MITCH NEGUS
PhD Candidate
UC Berkeley, Dept. of Nuclear Engineering

NO DATA, NO PROBLEM

Giving nuclear inspectors better tools without revealing state secrets

ENIGMA

View these slides online at www.mitchnegus.com/enigma2021

SAND2021-0391 C

The following content includes static images of terrorism that some may find distressing.

Viewer discretion is advised.

Nuclear inspectors prevent material from being diverted to weapons purposes.

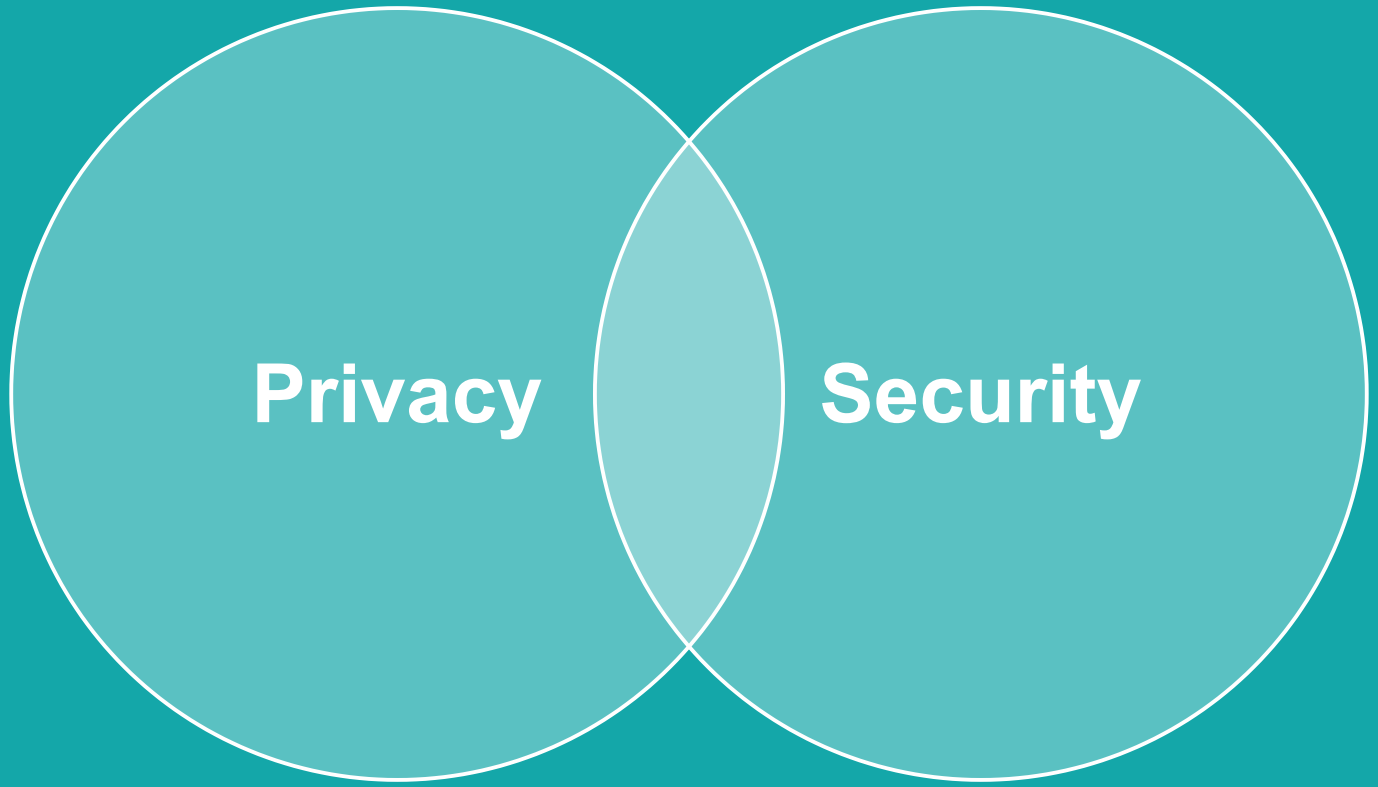

IAEA

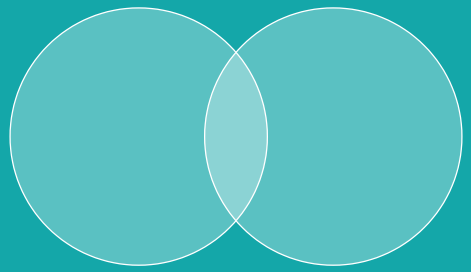
The Treaty on the Non-Proliferation of Nuclear Weapons

Privacy

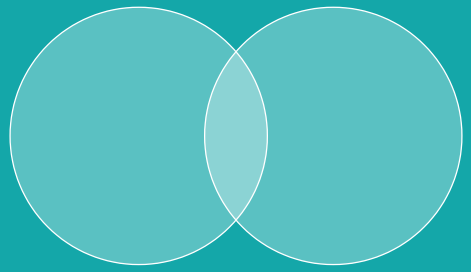
Privacy

Security


Privacy
Security



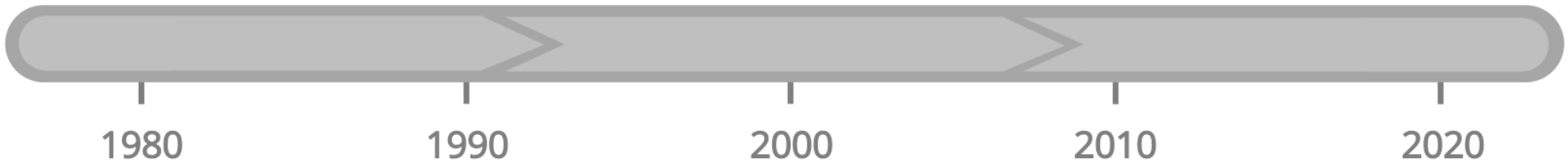
Secure Multiparty Computation



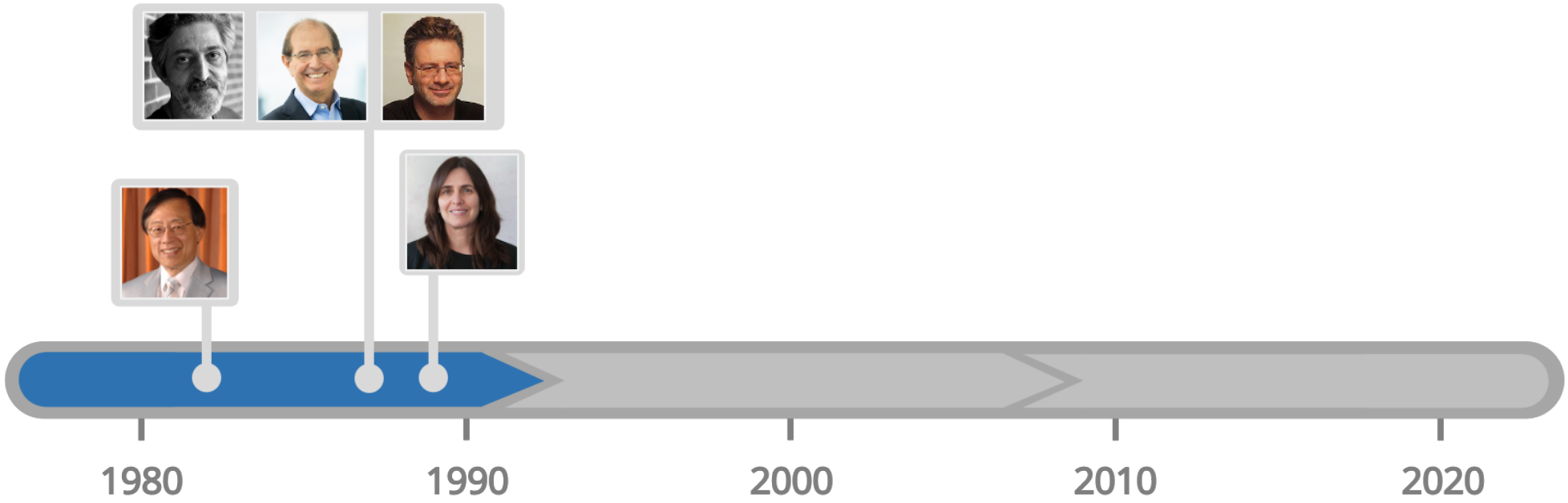
Secure Multiparty Computation

MPC

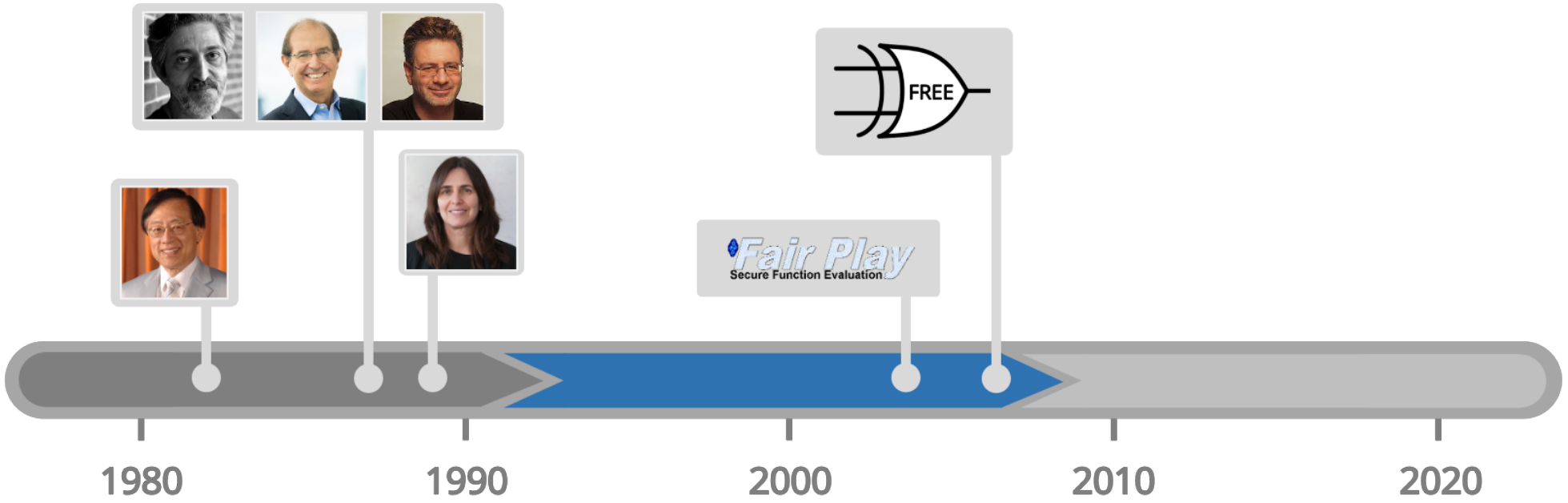
A Brief History of MPC



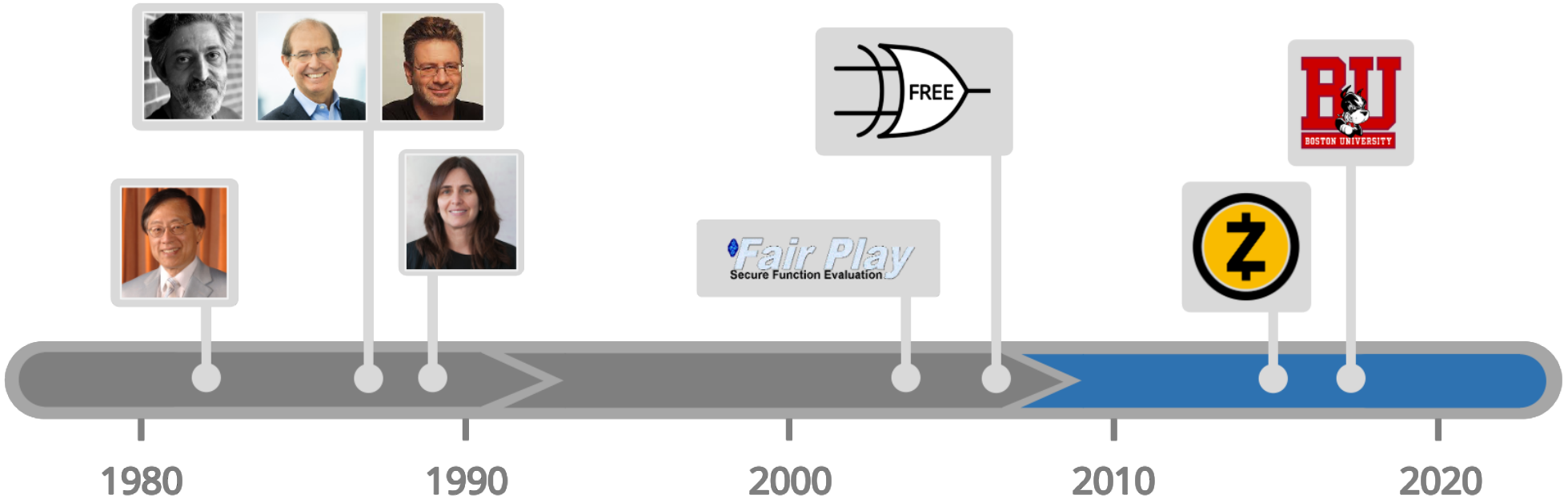
A Brief History of MPC



A Brief History of MPC



A Brief History of MPC



What can we **DO**?

What can we **DO**?

What types of **DATA**?

What can we **DO**?

What types of **DATA**?

Why hasn't it been **DEPLOYED**?

What can we **DO**?

What types of **DATA**?

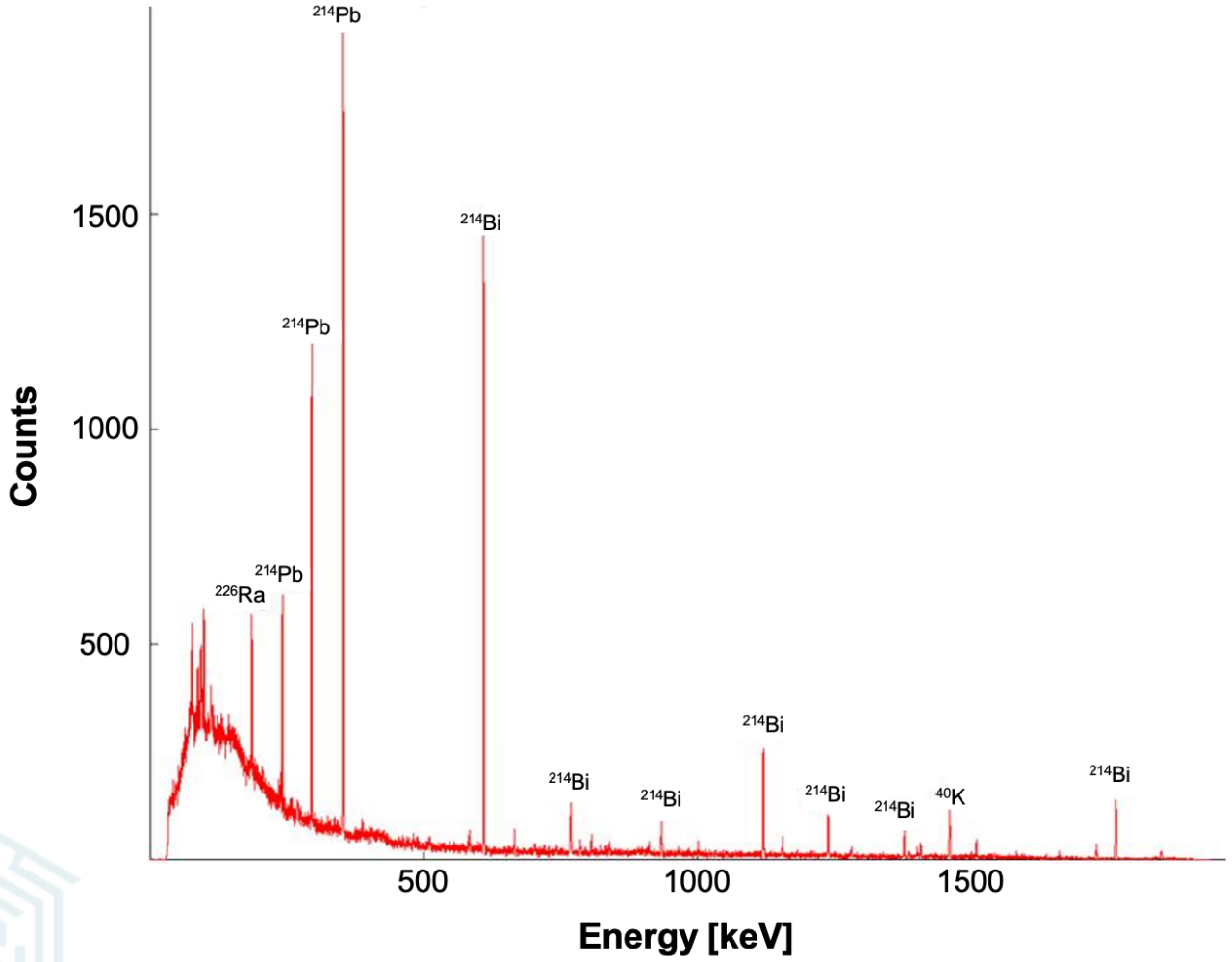
Why hasn't it been **DEPLOYED**?

What can we **DO**?

What types of **DATA**?

Why hasn't it been **DEPLOYED**?

Radiation Spectra



keV: kiloelectronvolts

What can we **DO**?

What types of **DATA**?

Why hasn't it been **DEPLOYED**?

What can we **DO**?

What types of **DATA**?

Why hasn't it been **DEPLOYED**?

MPC isn't yet used in safeguards today, due in part to:

MPC isn't yet used in safeguards today, due in part to:

MPC isn't yet used in safeguards today, due in part to:

Technical requirements

Viable MPC is a relatively new development.

MPC isn't yet used in safeguards today, due in part to:

Technical requirements

Viable MPC is a relatively new development.

Risk-averse inspectorate

Technologies must be rigorously proven, limiting reliance on the cutting edge.

MPC isn't yet used in safeguards today, due in part to:

Technical requirements

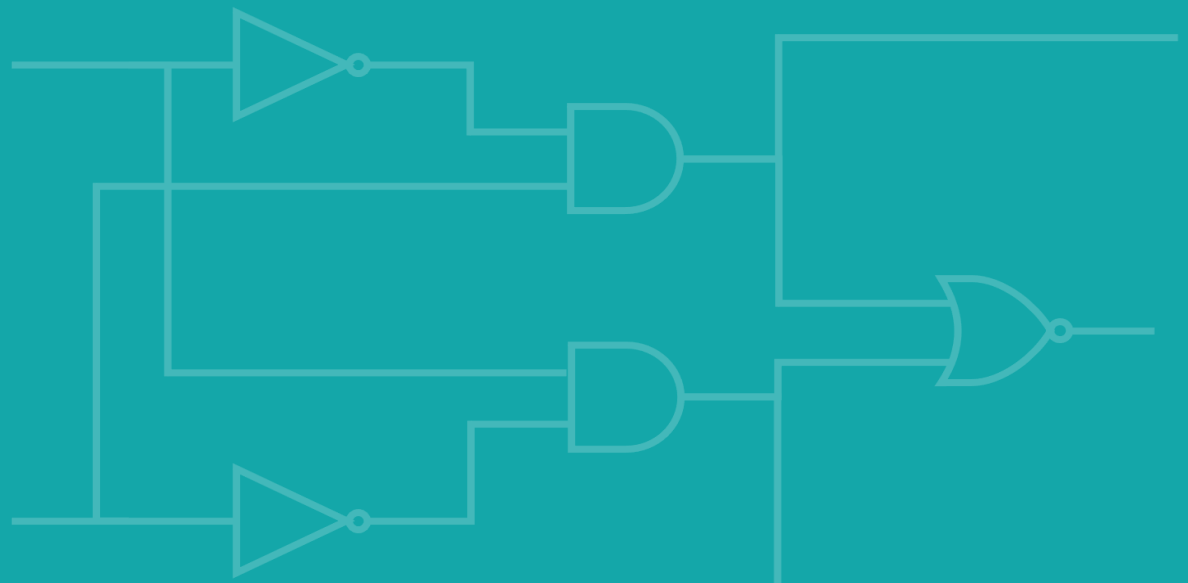
Viable MPC is a relatively new development.

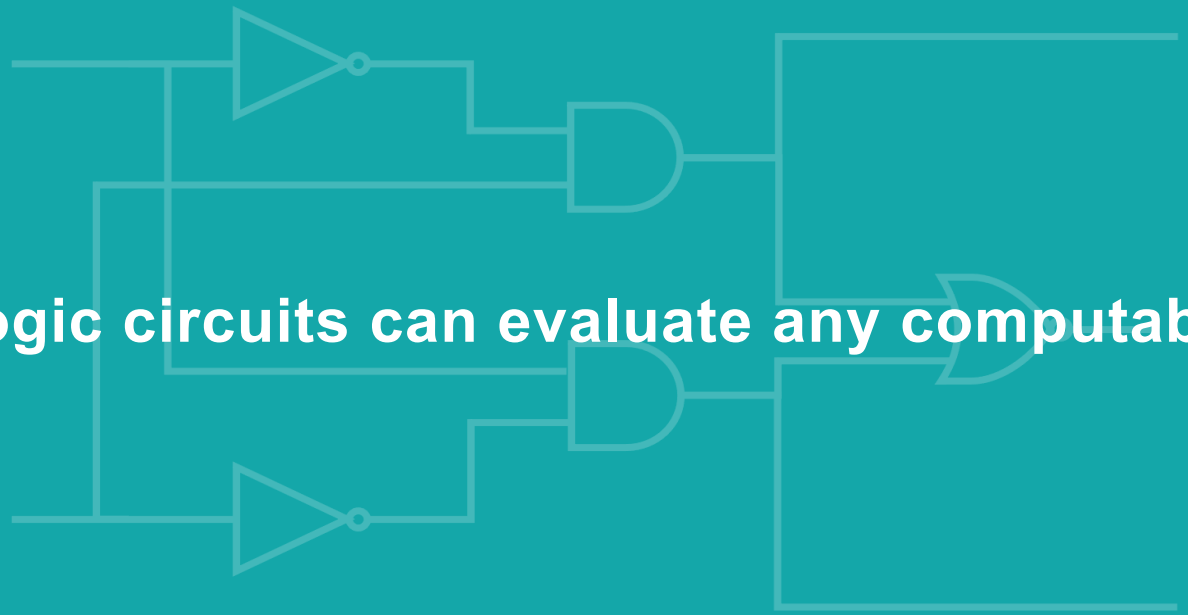
Risk-averse inspectorate

Technologies must be rigorously proven, limiting reliance on the cutting edge.

Limited pool of expertise

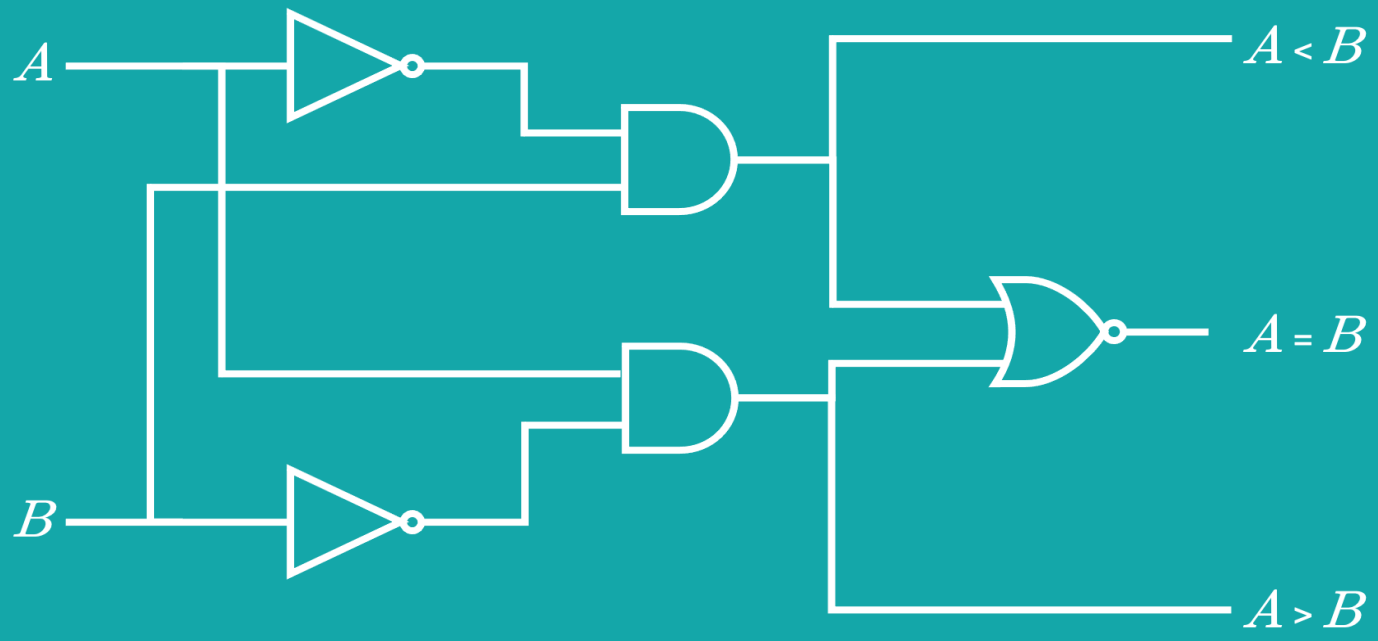
Primary focus is on nuclear technology, so overlap with advanced cryptography is thin.



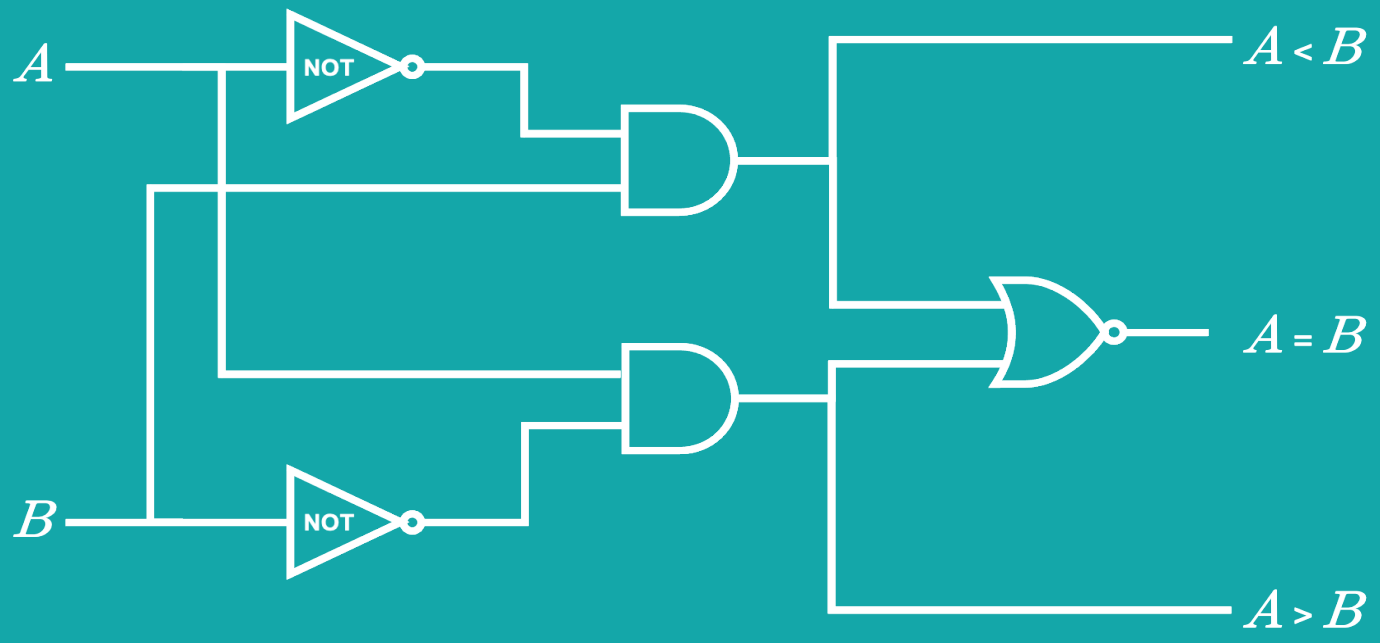


Digital logic circuits can evaluate any computable function.

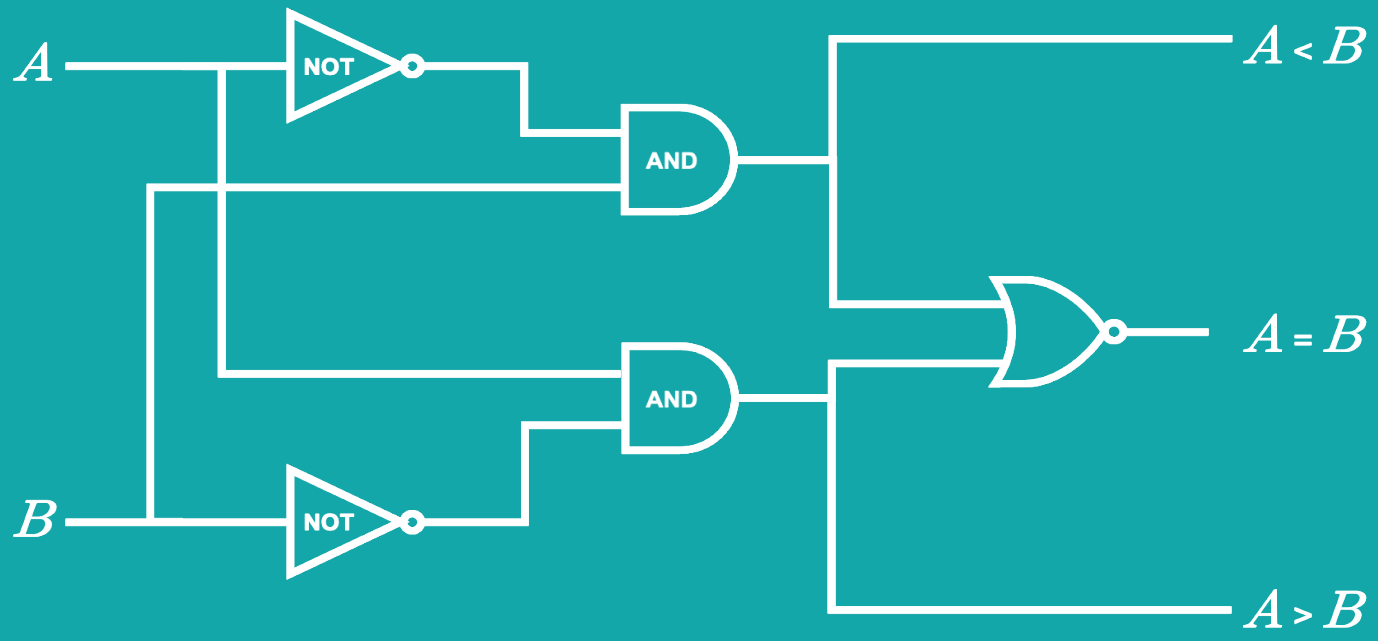
$$A \stackrel{?}{=} B$$



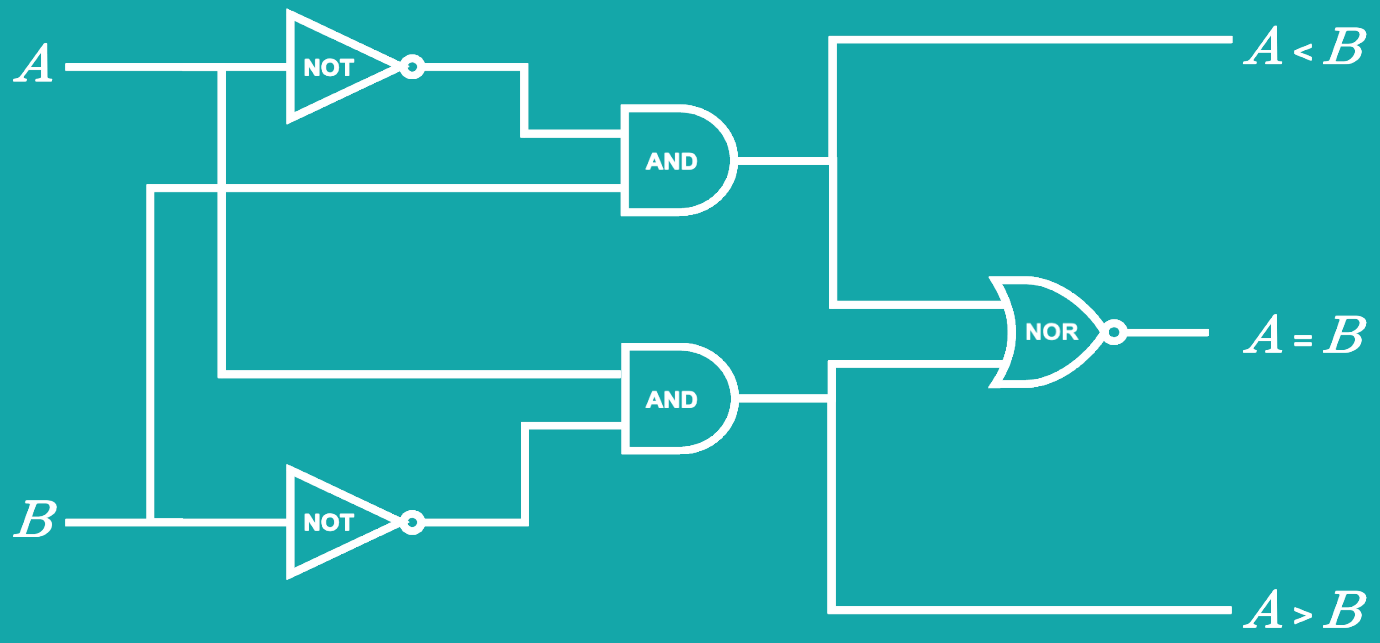
$$A \stackrel{?}{=} B$$



$$A \stackrel{?}{=} B$$



$$A \stackrel{?}{=} B$$



2 Parties

2 Parties

1. Facility: F

2 Parties

1. Facility: F

2. IAEA: I

2 Parties

1. Facility: F

2. IAEA: I

$$F \stackrel{?}{=} I$$

2 Parties $\times$ 2 Inputs

F

I

$F \stackrel{?}{=} I$

2 Parties $\times$ 2 Inputs

$$F = F_1 F_0$$

$$I = I_1 I_0$$

$$F \stackrel{?}{=} I$$

2 Parties $\times$ 2 Inputs

$$F = F_1 F_0$$

$$I = I_1 I_0$$

$$\left\{ \right.$$

$$F \overset{?}{=} I$$

2 Parties $\times$ 2 Inputs

$0 = 00_2$

$$F = F_1 F_0$$

$$I = I_1 I_0$$

$$F \stackrel{?}{=} I$$

2 Parties $\times$ 2 Inputs

$0 = 00_2$

$F = F_1 F_0$

$1 = 01_2$

$I = I_1 I_0$

$\{$

$F \overset{?}{=} I$

2 Parties $\times$ 2 Inputs

$$F = F_1 F_0$$

$$I = I_1 I_0$$

$$F \stackrel{?}{=} I$$

$$\begin{cases} 0 = 00_2 \\ 1 = 01_2 \\ 2 = 10_2 \end{cases}$$

2 Parties $\times$ 2 Inputs

$$0 = 00_2$$

$$F = F_1 F_0$$

$$1 = 01_2$$

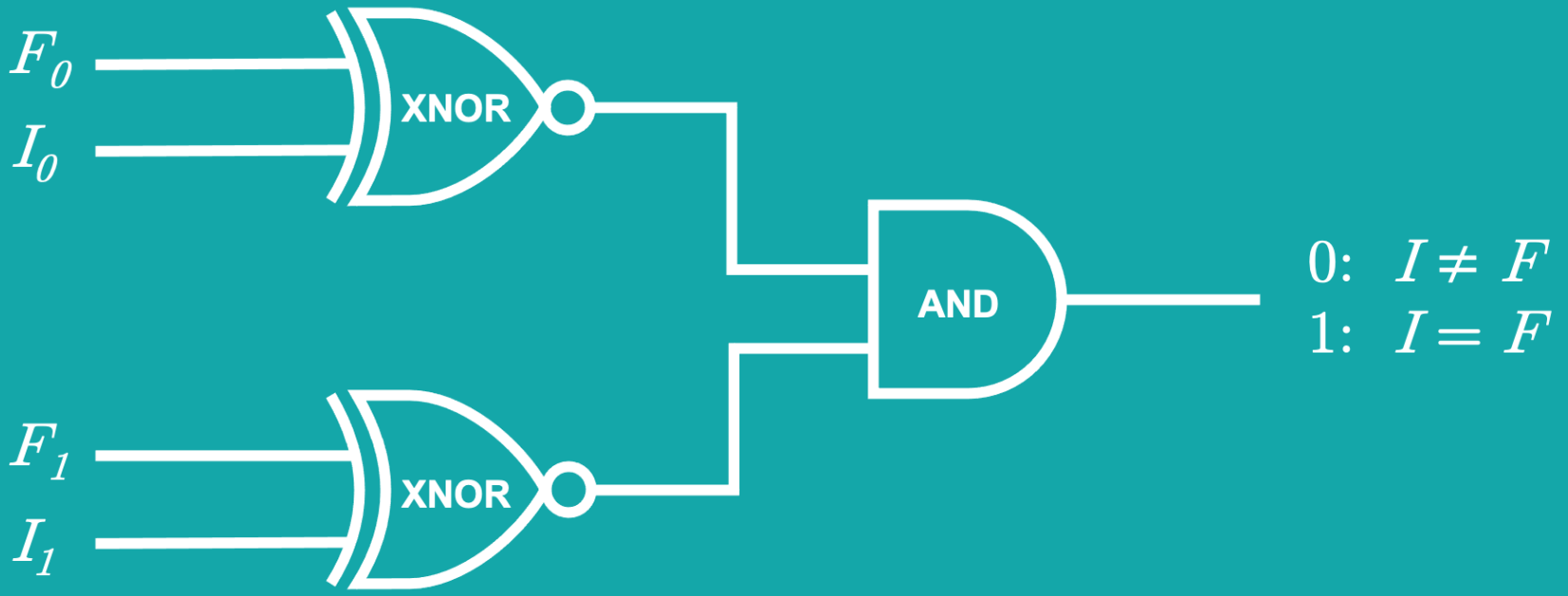
$$I = I_1 I_0$$

$$\begin{cases} 2 = 10_2 \\ 3 = 11_2 \end{cases}$$

$$F \stackrel{?}{=} I$$

$F = F_1 F_0$

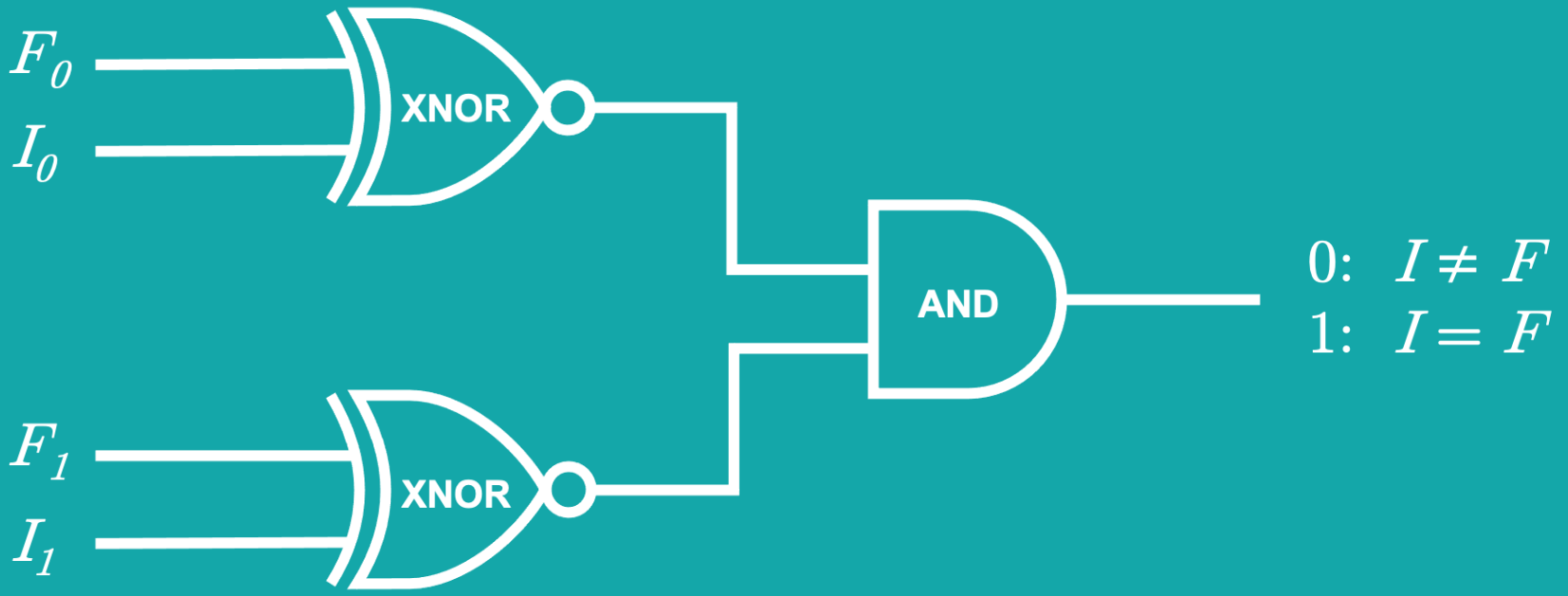
$I = I_1 I_0$



F_0	I_0	X_0
0	0	1
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

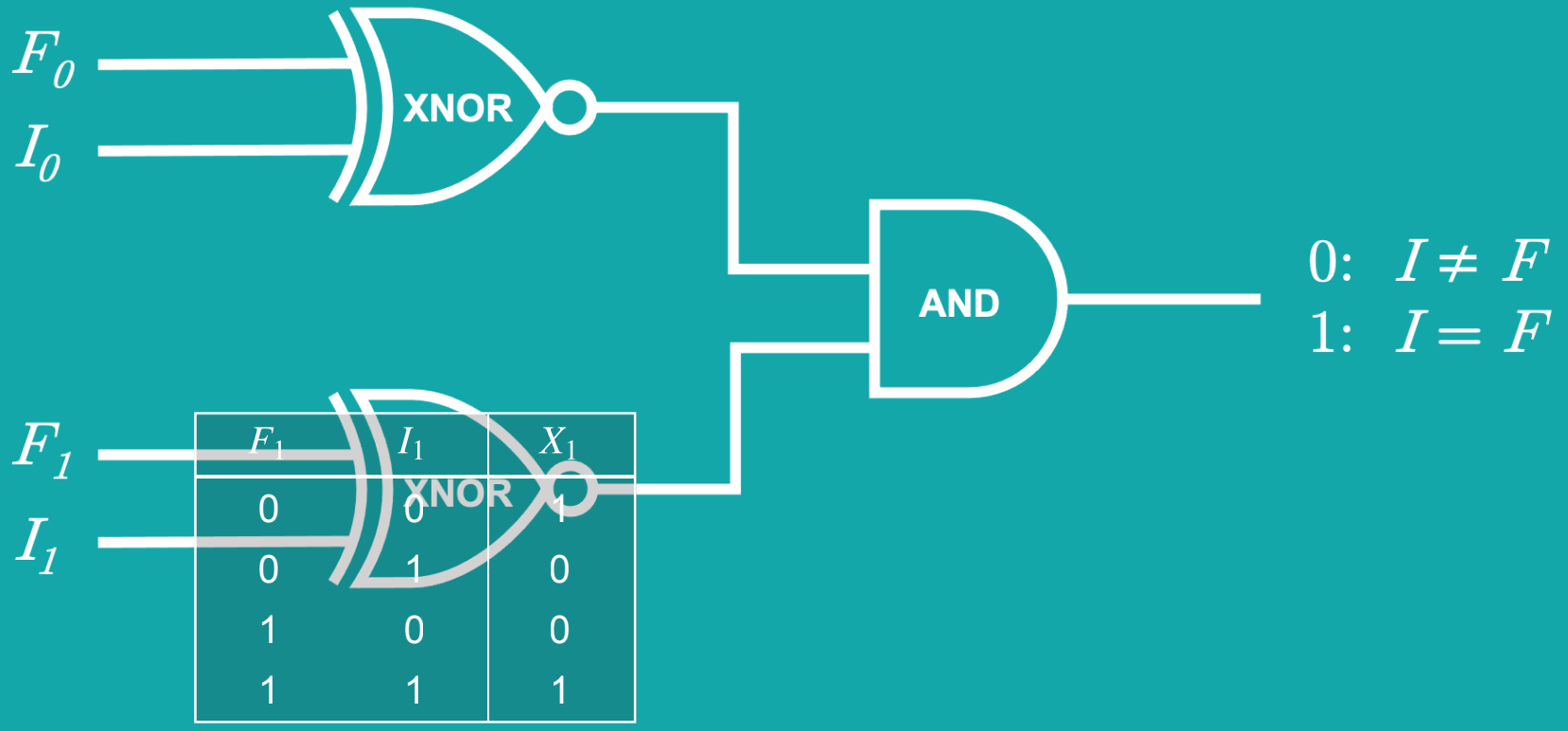
$$I = I_1 I_0$$



F_0	I_0	X_0
0	0	1
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



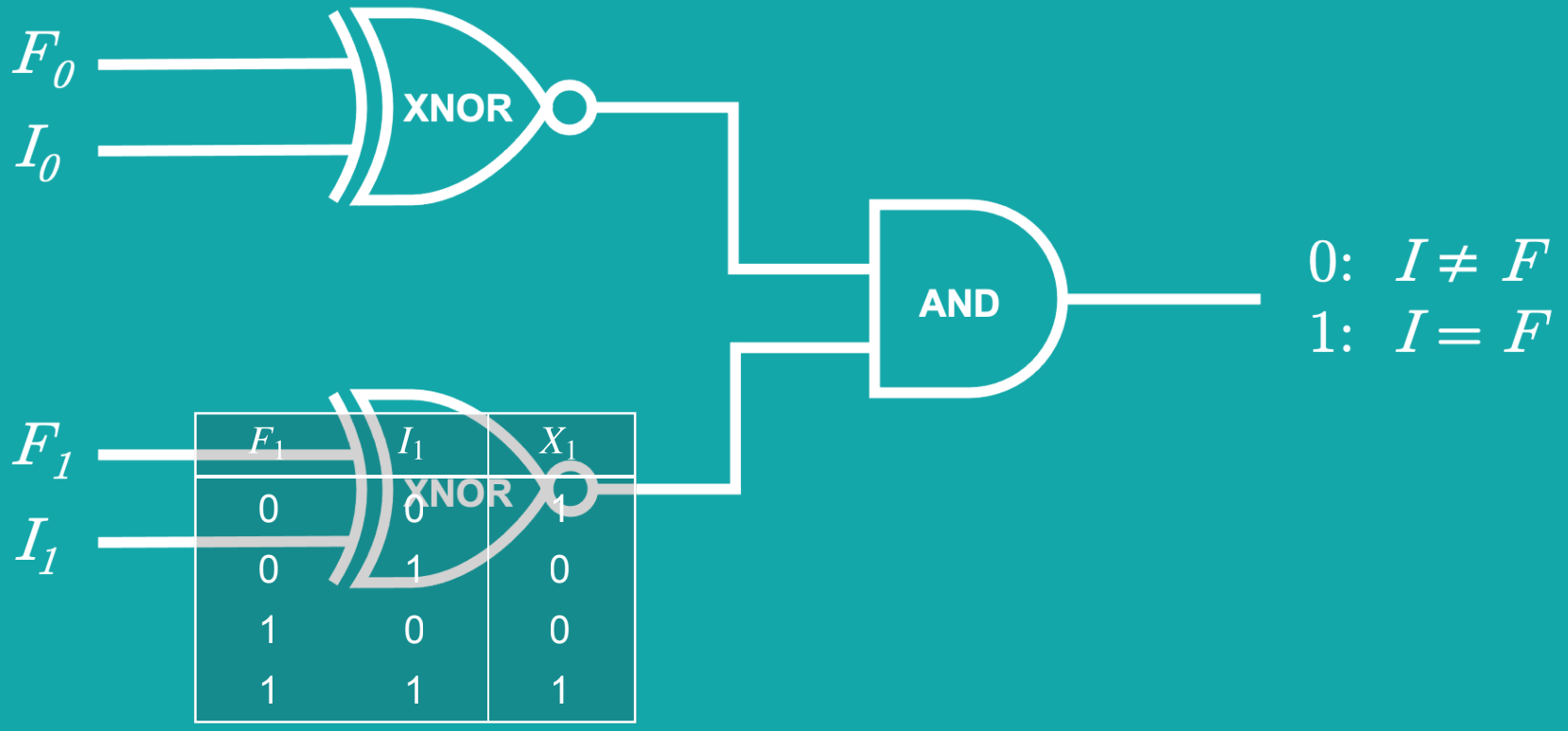
F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

F_0	I_0	X_0
0	0	1
0	1	0
1	0	0
1	1	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

0: $I \neq F$

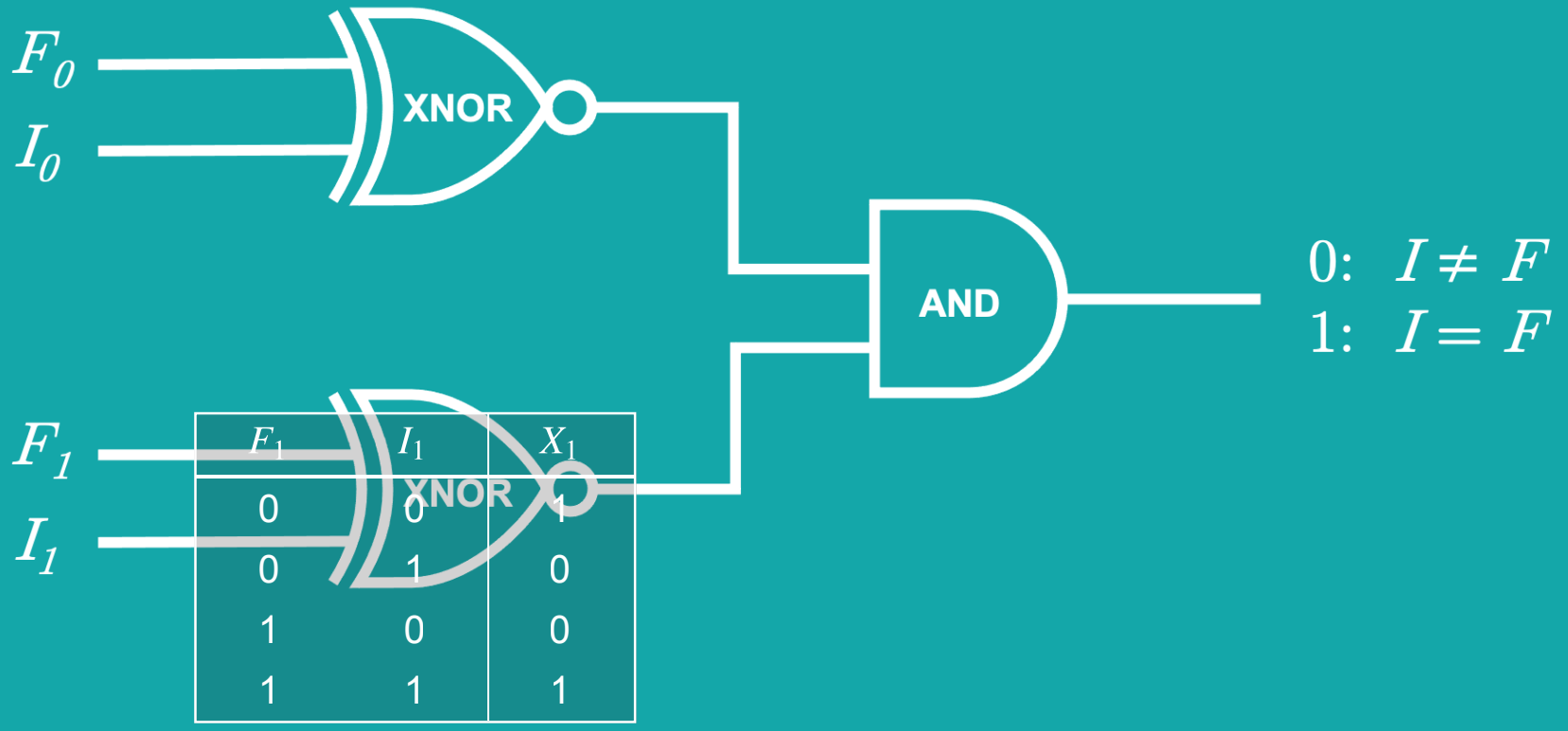
1: $I = F$

F_0	I_0	X_0
0	0	1
0	1	0
1	0	0
1	1	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



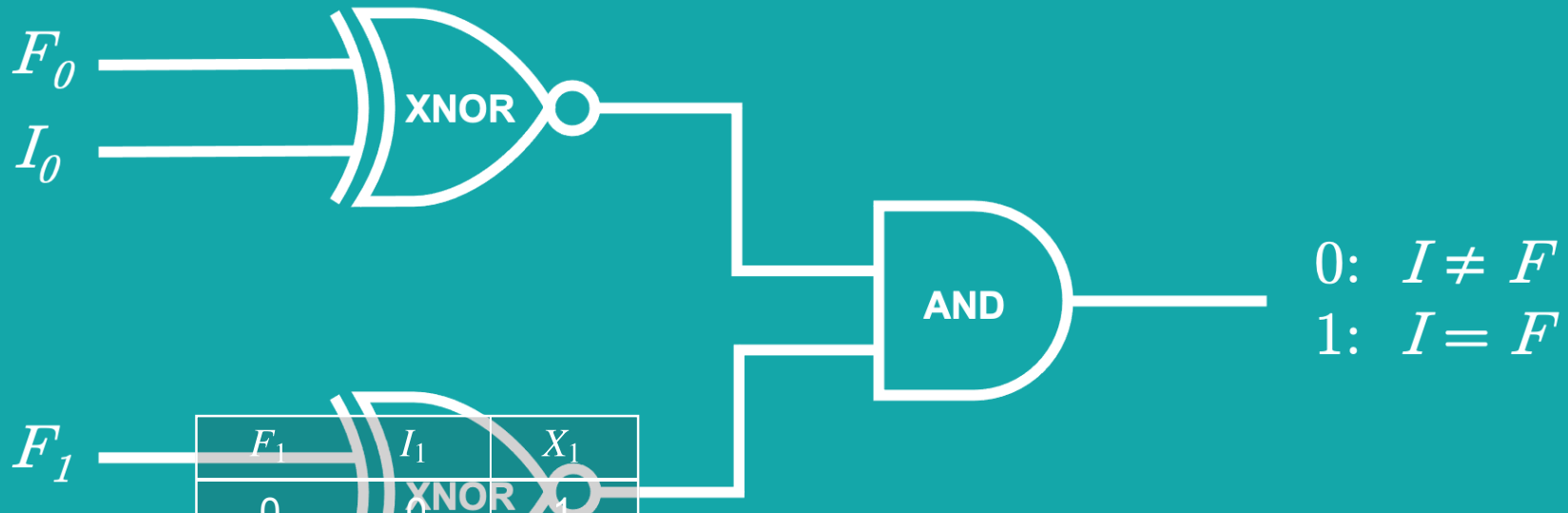
F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

F_0	I_0	X_0
6fd0	0	1
6fd0	1	0
1	0	0
1	1	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \; I \neq F$

$1: \; I = F$

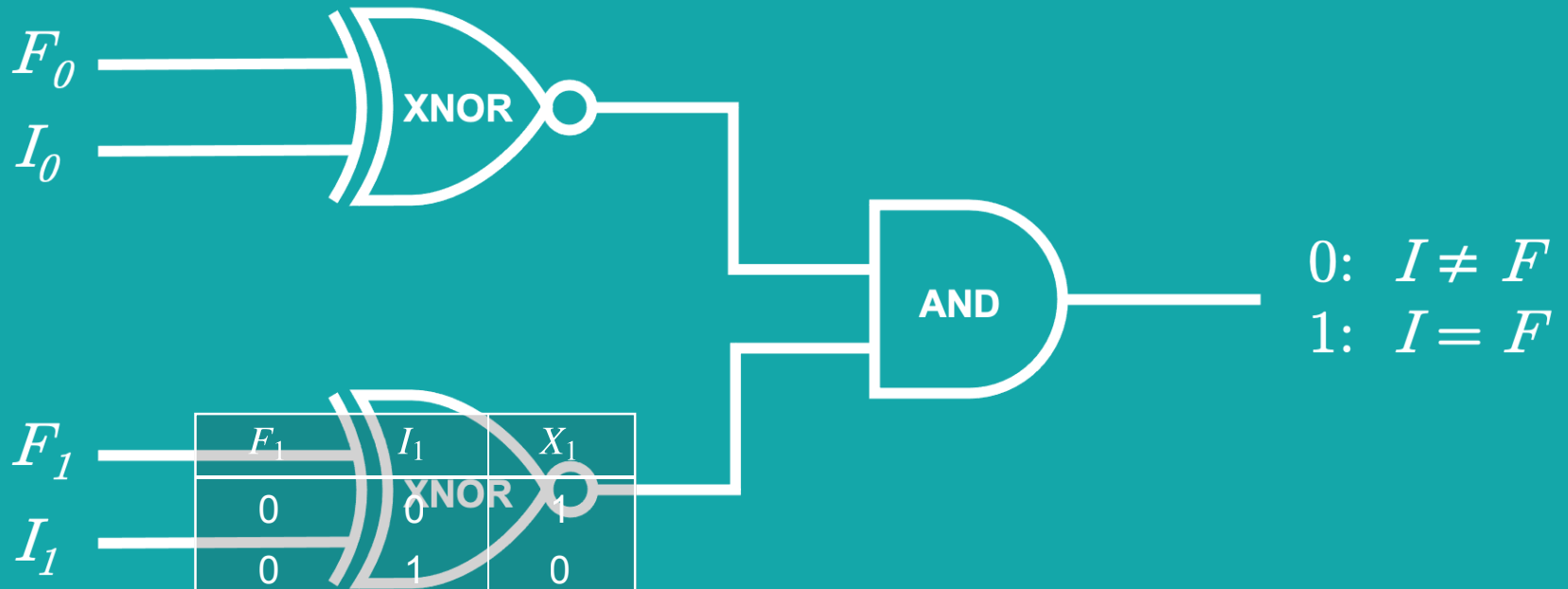
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	0	1
6fd0	1	0
131b	0	0
131b	1	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \; I \neq F$

$1: \; I = F$

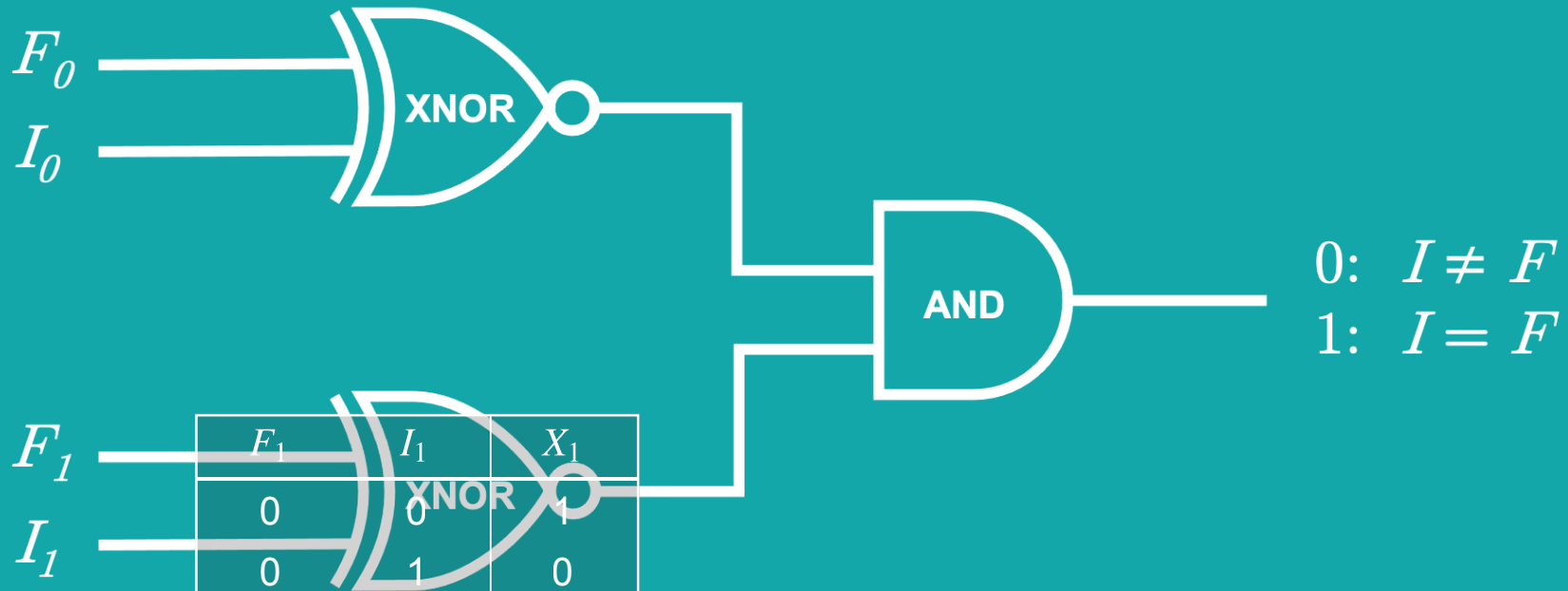
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	1
6fd0	1	0
131b	32f1	0
131b	1	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \ I \neq F$

$1: \ I = F$

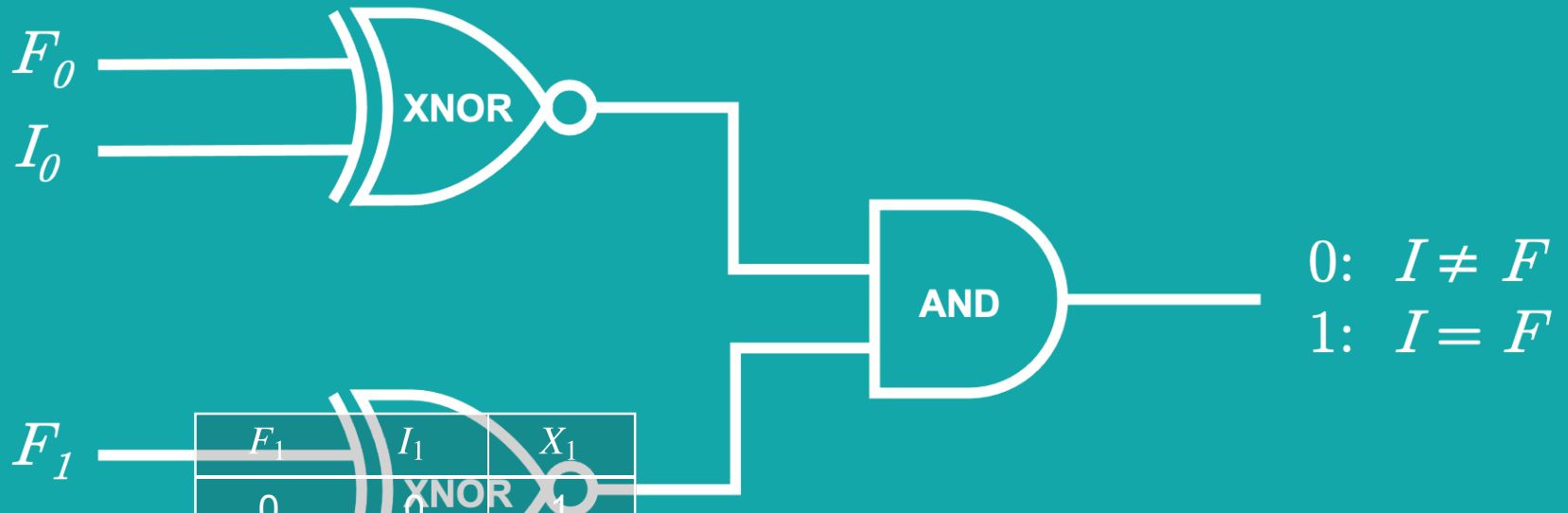
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	1
6fd0	c4d4	0
131b	32f1	0
131b	c4d4	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \ I \neq F$

$1: \ I = F$

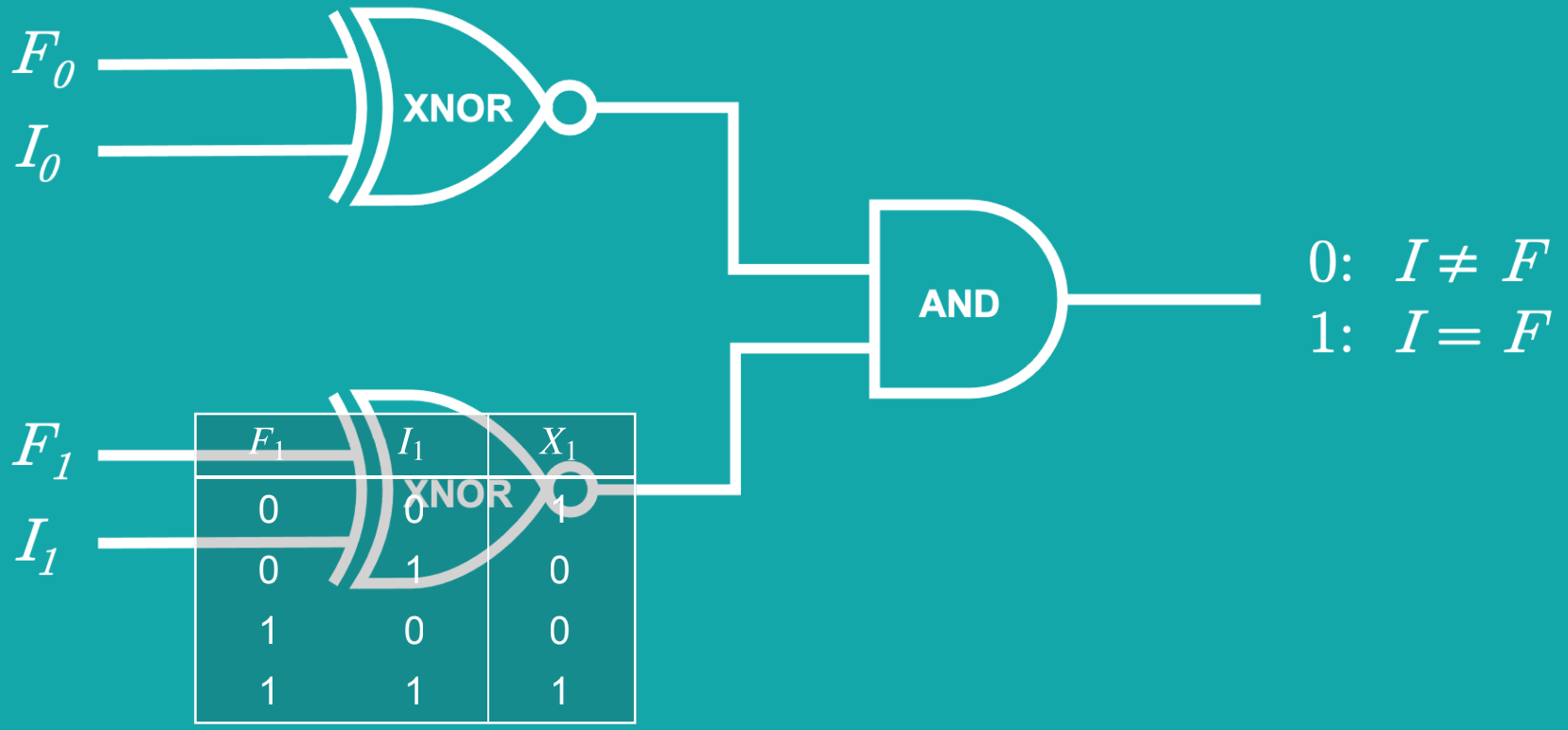
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	1
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	1

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

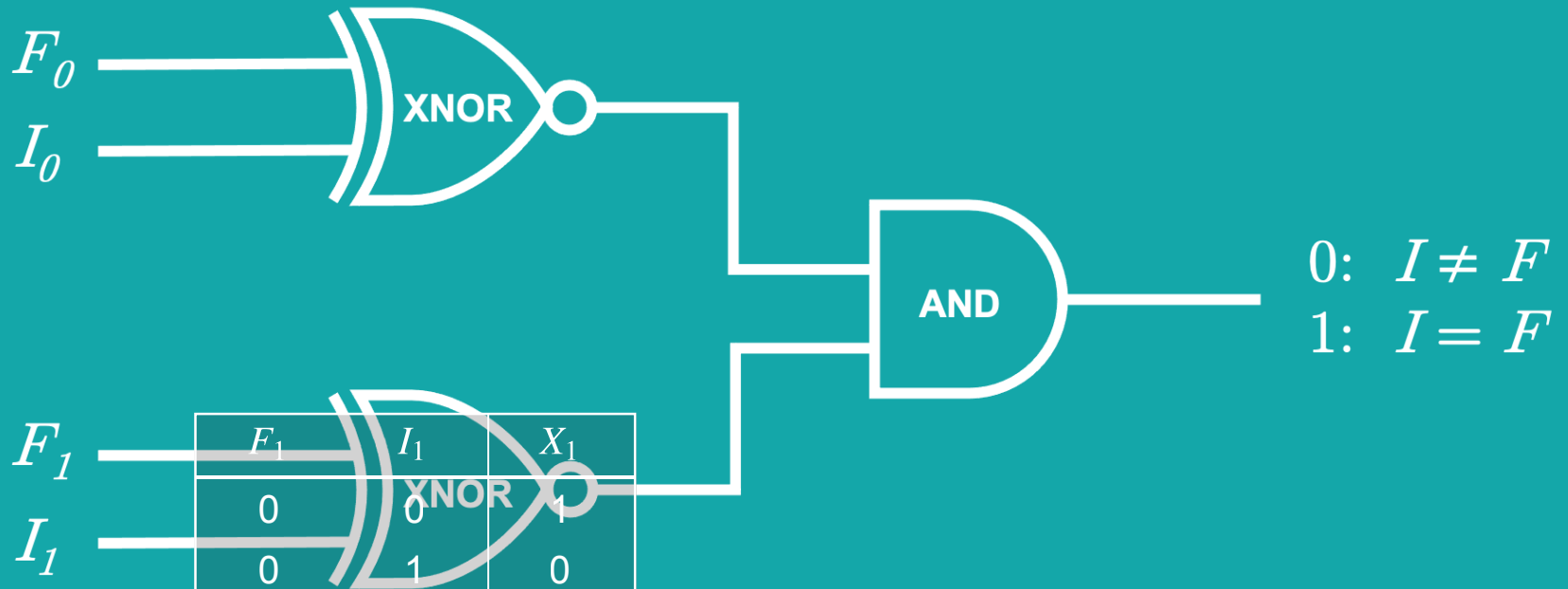
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \ I \neq F$

$1: \ I = F$

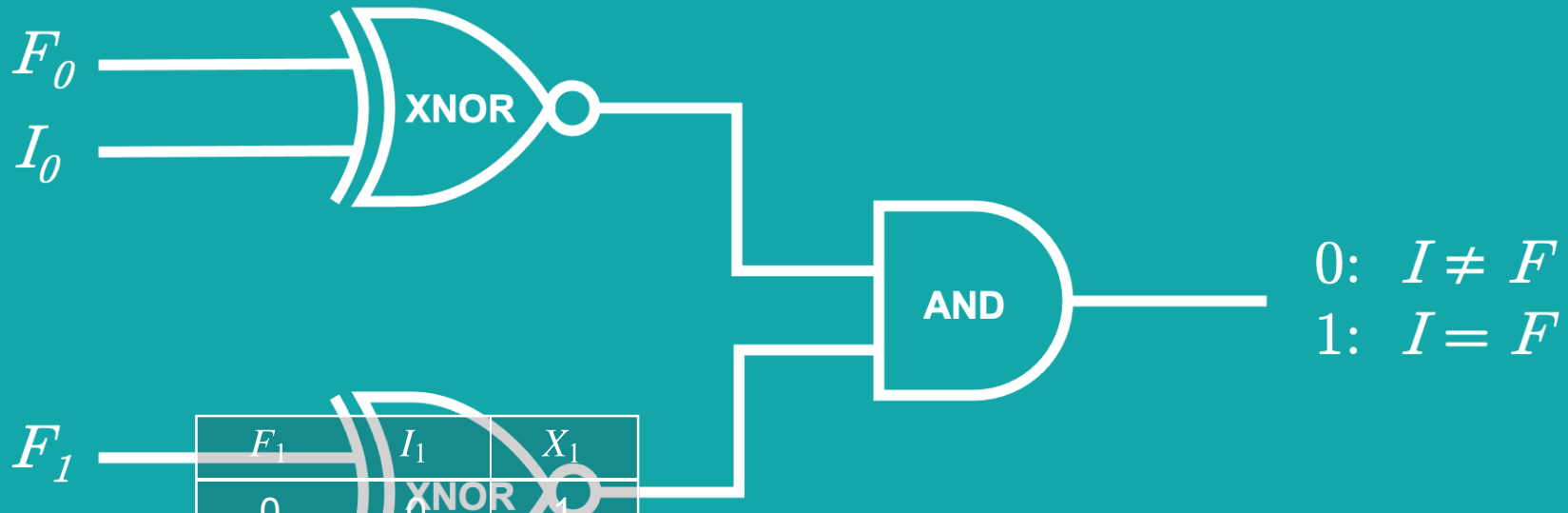
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \; I \neq F$

$1: \; I = F$

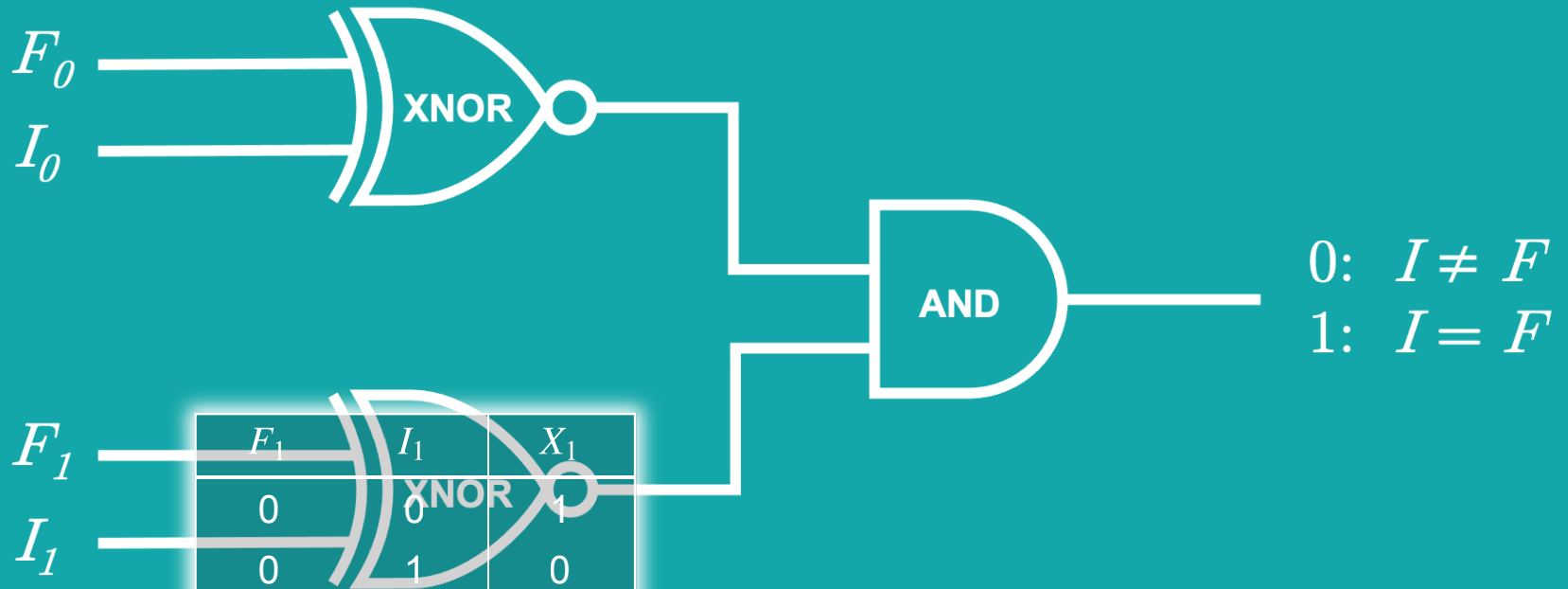
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
0	0	1
0	1	0
1	0	0
1	1	1

$0: \ I \neq F$

$1: \ I = F$

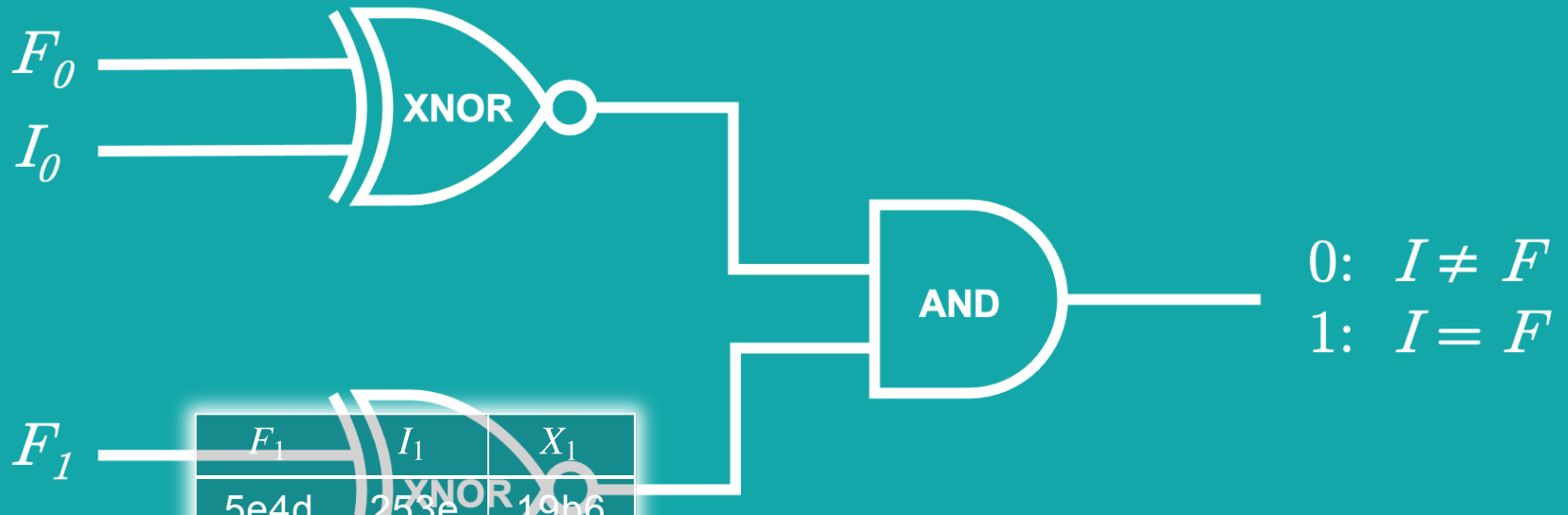
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

$0: \ I \neq F$

$1: \ I = F$

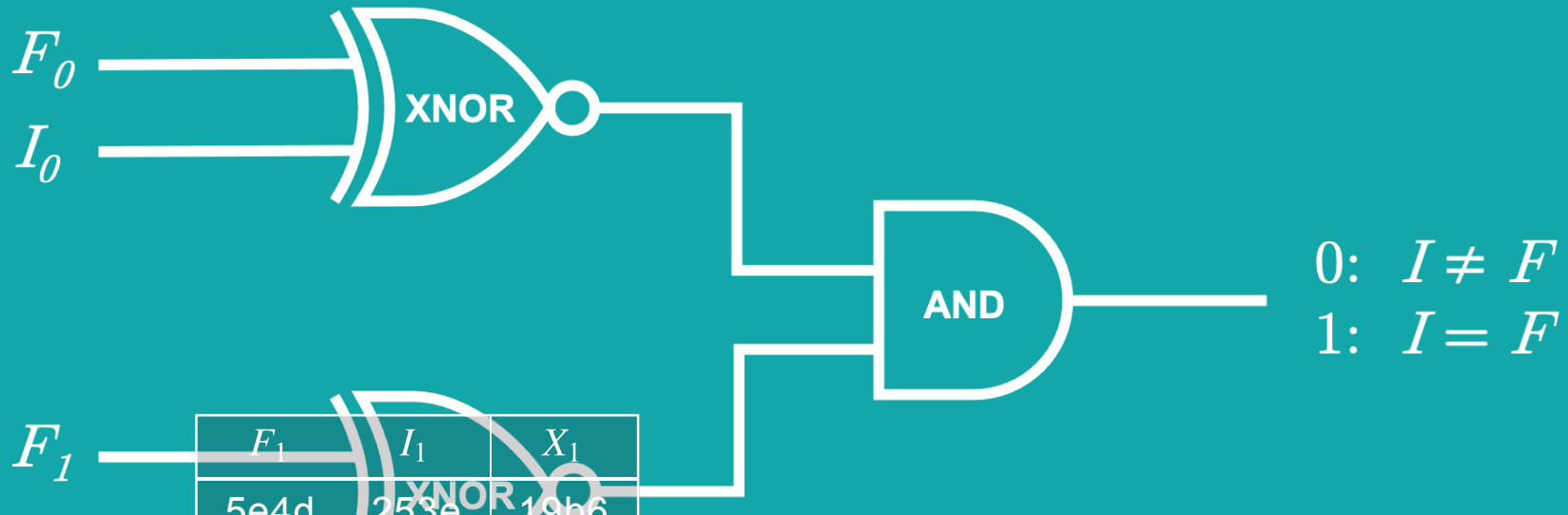
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

0: $I \neq F$

1: $I = F$

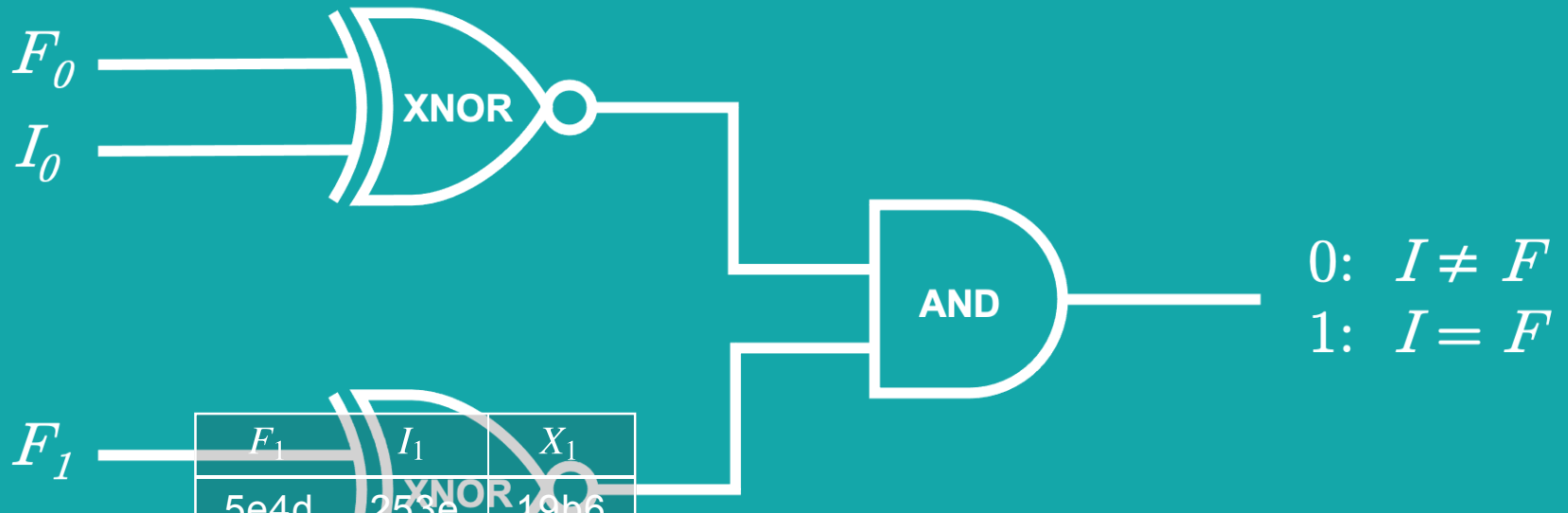
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
0	0	0
0	1	0
1	0	0
1	1	1

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

0: $I \neq F$

1: $I = F$

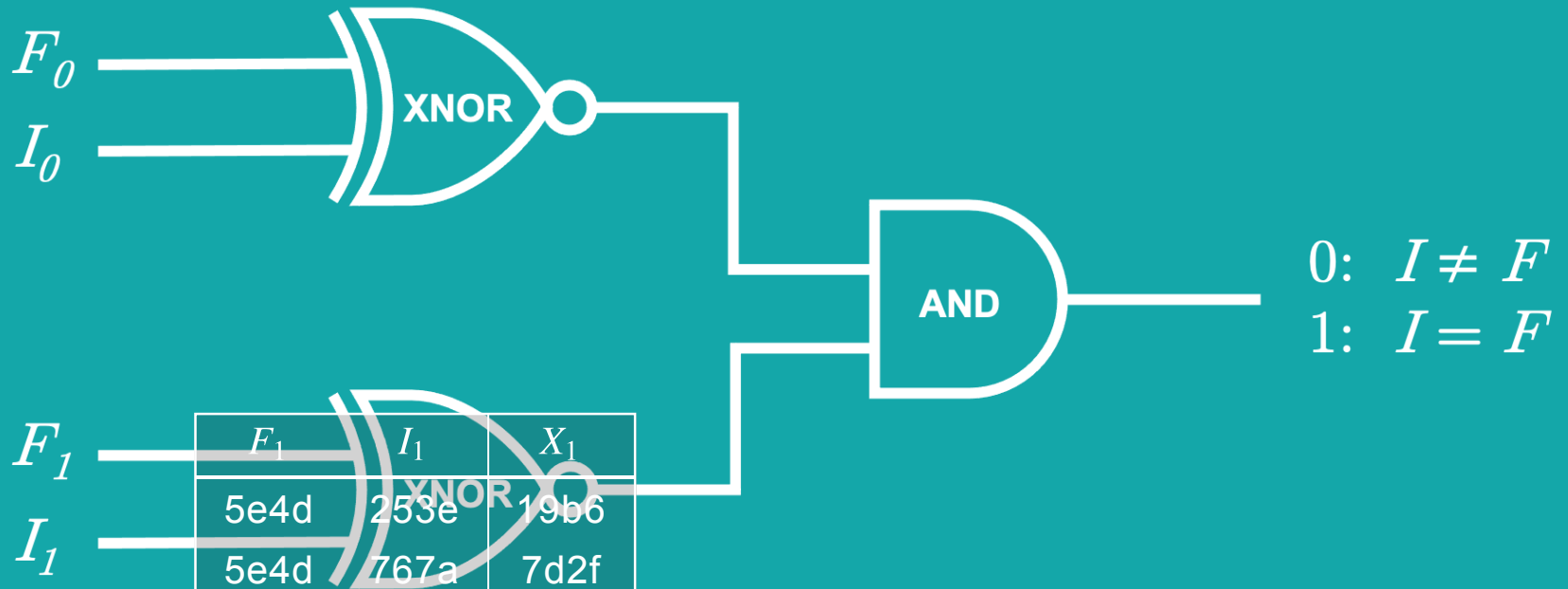
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

0: $I \neq F$

1: $I = F$

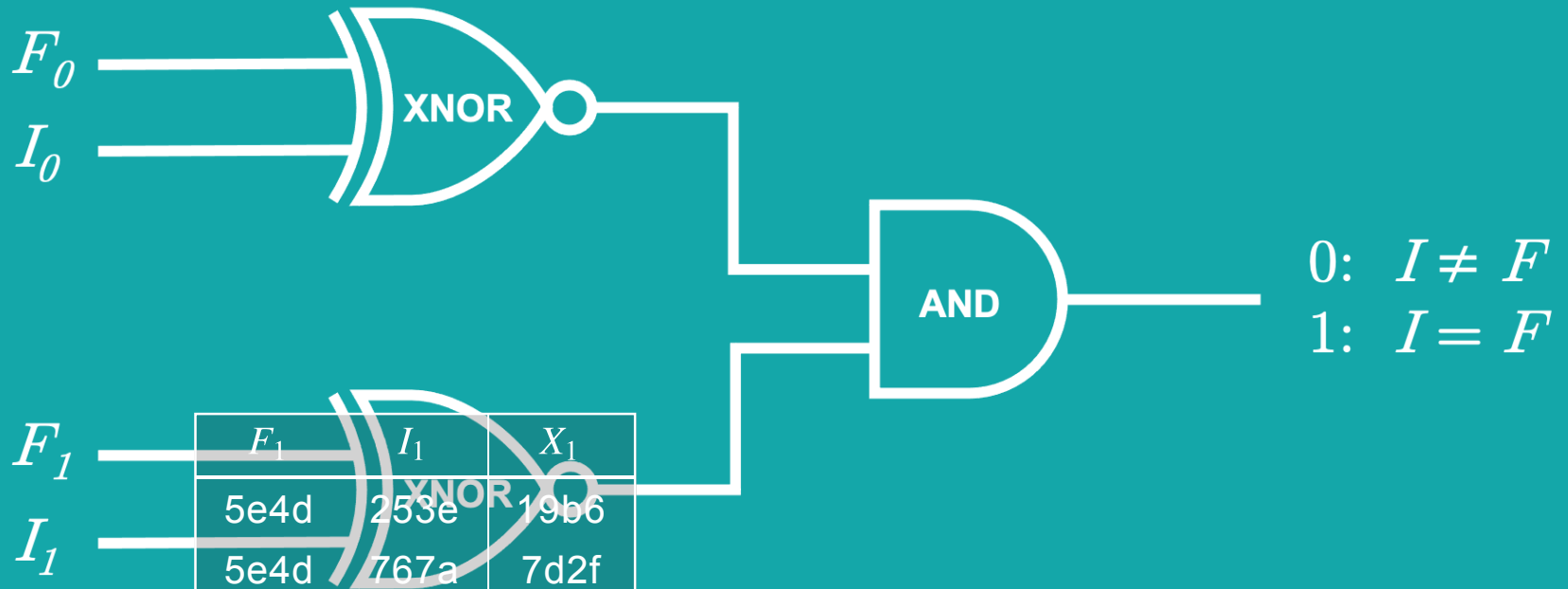
FACILITY'S VIEWPOINT

F_0	I_0	X_0
6fd0	32f1	ed56
6fd0	c4d4	bd67
131b	32f1	bd67
131b	c4d4	ed56

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

0: $I \neq F$

1: $I = F$

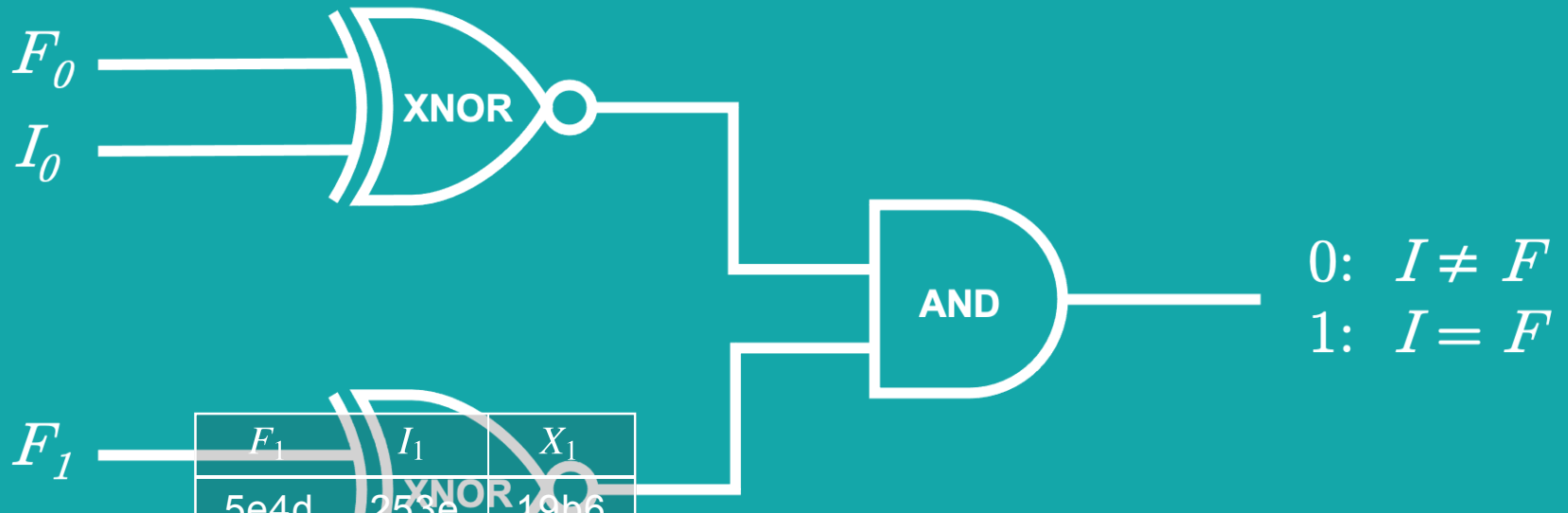
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
6fd0	32f1	ed56	
6fd0	c4d4	bd67	
131b	32f1	bd67	
131b	c4d4	ed56	

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$

$$I = I_1I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

$0: \ I \neq F$

$1: \ I = F$

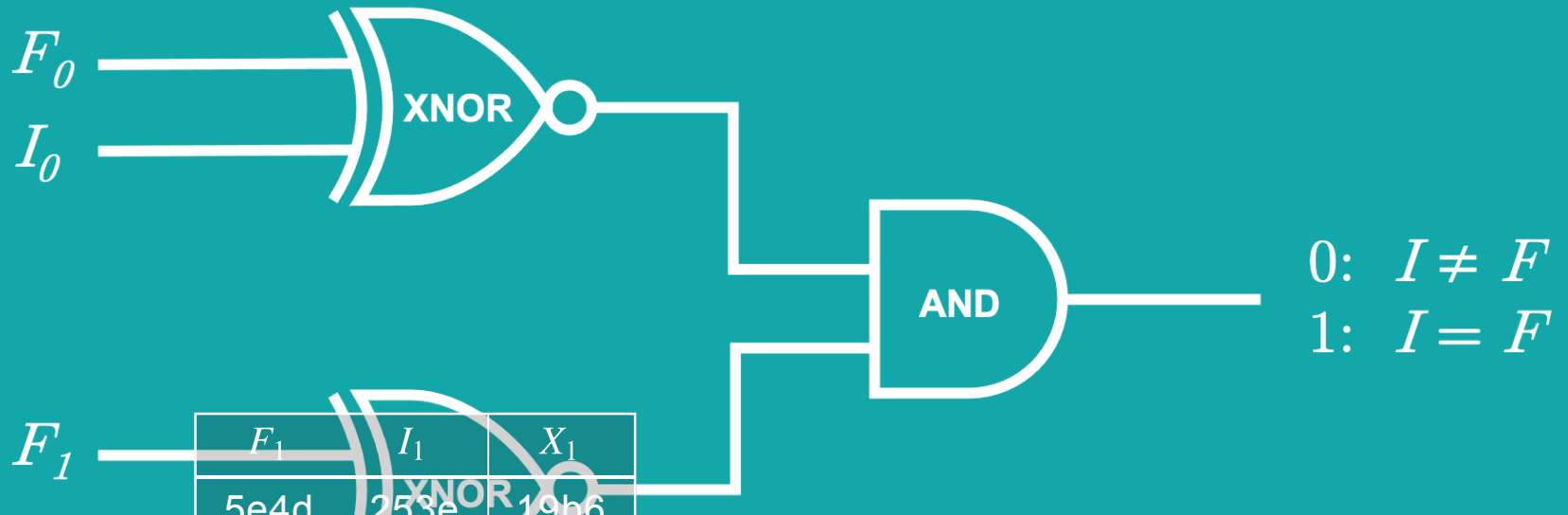
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
6fd0	c4d4	bd67	
131b	32f1	bd67	
131b	c4d4	ed56	

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$

$$I = I_1I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

$$0: \ I \neq F$$

$$1: \ I = F$$

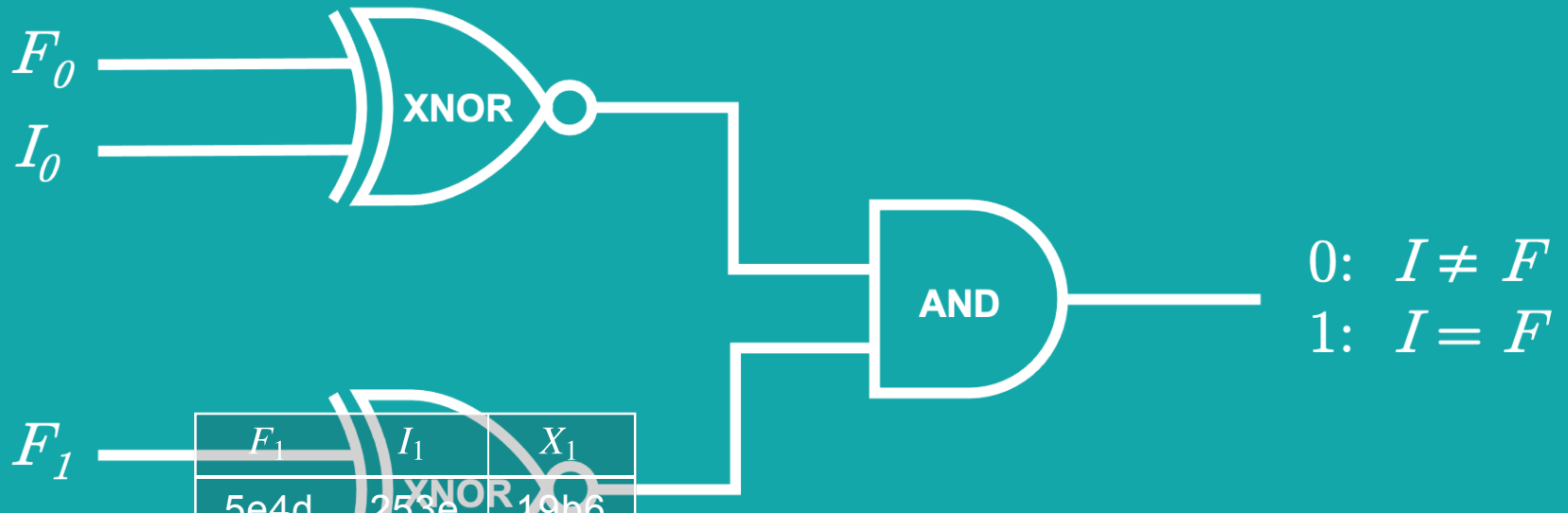
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
131b	32f1	bd67	
131b	c4d4	ed56	

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$

$$I = I_1I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

$$0: \ I \neq F$$

$$1: \ I = F$$

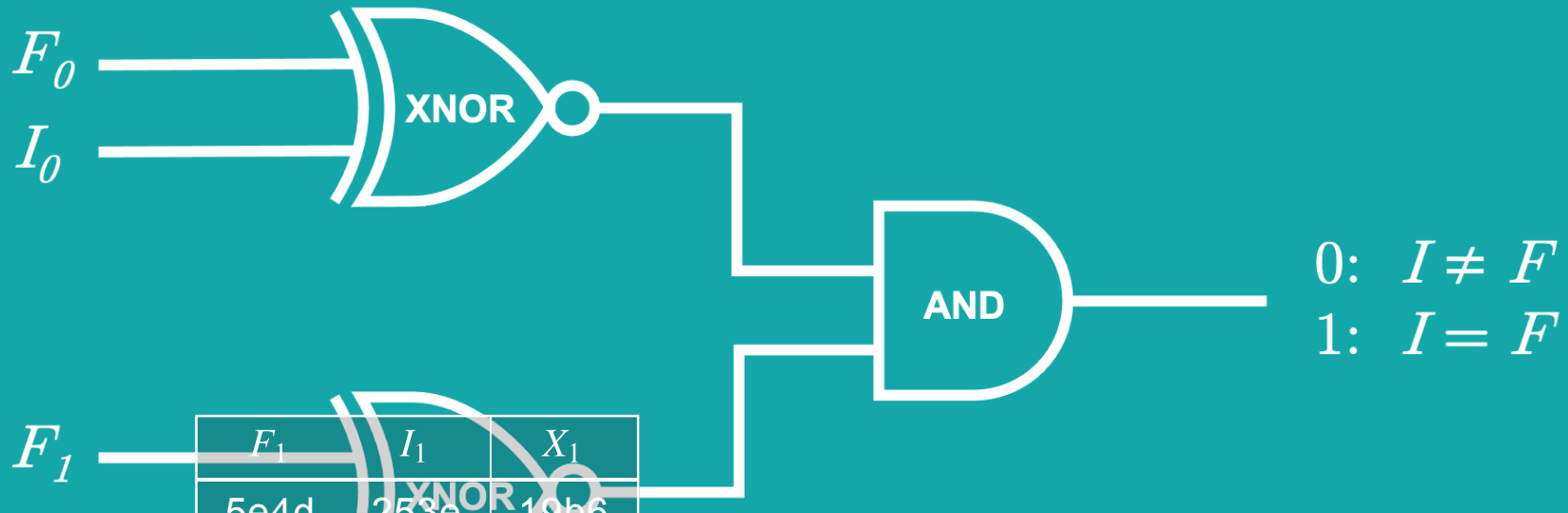
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
🔑	🔑	••••	c2bf
131b	c4d4	ed56	

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$

$$I = I_1I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

$$0: \ I \neq F$$

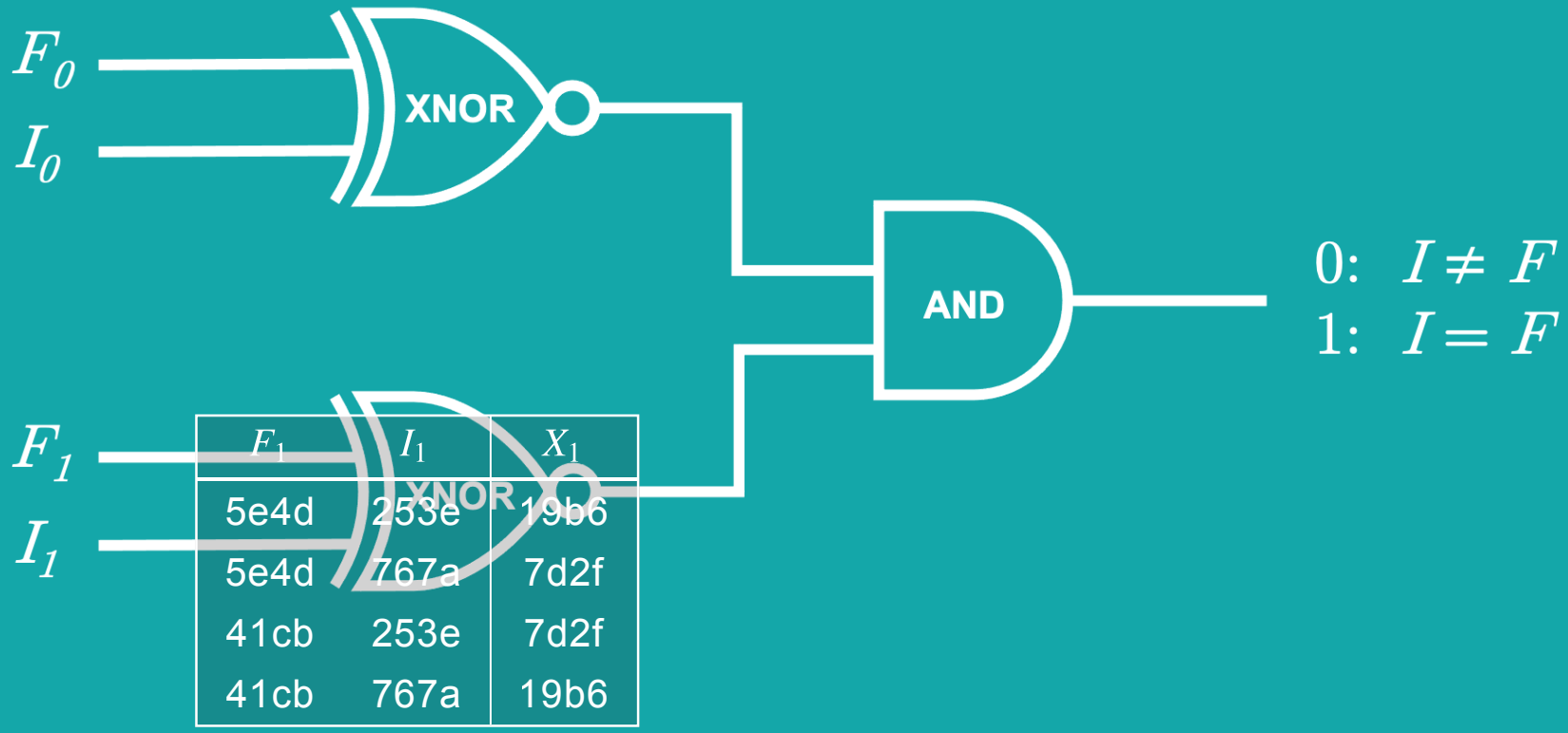
$$1: \ I = F$$

FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
🔑	🔑	••••	c2bf
🔑	🔑	••••	4b0e

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$
$$I = I_1I_0$$



F_1	I_1	X_1
5e4d	253e	19b6
5e4d	767a	7d2f
41cb	253e	7d2f
41cb	767a	19b6

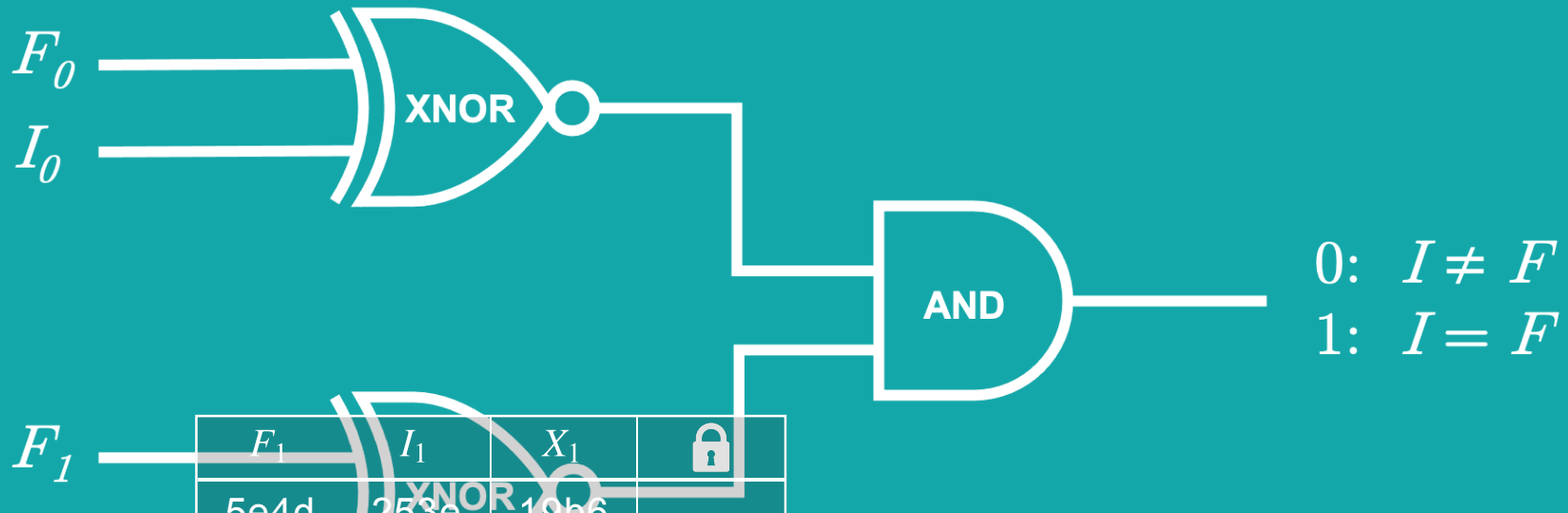
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
🔑	🔑	••••	c2bf
🔑	🔑	••••	4b0e

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$

$$I = I_1I_0$$



$$0: \ I \neq F$$

$$1: \ I = F$$

F_1	I_1	X_1	🔒
5e4d	253e	19b6	
5e4d	767a	7d2f	
41cb	253e	7d2f	
41cb	767a	19b6	

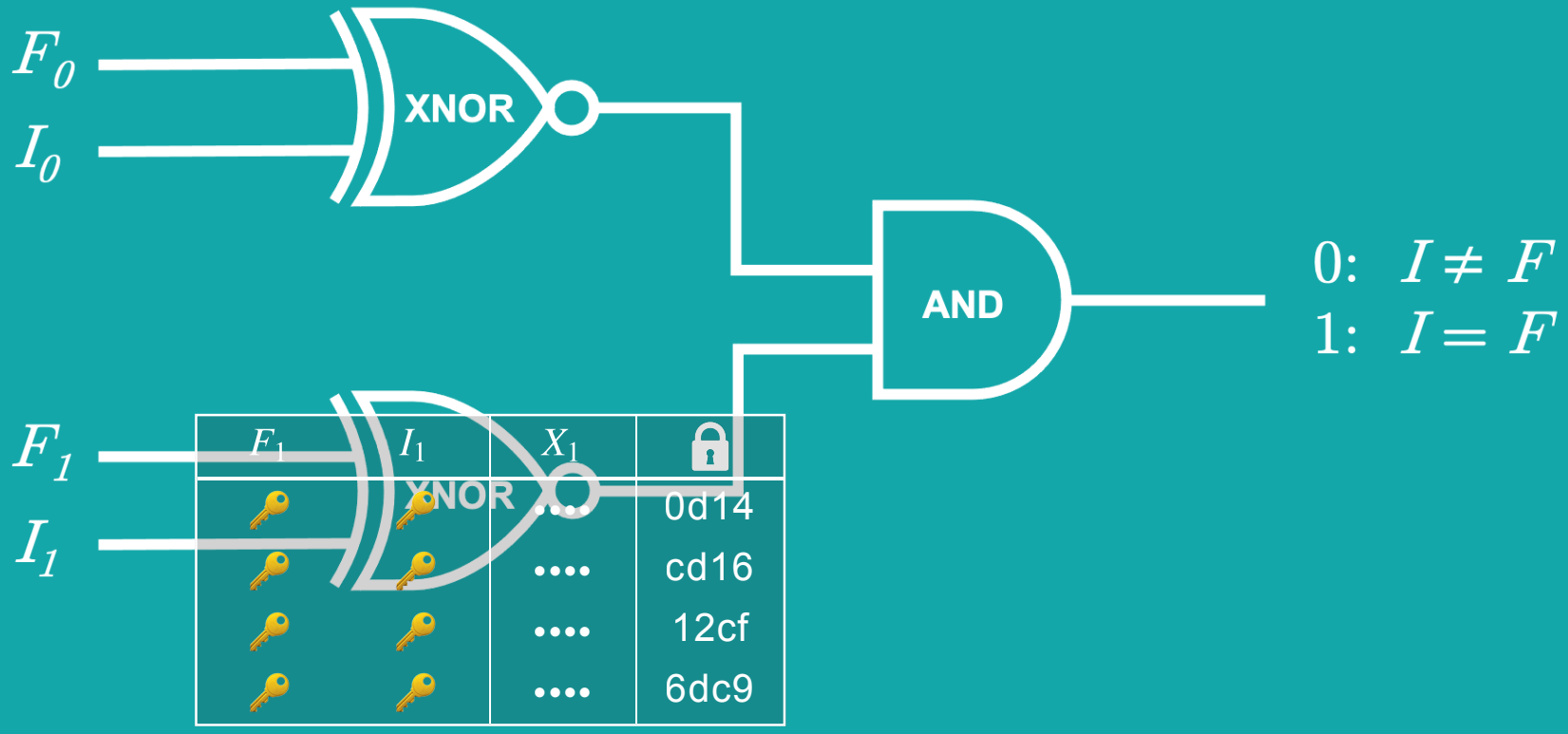
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
🔑	🔑	••••	c2bf
🔑	🔑	••••	4b0e

X_0	X_1	X
bd67	7d2f	bbe9
bd67	19b6	bbe9
ed56	7d2f	bbe9
ed56	19b6	0084

$$F = F_1F_0$$

$$I = I_1I_0$$



$$0: \ I \neq F$$

$$1: \ I = F$$

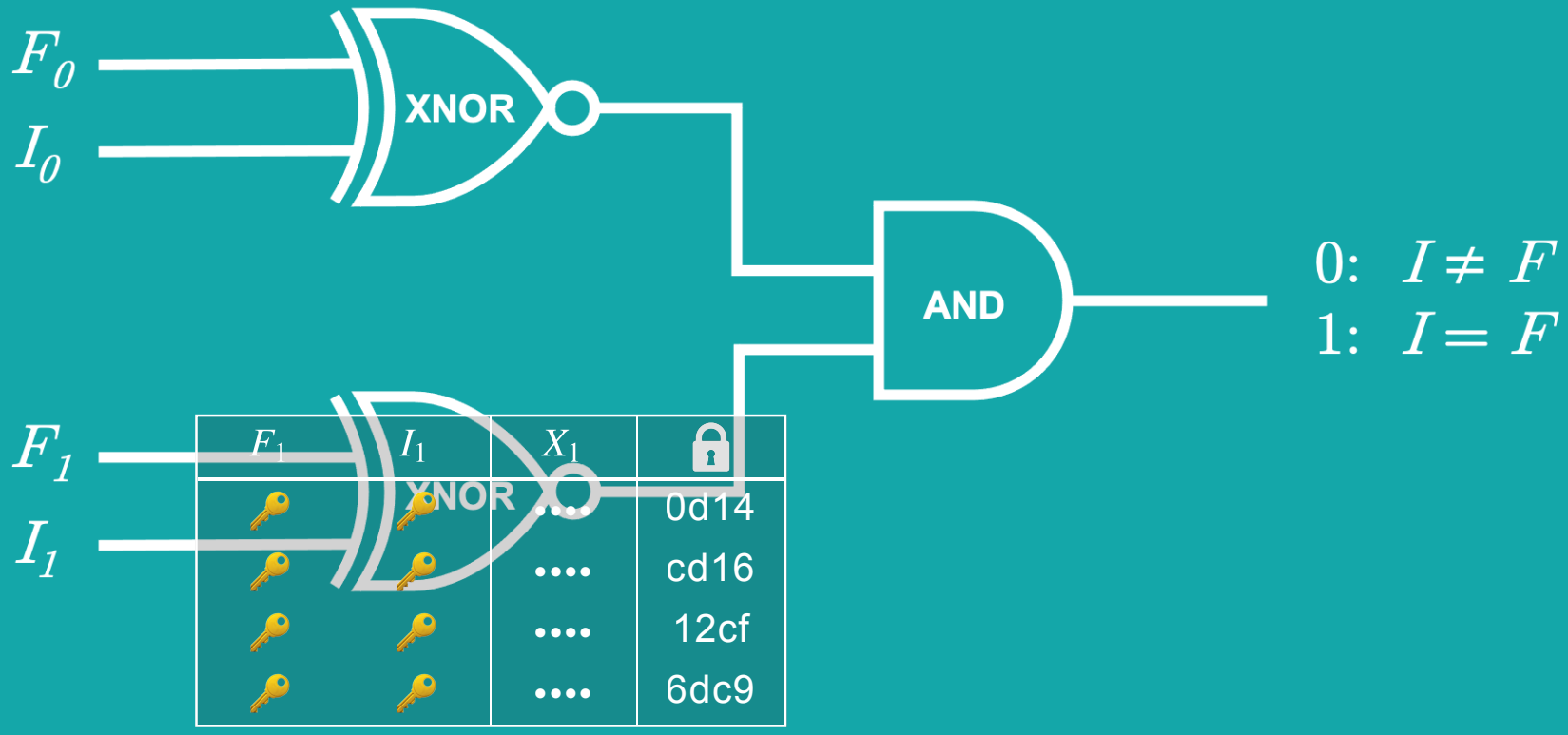
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
🔑	🔑	••••	c2bf
🔑	🔑	••••	4b0e

X_0	X_1	X	🔒
bd67	7d2f	bbe9	
bd67	19b6	bbe9	
ed56	7d2f	bbe9	
ed56	19b6	0084	

$$F = F_1F_0$$

$$I = I_1I_0$$



F_1	I_1	X_1	🔒
🔑	🔑	••••	0d14
🔑	🔑	••••	cd16
🔑	🔑	••••	12cf
🔑	🔑	••••	6dc9

$0: \ I \neq F$

$1: \ I = F$

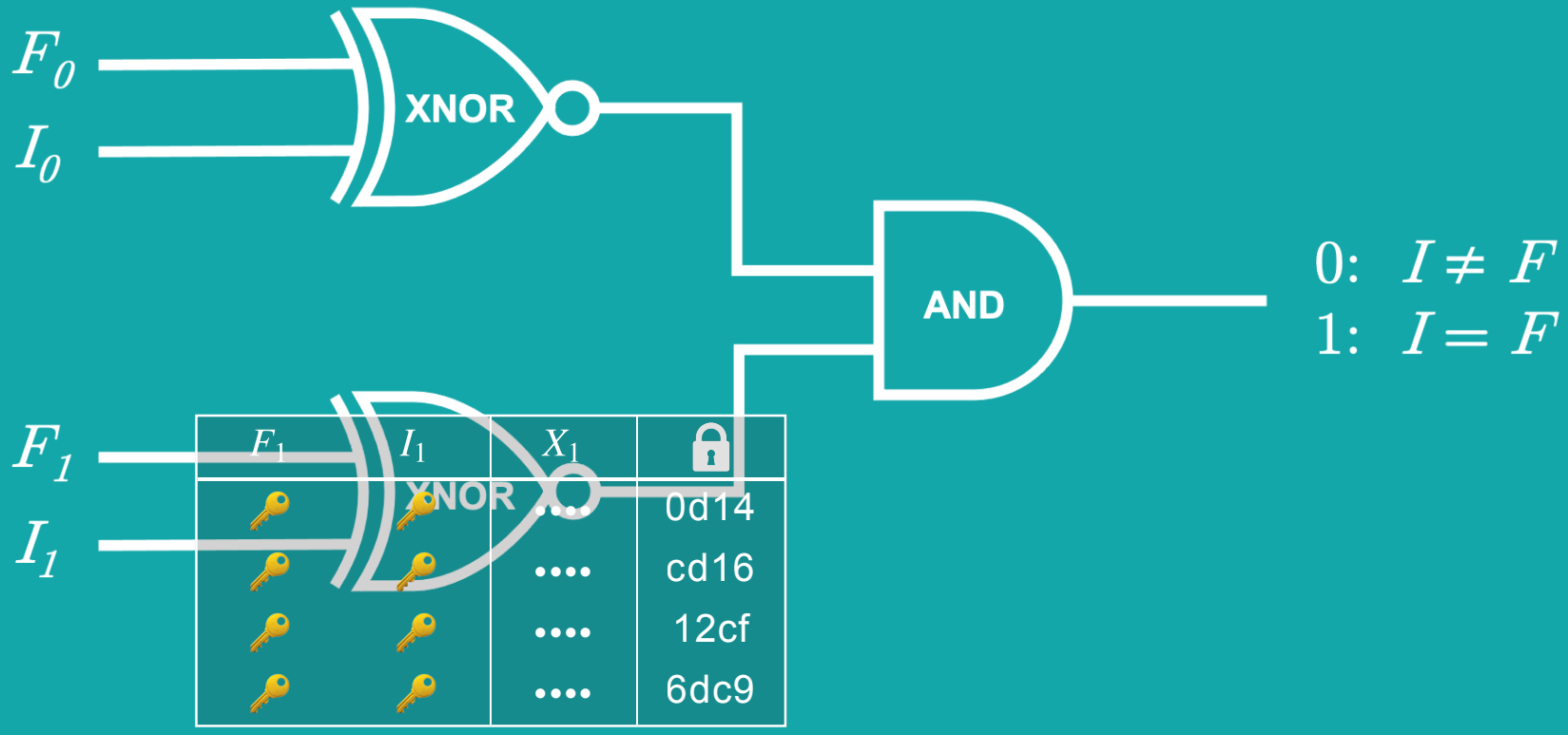
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	fddd
🔑	🔑	••••	ad11
🔑	🔑	••••	c2bf
🔑	🔑	••••	4b0e

X_0	X_1	X	🔒
🔑	🔑	••••	6f4e
🔑	🔑	••••	b49c
🔑	🔑	••••	712a
🔑	🔑	••••	f4de

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1	🔒
🔑	🔑	••••	0d14
🔑	🔑	••••	cd16
🔑	🔑	••••	12cf
🔑	🔑	••••	6dc9

$0: \ I \neq F$

$1: \ I = F$

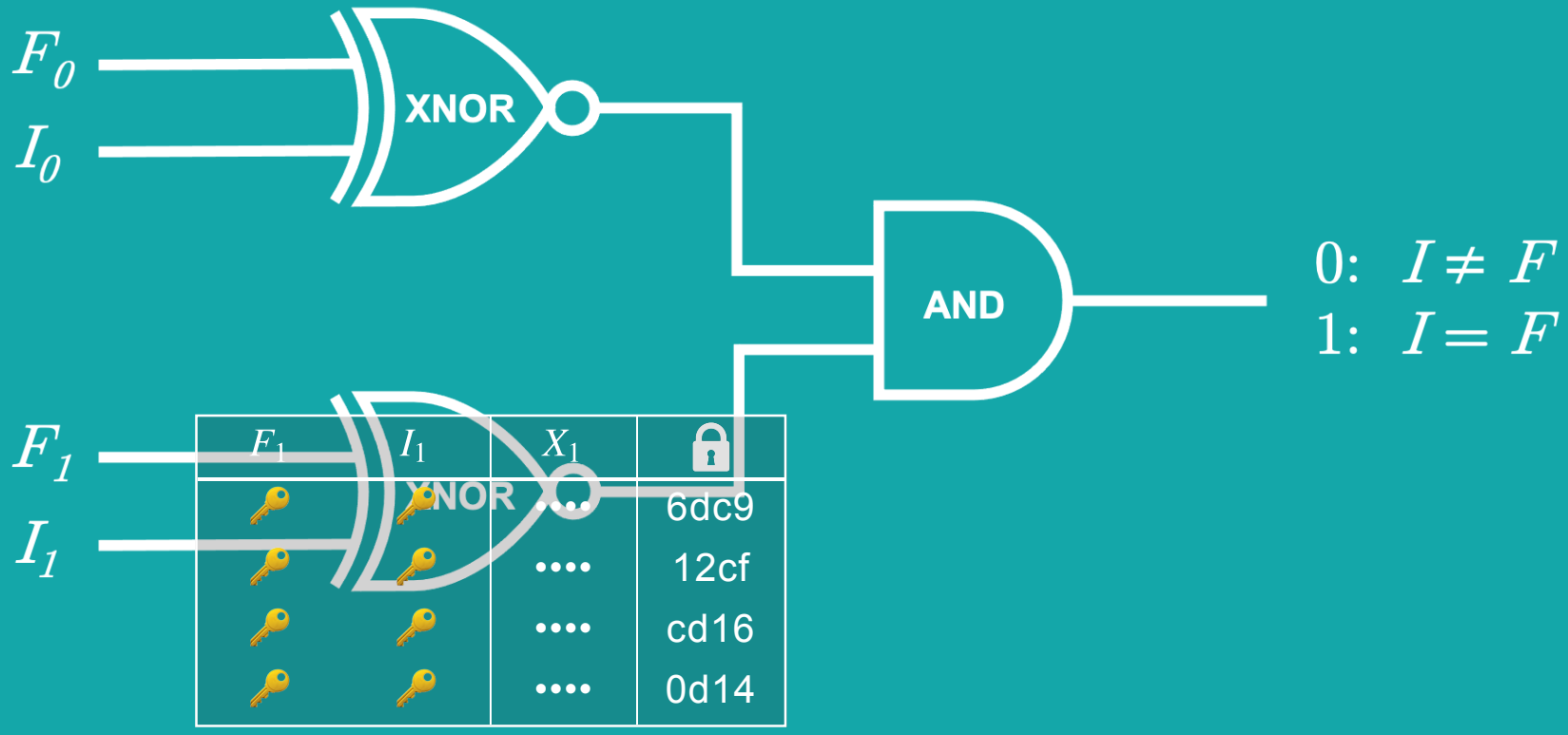
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	ad11
🔑	🔑	••••	4b0e
🔑	🔑	••••	fddd
🔑	🔑	••••	c2bf

X_0	X_1	X	🔒
🔑	🔑	••••	712a
🔑	🔑	••••	b49c
🔑	🔑	••••	f4de
🔑	🔑	••••	6f4e

$$F = F_1 F_0$$

$$I = I_1 I_0$$



F_1	I_1	X_1	🔒
🔑	🔑	••••	6dc9
🔑	🔑	••••	12cf
🔑	🔑	••••	cd16
🔑	🔑	••••	0d14

$$0: \; I \neq F$$

$$1: \; I = F$$

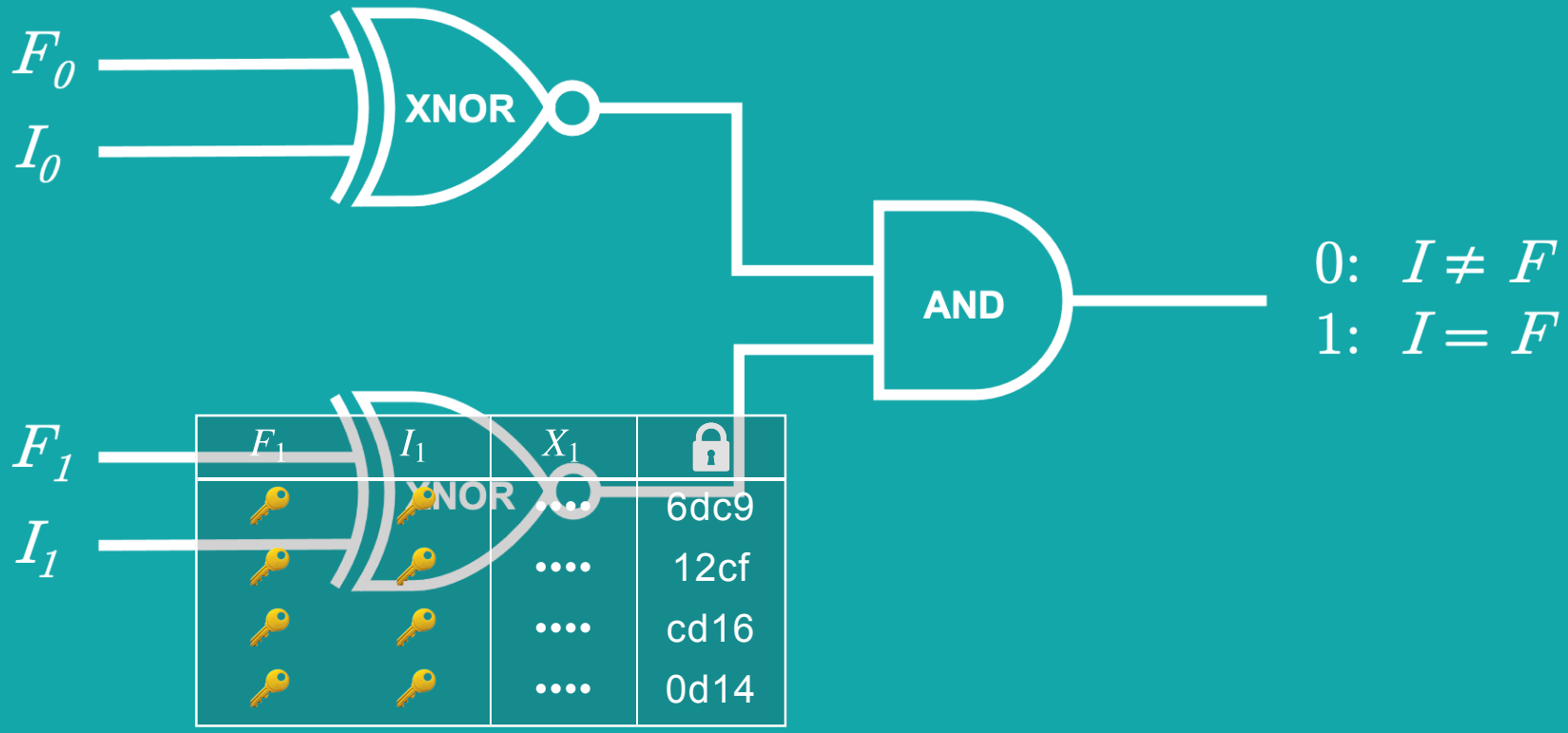
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	ad11
🔑	🔑	••••	4b0e
🔑	🔑	••••	fddd
🔑	🔑	••••	c2bf

X_0	X_1	X	🔒
🔑	🔑	••••	712a
🔑	🔑	••••	b49c
🔑	🔑	••••	f4de
🔑	🔑	••••	6f4e

$F = 1\,1_2$

$I = I_1 I_0$



F_1	I_1	X_1	🔒
🔑	🔑	••••	6dc9
🔑	🔑	••••	12cf
🔑	🔑	••••	cd16
🔑	🔑	••••	0d14

$0: \; I \neq F$

$1: \; I = F$

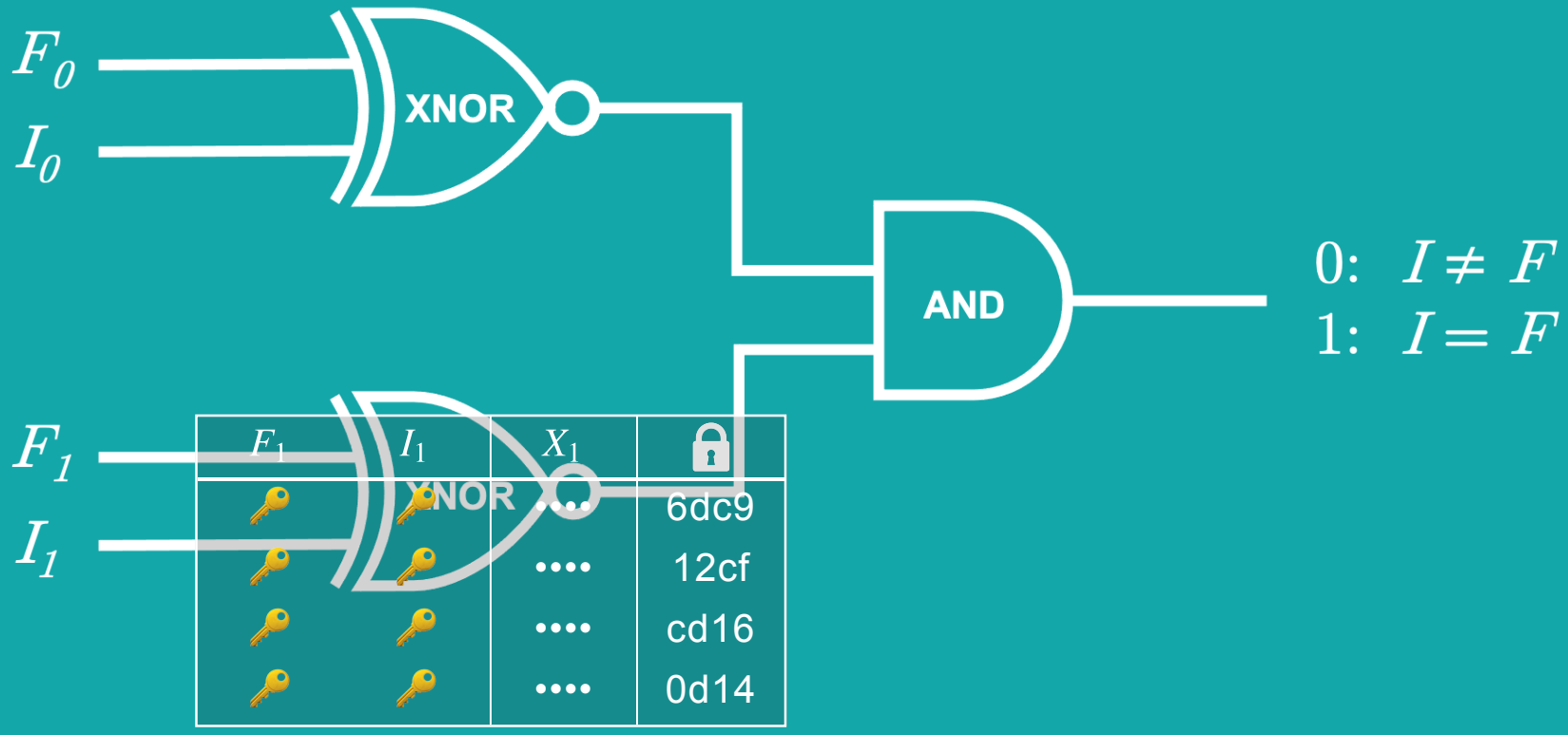
FACILITY'S VIEWPOINT

F_0	I_0	X_0	🔒
🔑	🔑	••••	ad11
🔑	🔑	••••	4b0e
🔑	🔑	••••	fddd
🔑	🔑	••••	c2bf

X_0	X_1	X	🔒
🔑	🔑	••••	712a
🔑	🔑	••••	b49c
🔑	🔑	••••	f4de
🔑	🔑	••••	6f4e

$F = 1\,1_2$

$I = ??$



F_1	I_1	X_1	🔒
🔑	🔑	••••	6dc9
🔑	🔑	••••	12cf
🔑	🔑	••••	cd16
🔑	🔑	••••	0d14

$0: \; I \neq F$

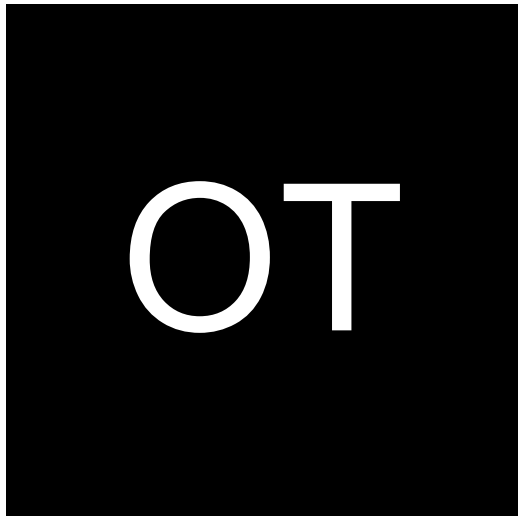
$1: \; I = F$

FACILITY'S VIEWPOINT

Oblivious Transfer

Facility

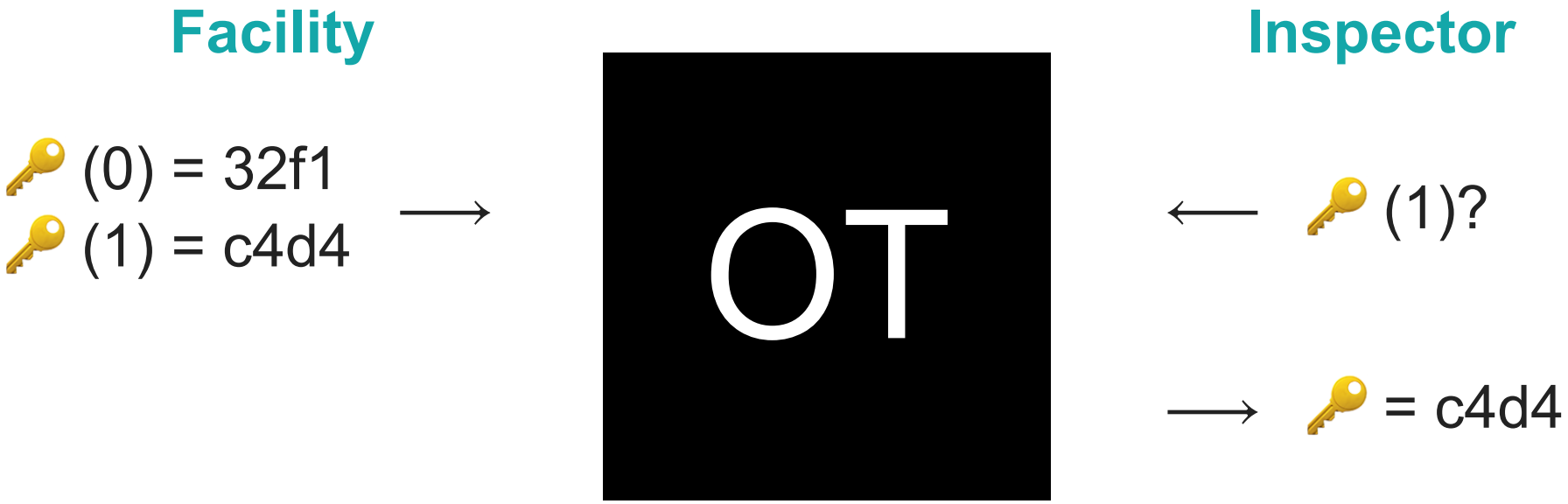
🔑 (0) = 32f1
🔑 (1) = c4d4



Inspector

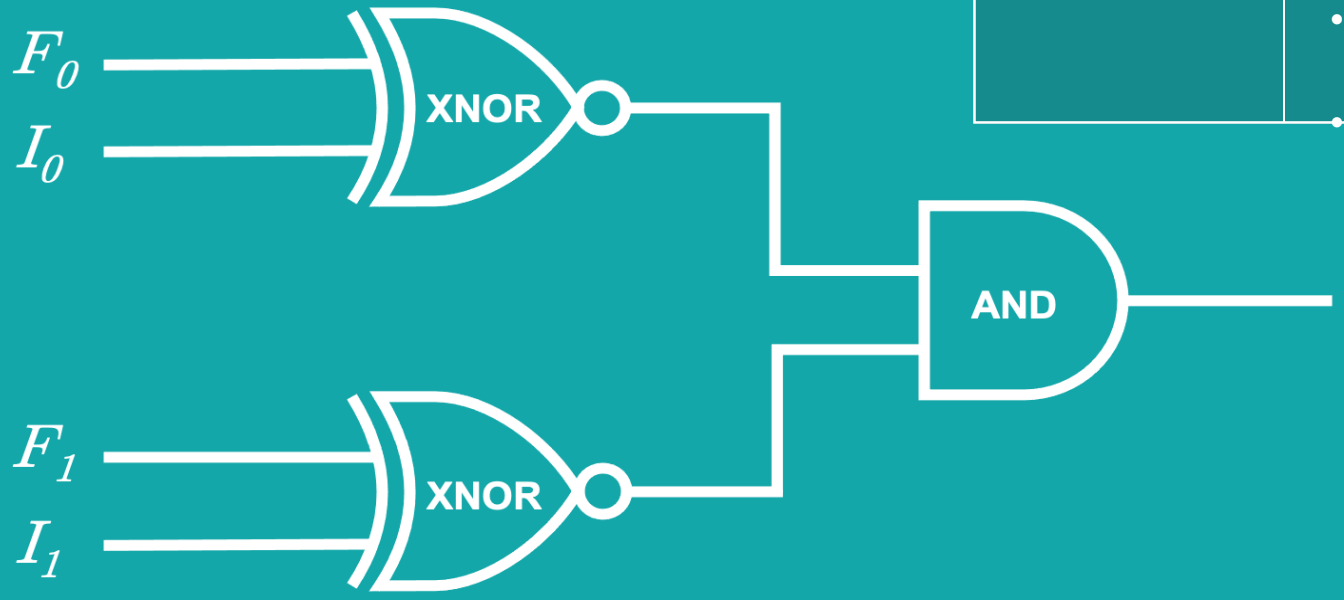
🔑 (1)?

Oblivious Transfer



F_0	I_0	X_0	
		••••	ad11
		••••	4b0e
		••••	fddd
		••••	c2bf

X_0	X_1	X	
		••••	712a
		••••	b49c
		••••	f4de
		••••	6f4e



$$F = F_1 F_0$$

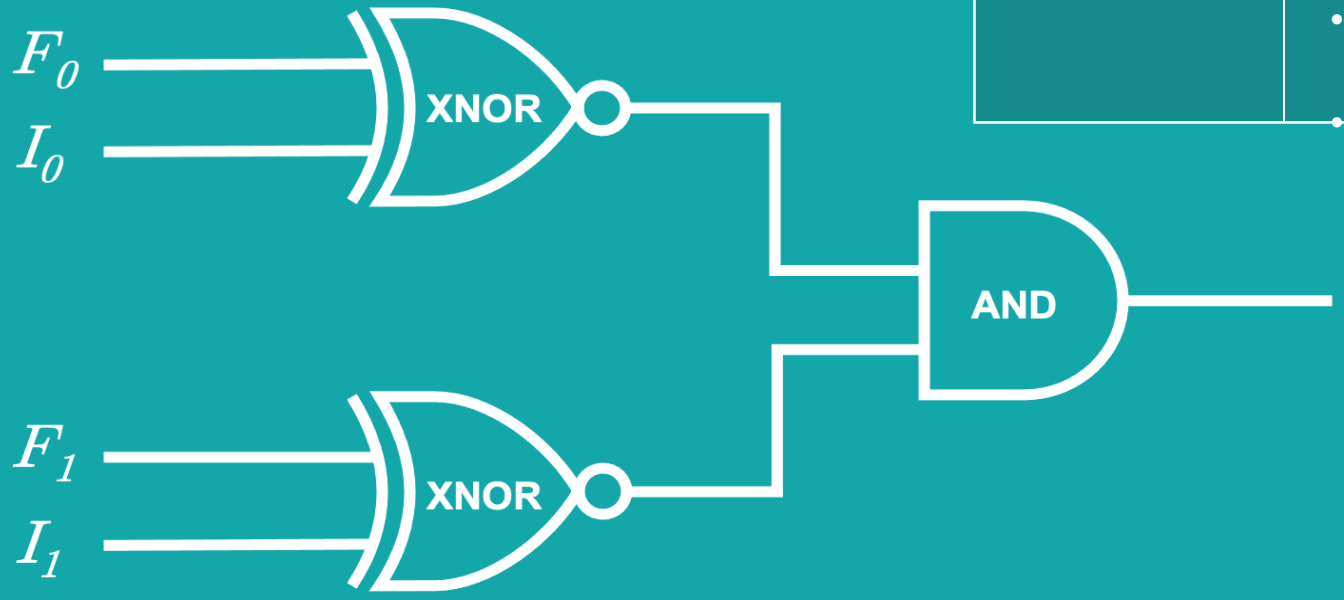
$$I = I_1 I_0$$

$$0: \quad I \neq F$$
$$1: \quad I = F$$

F_1	I_1	X_1	
		••••	6dc9
		••••	12cf
		••••	cd16
		••••	0d14

F_0	I_0	X_0	
		••••	ad11
		••••	4b0e
		••••	fddd
		••••	c2bf

X_0	X_1	X	
		••••	712a
		••••	b49c
		••••	f4de
		••••	6f4e



$$F = F_1 F_0$$

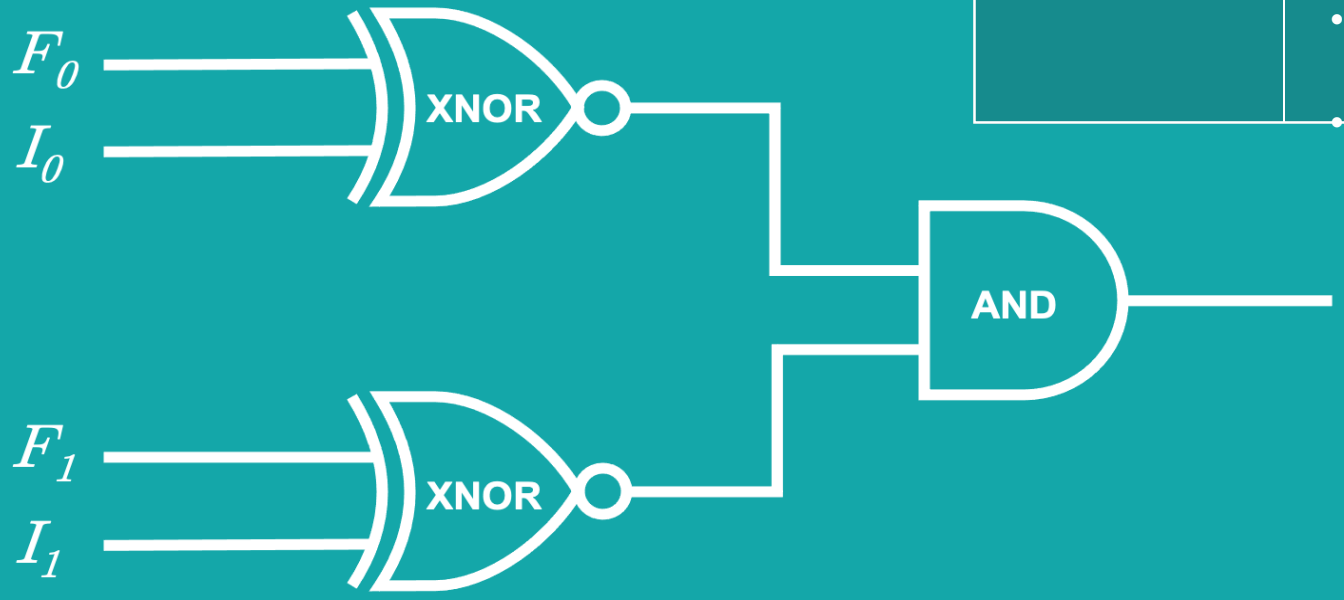
$$I = 1\,0_2$$

$$0\text{:}\quad I \neq F$$
$$1\text{:}\quad I = F$$

F_1	I_1	X_1	
		••••	6dc9
		••••	12cf
		••••	cd16
		••••	0d14

F_0	I_0	X_0	
		••••	ad11
		••••	4b0e
		••••	fddd
		••••	c2bf

X_0	X_1	X	
		••••	712a
		••••	b49c
		••••	f4de
		••••	6f4e



$F = ??$

$I = 10_2$

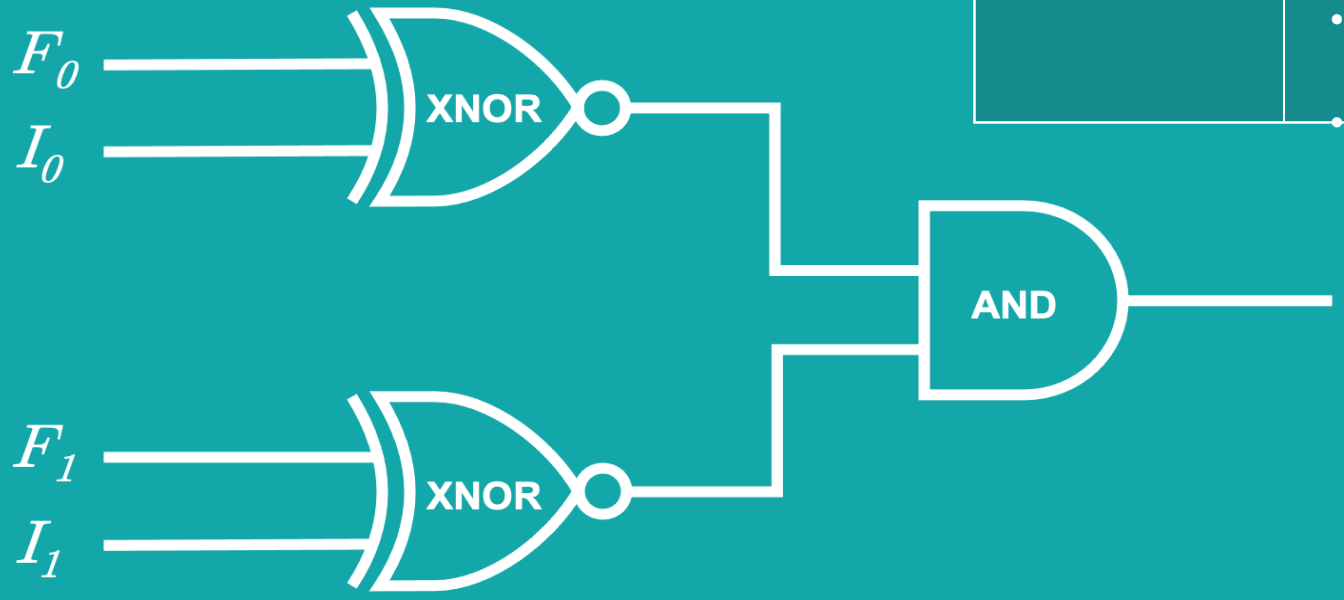
$0: \; I \neq F$

$1: \; I = F$

F_1	I_1	X_1	
		••••	6dc9
		••••	12cf
		••••	cd16
		••••	0d14

F_0	I_0	X_0	🔒
131b		•••• •••• •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
		•••• •••• •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

$0: \quad I \neq F$

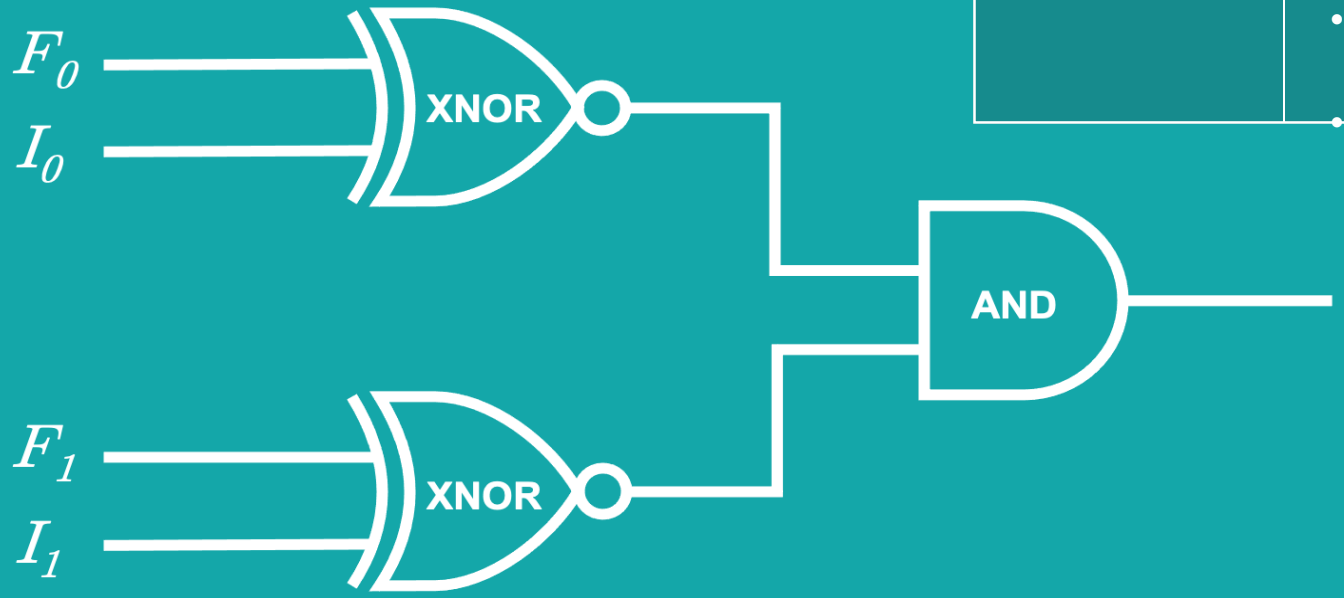
$1: \quad I = F$

F_1	I_1	X_1	🔒
		•••• •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	••••	ad11
		••••	4b0e
		••••	fddd
		••••	c2bf

X_0	X_1	X	🔒
		••••	712a
		••••	b49c
		••••	f4de
		••••	6f4e



$F = ??$

$I = 10_2$

$0: \; I \neq F$

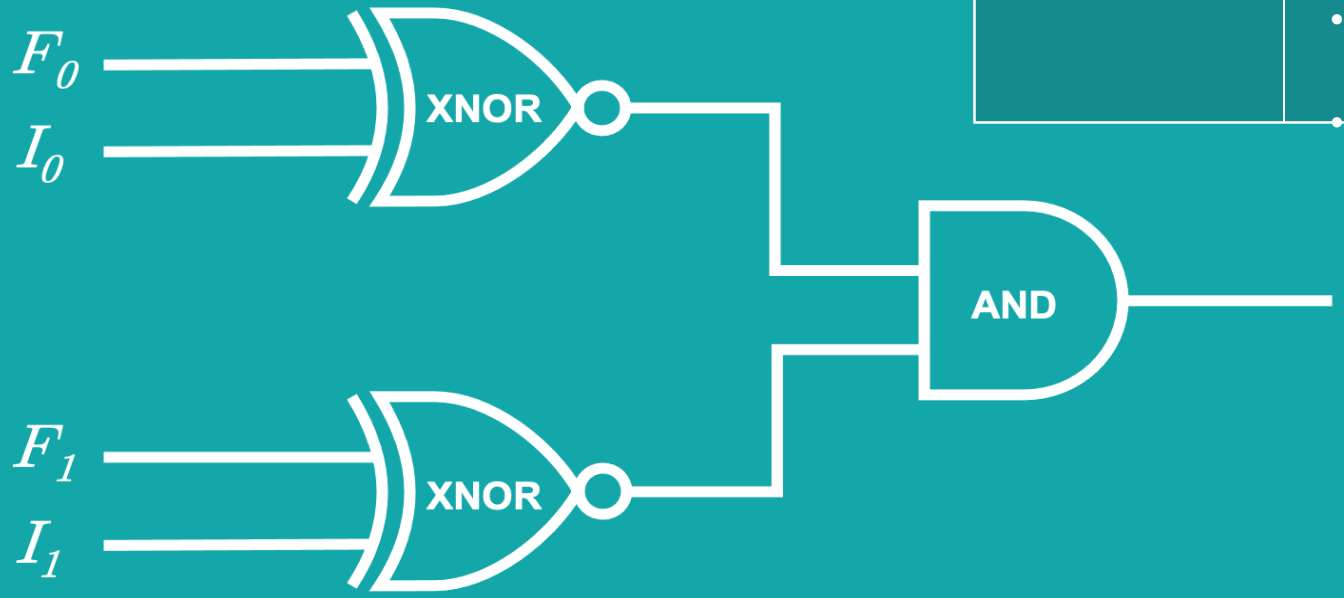
$1: \; I = F$

F_1	I_1	X_1	🔒
		••••	6dc9
		••••	12cf
		••••	cd16
		••••	0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	•••• bd67 •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
bd67		•••• •••• •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

$0: \; I \neq F$

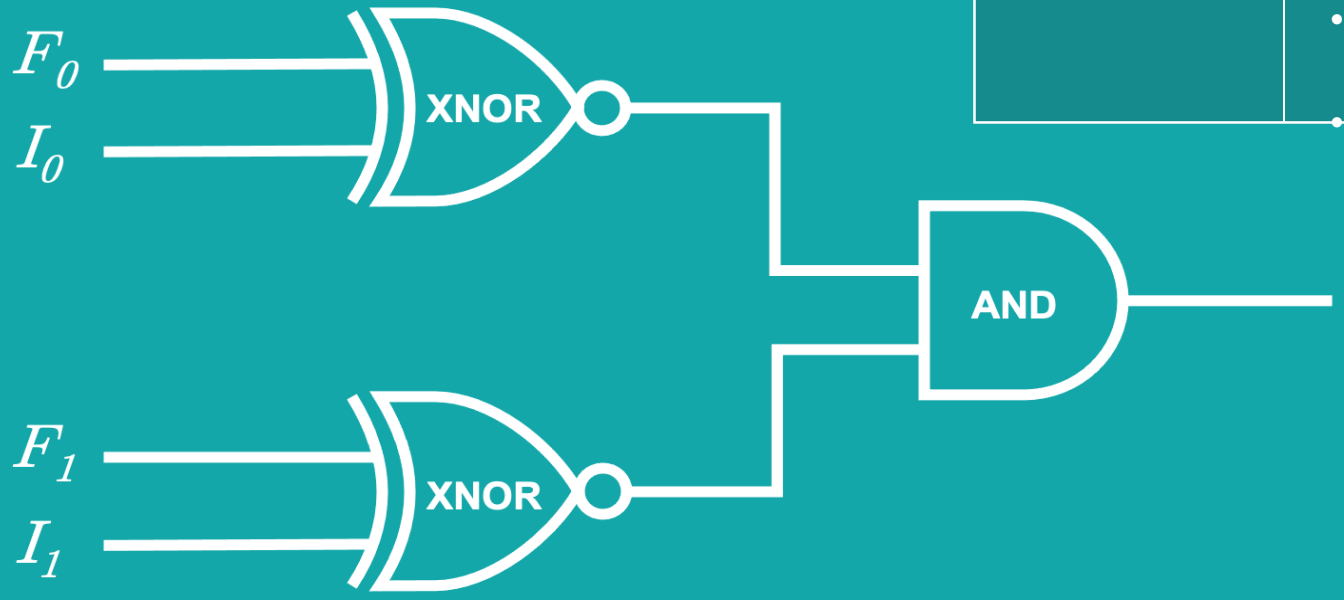
$1: \; I = F$

F_1	I_1	X_1	🔒
		•••• •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	•••• bd67 •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
bd67		•••• •••• •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

$0: \; I \neq F$

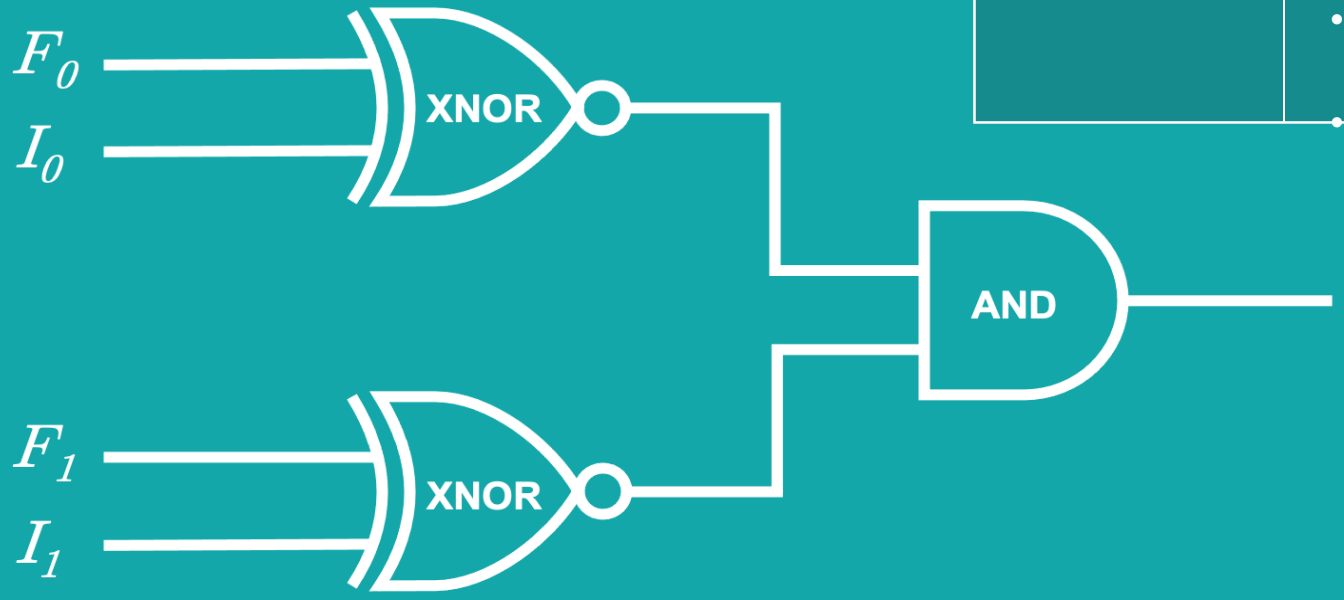
$1: \; I = F$

F_1	I_1	X_1	🔒
41cb		•••• •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	•••• bd67 •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
bd67		•••• •••• •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

$0: \; I \neq F$

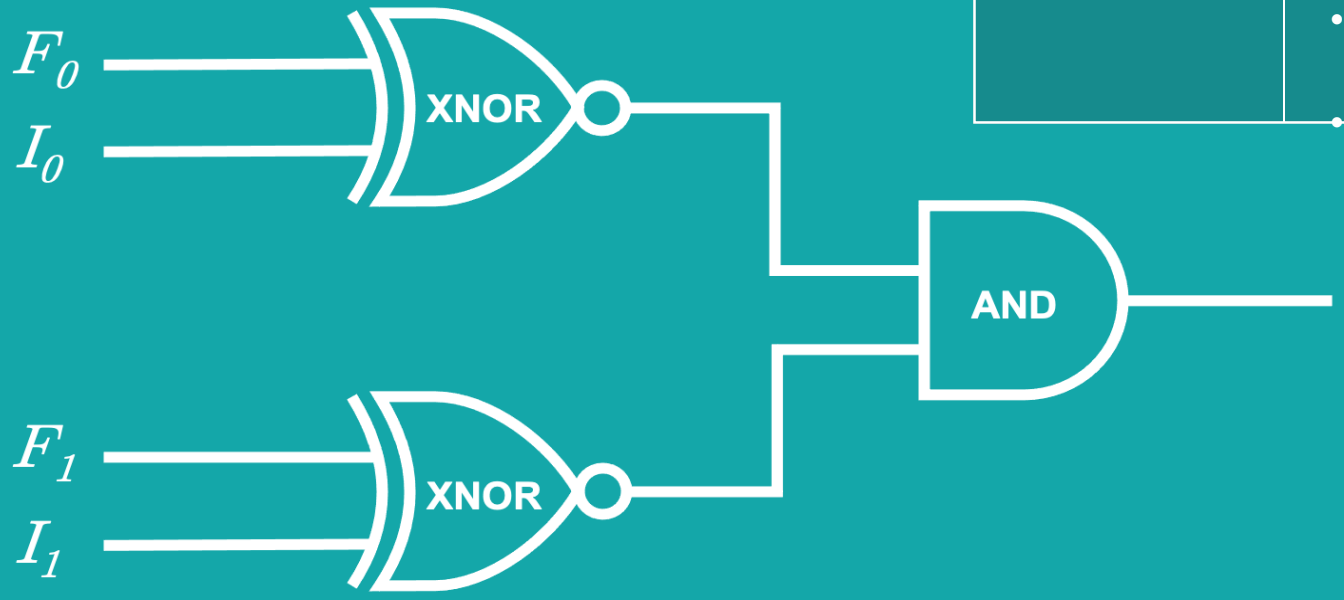
$1: \; I = F$

F_1	I_1	X_1	🔒
41cb	767a	•••• •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	•••• bd67 •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
bd67	19b6	•••• •••• •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

$0: \ I \neq F$

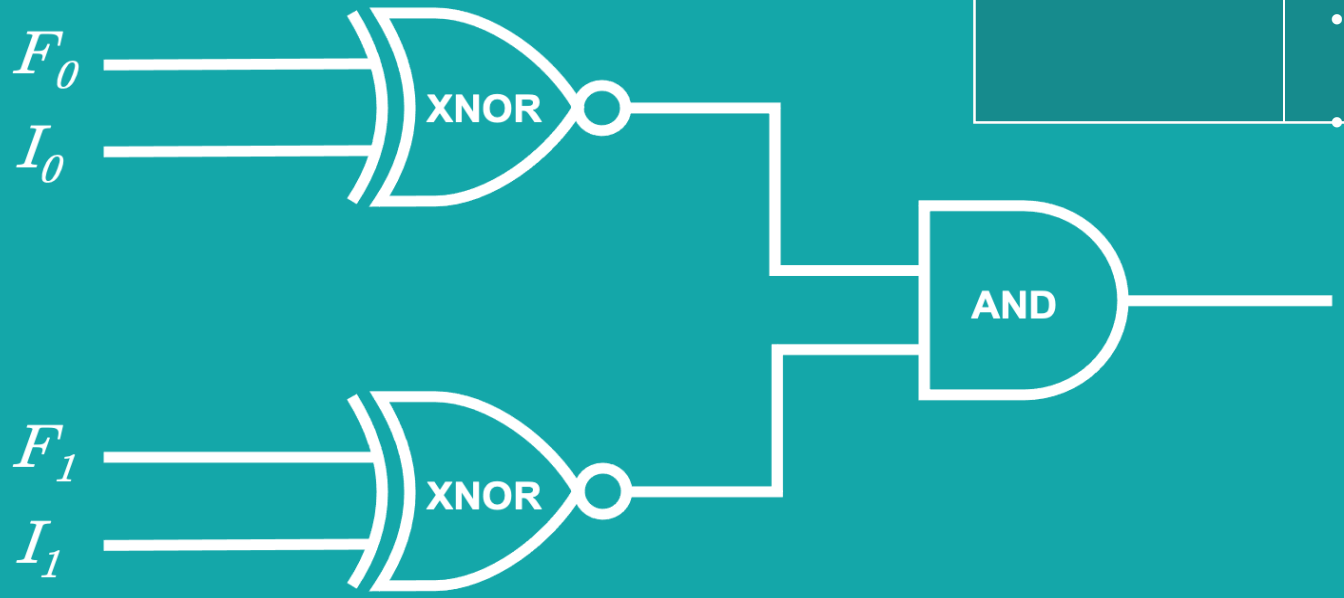
$1: \ I = F$

F_1	I_1	X_1	🔒
41cb	767a	19b6 •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	•••• bd67 •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
bd67	19b6	•••• bbe9 •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

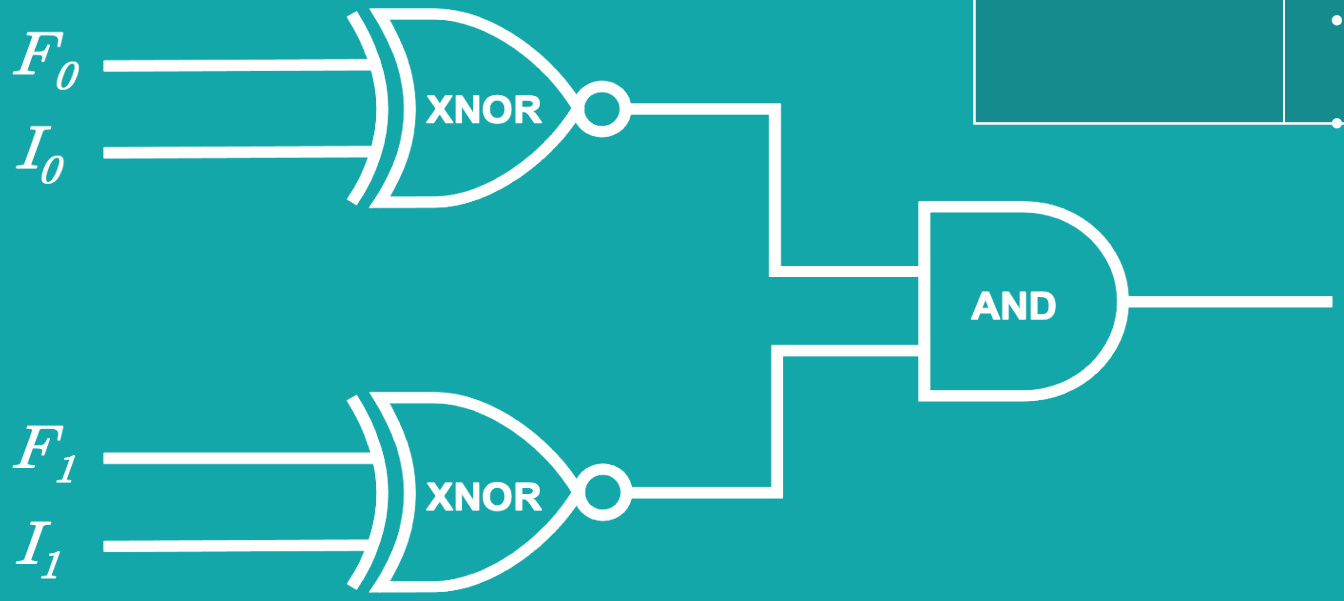
0: $I \neq F$
1: $I = F$

F_1	I_1	X_1	🔒
41cb	767a	19b6 •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

F_0	I_0	X_0	🔒
131b	32f1	•••• bd67 •••• ••••	ad11 4b0e fddd c2bf

X_0	X_1	X	🔒
bd67	19b6	•••• 0 •••• ••••	712a b49c f4de 6f4e



$F = ??$

$I = 10_2$

0: $I \neq F$

1: $I = F$

F_1	I_1	X_1	🔒
41cb	767a	19b6 •••• •••• ••••	6dc9 12cf cd16 0d14

INSPECTOR'S VIEWPOINT

Existing Frameworks

Fair Play
Secure Function Evaluation

ABY

Obliv-C

(and more...)

SoK: General Purpose Compilers for Secure Multi-Party Computation

Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic
University of Pennsylvania
{ mhast, fbrett, dgnoble, stevez } @cis.upenn.edu

***Abstract*—Secure multi-party computation (MPC) allows a group of mutually distrustful parties to compute a joint function on their inputs without revealing any information beyond the result of the computation. This type of computation is extremely powerful and has wide-ranging applications in academia, industry, and government. Protocols for secure computation have existed for decades, but only recently have general-purpose compilers for executing MPC on arbitrary functions been developed. These projects rapidly improved the state of the art, and began to make MPC accessible to non-expert users. However, the field is changing so rapidly that it is difficult even for experts to keep track of the varied capabilities of modern frameworks.**

In this work, we survey general-purpose compilers for secure multi-party computation. These tools provide high-level abstractions to describe arbitrary functions and execute secure computation protocols. We consider eleven systems: EMP-toolkit, Obliv-C, ObliVM, TinyGarble, SCALE-MAMBA (formerly SPDZ), Wysteria, Sharemind, PICCO, ABY, Frigate and CBMC-GC. We evaluate these systems on a range of criteria, including language expressibility, capabilities of the cryptographic back-end, and accessibility to developers. We advocate for improved documentation of MPC frameworks, standardization within the community, and make recommendations for future directions in compiler development. Installing and running these systems can be challenging, and for each system,

[89], [136] and satellite collision detection [78], [79], [90].

Despite the demand for MPC technology, practical adoption has been limited, partly due to the *efficiency* of the underlying protocols. General-purpose MPC protocols, capable of securely computing *any* function, have been known to the cryptographic community for 30 years [33], [73], [131], [132]. Until recently such protocols were mainly of theoretical interest, and were considered too inefficient (from the standpoint of computation and communication complexity) to be useful in practice.

To address efficiency concerns, cryptographers have developed highly-optimized, special-purpose MPC protocols for a variety of use-cases. Unfortunately, this mode of operation does not foster widespread deployment or adoption of MPC in the real world. Even if these custom-tailored MPC protocols are theoretically *efficient* enough for practical use, designing, analyzing and implementing a custom-tailored protocol from the ground up for each application is not a scalable solution.

General-purpose MPC *compilers*, could drastically reduce the burden of designing multiple custom protocols and could allow non-experts to quickly prototype

750 hours

SoK: General Purpose Compilers for Secure Multi-Party Computation

Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic
University of Pennsylvania
{ mhast, fbrett, dgnoble, stevez } @cis.upenn.edu

750 hours **31 ¼ days**

SoK: General Purpose Compilers for Secure Multi-Party Computation

Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic
University of Pennsylvania
{ mhast, fbrett, dgnoble, stevez } @cis.upenn.edu

CypherCircuit

CypherCircuit

Circuits can be built and evaluated in just a few lines of code.

Facility

```
# Build a circuit
circuit = CircuitBoard()
A, B = Wire(circuit), Wire(circuit)
OneBitComparator(A, B)

# Run the protocol as the circuit generator
with Generator(circuit, evaluator_address) as facility:
        vector = '1-'
        facility.evaluate_protocol(vector)
```

Inspector

```
# Run the protocol as the circuit evaluator
with Evaluator(circuit, generator_address) as inspector:
        vector = '-0'
        inspector.evaluate_protocol(vector)
```

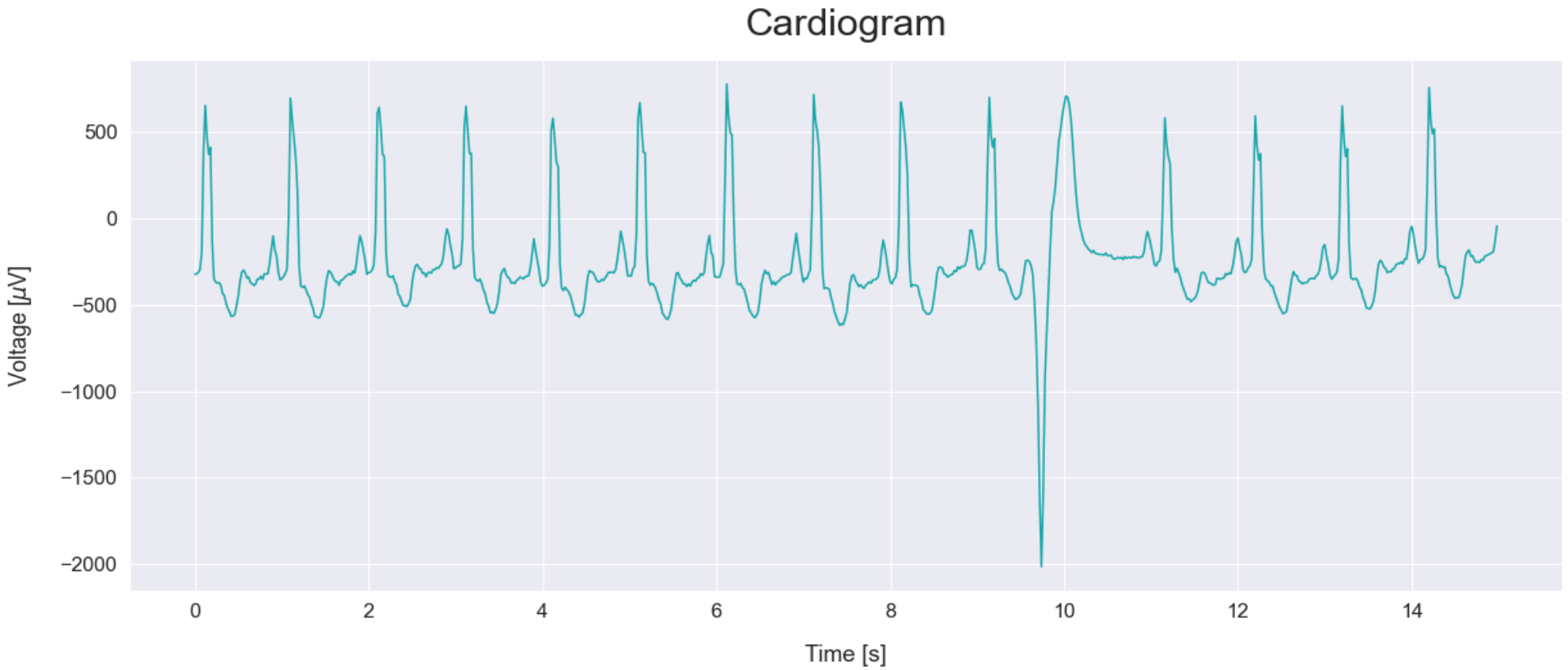
CypherCircuit

Circuits can be explored and analyzed on the fly.

```
>>> wire0.value
>>> wire1.value
False

>>> wire2.value
True

>>> and_gate = And(wire1, wire2)
>>> and_gate.output_wire.value
False

>>> and_gate.truthtable
W0001  W0002  |  W0003
------------------------
  0      0    |    0
  0      1    |    0
  1      0    |    0
  1      1    |    1
```

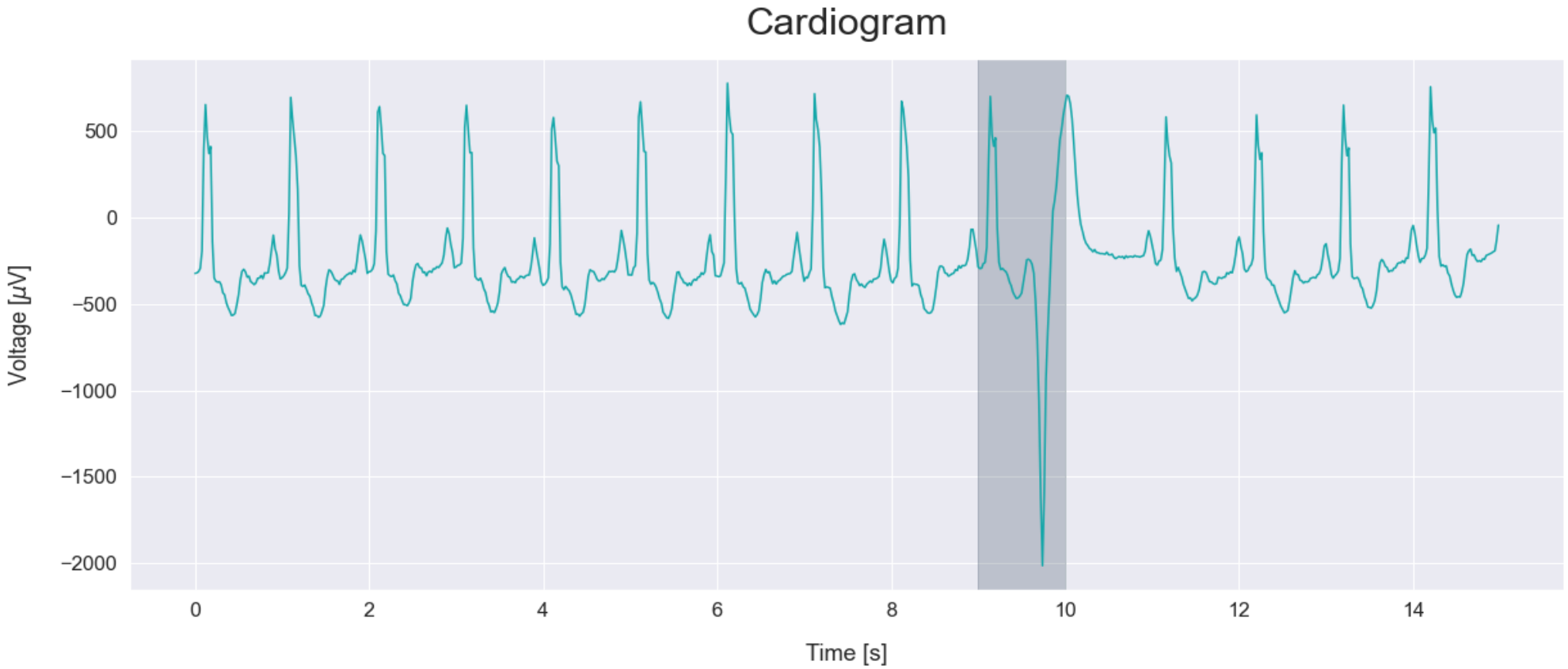
```
>>> and_gate.label()
>>> and_gate.labeltable()
 W0001    W0002   |   W0003
-------------------------------
70850a…  b54f72…  |  e785bd…
70850a…  d430d6…  |  e785bd…
11faae…  b54f72…  |  e785bd…
11faae…  d430d6…  |  86fa19…

>>> and_gate.garble()
>>> and_gate.tokentable
encrypted
---------
 44e869…
 98ddc3…
 bf0f97…
 590a8a…
```

ECG



Cardiogram data sourced from the Beth Israel Deaconness Congestive Heart Failure database

ECG



Heartbeat Anomaly Detected

Cardiogram data sourced from the Beth Israel Deaconness Congestive Heart Failure database

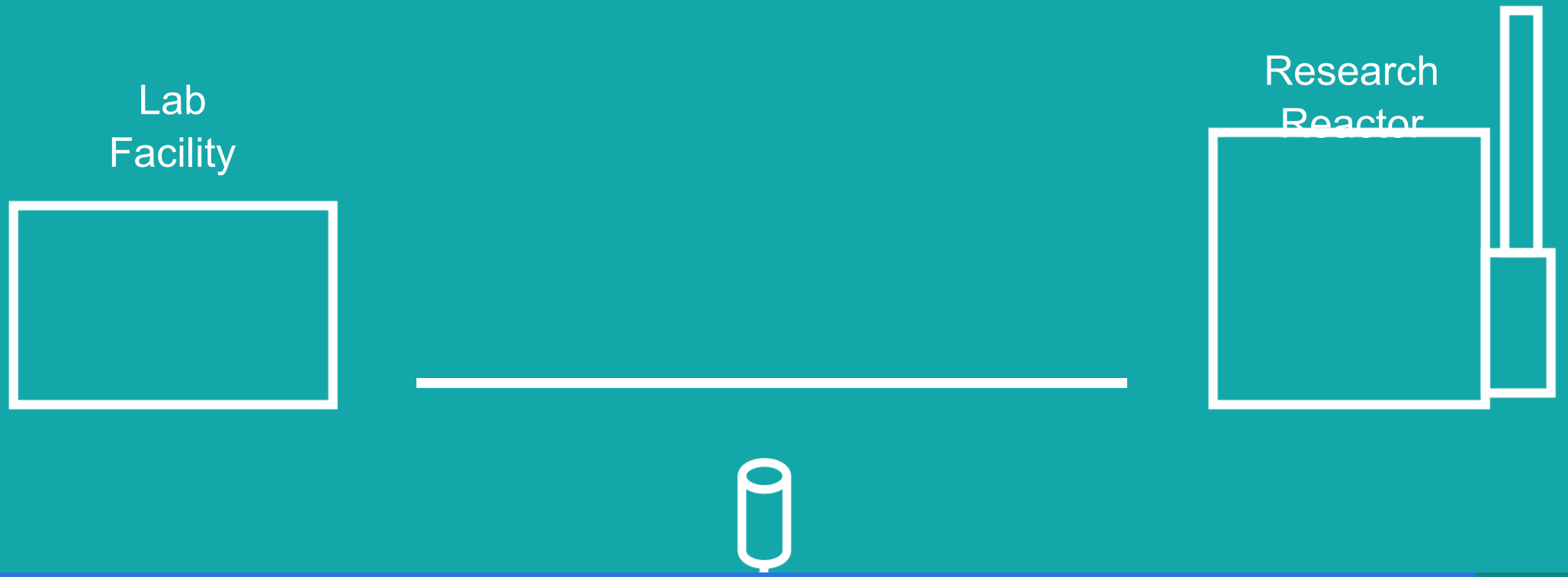
Modeling Urban Scenarios and Experiments

MUSE

Modeling Urban Scenarios and Experiments

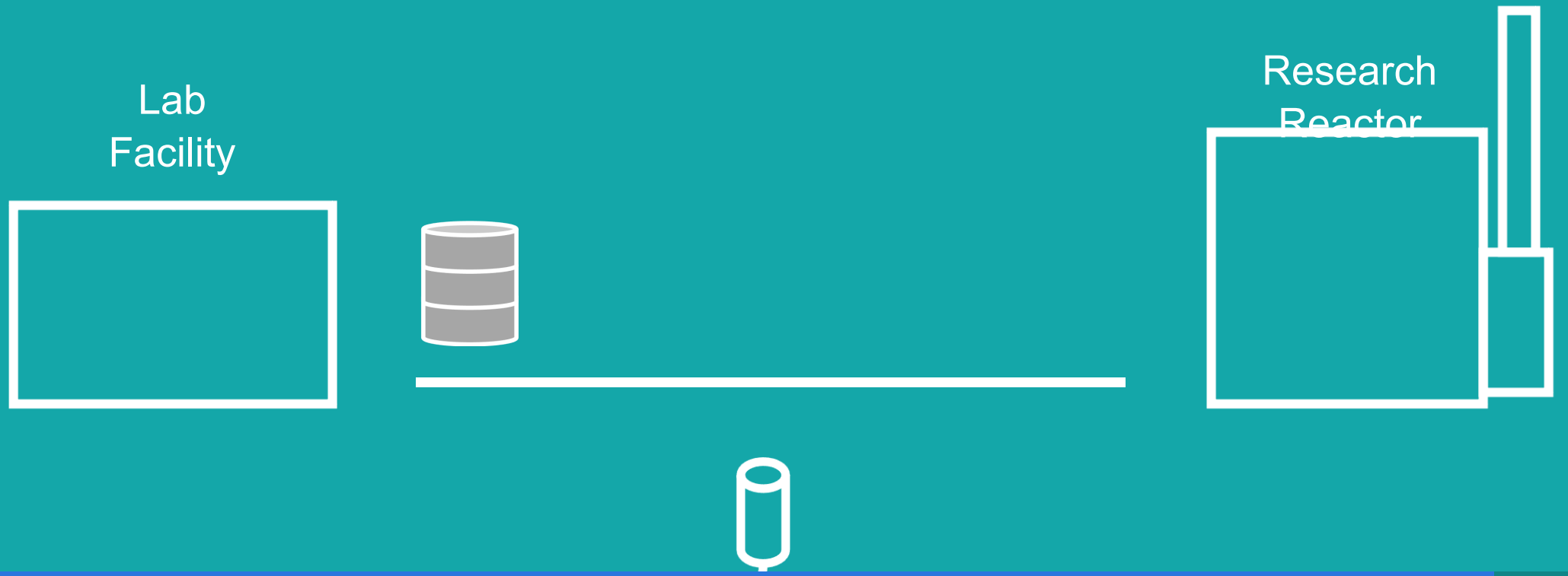
February 2019

Oak Ridge National Laboratory



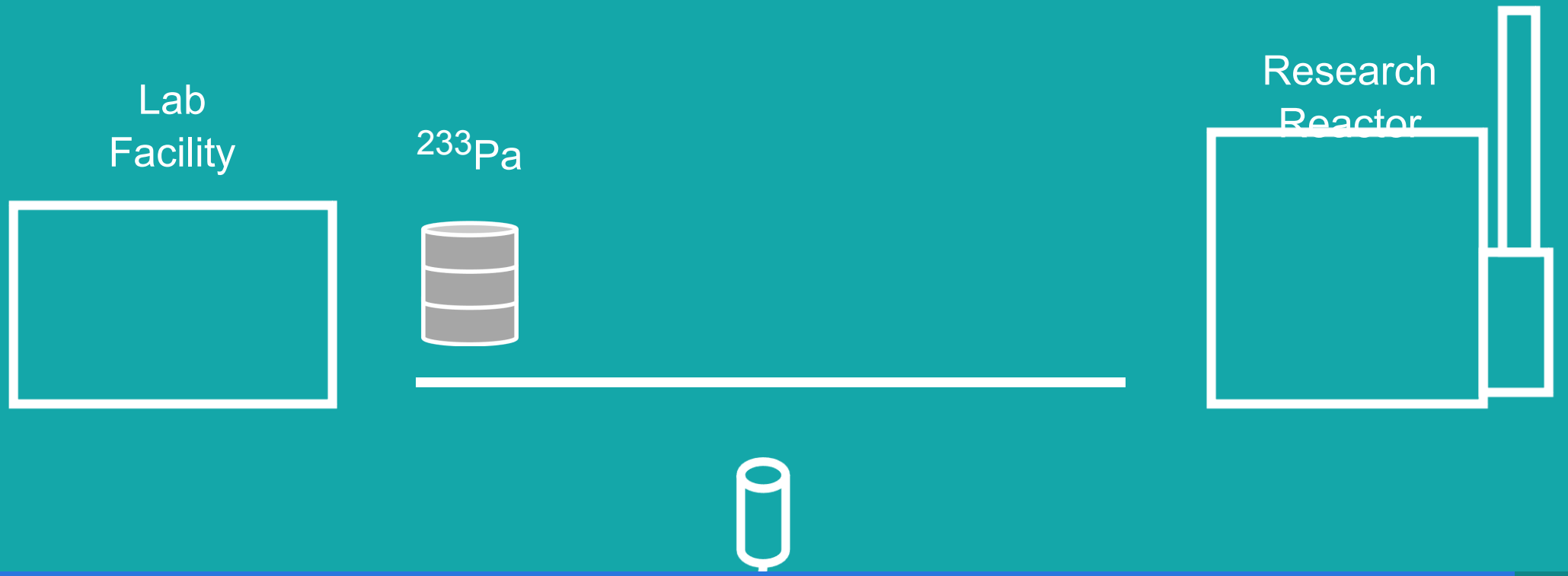
February 2019

Oak Ridge National Laboratory



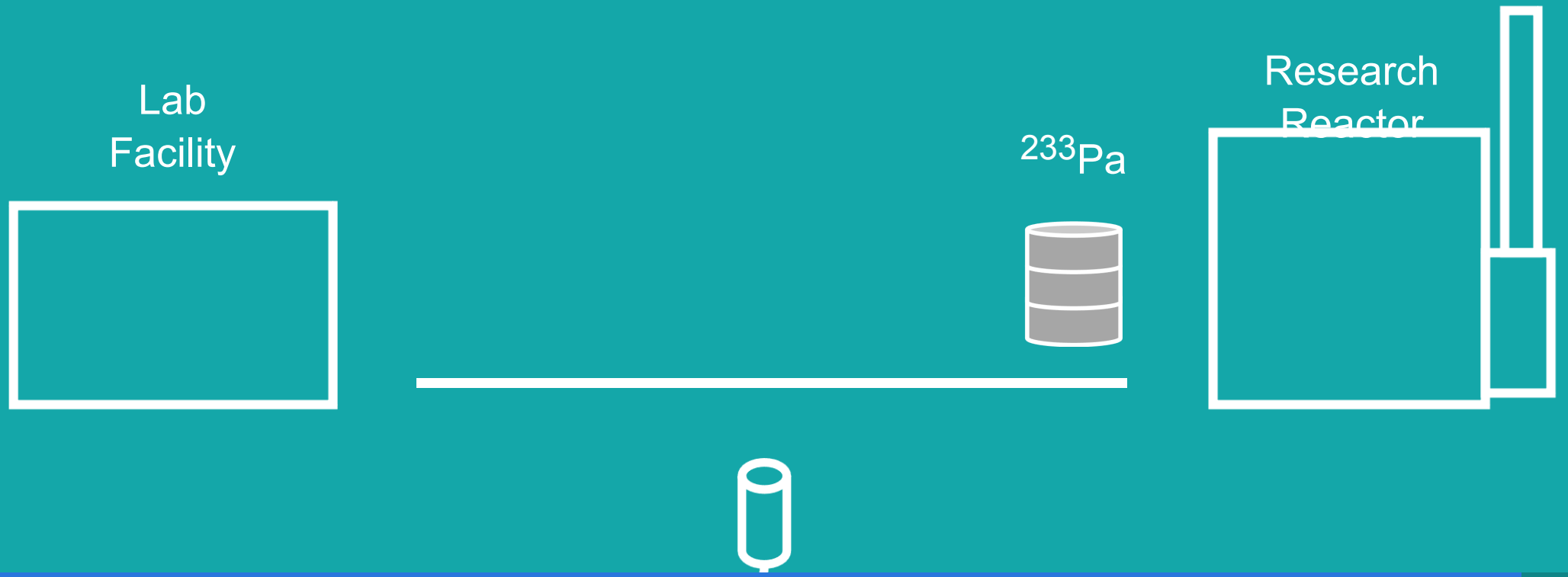
February 2019

Oak Ridge National Laboratory

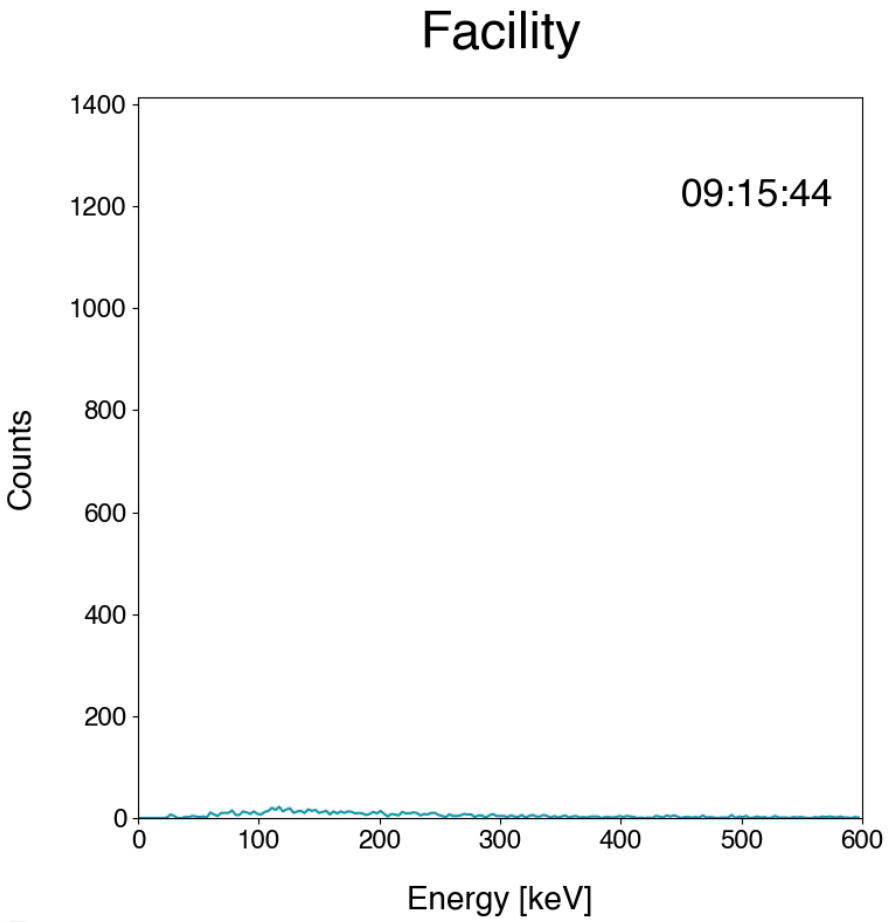


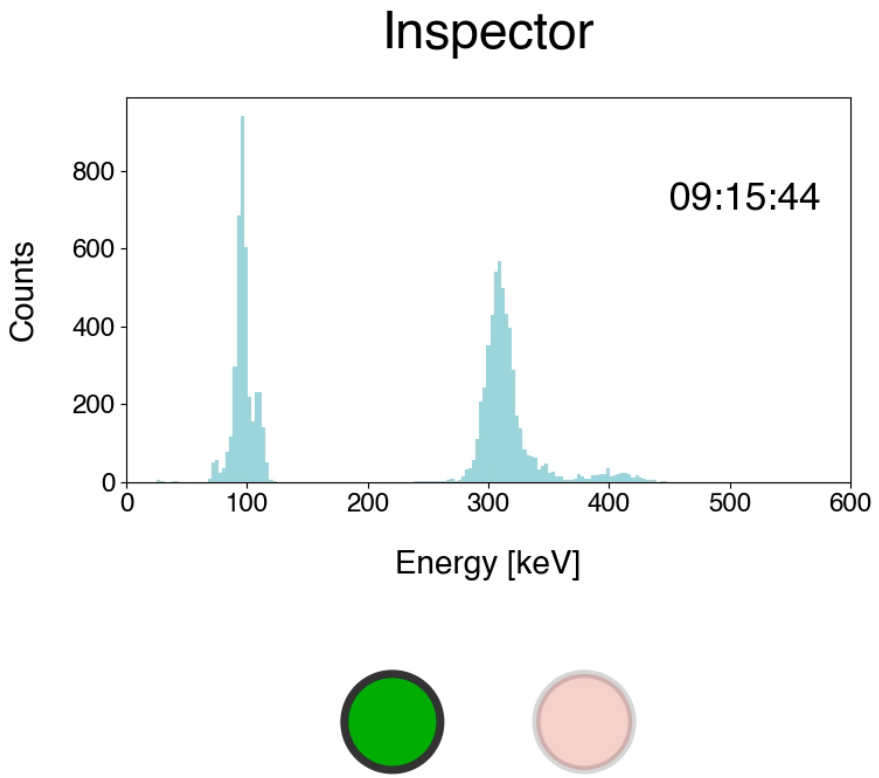
February 2019

Oak Ridge National Laboratory



MUSE – Oblivious Safeguards Anomaly Detection





keV: kiloelectronvolts

Still to come...

Still to come...

- Enhanced efficiency

Still to come...

- Enhanced efficiency
- Malicious adversaries

Still to come...

- Enhanced efficiency
- Malicious adversaries
- Spoofed inputs

This research was advised by Dr. Rachel Slaybaugh (UC Berkeley) and Dr. David Farley (Sandia National Laboratories).

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

We acknowledge the support of the NA-22 Office of Proliferation Detection (NA-221) and especially that of the NA-221/Safeguards Program manager, Dr. Chris Ramos, in funding this work.

Special thanks goes to Jared Johnson, Andrew Nicholson, Daniel Archer, Michael Willis, Irakli Garishvili, Andrew Rowe, Ian Stewart, and James Ghawaly developing, curating, and providing access to the MUSE dataset.

Approved for unlimited unclassified release (SAND2021-0391 C).

Get in touch with Mitch by reaching out to **negus@berkeley.edu**

Image Attributions

- "WTC smoking on 9-11", Michael Foran, CC BY 2.0, via Wikimedia Commons
- "Boston Marathon explosions", Aaron "tango" Tang from Cambridge, MA, USA, CC BY 2.0, via Wikimedia Commons
- "IAEA Inspectors", Dean Calma, Attribution, via Wikimedia Commons
- "IAEA Mass Spectrometry", Dean Calma/IAEA, Attribution-NonCommercial-NoDerivs 2.0 Generic (CC BY-NC-ND 2.0), via Flickr
- "IAEA Headquarters", Rodolfo Quevenco/IAEA, Attribution-ShareAlike 2.0 Generic (CC BY-SA 2.0), via Flickr
- "NPT Signatories", File:NPT Participation.svg: Allstar86, L.tak, Danlaycockderivative work: Danlaycock, CC BY-SA 3.0, via Wikimedia Commons

  (edited to separate figure from legend)
- "Gamma spectrum of the shown Uranium...", Wusel007, CC BY-SA 3.0, via Wikimedia Commons

  (edited to replace uranium image and improve resolution of fonts)
- "Uranium Ore", Andrew Silver, USGS, Public domain, via Wikimedia Commons