Anti-Piracy of Analog and Mixed-Signal Circuits in FD-SOI

Mariam TLILI, Alhassan Sayed, Doaa Mahmoud, Marie-Minerve Louërat, Hassan Aboushady, Haralampos-G. Stratigopoulos

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257
cnrs
LIP6

Outlines

- IP piracy attacks
- IC life cycle with locking
- Prior art on locking AMS ICs
- Body biasing in FDSOI
- Proposed locking for FDSOI designs
- Case study and results
- Conclusion and perspectives

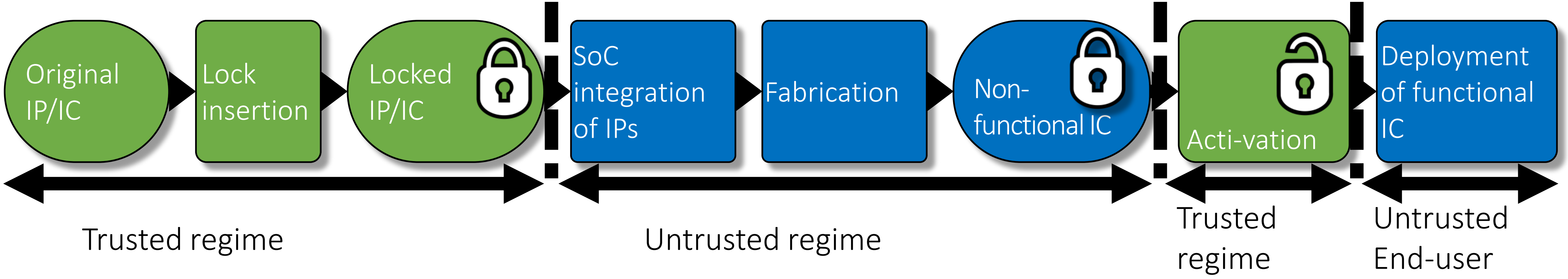
IP piracy of AMS ICs

- Advantages when going fabless: reduced capital and time-to-market
- Global revenue loss of about $100 billion every year because of counterfeiting
- Around 1% of semiconductor sales are estimated to be those of counterfeit ICs
- About 25% of reported incidents concern analog ICs

	IP design	SoC design	Fabrication	Testing	End user	End of life
Reverse engineering		x	x	x	x	
Counterfeiting		x clone	x clone, overproduce	x remark	x clone	x recycle

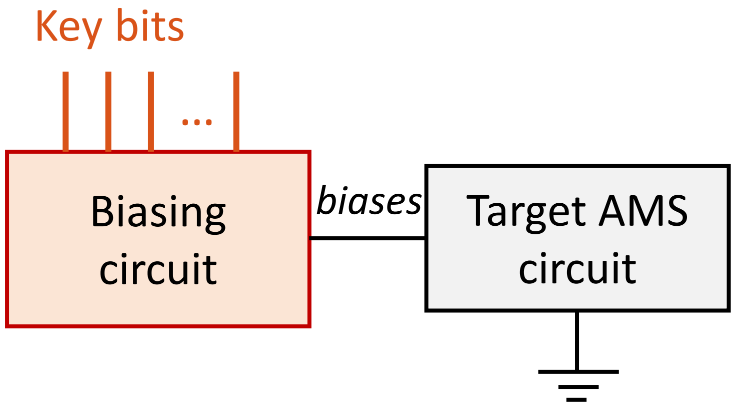
Guin et al., Proc. IEEE'14

IC Life Cycle with Locking



- Locking transforms original circuit to a circuit with a lock, requiring secret key to restore nominal functionality; key typically a bit-string
- IP/IC owner inserts lock and keeps correct key secret
- Circuit remains locked throughout manufacturing
- Activation by trusted party
- Locking as end-to-end protection
- Logic locking for digital ICs

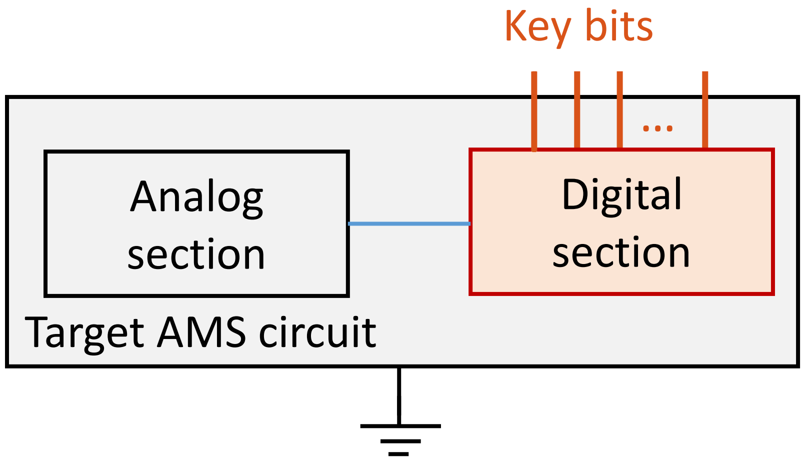
Prior art on locking AMS ICs



Biasing locking

Hoe *et al.*, ASVLSI’14, Rao *et al.*, LATS’17 & ISCAS’19, Wang *et al.*, ITC’17, Volanis *et al.*, VTS’19

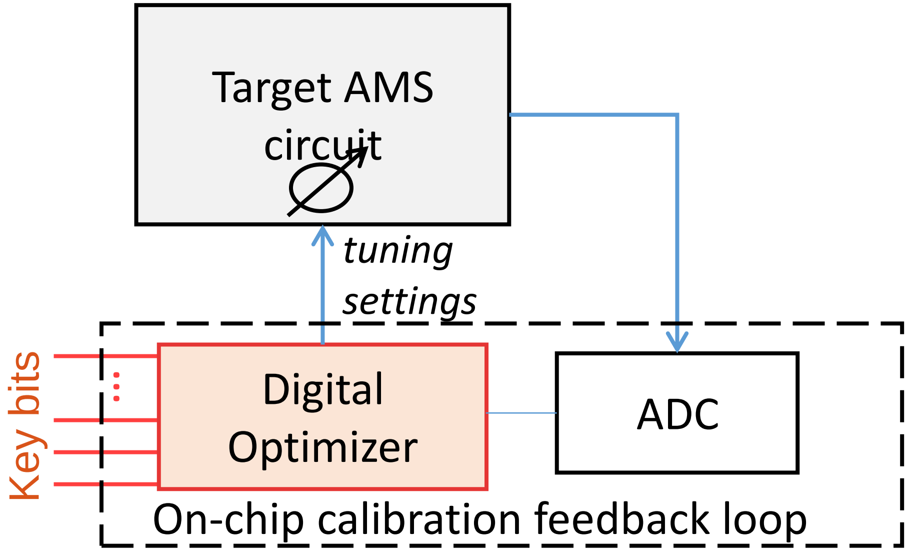
- There exist effective counter-attacks that remove the lock and/or extract the secret key (Jayasankaran, *TVLSI*’20, Acharya, *HOST*’20, Leonhard *ASP-DAC*’21)



Mixed-signal locking

Leonhard, DATE’19

- Justifiable but non-negligible overhead



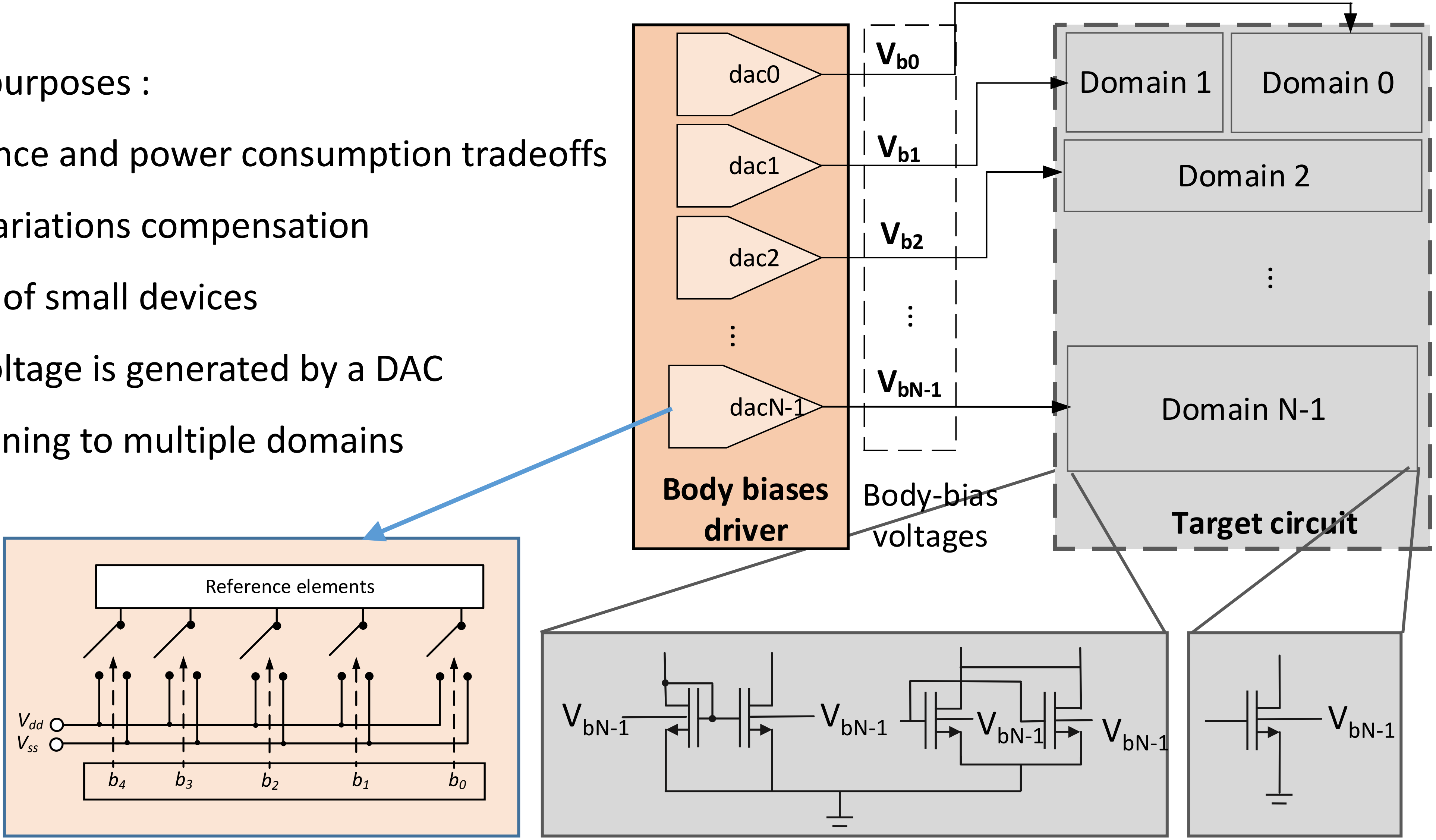
Calibration locking

Jayasankaran et al., ICCAD’18 Elshamy et al., DATE’20, Nimmalapudi et al., DATE’20

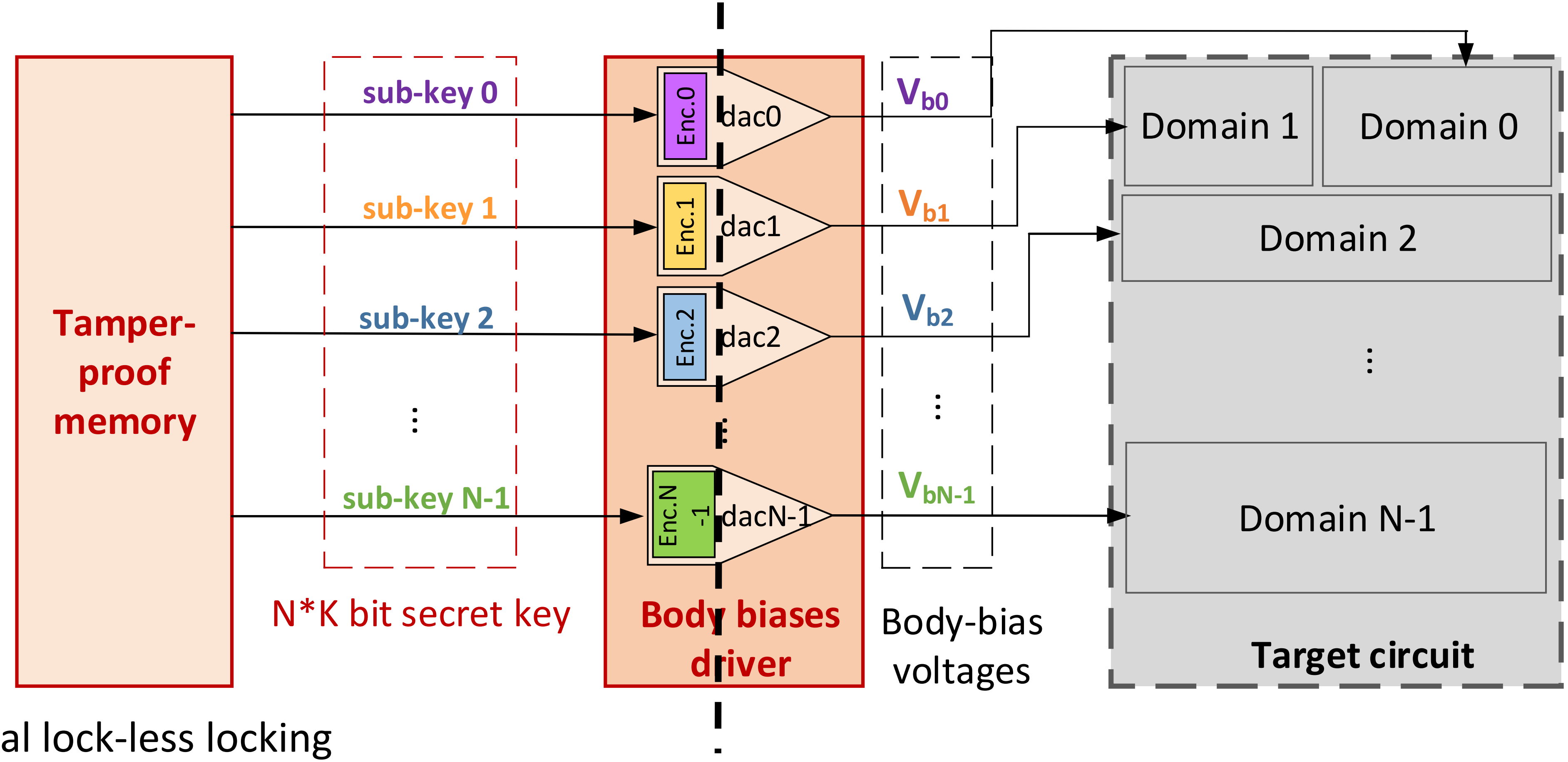
- Calibration locking requires a complex enough calibration algorithm to be devised or re-designed in hardware by the attacker, an assumption that is not always met

Body biasing in FDSOI

- Body biasing purposes :
  - Performance and power consumption tradeoffs
  - Process variations compensation
  - Matching of small devices
- A body bias voltage is generated by a DAC
- Circuit partionning to multiple domains



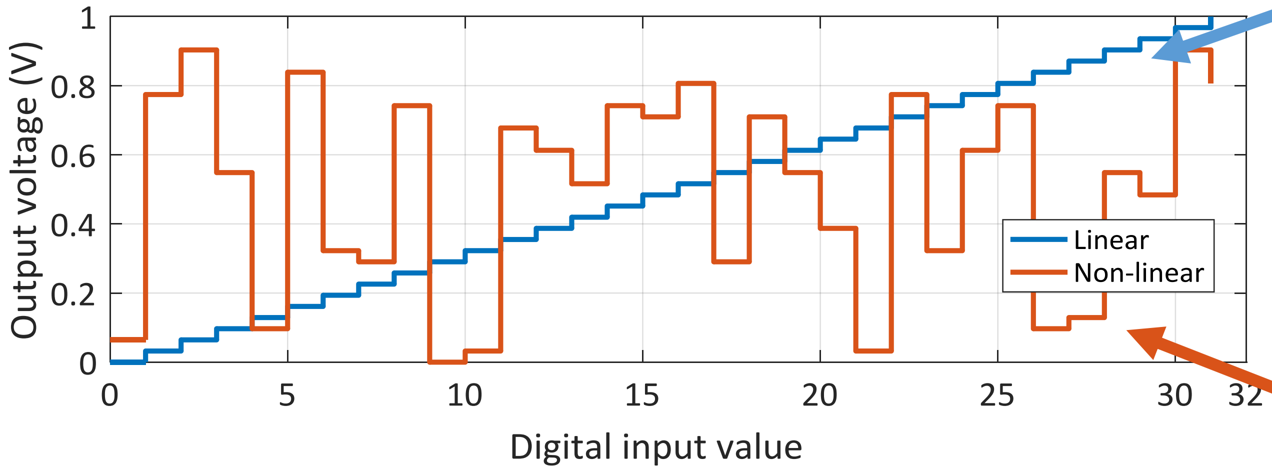
Proposed locking for FDSOI designs



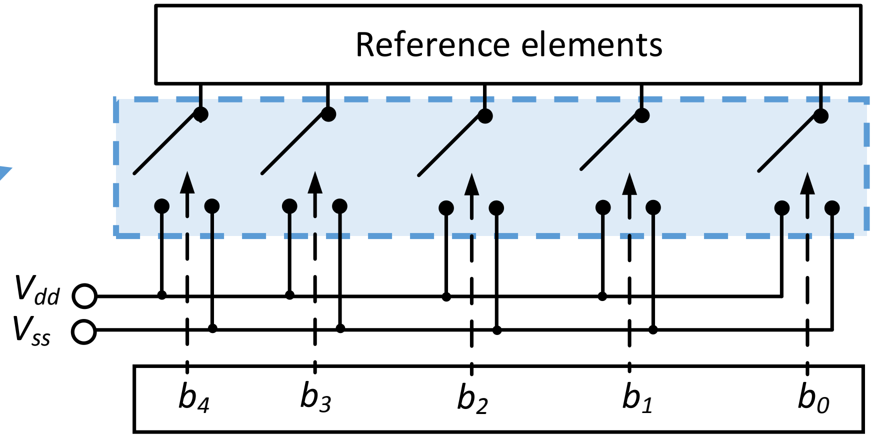
- A natural lock-less locking
- Body bias voltages are obfuscated
- A DAC maps a digital sub-key to a domain
- A global secret key is created by concatenation of all sub-key

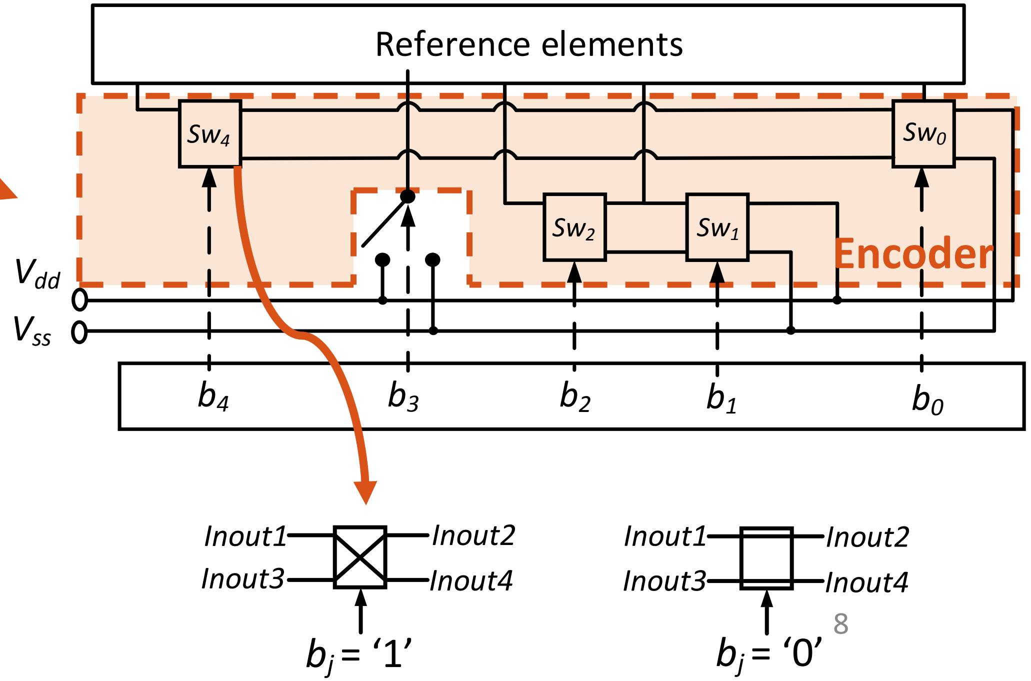
Non-linear DAC transformation

- Slows down the optimization
- Protects body-bias domains that are fixed to the reference voltages



Original code	Equivalent code
00000	10100
01101	11011
11111	01000



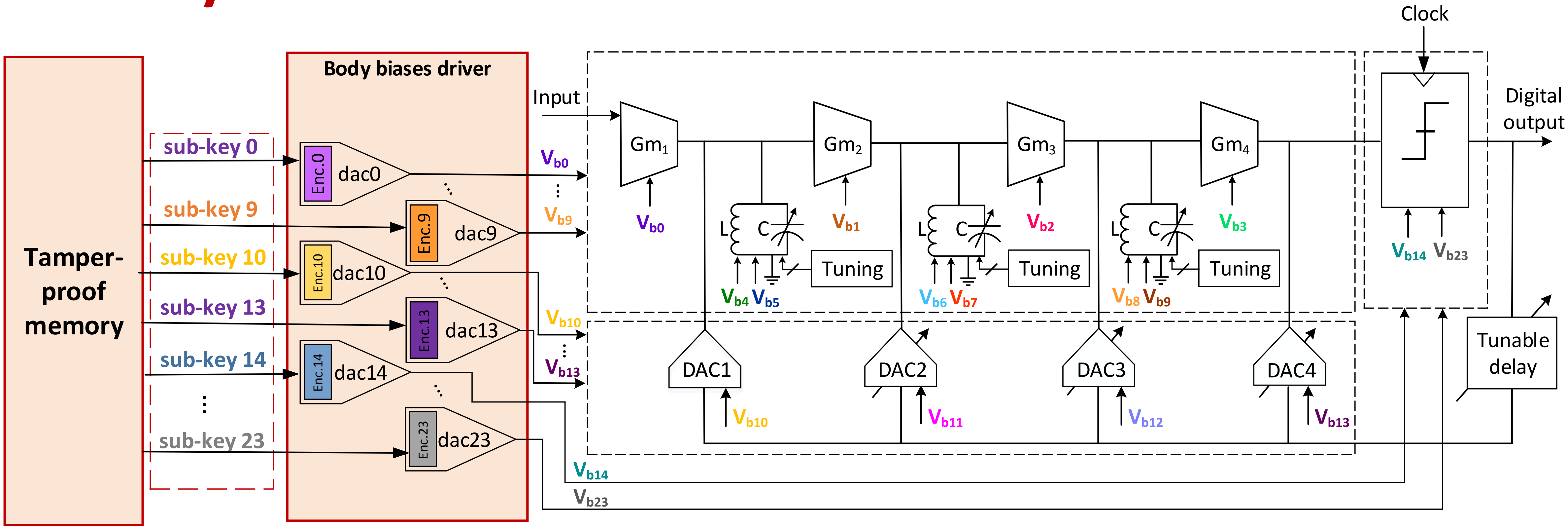


Properties and attacks resilience

- Properties :
  1) Adapted to static body-biasing
  2) Wide applicability to FDSOI designs
  3) Non-intrusiveness to the design
  4) Low-overhead

- Attack scenarios :
  1) <u>Logic locking attacks</u>: not applicable in the analog domain
  2) <u>Brute-Force attacks</u> : impractical for large size keys, analog simulation is slow
  3) <u>Optimization attacks</u> : behave like a randomized brute-force attack

Case study - Circuit



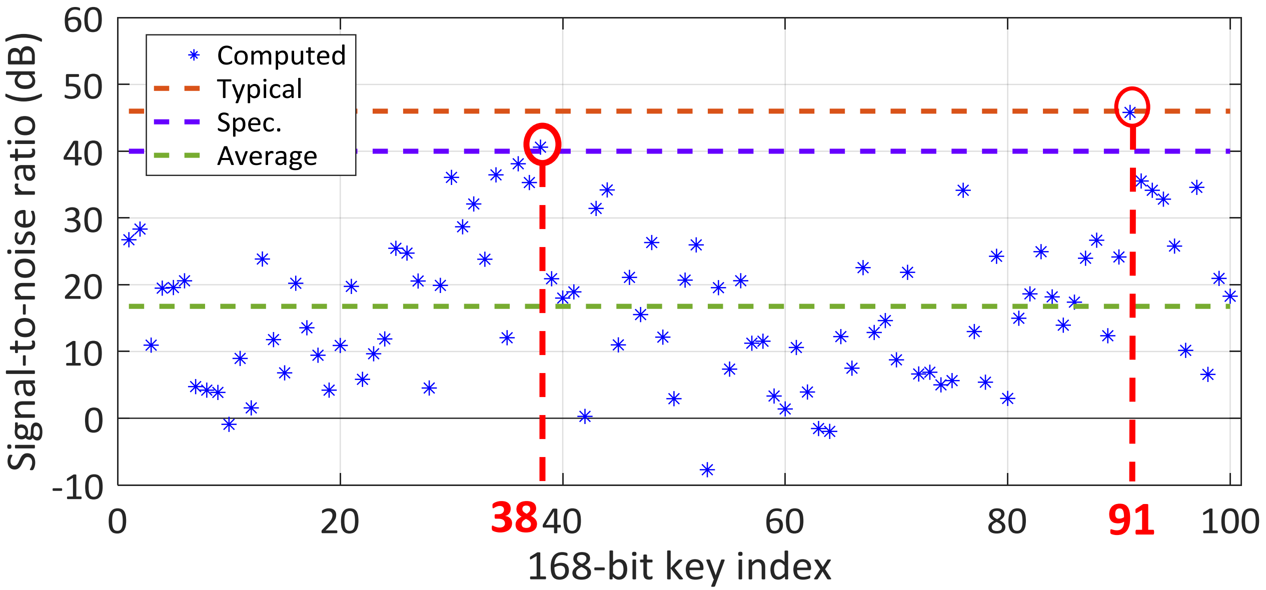
- Target circuit : 6th order sigma-delta modulator
  mono-transistor domains only

- Security mechanism : 24 7-bit DACs
  global secret key size 7*24 = 168 bits
  24 different encoders

Center frequency (1-4 GHz)	Sampling rate (4-16 GHz)
3 GHz	12 GHz

Typical SNR	Spec.
46 dB @ 90 MHz	40 dB

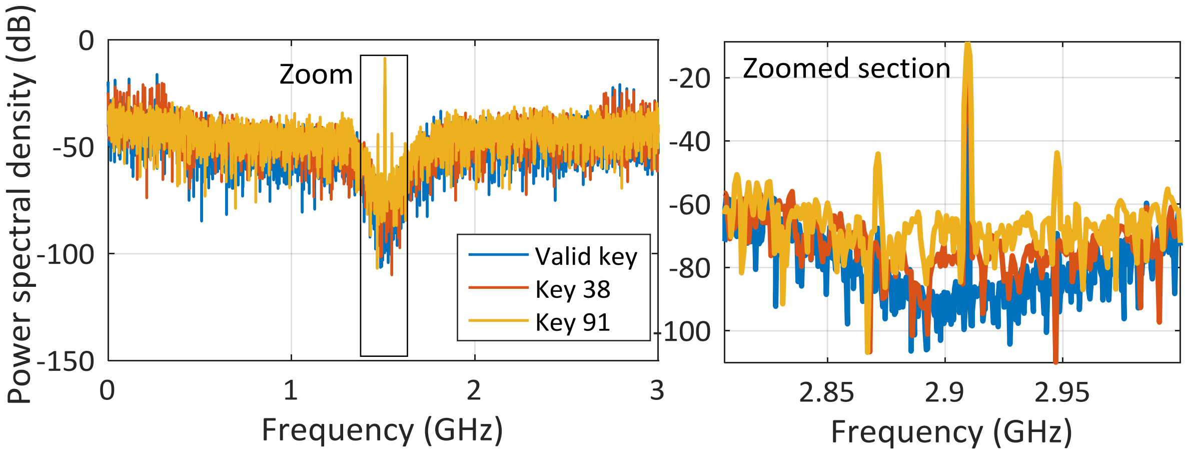
Case study - Results



Average SNR (dB)	Mean absolute error (dB)	Minimum error (dB)
16.74	29.26	2.6

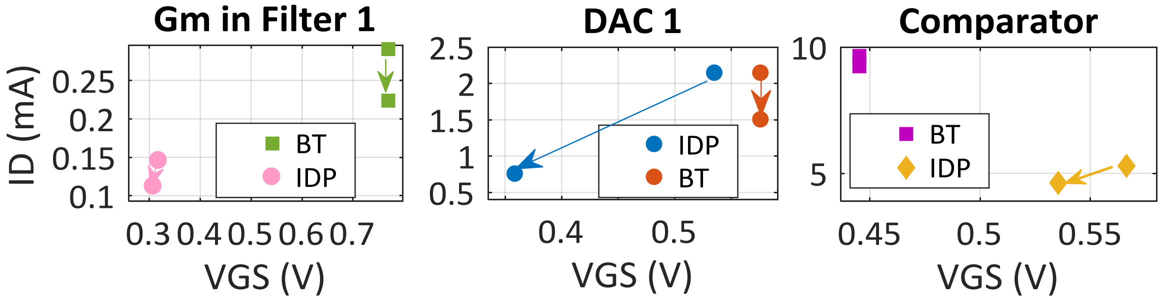
- High SNR degradation for 98 % of simulated keys
- Two keys with acceptable SNR degradation BUT missleading results

Small SNR degradation BUT :

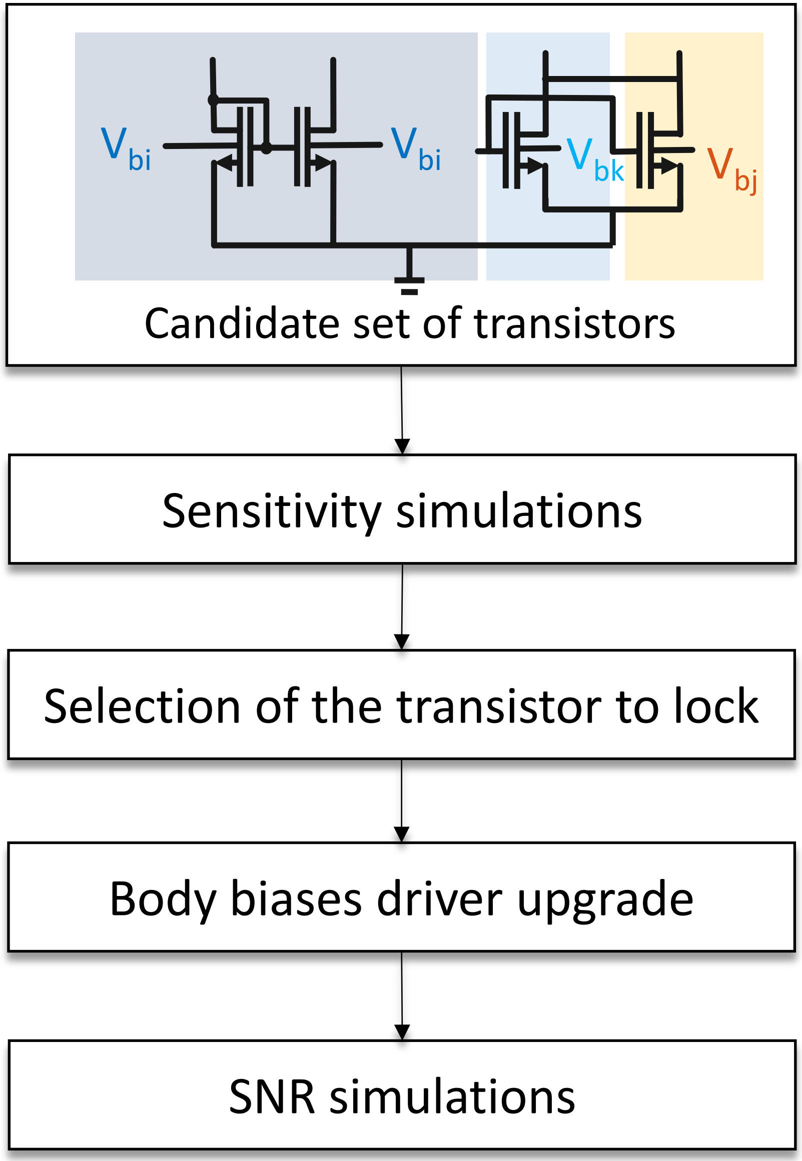


SFDR :

Original	Key 38	Key 39
31.39	24.97	20.02



Case study - Results



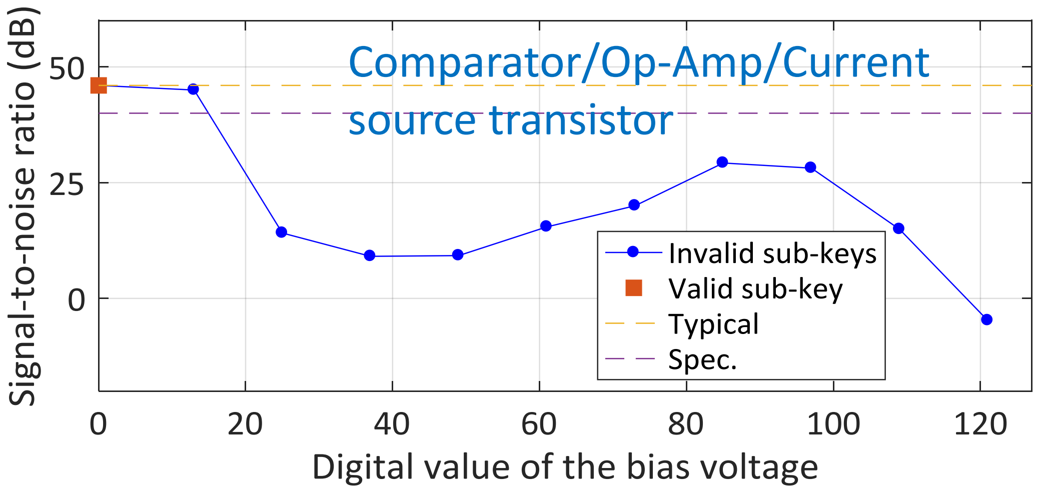
Candidate set of transistors

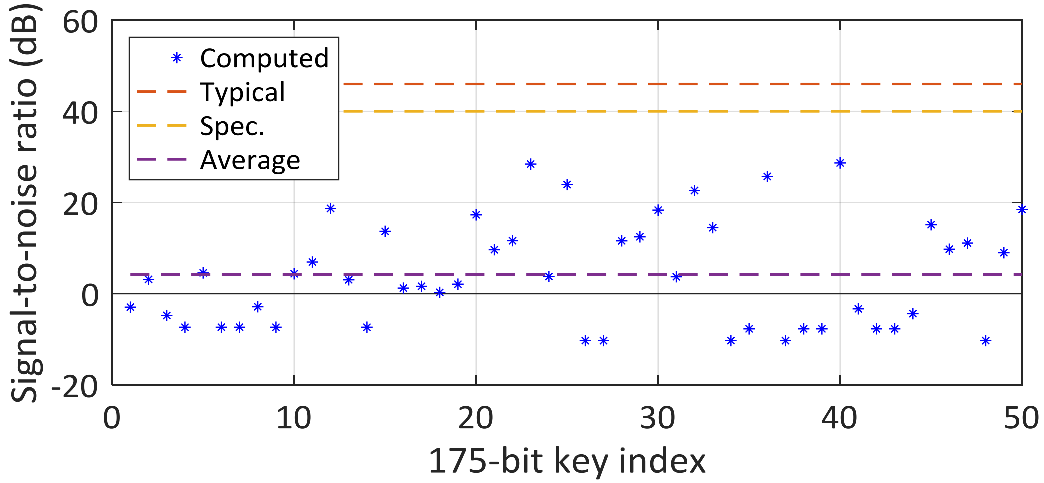
Sensitivity simulations

Selection of the transistor to lock

Body biases driver upgrade

SNR simulations





Average SNR (dB)	Mean absolute error (dB)	Minimum error (dB)
16.74	29.26	2.6
4.2	**41.8**	**17.3**

Conclusion and future work

- Natural lock-less body-bias voltages obfuscation as an anti-piracy defense for AMS ICs in FD-SOI
- An effective way to introduce a large-size digital key
- Invalid keys induce high functionality corruption
- Low-overhead re-design of the switching network of the DACs, non intrusiveness, wide applicability
- Demonstration on a sigma-delta modulator designed in 28 nm FDSOI from STMicroelectronics
- Potential to lock digital ICs in FDSOI
- How about FDSOI designs with dynamic body-biasing ?