COSIC
CRYPTOGRAPHY & CYBER SECURITY

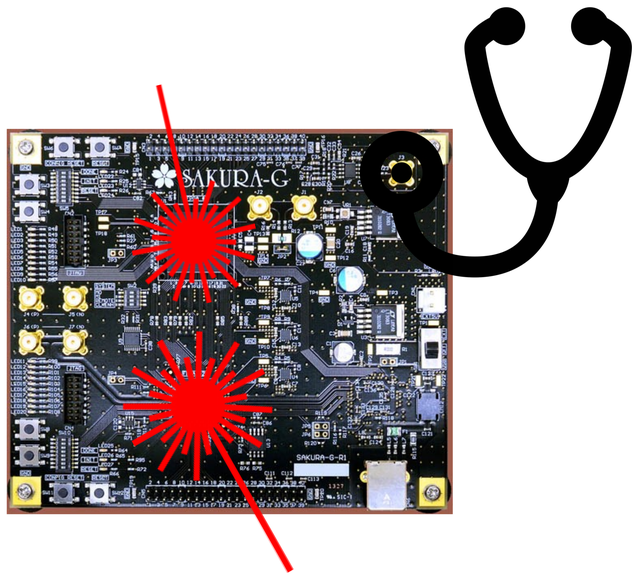
NINA: Proving Combined Security for Polynomial Masking

Siemen Dhooghe and Svetla Nikova

1: Combined Attacks

Observe device's behaviour while it is being tampered with

- Stronger than fault injections or power analysis alone



2: Combined Security

We consider an adversary who can

- Observe several wires (probes)
- Fault several wires

A circuit is secure if

- Its output is correct (or abort)
- The adversary does not learn sensitive variables

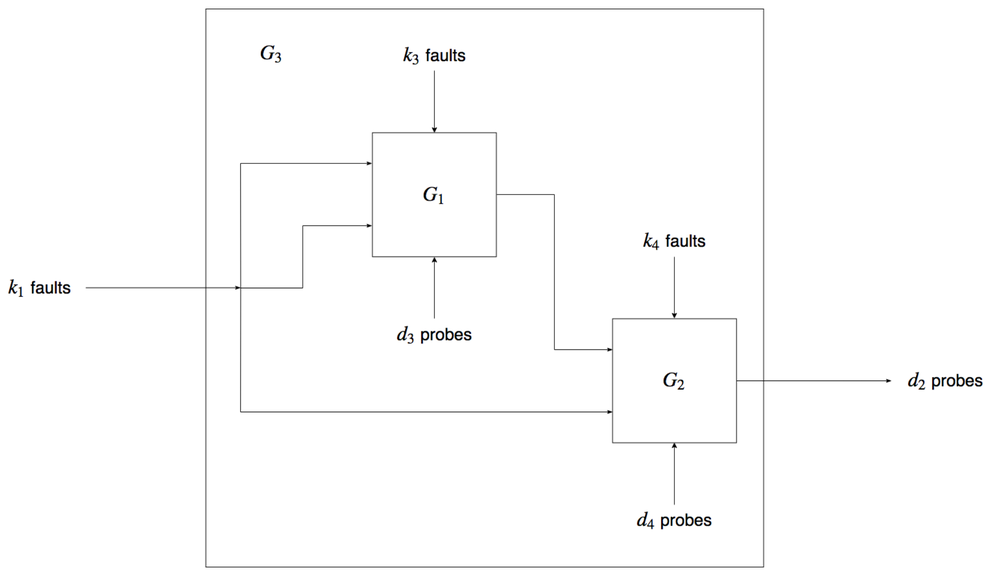
3: Compose a Circuit in Gadgets

Securing big circuits is difficult

- Instead secure smaller components

Need for composable security definitions

- Strong Non-Interference for passive security



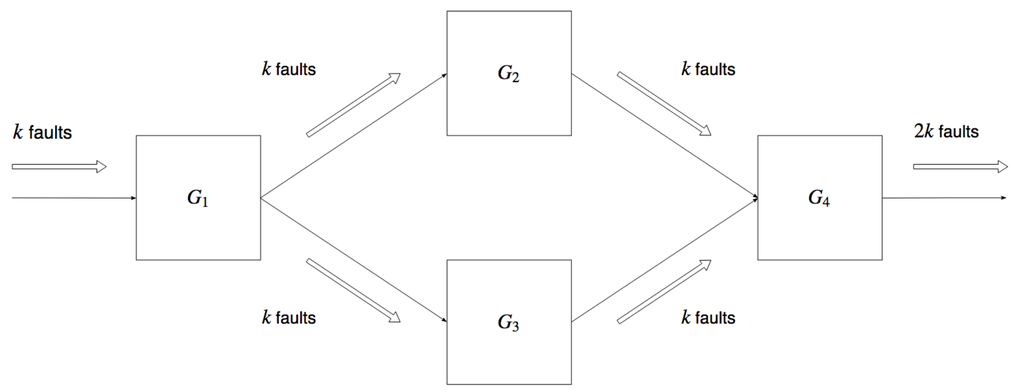
4: Composable Combined Security

NINA: Given a gadget which is probed and faulted

- Only a few output shares have faults (or abort)
- The adversary learns only a few input shares

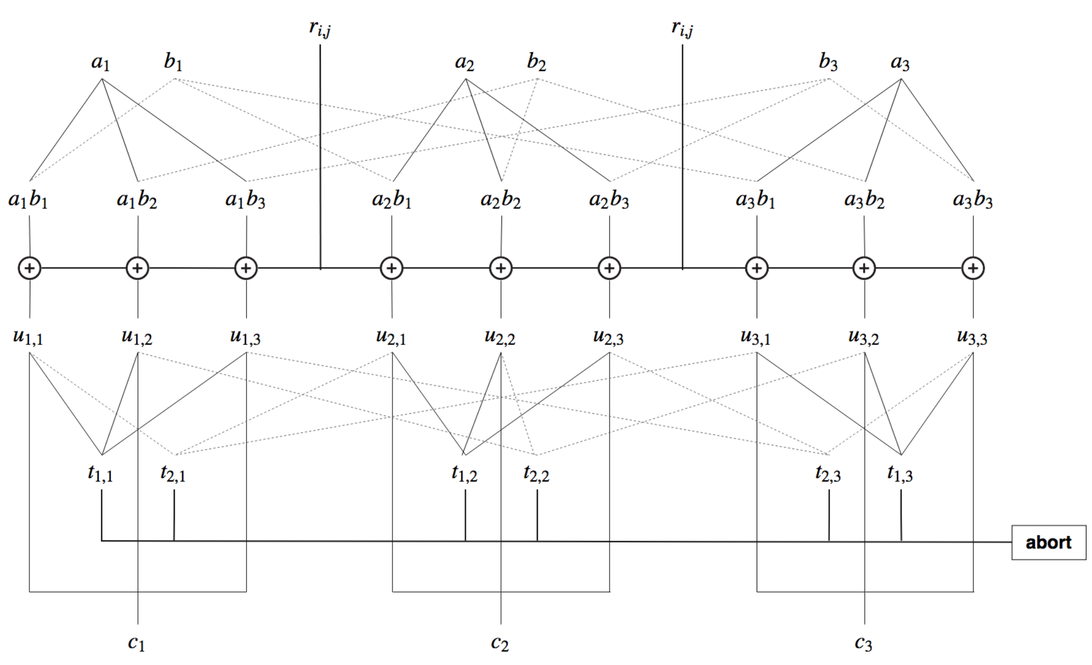
We give a stronger version of NINA (S-NINA)

- The composition of S-NINA gadgets is again S-NINA



5: Polynomial Masking

Shamir secret shares over a low degree polynomial
Add error detection tests against fault injections



PROOFS!
MANY PROOFS!

6: Conclusions

We define a notion of combined security
We propose a composable security definition
We create a combined secure methodology