Body biasing fault injection: Enhancements, analysis, modeling, and simulation

PhD thesis defense

Geoffrey Chancel Jean-Marc Gallière Philippe Maurine

2023/12/05

INTRODUCTION

Context

- Electronics systems are everywhere, from entertainment to business;
- They embed cryptographic algorithms to ensure secure operation;
- These implementations are fallible $\rightarrow$ they leak information.

PLACEHOLDER
PLACEHOLDER
PLACEHOLDER
PLACEHOLDER
PLACEHOLDER

PLACEHOLDER
PLACEHOLDER
PLACEHOLDER
PLACEHOLDER
PLACEHOLDER

Objectives

- Fault injection...;
- Side-channel attacks...;
- Main target $\rightarrow$ Modeling body biasing injection:
  - Characterize better practices for BBI;
  - Define electrical models for BBI simulation;
  - Understand the mechanisms at work;
  - Bring insights on substrate thinning and BBI.

State-of-the-art

Main flaws of algorithms implemented on actual circuits

LOCAL TITLE

content...
content...
content...

LOCAL TITLE

content...
content...
content...

Body biasing injection: state-of-the-art

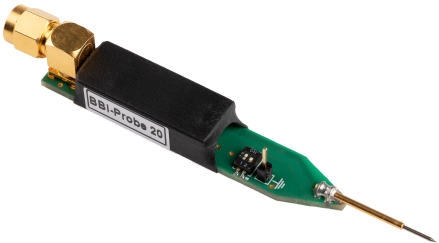
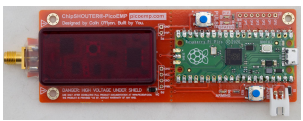
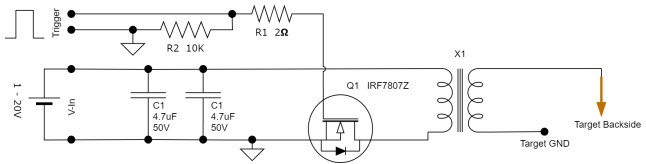
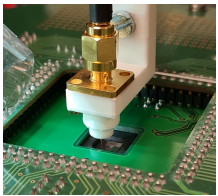
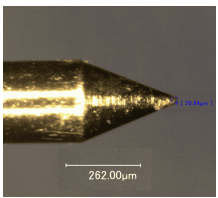


Figure caption.



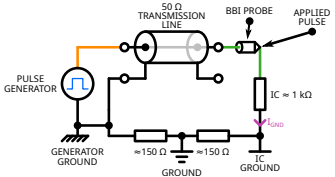





262.00µm

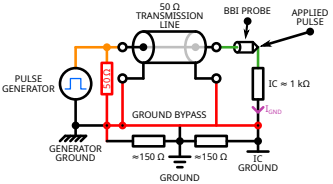
BBI IN PRACTICE

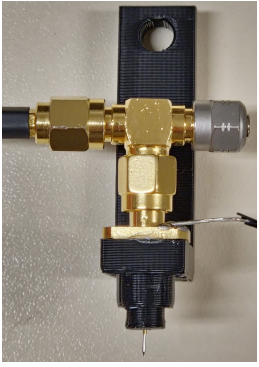
Typical platform



- aa

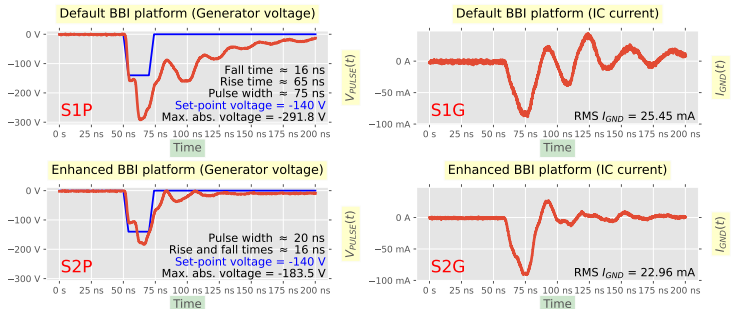
Enhanced platform





BBI in practice

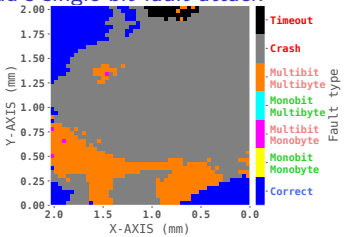
Actual results

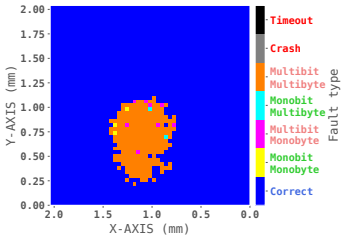


je

Actual benefits of the improvements

Giraud's single bit fault attack





Giraud's single bit fault attack

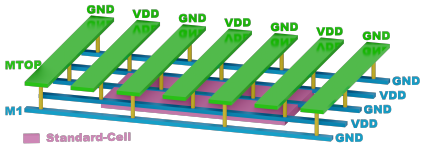
Results

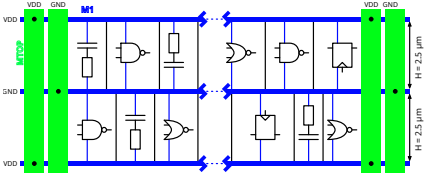
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K10	0xFF	0x1F	0x42	0xE8	0xEF	0x44	0xA5	0x6A	0xCA	0xE7	0x55	0x3C	0xFD	0x65	0x39	0x26
KEY	0x01	0x23	0x45	0x67	0x89	0xAB	0xCD	0xEF	0xDE	0xAD	0xBE	0xEF	0x12	0x34	0x43	0x21

Text content.

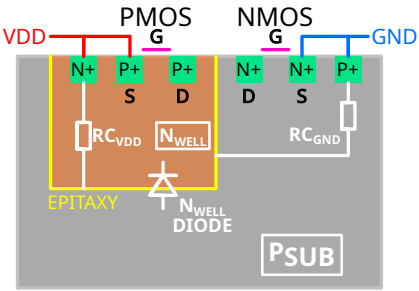
BBI IC MODELING

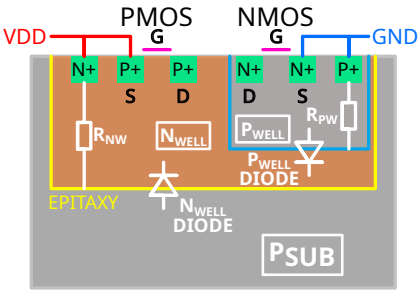
IC basic structure



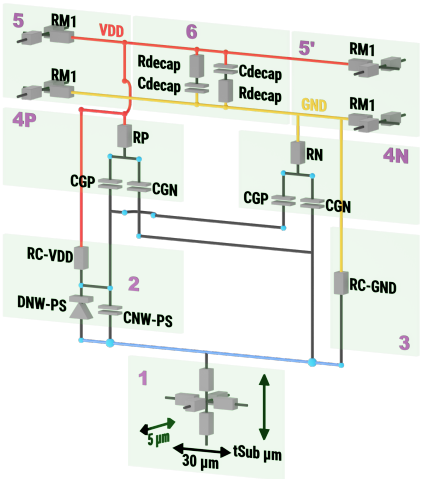


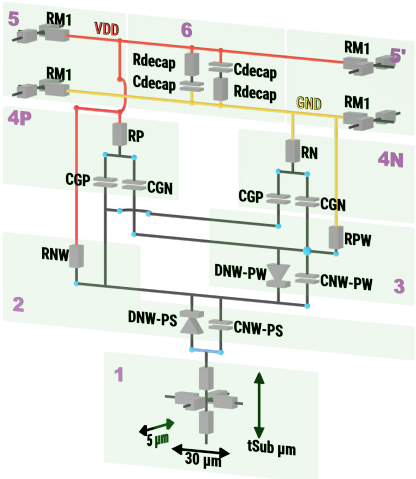
Bulk substrate types



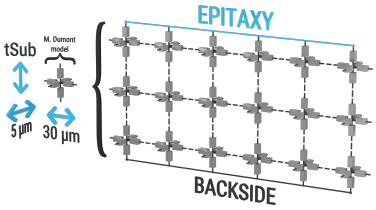


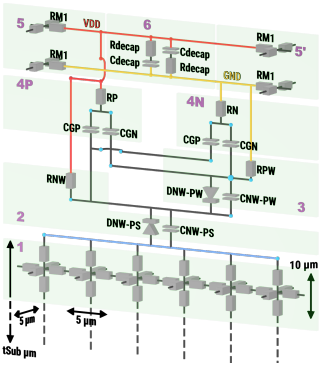
Standard-cell original models

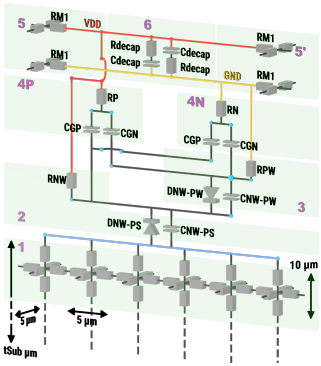




Standard-cell model substrate improvement

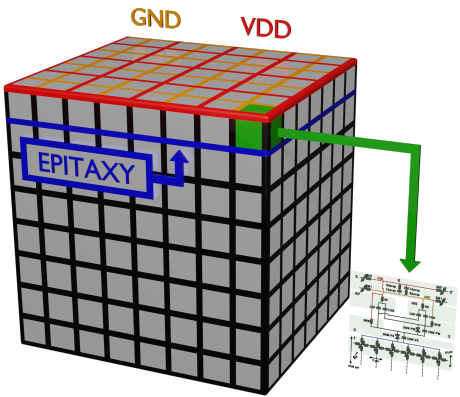






TITLE

SUBTITLE



TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE

TITLE

SUBTITLE