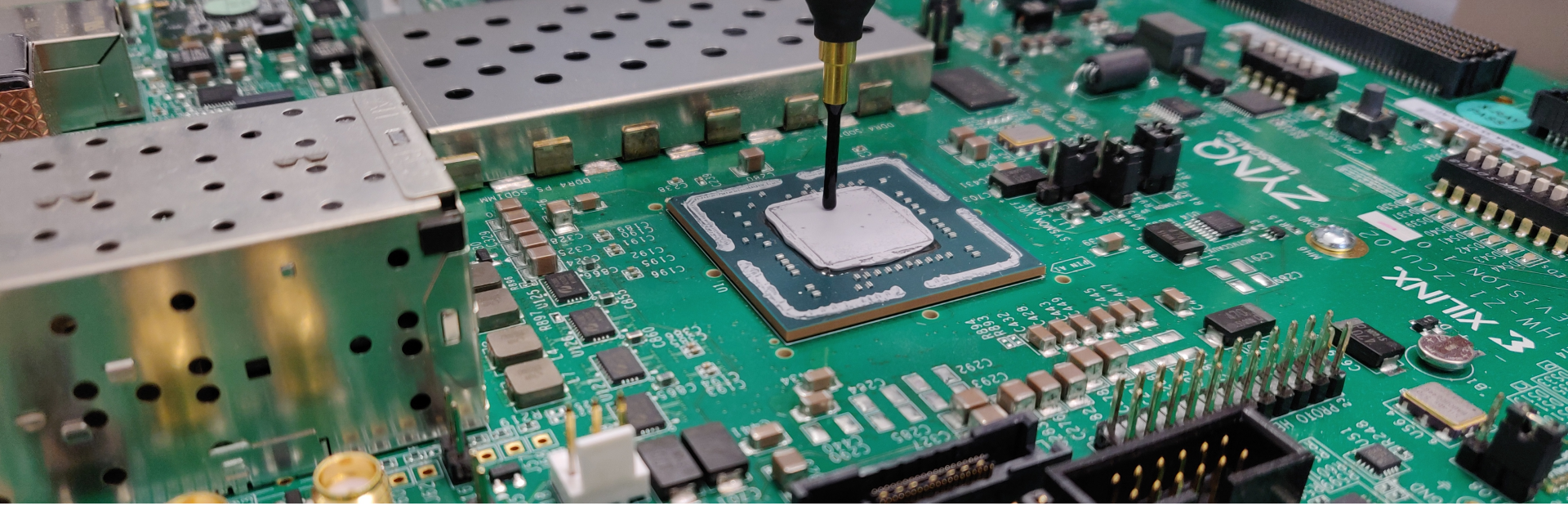


RUHR-UNIVERSITÄT BOCHUM

CASA
Cyber Security in the Age of Large-Scale Adversaries

RUHR UNIVERSITÄT BOCHUM

RUB

WPI

Quantitative Fault Injection Analysis

Jakob Feldtkeller

Tim Güneysu, Patrick Schaumont

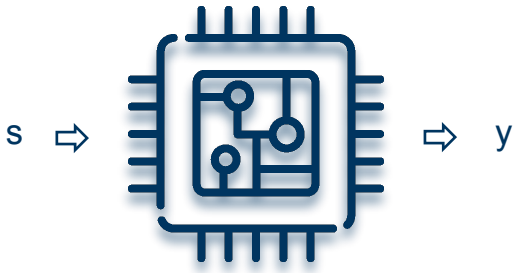
Chair for Security Engineering
Faculty of Computer Science
Ruhr University Bochum

SECURITY ENGINEERING

November 24, 2023

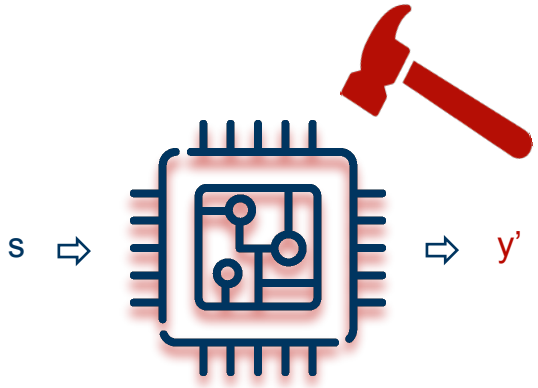
Where Are We?

Fault Attacks



Where Are We?

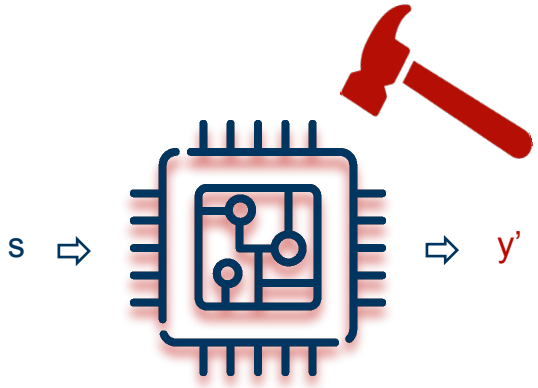
Fault Attacks



Fault-Injection Attacks

Where Are We?

Fault Attacks



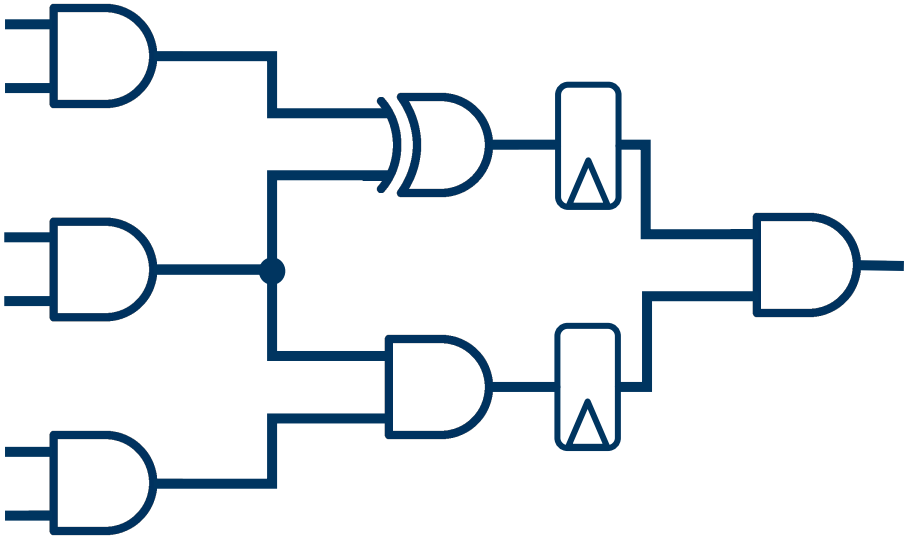
Fault-Injection Attacks

How much information about a secret s can an adversary learn by injecting a fault?

Adversary Model

Secret: s

Public: x



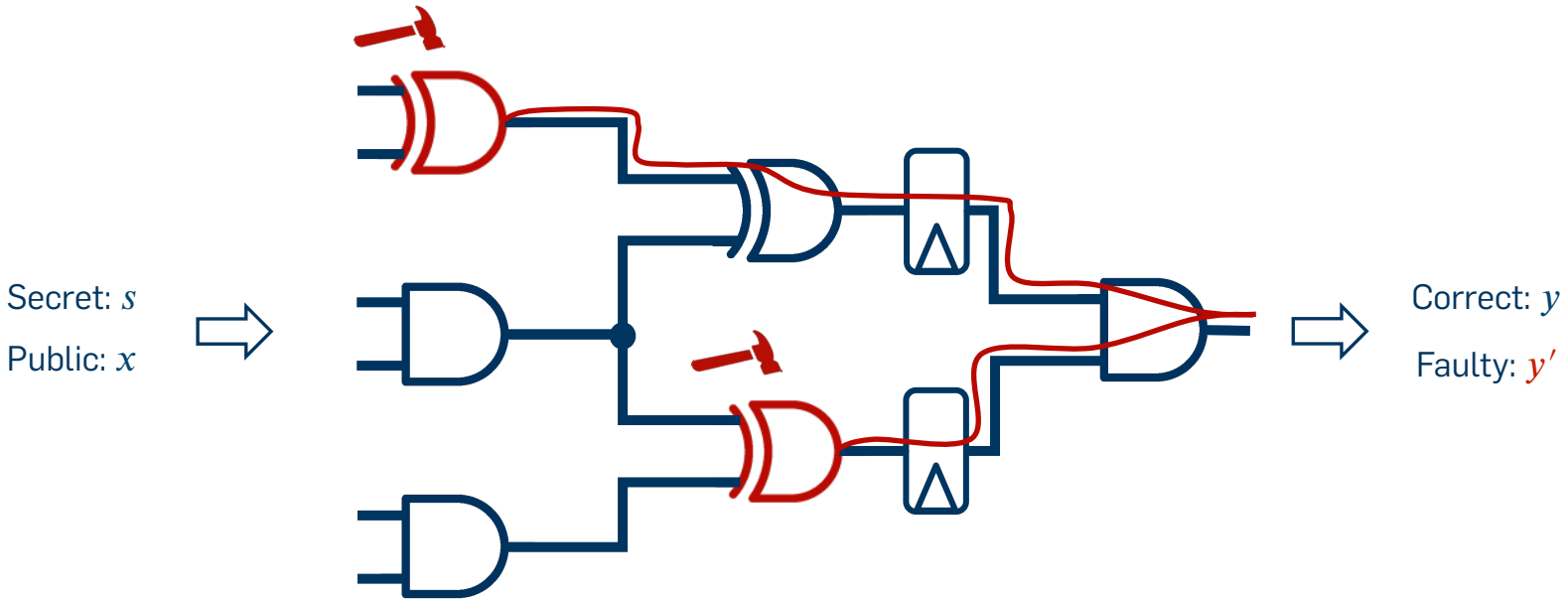
Correct: y

Fault Model:

Predefined set of gate transformations.

[Richter-Brockmann et al, 2022]

Adversary Model

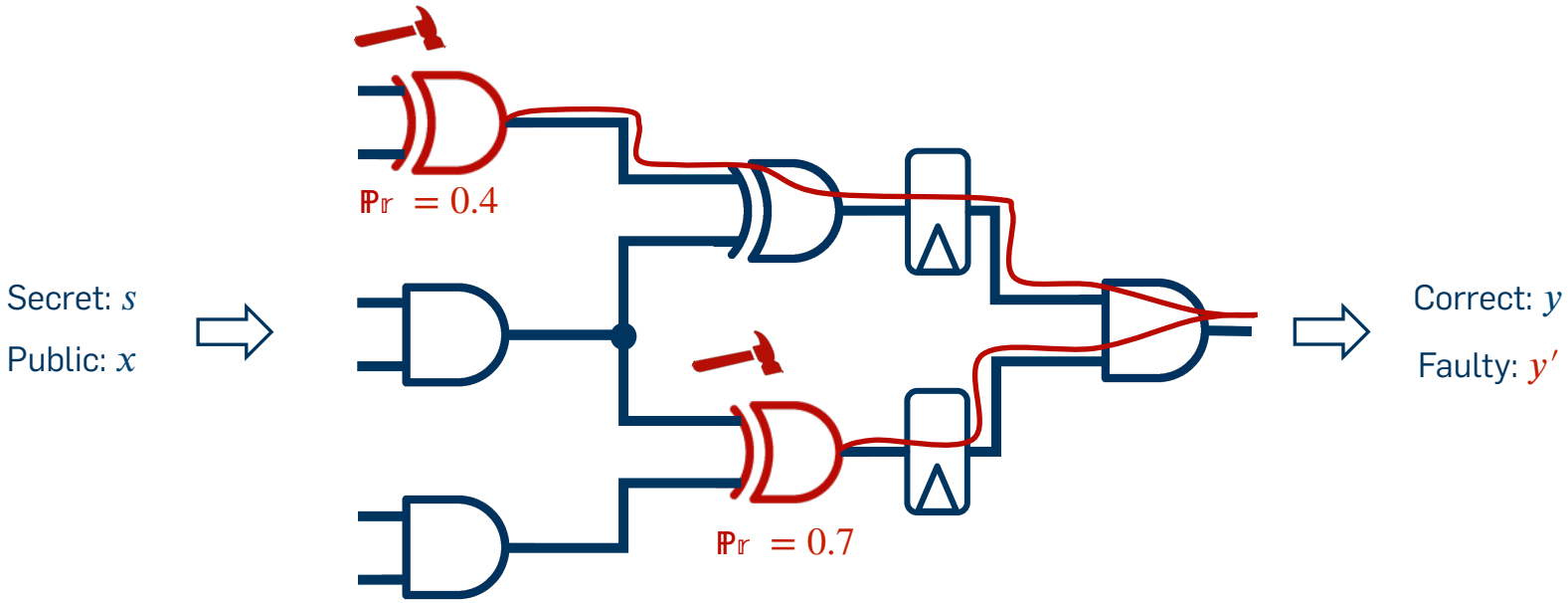


Fault Model:

Predefined set of gate transformations.

[Richter-Brockmann et al, 2022]

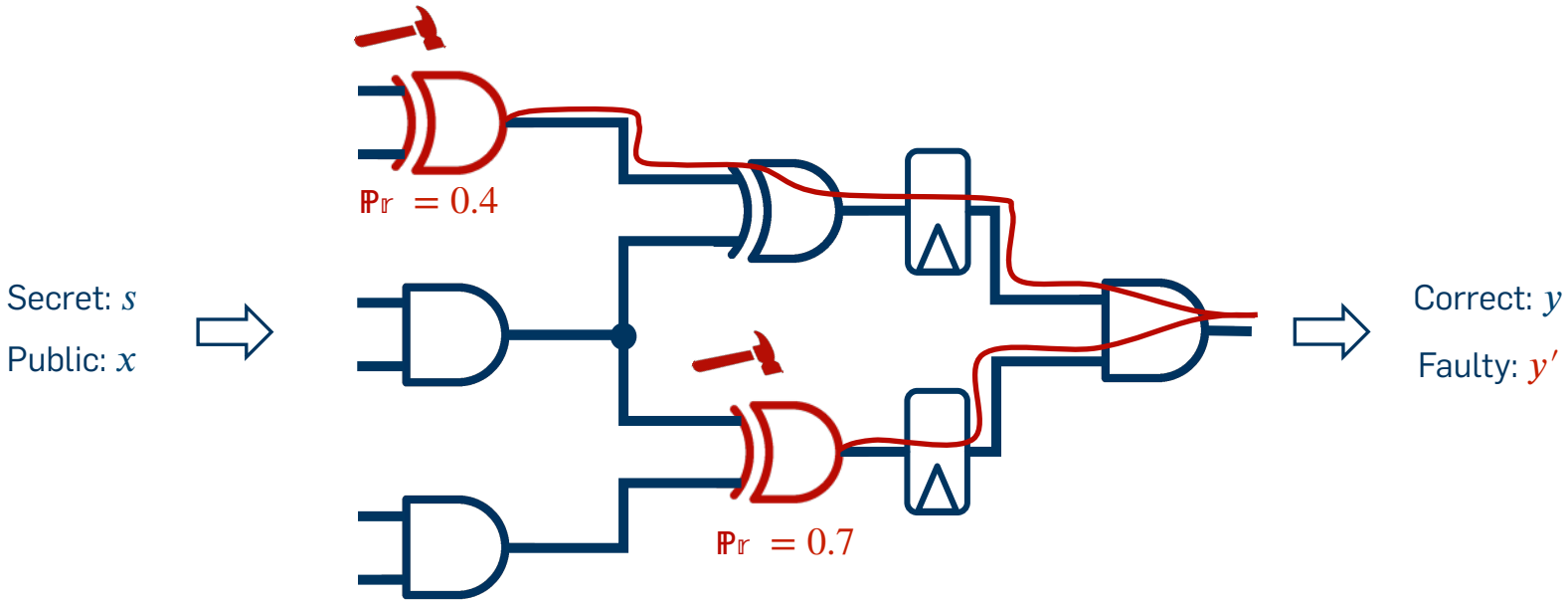
Adversary Model



Fault Model:

Distribution over a predefined set of gate transformations.

Adversary Model



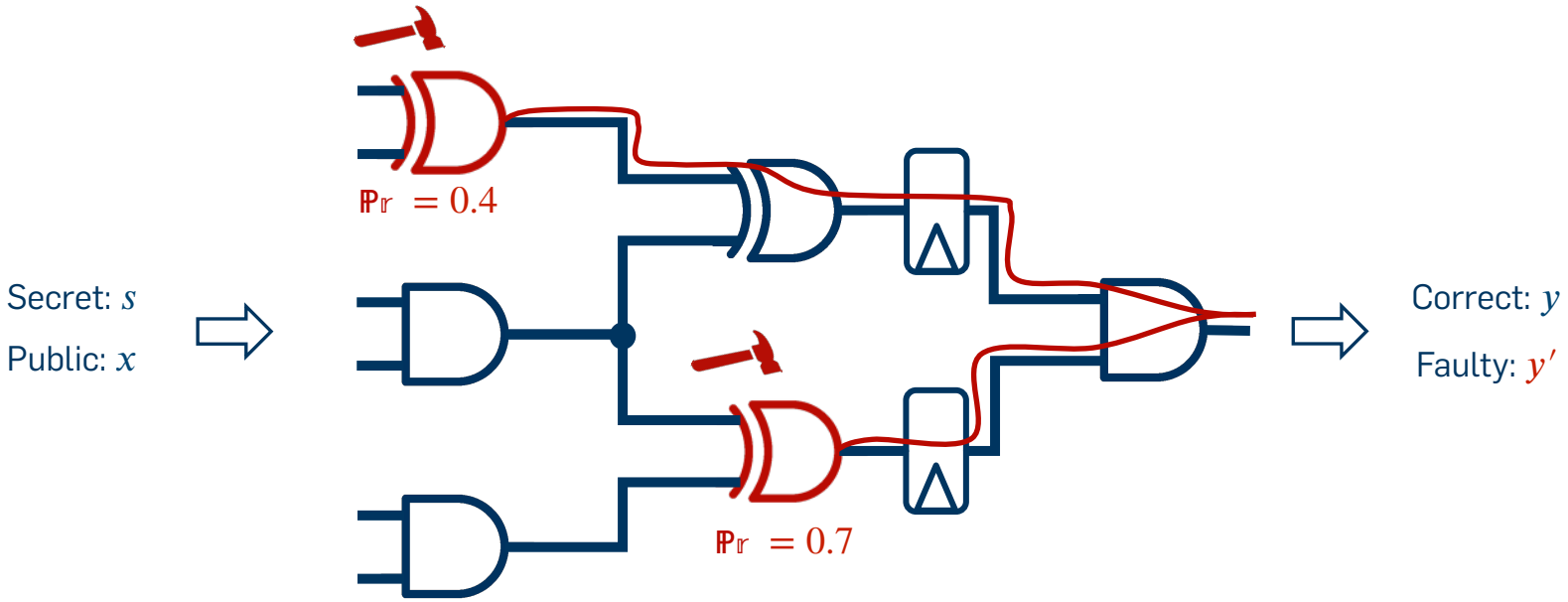
View of Adversary:

$\mathbb{DS}$ $\mathbb{DX}$

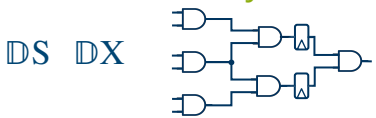
Fault Model:

Distribution over a predefined set of gate transformations.

Adversary Model



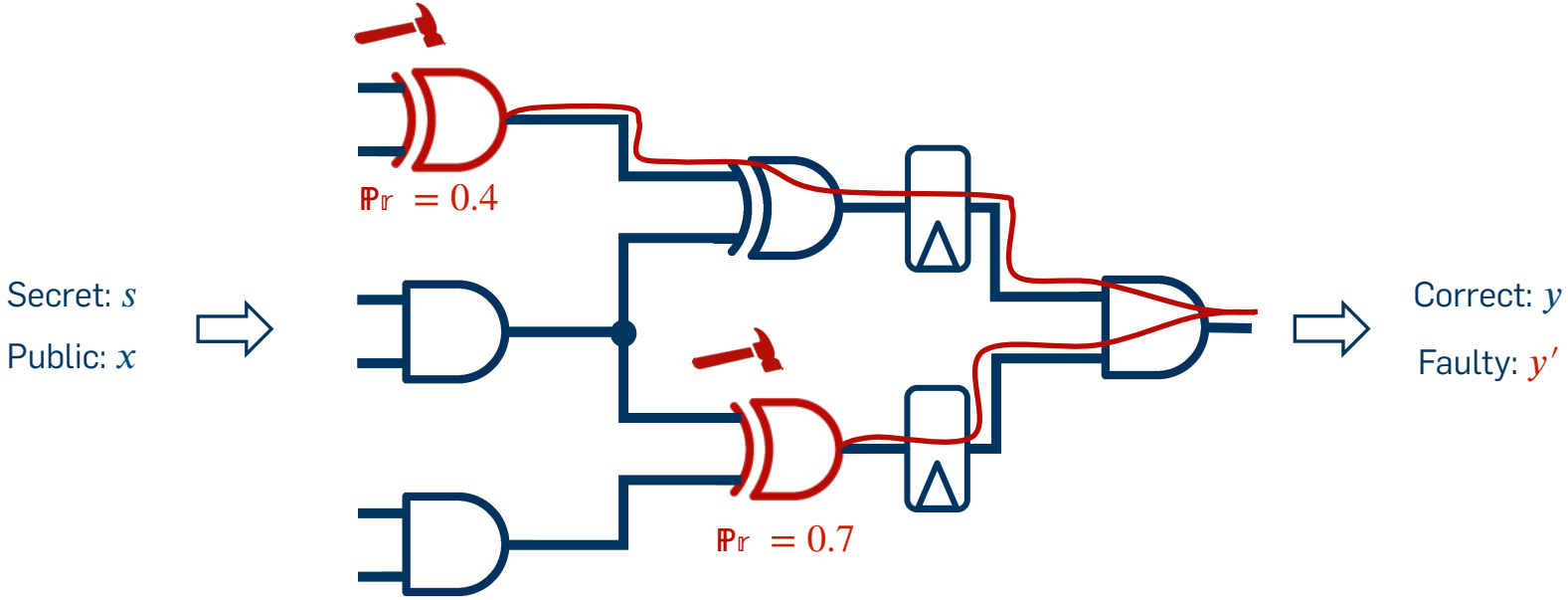
View of Adversary:



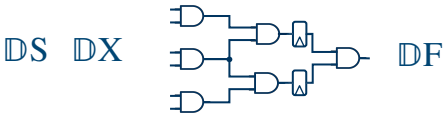
Fault Model:

Distribution over a predefined set of gate transformations.

Adversary Model



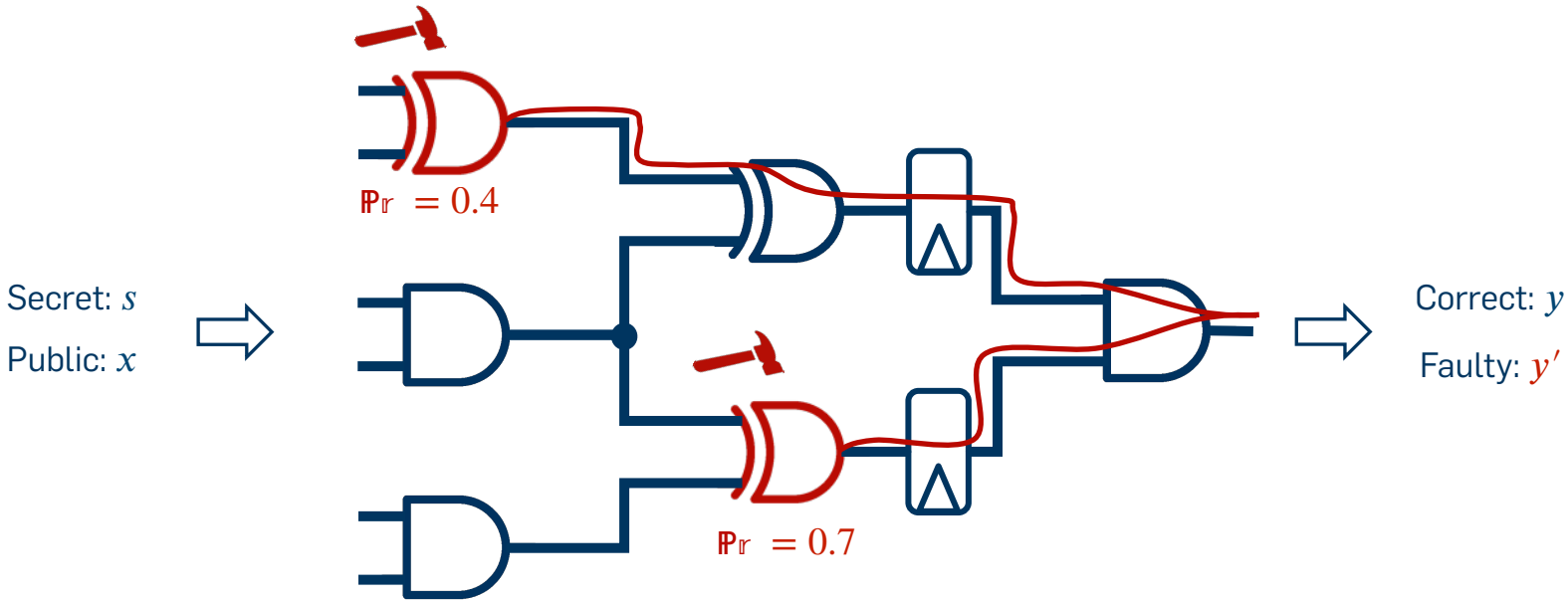
View of Adversary:



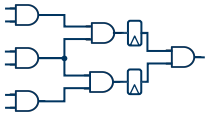
Fault Model:

Distribution over a predefined set of gate transformations.

Adversary Model



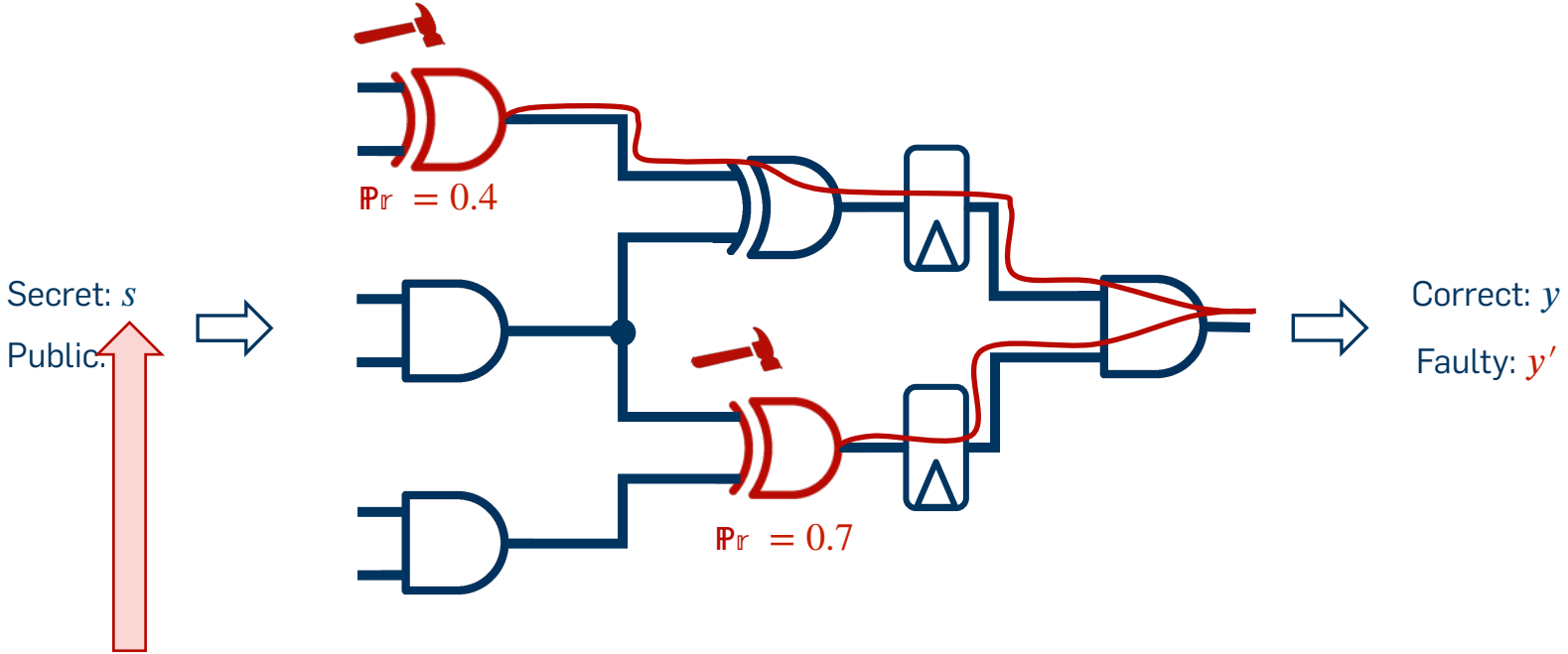
View of Adversary:

$\mathbb{DS}$ $\mathbb{DX}$  $\mathbb{DF}$ y y'

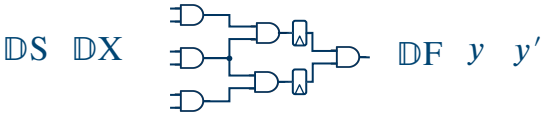
Fault Model:

Distribution over a predefined set of gate transformations.

Adversary Model



View of Adversary:

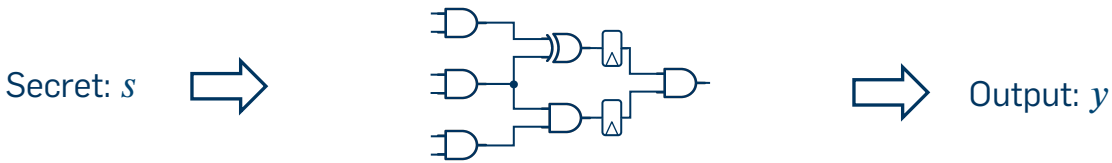


Fault Model:

Distribution over a predefined set of gate transformations.

Quantitative Information-Flow Analysis

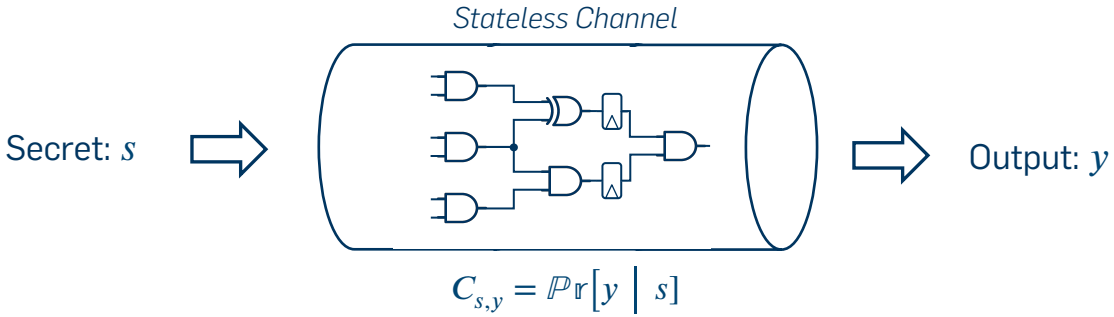
Vulnerability



[Smith, 2009]

Quantitative Information-Flow Analysis

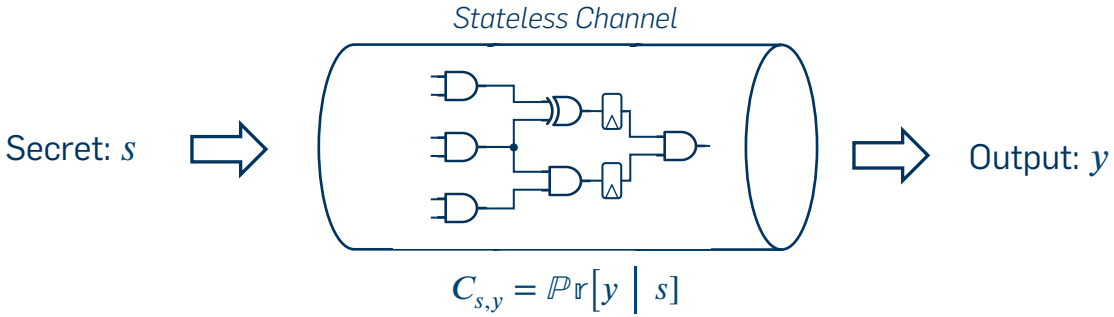
Vulnerability



[Smith, 2009]

Quantitative Information-Flow Analysis

Vulnerability



Vulnerability:

Expected probability that an adversary can guess a secret s.

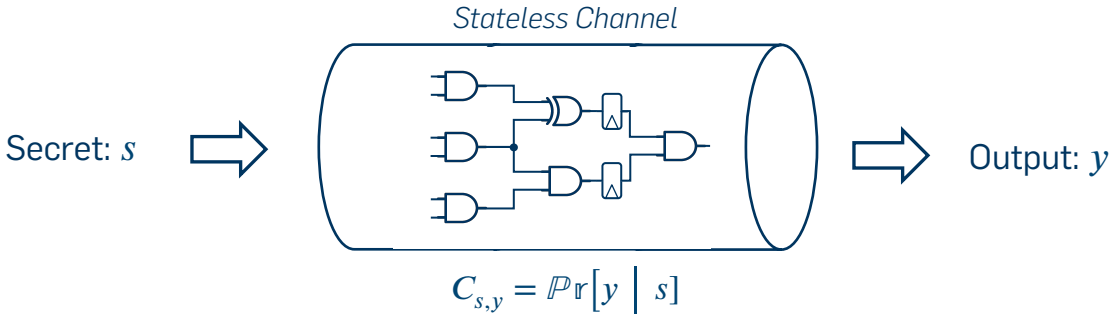
$$V[S] = max_{s \in S}(\mathbb{P}\mathrm{r}[S = s])$$

$$V[S \mid Y] = \sum_{y \in Y} \mathbb{P}\mathrm{r}[Y = y] \bullet max_{s \in S}(\mathbb{P}\mathrm{r}[S = s \mid Y = y])$$

[Smith, 2009]

Quantitative Information-Flow Analysis

Min-Entropy



Min-Entropy:

Remaining uncertainty about the secret in bits.

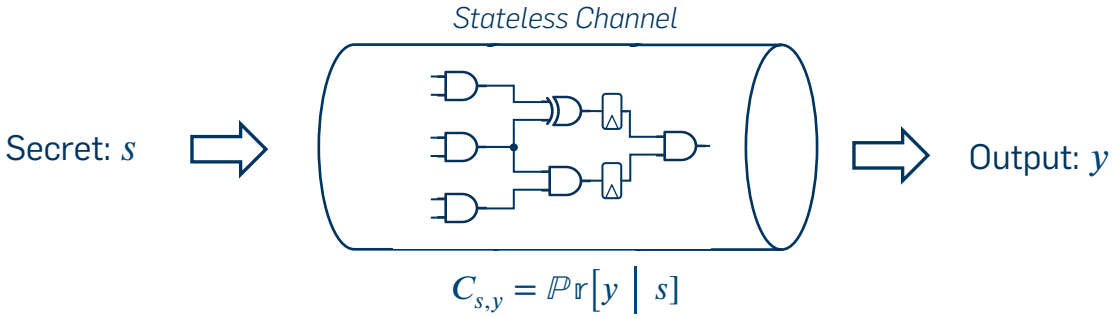
$$H_\infty[S] = log_2\left(\frac{1}{V[S]}\right)$$

$$H_\infty[S \mid Y] = log_2\left(\frac{1}{V[S \mid Y]}\right)$$

[Smith, 2009]

Quantitative Information-Flow Analysis

Information Leakage



Leakage:

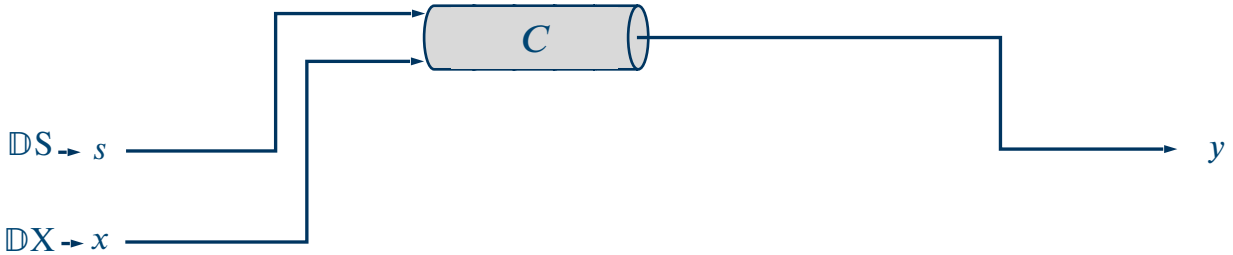
How many bits does an adversary learn about a secret s by observing some output y.

$$L[S \mid Y] = H_\infty[S] - H_\infty[S \mid Y]$$

[Smith, 2009]

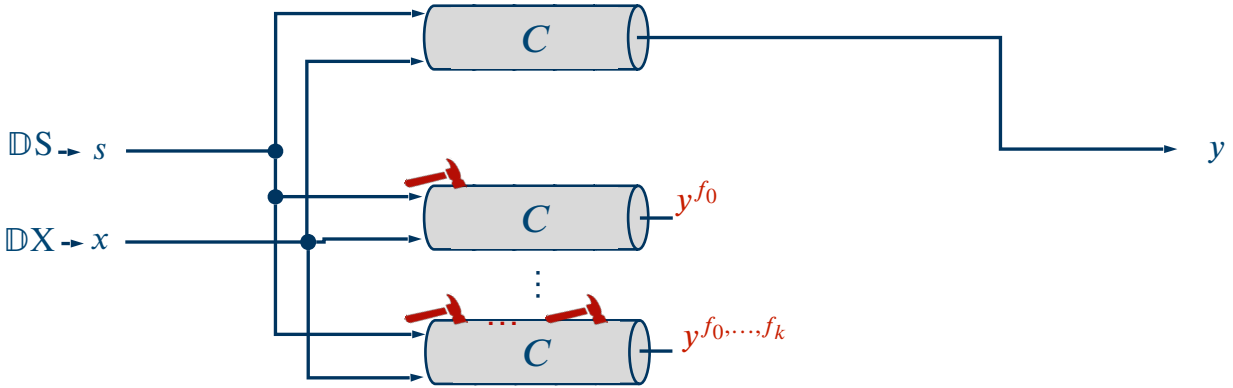
FIA Channel

Construction



FIA Channel

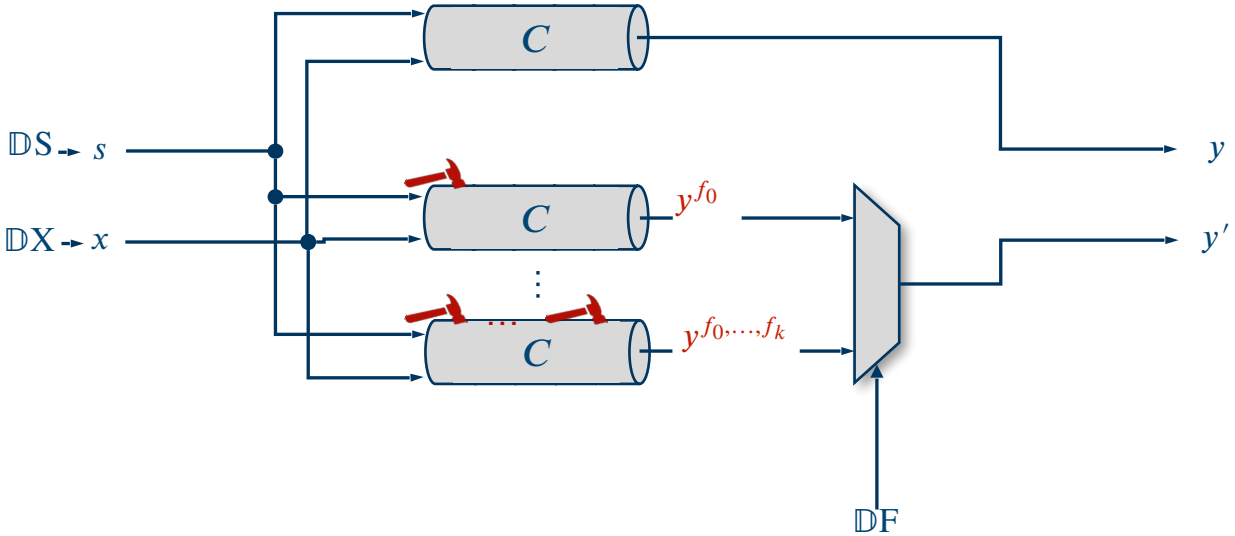
Construction



FIA Channel

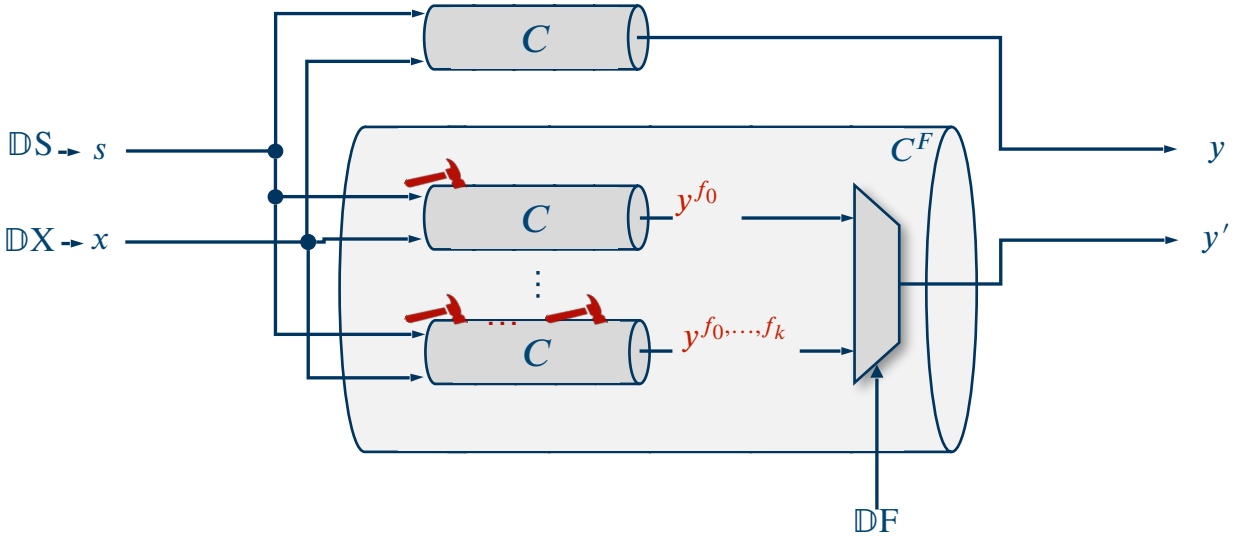
Construction

Stateless Channels



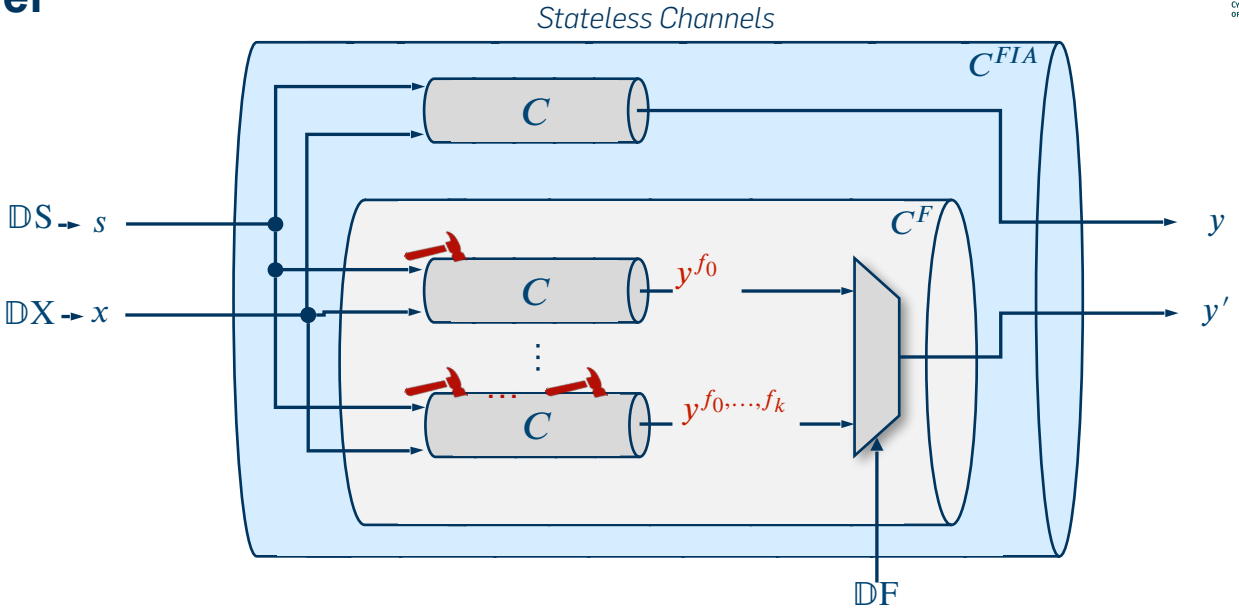
FIA Channel

Construction



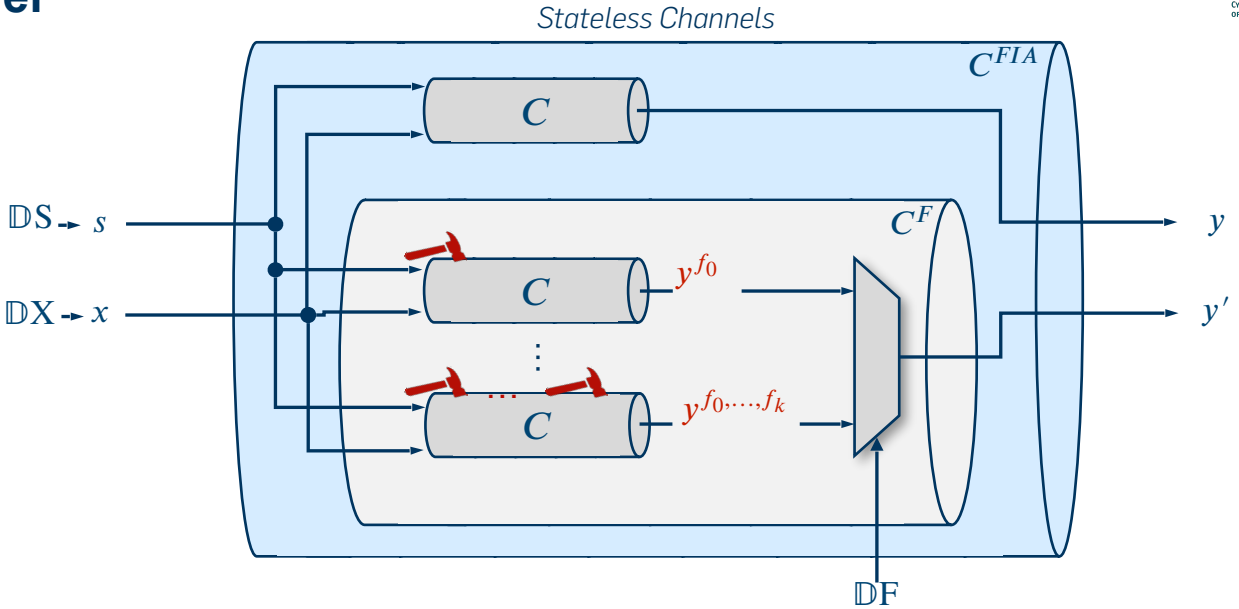
FIA Channel

Construction



FIA Channel

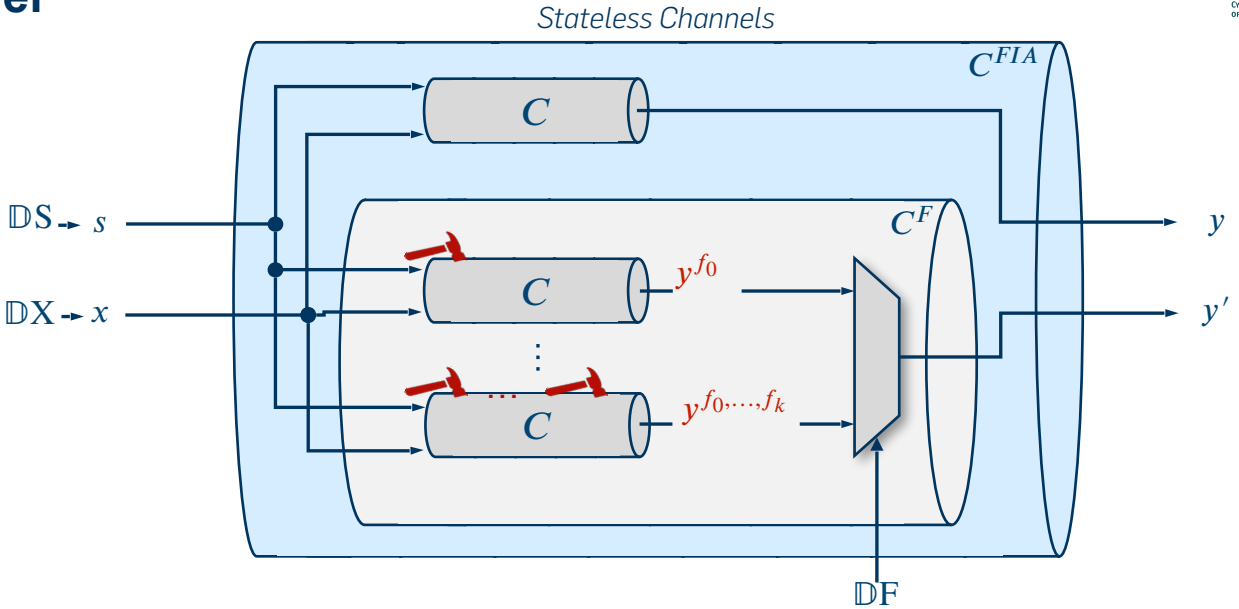
Construction



$$C^{FIA}_{(x,s),(y,y')} = C_{(x,s),y} \sum_{f \in F} \mathbb{P}\mathrm{r}[f] C^{f}_{(x,s),y'}$$

FIA Channel

Construction

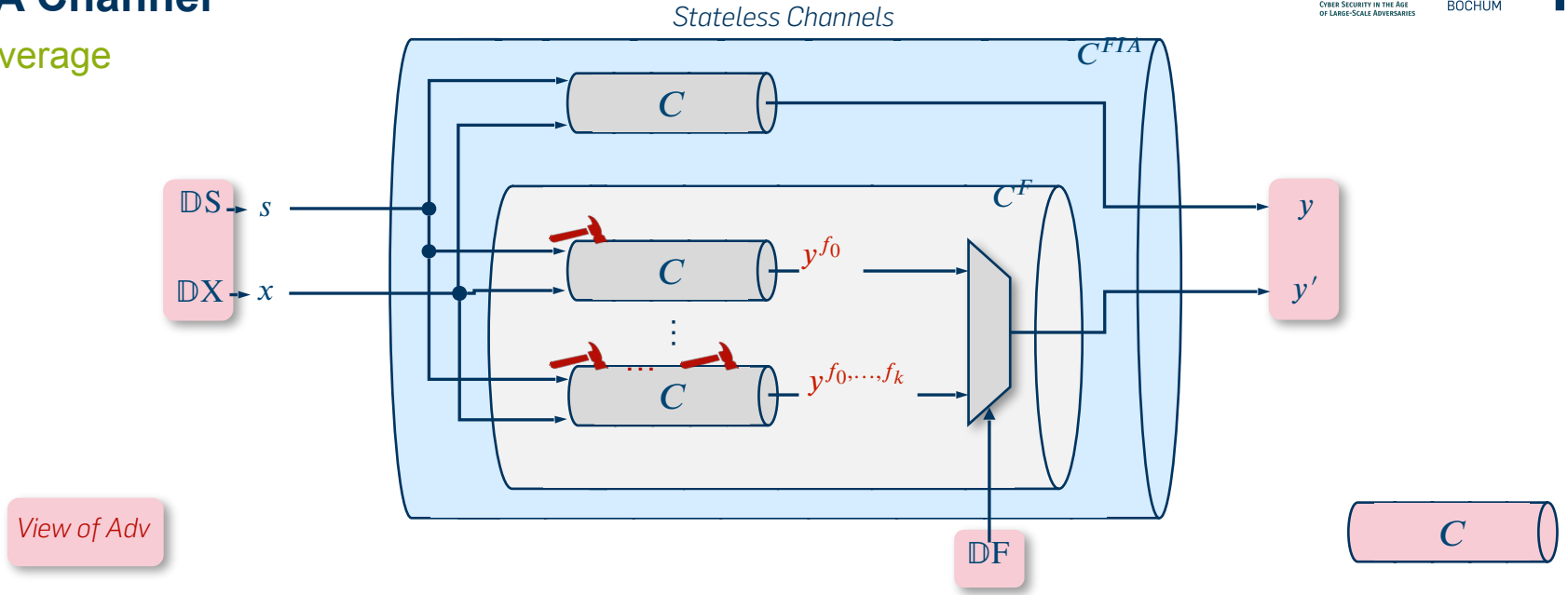


$$C^{FIA}_{(x,s),(y,y')} = C_{(x,s),y} \sum_{f \in F} \mathbb{P}r[f] C^{f}_{(x,s),y'}$$

$$V[S \mid Y, Y'] = \sum_{y,y'} max_s \left(\sum_{x} \mathbb{P}r[s]\mathbb{P}r[x]\mathbb{P}r[y \mid x, s] \sum_{f} \mathbb{P}r[f]\mathbb{P}r[y' \mid x, s] \right)$$

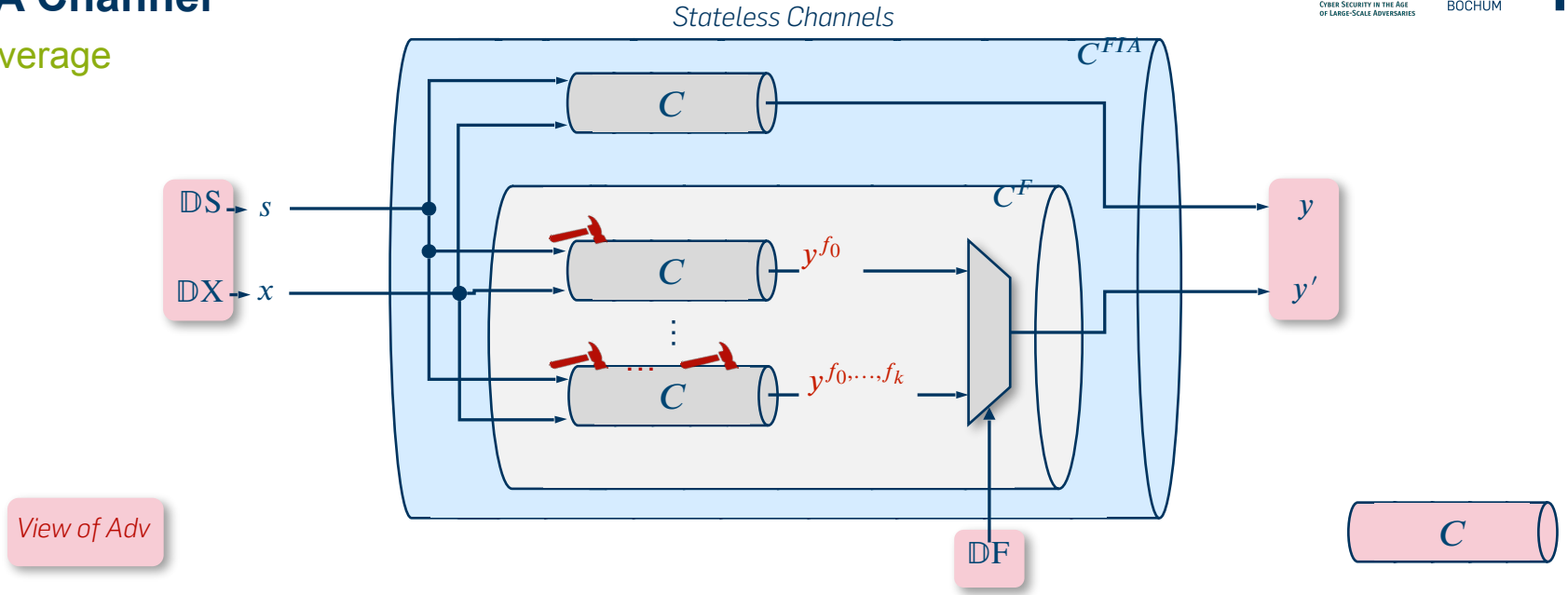
FIA Channel

Coverage



FIA Channel

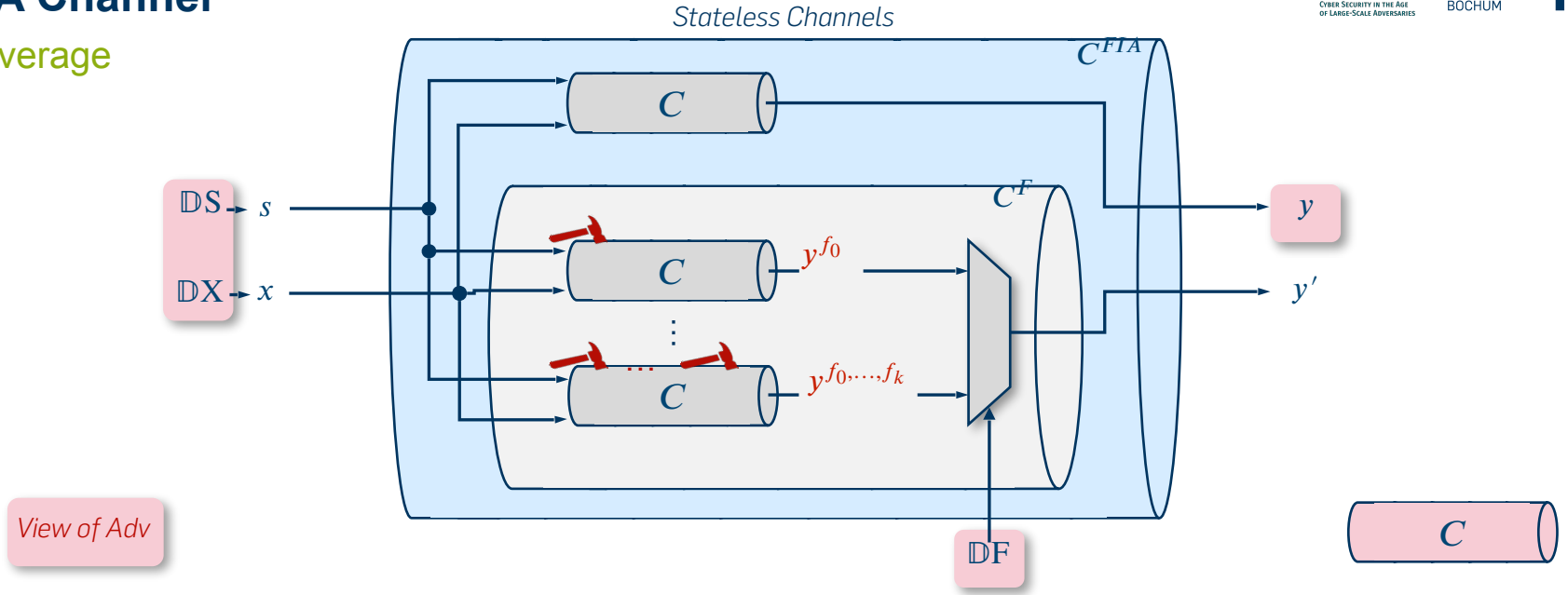
Coverage



✓ Adv has access to pair (y, y').

FIA Channel

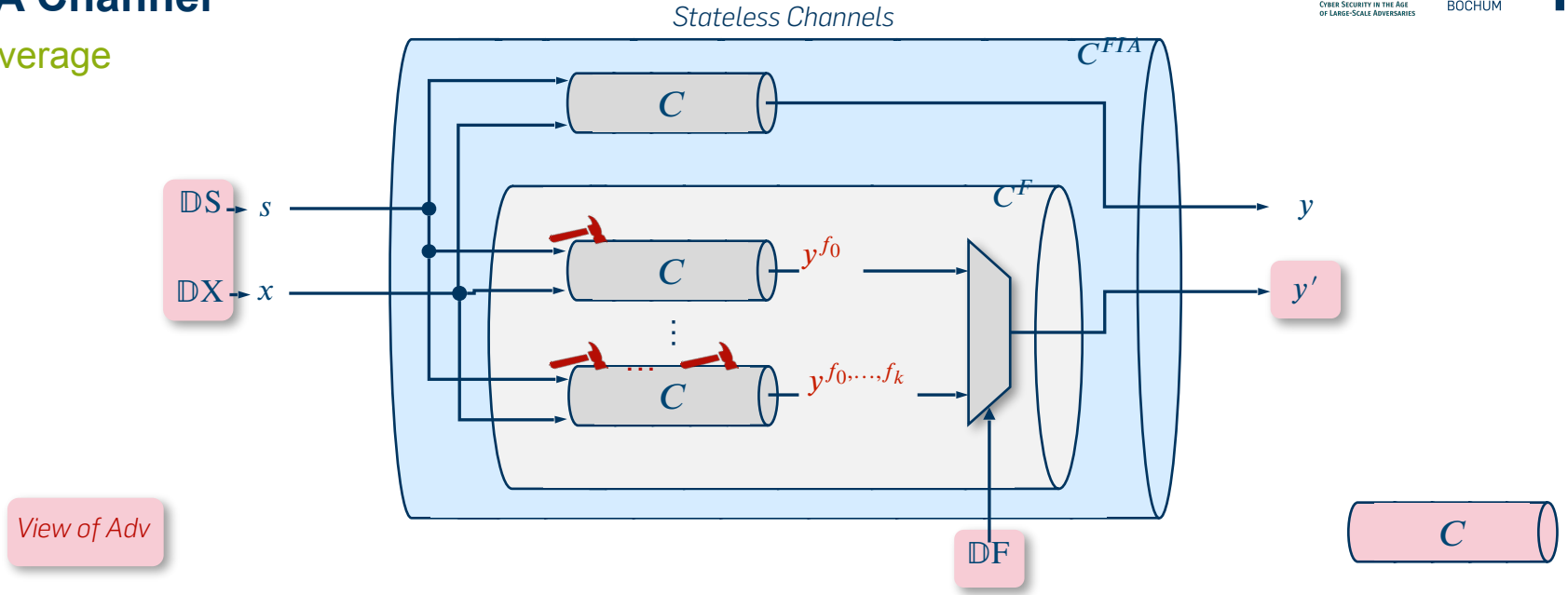
Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.

FIA Channel

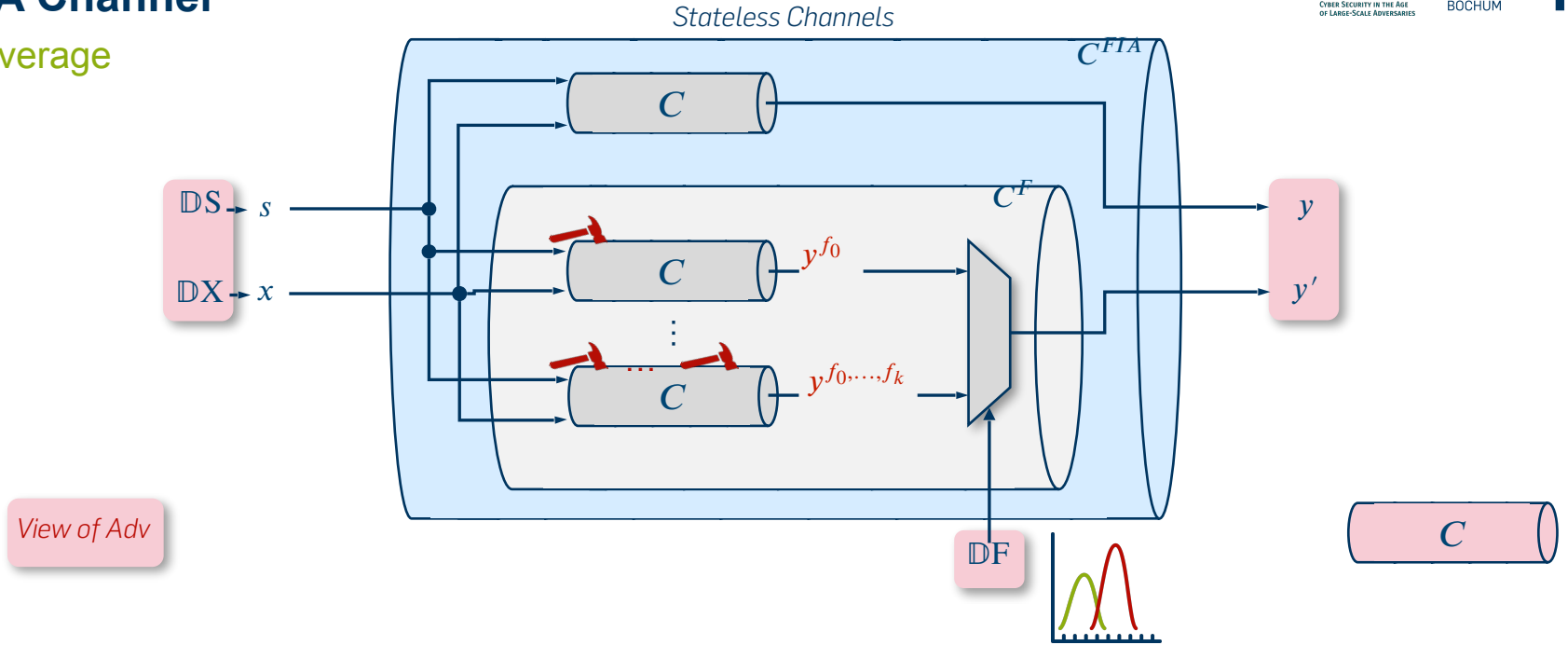
Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.
- ✓ Adv has access to y'.

FIA Channel

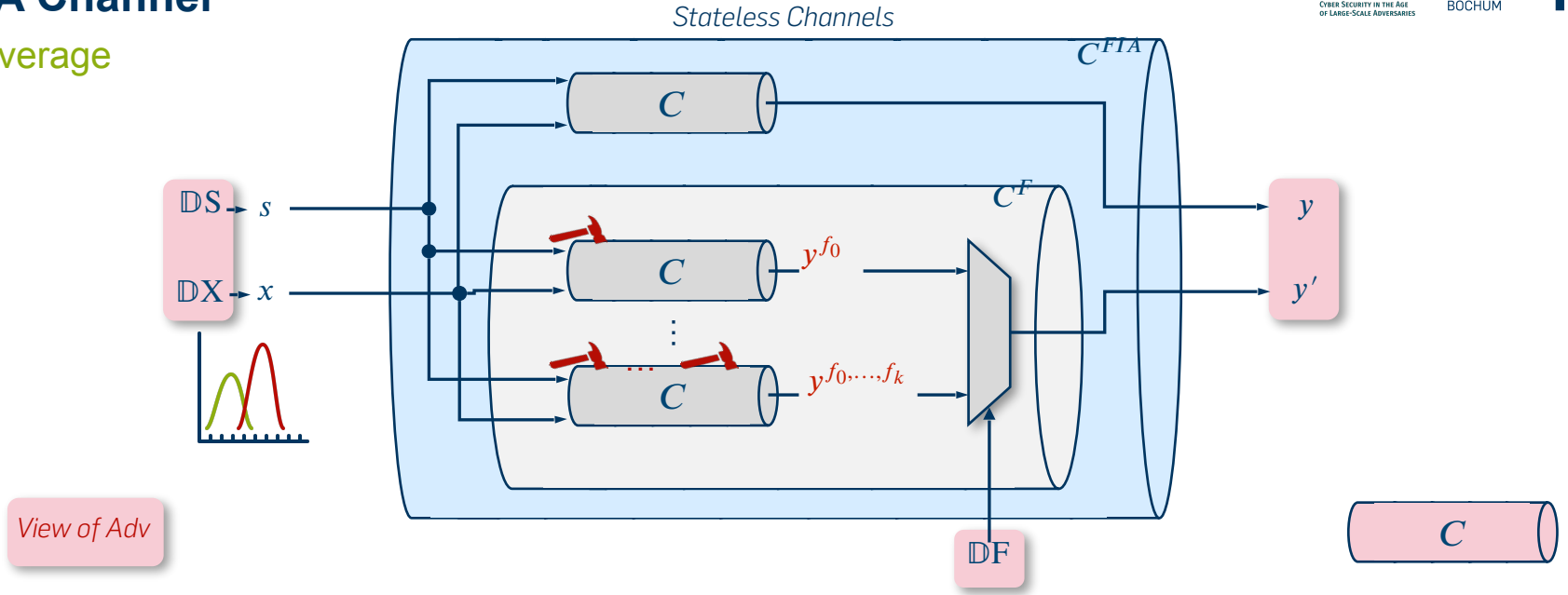
Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.
- ✓ Adv has access to y'.
- ✓ Precise/imprecise faults.

FIA Channel

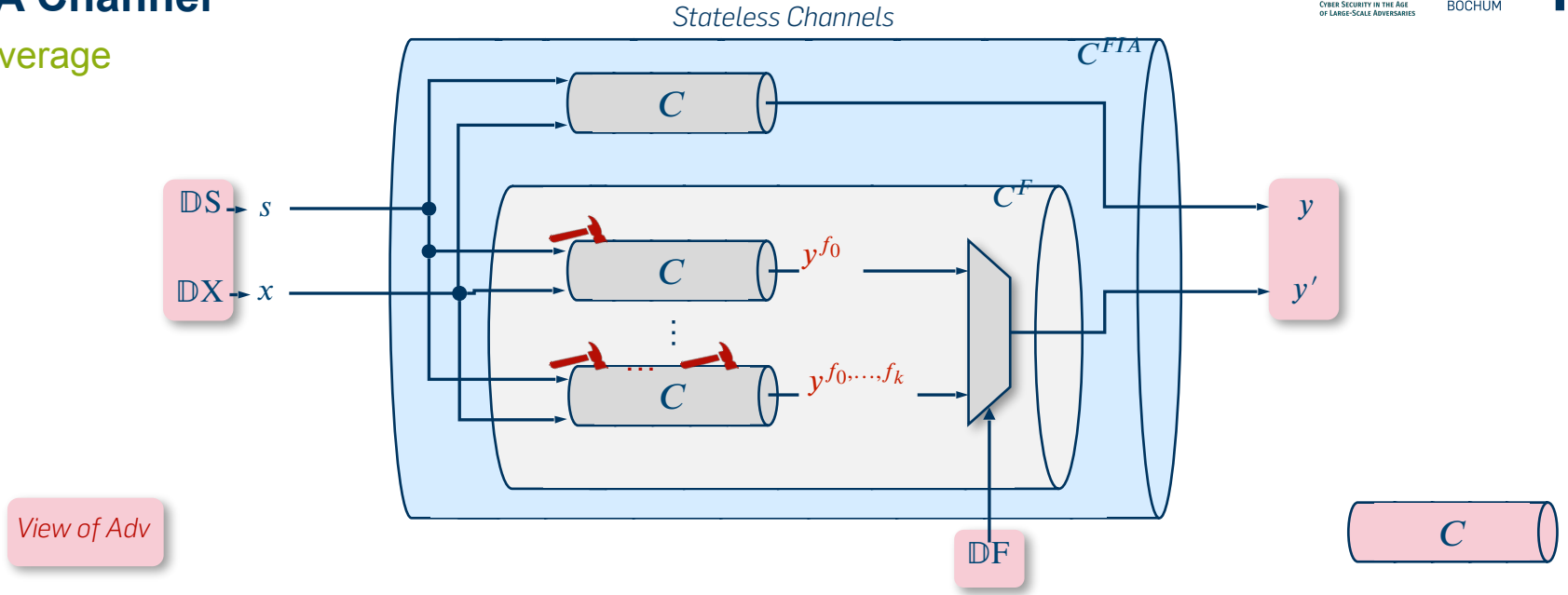
Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.
- ✓ Adv has access to y'.
- ✓ Precise/imprecise faults.
- ✓ Known/unknown "public" input.

FIA Channel

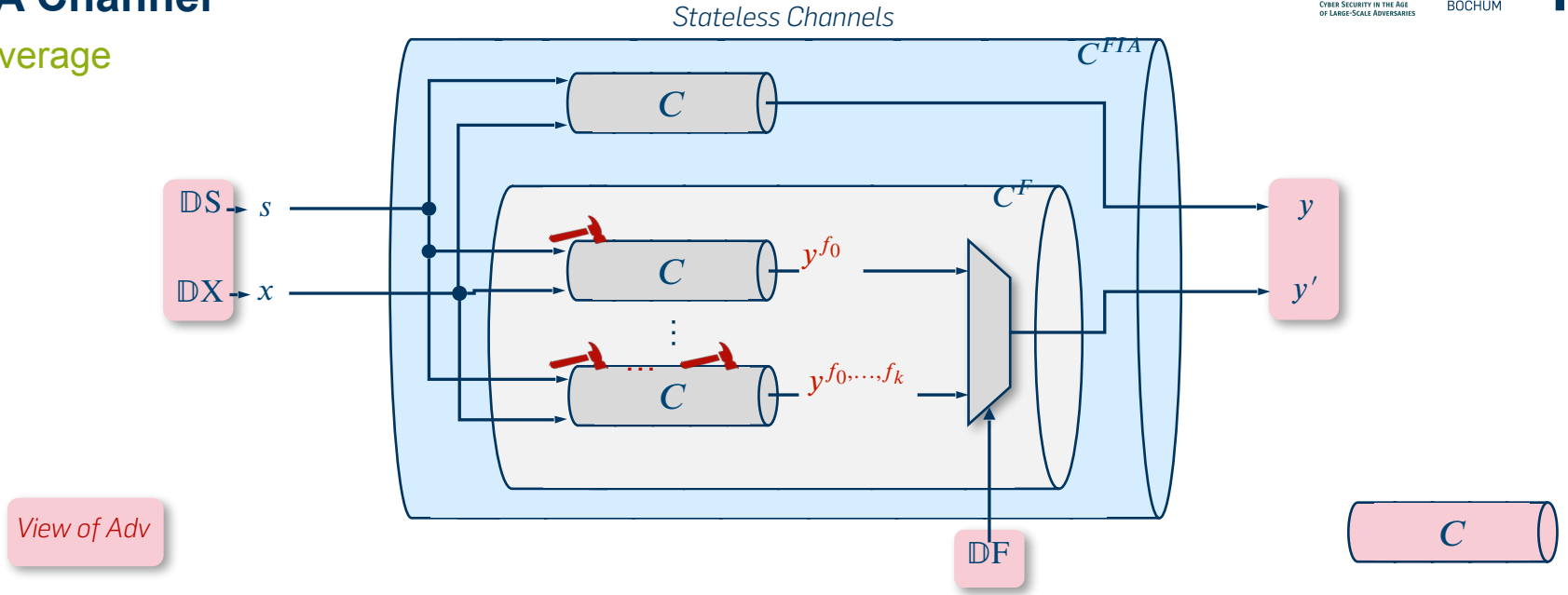
Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.
- ✓ Adv has access to y'.
- ✓ Precise/imprecise faults.
- ✓ Known/unknown "public" input.
- × Adv has access to multiple pairs (y_i, y'_i).

FIA Channel

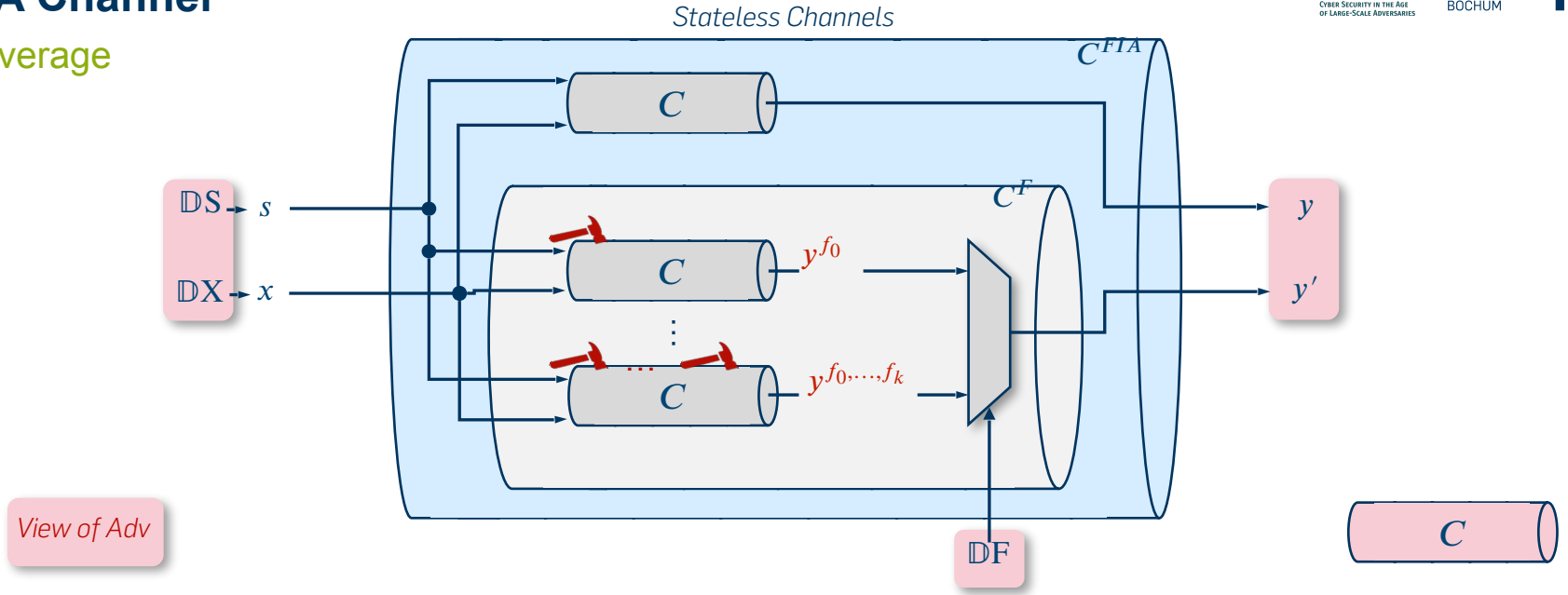
Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.
- ✓ Adv has access to y'.
- ✓ Precise/imprecise faults.
- ✓ Known/unknown "public" input.
- × Adv has access to multiple pairs (y_i, y'_i).
- × Adv has access to multiple y'_i.

FIA Channel

Coverage



- ✓ Adv has access to pair (y, y').
- ✓ Adv has access to y.
- ✓ Adv has access to y'.
- ✓ Precise/imprecise faults.
- ✓ Known/unknown "public" input.
- × Adv has access to multiple pairs (y_i, y'_i).
- × Adv has access to multiple y'_i.
- × Countermeasures that rely on the state of C.

Computation

Circuit Representation

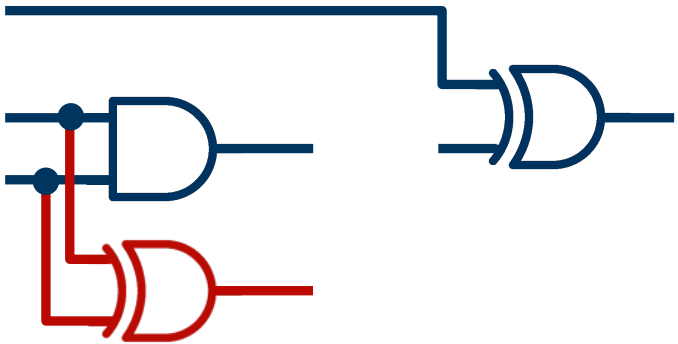
Circuit Transformation

Circuit Representation

Circuit Transformation

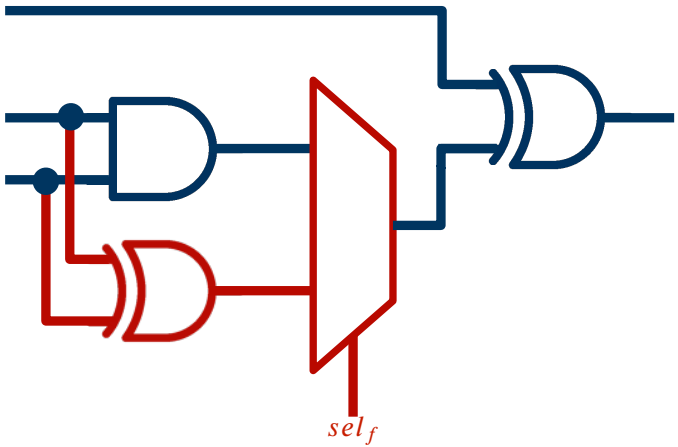
Circuit Representation

Circuit Transformation



Circuit Representation

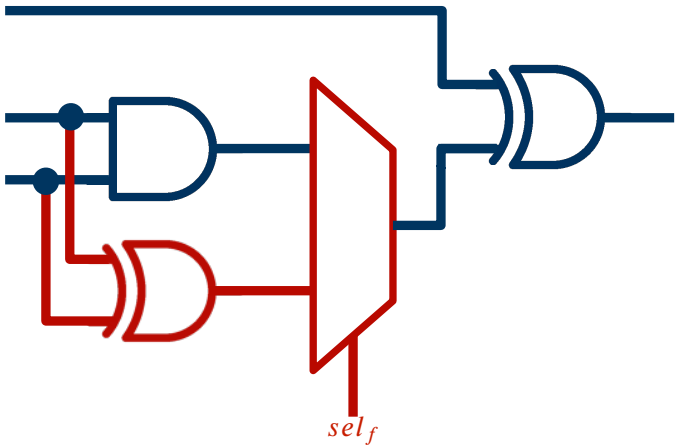
Circuit Transformation



Input signals for fault selection.

Circuit Representation

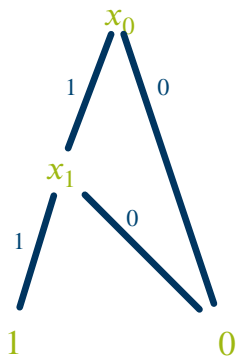
Circuit Transformation



Input signals for fault selection.

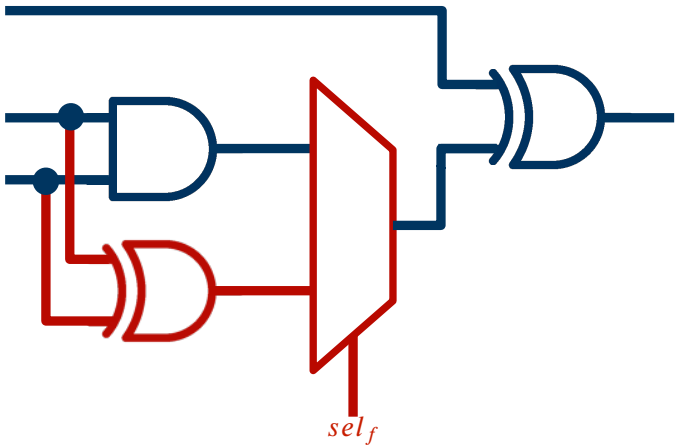
Circuit as BDD

Inputs: $x_0 \wedge x_1$



Circuit Representation

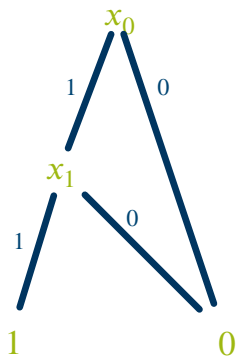
Circuit Transformation



Input signals for fault selection.

Circuit as BDD

Inputs: $x_0 \wedge x_1$



Easy retrieval of satisfying assignments.

Vulnerability Computation

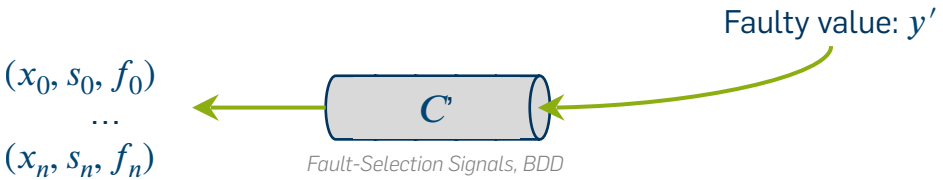
Based on BBD

Faulty value: y'

Implementation in VERICA [Richter-Brockmann et al. 2022]

Vulnerability Computation

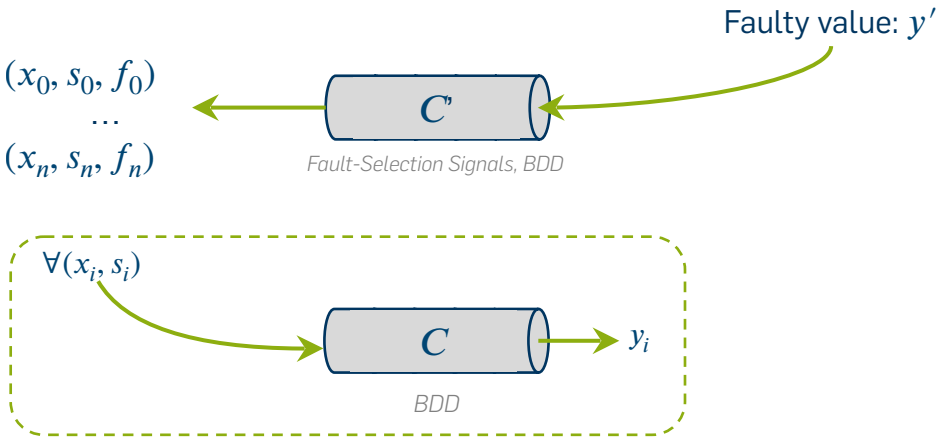
Based on BBD



Implementation in VERICA [Richter-Brockmann et al. 2022]

Vulnerability Computation

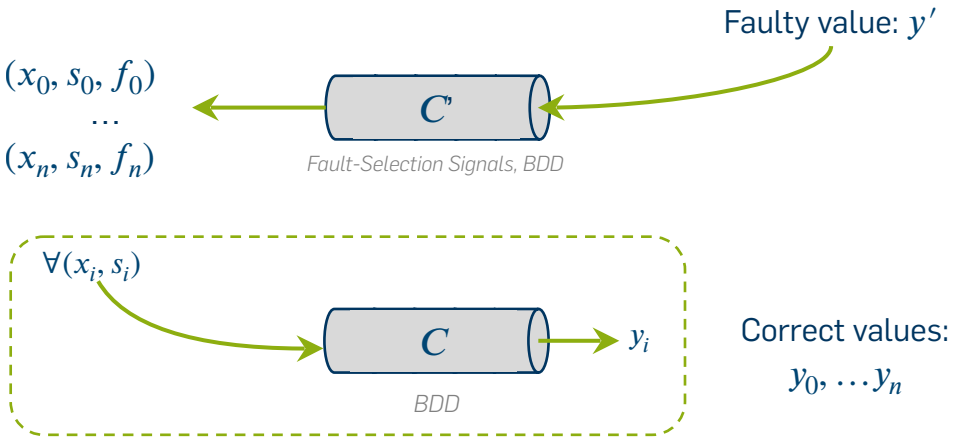
Based on BBD



Implementation in VERICA [Richter-Brockmann et al. 2022]

Vulnerability Computation

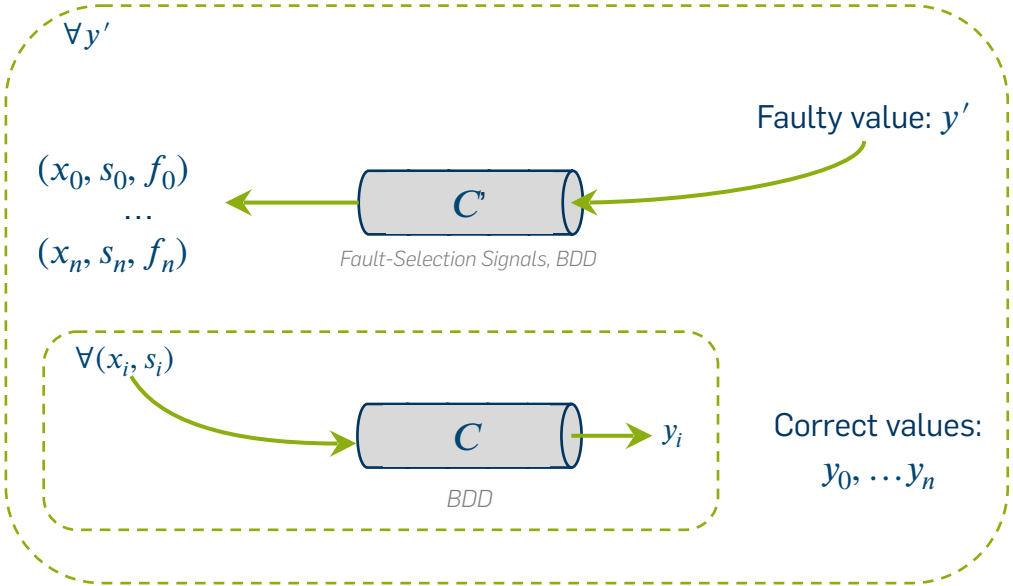
Based on BBD



Implementation in VERICA [Richter-Brockmann et al. 2022]

Vulnerability Computation

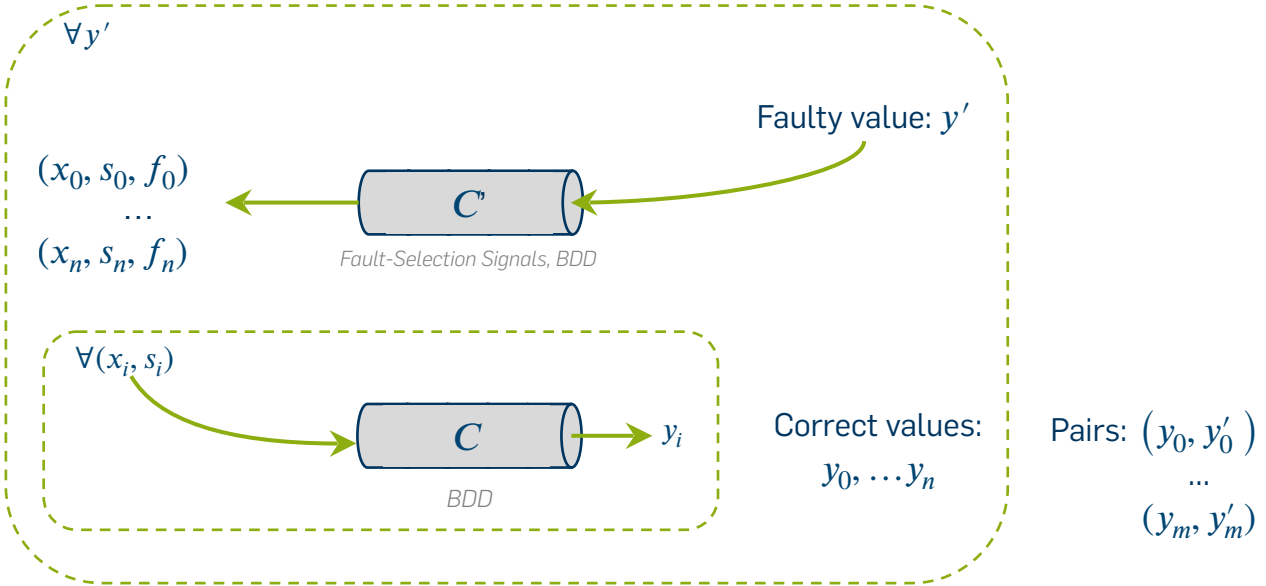
Based on BBD



Implementation in VERICA [Richter-Brockmann et al. 2022]

Vulnerability Computation

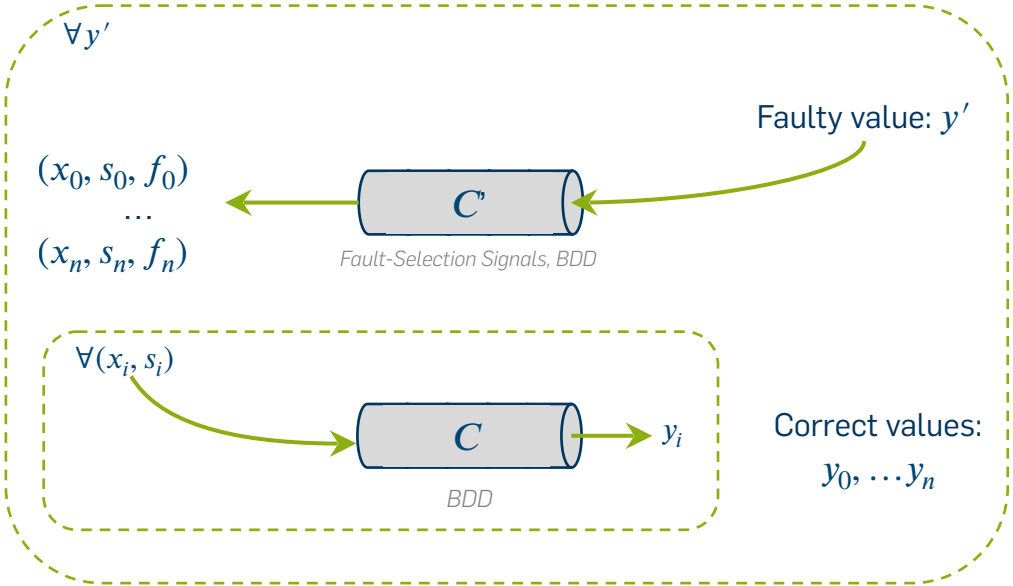
Based on BBD



Implementation in VERICA [Richter-Brockmann et al. 2022]

Vulnerability Computation

Based on BBD



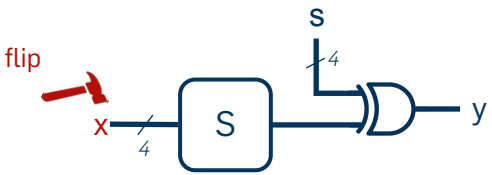
$$\Longrightarrow V[S \mid Y, Y']$$

Implementation in VERICA [Richter-Brockmann et al. 2022]

Evaluation

Differential Fault Analysis

Vulnerability Evaluation

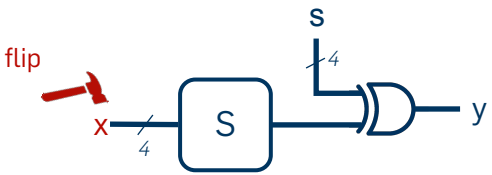


	Fault location	PRESENT L	PRESENT Key Candidates	DEFAULT L	DEFAULT Key Candidates
input	-	0.000	256×16	0.000	256×16
	$x_0\ x_1\ x_2\ x_3$	2.000	256×4	0.000	256×16
	x_0	2.000	256×4	1.000	256×8
	$x_0\ x_3$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_0\ x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_3	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_1	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	x_2	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_2\ x_3$	3.000	256×2	1.000	256×8

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$, $\mathsf{L}^{max}_{DEFAULT} = 4$.

Differential Fault Analysis

Vulnerability Evaluation

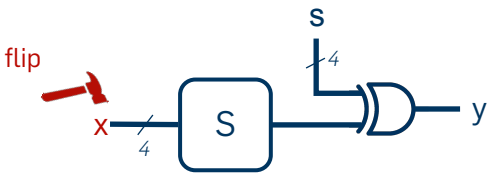


	Fault location	PRESENT L	PRESENT Key Candidates	DEFAULT L	DEFAULT Key Candidates
input	-	0.000	256×16	0.000	256×16
	$x_0\ x_1\ x_2\ x_3$	2.000	256×4	0.000	256×16
	x_0	2.000	256×4	1.000	256×8
	$x_0\ x_3$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_0\ x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_3	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_1	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	x_2	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_2\ x_3$	3.000	256×2	1.000	256×8

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$, $\mathsf{L}^{max}_{DEFAULT} = 4$.

Differential Fault Analysis

Vulnerability Evaluation

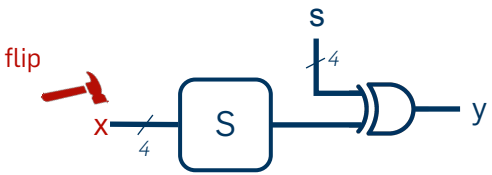


	Fault location	PRESENT L	PRESENT Key Candidates	DEFAULT L	DEFAULT Key Candidates
input	-	0.000	256×16	0.000	256×16
	$x_0\ x_1\ x_2\ x_3$	2.000	256×4	0.000	256×16
	x_0	2.000	256×4	1.000	256×8
	$x_0\ x_3$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_0\ x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_3	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_1	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	x_2	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_2\ x_3$	3.000	256×2	1.000	256×8

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$, $\mathsf{L}^{max}_{DEFAULT} = 4$.

Differential Fault Analysis

Vulnerability Evaluation

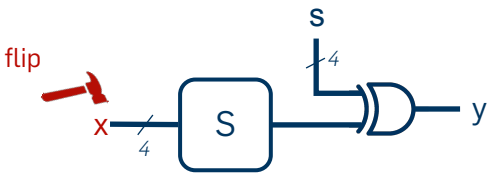


	Fault location	PRESENT L	PRESENT Key Candidates	DEFAULT L	DEFAULT Key Candidates
input	-	0.000	256×16	0.000	256×16
	$x_0\ x_1\ x_2\ x_3$	2.000	256×4	0.000	256×16
	x_0	2.000	256×4	1.000	256×8
	$x_0\ x_3$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_0\ x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_3	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_1	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	x_2	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_2\ x_3$	3.000	256×2	1.000	256×8

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$, $\mathsf{L}^{max}_{DEFAULT} = 4$.

Differential Fault Analysis

Vulnerability Evaluation

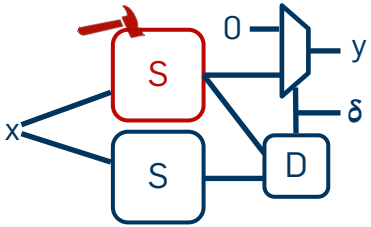


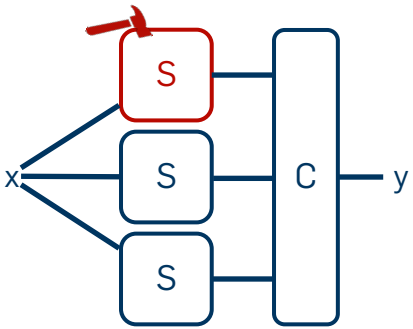
	Fault location	PRESENT L	PRESENT Key Candidates	DEFAULT L	DEFAULT Key Candidates
input	-	0.000	256×16	0.000	256×16
	$x_0\ x_1\ x_2\ x_3$	2.000	256×4	0.000	256×16
	x_0	2.000	256×4	1.000	256×8
	$x_0\ x_3$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	0.000	256×16
	$x_0\ x_1\ x_2$	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_3	2.585	$128 \times 2, 128 \times 4$	1.000	256×8
	x_1	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	x_2	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_1\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_0\ x_2\ x_3$	2.807	$192 \times 2, 64 \times 4$	1.000	256×8
	$x_1\ x_2\ x_3$	3.000	256×2	1.000	256×8

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$, $\mathsf{L}^{max}_{DEFAULT} = 4$.

Statistical Ineffective Fault Analysis

Vulnerability Evaluation



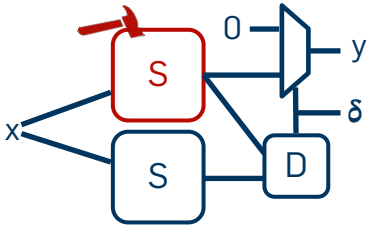


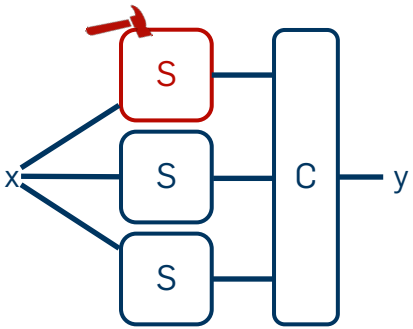
	Fault		Metric L				
	location	type	Plain	Detection (both - y, δ)	Detection (no flag - y)	Detection (flag only - δ)	Correction
input max	x_2	set	3.000	1.000	0.954	0.000	0.000
	x_2	reset	3.000	1.000	0.954	0.000	0.000
	x_2	flip	2.807	0.000	0.000	0.000	0.000
internal max	inv(x_1)	set	3.000	1.000	0.954	0.000	0.000
	inv(x_1)	reset	3.000	1.000	0.954	0.000	0.000
	and$(x_2, \bar{x}_1)$	flip	3.000	1.000	0.954	0.000	0.000

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$.

Statistical Ineffective Fault Analysis

Vulnerability Evaluation



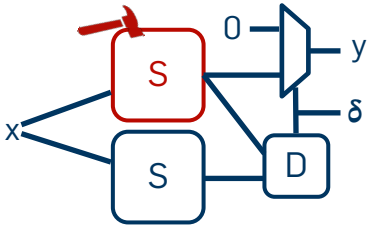


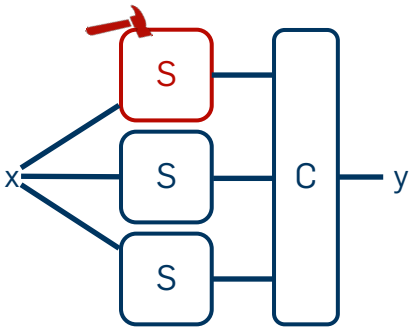
	Fault		Metric L				
	location	type	Plain	Detection (both - y, δ)	Detection (no flag - y)	Detection (flag only - δ)	Correction
input max	x_2	set	3.000	1.000	0.954	0.000	0.000
	x_2	reset	3.000	1.000	0.954	0.000	0.000
	x_2	flip	2.807	0.000	0.000	0.000	0.000
internal max	inv(x_1)	set	3.000	1.000	0.954	0.000	0.000
	inv(x_1)	reset	3.000	1.000	0.954	0.000	0.000
	and$(x_2, \bar{x}_1)$	flip	3.000	1.000	0.954	0.000	0.000

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$.

Statistical Ineffective Fault Analysis

Vulnerability Evaluation



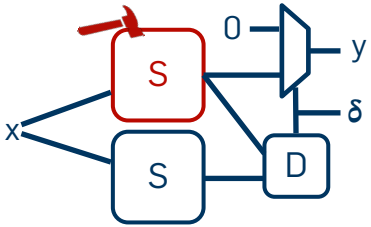


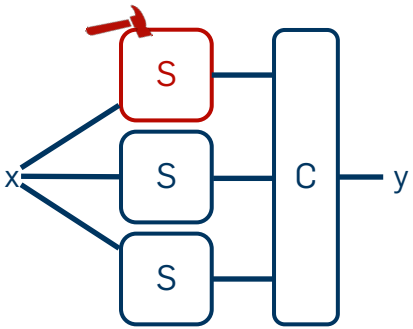
	Fault		Metric L				
	location	type	Plain	Detection (both - y, δ)	Detection (no flag - y)	Detection (flag only - δ)	Correction
input max	x_2	set	3.000	1.000	0.954	0.000	0.000
	x_2	reset	3.000	1.000	0.954	0.000	0.000
	x_2	flip	2.807	0.000	0.000	0.000	0.000
internal max	$\mathsf{inv}(x_1)$	set	3.000	1.000	0.954	0.000	0.000
	$\mathsf{inv}(x_1)$	reset	3.000	1.000	0.954	0.000	0.000
	$\mathsf{and}(x_2, \bar{x}_1)$	flip	3.000	1.000	0.954	0.000	0.000

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$.

Statistical Ineffective Fault Analysis

Vulnerability Evaluation



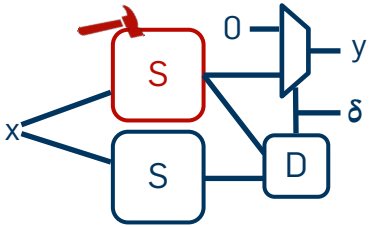


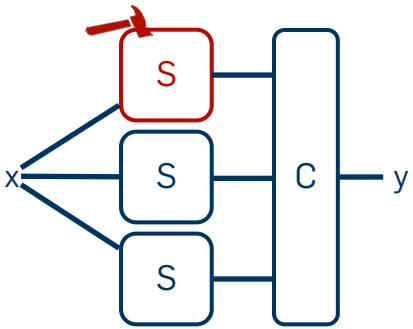
	Fault		Metric L				
	location	type	Plain	Detection (both - y, δ)	Detection (no flag - y)	Detection (flag only - δ)	Correction
input max	x_2	set	3.000	1.000	0.954	0.000	0.000
	x_2	reset	3.000	1.000	0.954	0.000	0.000
	x_2	flip	2.807	0.000	0.000	0.000	0.000
internal max	inv(x_1)	set	3.000	1.000	0.954	0.000	0.000
	inv(x_1)	reset	3.000	1.000	0.954	0.000	0.000
	and$(x_2, \bar{x}_1)$	flip	3.000	1.000	0.954	0.000	0.000

Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$.

Statistical Ineffective Fault Analysis

Vulnerability Evaluation





	Fault		Metric L				
	location	type	Plain	Detection (both - y, δ)	Detection (no flag - y)	Detection (flag only - δ)	Correction
input max	x_2	set	3.000	1.000	0.954	0.000	0.000
	x_2	reset	3.000	1.000	0.954	0.000	0.000
	x_2	flip	2.807	0.000	0.000	0.000	0.000
internal max	$\mathsf{inv}(x_1)$	set	3.000	1.000	0.954	0.000	0.000
	$\mathsf{inv}(x_1)$	reset	3.000	1.000	0.954	0.000	0.000
	$\mathsf{and}(x_2, \bar{x}_1)$	flip	3.000	1.000	0.954	0.000	0.000

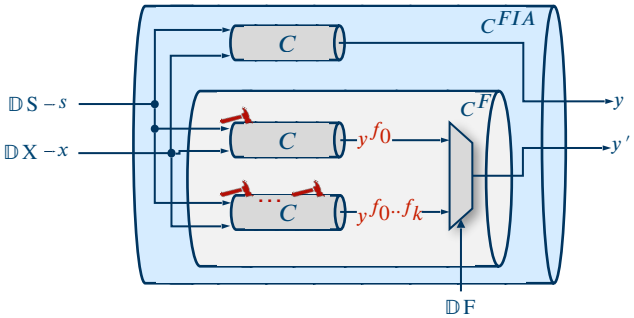
Theoretical maximum: $\mathsf{L}^{max}_{PRESENT} = 4$.

SIFA Leakage with Independent Detection Flag

Contradicting Hadzic et al., 2021

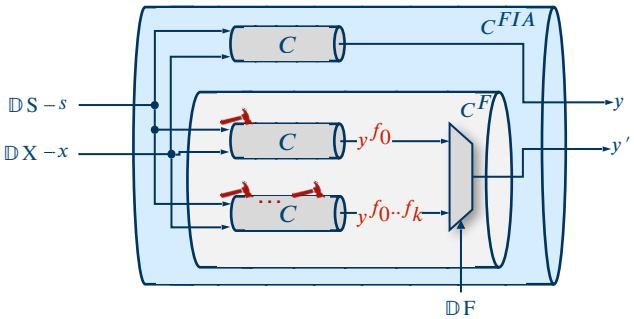
Conclusion

Channel for Fault Analysis

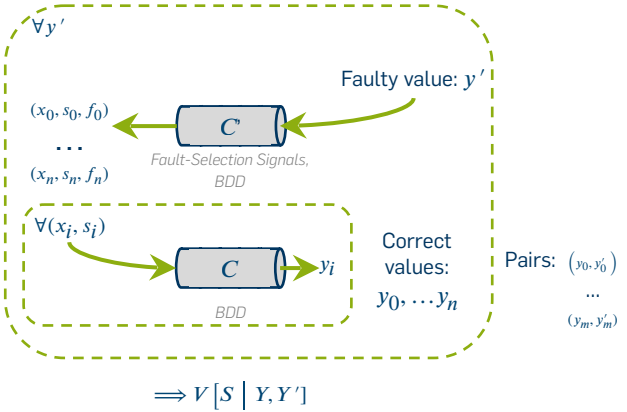


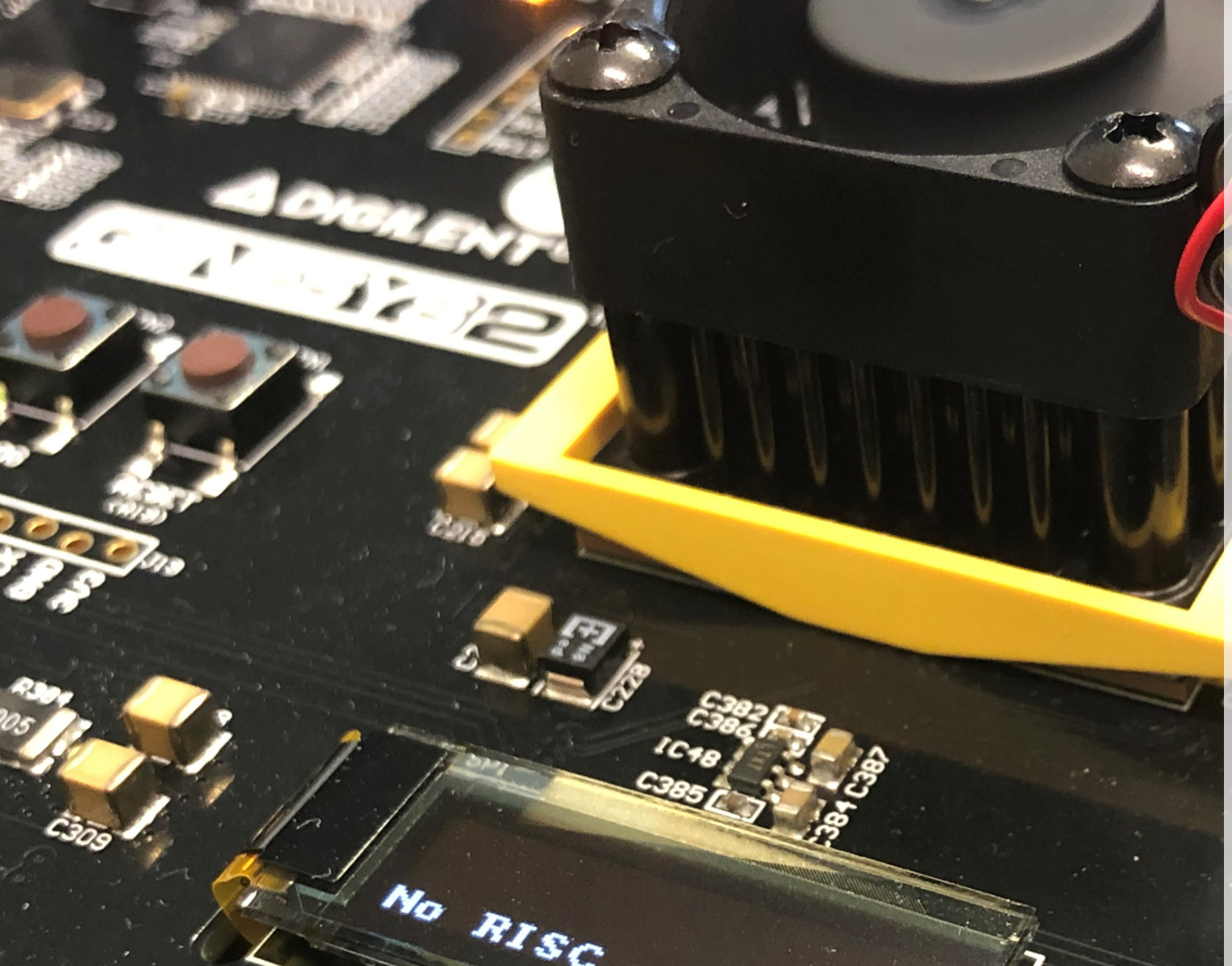
Conclusion

Channel for Fault Analysis



Vulnerability Computation





CASA
Cyber Security in the Age of Large-Scale Adversaries

RUHR UNIVERSITÄT BOCHUM

RUB

WPI

Thank you!

VERICA

Jakob Feldtkeller

Chair for Security Engineering
Faculty of Computer Science
Ruhr University Bochum

SECURITY ENGINEERING