RE-TRUST Meeting, St. Petersburg

Private Circuits Revisited:

Provable Security Guarantees on Boolean Circuits

Sebastian Faust

KU Leuven, ESAT-COSIC

Gap in Provable Security

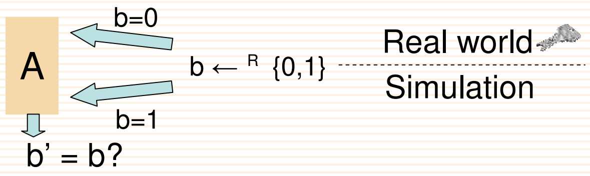
Approach in provable security

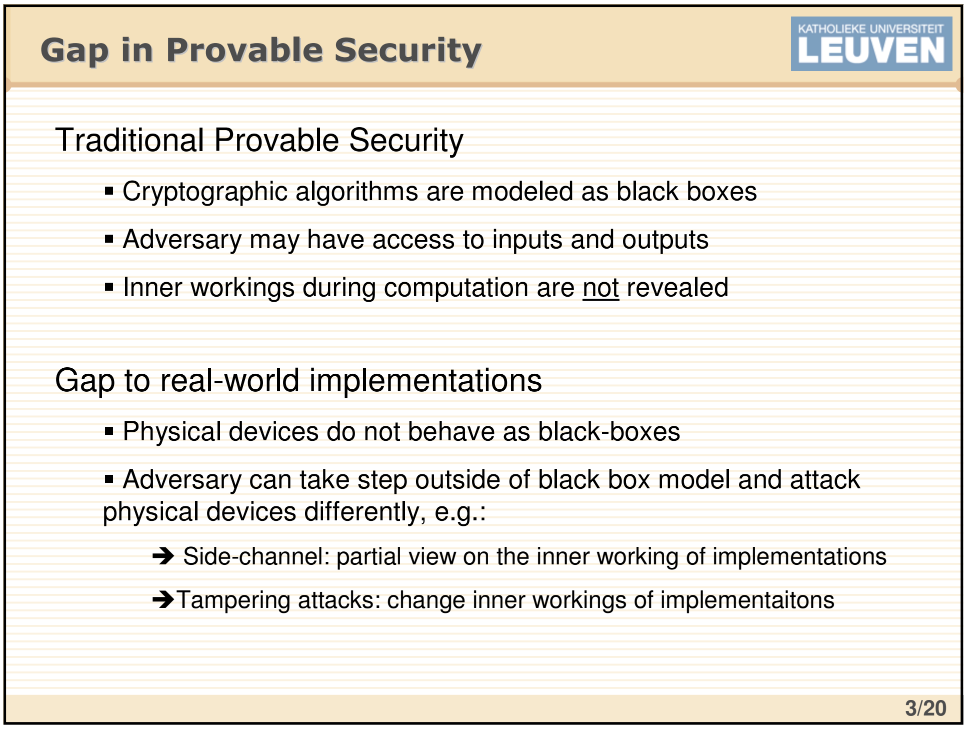
- Develop adversarial model
- Define what is understood under the security of algorithm
- Prove that **no** adversary can exist under reasonable assumptions

  ➔ prove security always against **any** adversary

Proof by simulation

Show that there exists a simulator that without the „secret“ can produce an outcome that is indistinguishable from „real world“.





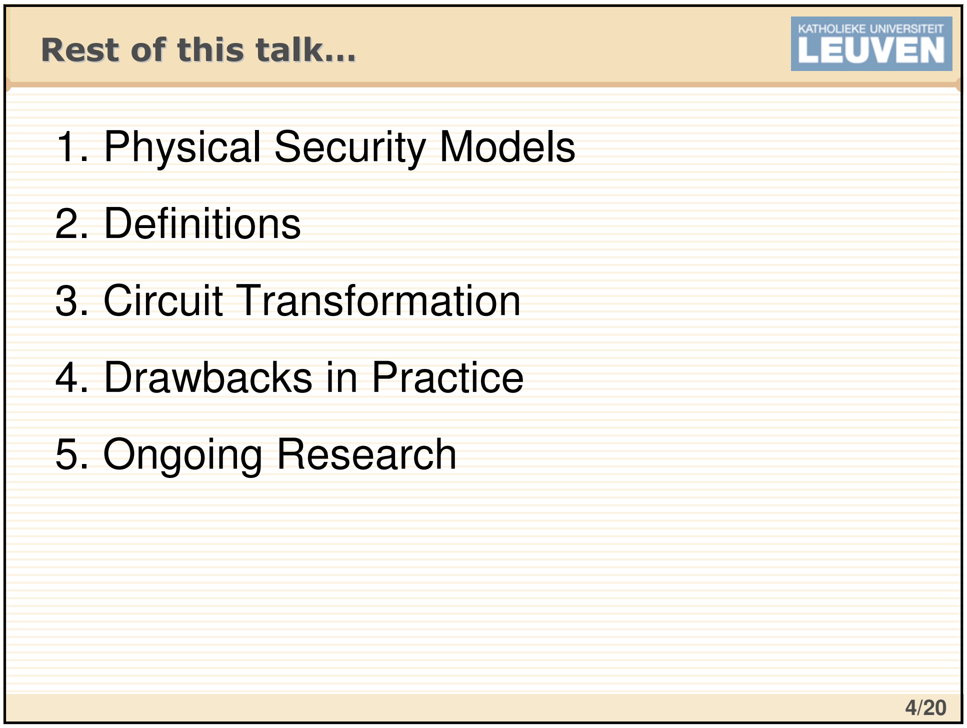
Gap in Provable Security

Traditional Provable Security

- Cryptographic algorithms are modeled as black boxes
- Adversary may have access to inputs and outputs
- Inner workings during computation are not revealed

Gap to real-world implementations

- Physical devices do not behave as black-boxes
- Adversary can take step outside of black box model and attack physical devices differently, e.g.:
  - ➔ Side-channel: partial view on the inner working of implementations
  - ➔Tampering attacks: change inner workings of implementaitons



Rest of this talk…

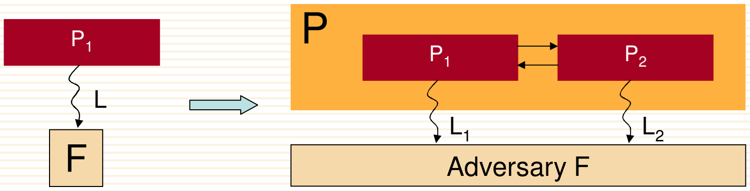
1. Physical Security Models
2. Definitions
3. Circuit Transformation
4. Drawbacks in Practice
5. Ongoing Research

1. Physical Security Models

KATHOLIEKE UNIVERSITEIT LEUVEN

Close the gap in provable security

1. M&R Model: Model computation as Turing machine but augement it with leakage function to cover all possible leakages
   - Goal: Given PO secure building block P_1, can we build more complex constructions P?



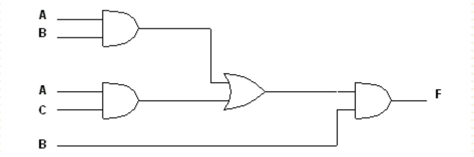
   - The M&R model seems not to be suitable for the analysis of practical constructions ➔ For every scheme new tailored PO assumptions on underlying building blocks are required

1. Physical Security Models

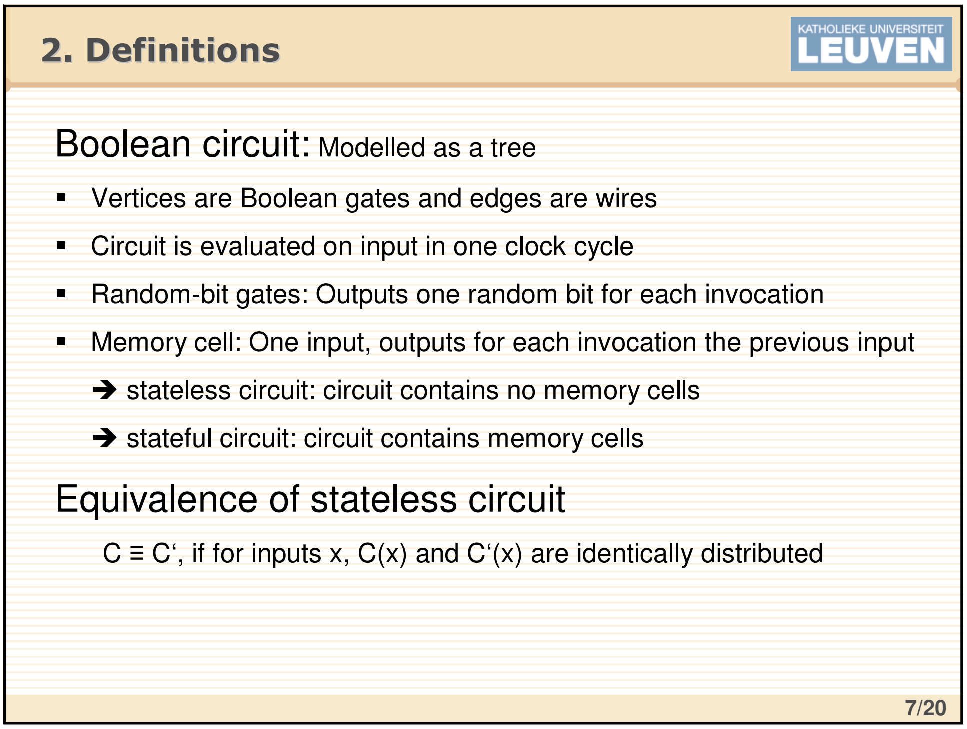
KATHOLIEKE UNIVERSITEIT LEUVEN

Close the gap in provable security

2. ISW03 model: Consider specific implementations and a particular adversarial model
   - Computing device: Only boolean circuits with very limited instruction set and memory



   - Adversarial Model: Adversary is „only" allowed to probe t wires
   - Goal: Construction where the adversary learns **no** additional information (e.g. content of memory) by probing t wires (i.t.)



2. Definitions

KATHOLIEKE UNIVERSITEIT LEUVEN

Boolean circuit: Modelled as a tree

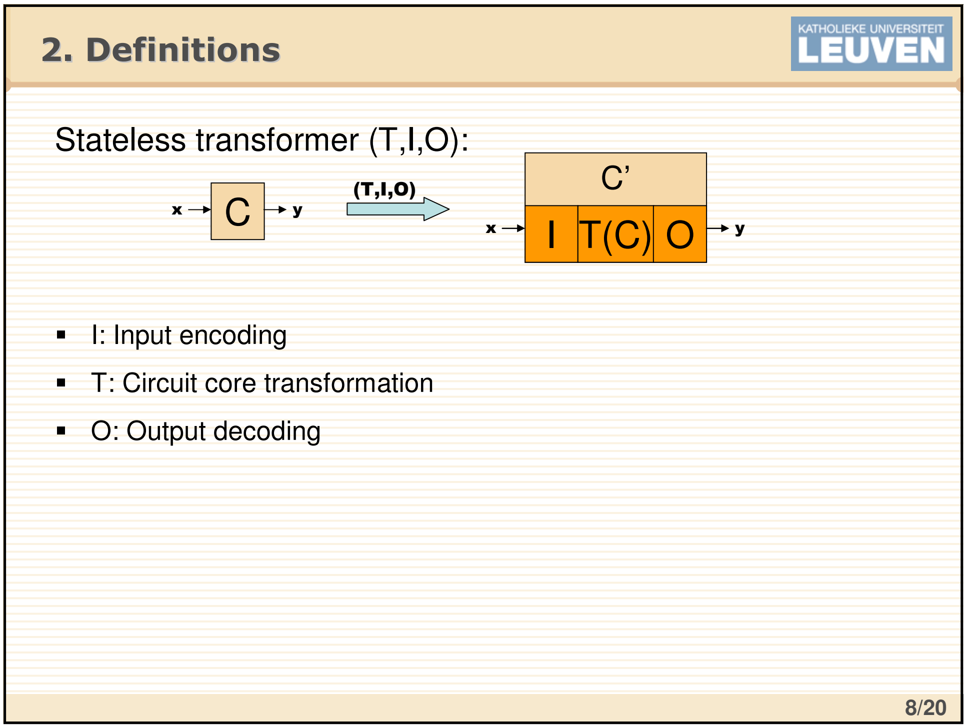
- Vertices are Boolean gates and edges are wires
- Circuit is evaluated on input in one clock cycle
- Random-bit gates: Outputs one random bit for each invocation
- Memory cell: One input, outputs for each invocation the previous input

➔ stateless circuit: circuit contains no memory cells

➔ stateful circuit: circuit contains memory cells

Equivalence of stateless circuit

$C \equiv C'$, if for inputs x, $C(x)$ and $C'(x)$ are identically distributed



2. Definitions

KATHOLIEKE UNIVERSITEIT LEUVEN

Stateless transformer (T,I,O):

x
C
y
(T,I,O)
C'
x
I
T(C)
O
y

- I: Input encoding
- T: Circuit core transformation
- O: Output decoding

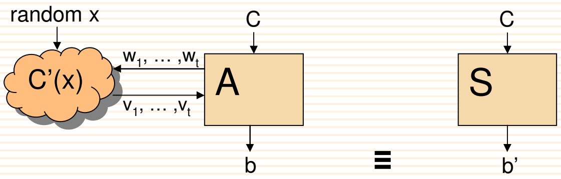
2. Definitions

Properties of a Stateless Transformer (T,I,O)

- Soundness: For all C it holds that C ≡ O ○ T(C) ○ I
- Privacy: For every t-limited adversary A there exists a 0-limited simulator S, such that for every circuit C and every input x, the output distribution of A and S are identically distributed.

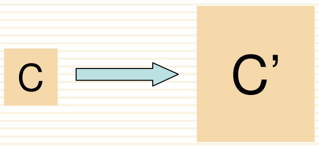
  ➔ A learns no new information by probing

  ➔ Note: A tries to learn information on input/output of the circuit



3. Circuit Transformation

Theorem [ISW03]: There exists a t-private stateless transformer (T,I,O) which maps any circuit C of size n to a randomized stateless circuit of size $O(nt^2)$

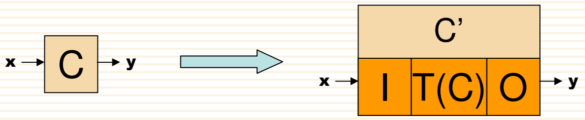


Basic Idea:

- Use additive secret sharing and split every input in t shares
- Replace every gate in C by a new (secure) gadget in C'
- Show for every input x to C: Pr[x = 1| Adversary probes t wires] = 1/2

3. Circuit Transformation

Transformation (T,I,O):

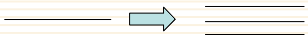


- Input Encoding I: Input: x; Output: t+1 additive shares $r_1, \ldots, r_{t+1}$ of x
  - Choose t random bits: $r_1, \ldots, r_t$
  - $r_{t+1} = x + r_1 + \ldots r_t$
- Output Decoding O: Input: t+1 shares of y; Output: y
  - $y = y_1 + \ldots + y_{t+1}$

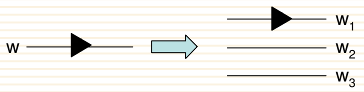
3. Circuit Transformation

Circuit Core Transformation T(C) (wlog C has only NOT and AND gates):

- Replace every wire w in C by t+1 wires carrying an (t+1,t+1) additive secret sharing of the value on w



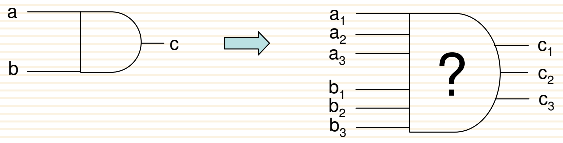
- NOT gate on wire w: put NOT gate on w_1



$\rightarrow \neg w = \neg w_1 + w_2 + w_3$

3. Circuit Transformation

AND gate with inputs a,b and output c



Observe: $c = ab = (a_1 + ... + a_{t+1})(b_1 + ... + b_{t+1}) = a_1b_1 + ... + a_{t+1}b_{t+1}$

First attempt: $c_i = a_ib_1 + \dots + a_ib_{t+1} = a_i (b_1 + ... + b_{t+1})$

- Soundness: $c = c_1 + .. + c_{t+1}$
- Privacy: No! Probing only one wire results in bias
  - Let t=3. Probing of $c_1 = a_1b$ ➔ $\Pr[b = 1|c_1 = 1] = 1 \neq ½$

3. Circuit Transformation

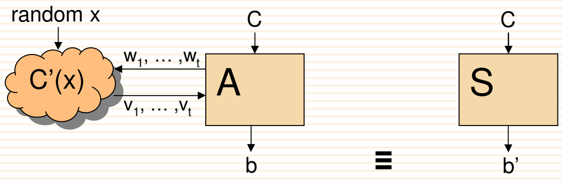
AND gate with inputs a,b and output c

- Compute intermediate values z_{ij} for $i \neq j$
  - If $1 <= i < j <= t+1$: Introduce a random bit gate z_{ij}
  - Else: $z_{ij} = (z_{ji} + a_ib_j) + a_jb_i$
- Output of AND gate: $c_i = a_ib_i + z_{i1} + \dots + z_{it+1}$
- Soundness:
  - Observe: $z_{ij} + z_{ji} = a_ib_j + a_jb_i$

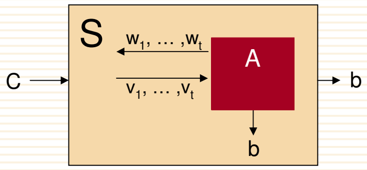
$$\begin{array}{c} c_1 \\ c_2 \\ c_3 \end{array} \begin{pmatrix} a_1b_1 & z_{12} & z_{13} \\ z_{21} & a_2b_2 & z_{23} \\ z_{31} & z_{32} & a_3b_3 \end{pmatrix}$$

3. Circuit Transformation

Privacy: For every t-limited adversary A there exists a 0-limited simulator S, such that for every circuit C and every input x, the output distribution of A and S are identically distributed.



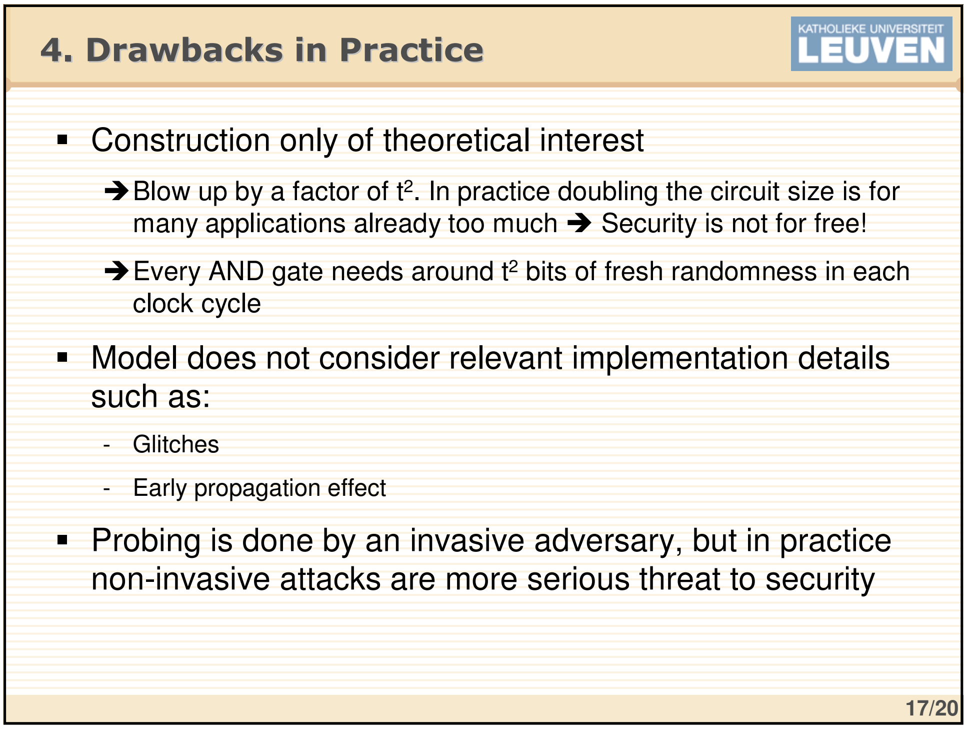
Proof idea:



3. Circuit Transformations

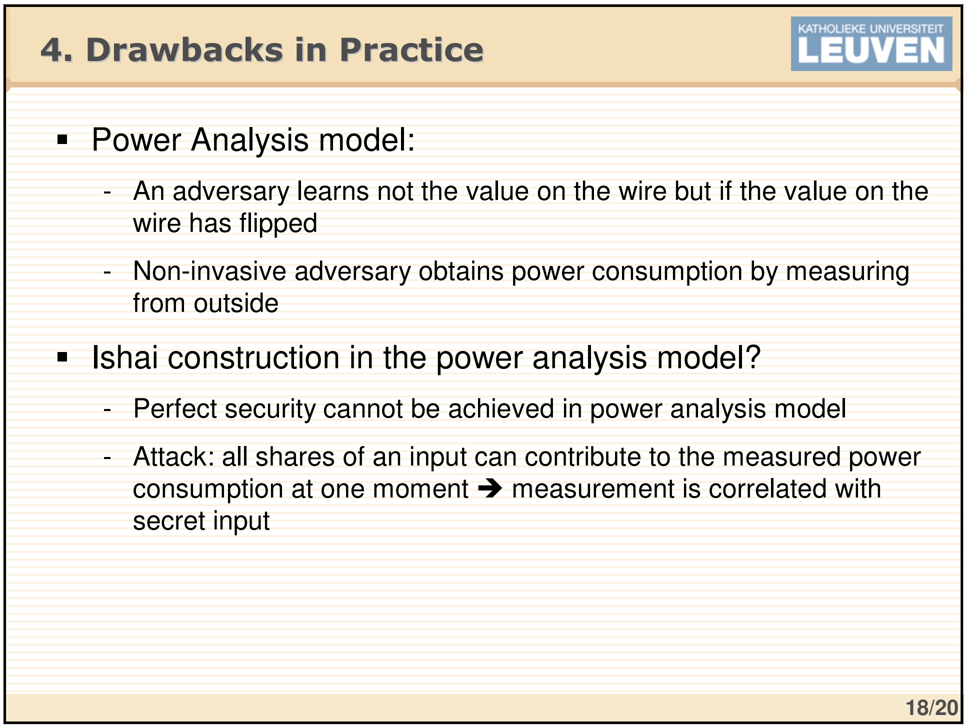
Further Results (Ishai et al.):

- More efficient constructions for statistic security
  - Statistic security: Small (but negligible) simulation error
  - Blow up of circuit size by only a factor of t, but the construction hides large constants ➔ only more efficient for large t
- More efficient constructions for a particular cryptographic scheme
  - Deterministic PRNG circuit with size O(nt)
  - The PRNG circuit can be used to replace the randmom bit gates in the general construction



4. Drawbacks in Practice

- Construction only of theoretical interest
  - ➔Blow up by a factor of t^2. In practice doubling the circuit size is for many applications already too much ➔ Security is not for free!
  - ➔Every AND gate needs around t^2 bits of fresh randomness in each clock cycle
- Model does not consider relevant implementation details such as:
  - Glitches
  - Early propagation effect
- Probing is done by an invasive adversary, but in practice non-invasive attacks are more serious threat to security



4. Drawbacks in Practice

- Power Analysis model:
  - An adversary learns not the value on the wire but if the value on the wire has flipped
  - Non-invasive adversary obtains power consumption by measuring from outside
- Ishai construction in the power analysis model?
  - Perfect security cannot be achieved in power analysis model
  - Attack: all shares of an input can contribute to the measured power consumption at one moment ➔ measurement is correlated with secret input

5. Ongoing Work

- New model to analyze security of boolean circuits in power analysis model that incorporates…
  - Glitches,
  - Early propagation effect,
  - Memory effect,
  - ……

Super-Model

- Design new logic style that achieves some provable security but still has practical relevance
  - ➔ Small blow-up factor
  - ➔ Only few fresh randomness per clock cycle

RE-TRUST Meeting, St. Petersburg

Thank you for your attention!