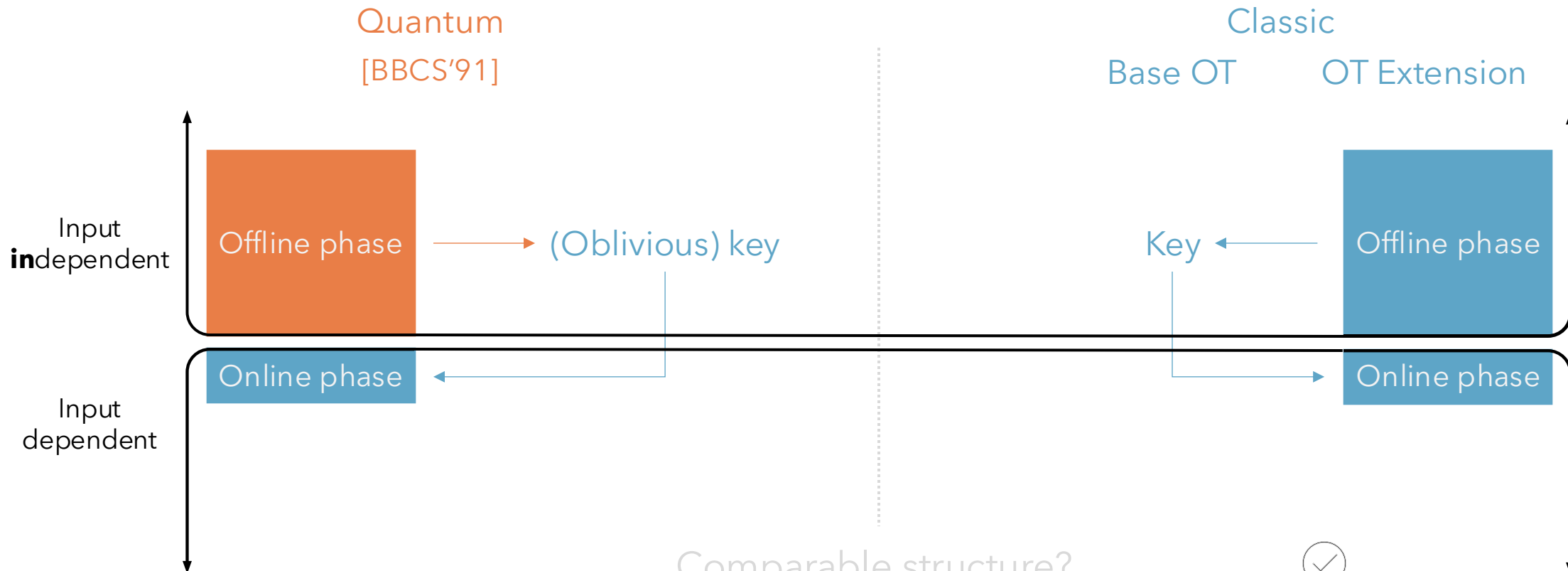
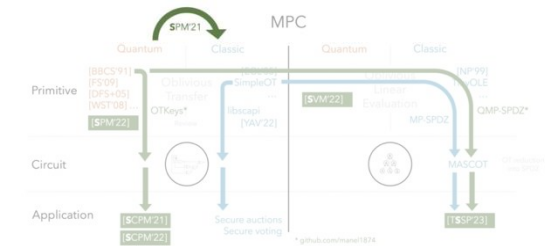
The diagram illustrates the evolution of MPC protocols across three rows: Primitive, Circuit, and Application. The diagram is divided into Quantum and Classic phases.

- Primitive:**
  - Quantum:** BB84<sup>[91]</sup>, PSW<sup>[9]</sup>, DPS<sup>[45]</sup>, NIST88<sup>[1]</sup>, SPM22<sup>[22]</sup>.
  - Classic:** Oblivious Transfer, SimpleOT<sup>[1]</sup>, Tlscape<sup>[18]</sup>, Tlscape<sup>[18]</sup>, Tlscape<sup>[18]</sup>.
- Circuit:**
  - Quantum:** A quantum circuit diagram showing a T gate and a CNOT gate.
  - Classic:** A classical circuit diagram showing a T gate and a CNOT gate.
- Application:**
  - Quantum:** SCFPM21<sup>[21]</sup>, Secure auctions, Secure voting.
  - Classic:** TSP23<sup>[23]</sup>, MAScot<sup>[19]</sup>, TSP23<sup>[23]</sup>.

A green arrow labeled SPM21 points from the Quantum phase to the Classic phase in the Primitive row.



# Quantum and classical OT



Comparable structure?

Corresponding phases with same technology?

Any practical insight?





The diagram illustrates the evolution of MPC protocols across three rows: Primitive, Circuit, and Application. The diagram is divided into Quantum and Classic phases.

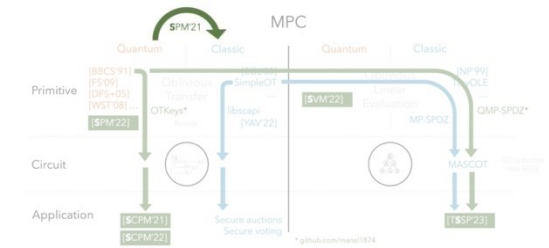
- Primitive:**
  - Quantum:** [BBC<sup>+</sup>91], [PSW99], [DPS+05], [MST08], [SPM22]
  - Classic:** [Oblivious Transfer], [OTkeys\*], [SimpleOT], [Ibscp], [WAV22], [SVM22], [Linear Evaluation], [MP-SPDZ], [N<sup>th</sup>99], [NIOLE], [OMP-SPDZ\*]
- Circuit:**
  - Quantum:** (Circuit diagram)
  - Classic:** [MASCOT]
- Application:**
  - Quantum:** [SCPM21]
  - Classic:** [Secure auctions], [Secure voting], [TSP23]

A green arrow labeled SPM21 points from the Quantum phase to the Classic phase in the Primitive row.

\* github.com/mayne1874



# Quantum and classical OT



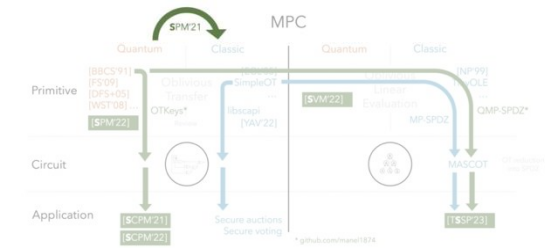
Classic

Base OT

OT Extension

Quantum  
[BBCS'91]

# Quantum and classical OT



## Classic

## Base OT

## OT Extension

Quantum  
[BBCS'91]

## Issue: PK operations

The diagram illustrates the evolution of MPC protocols across three rows: Primitive, Circuit, and Application. The diagram is divided into Quantum and Classic phases.

- Primitive:**
  - Quantum:** BB84<sup>[91]</sup>, PSW<sup>[9]</sup>, DPS<sup>[45]</sup>, NIST88<sup>[1]</sup>, SPM22<sup>[22]</sup>.
  - Classic:** Oblivious Transfer, SimpleOT<sup>[1]</sup>, Tlsapi<sup>[14]</sup>, Tlsapi<sup>[14]</sup>, Tlsapi<sup>[14]</sup>.
- Circuit:**
  - Quantum:** A circuit diagram showing a T gate and a T gate.
  - Classic:** A circuit diagram showing a T gate and a T gate.
- Application:**
  - Quantum:** SCFM21<sup>[21]</sup>, Secure auctions, Secure voting.
  - Classic:** TSP23<sup>[23]</sup>, MAScot<sup>[1]</sup>, MAScot<sup>[1]</sup>.

A green arrow labeled SPM21 points from the Quantum phase to the Classic phase in the Primitive row.

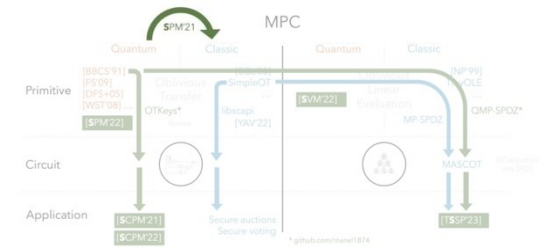
## OT Extension

Quantum  
[BBCS'91]

Diagram illustrating a transformation:

- Input: 128 Base OT (represented by a dashed box)
- Operation: Sym (indicated by a blue arrow)
- Output: ~10M OT (represented by a dashed box)

# Quantum and classical OT



Quantum  
[BBCS'91]

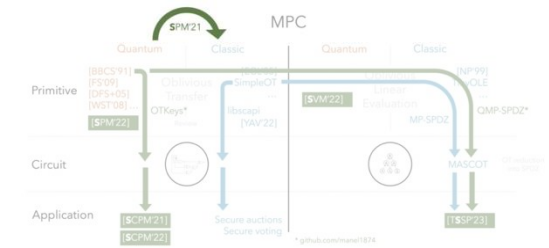
## Classic

## Base OT

## OT Extension

	OT/s			10M OT
[NP'01]	56		[ALSZ'13]	2.68 s
SimpleOT	1 375	<	[KOS'15]	3.35 s
NTRU-OT	728			
Kyber-OT	41			

# Quantum and classical OT



Classic

Base OT

OT Extension

Quantum  
[BBCS'91]

Base OT		OT Extension	
	OT/s		10M OT
[NP'01]	56	[ALSZ'13]	2.68 s
SimpleOT	1 375	[KOS'15]	3.35 s
NTRU-OT	728		
Kyber-OT	41		

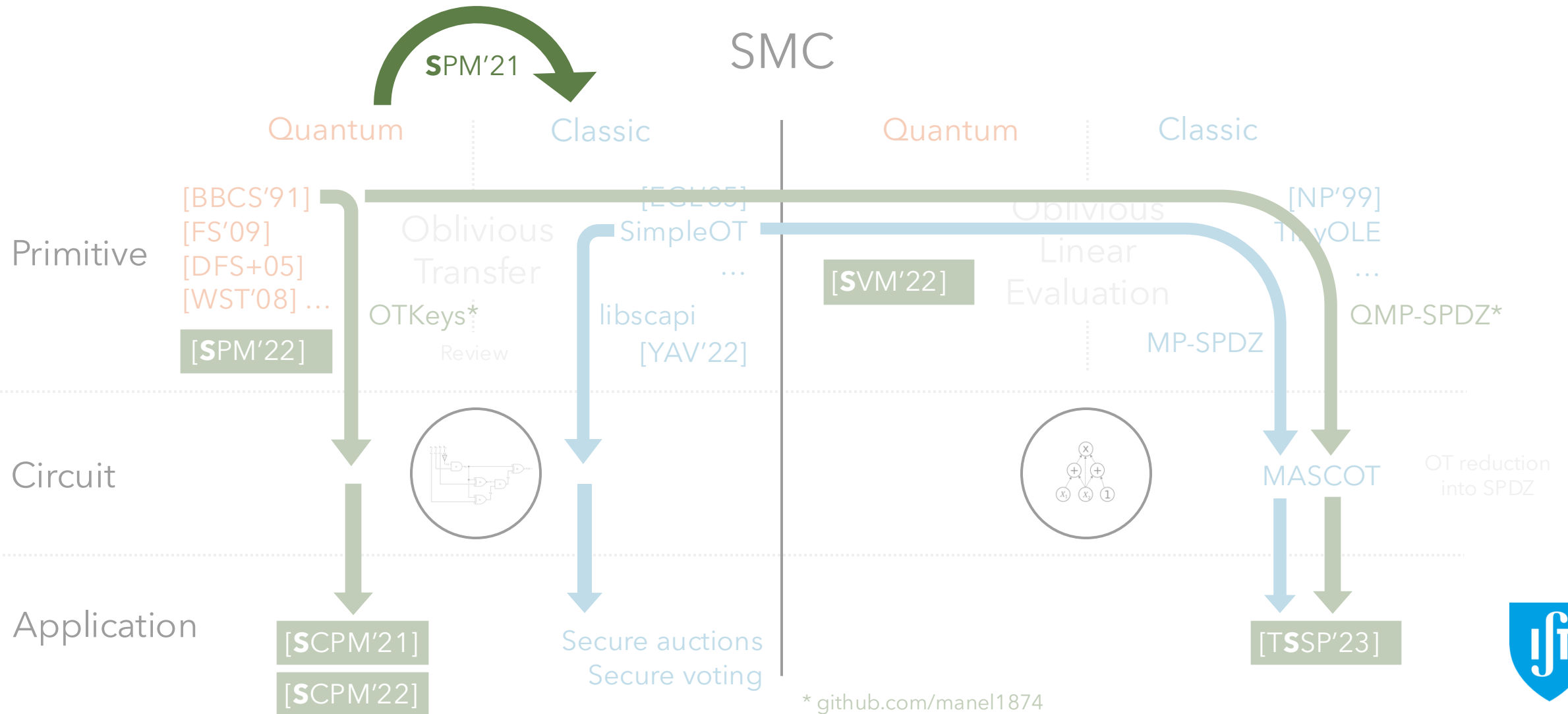
Online phase for  $m$  OTs

	Computation	Communication
[ALSZ'13]	$\mathcal{O}^{\text{ALSZ}} - \mathcal{O}^{\text{BBCS}} > m \log m$	$\mathcal{C}^{\text{ALSZ}} - \mathcal{C}^{\text{BBCS}} = 0$
[KOS'15]	$\mathcal{O}^{\text{KOS}} - \mathcal{O}^{\text{BBCS}} > m \log m + 5ml$	$\mathcal{C}^{\text{KOS}} - \mathcal{C}^{\text{BBCS}} \gtrsim 0$

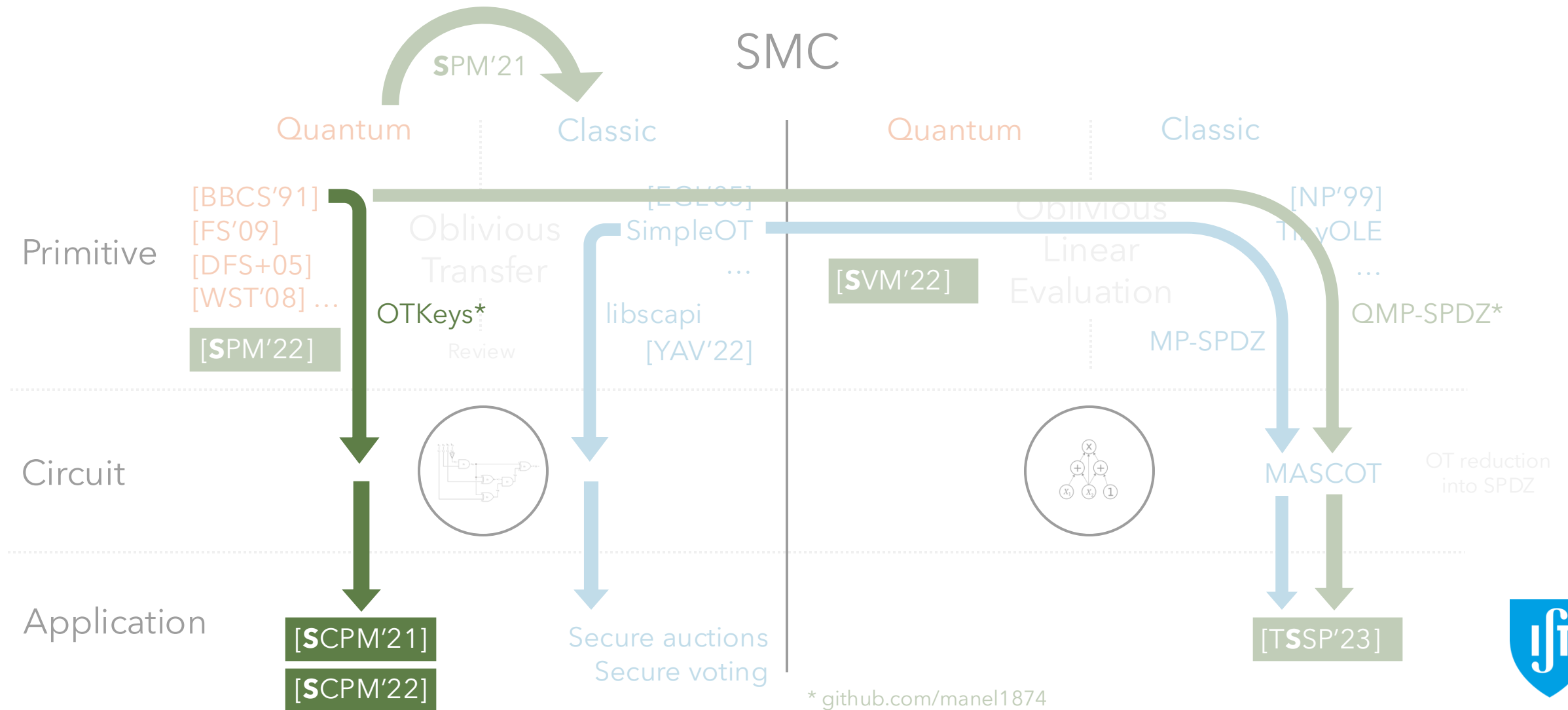
BBCS



# Quantum and classical OT

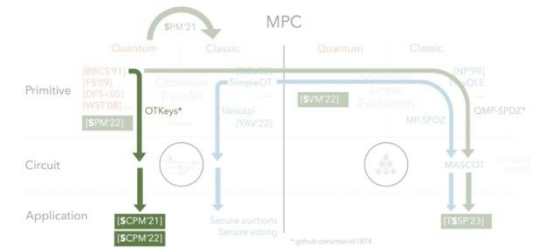


# Private phylogenetic trees

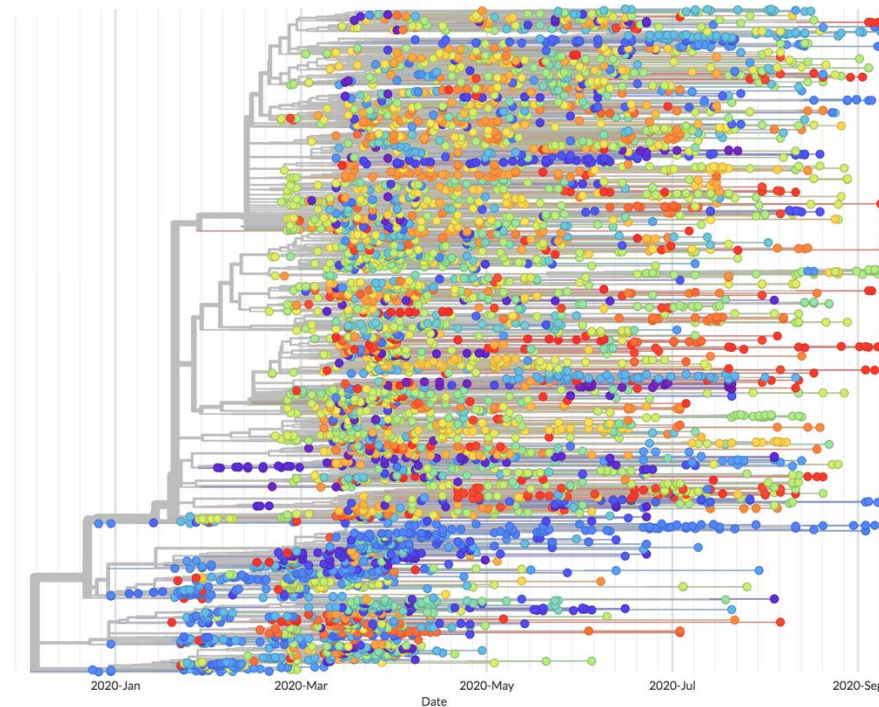




# Private phylogenetic trees



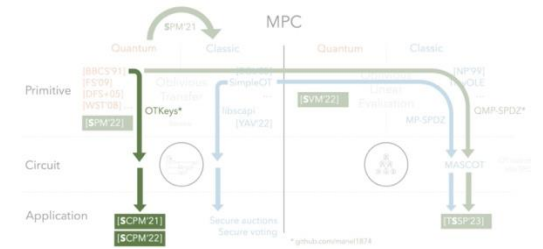
Shows the **evolutionary relationship** between **DNA** sequences in a **tree**.



# Private phylogenetic trees

## Results summary

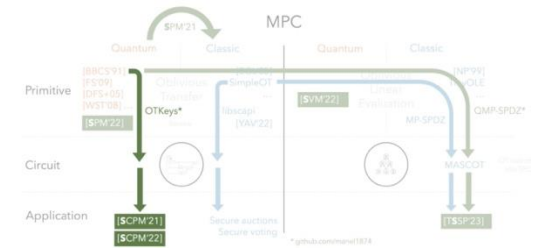
- Tailored SMC protocol for phylogenetic trees algorithms



# Private phylogenetic trees

## Results summary

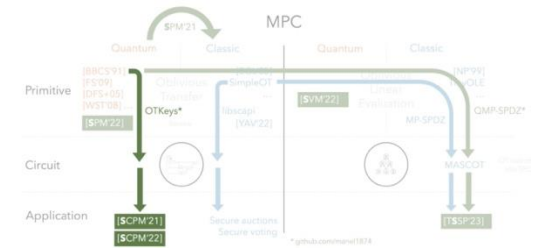
- Tailored SMC protocol for phylogenetic trees algorithms
- Classical implementation
  - CBMC-GC: circuit generation
  - MPC-Benchmark: yao protocol based on Libscapi
  - PHYLIP: phylogeny analysis



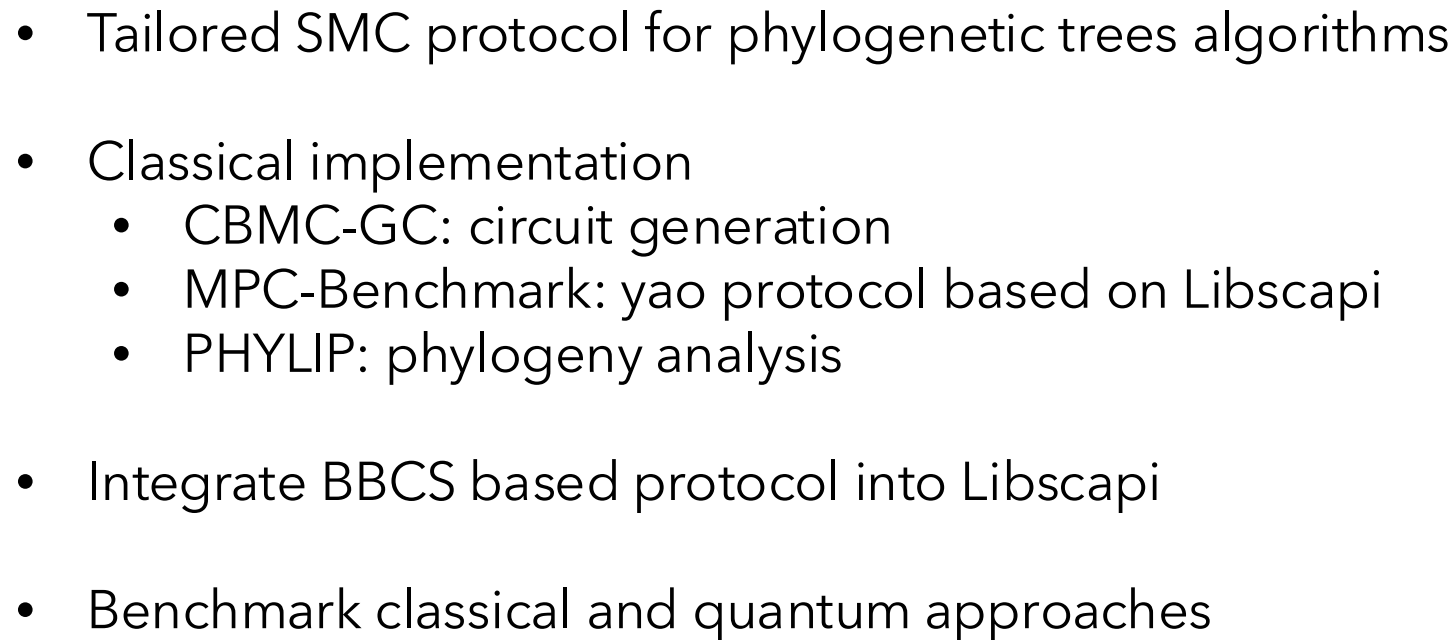
# Private phylogenetic trees

## Results summary

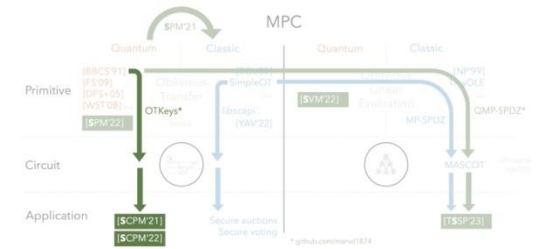
- Tailored SMC protocol for phylogenetic trees algorithms
- Classical implementation
  - CBMC-GC: circuit generation
  - MPC-Benchmark: yao protocol based on Libscapi
  - PHYLIP: phylogeny analysis
- Integrate BBCS based protocol into Libscapi



## Results summary



# Performance evaluation



Setup:

- **3 parties:** VMs running Ubuntu 16.04.3
- **30** SARS-CoV-2 genome **sequences\*** with **32 000 length**

Boolean circuit:

- ~3 minutes (CBMC-GC)
- ~2.2 million gates
- 128 000 input wires

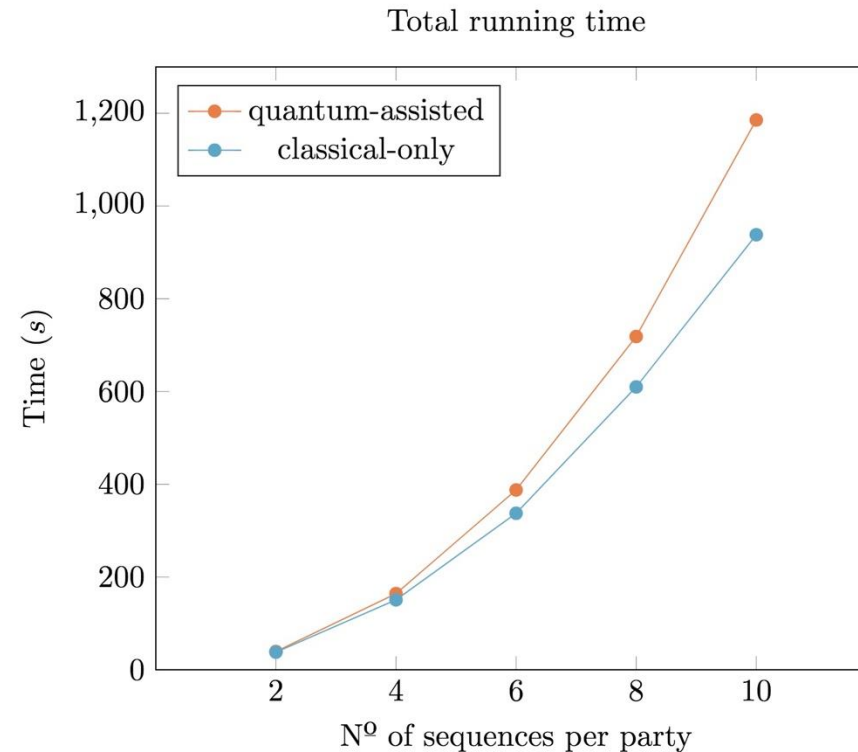
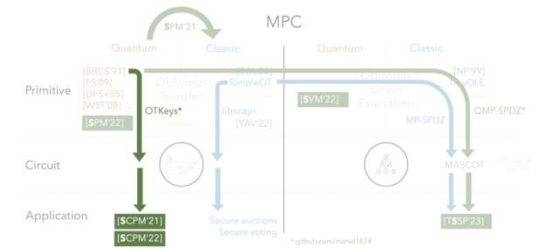
\*GISAID database



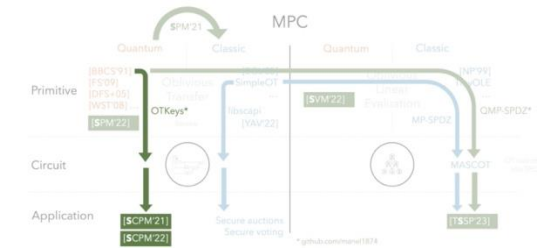
# Performance evaluation

Setup:

- **3 parties:** VMs running Ubuntu 16.04.3
- **30** SARS-CoV-2 genome **sequences\*** with **32 000 length**

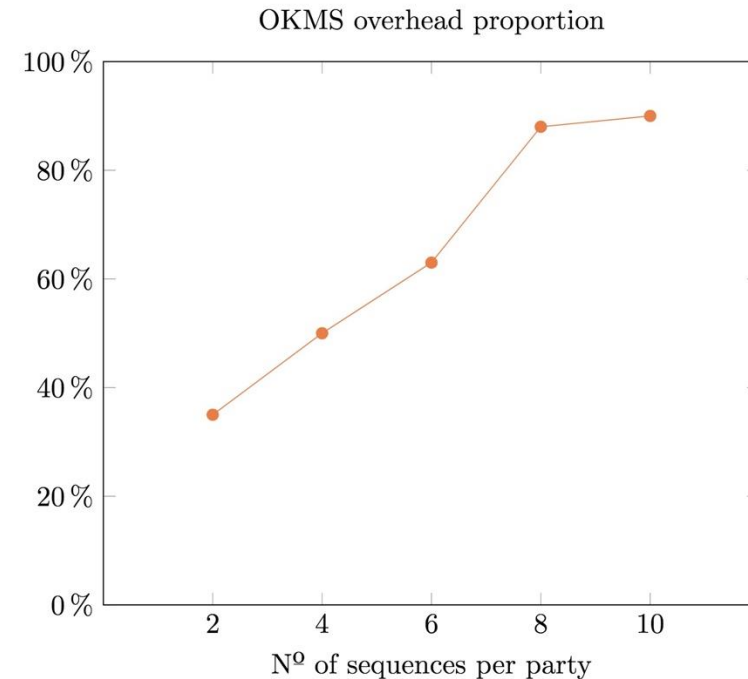
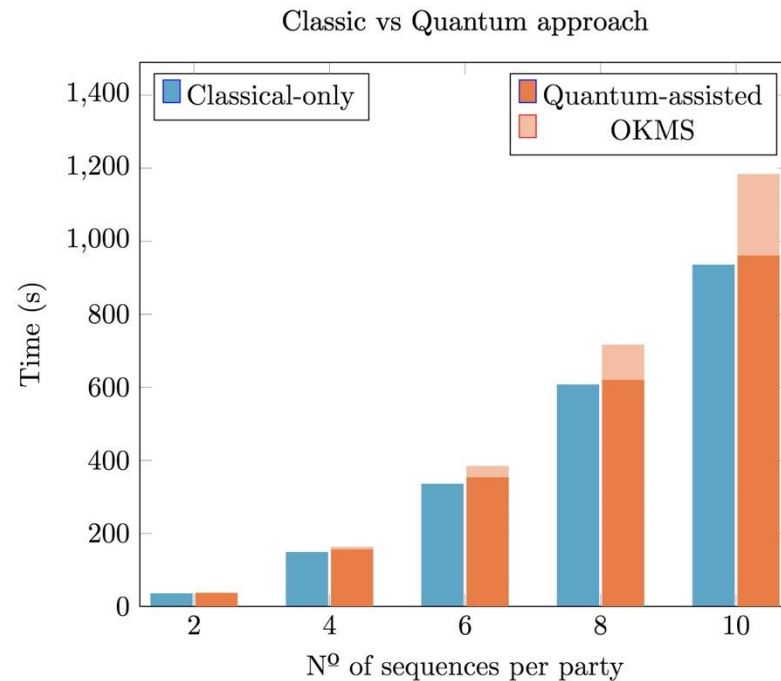


# Performance evaluation



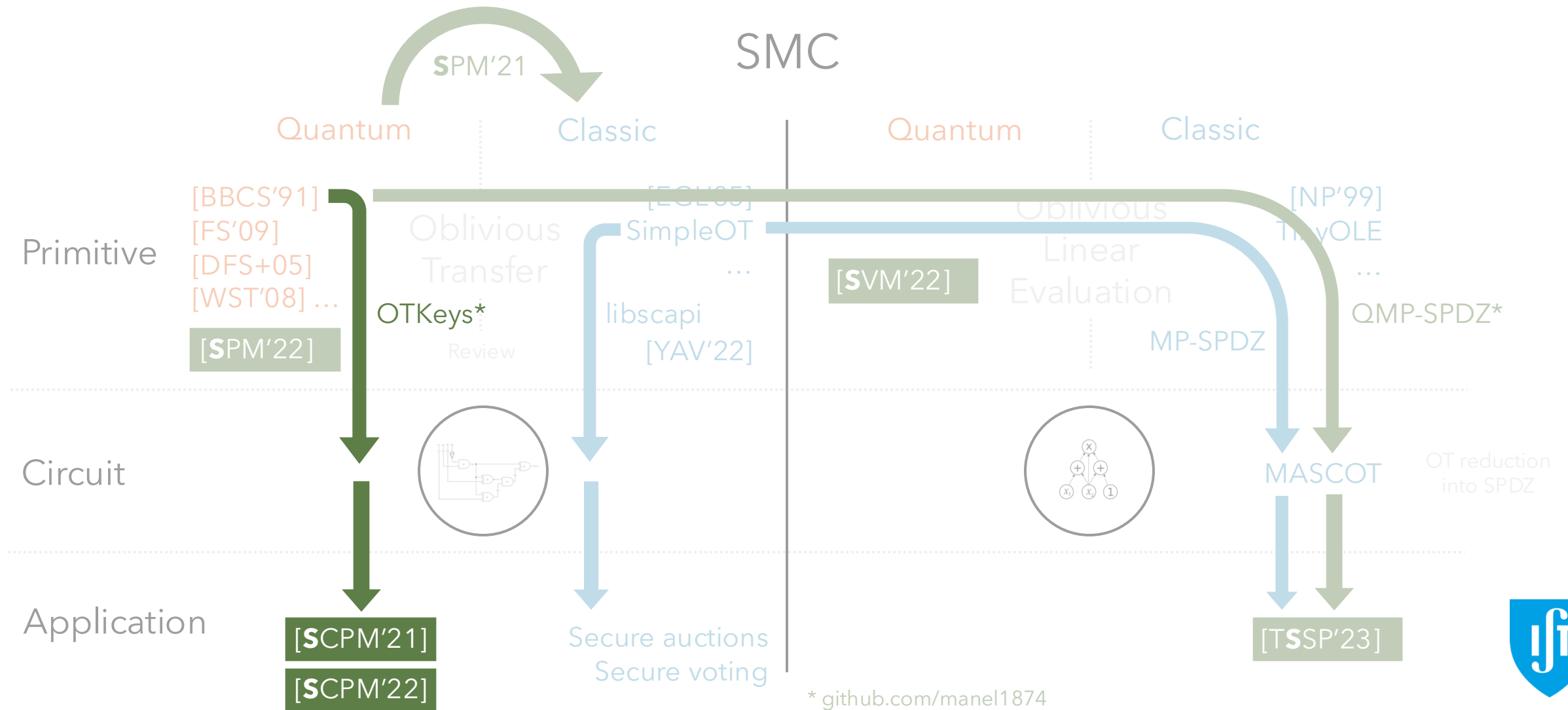
Setup:

- **3 parties:** VMs running Ubuntu 16.04.3
- **30** SARS-CoV-2 genome **sequences\*** with **32 000 length**

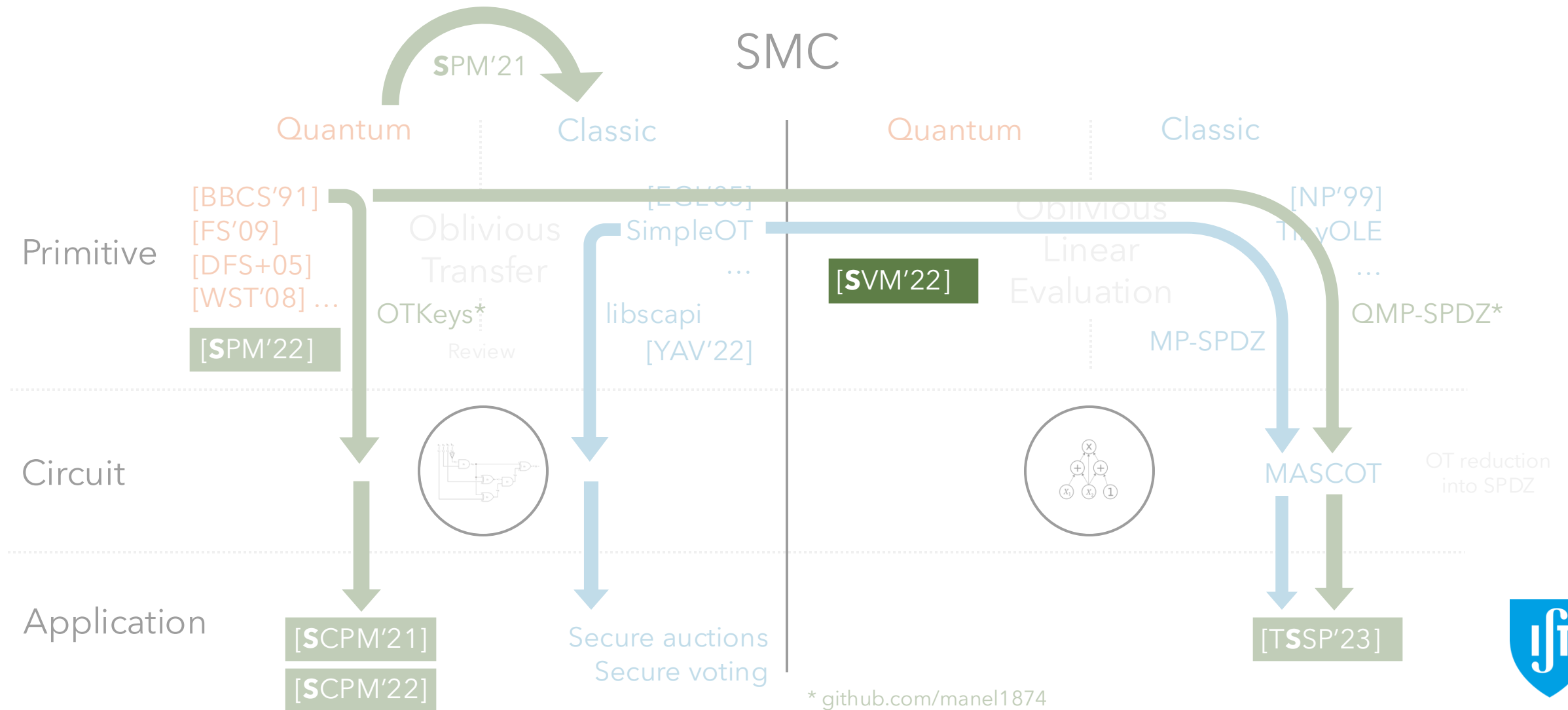




# Private phylogenetic trees



# Quantum OLE



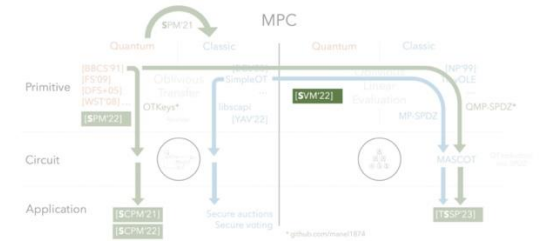
## Results summary

- 
- The diagram illustrates the mapping of MPC protocols to Quantum and Classical layers across three levels: Primitive, Circuit, and Application.
- Quantum Layer:**
- Primitive:** Includes protocols like [BBC91], [PS99], [SPZ08], [WST08], and [SPZ21].
  - Circuit:** Includes protocols like [SPZ21] and [SPZ22].
  - Application:** Includes protocols like [SPZ21] and [SPZ22].
- Classical Layer:**
- Primitive:** Includes protocols like [NP99], [NOLE], and [GMP-SPZ\*].
  - Circuit:** Includes protocols like [NP99], [NOLE], and [GMP-SPZ\*].
  - Application:** Includes protocols like [NP99], [NOLE], and [GMP-SPZ\*].
- Mapping and Transitions:**
- Quantum to Classical:** Indicated by a green arrow labeled "SPM21" at the top.
  - Classical to Quantum:** Indicated by a green arrow labeled "SPM21" at the top.
  - Primitive to Circuit:** Indicated by a green arrow labeled "OTkeys" and "Secure".
  - Circuit to Application:** Indicated by a green arrow labeled "Secure auctions" and "Secure voting".
  - Classical to Circuit:** Indicated by a green arrow labeled "SimpleOT" and "Recomp [WAV22]".
  - Circuit to Application:** Indicated by a green arrow labeled "Secure auctions" and "Secure voting".
  - Quantum to Application:** Indicated by a green arrow labeled "SimpleOT" and "Recomp [WAV22]".
  - Classical to Application:** Indicated by a green arrow labeled "SimpleOT" and "Recomp [WAV22]".
- Legend:**
- Quantum:** Represented by a blue circle with a quantum symbol.
  - Classical:** Represented by a blue circle with a classical symbol.
- Footnote:**
- \* ggithub.com/marcel1874

# Quantum OLE

## Results summary

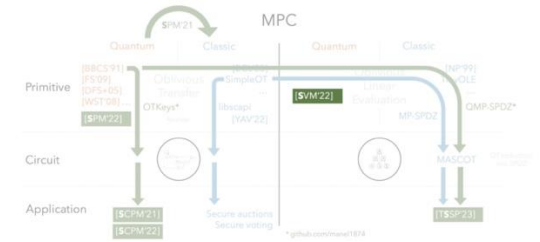
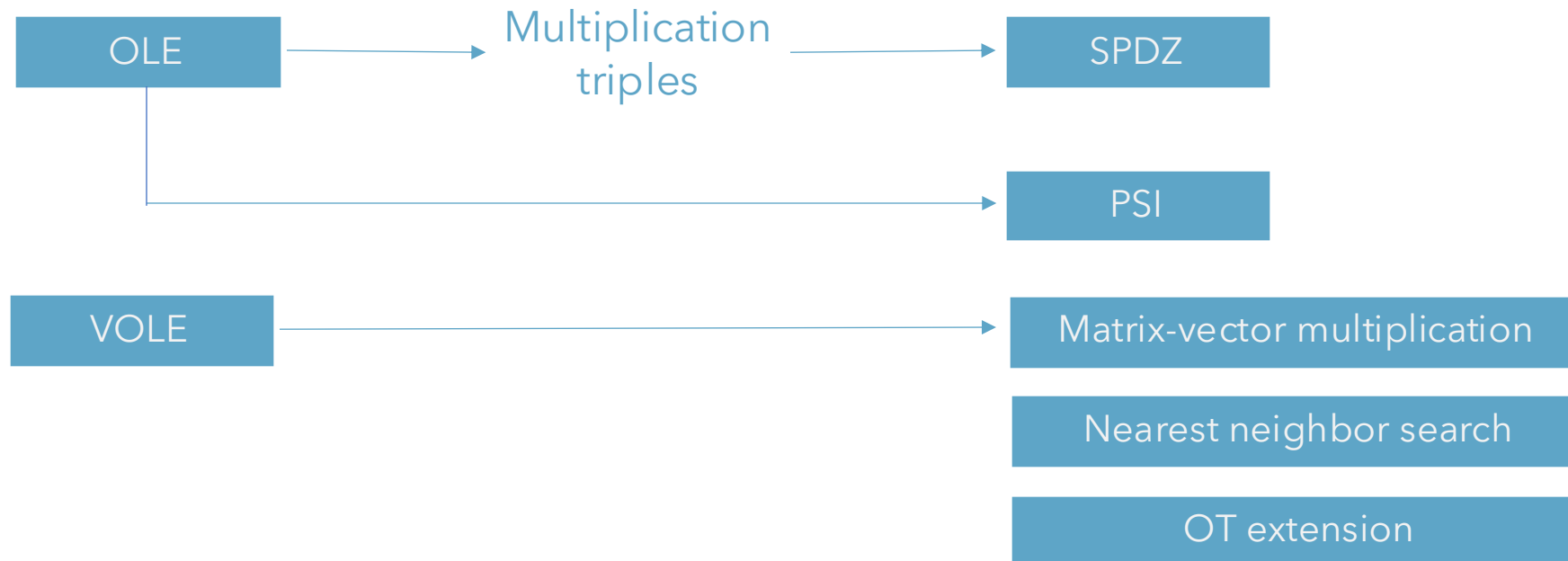
- Oblivious Linear Evaluation (OLE)
- Vector OLE



# Quantum OLE

## Results summary

- Oblivious Linear Evaluation (OLE)
- Vector OLE

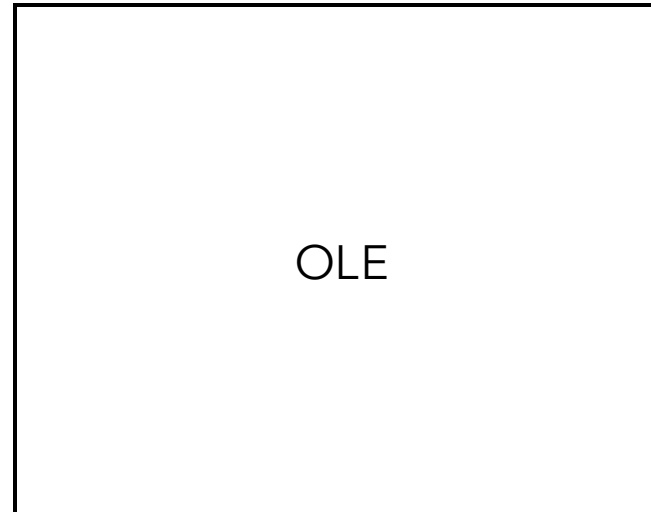
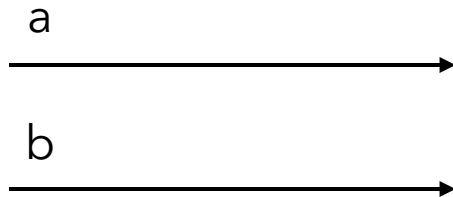


# Quantum OLE

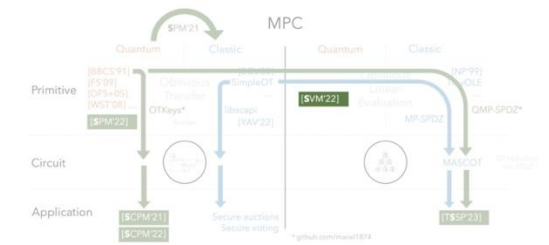
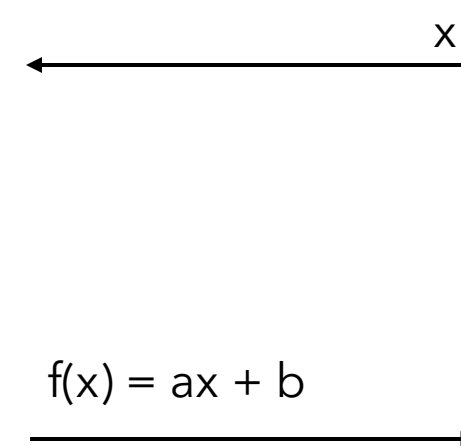
## Results summary

- Oblivious Linear Evaluation (OLE)
- Vector OLE

Alice



Bob

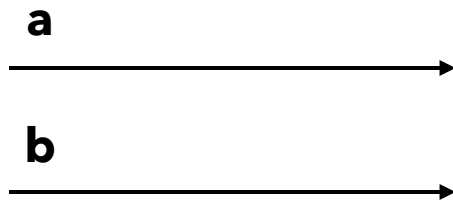


# Quantum OLE

## Results summary

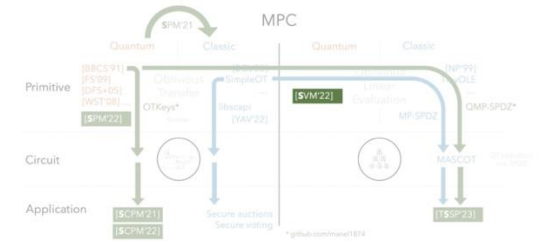
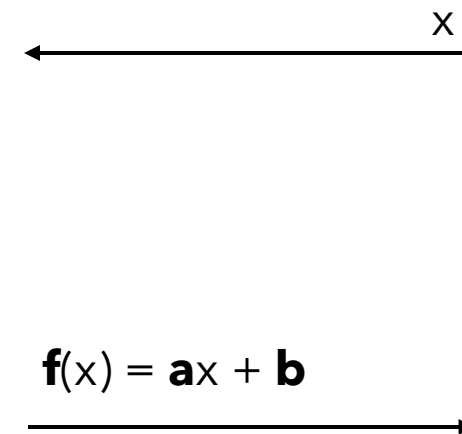
- Oblivious Linear Evaluation (OLE)
- Vector OLE

Alice

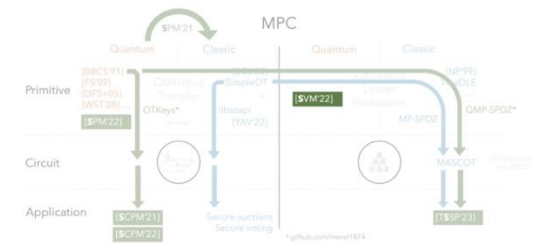


VOLE

Bob



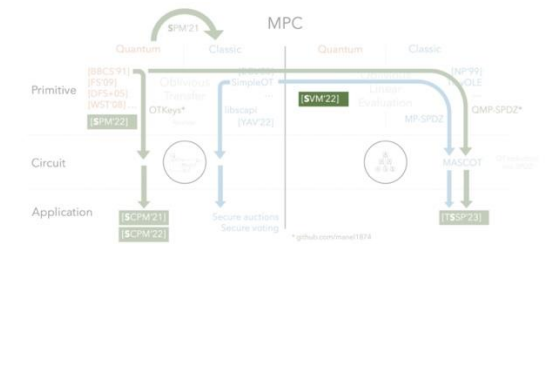
# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$



# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

The diagram illustrates the workflow of MPC (Multi-Party Computation) across four layers: Primitive, Circuit, Application, and a top layer. The workflow is divided into Quantum and Classic phases.

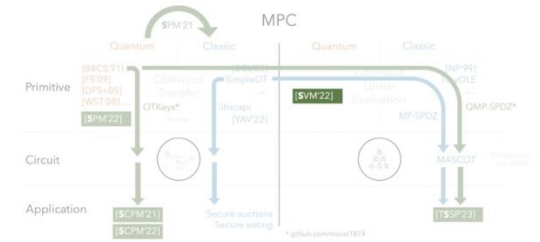
- Primitive Layer:**
  - Quantum:** BRCS91, PS91, SPFA05, WST08, SPW22.
  - Classic:** Garbled Circuit Generator, OTkeys\*.
- Circuit Layer:**
  - Quantum:** SPW22, Garbled Circuit (G).
  - Classic:** Secure Evaluation, Garbled Circuit (G).
- Application Layer:**
  - Quantum:** SPW22, SPW22.
  - Classic:** SPW22, SPW22.
- Top Layer:**
  - Quantum:** SPW21.
  - Classic:** MPC.

The diagram also includes a legend for Quantum (orange) and Classic (blue) phases.

$$\{|e_r^x\rangle\}_{r\in\mathbb{Z}_d}$$
$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r\in\mathbb{Z}_d}$$

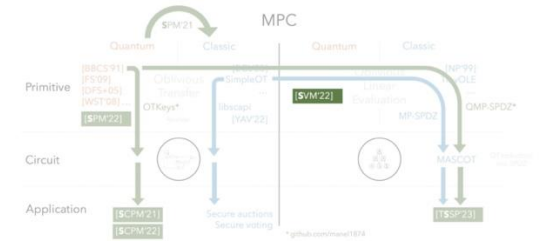
## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

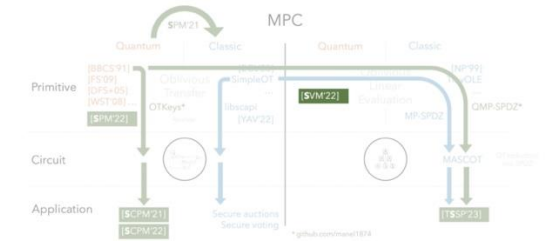
## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

## Definition:

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

The diagram shows the evolution of MPC across four levels: Primitive, Circuit, Application, and a final Application level. It is divided into Quantum and Classic domains.

- Primitive Level:**
  - Quantum:** [BRCS'91], [PS99], [SP94-00], [WOT98], [SPM22]
  - Classic:** [SimpleOT], [OTKeys\*], [Libspc], [YAW22]
- Circuit Level:**
  - Quantum:** [SPM22]
  - Classic:** [SimpleOT], [Libspc], [YAW22]
- Application Level (First):**
  - Quantum:** [SCPM21], [SCPM22]
  - Classic:** [Secure auctions], [Secure voting]
- Application Level (Second):**
  - Quantum:** [SPM22]
  - Classic:** [SimpleOT], [Libspc], [YAW22]
- Application Level (Third):**
  - Quantum:** [SPM22]
  - Classic:** [SimpleOT], [Libspc], [YAW22]
- Application Level (Fourth):**
  - Quantum:** [SPM22]
  - Classic:** [SimpleOT], [Libspc], [YAW22]

Arrows indicate the flow of information and dependencies between these components across the different levels.

## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

The diagram shows the evolution of MPC across four levels: Primitive, Circuit, Application, and a final Application level. It is divided into Quantum and Classic domains.

- Primitive Level:**
  - Quantum:** [BRCS'91], [FS99], [SPS+00], [WOT08], [SPM22]
  - Classic:** [SimpleOT], [OTKeys\*], [Libspc], [NAV22]
- Circuit Level:**
  - Quantum:** [SPM22]
  - Classic:** [SimpleOT], [Libspc], [NAV22]
- Application Level (Top):**
  - Quantum:** [SPM21]
  - Classic:** [SimpleOT], [Libspc], [NAV22]
- Application Level (Bottom):**
  - Quantum:** [SPM21], [SPM22]
  - Classic:** [SimpleOT], [Libspc], [NAV22]

Arrows indicate the flow of information and dependencies between these components across the different levels.

$$\{|e_r^x\rangle\}_{r\in\mathbb{Z}_d}$$
$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

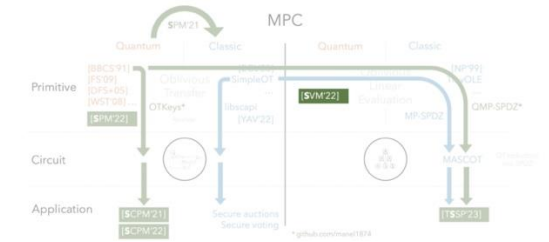
Bob,  $x$

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

Alice,  $(a,b)$

Bob,  $x$

$$|e_r^x\rangle$$

## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

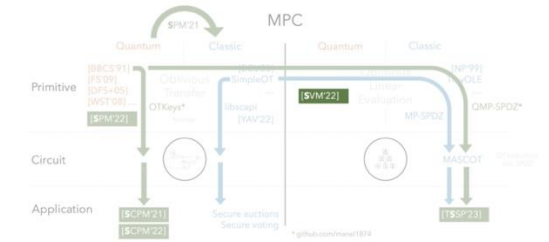
$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

## Definition:

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$



# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

Alice,  $(a,b)$

Bob,  $x$

$$|e_r^x\rangle \longleftarrow |e_r^x\rangle$$

**Definition:**

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

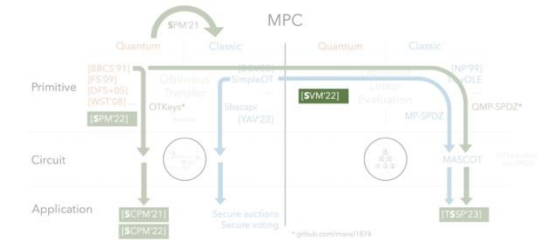
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

**Definition:**

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle\psi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}$$

## Definition:

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

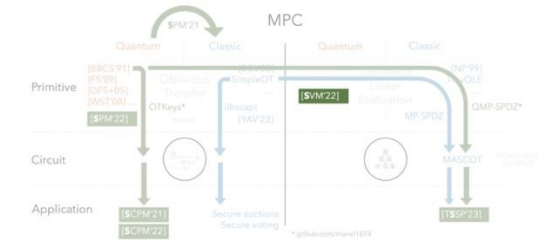
Alice,  $(a,b)$

Bob,  $x$

$$|e_r^x\rangle \longleftarrow |e_r^x\rangle$$

$$V_a^b |e_r^x\rangle$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

Alice,  $(a,b)$

Bob,  $x$

$$|e_r^x\rangle \longleftarrow |e_r^x\rangle$$

$$|e_{ax-b+r}^x\rangle$$

**Definition:**

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

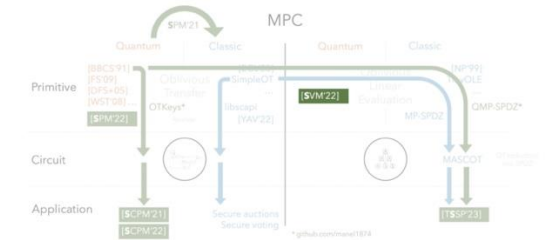
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

**Definition:**

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

## Definition:

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle \langle l|$$

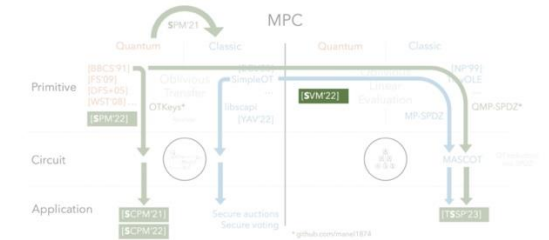
Alice,  $(a,b)$

Bob,  $x$

$$|e_r^x\rangle \longleftarrow |e_r^x\rangle$$

$$|e_{ax-b+r}^x\rangle \longrightarrow |e_{ax-b+r}^x\rangle$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

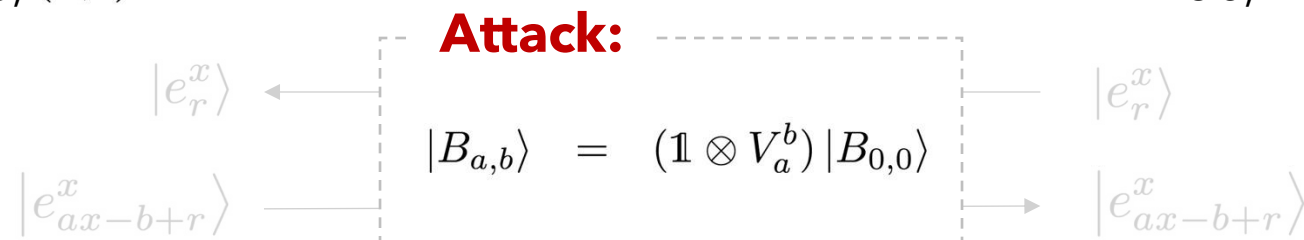
$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

Alice,  $(a,b)$

Bob,  $x$



**Definition:**

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

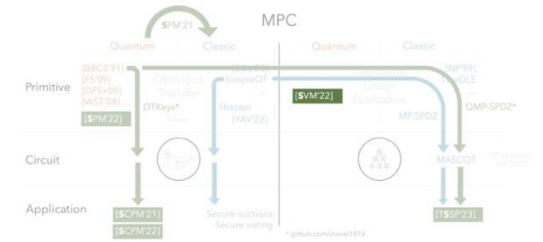
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

**Definition:**

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle \langle l|$$

# Quantum OLE | Main tool



In an Hilbert space of dimension  $d$ , there exists a set of MUBs

$$\{|e_r^x\rangle\}_{r \in \mathbb{Z}_d}$$

which, upon the action of the Heisenberg-Weyl operators,  $V_a^b$

$$V_a^b |e_r^x\rangle = c_{a,b,x,r} |e_{ax-b+r}^x\rangle$$

## Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \dots, |\phi_d\rangle\}$$

$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

$$|\langle \psi_i | \phi_j \rangle| = \frac{1}{\sqrt{d}}$$

## Definition:

$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b} |l+a\rangle\langle l|$$

Alice,  $(a,b)$

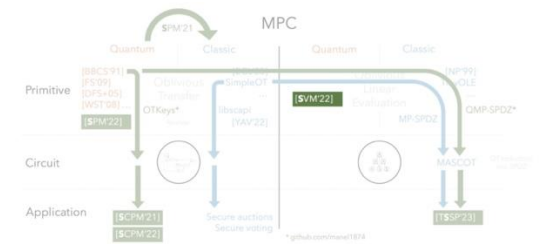
Bob,  $x$



# Quantum OLE | Protocol

Alice,  $(a, b)$

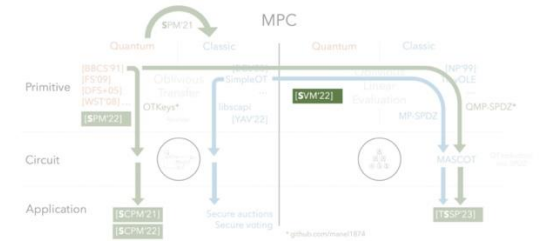
Bob,  $x$



Quantum phase

Classical phase

# Quantum OLE | Protocol



Alice,  $(a,b)$

$i \in [m]$

Bob,  $x$

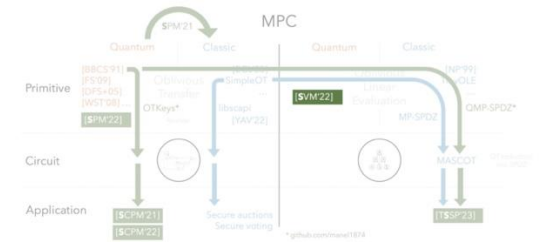
$$\left| e_{r_i}^{x_i^0} \right\rangle$$

Quantum phase

Classical phase



# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^0\rangle$$

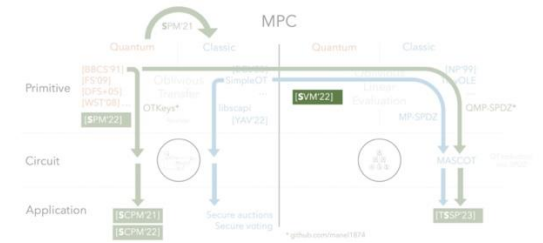
$$V_{a_i^0}^{b_i^0} |e_{r_i}^0\rangle$$

$$|e_{r_i}^0\rangle$$

Quantum phase

Classical phase

# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^0\rangle$$

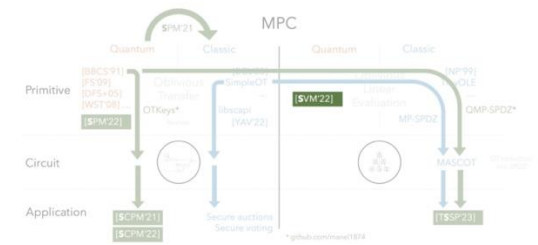
$$V_{a_i^0}^{b_i^0} |e_{r_i}^0\rangle$$

$$|e_{r_i}^0\rangle$$

Quantum phase

Classical phase

# Quantum OLE | Protocol



Alice,  $(a,b)$

Bob,  $x$

$$i \in [m]$$

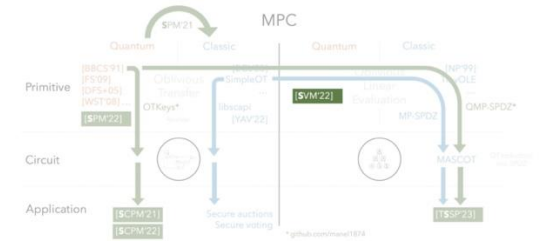
$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

$$\left| e^{x_i^0} a_i^0 x_i^0 - b_i^0 + r_i \right\rangle$$

# Quantum phase

# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

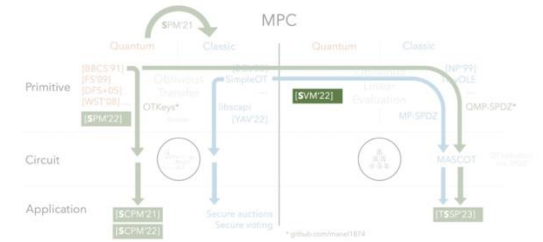
$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

**Commit-and-open phase**

Quantum phase

Classical phase

# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$



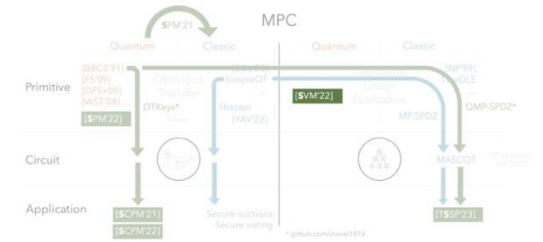
**Commit-and-open phase**

$\text{commit}(i, x_i^0, r_i)_{i \in [m]}$

Quantum phase

Classical phase

# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

$$T \subset [m]$$

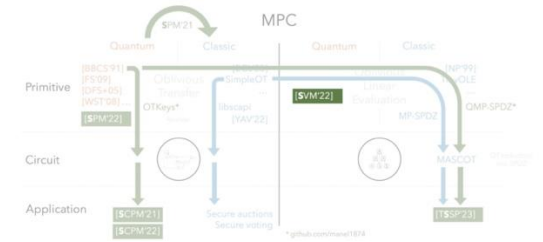
**Commit-and-open phase**

$$\text{commit}(i, x_i^0, r_i)_{i \in [m]}$$

Quantum phase

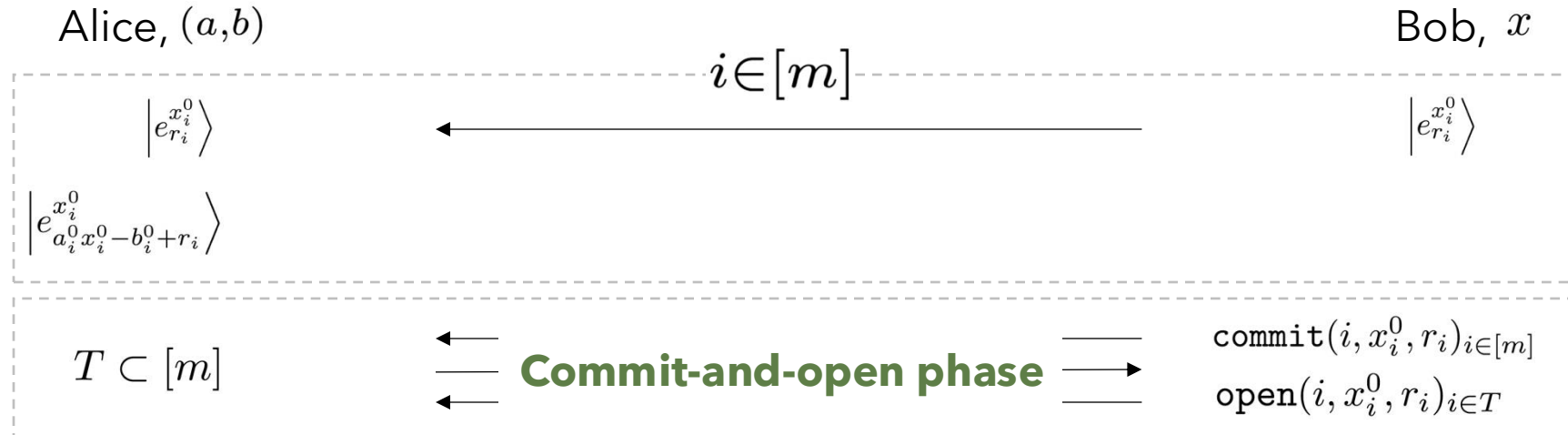
Classical phase

# Quantum OLE | Protocol

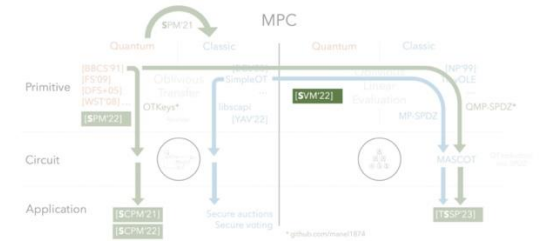


Quantum phase

Classical phase



# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

$$T \subset [m]$$

**Commit-and-open phase**

$\text{commit}(i, x_i^0, r_i)_{i \in [m]}$   
 $\text{open}(i, x_i^0, r_i)_{i \in T}$

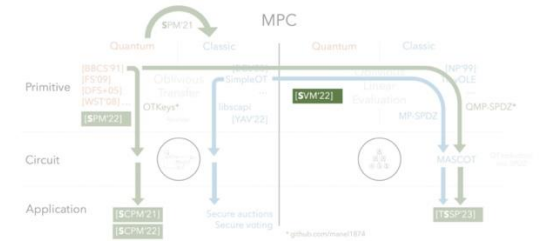
$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

Quantum phase

Classical phase



# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

$$T \subset [m]$$

**Commit-and-open phase**

$\text{commit}(i, x_i^0, r_i)_{i \in [m]}$   
 $\text{open}(i, x_i^0, r_i)_{i \in T}$

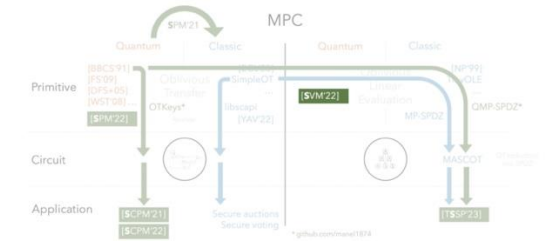
$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

Quantum phase

Classical phase

# Quantum OLE | Protocol



Alice,  $(a, b)$

Bob,  $x$

$i \in [m]$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

$$T \subset [m]$$

**Commit-and-open phase**

$\text{commit}(i, x_i^0, r_i)_{i \in [m]}$   
 $\text{open}(i, x_i^0, r_i)_{i \in T}$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

$$|e_{a_i^0 x_i^0 - b_i^0 + r_i}^{x_i^0}\rangle$$

**Derandomization:**

$n$  ROLE

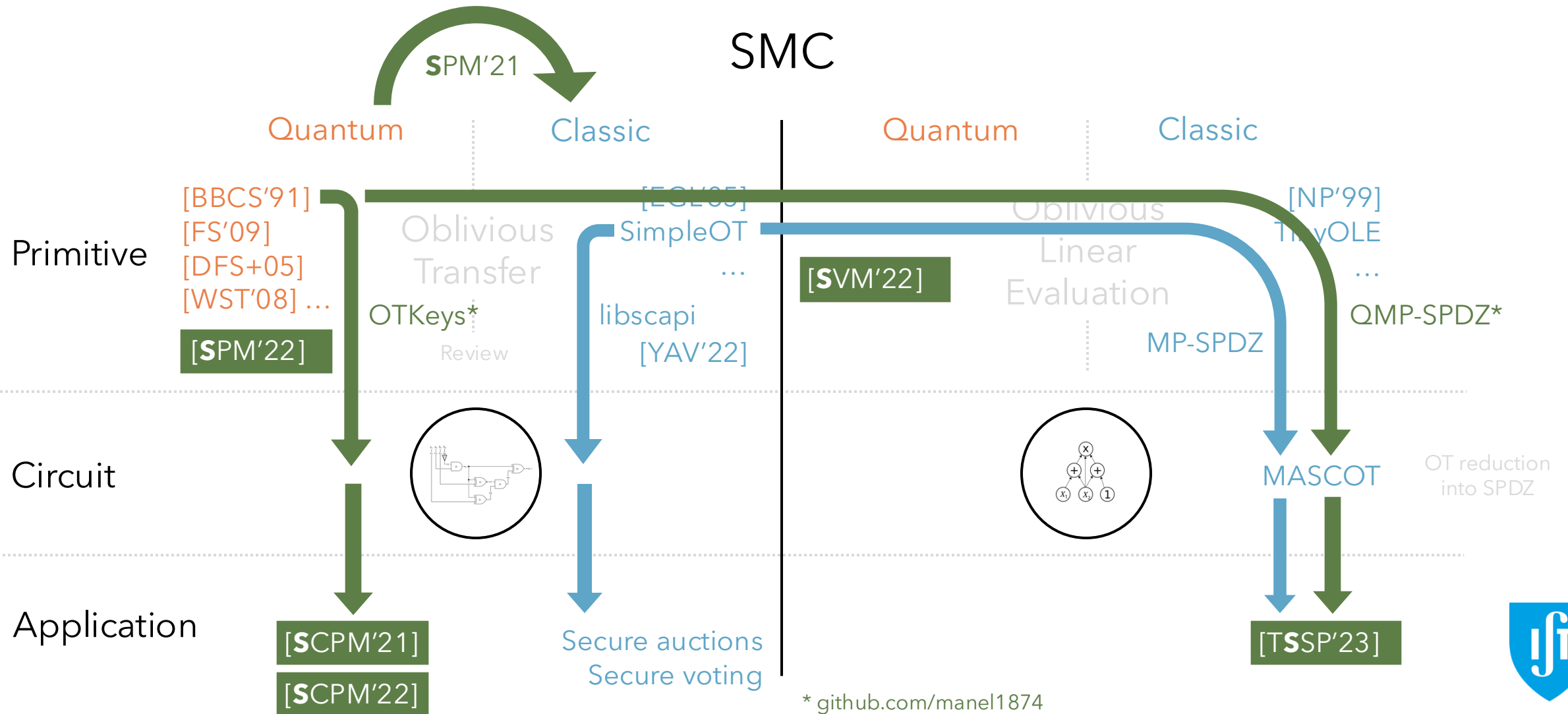
$n$  OLE

Quantum phase

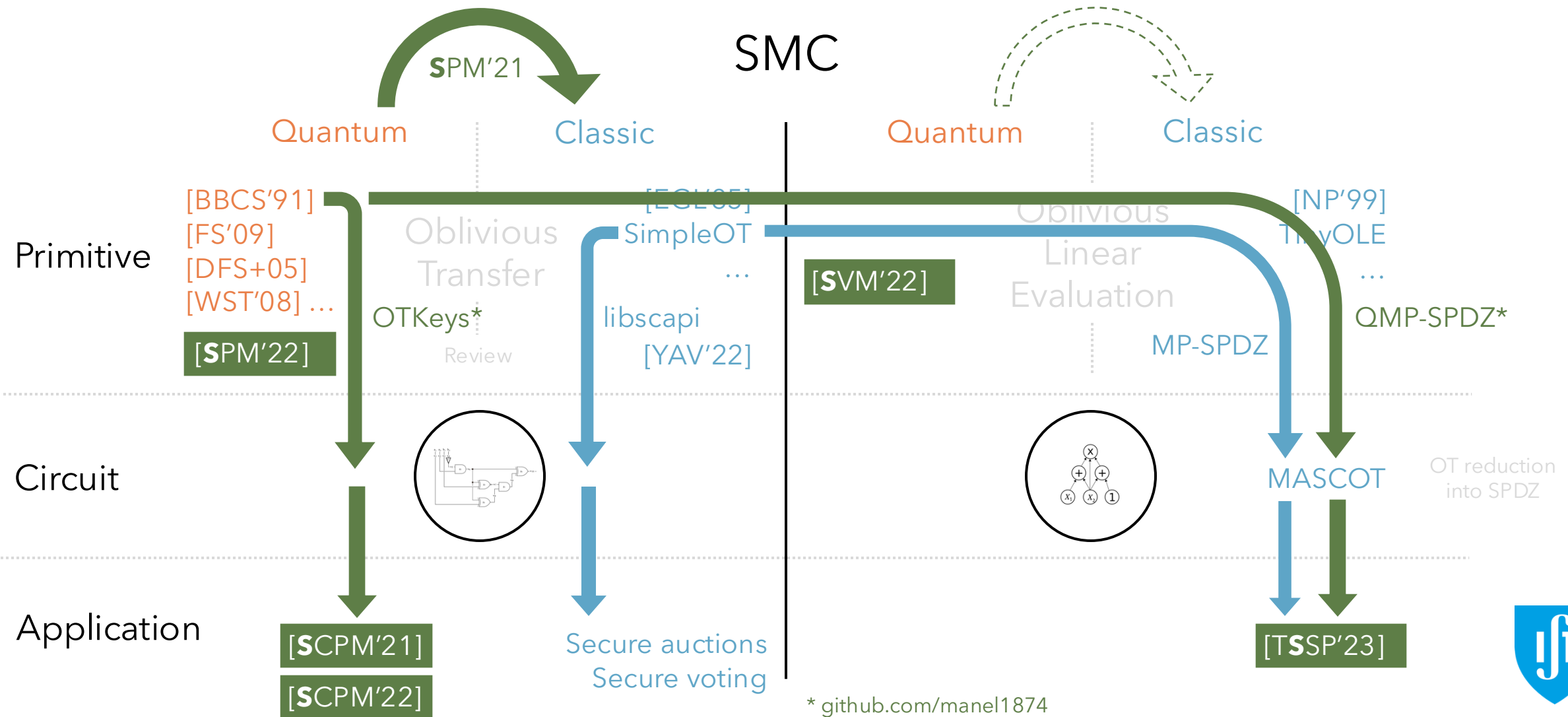
Classical phase



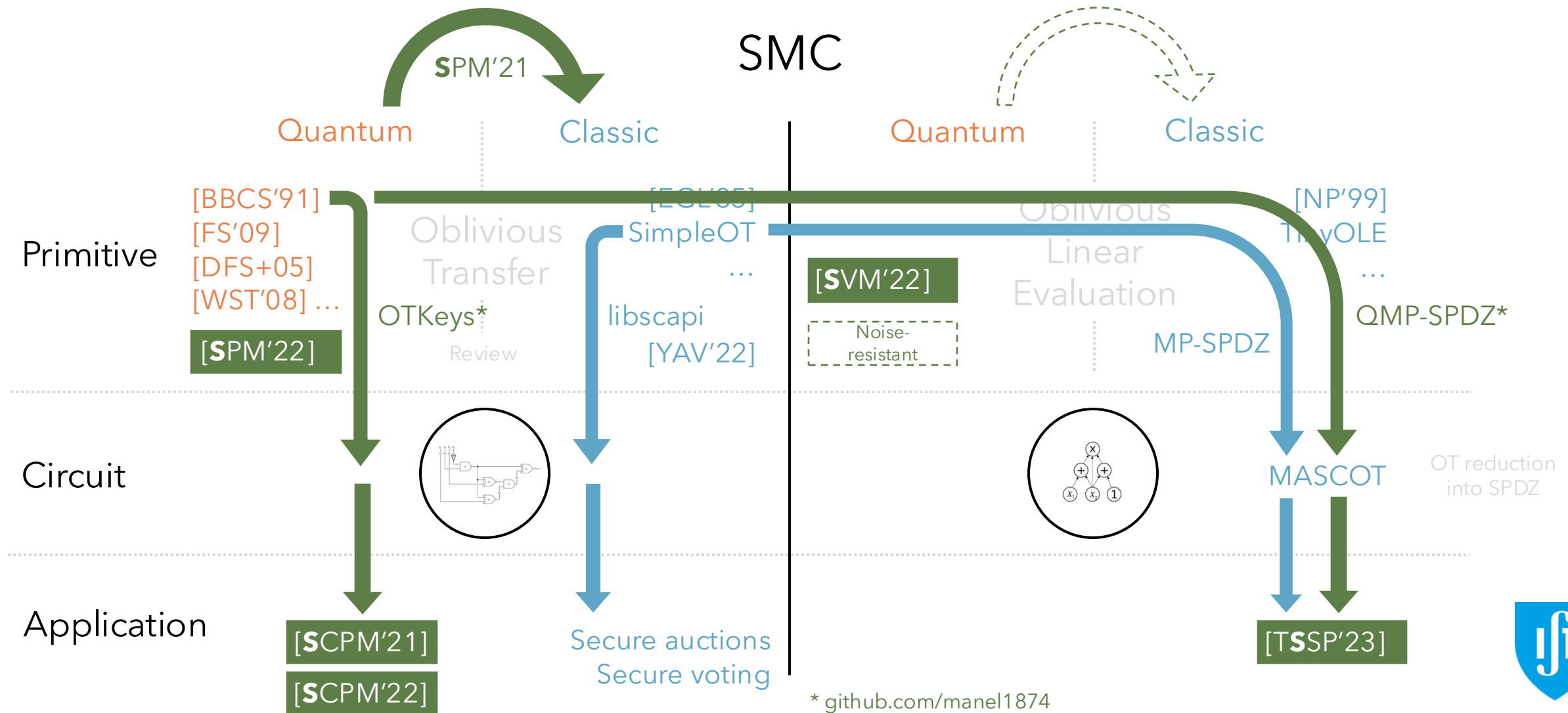
# Future work



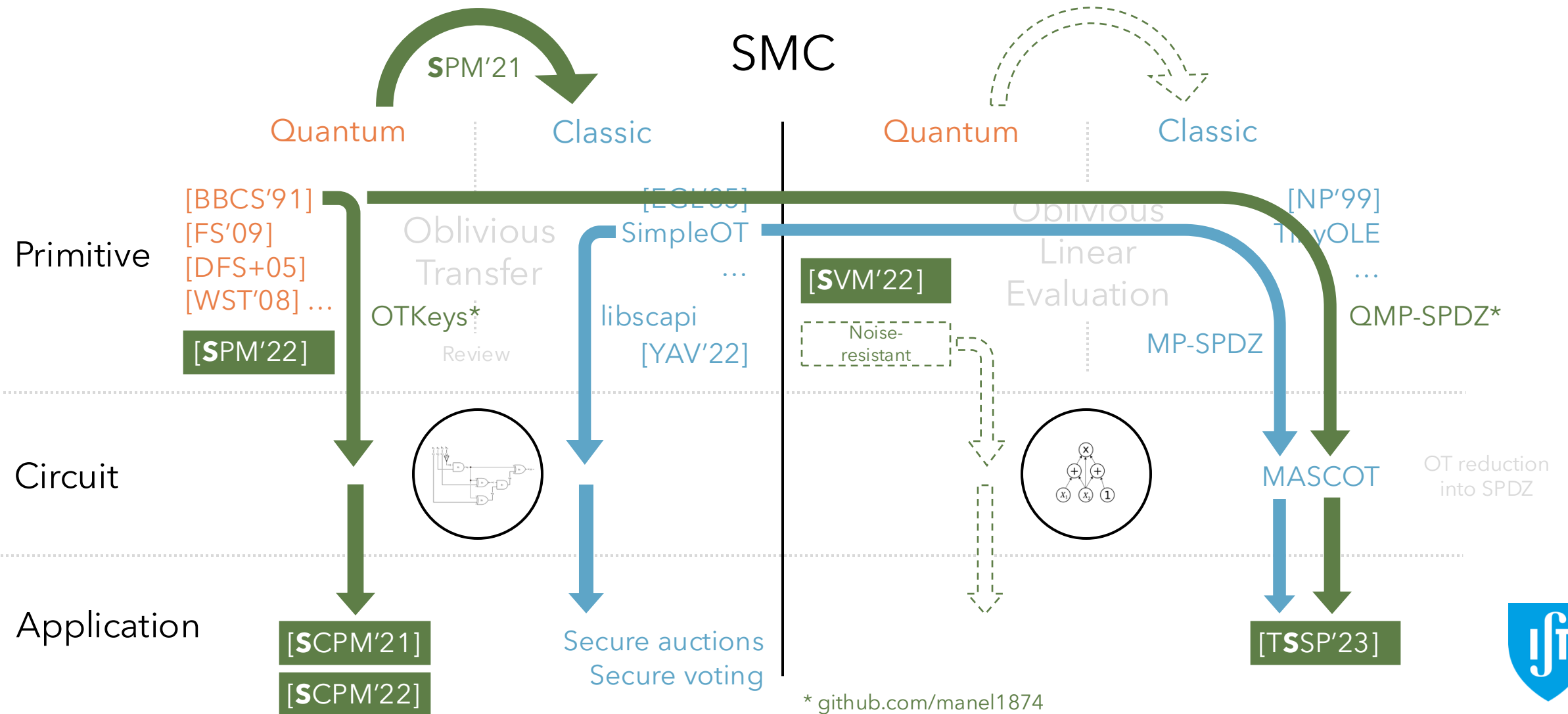
# Future work



# Future work



# Future work



# Thank you

I acknowledge Fundação para a Ciência e a Tecnologia (FCT, Portugal) for its support through the PhD grant SFRH/BD/ 144806/2019 in the context of the Doctoral Program in the Information Security (IS).



# Quantum Assisted Secure Multiparty Computation

Manuel Batalha dos Santos

Thesis defense  
16 January 2025

