THALES

New Challenges to Counteract Higher-Order Side-Channel Attacks

Sonia Belaïd

Journées Nationales 2017 Pré-GDR Sécurité Informatique

31-05-2017

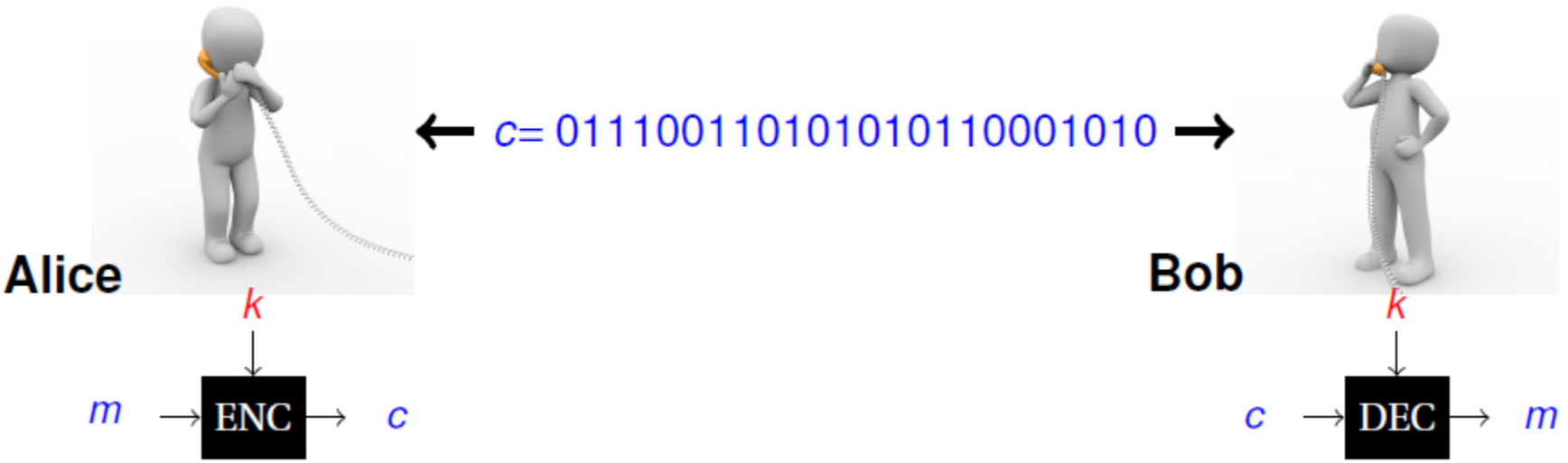
Outline

- Power-Analysis Attacks and Countermeasures
- The Case of Small Orders Attacks
- New Challenges to Counteract Higher-Order Attacks
- Perspectives

Outline

- Power-Analysis Attacks and Countermeasures
- The Case of Small Orders Attacks
- New Challenges to Counteract Higher-Order Attacks
- Perspectives

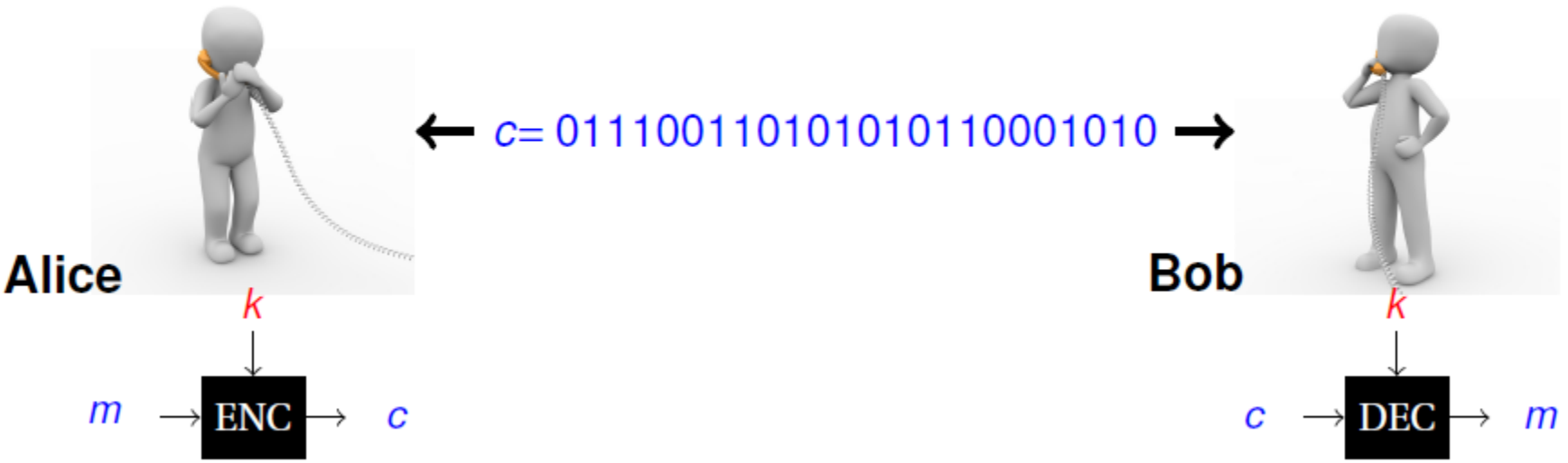
Symmetric Cryptography



Cryptanalysis

Black-box cryptanalysis: $A \leftarrow (m, c)$

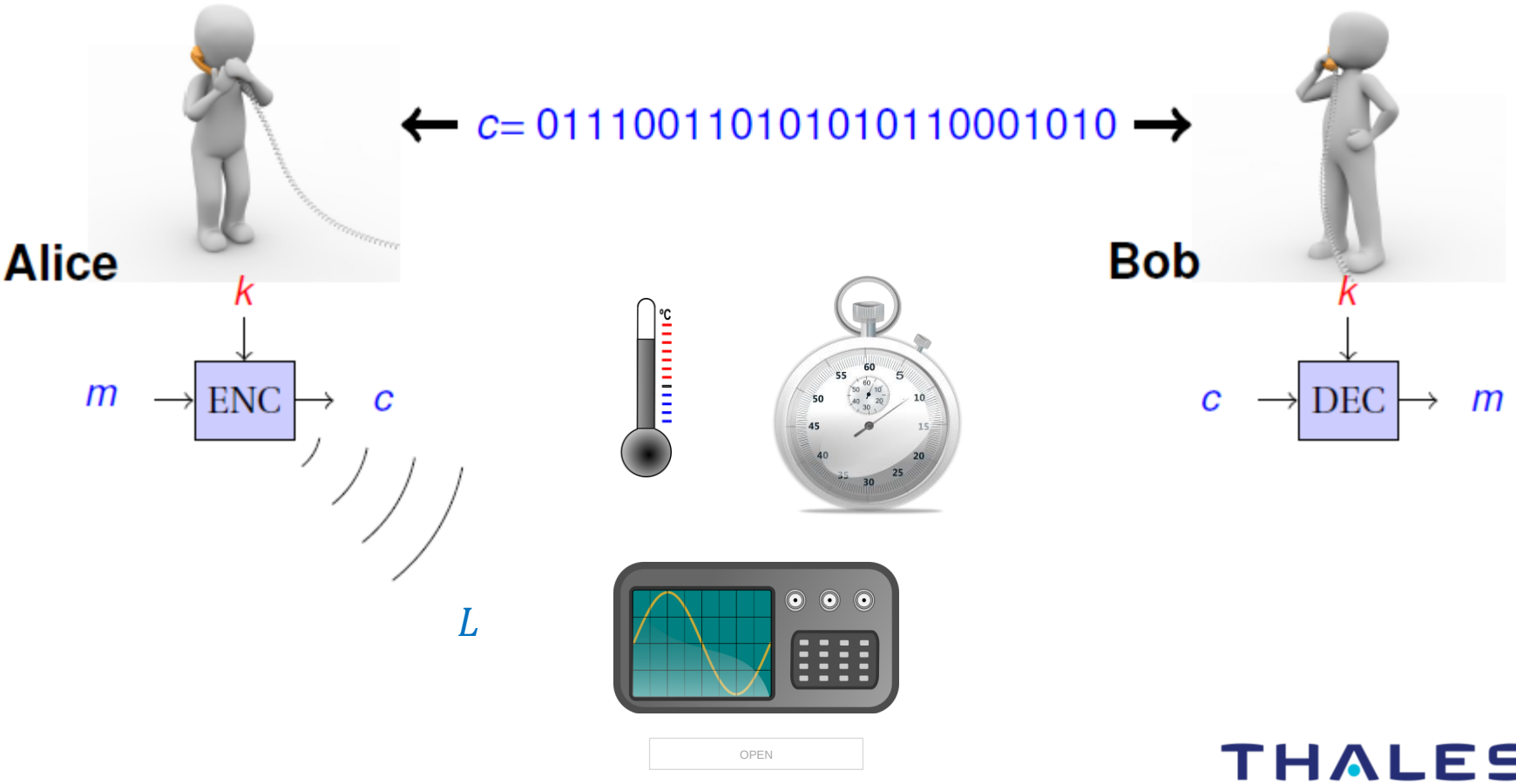
Side-channel analysis: $A \leftarrow (m, c, L)$



Cryptanalysis

Black-box cryptanalysis: $A \leftarrow (m, c)$

Side-channel analysis: $A \leftarrow (m, c, L)$

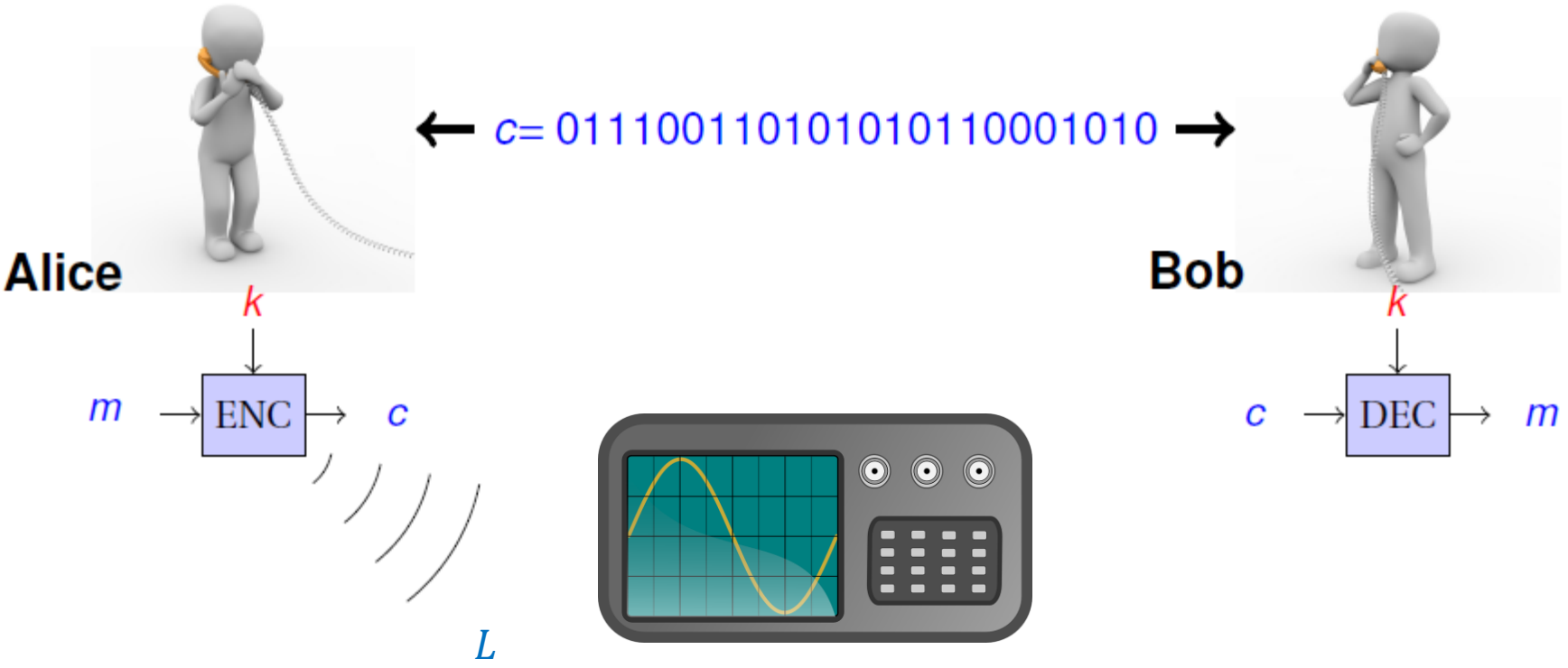


THALES

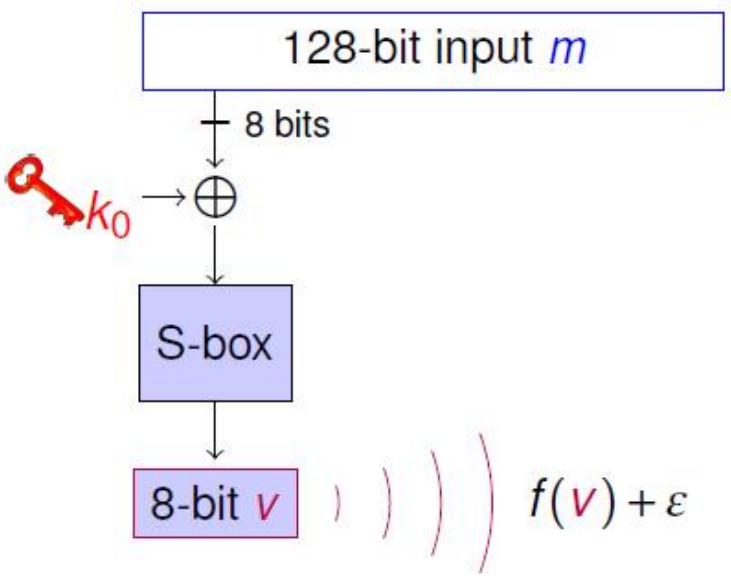
Cryptanalysis

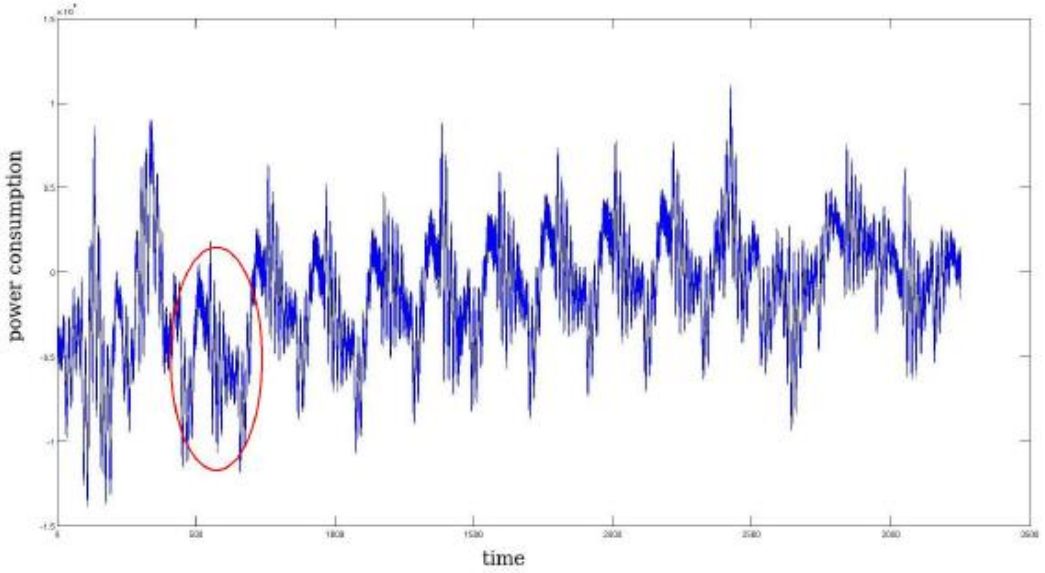
Black-box cryptanalysis: $A \leftarrow (m, c)$

Side-channel analysis: $A \leftarrow (m, c, L)$



Classical Power-Analysis Attack against AES-128





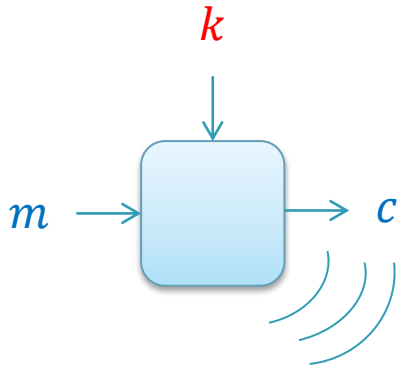
Attack on 8 bits

- Prediction of the outputs for the 256 possible 8-bit secret
- Correlation between predictions and leakage
- Selection of the best correlation to find the correct 8-bit secret

Attack on 128 bits

- Repetition of the attack on each 8-bit block

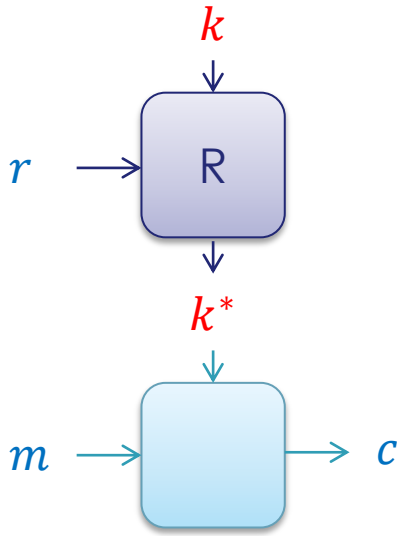
Countermeasures against Power-Analysis Attacks



Problem: the leakage is key-dependent

Fresh Re-keying

Idea: regularly change k



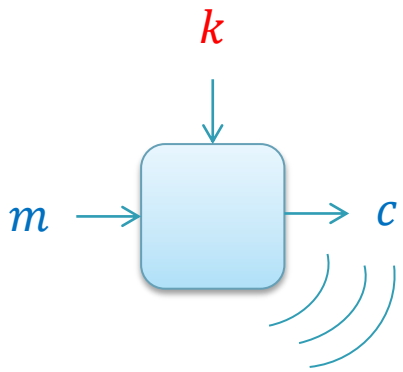
Masking

Idea: make the leakage random

Sensitive value $v = f(m, k)$

$$v_0 = v \oplus \bigoplus_{i=1}^{t} v_i \qquad v_1 \leftarrow \$ \qquad \dots \qquad v_t \leftarrow \$$$

Countermeasures against Power-Analysis Attacks



Problem: the leakage is key-dependent

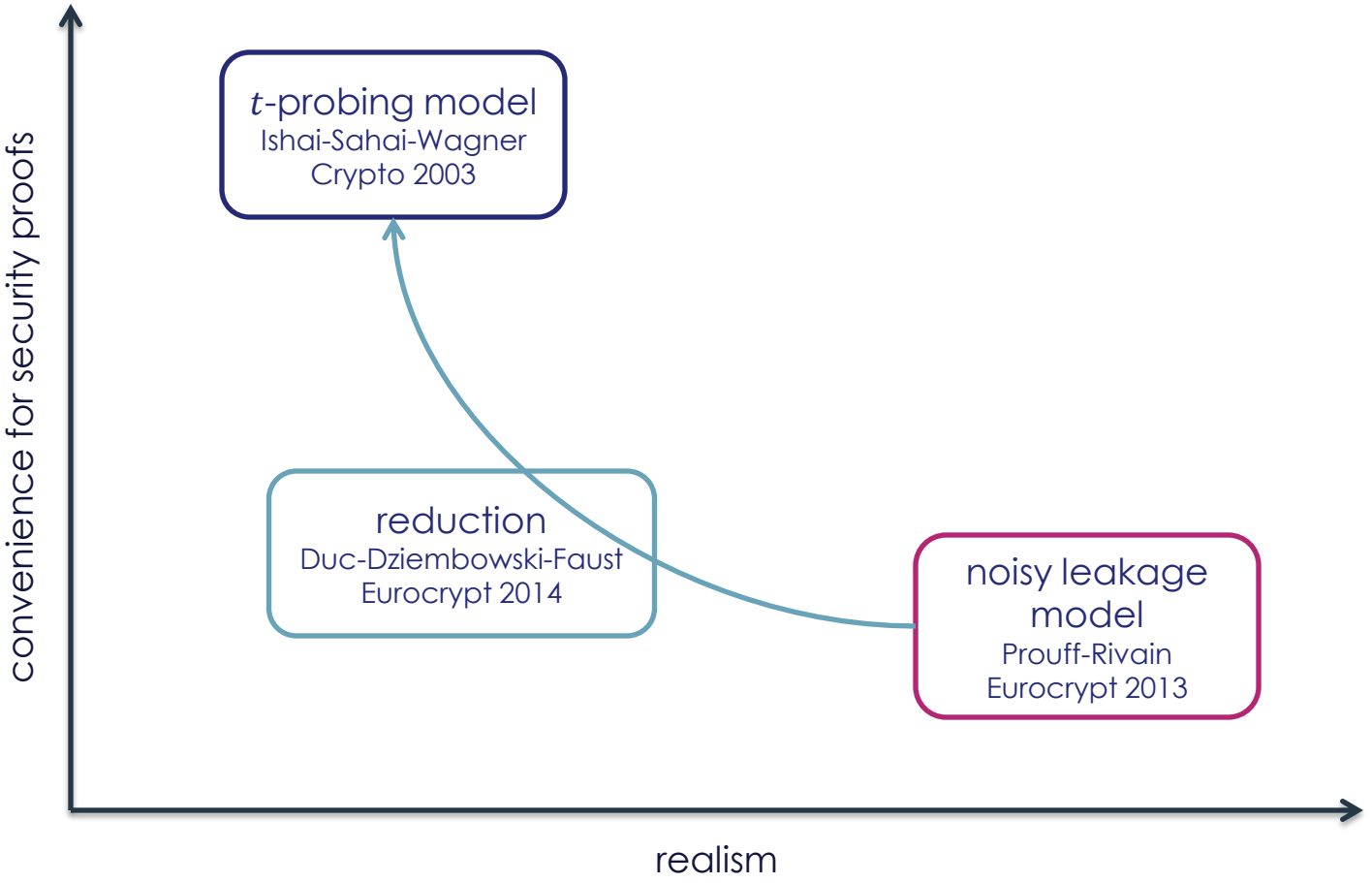
Masking

Idea: make the leakage random

Sensitive value $v = f(m, k)$

$$v_0 = v \oplus \bigoplus_{i=1}^{t} v_i \qquad v_1 \leftarrow \$ \qquad \dots \qquad v_t \leftarrow \$$$

Leakage Models: State of the Art



Outline

- Power-Analysis Attacks and Countermeasures
- **The Case of Small Orders Attacks**
- New Challenges to Counteract Higher-Order Attacks
- Perspectives

Security in the t-probing model

t-probing model assumptions:

- Only one variable is leaking at a time
- The attacker gets the exact values of at most t variables

Security is achieved if all the t-uples are independent from the secret

Verifying Proofs of Masking for Small Orders

x: sensitive variable / secret
v: random variables
c: constant

function Ex-t3(x_1, x_2, x_3, x_4, c):

$(* \; x_1, x_2, x_3 \leftarrow \$ \; *)$
$(* \; x_4 \leftarrow x \oplus x_1 \oplus x_2 \oplus x_3 \; *)$
$r_1 \leftarrow \$$
$r_2 \leftarrow \$$
$y_1 \leftarrow x_1 \oplus r_1$
$y_2 \leftarrow (x \oplus x_1 \oplus x_2 \oplus x_3) \oplus r_2$
$t_1 \leftarrow x_2 \oplus r_1$
$t_2 \leftarrow (x_2 \oplus r_1) \oplus x_3$
$y_3 \leftarrow (x_2 \oplus r_1 \oplus x_3) \oplus r_2$
$y_4 = c \oplus r_2$

return(y_1, y_2, y_3, y_4)

Verifying Proofs of Masking for Small Orders

x: sensitive variable / secret
v: random variables
c: constant

function Ex-t3(x_1, x_2, x_3, x_4, c):

$(* \; x_1, x_2, x_3 \leftarrow \$ \; *)$
$(* \; x_4 \leftarrow x \oplus x_1 \oplus x_2 \oplus x_3 \; *)$
$r_1 \leftarrow \$$
$r_2 \leftarrow \$$
$y_1 \leftarrow x_1 \oplus r_1$
$y_2 \leftarrow (x \oplus x_1 \oplus x_2 \oplus x_3) \oplus r_2$
$t_1 \leftarrow x_2 \oplus r_1$
$t_2 \leftarrow (x_2 \oplus r_1) \oplus x_3$
$y_3 \leftarrow (x_2 \oplus r_1 \oplus x_3) \oplus r_2$
$y_4 = c \oplus r_2$
return(y_1, y_2, y_3, y_4)

Independent from the secret?

Verifying Proofs of Masking for Small Orders

x: sensitive variable / secret
v: random variables
c: constant

function Ex-t3(x_1, x_2, x_3, x_4, c):

$(* \; x_1, x_2, x_3 \leftarrow \$ \; *)$
$(* \; x_4 \leftarrow x \oplus x_1 \oplus x_2 \oplus x_3 \; *)$
$r_1 \leftarrow \$$
$r_2 \leftarrow \$$
$y_1 \leftarrow x_1 \oplus r_1$
$y_2 \leftarrow (x \oplus x_1 \oplus x_2 \oplus x_3) \oplus r_2$
$t_1 \leftarrow x_2 \oplus r_1$
$t_2 \leftarrow (x_2 \oplus r_1) \oplus x_3$
$y_3 \leftarrow (x_2 \oplus r_1 \oplus x_3) \oplus r_2$
$y_4 = c \oplus r_2$
return(y_1, y_2, y_3, y_4)

Independent from the secret?

Verifying Proofs of Masking for Small Orders

x: sensitive variable / secret
v: random variables
c: constant

function Ex-t3(x_1, x_2, x_3, x_4, c):

$(* \; x_1, x_2, x_3 \leftarrow \$ \; *)$
$(* \; x_4 \leftarrow x \oplus x_1 \oplus x_2 \oplus x_3 \; *)$
$r_1 \leftarrow \$$
$r_2 \leftarrow \$$
$y_1 \leftarrow x_1 \oplus r_1$
$y_2 \leftarrow (x \oplus x_1 \oplus x_2 \oplus x_3) \oplus r_2$
$t_1 \leftarrow x_2 \oplus r_1$
$t_2 \leftarrow (x_2 \oplus r_1) \oplus x_3$
$y_3 \leftarrow (x_2 \oplus r_1 \oplus x_3) \oplus r_2$
$y_4 = c \oplus r_2$
return(y_1, y_2, y_3, y_4)

Independent from the secret?

Verifying Proofs of Masking for Small Orders

x: sensitive variable / secret
v: random variables
c: constant

function Ex-t3(x_1, x_2, x_3, x_4, c):

$(* \; x_1, x_2, x_3 \leftarrow \$ \; *)$
$(* \; x_4 \leftarrow x \oplus x_1 \oplus x_2 \oplus x_3 \; *)$
$r_1 \leftarrow \$$
$r_2 \leftarrow \$$
$y_1 \leftarrow x_1 \oplus r_1$
$y_2 \leftarrow (x \oplus x_1 \oplus x_2 \oplus x_3) \oplus r_2$
$t_1 \leftarrow x_2 \oplus r_1$
$t_2 \leftarrow (x_2 \oplus r_1) \oplus x_3$
$y_3 \leftarrow (x_2 \oplus r_1 \oplus x_3) \oplus r_2$
$y_4 = c \oplus r_2$
return(y_1, y_2, y_3, y_4)

Independent from the secret?

→ many mistakes

Verifying Proofs of Masking for Small Orders

x: sensitive variable / secret
v: random variables
c: constant

function Ex-t3(x_1, x_2, x_3, x_4, c):

$(* \; x_1, x_2, x_3 \leftarrow \$ \; *)$
$(* \; x_4 \leftarrow x \oplus x_1 \oplus x_2 \oplus x_3 \; *)$
$r_1 \leftarrow \$$
$r_2 \leftarrow \$$
$y_1 \leftarrow x_1 \oplus r_1$
$y_2 \leftarrow (x \oplus x_1 \oplus x_2 \oplus x_3) \oplus r_2$
$t_1 \leftarrow x_2 \oplus r_1$
$t_2 \leftarrow (x_2 \oplus r_1) \oplus x_3$
$y_3 \leftarrow (x_2 \oplus r_1 \oplus x_3) \oplus r_2$
$y_4 = c \oplus r_2$
return(y_1, y_2, y_3, y_4)

Independent from the secret?

→ many mistakes

286 3-uples to test

→ missing cases
→ inefficient

Contribution for Small Orders: maskverif

Combination of two algorithms to address both steps

- Algo 1: determines if a t-uple is independent from the secret
- Algo 2: efficiently goes through to all possible sets

Underlying Formal Tool: EasyCrypt

Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub.
Verified proofs of higher-order masking.
EUROCRYPT 2015.

Outline

- Power-Analysis Attacks and Countermeasures
- The Case of Small Orders Attacks
- **New Challenges to Counteract Higher-Order Attacks**
- Perspectives

New Challenges

Leakage models

State of the art :
- Probing model
- Noisy leakage model

New challenges :
- Better reductions between leakage models
- Models which fit the reality of real components

Security

State of the art :
- Proofs in the probing and noisy models
- Formal proofs

New challenges :
- Formal proofs
- Proof of still unproven implementations
- New composition

Efficiency

State of the art :
- Masked high order gadgets

New challenges :
- Still less randomness for masked gadgets
- Less multiplications for masked gadgets

New Challenges

Leakage models

State of the art :
- Probing model
- Noisy leakage model

New challenges :
- Better reductions between leakage models
- Models which fit the reality of real components

Security

State of the art :
- Proofs in the probing and noisy models
- Formal proofs

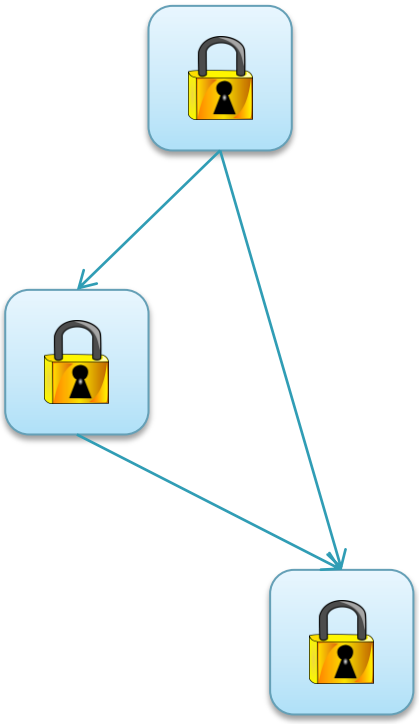
New challenges :
- Formal proofs
- Proof of still unproven implementations
- **New composition**

Efficiency

State of the art :
- Masked high order gadgets

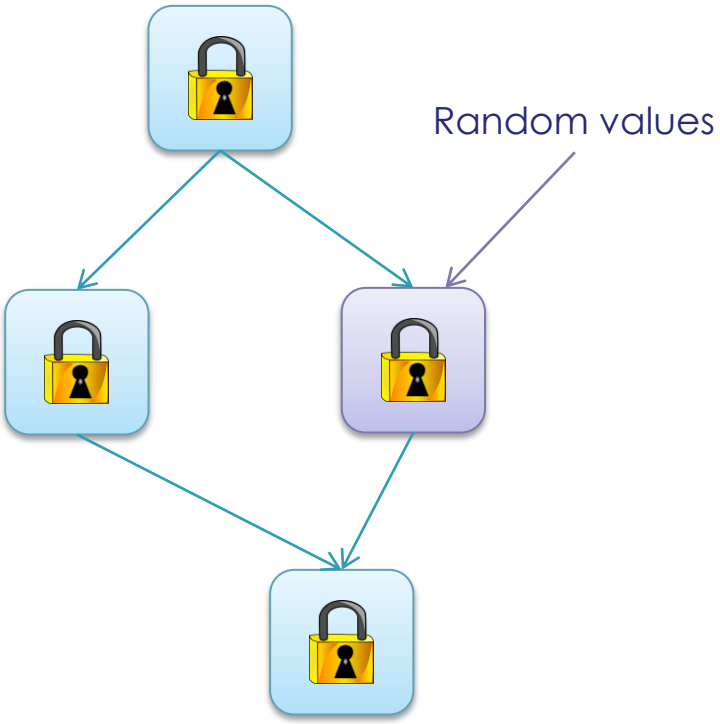
New challenges :
- Still less randomness for masked gadgets
- Less multiplications for masked gadgets

State-of-the-art for Composing Masking



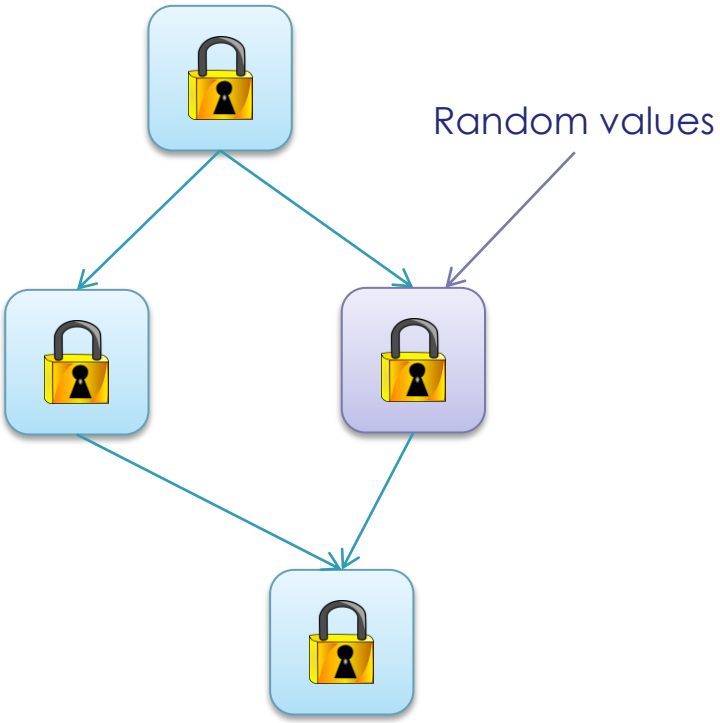
Is secure?

State-of-the-art for Composing Masking

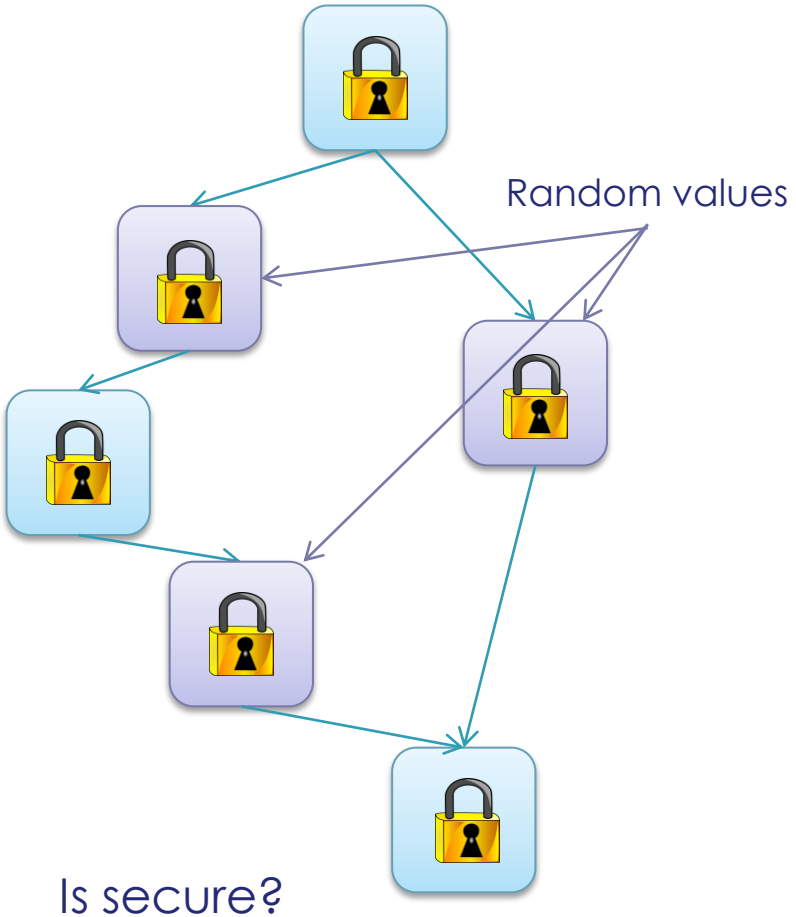


Is secure?

State-of-the-art for Composing Masking



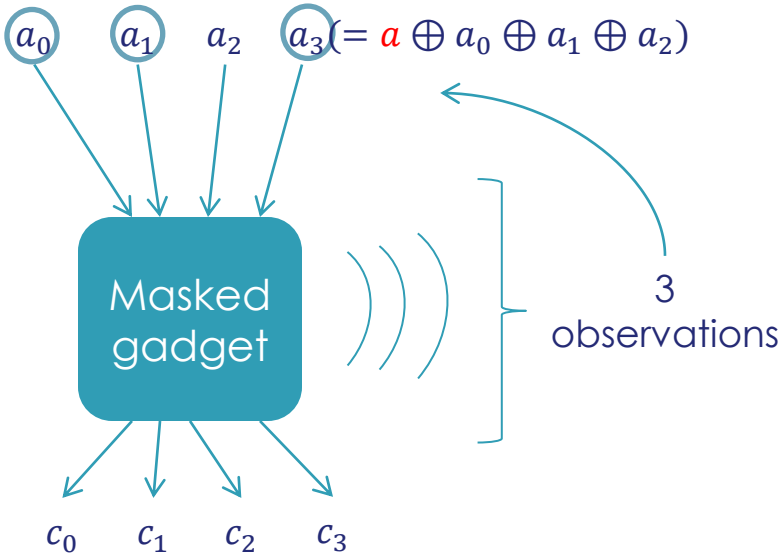
Is secure?



Is secure?

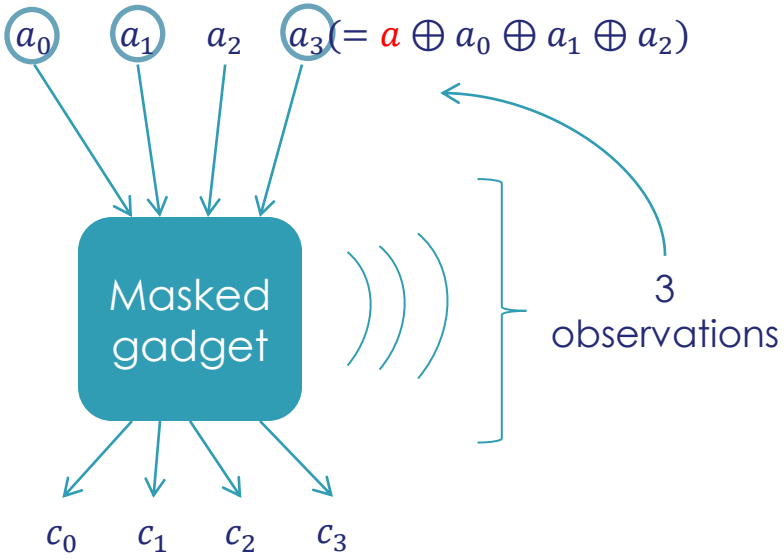
Security properties in the t-probing model

- **If t is fixed:** show that any set of t intermediate variables is independent from the secret
- **if t is not fixed:** show that any set of t intermediate variables can be simulated with at most t shares of each input (NI)



Security properties in the t-probing model

- **If t is fixed:** show that any set of t intermediate variables is independent from the secret
- **if t is not fixed:** show that any set of t intermediate variables can be simulated with at most t shares of each input (NI)

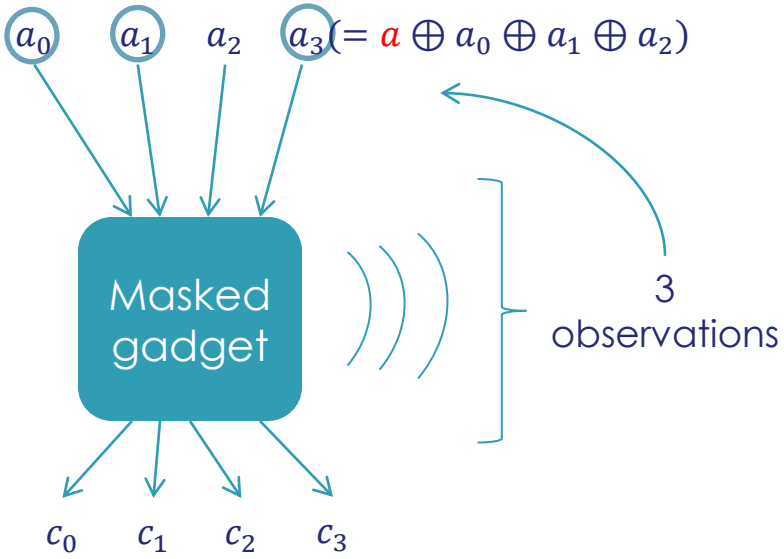


function Linear-t$(a_0, \dots, a_i, \dots a_t)$:
for $i = 0$ to t
$c_i \leftarrow f(a_i)$
return $(c_0, \dots, c_i, \dots, c_t)$

→ straightforward for linear functions

Security properties in the t-probing model

- **If t is fixed:** show that any set of t intermediate variables is independent from the secret
- **if t is not fixed:** show that any set of t intermediate variables can be simulated with at most t shares of each input (NI)

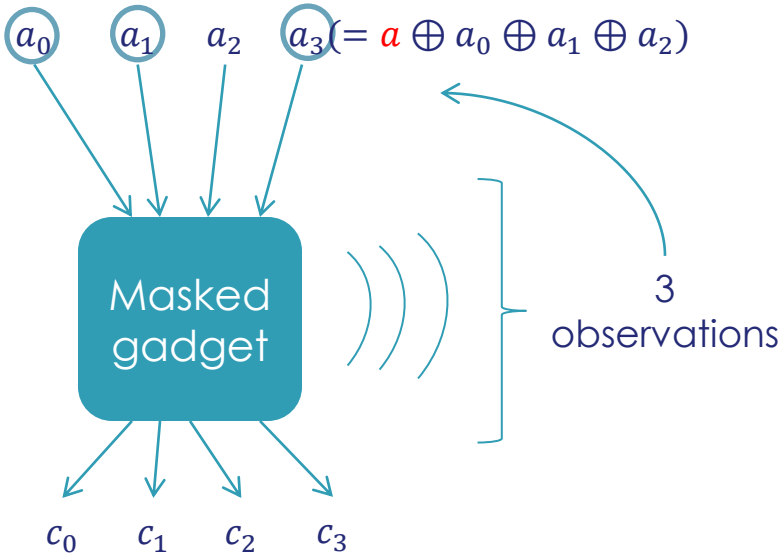


function Linear-t($a_0, \ldots, a_i, \ldots a_t$):
for $i = 0$ to t
    $c_i \leftarrow f(a_i)$
return $(c_0, \ldots, c_i, \ldots, c_t)$

→ straightforward for linear functions

Security properties in the t-probing model

- **If t is fixed:** show that any set of t intermediate variables is independent from the secret
- **if t is not fixed:** show that any set of t intermediate variables can be simulated with at most t shares of each input (NI)

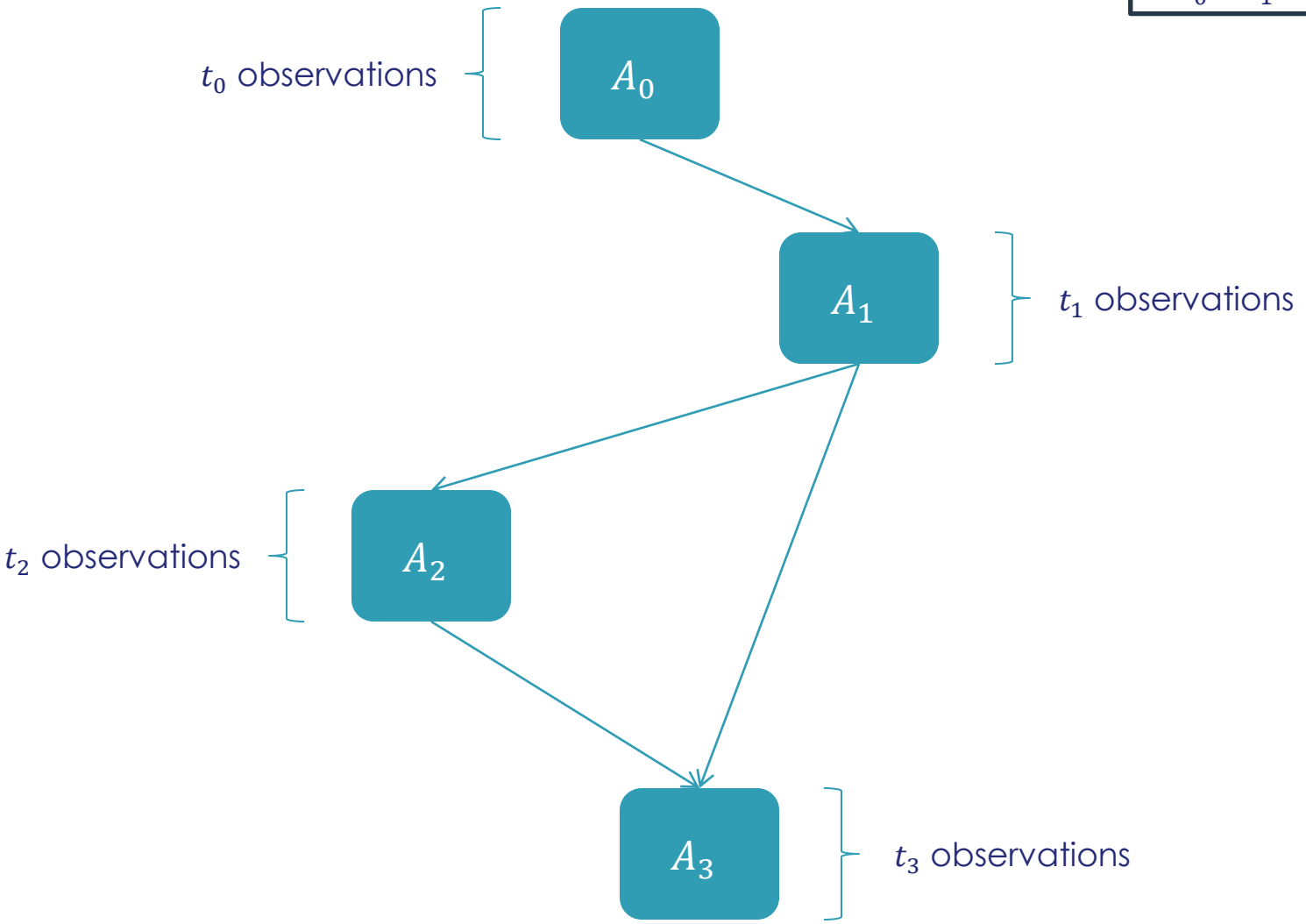


function Linear-t($a_0, \ldots, a_i, \ldots a_t$):
for $i = 0$ to t
    $c_i \leftarrow f(a_i)$
return $(c_0, \ldots, c_i, \ldots, c_t)$

→ straightforward for linear functions
→ formal proofs with EasyCrypt and pen-and paper proofs for small non-linear functions

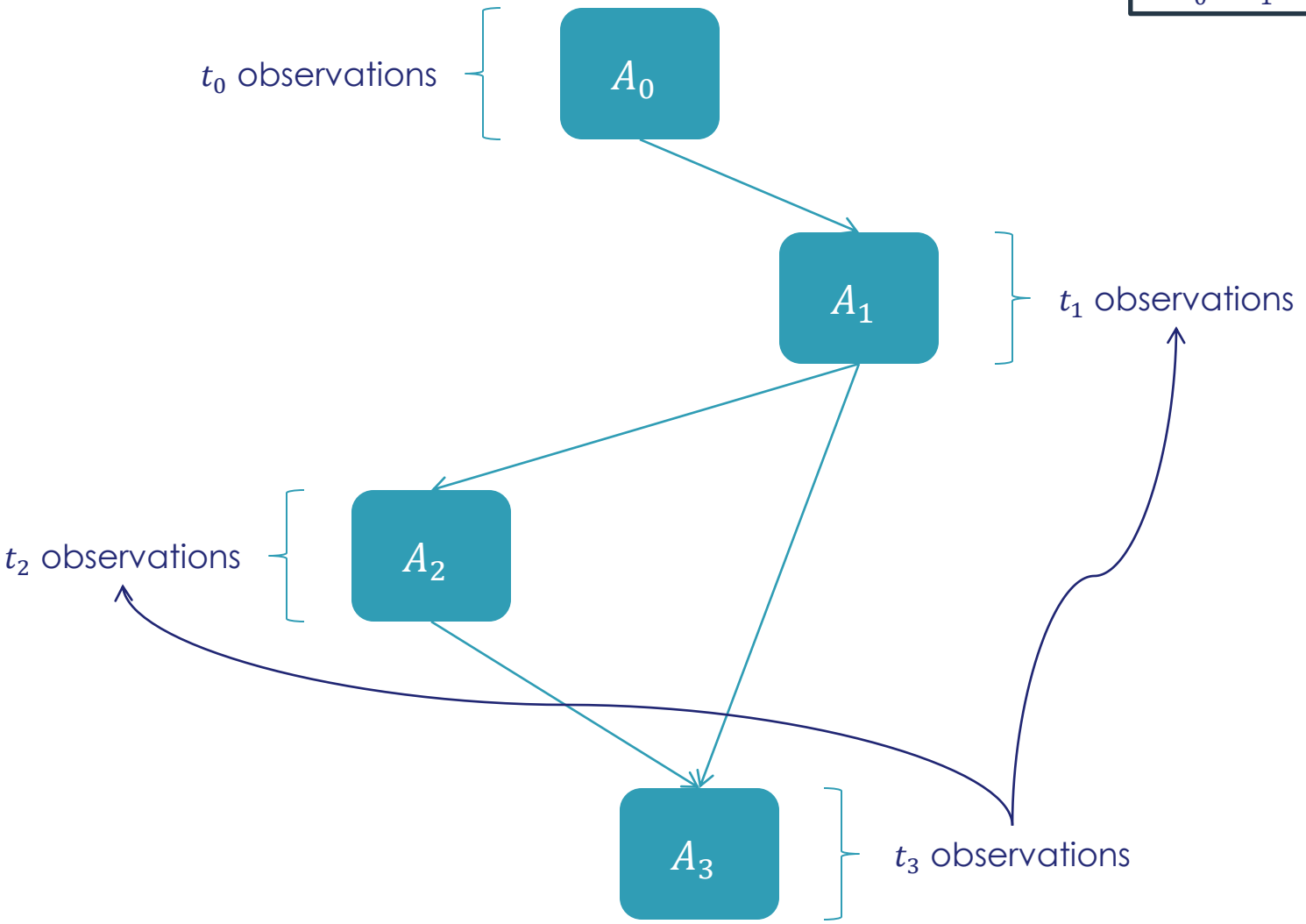
Current Issues

$t_0 + t_1 + t_2 + t_3 \leq t$



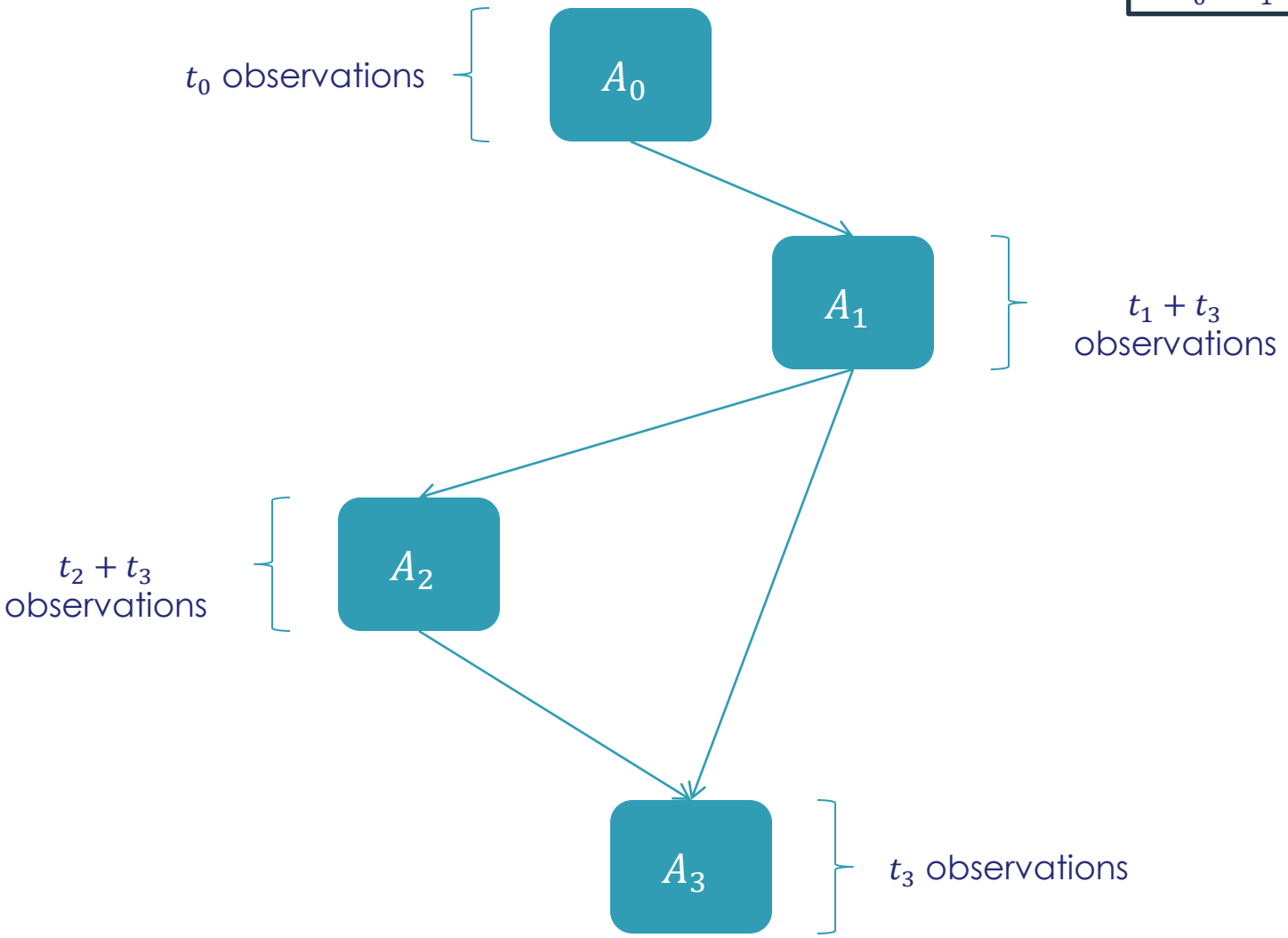
Current Issues

$t_0 + t_1 + t_2 + t_3 \leq t$



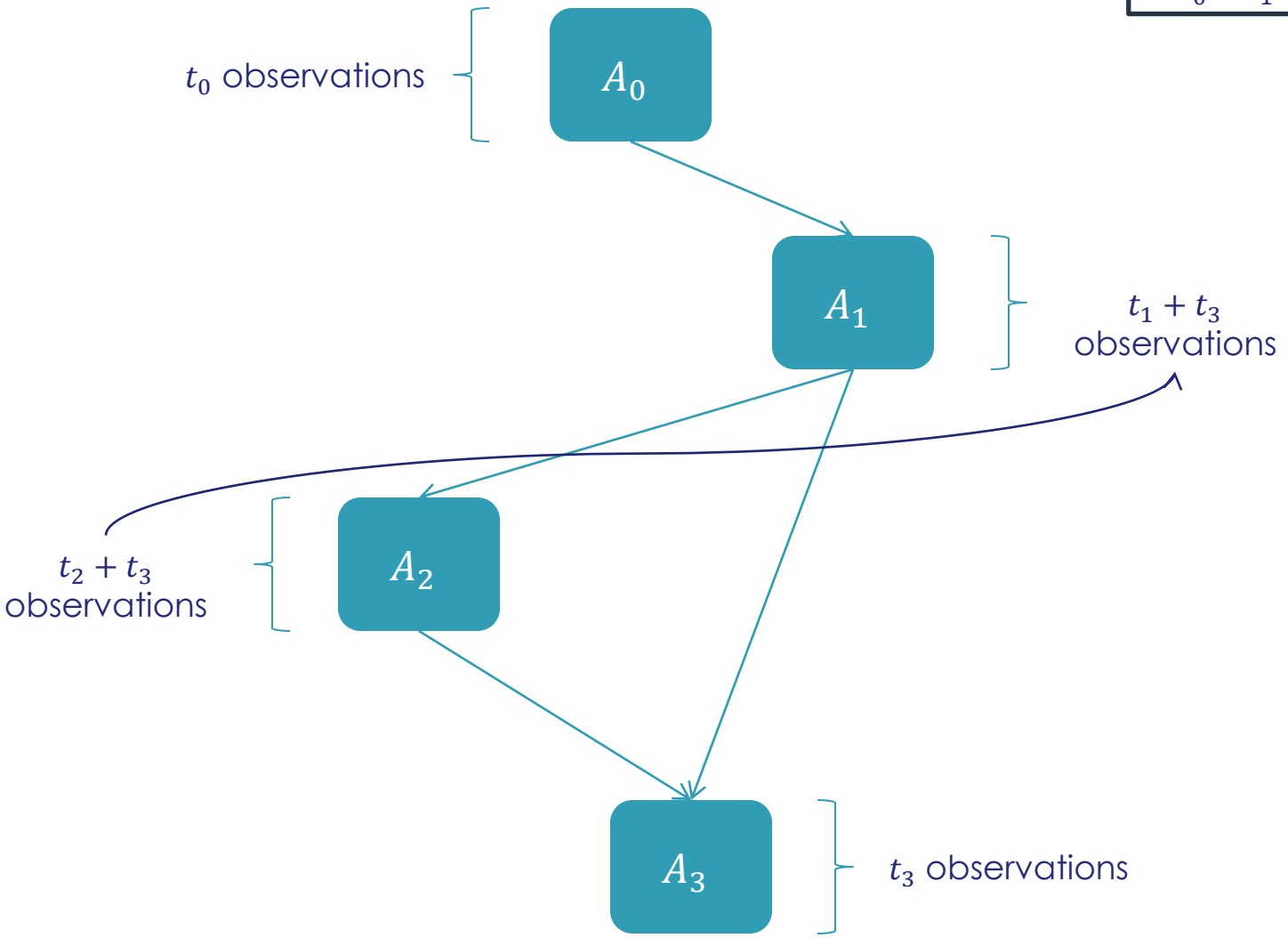
Current Issues

$t_0 + t_1 + t_2 + t_3 \leq t$



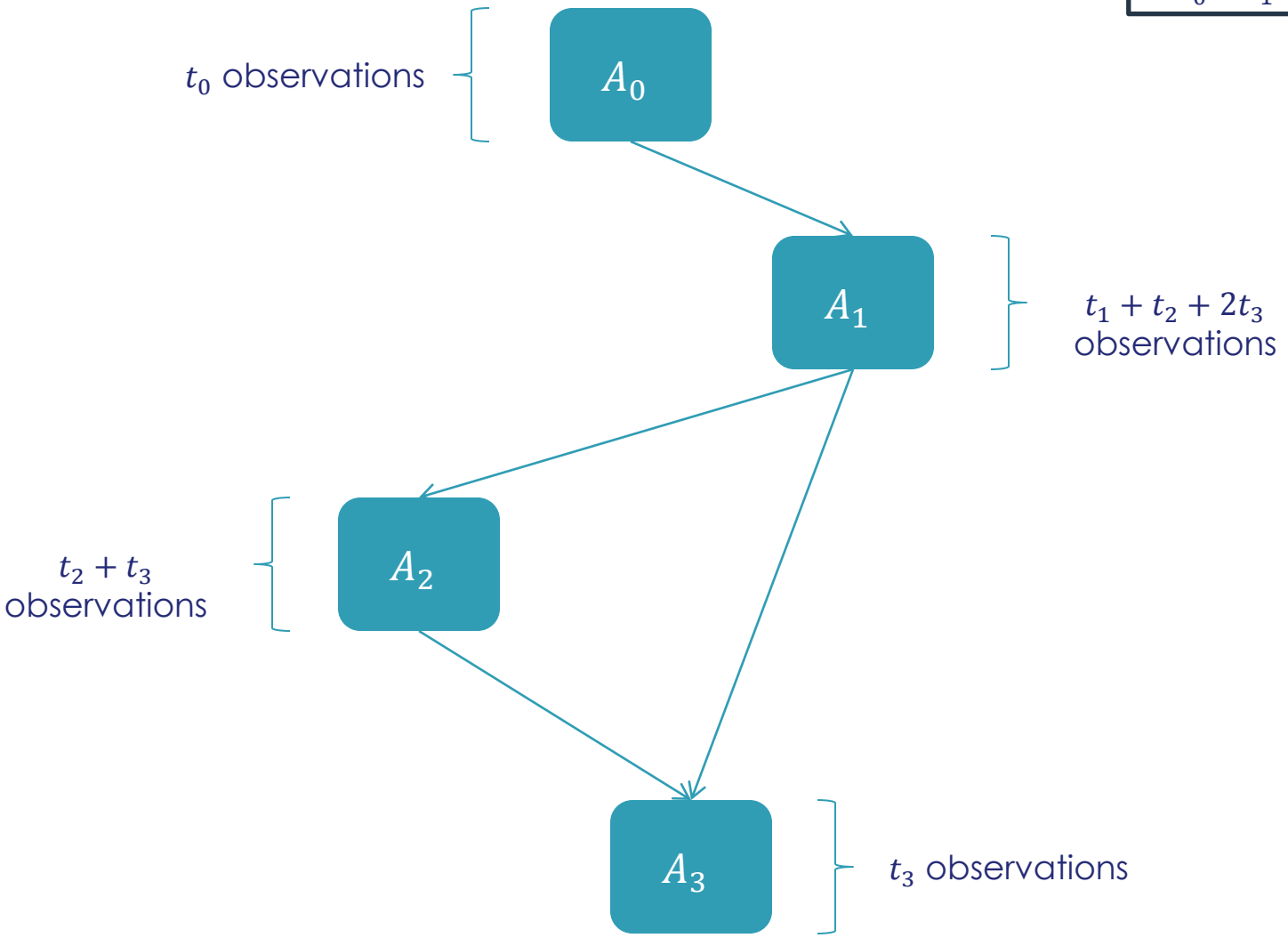
Current Issues

$t_0 + t_1 + t_2 + t_3 \leq t$



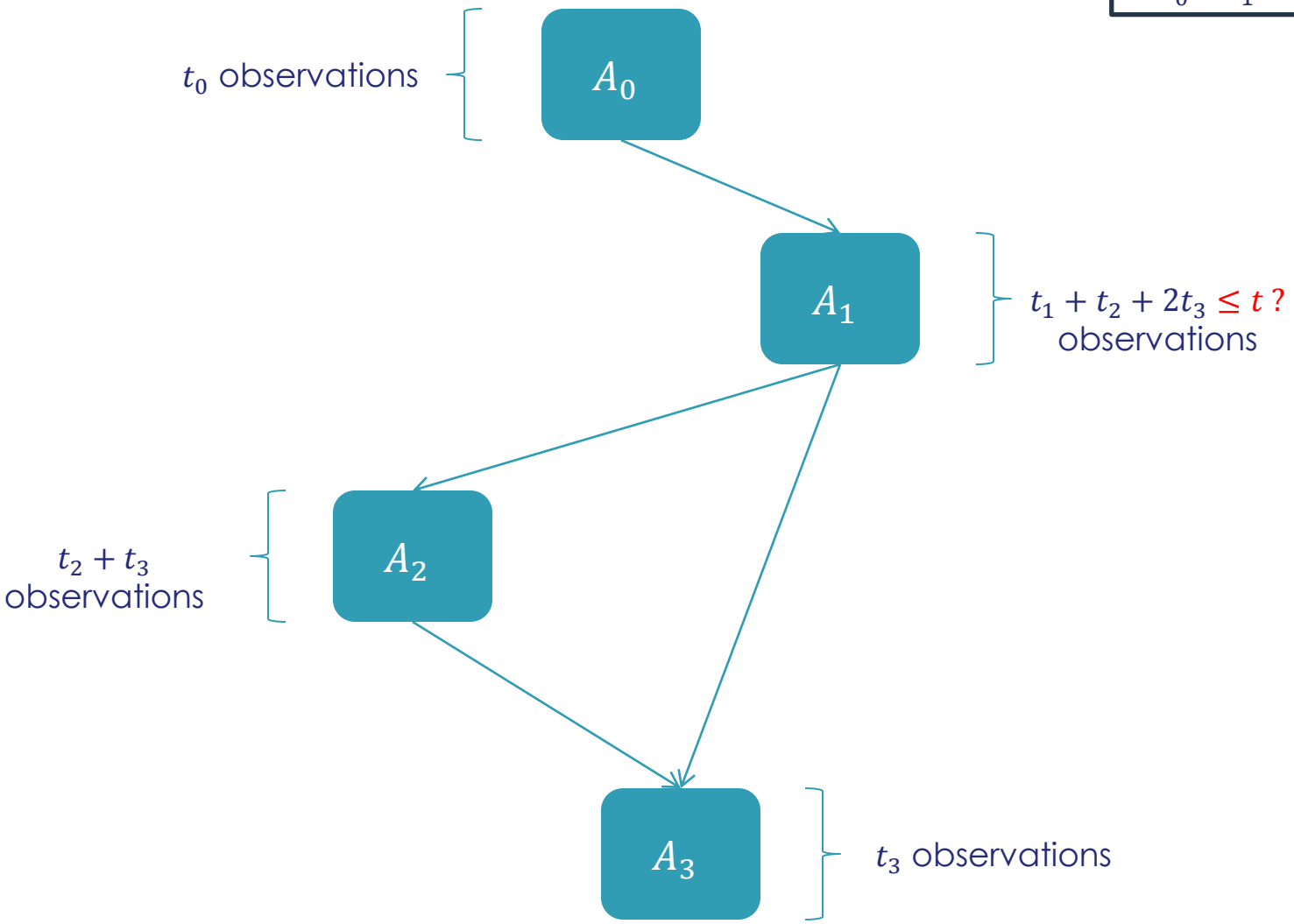
Current Issues

$t_0 + t_1 + t_2 + t_3 \leq t$



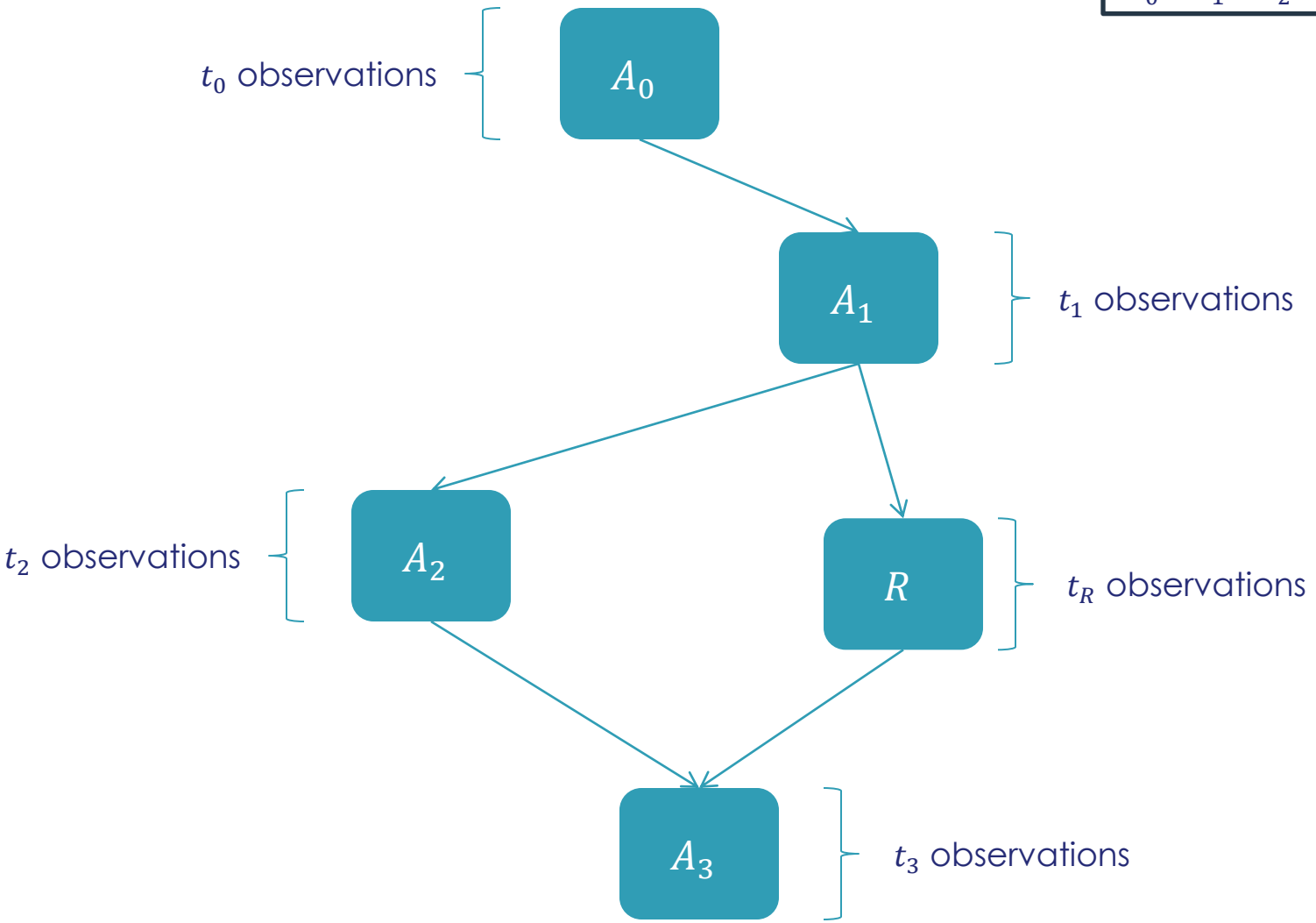
Current Issues

$t_0 + t_1 + t_2 + t_3 \leq t$



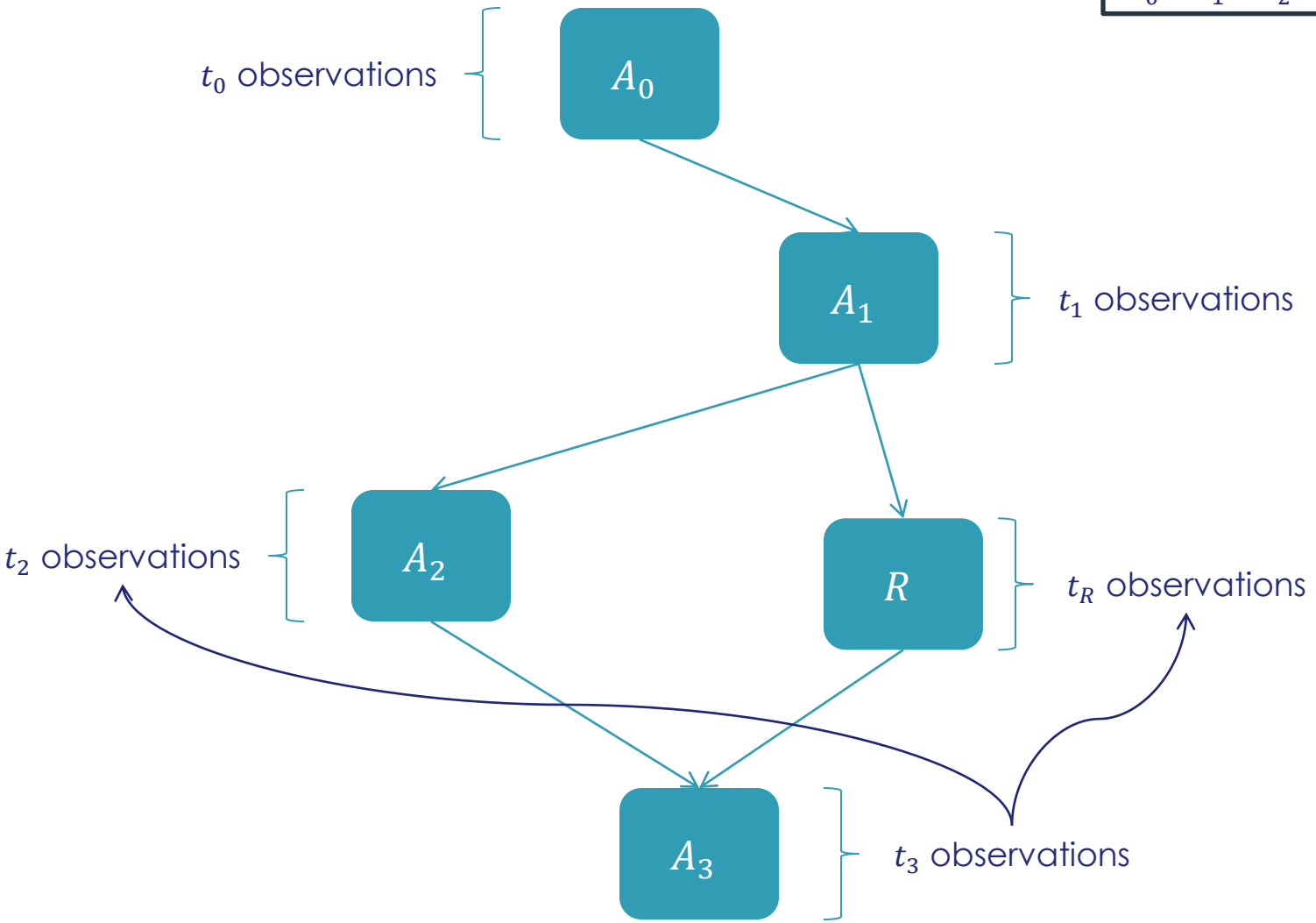
Current Issues

$$t_0 + t_1 + t_2 + t_3 + t_R \leq t$$



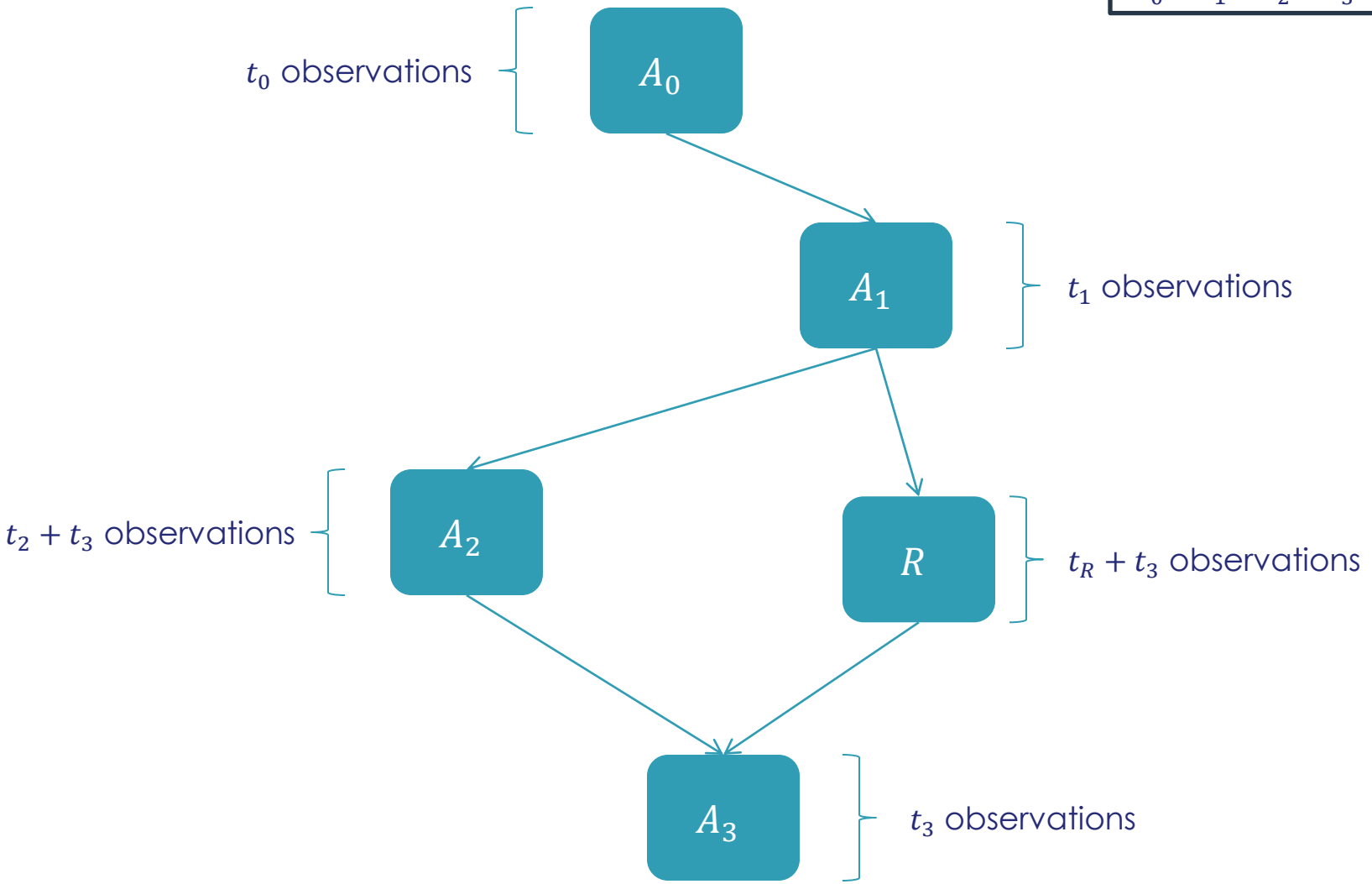
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



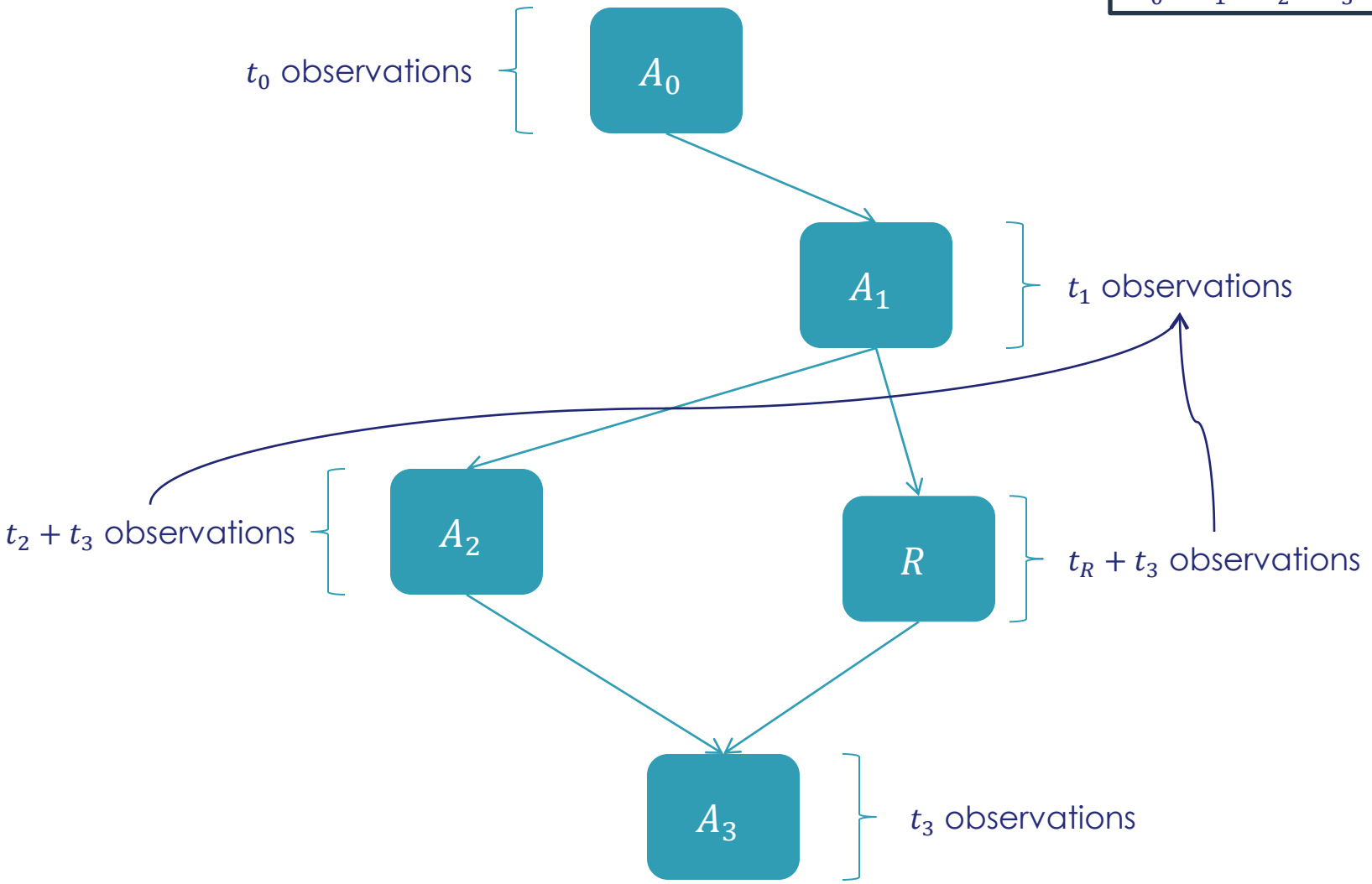
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



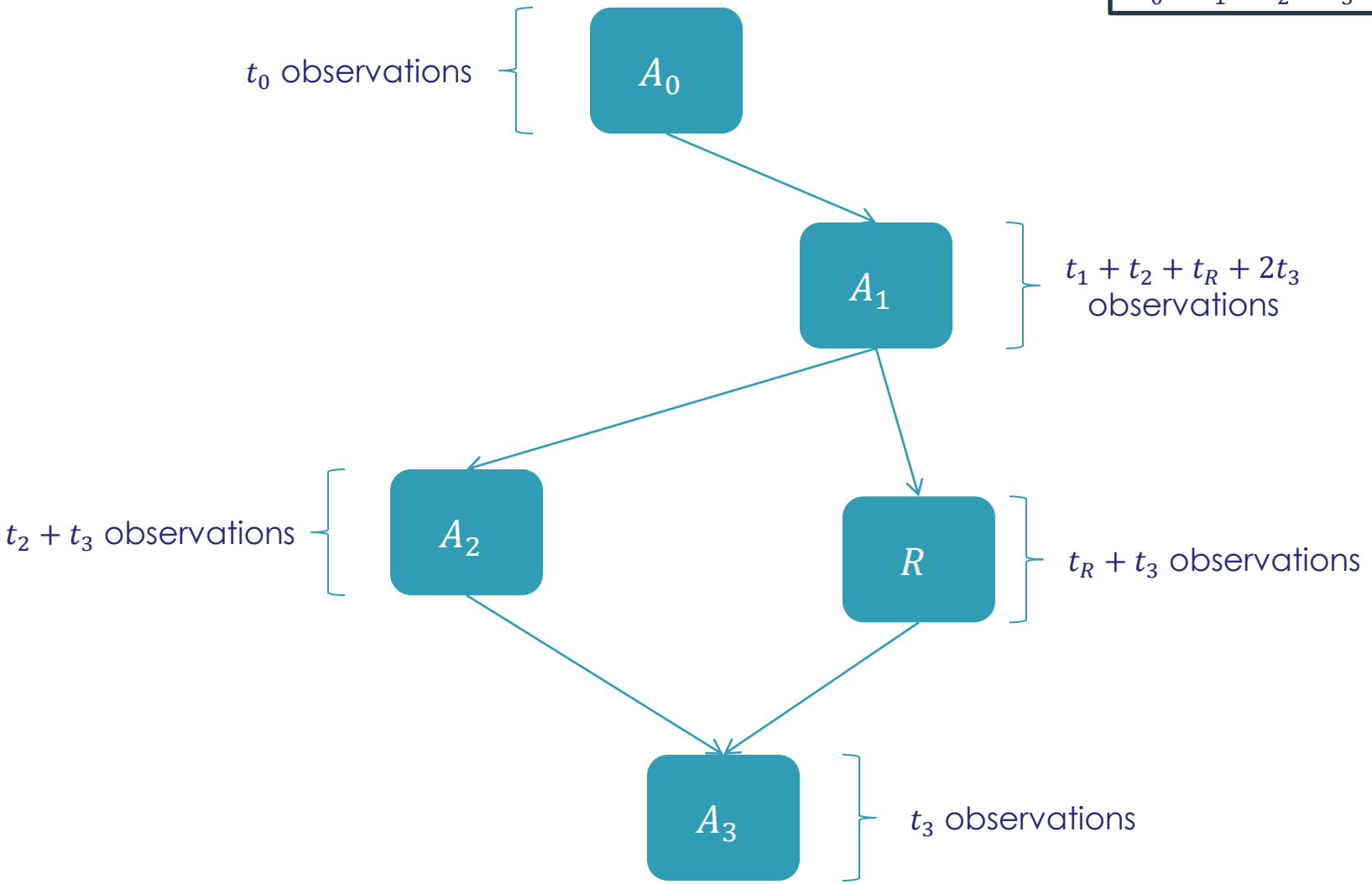
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



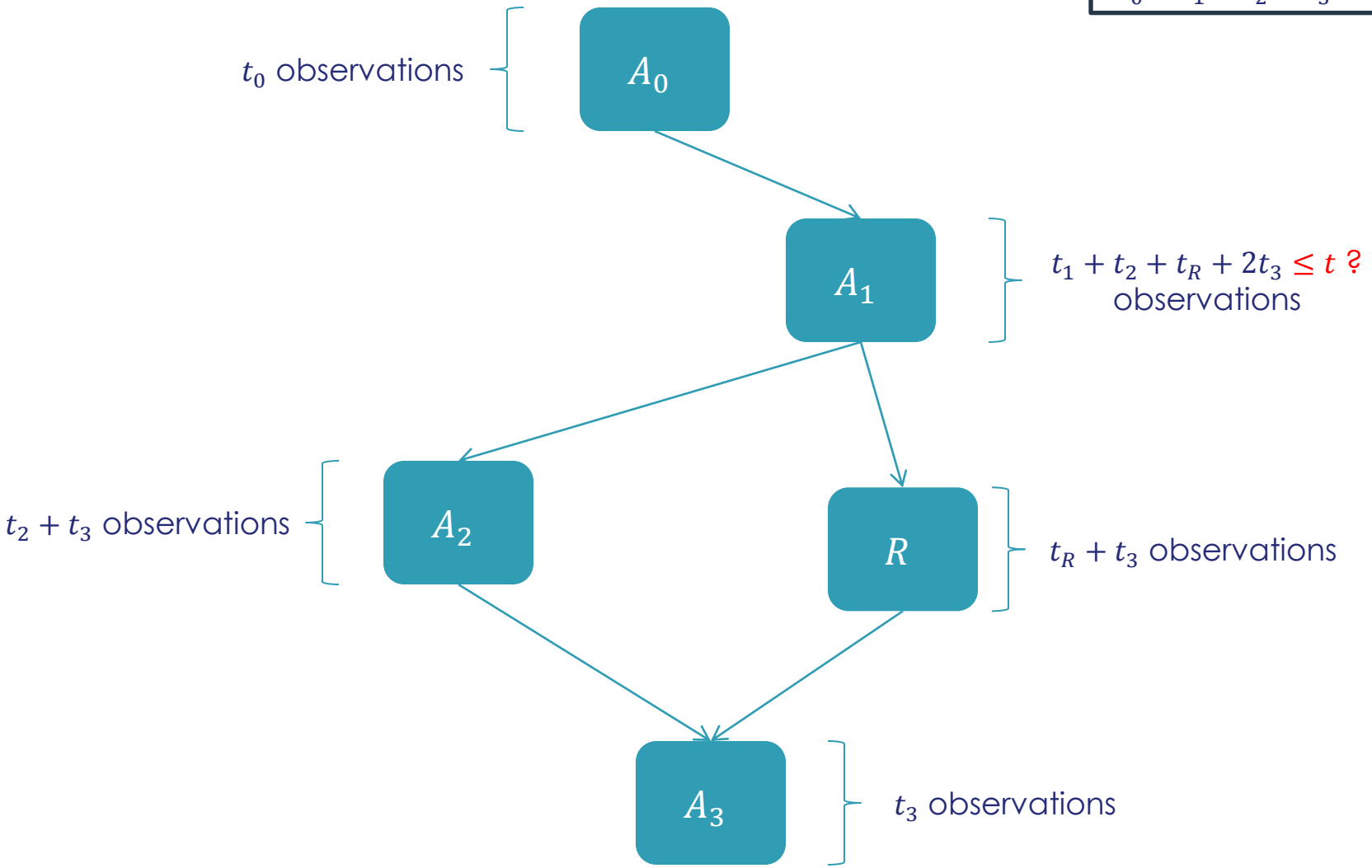
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$

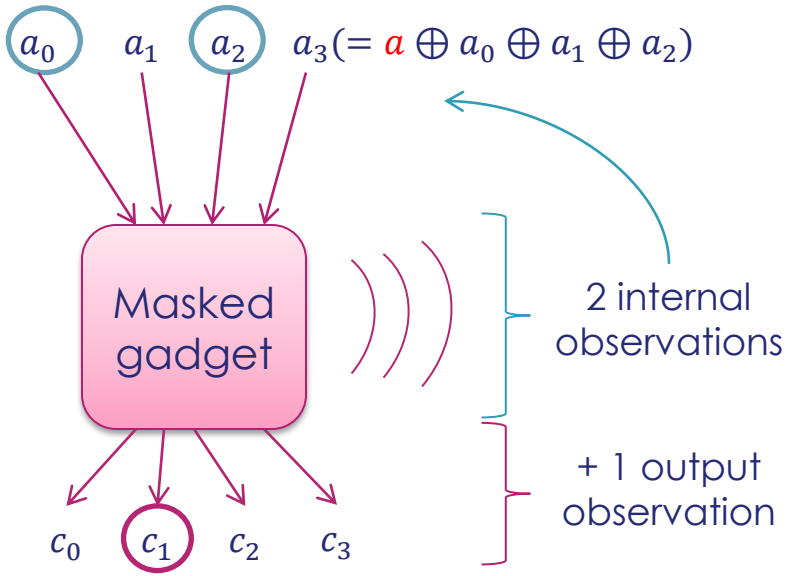


Stronger security properties in the t-probing model

Strong non-interference in the t-probing model

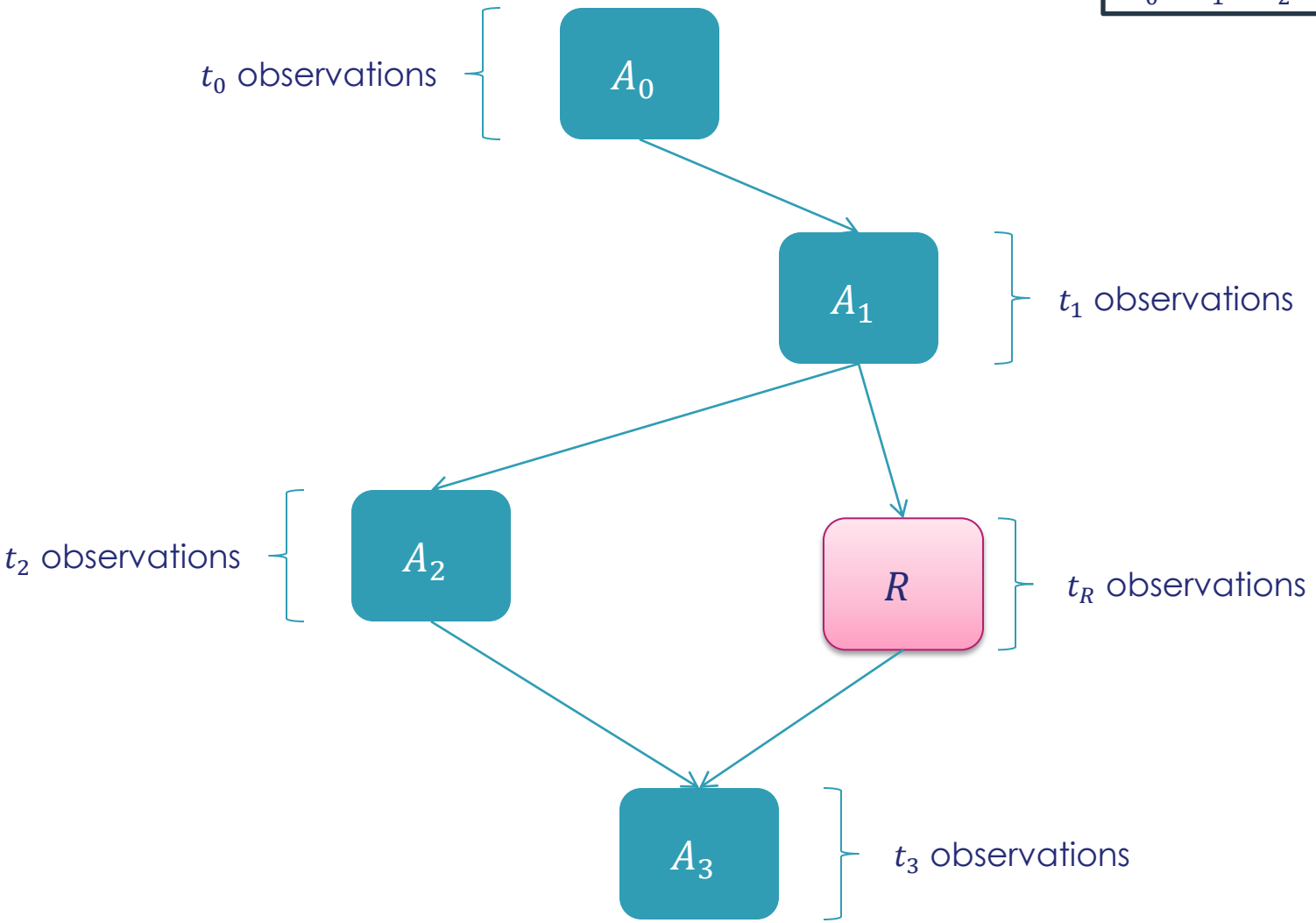
- If t is not fixed: show that any set of t intermediate variables with
  - t_1 on internal variables
  - $t_2 = t - t_1$ on the outputs

  can be simulated with at most t_1 shares of each input



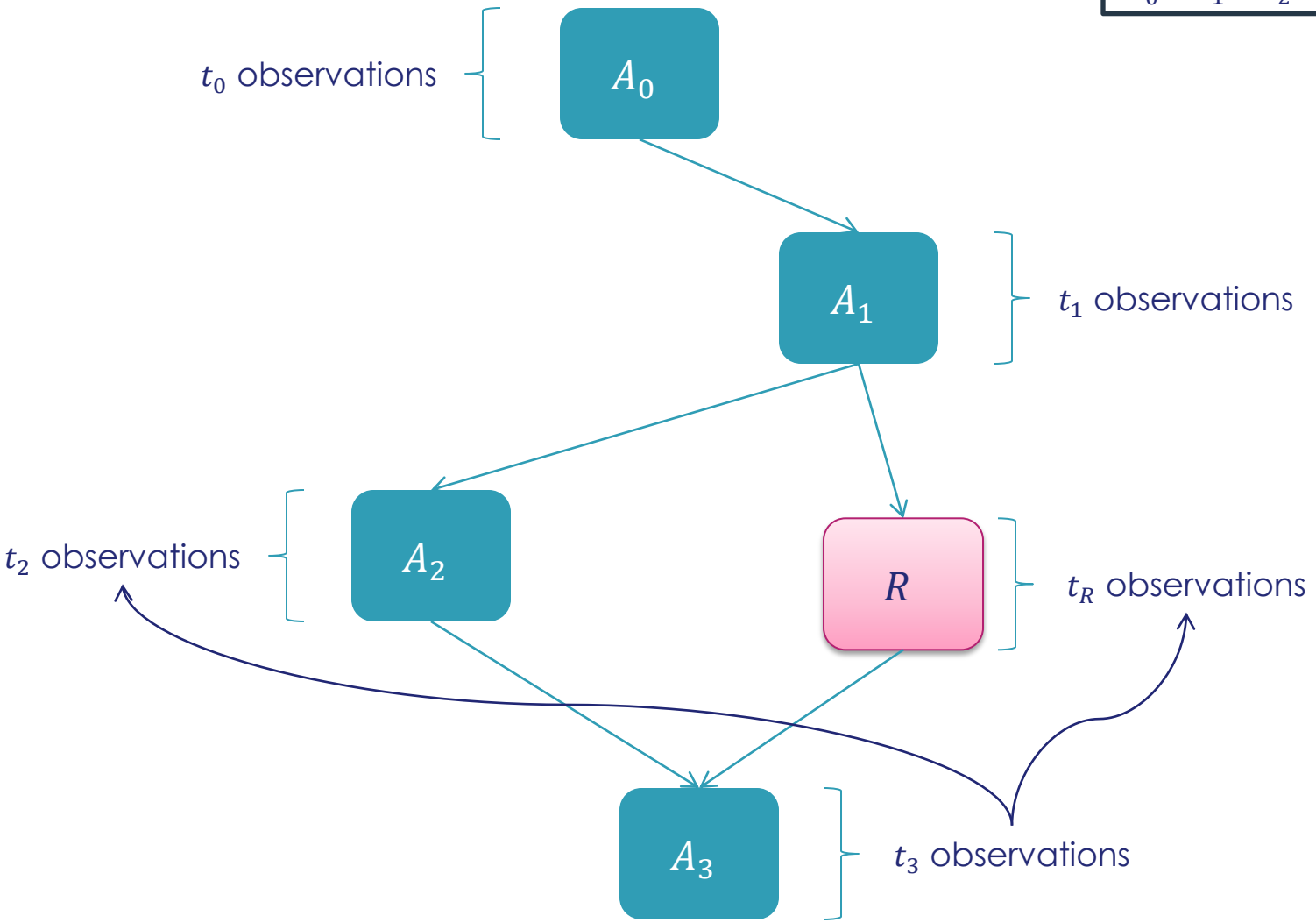
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



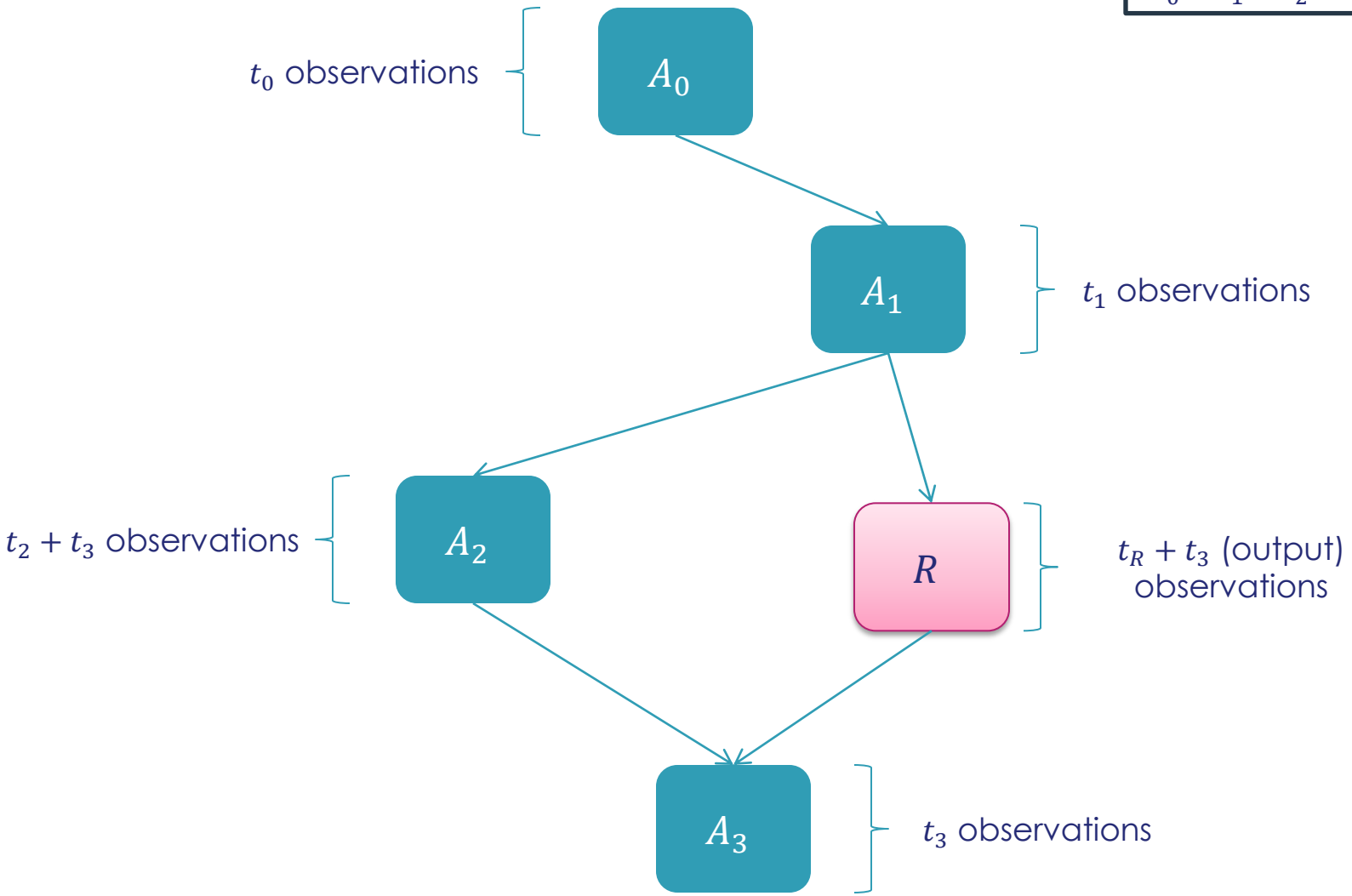
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



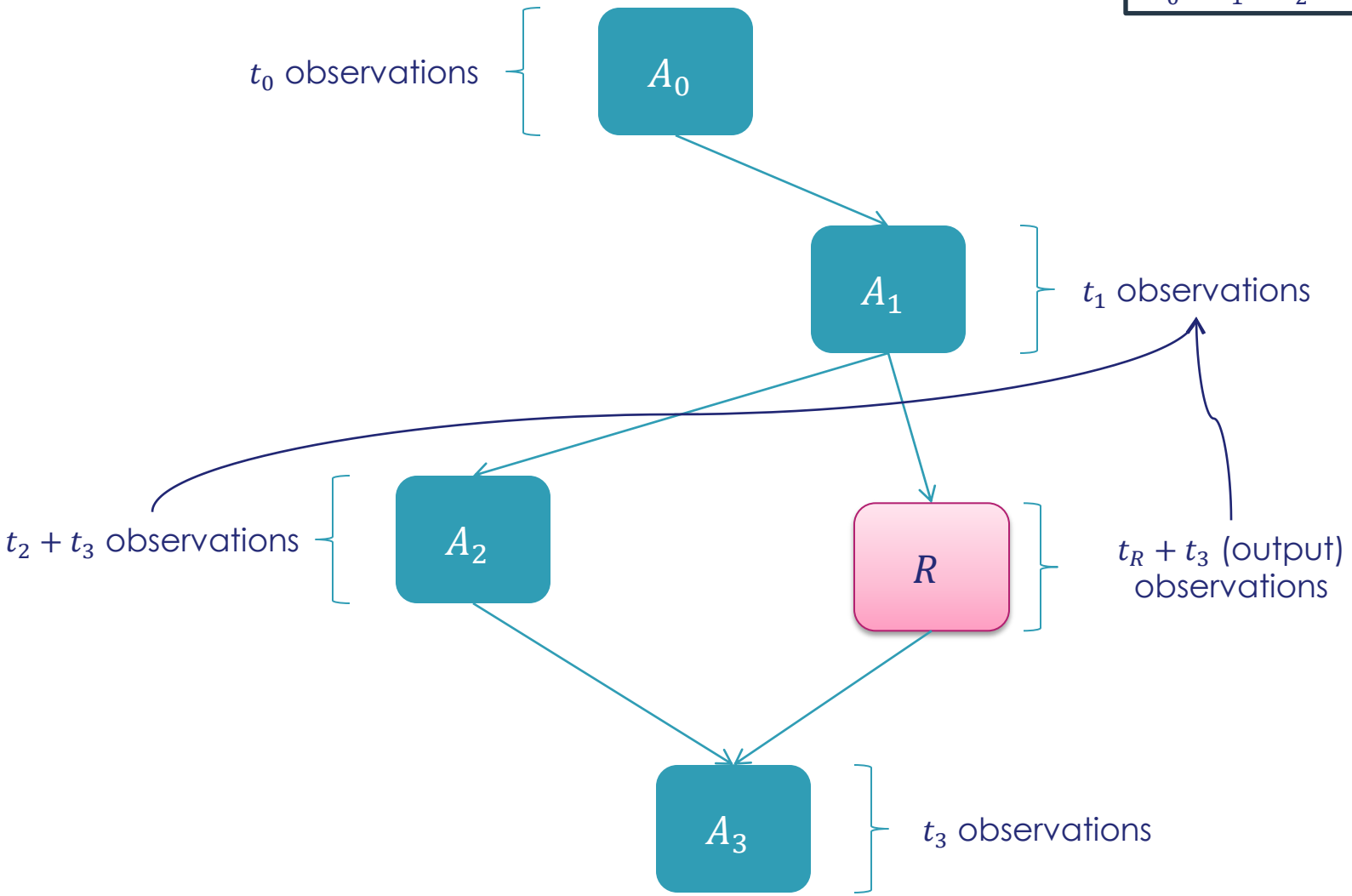
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



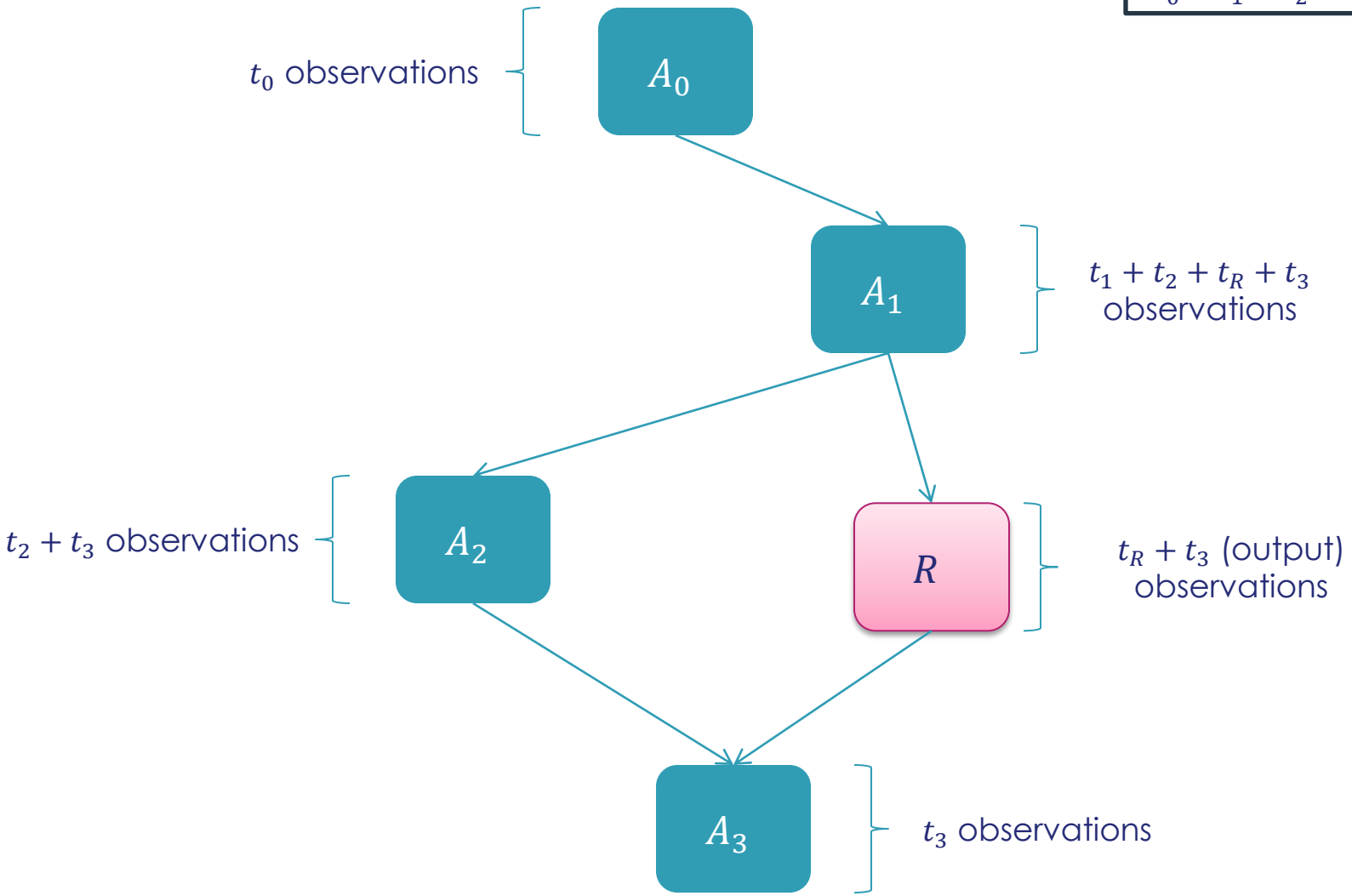
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



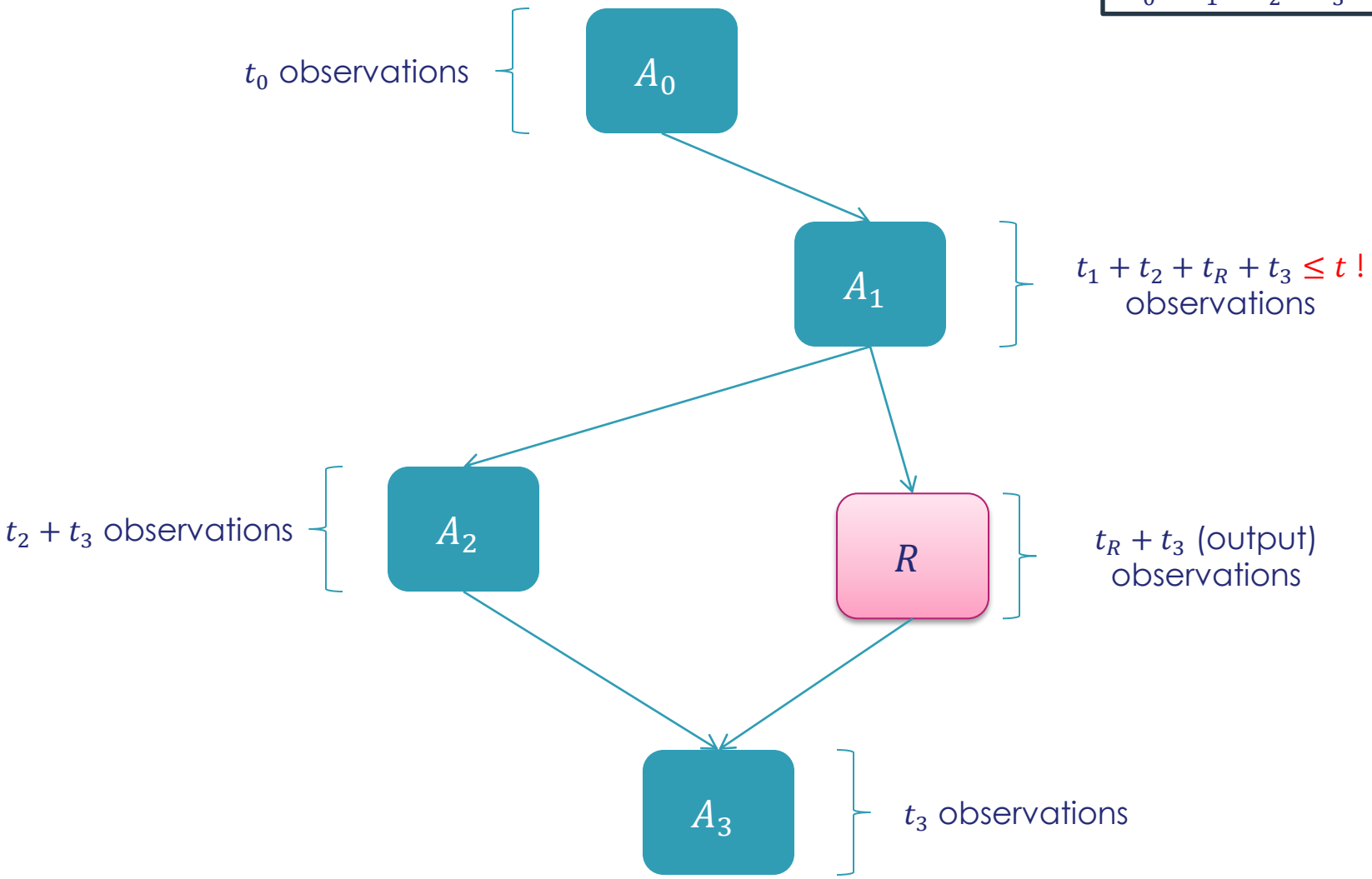
Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



Current Issues

$t_0 + t_1 + t_2 + t_3 + t_R \leq t$



MaskComp

New properties

- New properties on individual blocks
- Theorems based on these new properties to combine blocks

Underlying Formal Tool: EasyCrypt

Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, and Rebecca Zucchini.
Strong Non-Interference and Type-Directed Higher-Order Masking.
CCS 2016.

New Notion: f-NI

f non-interference in the t-probing model

- If t is not fixed: show that any set of t intermediate variables with
  - t_1 on internal variables
  - $t_2 = t - t_1$ on the outputs

  can be simulated with at most $f(t_1, t_2)$ shares of each input

$$f(t_1, t_2) = t_1 \leftrightarrow SNI$$
$$f(t_1, t_2) = t_1 + t_2 \leftrightarrow NI$$

Two main applications so far

- More accurate composition with granularity
- Composition of glitch-free functions for which $f(t_1, t_2)$ may be greater than $t_1 + t_2$

New Challenges

Leakage models

State of the art :
- Probing model
- Noisy leakage model

New challenges :
- Better reductions between leakage models
- Models which fit the reality of real components

Security

State of the art :
- Proofs in the probing and noisy models
- Formal proofs

New challenges :
- Formal proofs
- Proof of still unproven implementations
- New composition

Efficiency

State of the art :
- Masked high order gadgets

New challenges :
- **Still less randomness for masked gadgets**
- **Less multiplications for masked gadgets**

Efficiency for Higher-Order Probing Secure Multiplications

Current deployed t^{th}-order multiplication: ISW

- Security: SNI
- Efficiency:
  - random elements: $\frac{t(t+1)}{2}$
  - bilinear multiplications: t^2

$$c = a \cdot b$$

$$\downarrow$$

$$\forall\, i < j, \qquad r_{i,j} \leftarrow \$$$

$$\forall\, 0 \leq i \leq t, \qquad c_i = a_i \cdot b_i + \sum_{j=0}^{i-1} (r_{j,i} + a_i \cdot b_j + a_j \cdot b_i) + \sum_{j=i+1}^{t} r_{i,j}$$

Reducing the Randomness Complexity

Bounds on the randomness complexity

- Linear lower bound: $t + 1$ when $t \geq 3$
- Quasi-linear upper bound $O(t \log t)$

New t-NI multiplication gadget

- $\lfloor \frac{t^2}{4} \rfloor + t$ random bits instead of $\frac{t(t+1)}{2}$
- Main idea: repetition of the same random elements in different output shares

New NI multiplication gadgets for orders 2, 3 and 4

- linear bound of randomness complexity

Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud.
Randomness Complexity of Private Circuits for Multiplication.
Eurocrypt 2016.

Reducing the Randomness Complexity or the number of Multiplications

New t-SNI multiplication gadget with less bilinear multiplications

- $2t + 1$ instead of $O(t^2)$
- In large enough finite fields
- Main idea ($\delta_{i,j} = 1 - \gamma_{i,j}$):

$$a \cdot b = \left(a_0 + \sum_{i=1}^{t}(r_i + a_i)\right)\left(b_0 + \sum_{i=1}^{t}(s_i + b_i)\right) - \sum_{i=1}^{t} r_i\left(b_0 + \sum_{j=1}^{t}(\delta_{i,j}s_j + b_j)\right) - \sum_{i=1}^{t} s_i\left(a_0 + \sum_{j=1}^{t}(\gamma_{i,j}r_j + a_j)\right)$$

New t-NI multiplication gadget with less random elements

- t instead of $O(t \log t)$
- In large enough finite fields
- Output shares: $c_i = a_0 b_i + \sum_{j=1}^{t}(\gamma_{i,j}r_j + a_j b_i)$

Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud.
Private Multiplication over Finite Fields.
To appear in the proceedings of CRYPTO 2017.

Efficiency for Higher-Order Probing Secure Multiplications

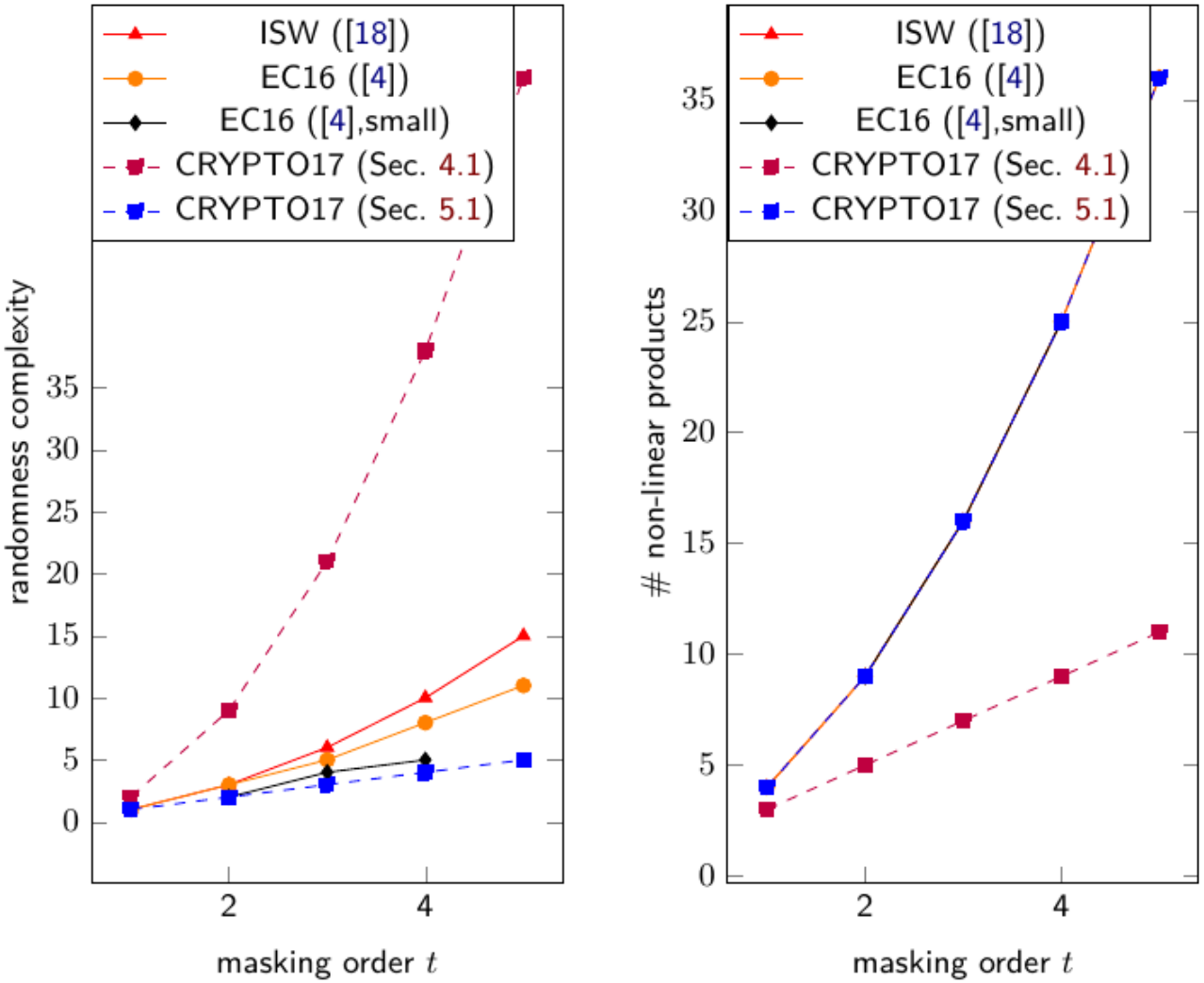


Fig. 1: Complexity in number of random elements in $\mathbb{F}_q$ (left) and on number of non-linear multiplications (right) in new and existing constructions

THALES

Outline

- Power-Analysis Attacks and Countermeasures
- The Case of Small Orders Attacks
- New Challenges to Counteract Higher-Order Attacks
- **Perspectives**

Perspectives

Leakage models

- New leakage models which
  - Fit the reality of embedded devices
  - Are convenient for security proofs
- Improve the reduction bounds between existing ones

Security

- Properly define f-NI notion to obtain more efficient and secure gadgets

Efficiency

- Still less randomness and number of multiplications in higher-order secure gadgets

Perspectives

Leakage models

- New leakage models which
  - Fit the reality of embedded devices
  - Are convenient for security proofs
- Improve the reduction bounds between existing ones

Security

- Properly define f-NI notion to obtain more efficient and secure gadgets

Efficiency

- Still less randomness and number of multiplications in higher-order secure gadgets

Thank you.