Quantum Assisted Secure Multiparty Computation

Manuel Batalha dos Santos

Thesis defence
16 January 2025

TÉCNICO LISBOA

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

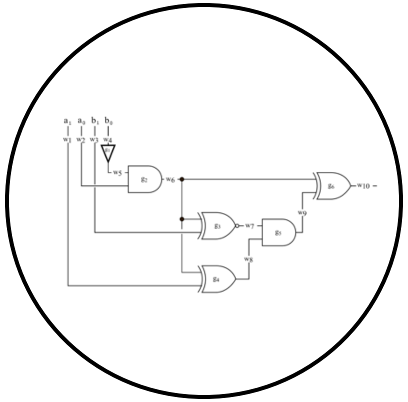
Motivation

SMC

Motivation

SMC

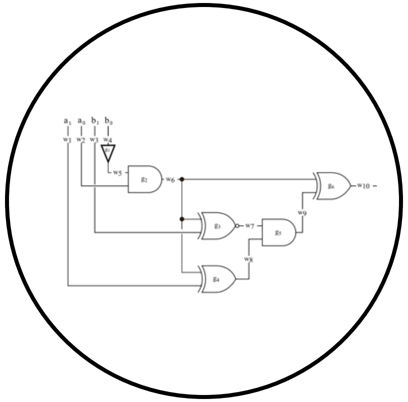
Boolean



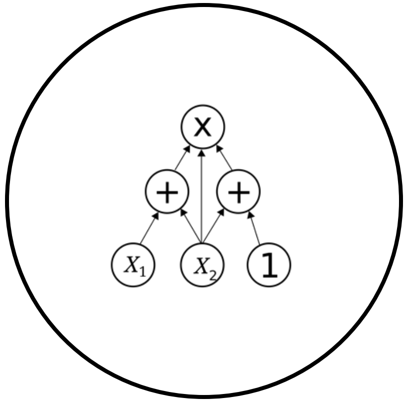
Motivation

SMC

Boolean



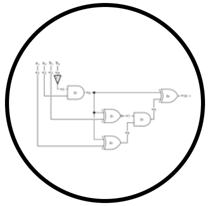
Arithmetic

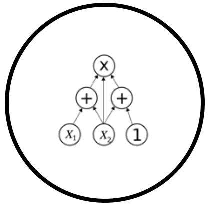


Motivation

SMC

Circuit



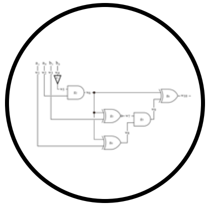


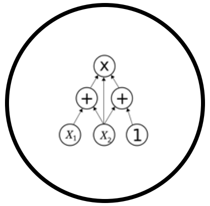
Motivation

SMC

Primitive

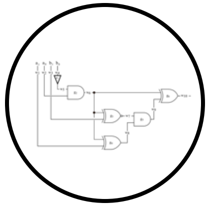
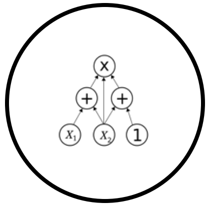
Circuit





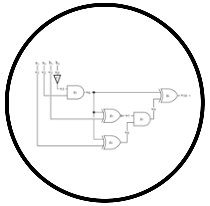
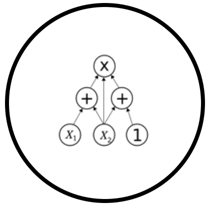
Motivation

SMC

Primitive	Oblivious Transfer	
Circuit		

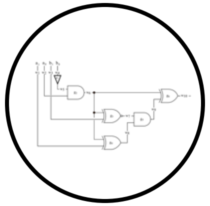
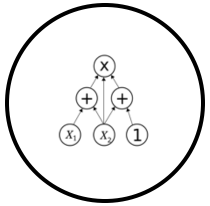
Motivation

SMC

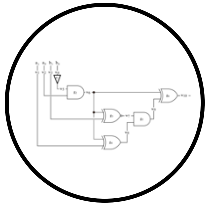
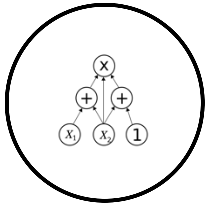
Primitive	Oblivious Transfer	Oblivious Linear Evaluation
Circuit		

Motivation

SMC

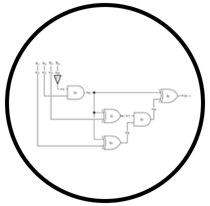
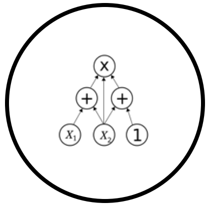
	Classic	Classic
Primitive	Oblivious Transfer	Oblivious Linear Evaluation
Circuit		

Motivation

	SMC			
	Quantum	Classic	Quantum	Classic
Primitive	Oblivious Transfer		Oblivious Linear Evaluation	
Circuit				

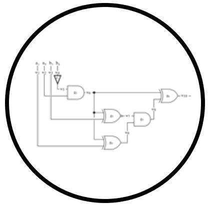
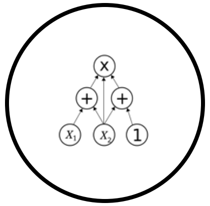
Motivation

SMC

	Quantum	Classic	Quantum	Classic
Primitive	[BBCS'91]	Oblivious Transfer		Oblivious Linear Evaluation
Circuit				

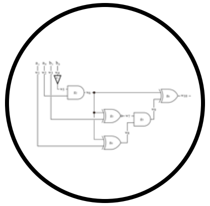
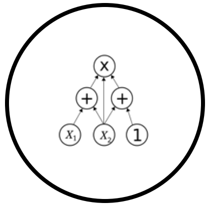
Motivation

SMC

	Quantum	Classic	Quantum	Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer		Oblivious Linear Evaluation
Circuit				

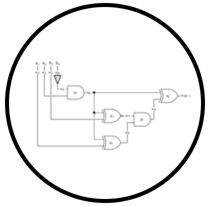
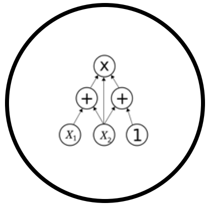
Motivation

SMC

	Quantum		Classic	Quantum		Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer	[EGL'85] SimpleOT …		Oblivious Linear Evaluation	
Circuit						

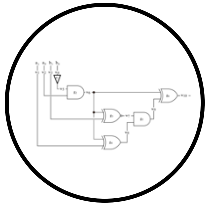
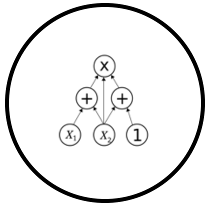
Motivation

SMC

	Quantum	Oblivious Transfer	Classic	Quantum	Oblivious Linear Evaluation	Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Review	[EGL'85] SimpleOT … [YAV'22]			
Circuit						

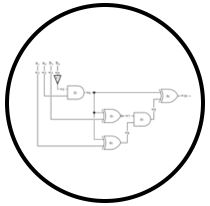
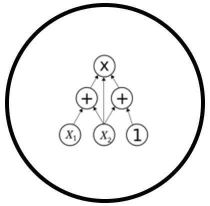
Motivation

SMC

	Quantum		Classic	Quantum		Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer Review	[EGL'85] SimpleOT … [YAV'22]		Oblivious Linear Evaluation	
Circuit						

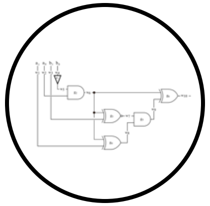
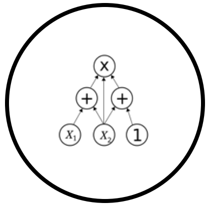
Motivation

SMC

	Quantum		Classic	Quantum		Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer Review	[EGL'85] SimpleOT … [YAV'22]		Oblivious Linear Evaluation	
Circuit						

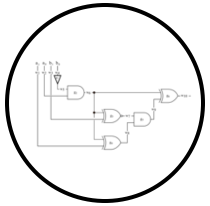
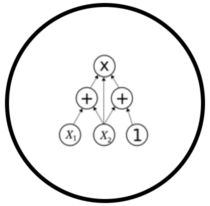
Motivation

SMC

	Quantum		Classic	Quantum		Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer Review	[EGL'85] SimpleOT … libscapi [YAV'22]		Oblivious Linear Evaluation	
Circuit						

Motivation

SMC

	Quantum		Classic	Quantum		Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer Review	[EGL'85] SimpleOT … libscapi [YAV'22]		Oblivious Linear Evaluation	
Circuit						

Motivation

SMC

Quantum

Classic

Quantum

Classic

Primitive

[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …

Oblivious Transfer

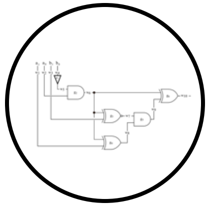
Review

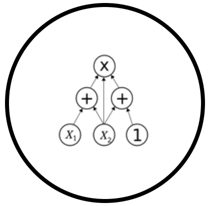
[EGL'85]
SimpleOT
…

libscapi
[YAV'22]

Oblivious Linear Evaluation

Circuit



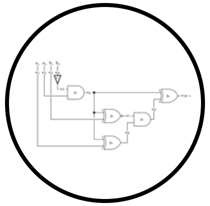
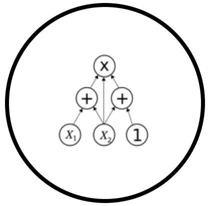


Application

Secure auctions
Secure voting

Motivation

SMC

	Quantum	Classic	Quantum	Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	Oblivious Transfer Review [EGL'85] SimpleOT … libscapi [YAV'22]	Oblivious Linear Evaluation	
Circuit				
Application		Secure auctions Secure voting		

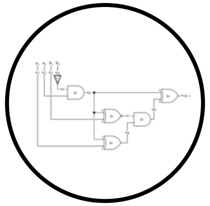
Motivation

SMC

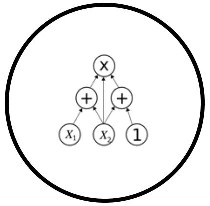
	Quantum	Classic	Quantum	Classic
Primitive	[BBCS'91] [FS'09] [DFS+05] [WST'08] …	[EGL'85] SimpleOT … libscapi [YAV'22]		[NP'99] TinyOLE …
Circuit				
Application		Secure auctions Secure voting		

Oblivious Transfer

Review



Oblivious Linear Evaluation



Motivation

SMC

Quantum | Classic

Primitive

[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …

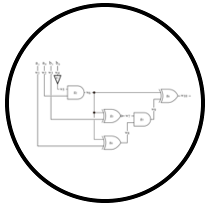
Oblivious Transfer

Review

[EGL'85]
SimpleOT
…

libscapi
[YAV'22]

Circuit



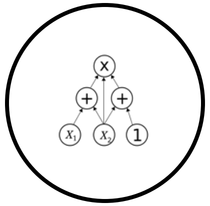
Application

Secure auctions
Secure voting

Quantum | Classic

Oblivious Linear Evaluation

[NP'99]
TinyOLE
…



Motivation

SMC

Quantum | Classic

Primitive

[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …

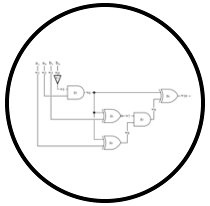
Oblivious Transfer

Review

[EGL'85]
SimpleOT
…

libscapi
[YAV'22]

Circuit



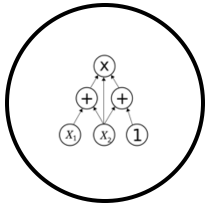
Application

Secure auctions
Secure voting

Quantum | Classic

Oblivious Linear Evaluation

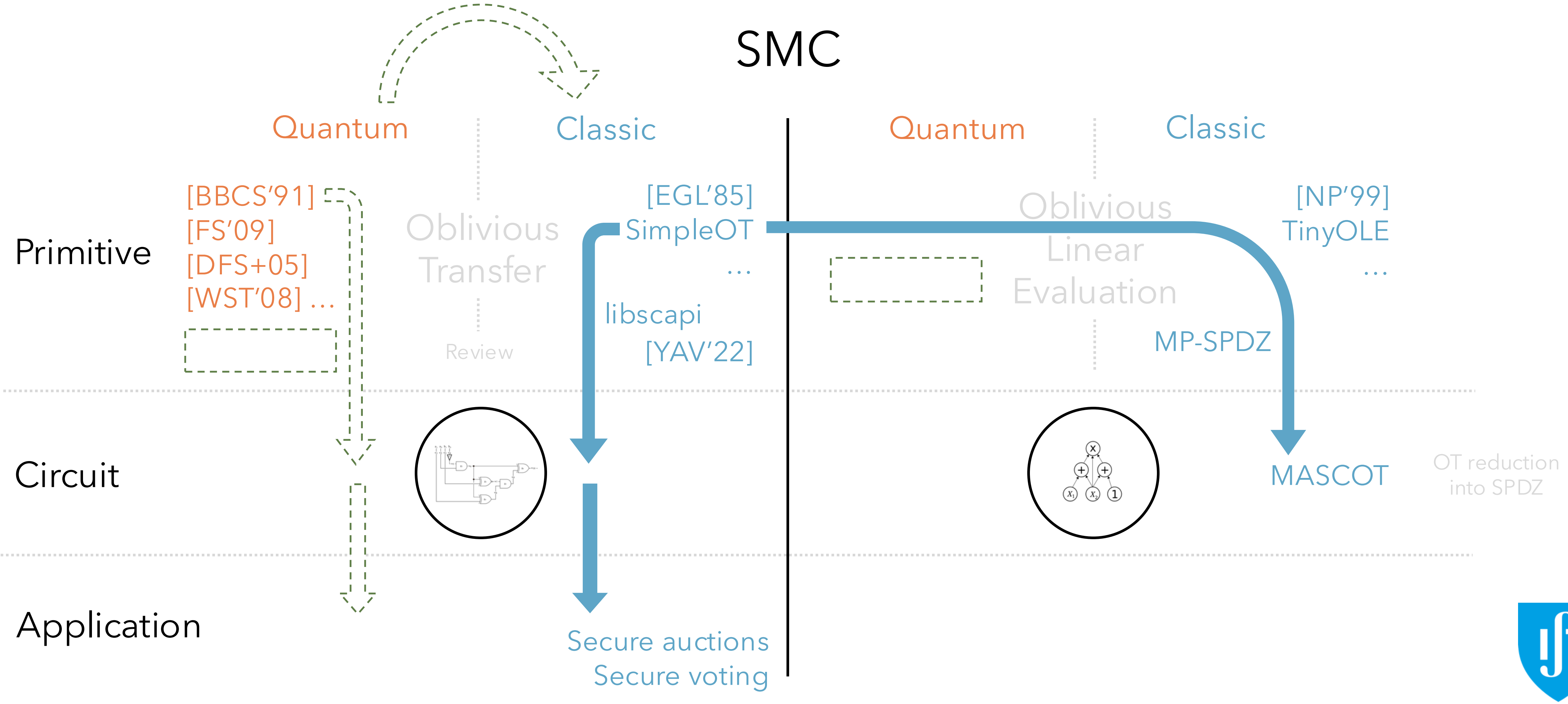
[NP'99]
TinyOLE
…



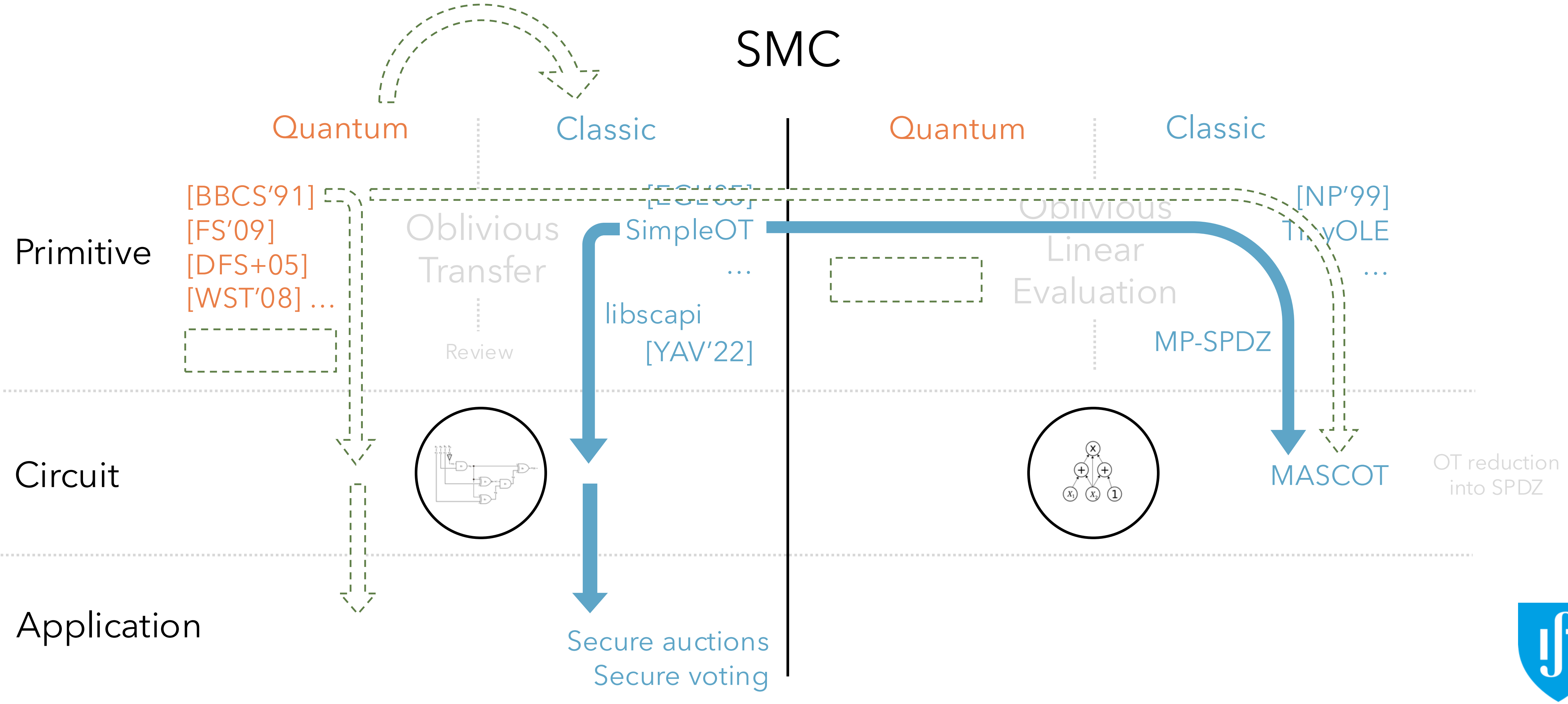
MASCOT

OT reduction into SPDZ

Motivation

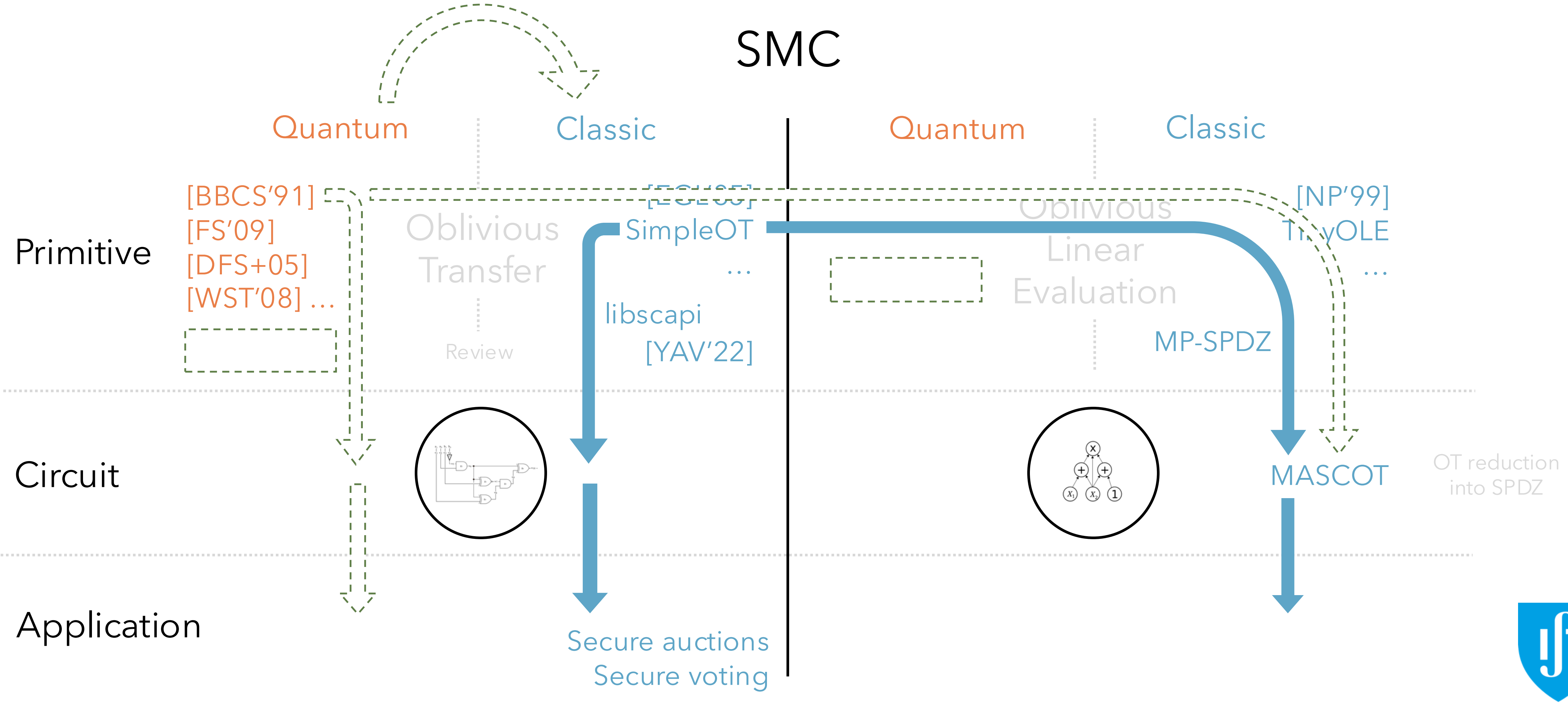

SMC
Quantum
Classic
Quantum
Classic
Primitive
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
Oblivious
Transfer
Review
[EGL'85]
SimpleOT
…
libscapi
[YAV'22]
Oblivious
Linear
Evaluation
[NP'99]
TinyOLE
…
MP-SPDZ
Circuit
MASCOT
OT reduction
into SPDZ
Application
Secure auctions
Secure voting

Motivation

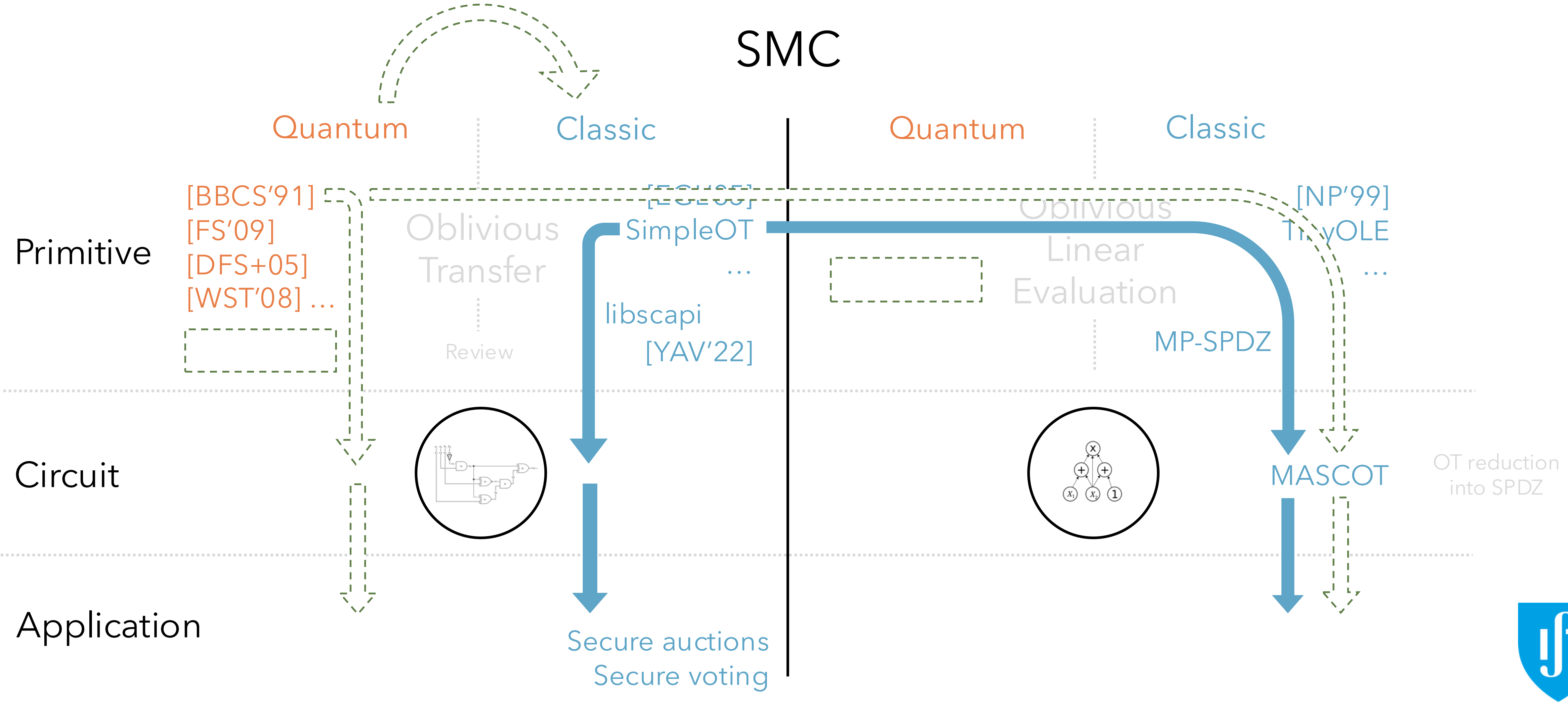


SMC
Quantum
Classic
Quantum
Classic
Primitive
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] ...
Oblivious
Transfer
Review
SimpleOT
...
libscapi
[YAV'22]
Oblivious
Linear
Evaluation
[NP'99]
...
MP-SPDZ
Circuit
MASCOT
OT reduction
into SPDZ
Application
Secure auctions
Secure voting

Motivation

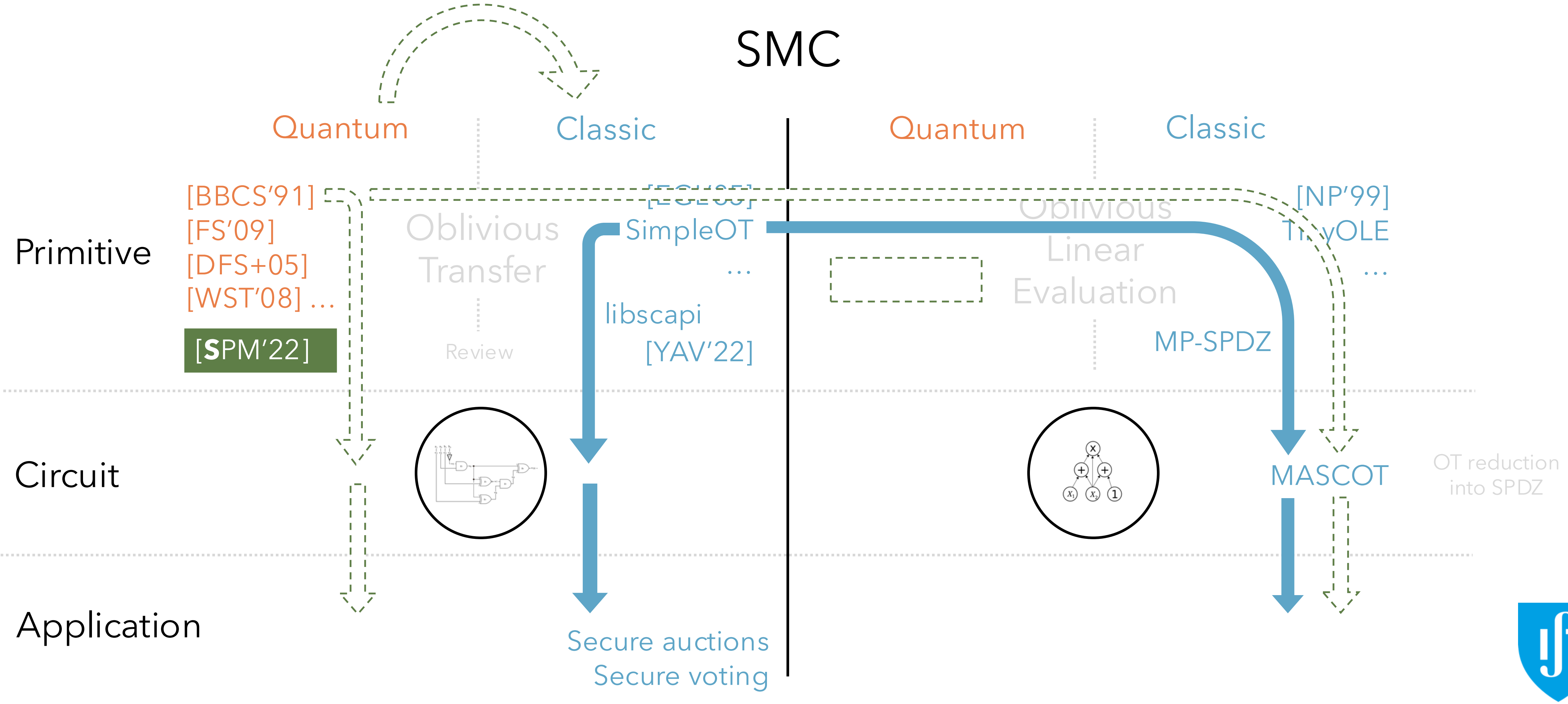

SMC
Quantum
Classic
Quantum
Classic
Primitive
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
Oblivious
Transfer
Review
SimpleOT
…
libscapi
[YAV'22]
Oblivious
Linear
Evaluation
[NP'99]
…
MP-SPDZ
Circuit
MASCOT
OT reduction
into SPDZ
Application
Secure auctions
Secure voting

Motivation



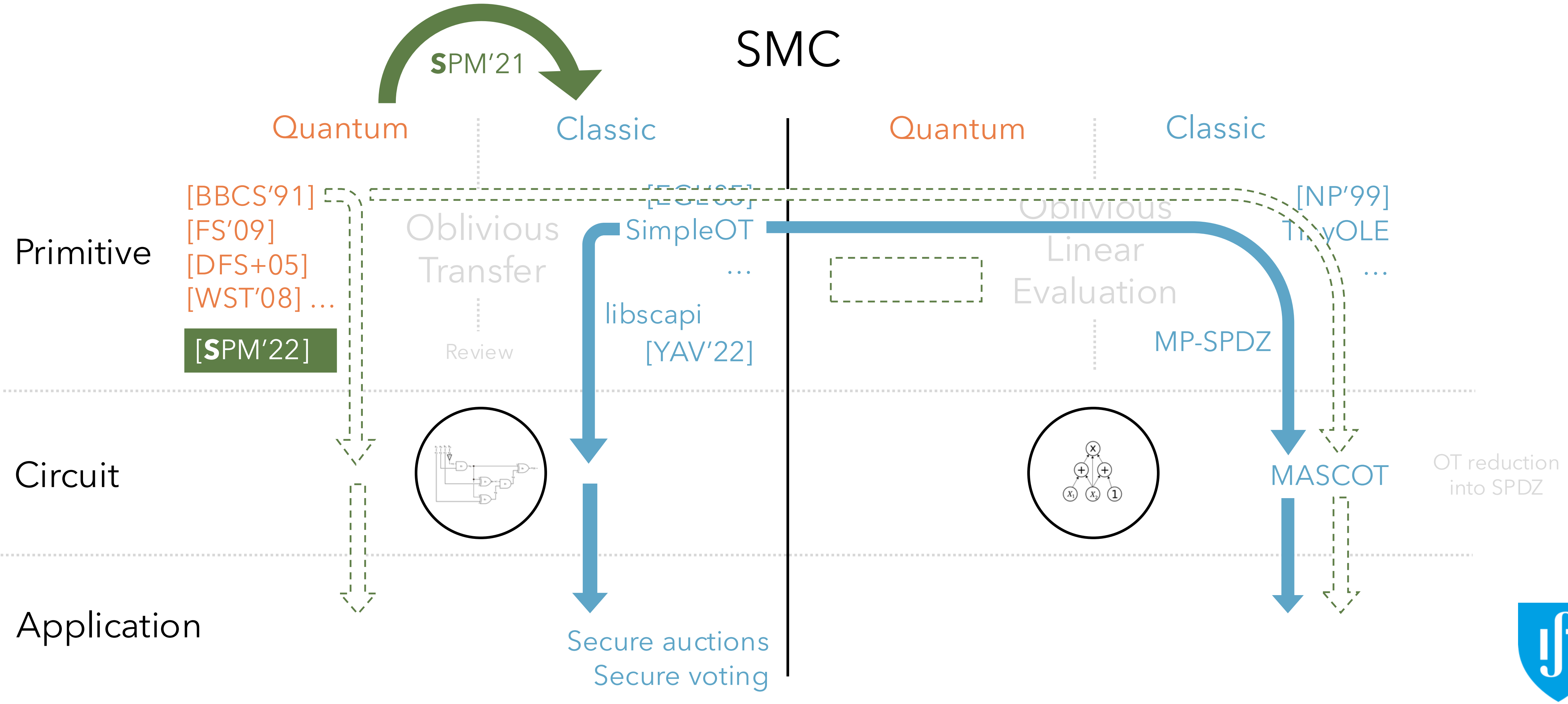
SMC
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
Oblivious
Transfer
Review
[EGL'85]
SimpleOT
…
libscapi
[YAV'22]
Secure auctions
Secure voting
Oblivious
Linear
Evaluation
[NP'99]
TinyOLE
…
MP-SPDZ
MASCOT
OT reduction
into SPDZ

Outcomes



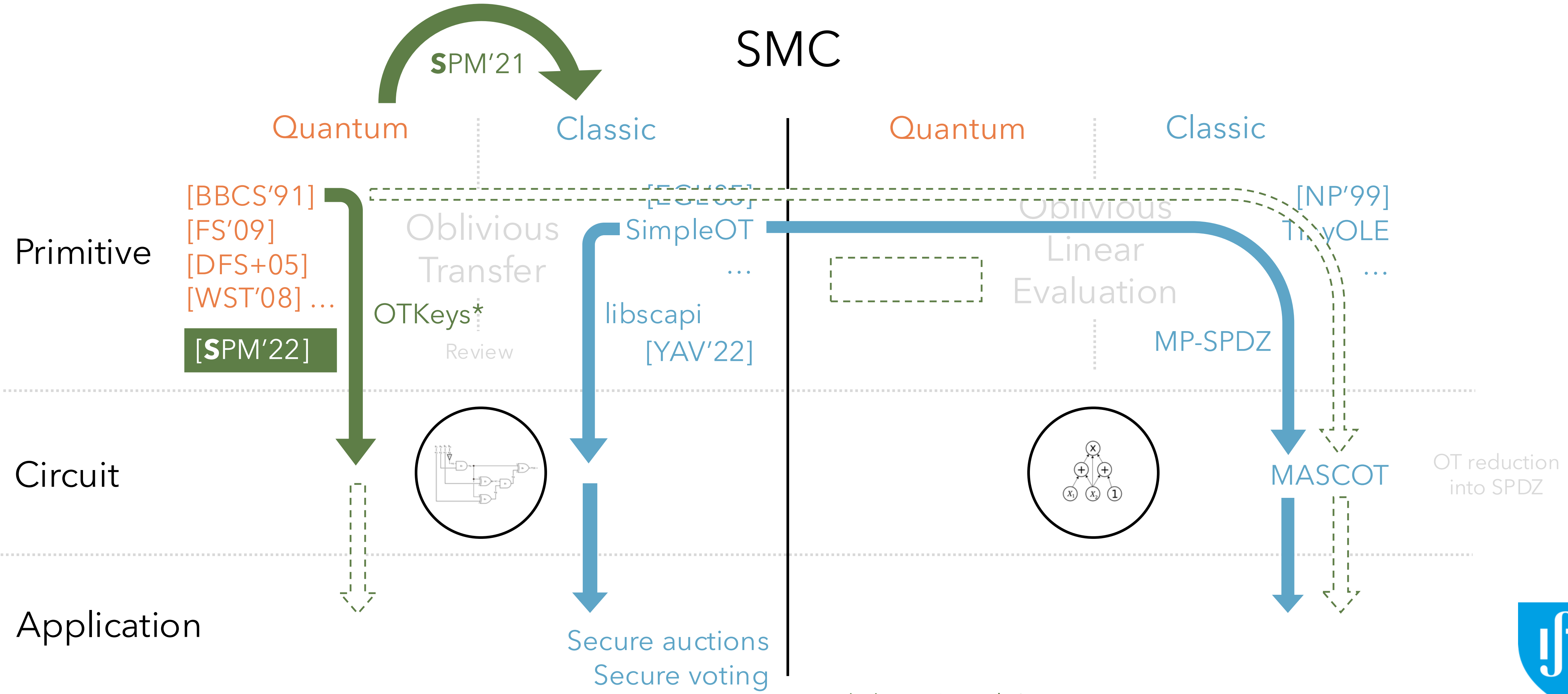
SMC
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious Transfer
Review
SimpleOT
…
libscapi
[YAV'22]
Oblivious Linear Evaluation
[NP'99]
…
MP-SPDZ
MASCOT
OT reduction into SPDZ
Secure auctions
Secure voting

Outcomes



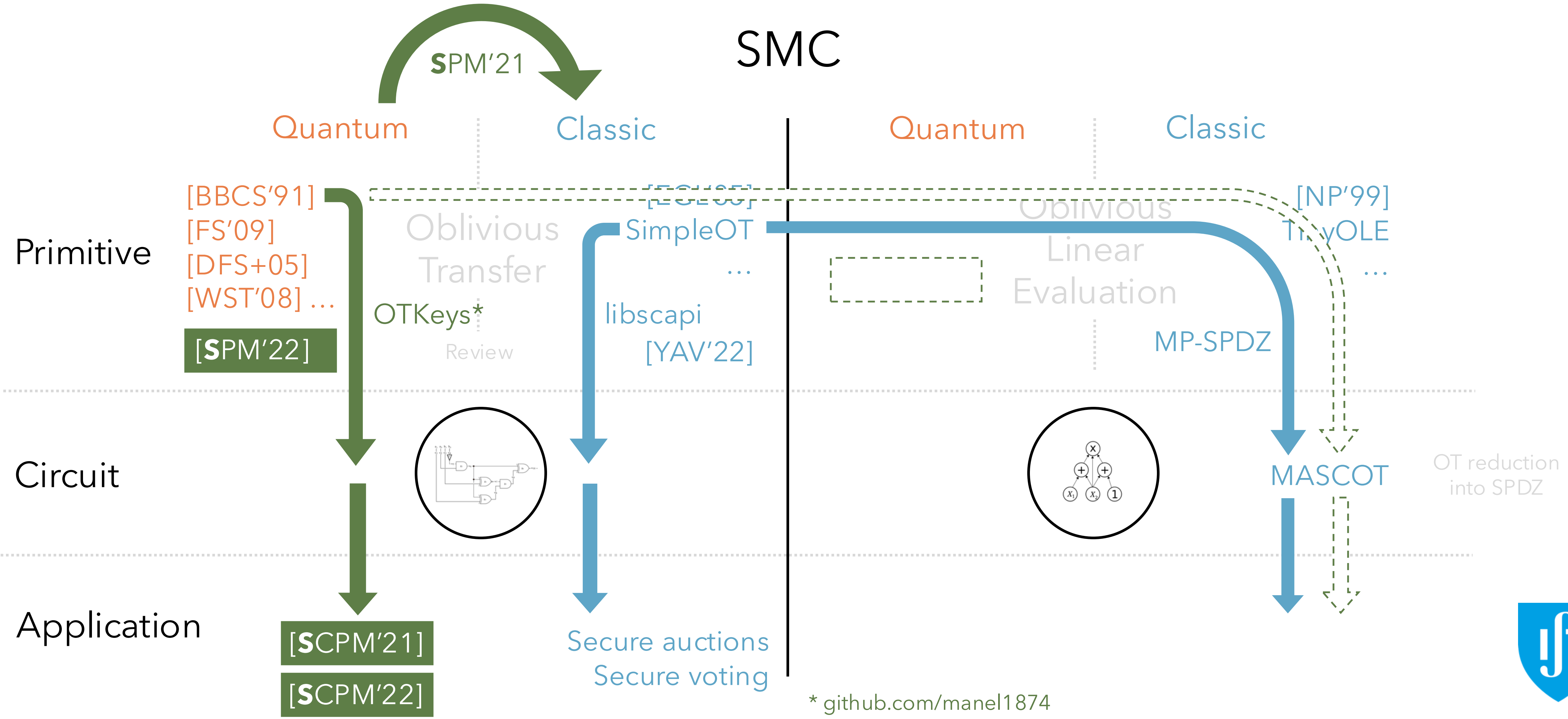
SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious Transfer
Review
SimpleOT
…
libscapi
[YAV'22]
Secure auctions
Secure voting
Oblivious Linear Evaluation
[NP'99]
…
MP-SPDZ
MASCOT
OT reduction into SPDZ

Outcomes



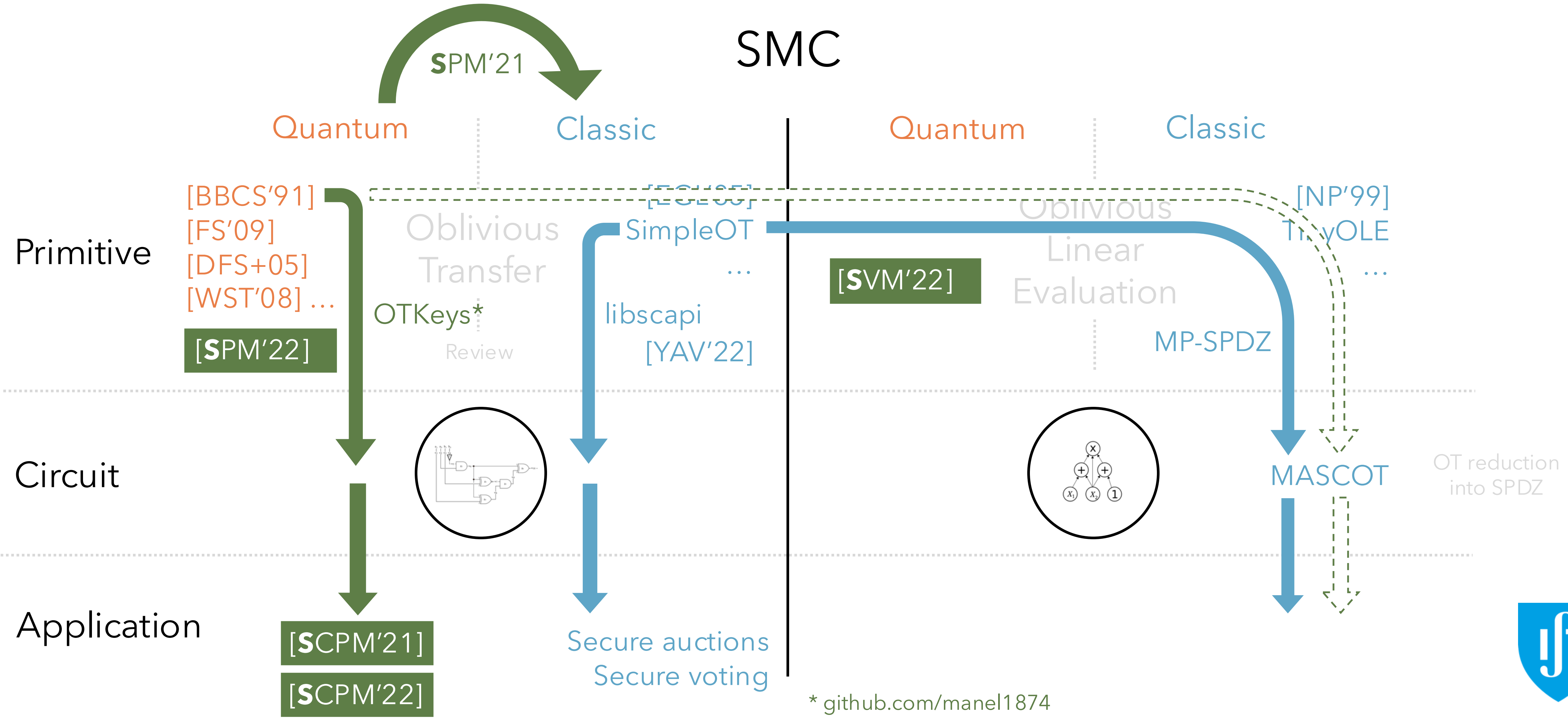
* github.com/manel1874

Outcomes

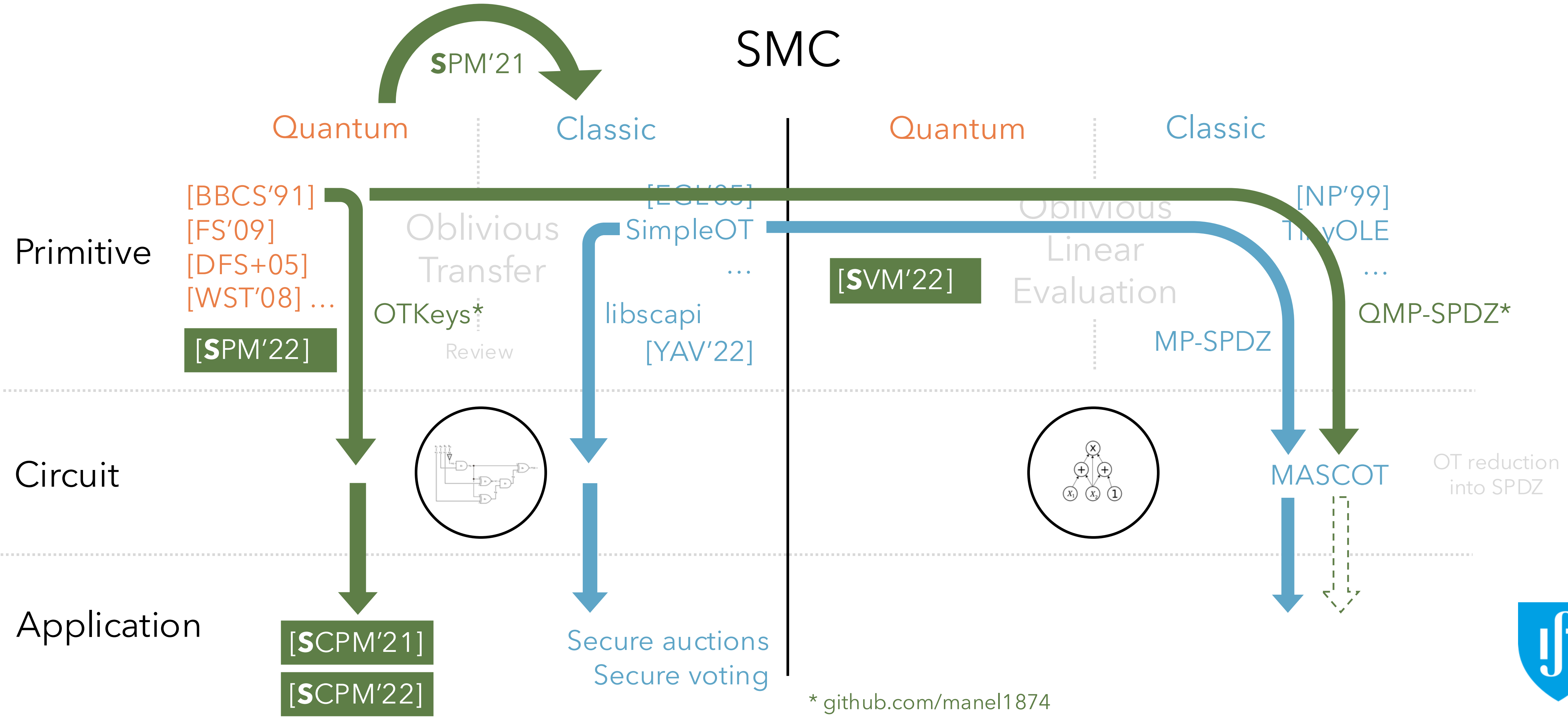


SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious
Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
Oblivious
Linear
Evaluation
[NP'99]
…
MP-SPDZ
MASCOT
OT reduction
into SPDZ
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
* github.com/manel1874

Outcomes

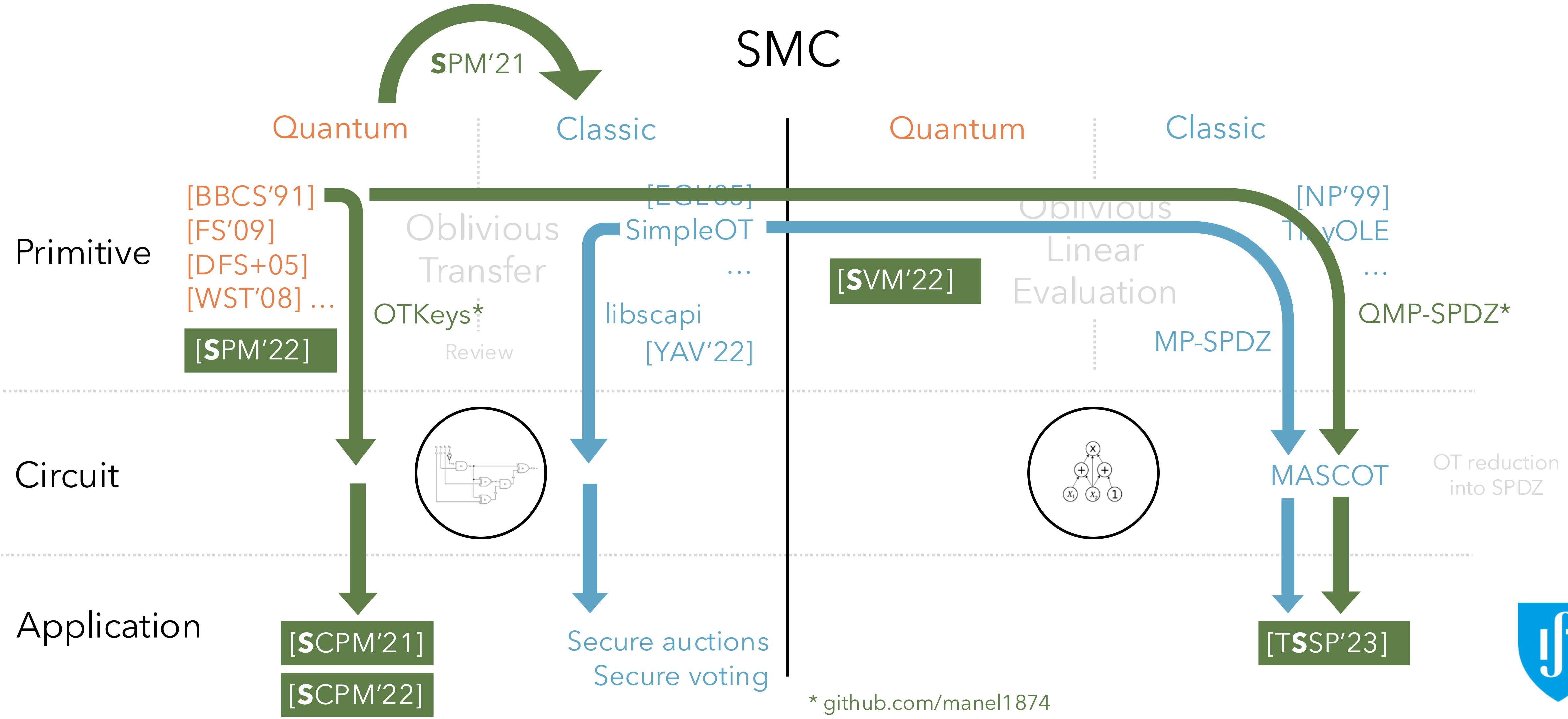

SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
[SVM'22]
Oblivious Linear Evaluation
MP-SPDZ
[NP'99]
…
MASCOT
OT reduction into SPDZ
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
* github.com/manel1874

Outcomes



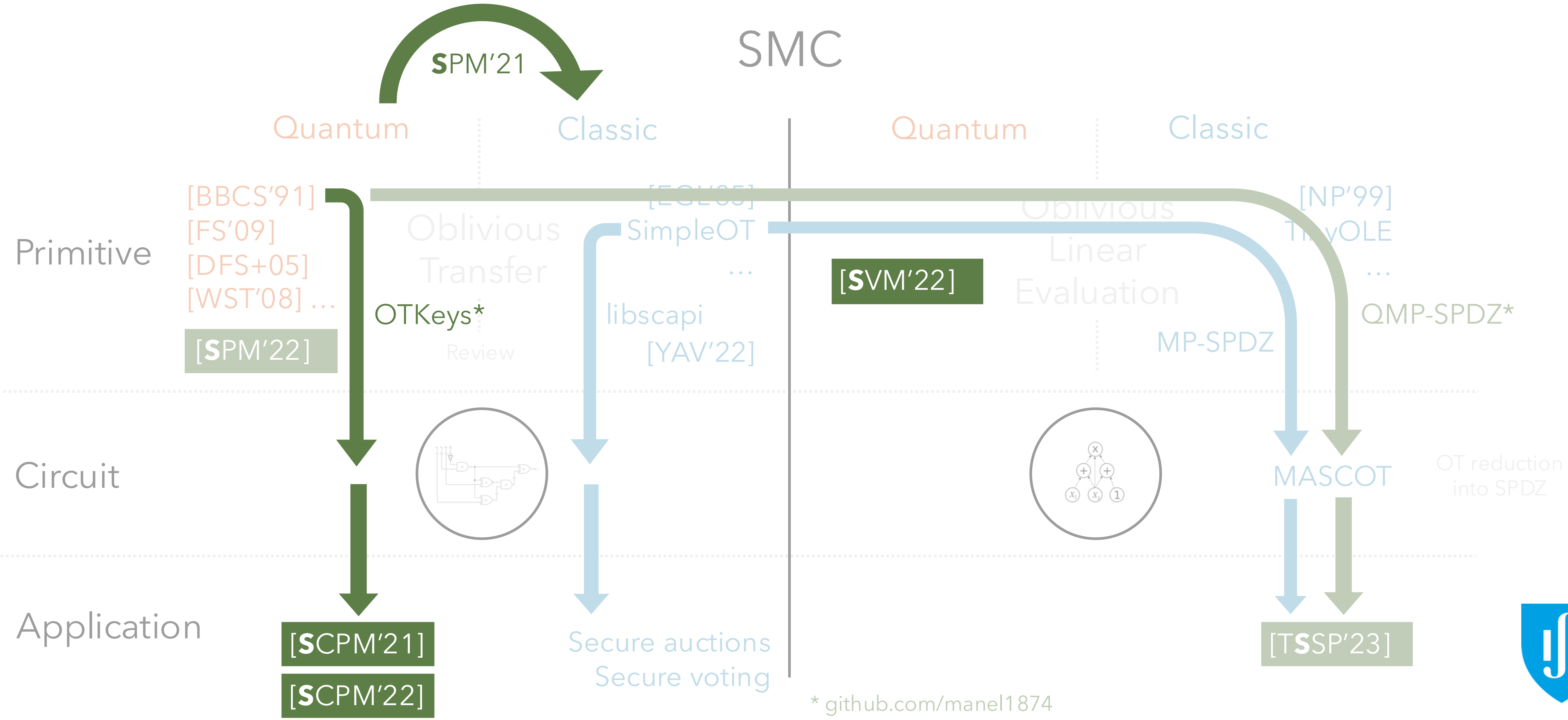
* github.com/manel1874

Outcomes



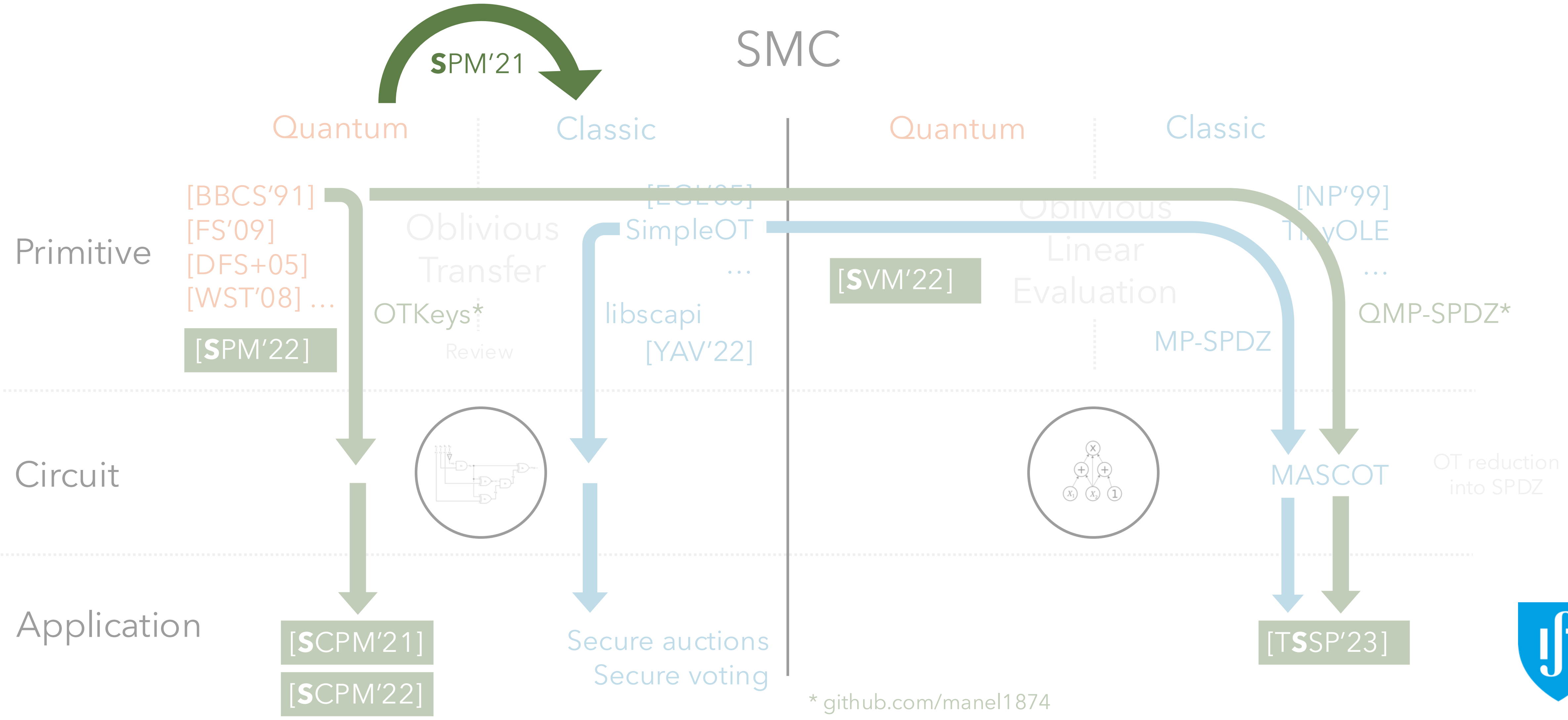
* github.com/manel1874

Outcomes



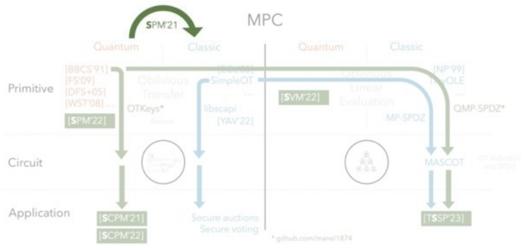
SPM'21
SMC
Quantum
Classic
Quantum
Classic
Primitive
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
[SVM'22]
Oblivious Linear Evaluation
[NP'99]
…
QMP-SPDZ*
MP-SPDZ
Circuit
MASCOT
OT reduction into SPDZ
Application
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
[TSSP'23]
* github.com/manel1874

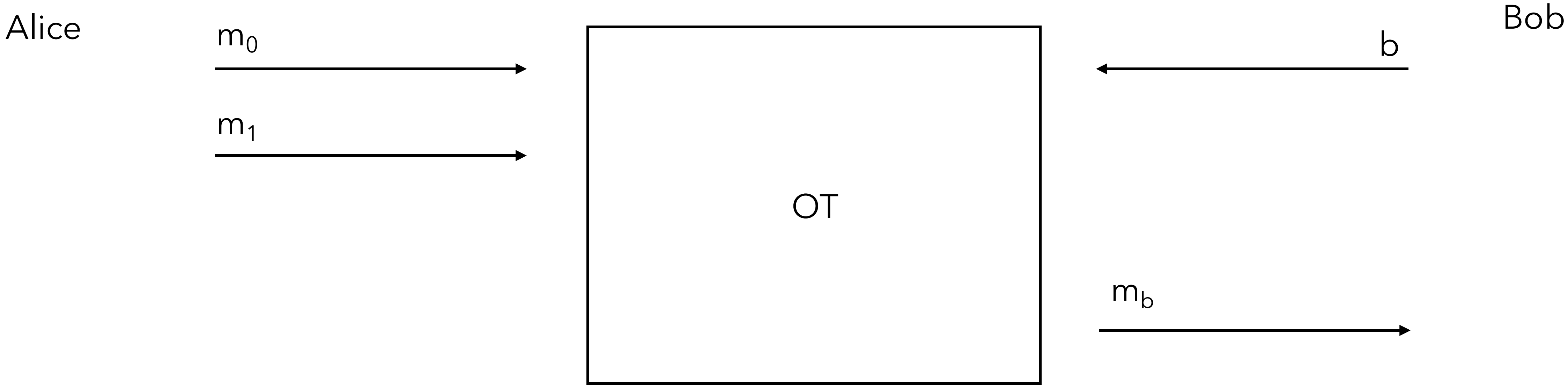
Quantum and classical OT



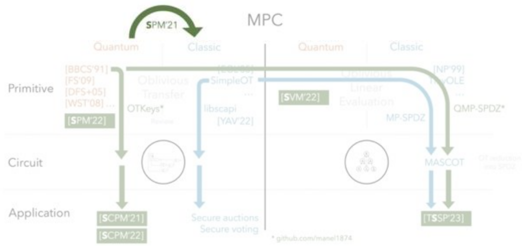
* github.com/manel1874

Oblivious Transfer





Quantum and classical OT



Quantum

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

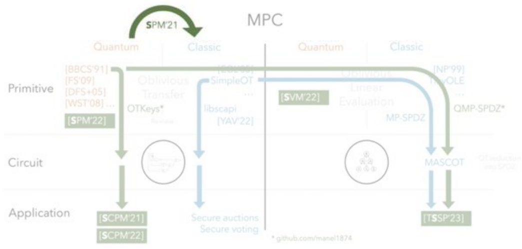
Classic

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

No previous work

How can we compare?

Quantum and classical OT



Quantum

[BBCS’91]
[DFS+05]
[WST’08]
[FS’09]
…

Classic

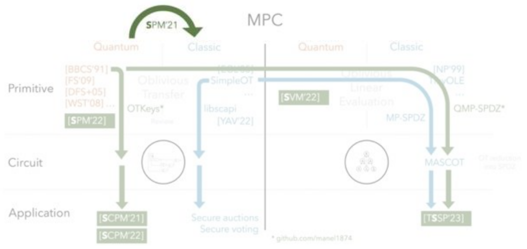
[EGL’85]
[BM’89]
[NP’01]
SimpleOT
…

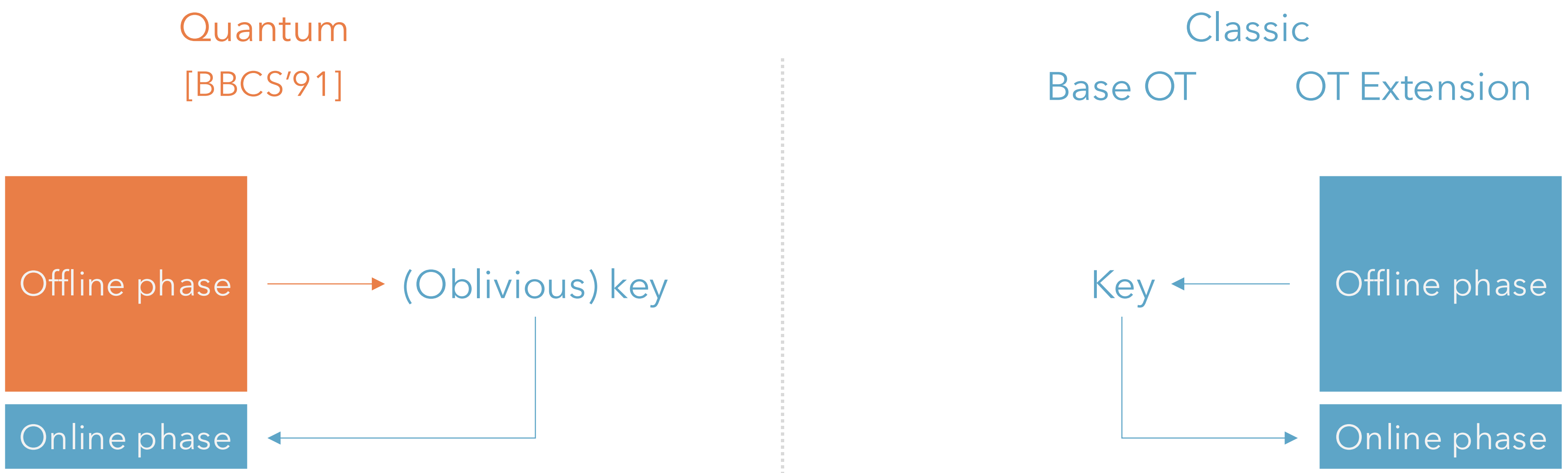
No previous work

How can we compare?

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

Quantum and classical OT



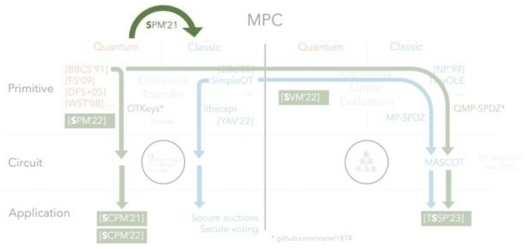


Comparable structure? ✓

Corresponding phases with same technology?

Any practical insight?

Quantum and classical OT



Quantum
[BBCS'91]

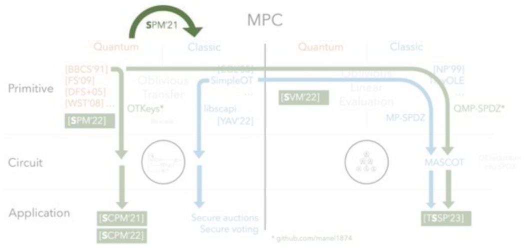
Classic
Base OT
OT Extension

Offline phase → (Oblivious) key
Online phase

Key ← Offline phase
Online phase

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

Quantum and classical OT



Quantum

[BBCS'91]

Classic

Base OT

OT Extension

Input **in**dependent

Offline phase → (Oblivious) key

Key ← Offline phase

Input dependent

Online phase

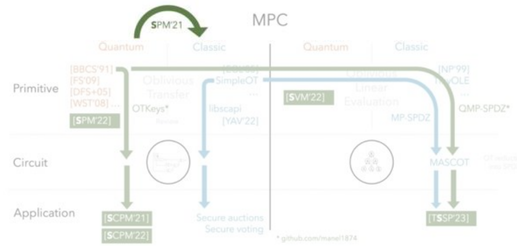
Online phase

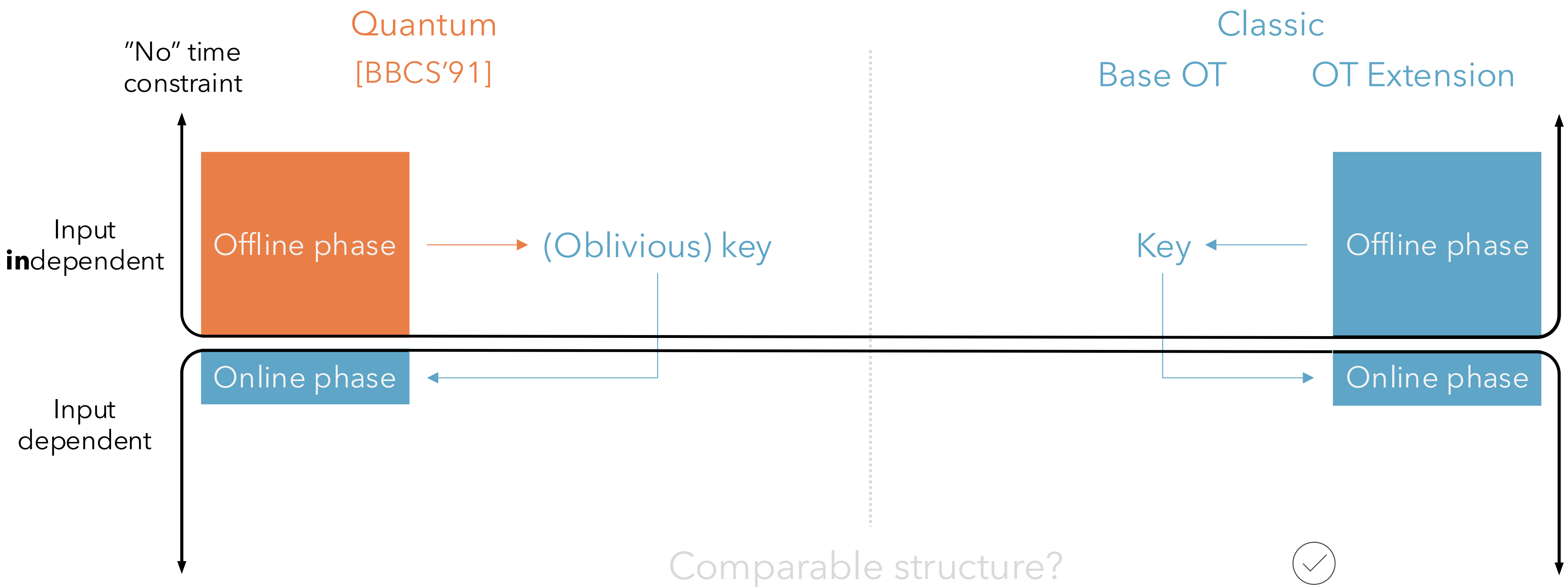
Comparable structure?

Corresponding phases with same technology?

Any practical insight?

Quantum and classical OT





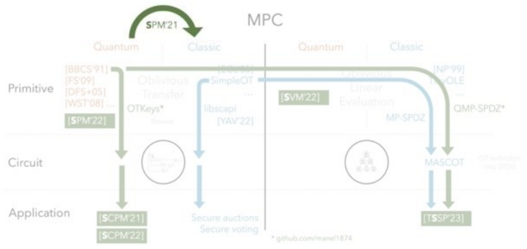
Time constraint

Comparable structure?

Corresponding phases with same technology?

Any practical insight?

Quantum and classical OT



Classic

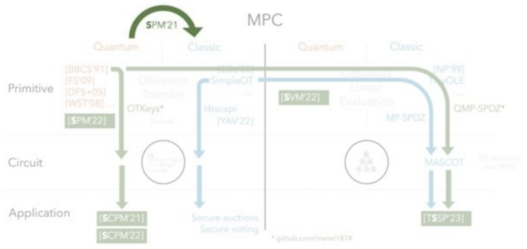
Quantum

Base OT

OT Extension

[BBCS'91]

Quantum and classical OT



Classic

Base OT

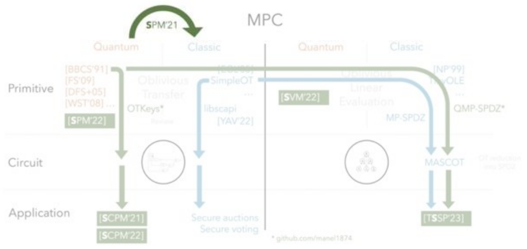
OT Extension

Quantum

[BBCS'91]

Issue: PK operations

Quantum and classical OT



Classic

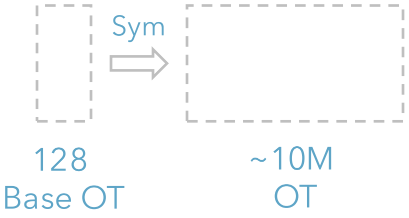
Base OT

OT Extension

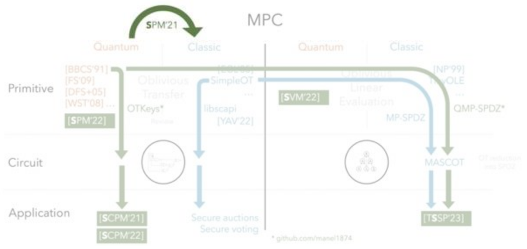
Quantum

[BBCS'91]

Issue: PK operations



Quantum and classical OT



Classic

Quantum

[BBCS'91]

Base OT

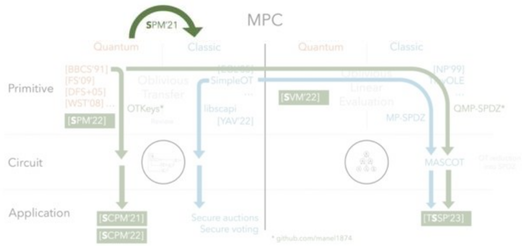
OT Extension

	OT/s
[NP'01]	56
SimpleOT	1 375
NTRU-OT	728
Kyber-OT	41

<

	10M OT
[ALSZ'13]	2.68 s
[KOS'15]	3.35 s

Quantum and classical OT



Classic

Base OT

	OT/s
[NP'01]	56
SimpleOT	1 375
NTRU-OT	728
Kyber-OT	41

<

OT Extension

	10M OT
[ALSZ'13]	2.68 s
[KOS'15]	3.35 s

Quantum

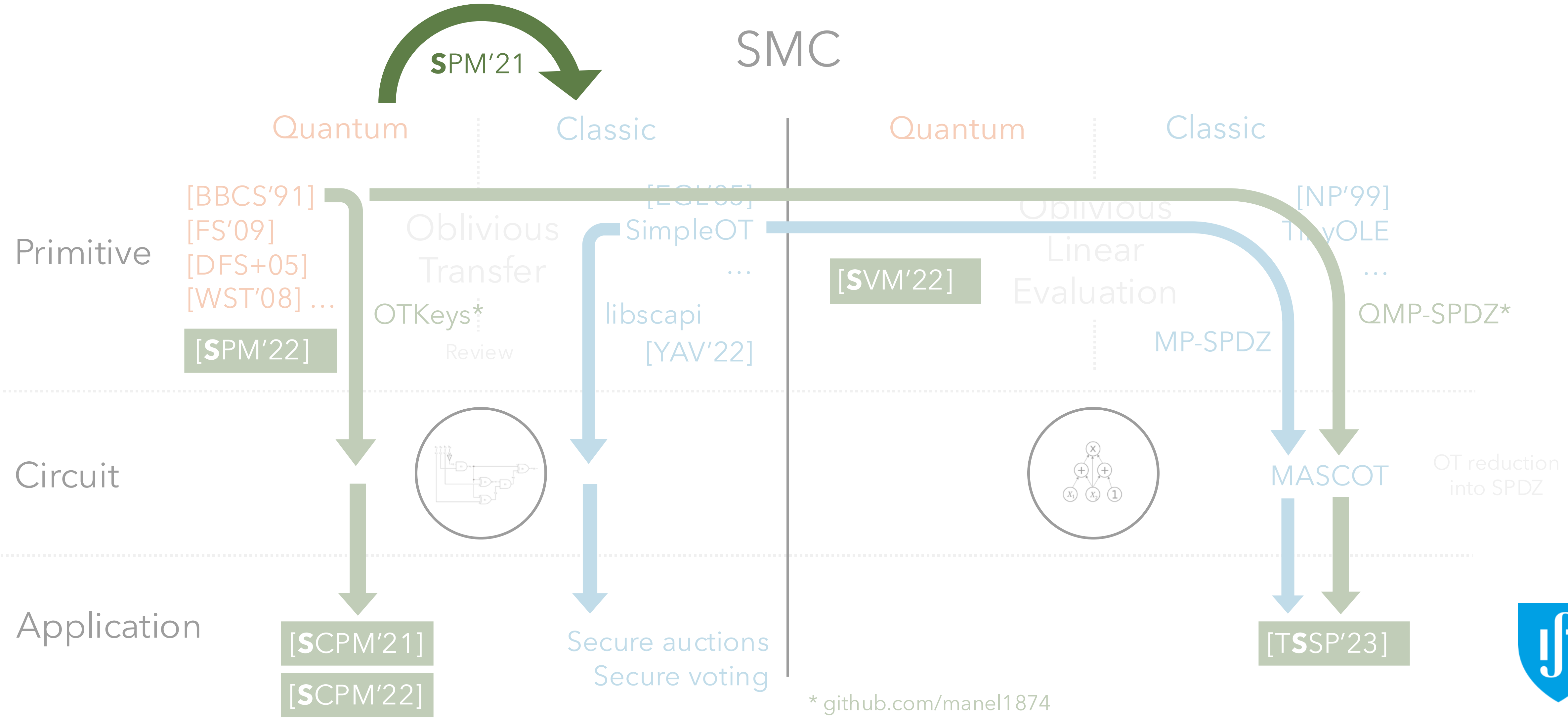
[BBCS'91]

Online phase for m OTs

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

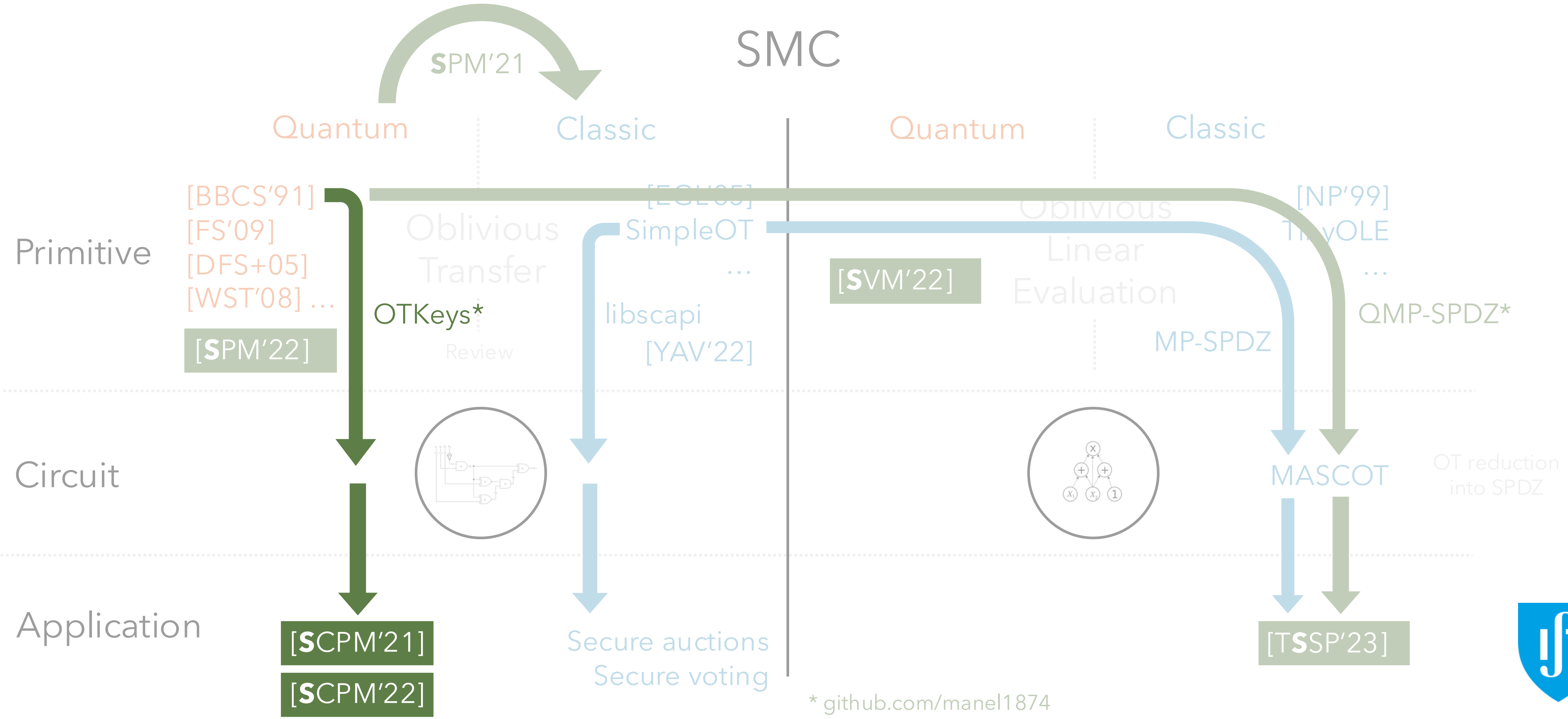
BBCS

Quantum and classical OT



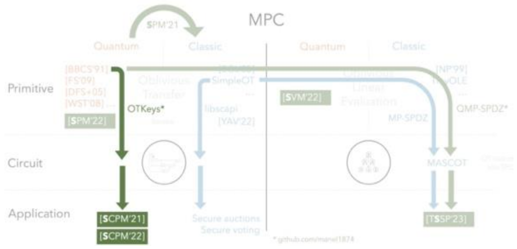
* github.com/manel1874

Private phylogenetic trees

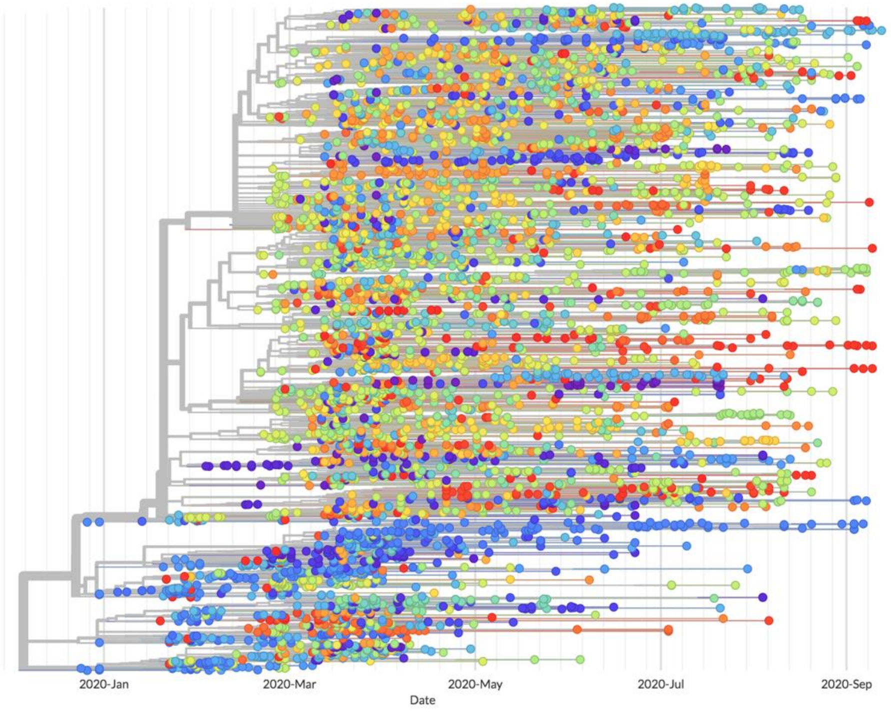


* github.com/manel1874

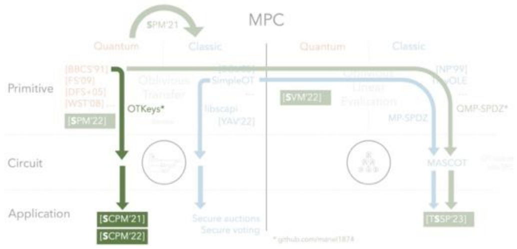
Private phylogenetic trees



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

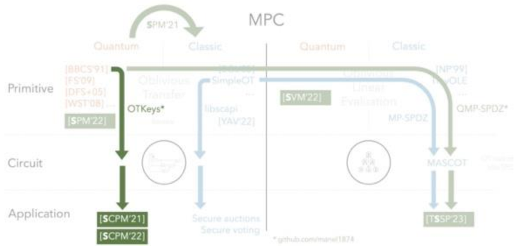


Private phylogenetic trees



Results summary

- Tailored SMC protocol for phylogenetic trees algorithms

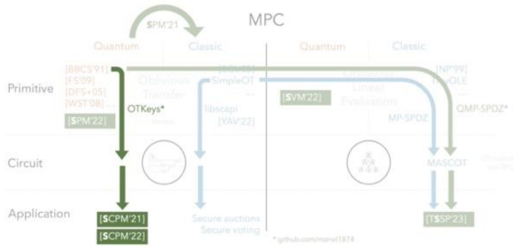


Private phylogenetic trees

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

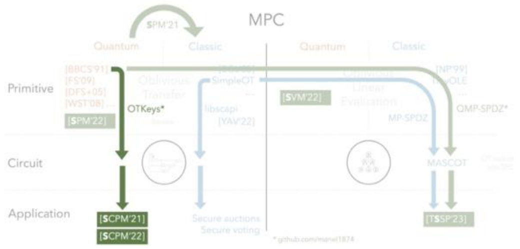
Private phylogenetic trees



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

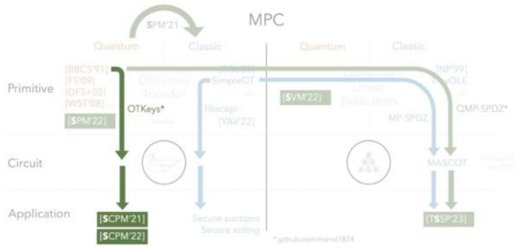
Private phylogenetic trees



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
- Benchmark classical and quantum approaches

Performance evaluation



Setup:

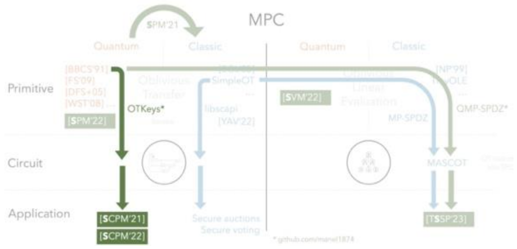
- **3 parties:** VMs running Ubuntu 16.04.3
- **30** SARS-CoV-2 genome **sequences*** with **32 000 length**

Boolean circuit:

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

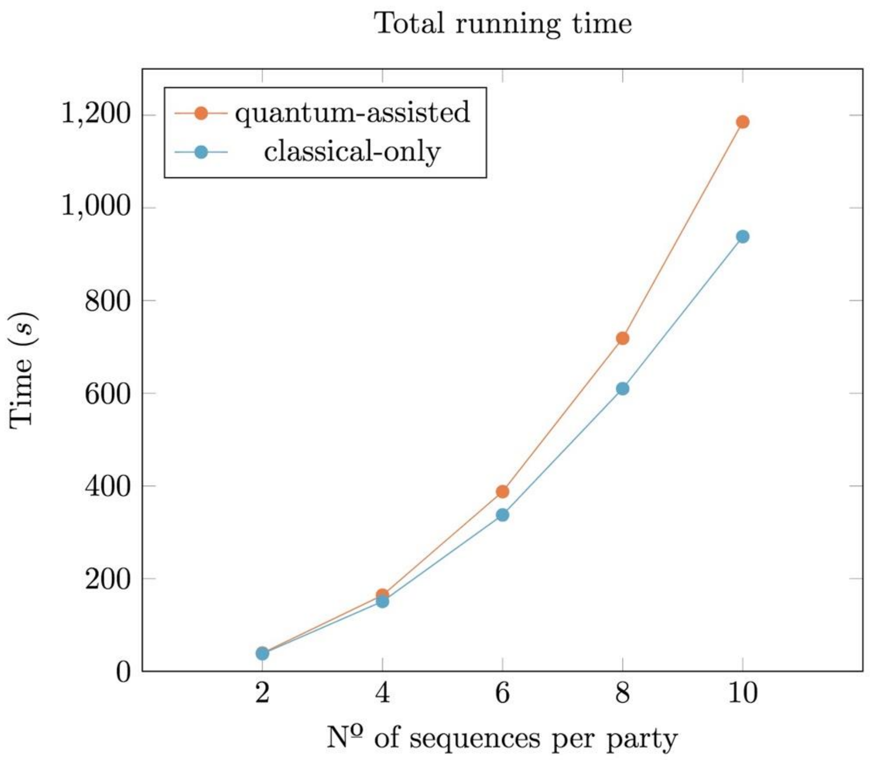
*GISAID database

Performance evaluation

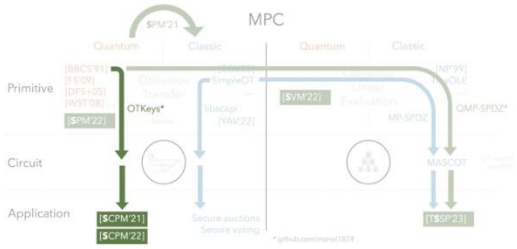


Setup:

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

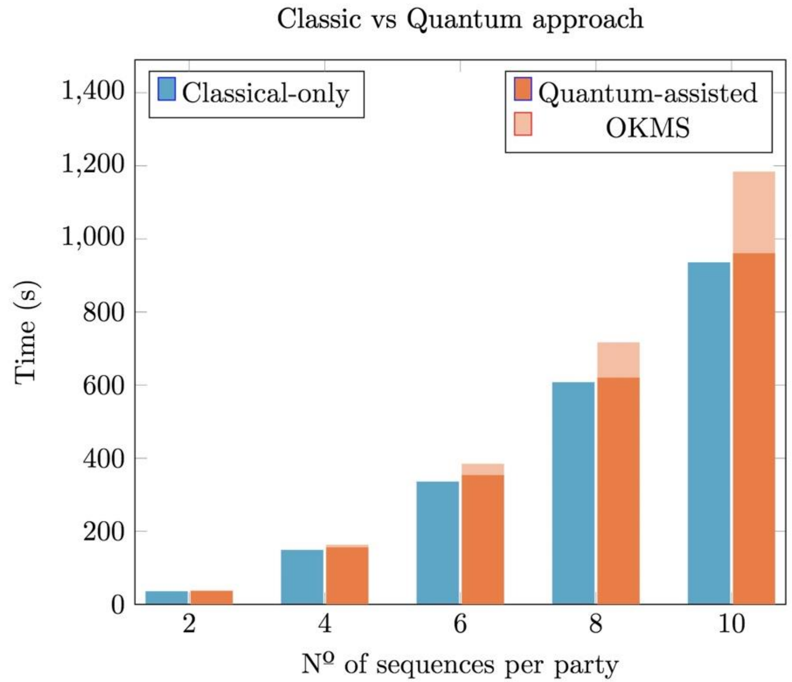


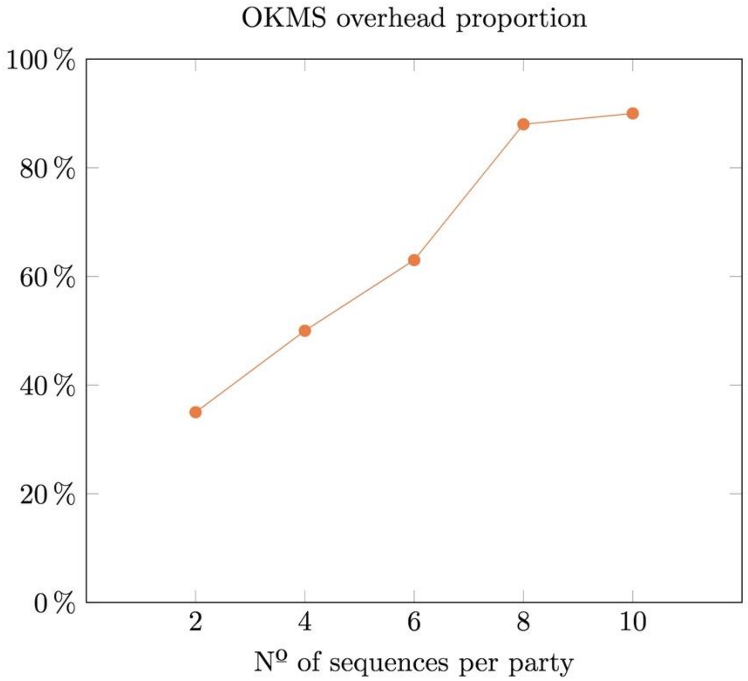
Performance evaluation



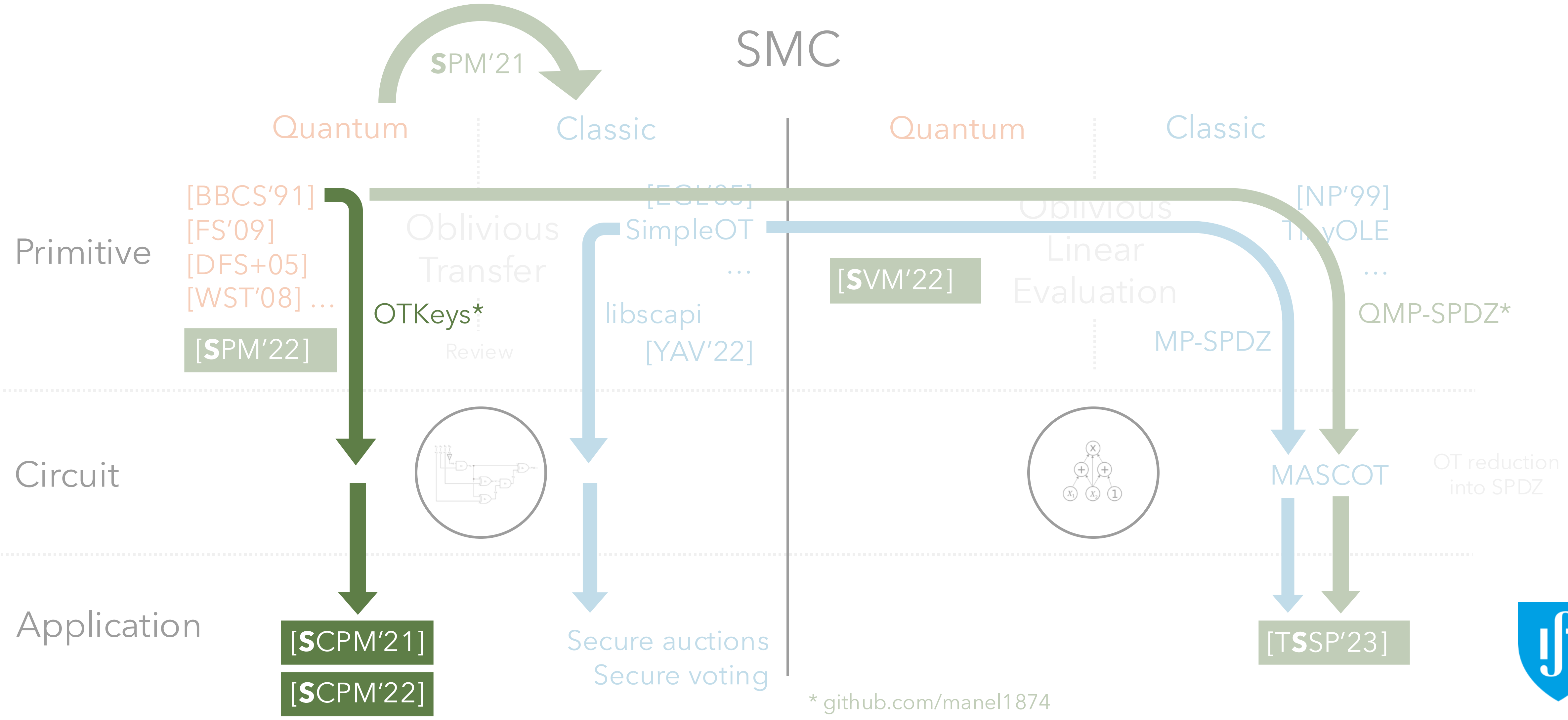
Setup:

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

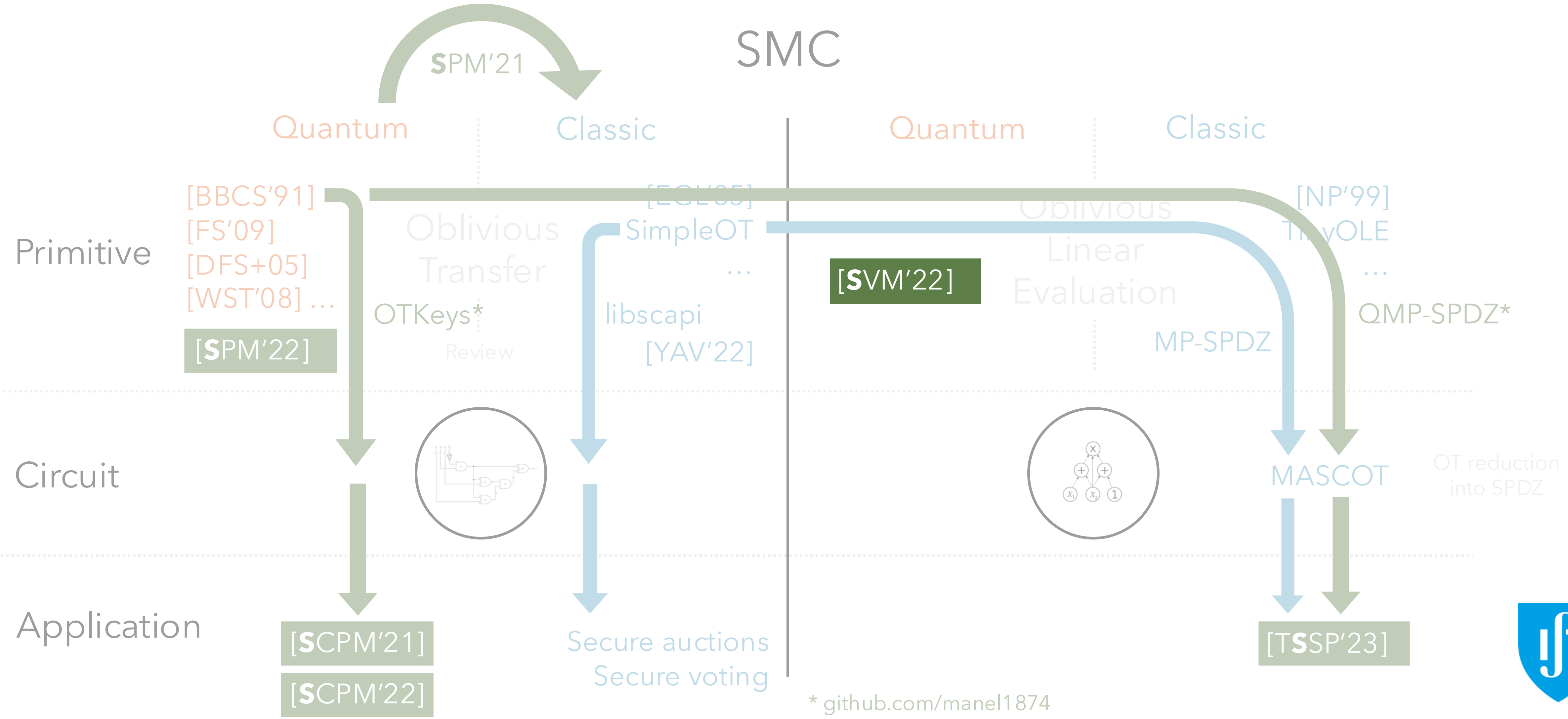




Private phylogenetic trees

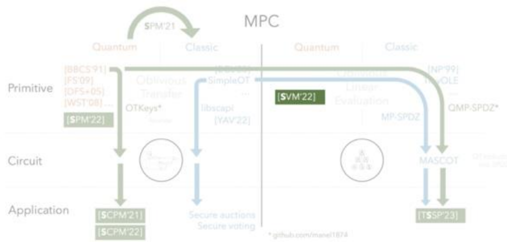


Quantum OLE


SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
[SVM'22]
Oblivious Linear Evaluation
MP-SPDZ
[NP'99]
…
QMP-SPDZ*
Circuit
MASCOT
OT reduction into SPDZ
Application
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
[TSSP'23]
* github.com/manel1874

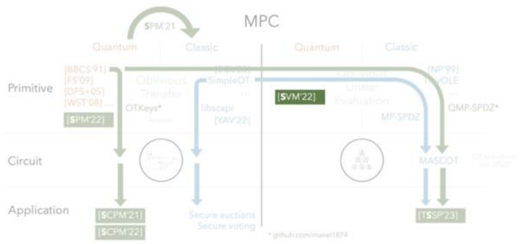
Quantum OLE

Results summary



- Oblivious Linear Evaluation (OLE)
- Vector OLE

Quantum OLE

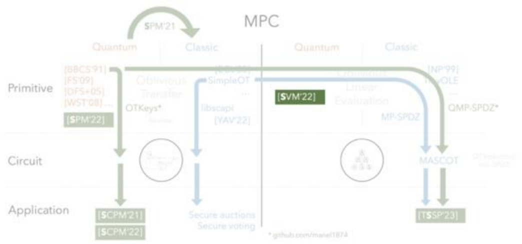


Results summary

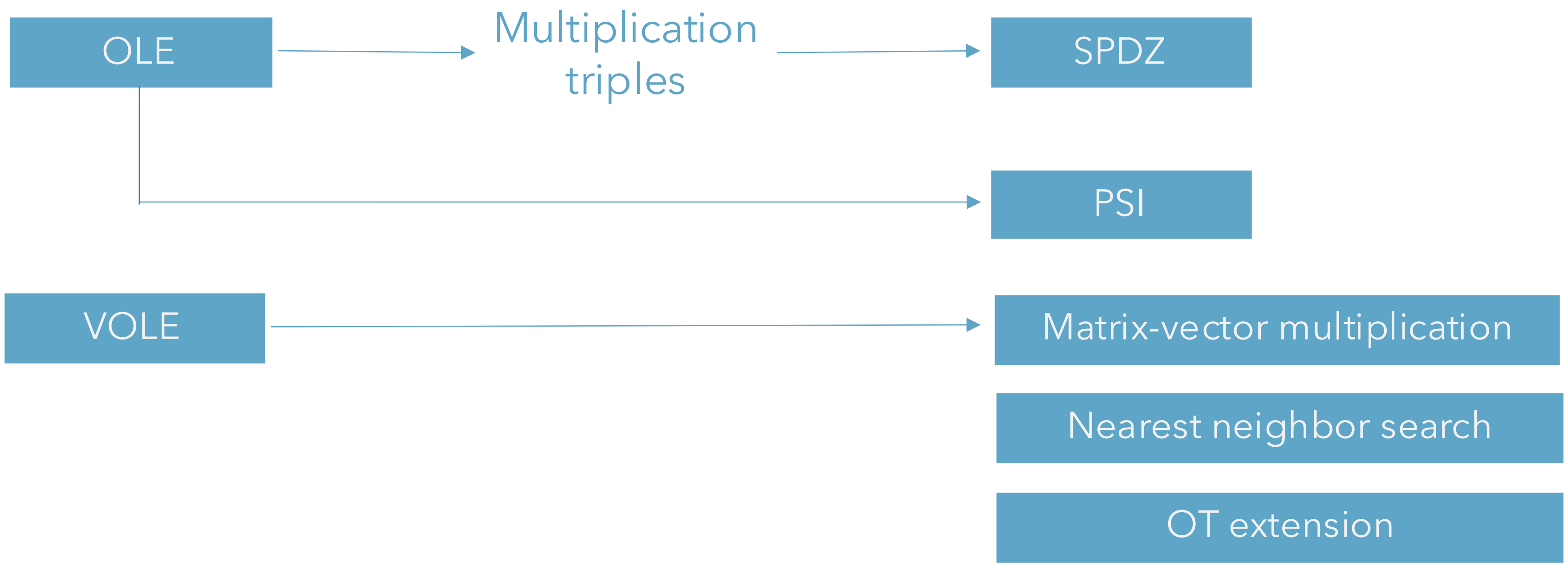
- Oblivious Linear Evaluation (OLE)
- Vector OLE

Quantum OLE

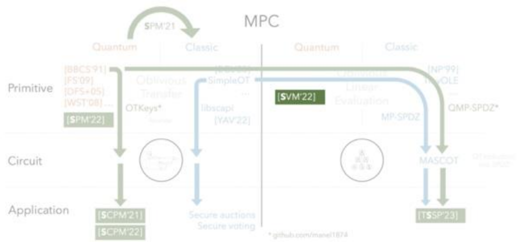
Results summary



- Oblivious Linear Evaluation (OLE)
- Vector OLE

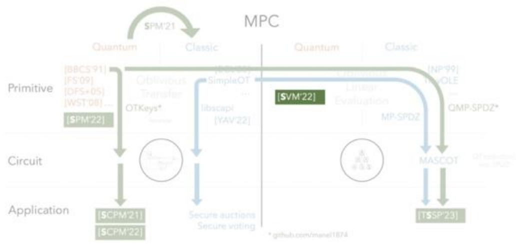


Quantum OLE



Results summary

- Oblivious Linear Evaluation (OLE)
- Vector OLE



Quantum OLE

Results summary

- Oblivious Linear Evaluation (OLE)
- Vector OLE

Alice

a

b

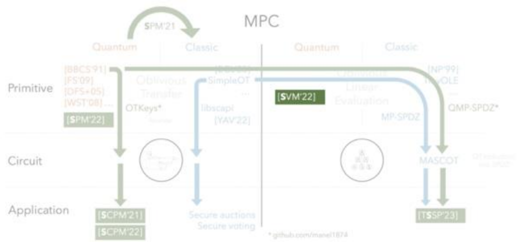
VOLE

Bob

x

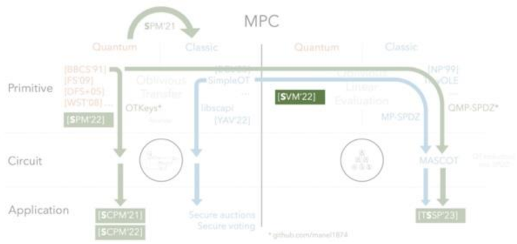
f(x) = **a**x + **b**

Quantum OLE | Main tool



In an Hilbert space of dimension *d*

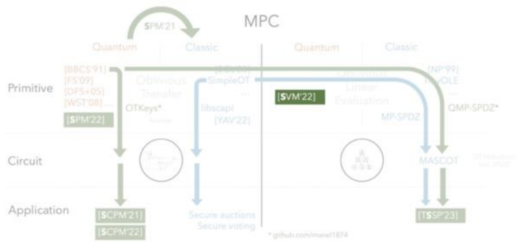
Quantum OLE | Main tool



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

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

Quantum OLE | Main tool



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

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

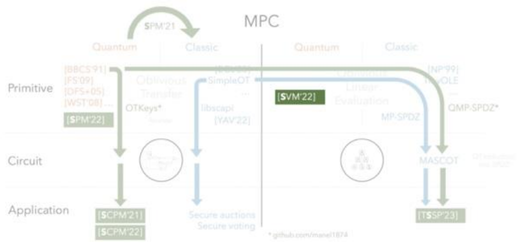
Definition:

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

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

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

Quantum OLE | Main tool



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

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

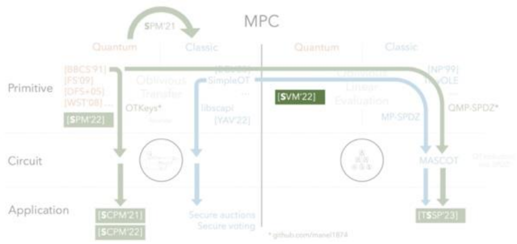
Definition:

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

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

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

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

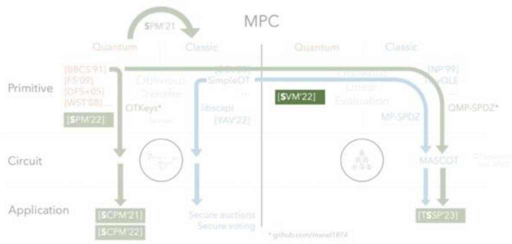
Definition:

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

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

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

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:

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

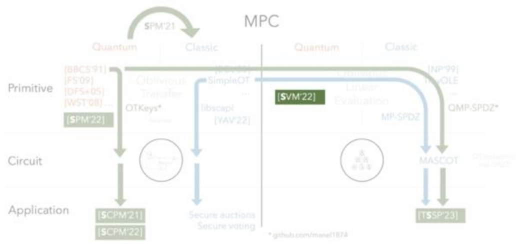
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

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

Definition:

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

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

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

Definition:

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

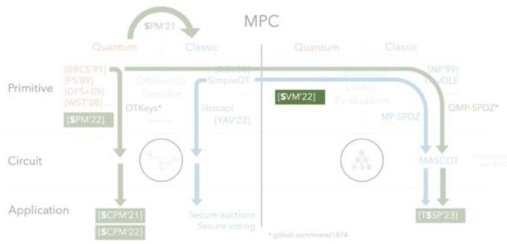
$$\mathcal{B}_0 = \{|\psi_1\rangle,\dots,|\psi_d\rangle\}$$

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

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

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

Alice, (a,b)

Bob, x

Definition:

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

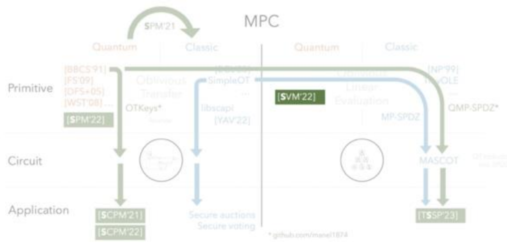
$$\mathcal{B}_0 = \{|\psi_1\rangle, \dots, |\psi_d\rangle\}$$

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

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

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

Alice, (a,b)

Bob, x

$|e_r^x\rangle$

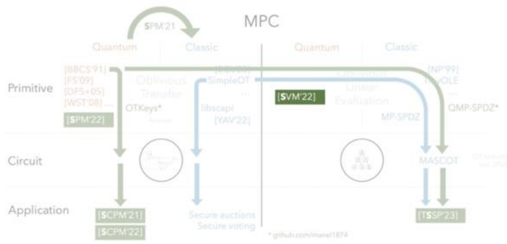
Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle,\ldots,|\phi_d\rangle\}$$
$$\mathcal{B}_0 = \{|\psi_1\rangle,\ldots,|\psi_d\rangle\}$$
$$|\langle\psi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}$$

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:

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

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

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

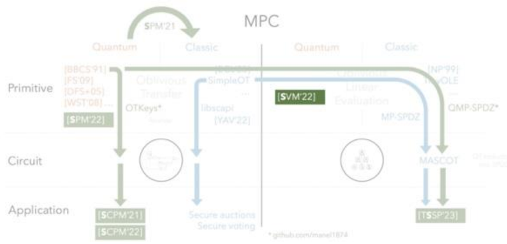
Definition:

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

Alice, (a,b) | Bob, x

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

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

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

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:

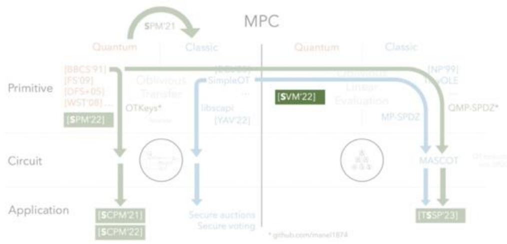
$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1}\omega^{(l+a)b}\,|l+a\rangle\langle l|$$

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

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

Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \ldots, |\phi_d\rangle\}$$
$$\mathcal{B}_0 = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$$
$$|\langle\psi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}$$

Definition:

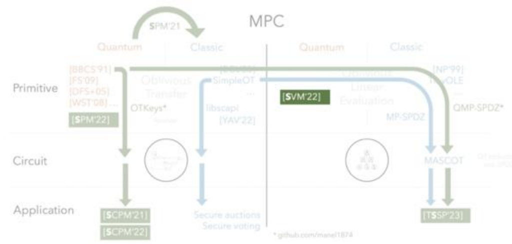
$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1} \omega^{(l+a)b}\,|l+a\rangle\langle l|$$

Alice, (a,b) | Bob, x

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

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

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

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

Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle,\ldots,|\phi_d\rangle\}$$
$$\mathcal{B}_0 = \{|\psi_1\rangle,\ldots,|\psi_d\rangle\}$$
$$|\langle\psi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}$$

Definition:

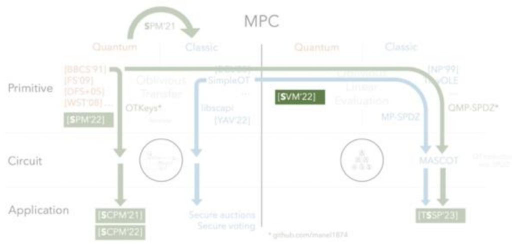
$$V_a^b := V_0^b V_a^0 = \sum_{l=0}^{d-1}\omega^{(l+a)b}|l+a\rangle\langle l|$$

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

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

Definition:

$$\mathcal{B}_1 = \{|\phi_1\rangle, \ldots, |\phi_d\rangle\}$$
$$\mathcal{B}_0 = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$$
$$|\langle\psi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}$$

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

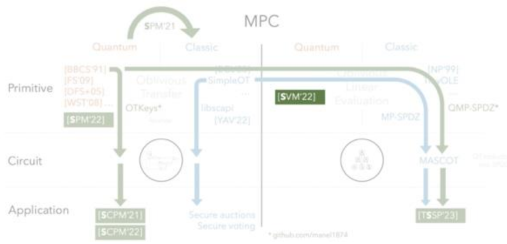
Attack:

$$|B_{a,b}\rangle = (\mathbb{1}\otimes V_a^b)\,|B_{0,0}\rangle$$

$|e_r^x\rangle \leftarrow$ $\qquad$ $\leftarrow |e_r^x\rangle$

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

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

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

Definition:

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

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

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

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

Attack:

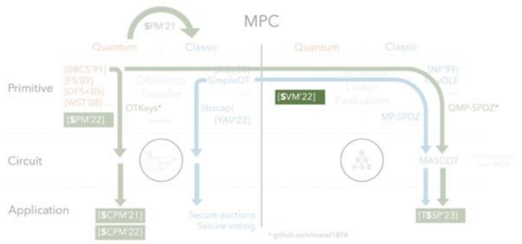
$|e_r^x\rangle$ ← $|e_r^x\rangle$

$|B_{a,b}\rangle = (1\otimes V_a^b)|B_{0,0}\rangle$

Commit-and-open phase

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

Quantum OLE | Protocol



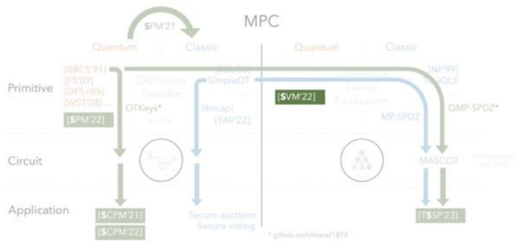
Alice, (a, b)

Bob, x

Quantum phase

Classical phase

Quantum OLE | Protocol



Alice, (a,b)

Bob, x

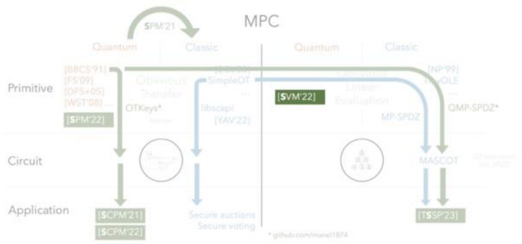
$i \in [m]$

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

Quantum phase

Classical phase

Quantum OLE | Protocol



Quantum phase

Classical phase

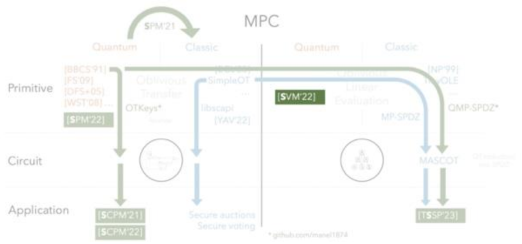
Alice, (a,b) | Bob, x

$i \in [m]$

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

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

Quantum OLE | Protocol



Quantum phase

Classical phase

Alice, (a,b)

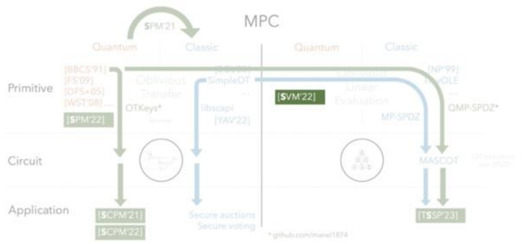
Bob, x

$i \in [m]$

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

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

Quantum OLE | Protocol



Quantum phase

Classical phase

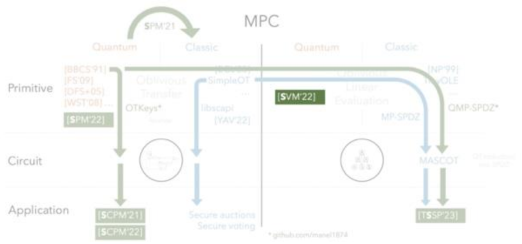
Alice, (a,b) — Bob, x

$i \in [m]$

$\left|e^{x_i^0}_{r_i}\right\rangle \longleftarrow \left|e^{x_i^0}_{r_i}\right\rangle$

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

Quantum OLE | Protocol



Quantum phase

Classical phase

Alice, (a,b)

Bob, x

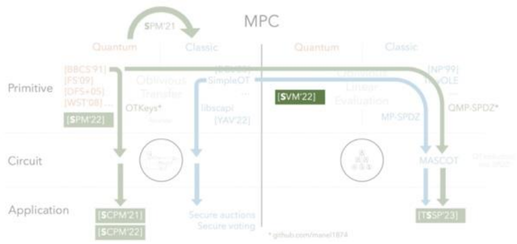
$i \in [m]$

$\left|e^{x_i^0}_{r_i}\right\rangle$ $\longleftarrow$ $\left|e^{x_i^0}_{r_i}\right\rangle$

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

Commit-and-open phase

Quantum OLE | Protocol



Quantum phase

Classical phase

Alice, (a,b)

Bob, x

$i \in [m]$

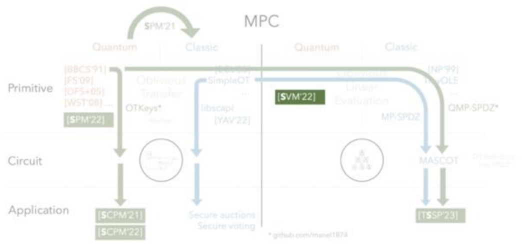
$\left|e^{x_i^0}_{r_i}\right\rangle \longleftarrow \left|e^{x_i^0}_{r_i}\right\rangle$

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

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

Commit-and-open phase

Quantum OLE | Protocol



Quantum phase

Classical phase

Alice, (a,b) | | Bob, x

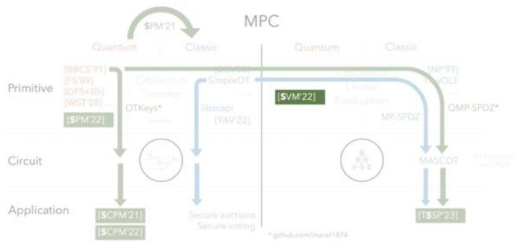
$i \in [m]$

$\left| e^{x_i^0}_{r_i} \right\rangle \longleftarrow \left| e^{x_i^0}_{r_i} \right\rangle$

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

$T \subset [m]$ **Commit-and-open phase** $\texttt{commit}(i, x_i^0, r_i)_{i \in [m]}$

Quantum OLE | Protocol



Quantum phase

Classical phase

Alice, (a,b) — Bob, x

$i \in [m]$

$\left|e^{x_i^0}_{r_i}\right\rangle \longleftarrow \left|e^{x_i^0}_{r_i}\right\rangle$

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

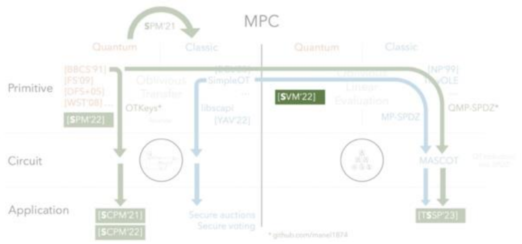
$T \subset [m]$

Commit-and-open phase

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

$\texttt{open}(i, x_i^0, r_i)_{i\in T}$

Quantum OLE | Protocol



Quantum phase

Classical phase

Alice, (a,b) — Bob, x

$i \in [m]$

$\left|e^{x_i^0}_{r_i}\right\rangle \longleftarrow \left|e^{x_i^0}_{r_i}\right\rangle$

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

$T \subset [m]$

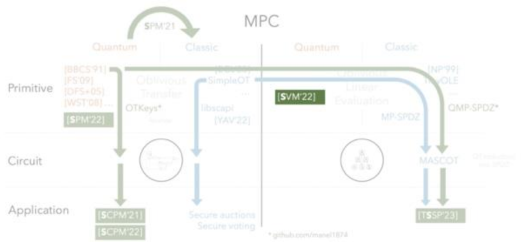
Commit-and-open phase

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

$\mathtt{open}(i, x_i^0, r_i)_{i\in T}$

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

Quantum OLE | Protocol



Quantum phase

Alice, (a,b) — Bob, x

$i \in [m]$

$\left|e^{x_i^0}_{r_i}\right\rangle \longleftarrow \left|e^{x_i^0}_{r_i}\right\rangle$

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

Commit-and-open phase

$T \subset [m]$

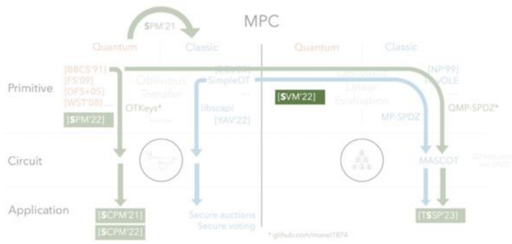
$\texttt{commit}(i, x_i^0, r_i)_{i\in[m]}$

$\texttt{open}(i, x_i^0, r_i)_{i\in T}$

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

Classical phase

Quantum OLE | Protocol



Alice, (a,b) | Bob, x

Quantum phase

$i \in [m]$

$|e^{x_i^0}_{r_i}\rangle$ ⟵ $|e^{x_i^0}_{r_i}\rangle$

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

$T \subset [m]$ **Commit-and-open phase** $\texttt{commit}(i, x_i^0, r_i)_{i\in[m]}$ $\texttt{open}(i, x_i^0, r_i)_{i\in T}$

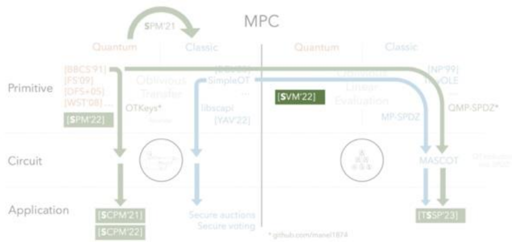
$|e^{x_i^0}_{a_i^0 x_i^0 - b_i^0 + r_i}\rangle$ ⟶ $|e^{x_i^0}_{a_i^0 x_i^0 - b_i^0 + r_i}\rangle$

Classical phase

Derandomization:

n ROLE ⟶ *n* OLE

Quantum OLE | Protocol



Alice, (a,b) | Bob, x

Quantum phase

$i \in [m]$

$|e^{x_i^0}_{r_i}\rangle \longleftarrow |e^{x_i^0}_{r_i}\rangle$

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

$T \subset [m]$ — **Commit-and-open phase** — $\texttt{commit}(i, x_i^0, r_i)_{i\in[m]}$, $\texttt{open}(i, x_i^0, r_i)_{i\in T}$

$|e^{x_i^0}_{a_i^0 x_i^0 - b_i^0 + r_i}\rangle \longrightarrow |e^{x_i^0}_{a_i^0 x_i^0 - b_i^0 + r_i}\rangle$

Classical phase

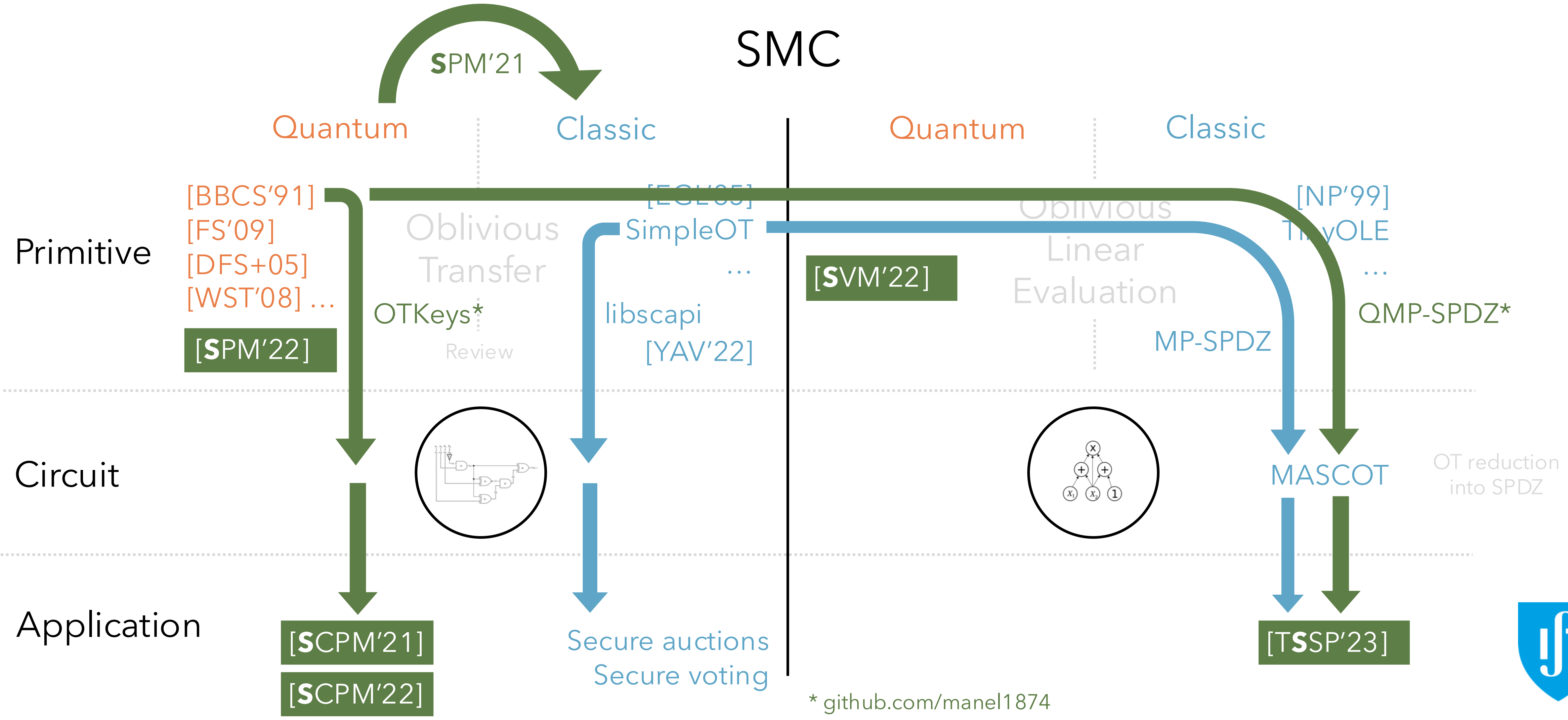
Derandomization:

n ROLE $\longrightarrow$ *n* OLE

Extraction: Privacy amplification + Combiner

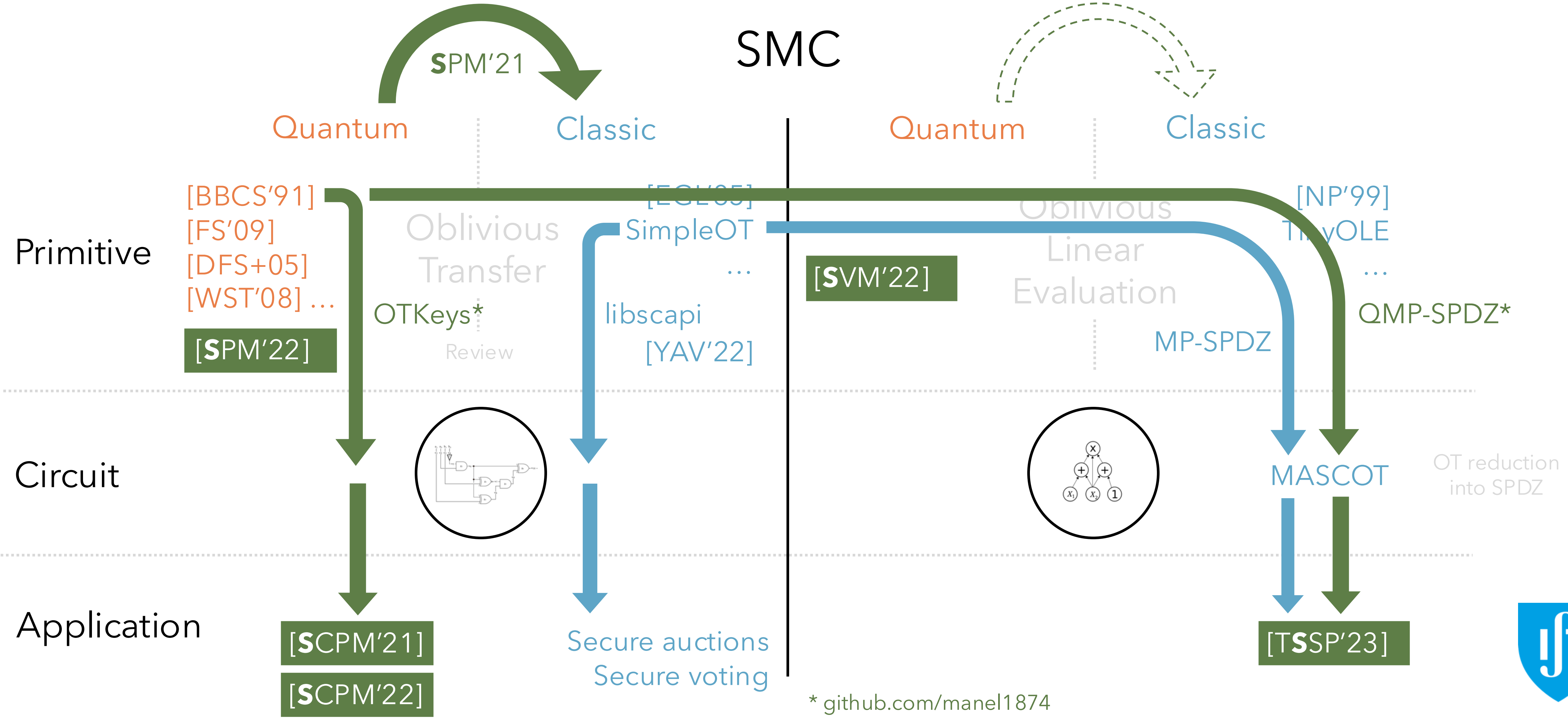
n OLE $\longrightarrow$ *1* OLE

Future work

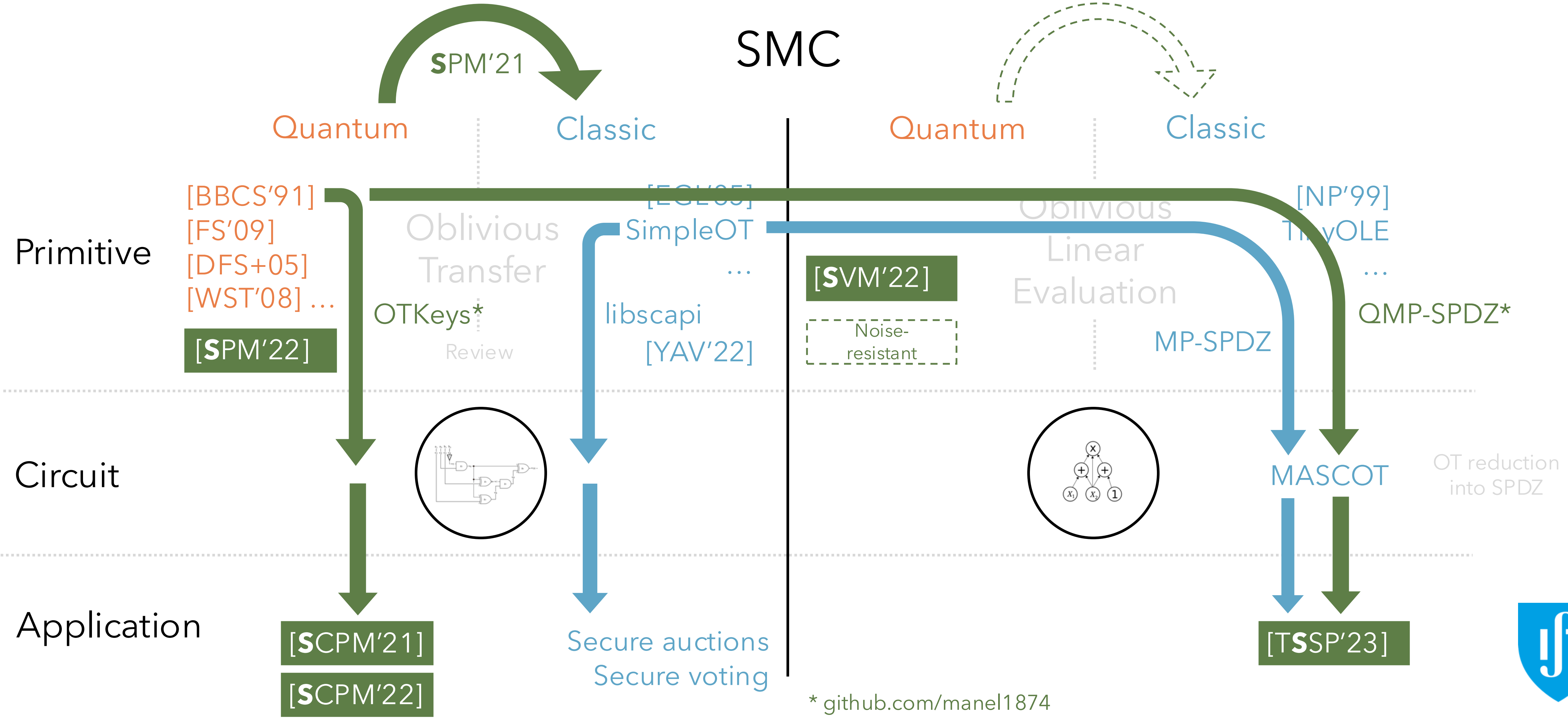


SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
[SVM'22]
Oblivious Linear Evaluation
[NP'99]
…
QMP-SPDZ*
MP-SPDZ
MASCOT
OT reduction into SPDZ
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
[TSSP'23]
* github.com/manel1874

Future work

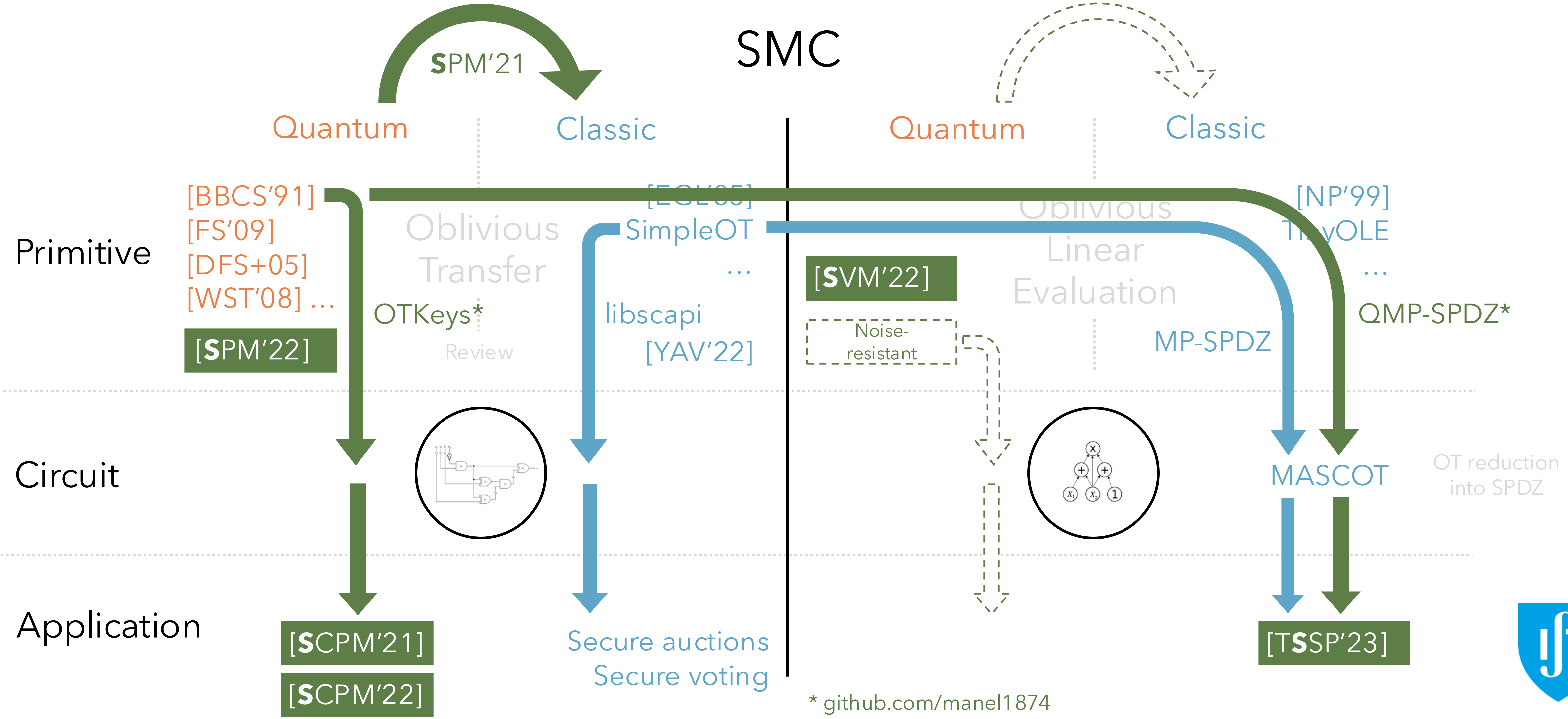

SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious
Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
[SVM'22]
Linear
Evaluation
[NP'99]
…
QMP-SPDZ*
MP-SPDZ
MASCOT
OT reduction
into SPDZ
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
[TSSP'23]
* github.com/manel1874

Future work



* github.com/manel1874

Future work


SMC
SPM'21
Quantum
Classic
Quantum
Classic
Primitive
Circuit
Application
[BBCS'91]
[FS'09]
[DFS+05]
[WST'08] …
[SPM'22]
Oblivious
Transfer
OTKeys*
Review
SimpleOT
…
libscapi
[YAV'22]
[SVM'22]
Noise-
resistant
Oblivious
Linear
Evaluation
[NP'99]
…
QMP-SPDZ*
MP-SPDZ
MASCOT
OT reduction
into SPDZ
[SCPM'21]
[SCPM'22]
Secure auctions
Secure voting
[TSSP'23]
* github.com/manel1874

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 defence

16 January 2025

TÉCNICO LISBOA