RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CRYP-T10**

My Gadget Just Cares For Me - How NINA Can Prove Security Against Combined Attacks

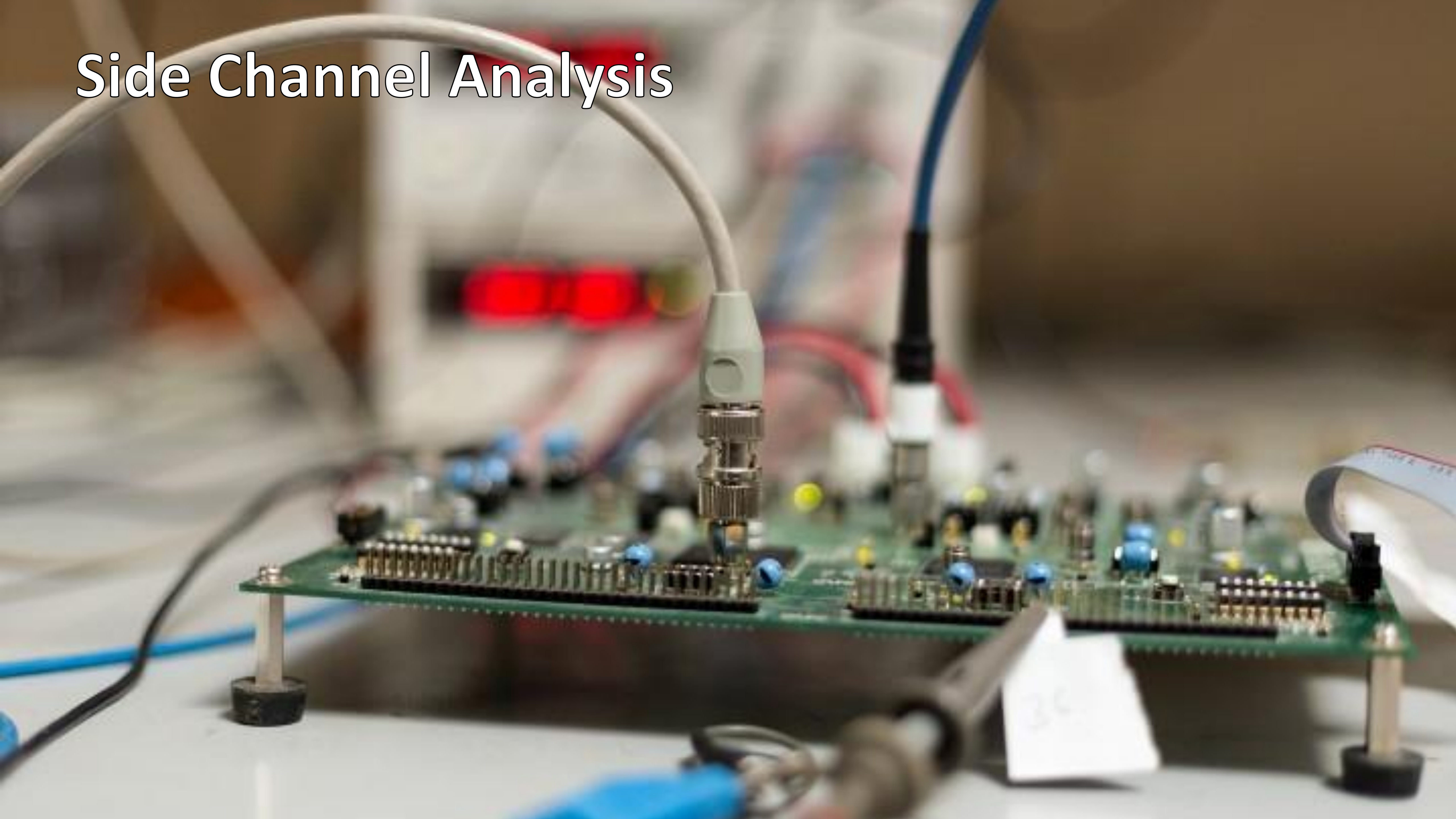
Siemen Dhooghe, Svetla Nikova

PhD Researcher
imec-COSIC, KU Leuven, Belgium

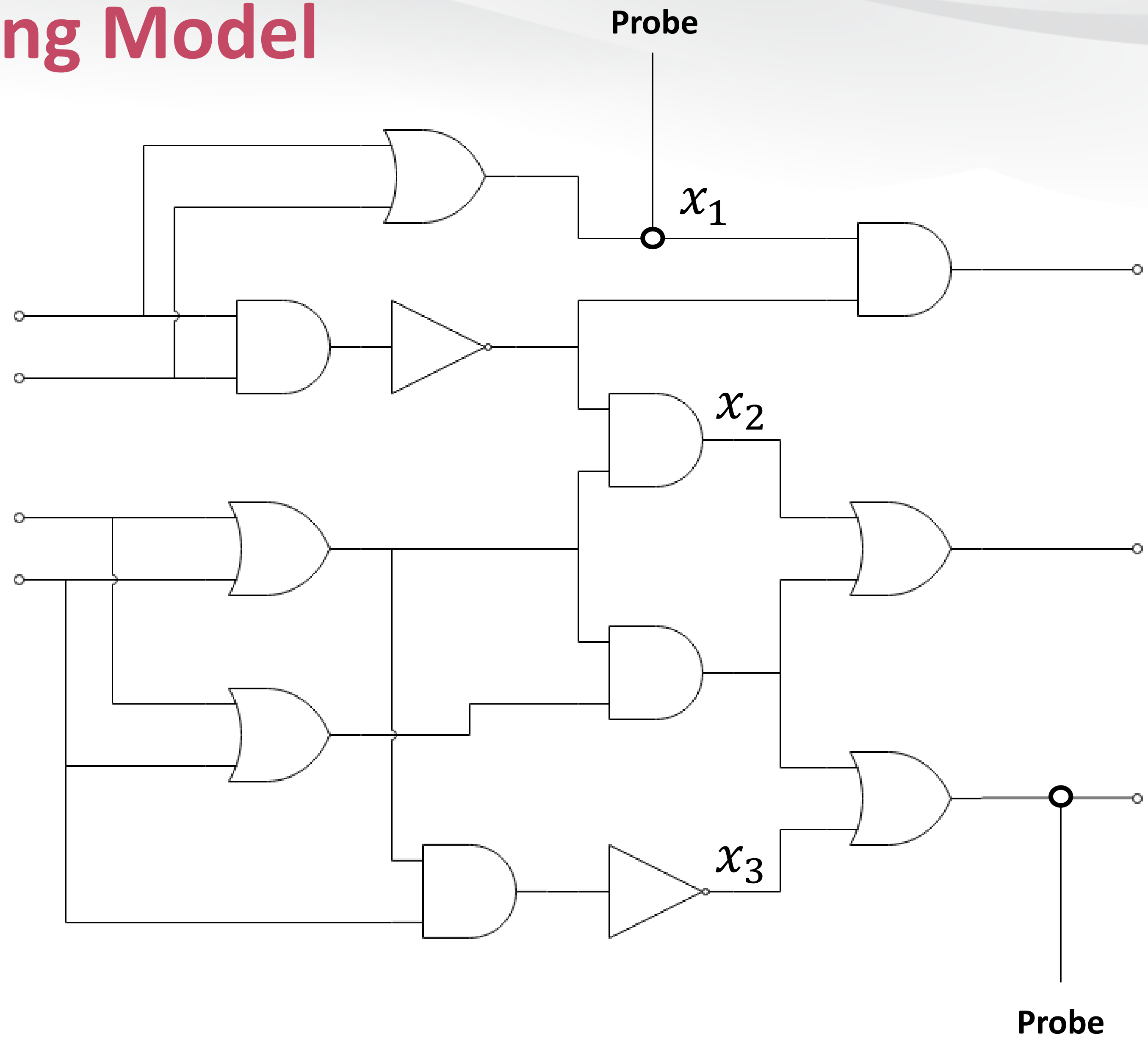
#RSAC

Embedded Security

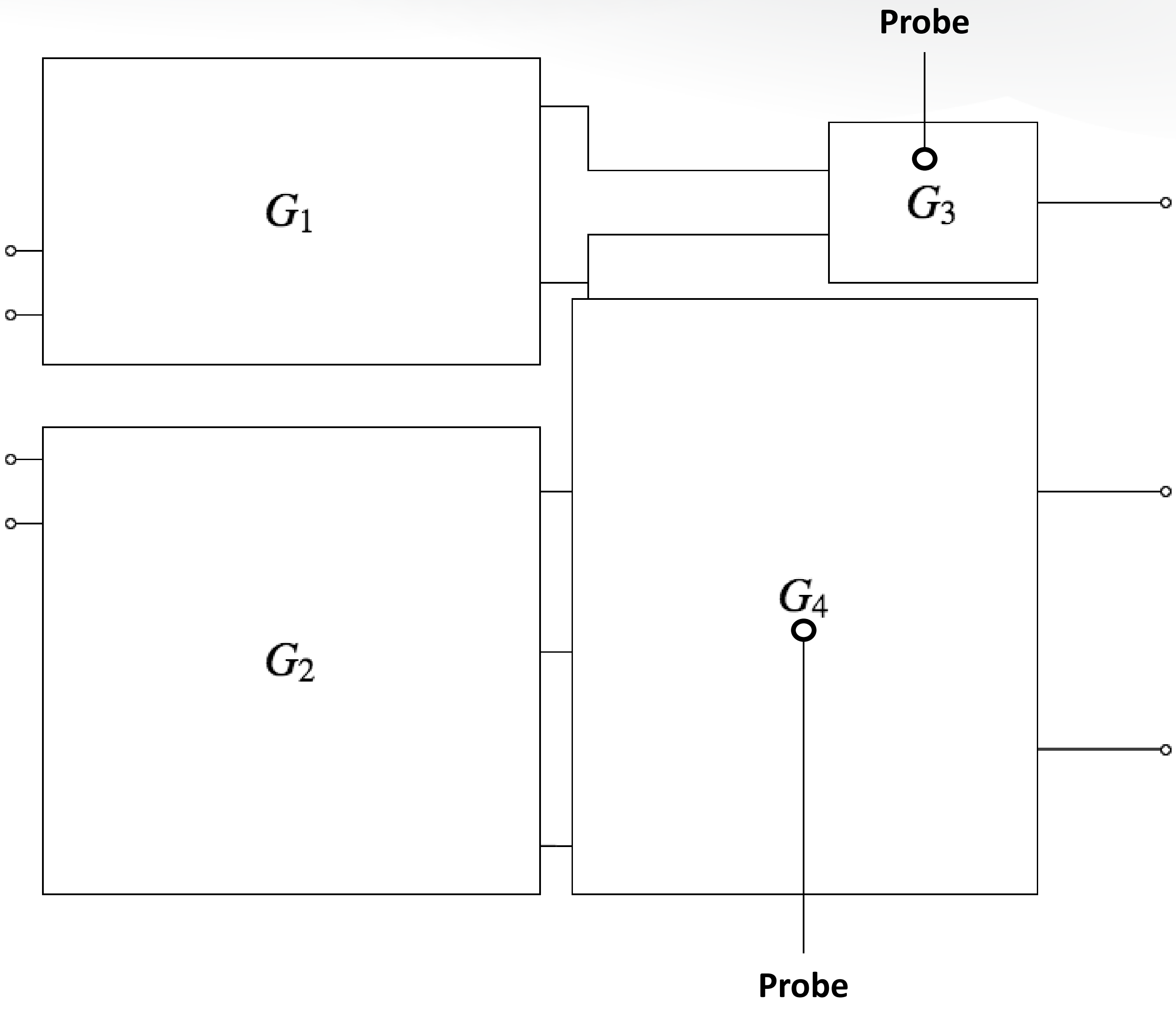
Side Channel Analysis



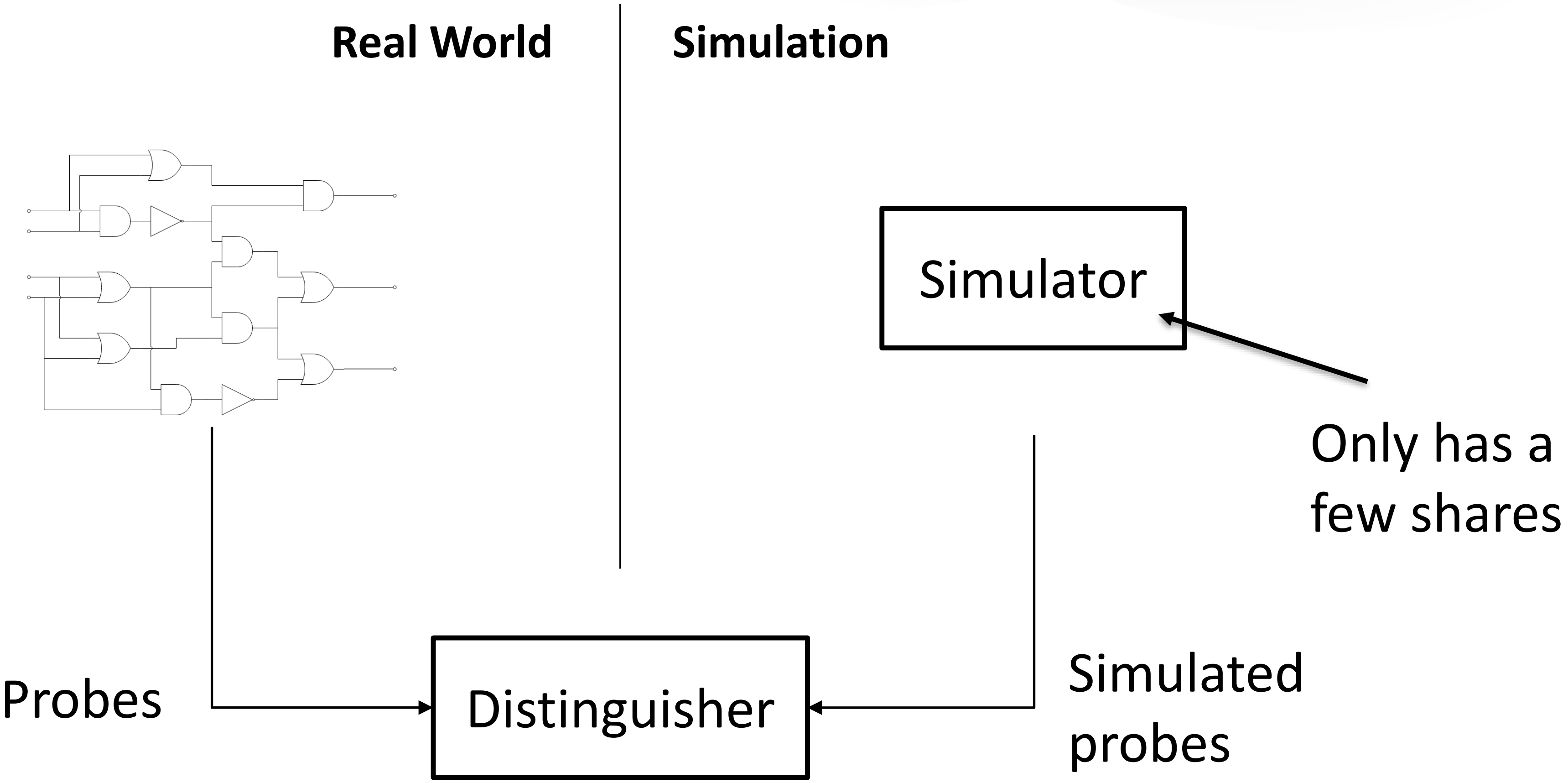
The Probing Model



Modular Circuits



Simulation Based Security



Real World

Simulation

Simulator

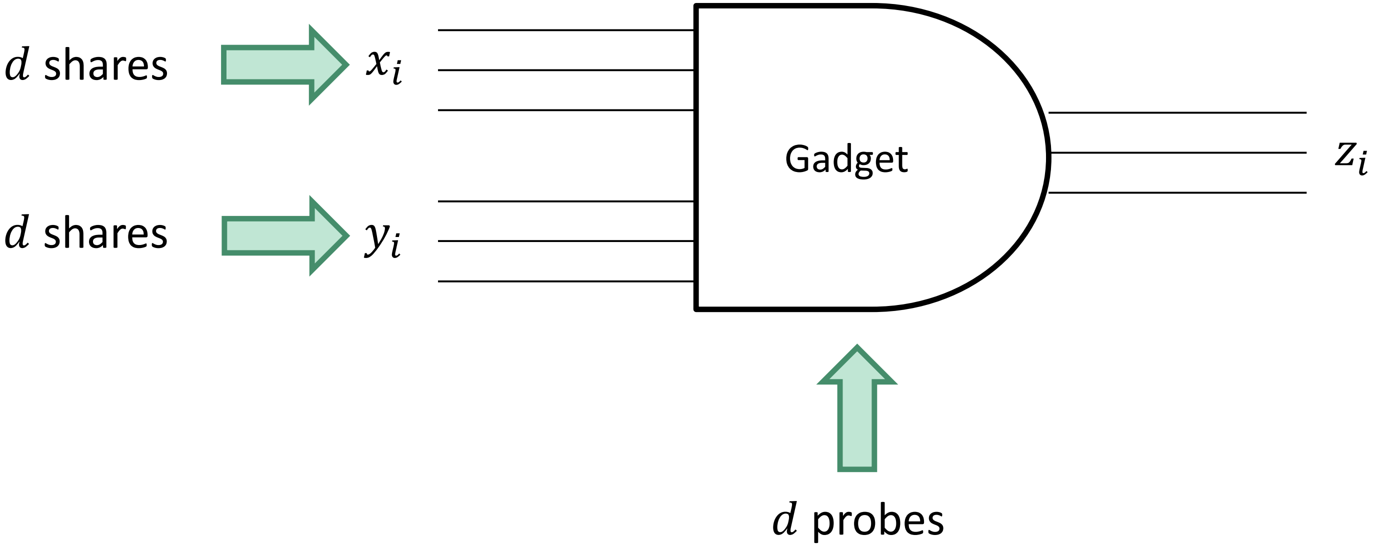
Only has a few shares

Probes

Distinguisher

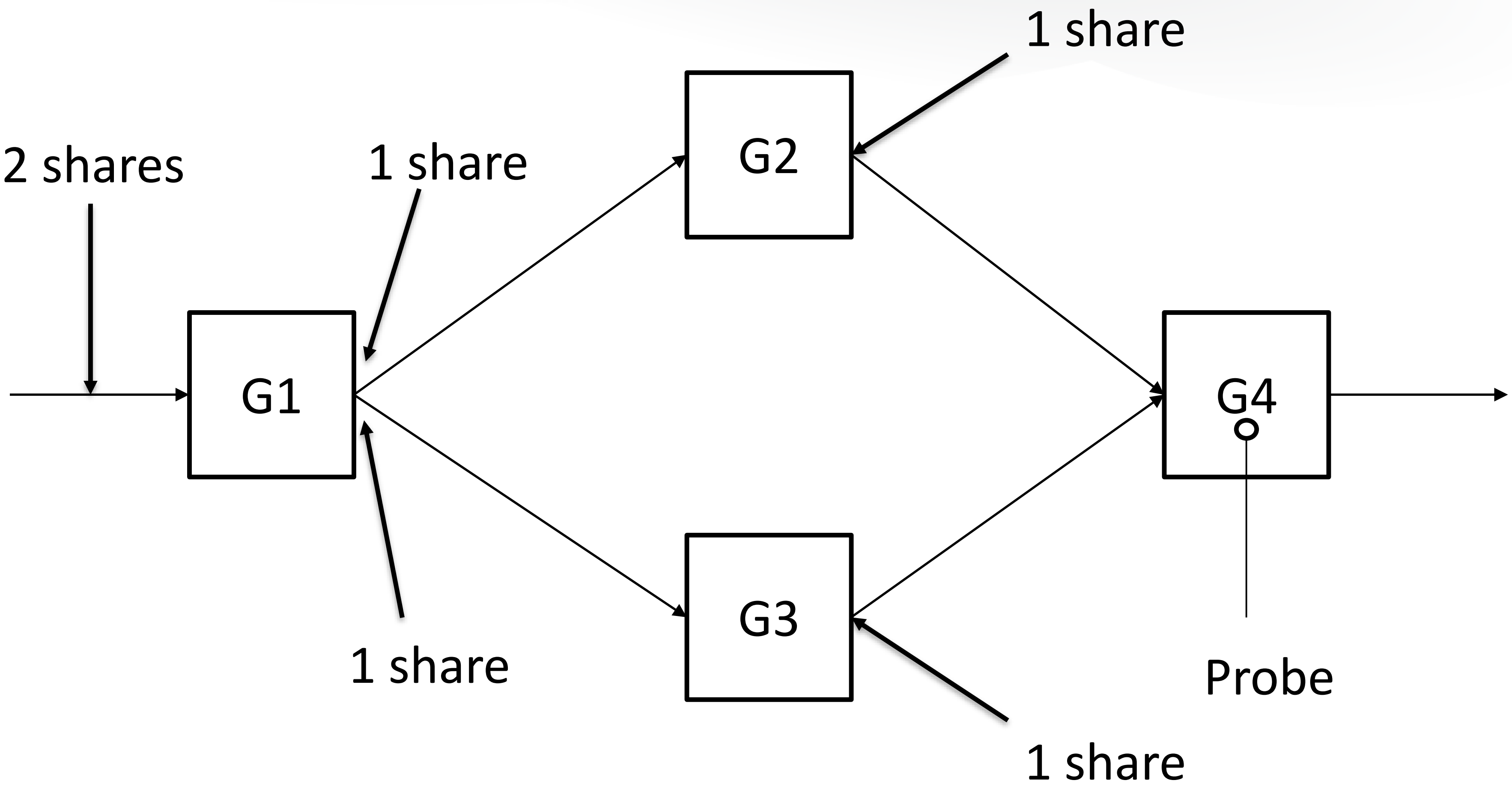
Simulated probes

Non-Interference

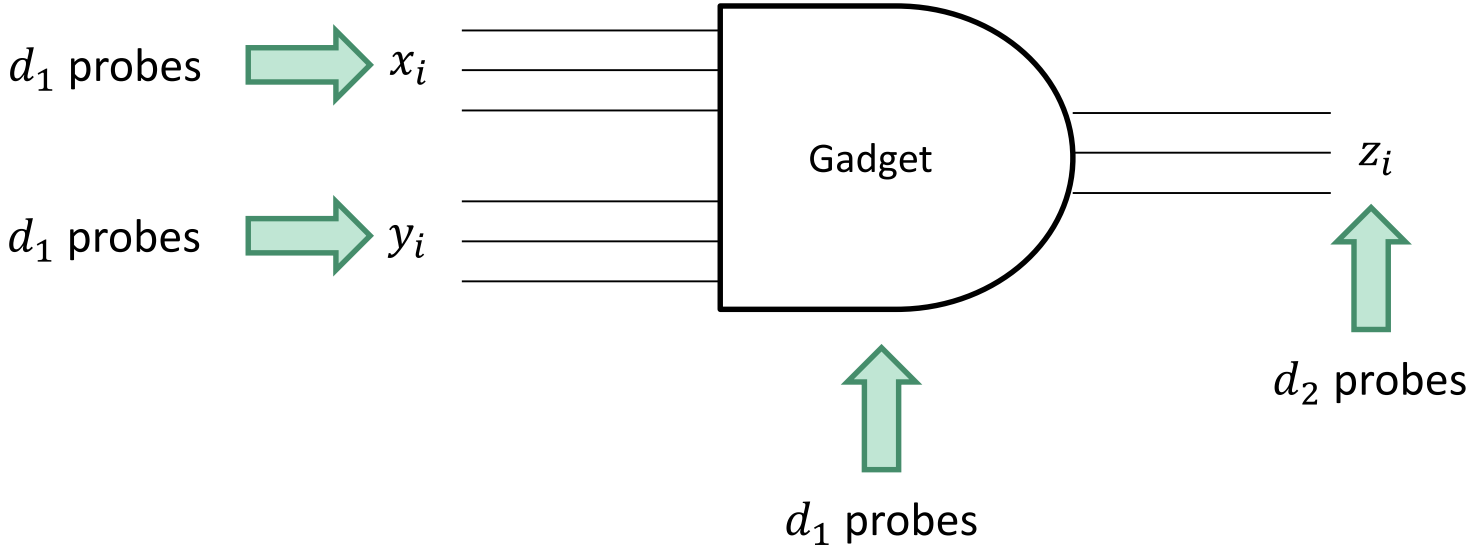


* Strong Non-Interference and Type-Directed Higher-Order Masking,
Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque,
Benjamin Grégoire, Pierre-Yves Strub, Rébecca Zucchini

Non-Interference

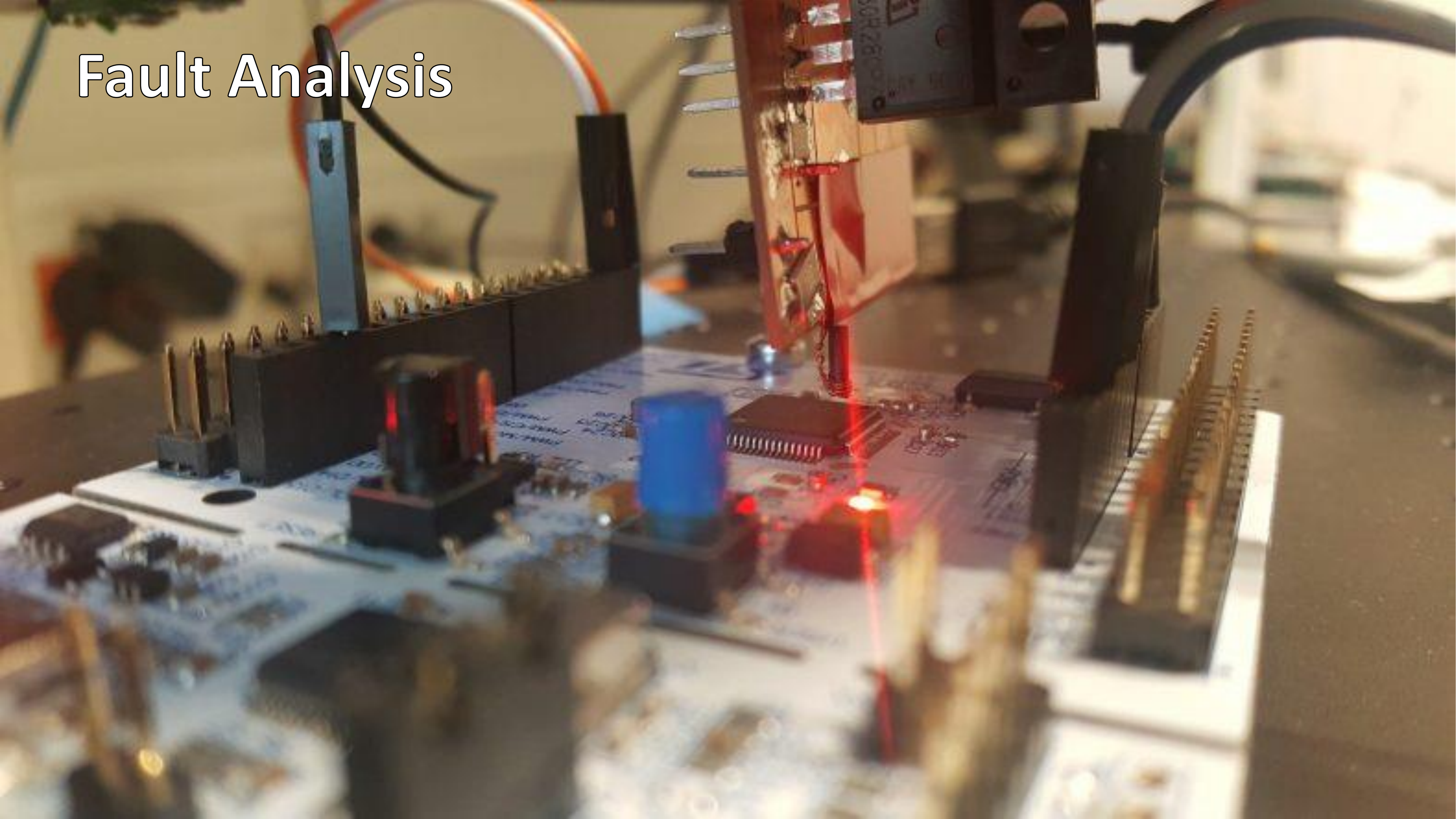


Strong Non-Interference

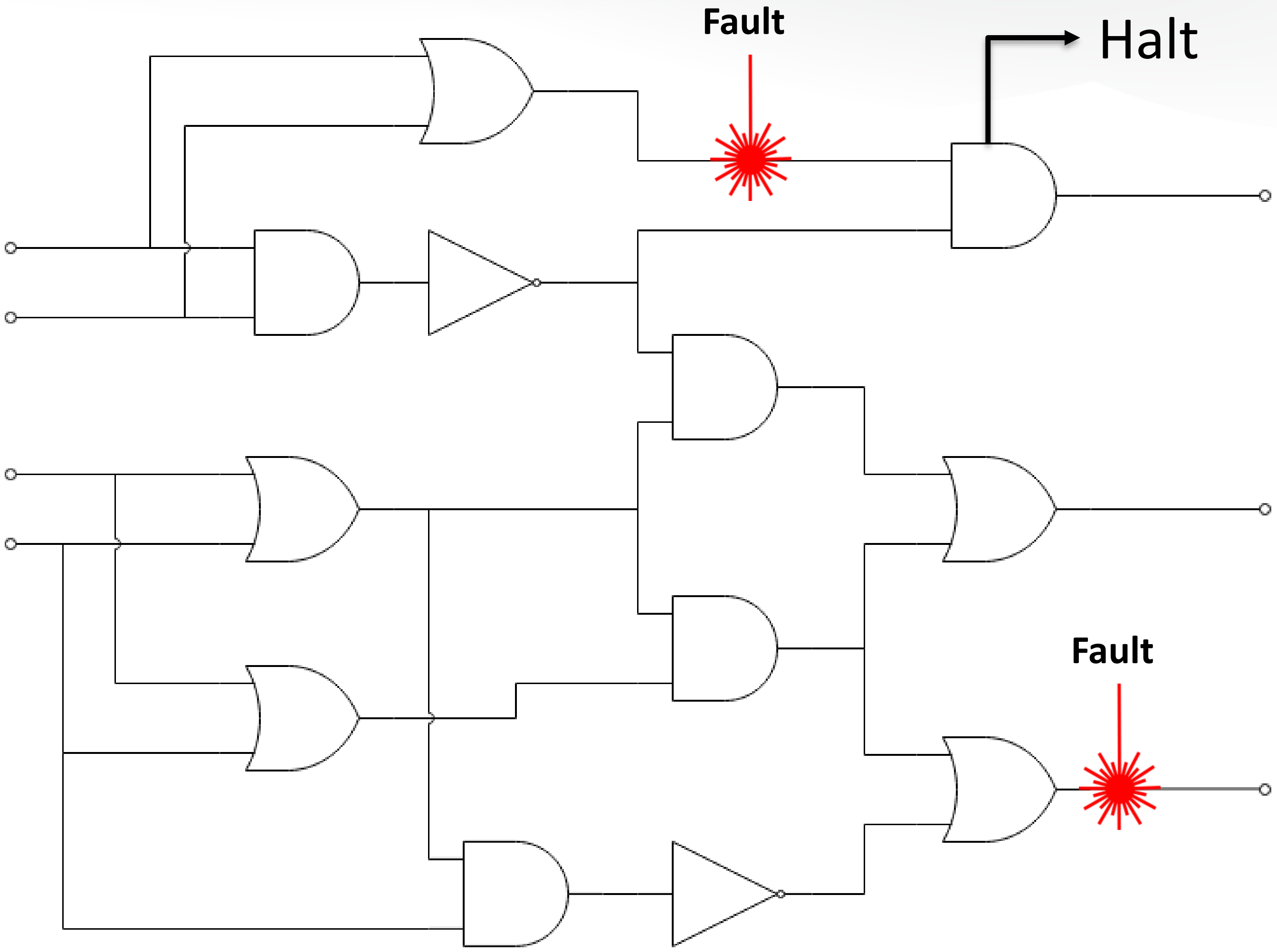


* Strong Non-Interference and Type-Directed Higher-Order Masking, Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, Rébecca Zucchini

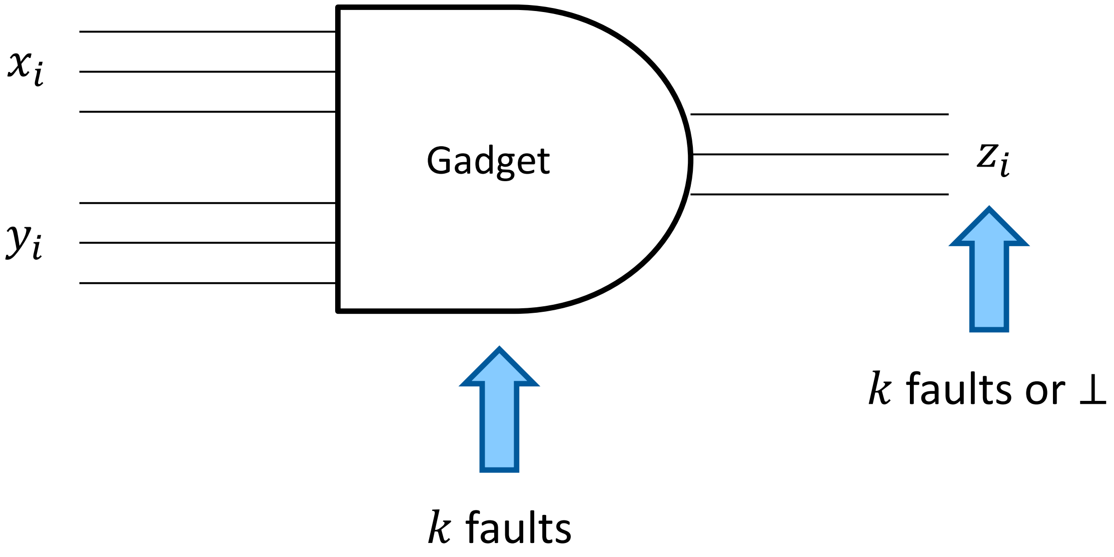
Fault Analysis



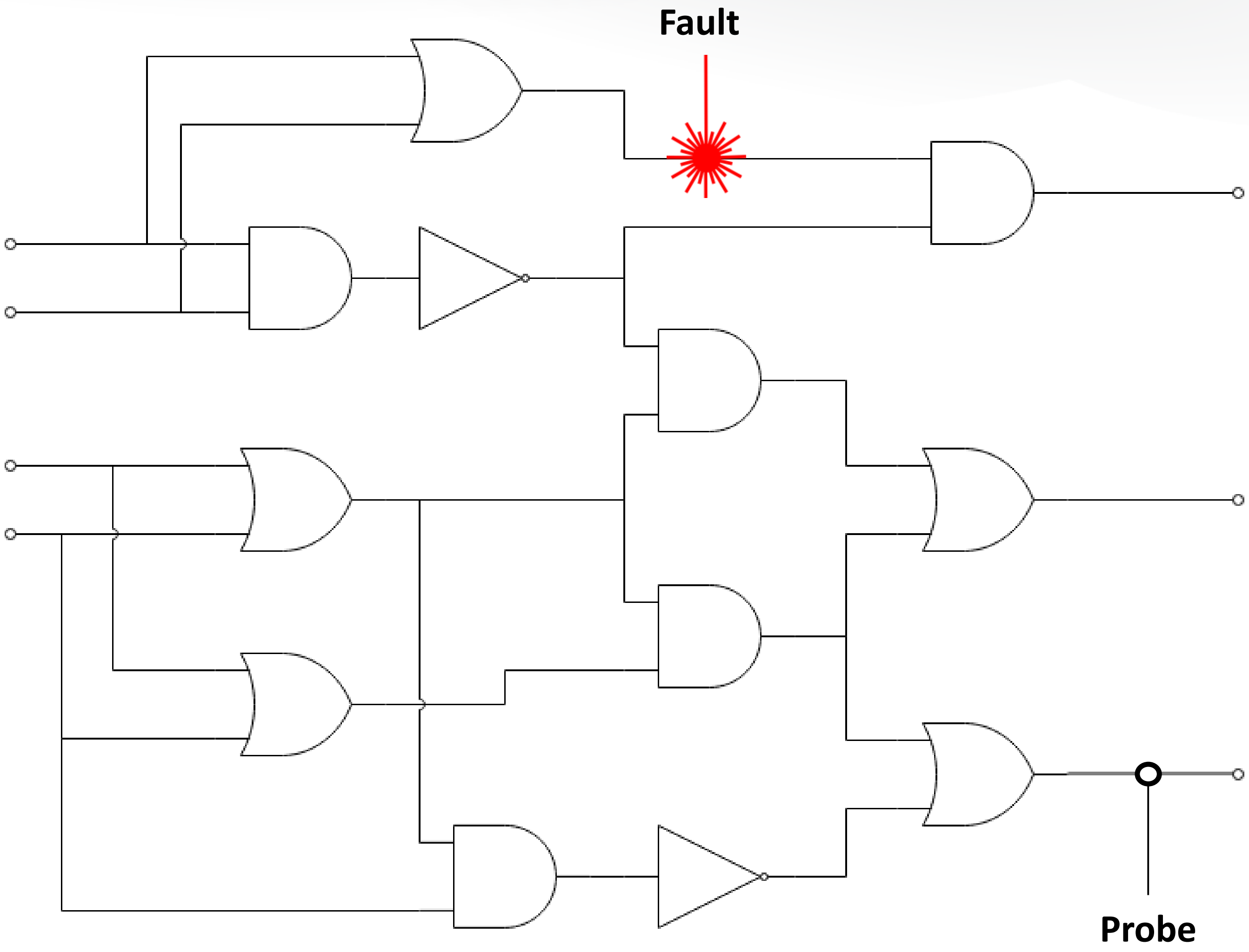
The Fault Model



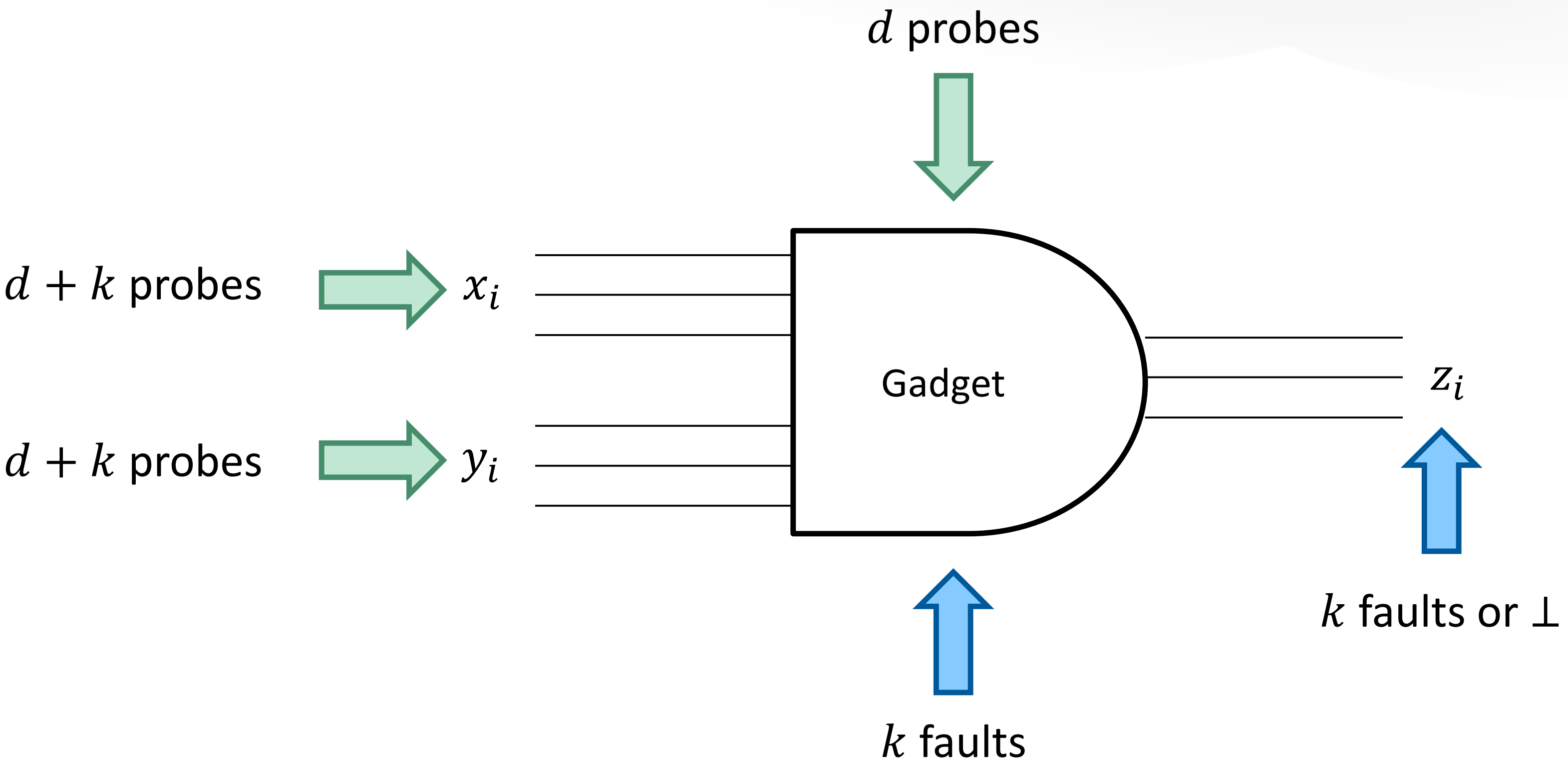
Non-Accumulation



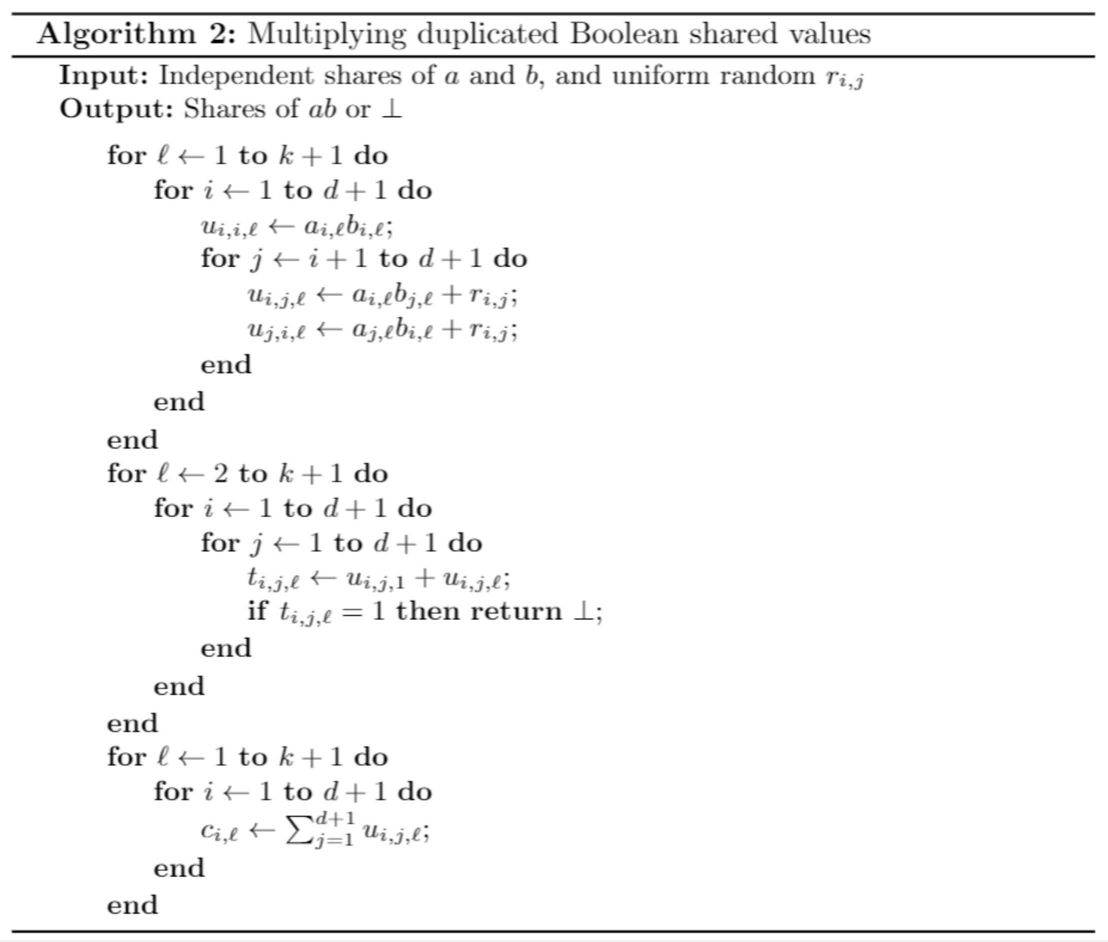
The Combined Model



NINA


d probes
$d + k$ probes
x_i
$d + k$ probes
y_i
Gadget
z_i
k faults or $\perp$
k faults

A NINA Gadget



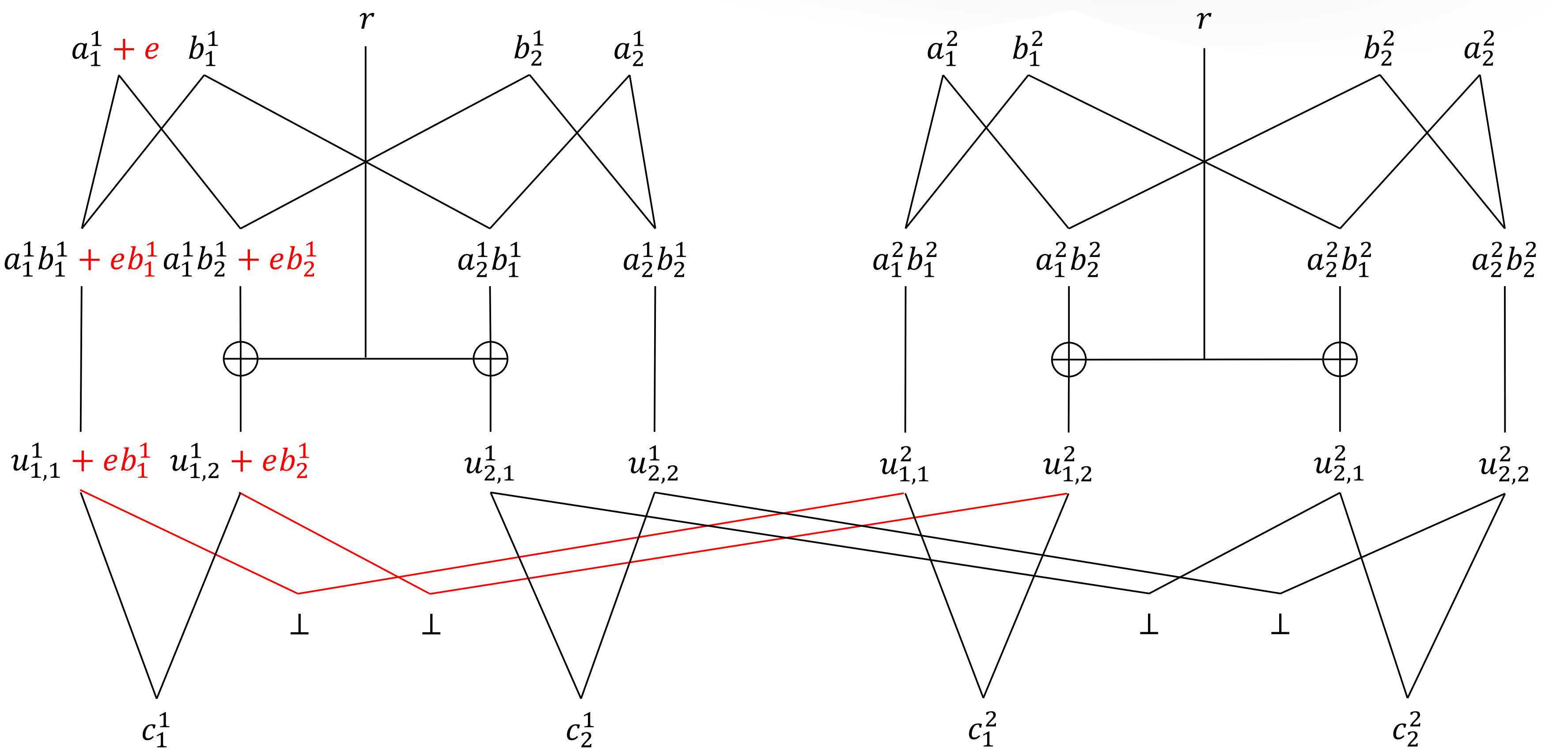
Algorithm 2: Multiplying duplicated Boolean shared values

Input: Independent shares of a and b, and uniform random $r_{i,j}$

Output: Shares of ab or $\perp$

```
for $\ell \leftarrow 1$ to $k+1$ do
    for $i \leftarrow 1$ to $d+1$ do
        $u_{i,i,\ell} \leftarrow a_{i,\ell} b_{i,\ell}$;
        for $j \leftarrow i+1$ to $d+1$ do
            $u_{i,j,\ell} \leftarrow a_{i,\ell} b_{j,\ell} + r_{i,j}$;
            $u_{j,i,\ell} \leftarrow a_{j,\ell} b_{i,\ell} + r_{i,j}$;
        end
    end
end
for $\ell \leftarrow 2$ to $k+1$ do
    for $i \leftarrow 1$ to $d+1$ do
        for $j \leftarrow 1$ to $d+1$ do
            $t_{i,j,\ell} \leftarrow u_{i,j,1} + u_{i,j,\ell}$;
            if $t_{i,j,\ell} = 1$ then return $\perp$;
        end
    end
end
for $\ell \leftarrow 1$ to $k+1$ do
    for $i \leftarrow 1$ to $d+1$ do
        $c_{i,\ell} \leftarrow \sum_{j=1}^{d+1} u_{i,j,\ell}$;
    end
end
```

A NINA Gadget



Applying the NINA Framework

- Create an algorithmic expression of your cipher
- Divide the algorithm in smaller subcomponents
- To each component apply the NINA framework
- Combine all secure components

Secure implementation of the cipher!

Thanks!

Questions?