EM Attack Is Non-Invasive?
- Design Methodology and Validity Verification of EM Attack Sensor

Naofumi Homma[1], Yu-ichi Hayashi[1], Noriyuki Miura[2], Daisuke Fujimoto[2], Daichi Tanaka[2], Makoto Nagata[2], and Takafumi Aoki[1]

[1] Tohoku University, Japan

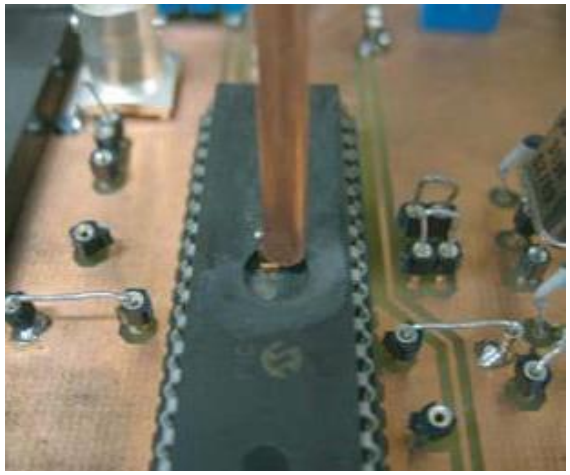
[2] Kobe University, Japan

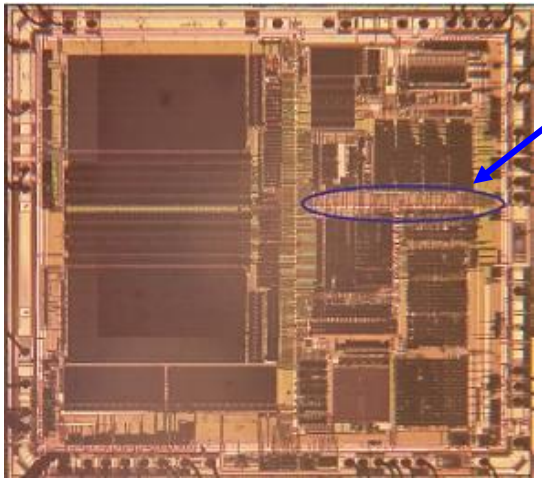
Outline

- Microprobe-based EM attack
- EM attack sensor and its design methodology
- Validity verification
- Concluding remarks

EM attack using microprobe

- Observe precise information leakage from a specific part of LSI by micro scale probing
  - performed on the surface of LSIs beyond conventional security assumptions (e.g., power/EM models)



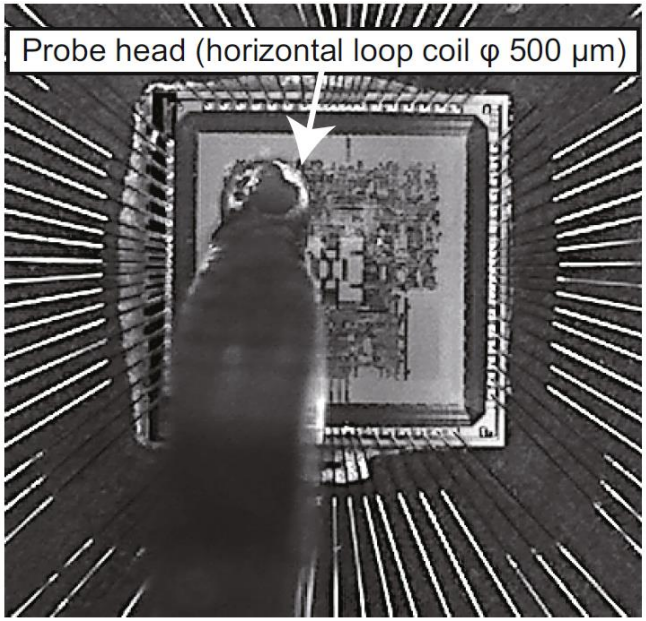


[8] E. Peeters, VLSI J 2007

Many microprobe-based EM attacks have been reported until now

Measurable leaks inside ASIC by microprobe

- Current-path leaks
  - In standard cell
  - Defeat gate-level countermeasures
- Internal-gate leaks (of XOR)
  - In standard cell
  - Defeat XOR-based countermeasures
- Geometric leaks
  - In memory macro
  - Defeat ROM-based countermeasures



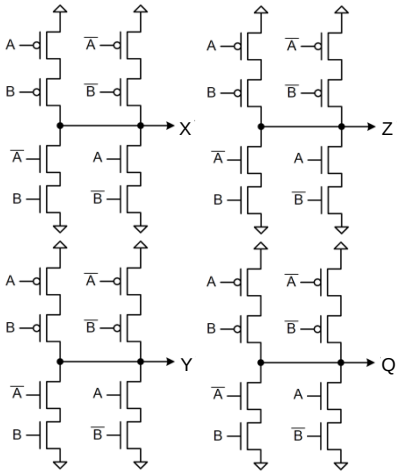
[10] T. Sugawara, CHES'13

Most of conventional countermeasures can be defeated if the above leaks are measured by attackers

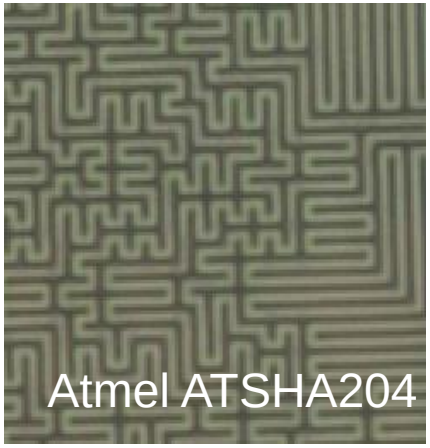
- Such threat would be more and more serious according to the advancement of measurement devices and techniques

Possible existing countermeasures

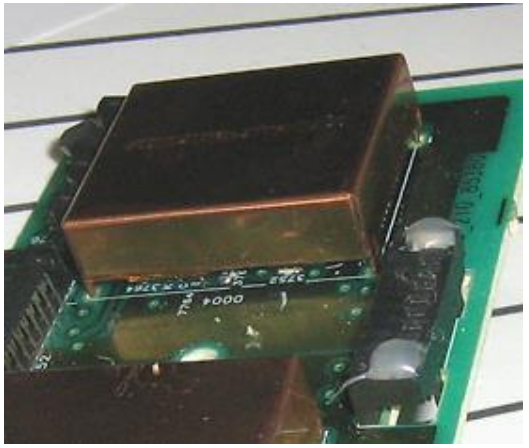
- Performance overhead and manufacturing cost of possible existing countermeasures are non-trivial



Transistor-level balancing (or hiding)



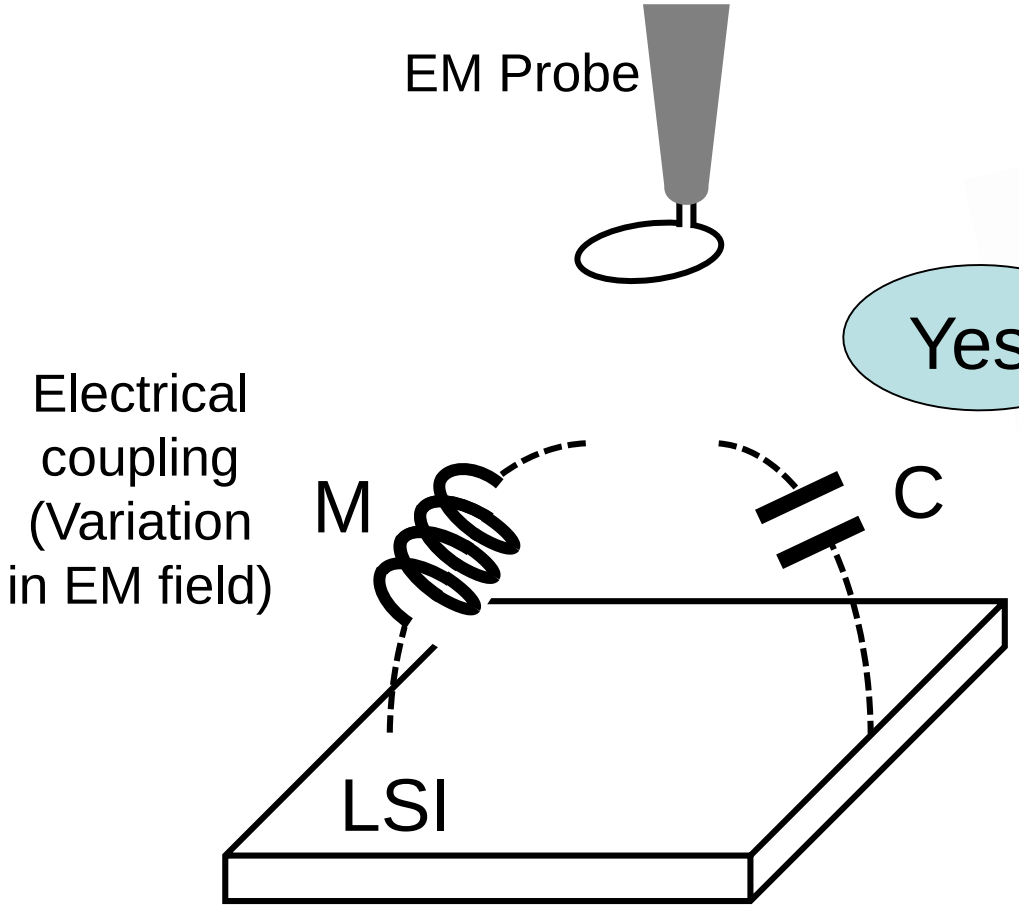
Active shielding on or around LSI

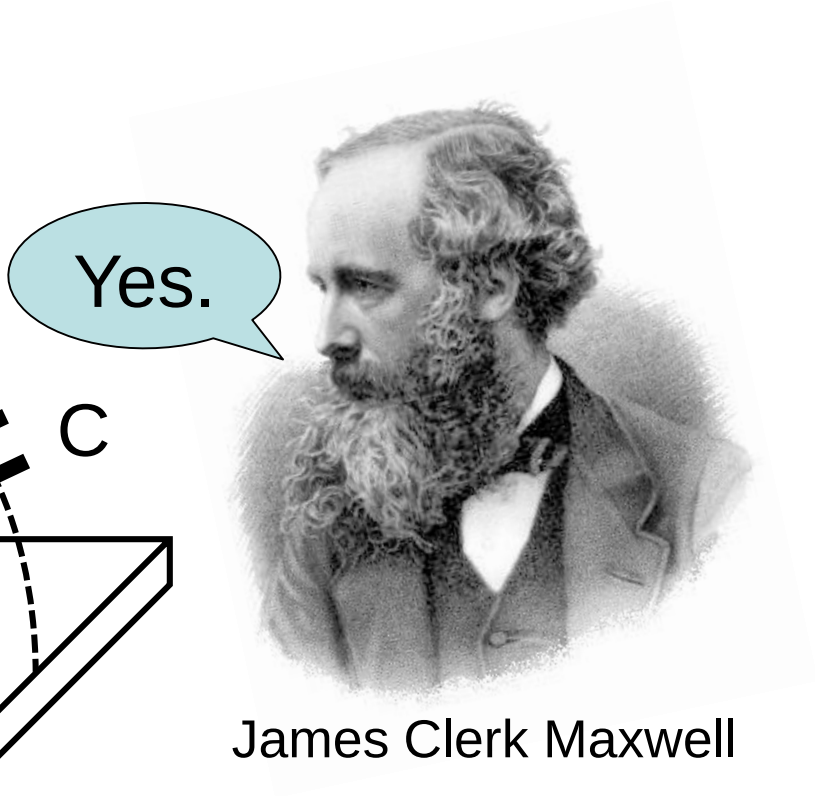


Special packaging

This work: slightly-analog yet reactive countermeasure that can sense microprobe-based EM attacks

Our idea





James Clerk Maxwell

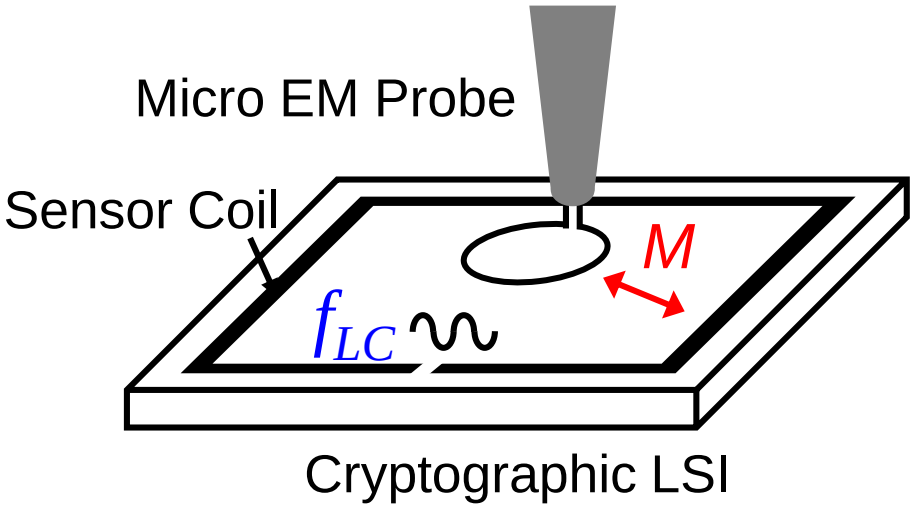
Physical law unavoidable in EM measurement

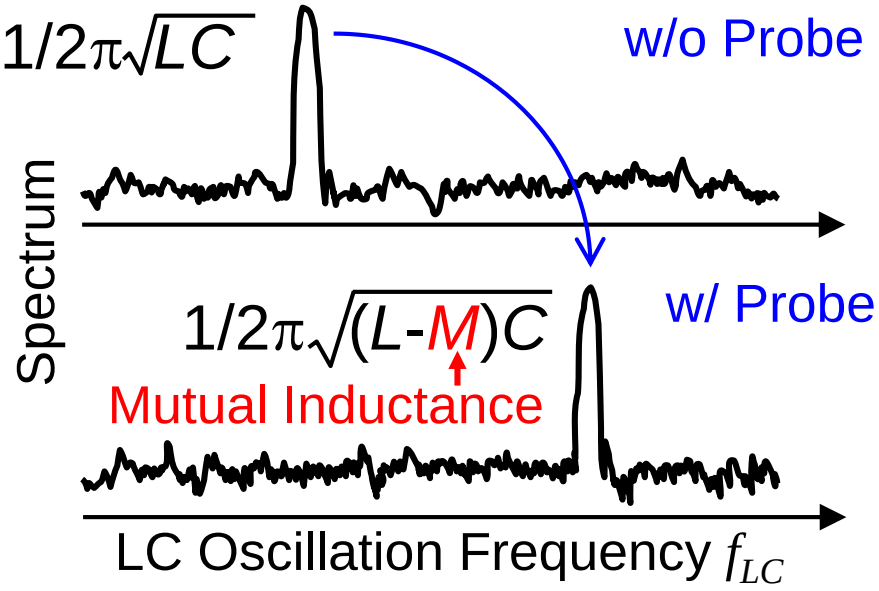
Sense EM attacks by observing EM field variation

Idea of sensor implementation

- Sense electrical coupling (EM field variation)
  - Robust to various attack scenarios
  - Low implementation and performance overhead

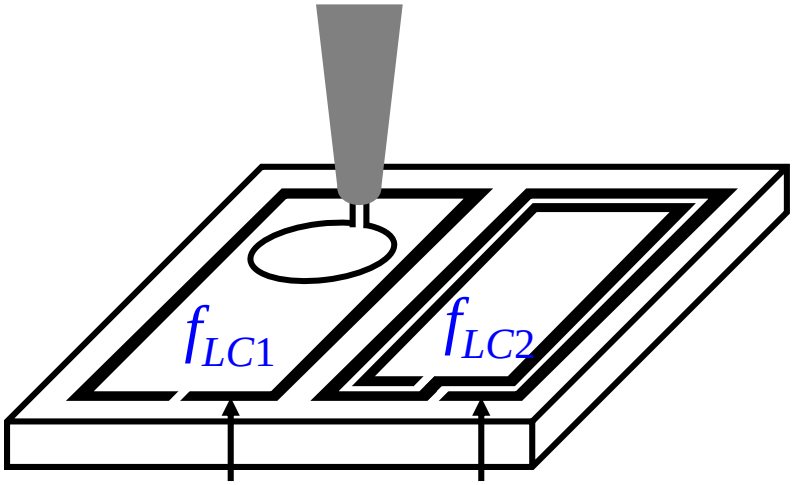
Our implementation idea



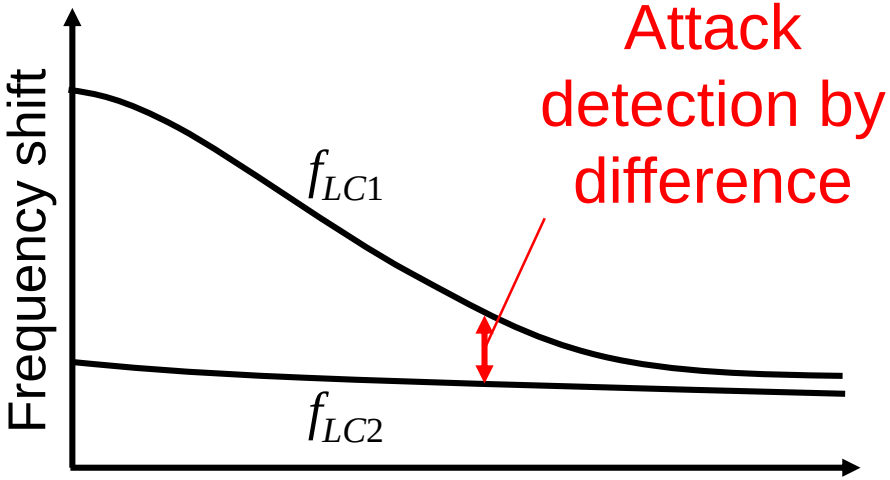


Detect the presence of a probe by
LC oscillation frequency shift

Dual-coil sensor architecture



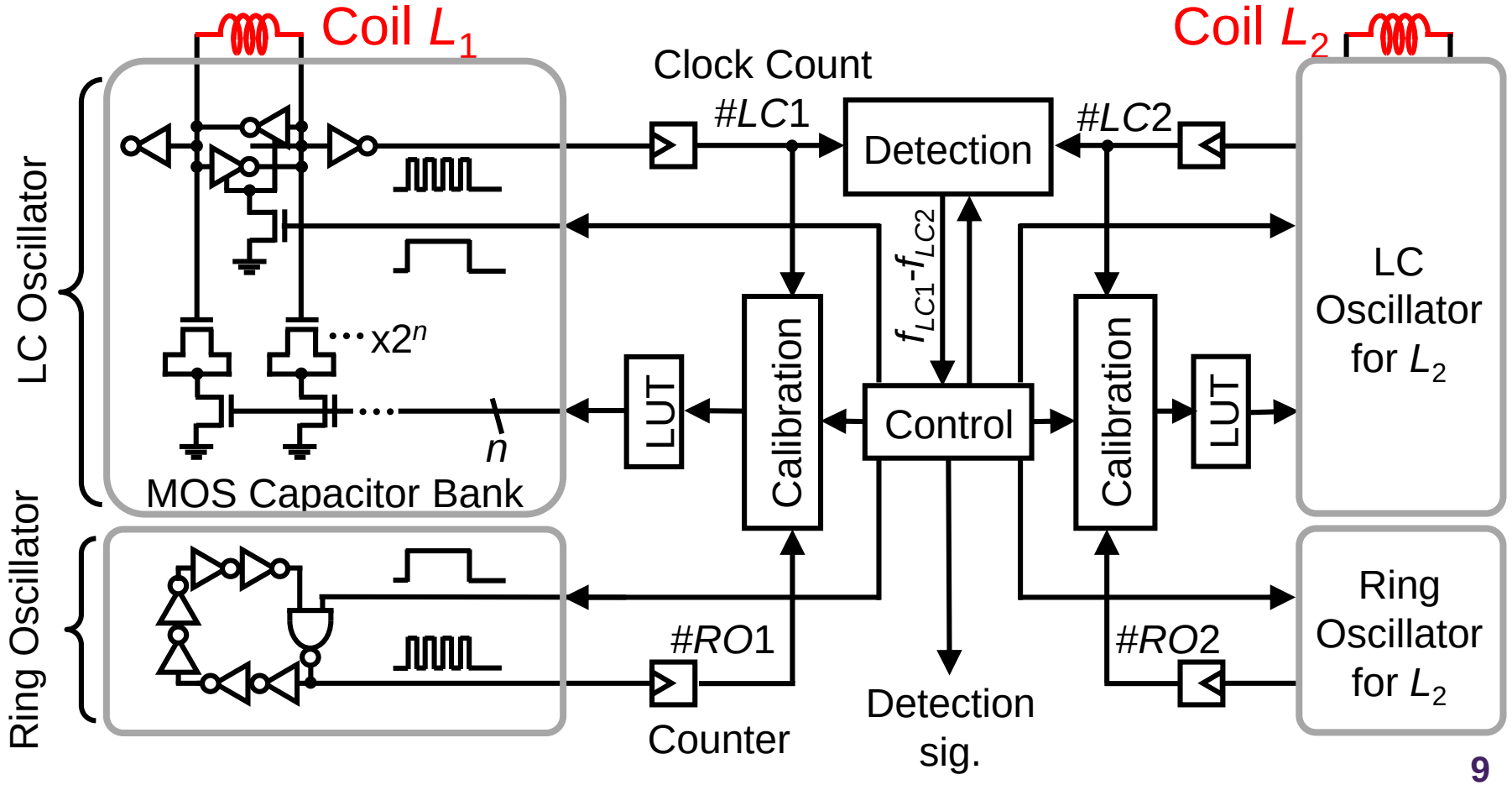
Dual sensor coils



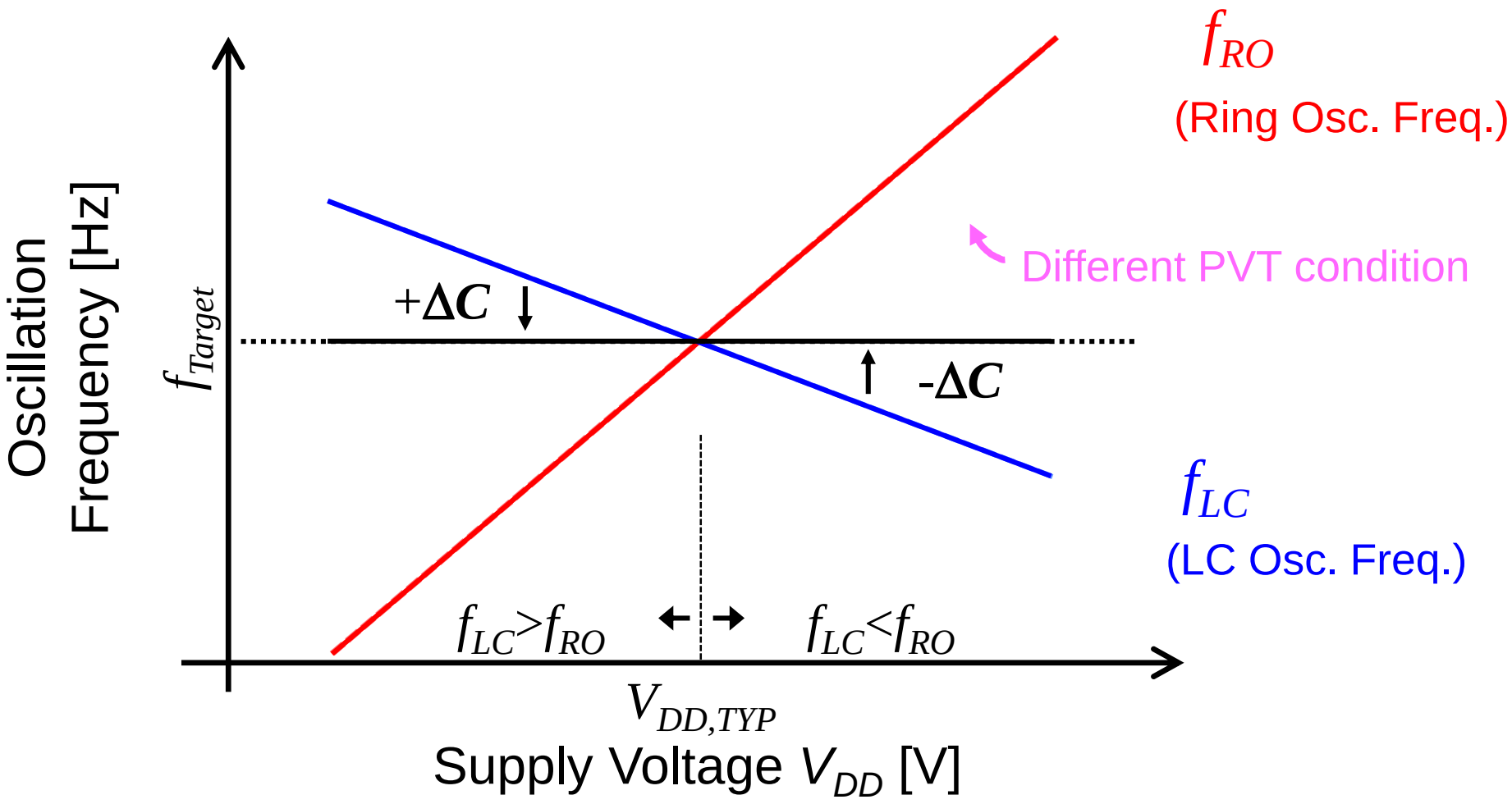
- No frequency reference needed
- Detect various probing scenarios by different coil shapes
- Calibrate PVT (Process, Voltage, and Temperature) variation in f_{LC} digitally

Sensor core

- Connected to two sensor coils
- Consist of LC and ring oscillators, detection logic, calibration logic, and control logic



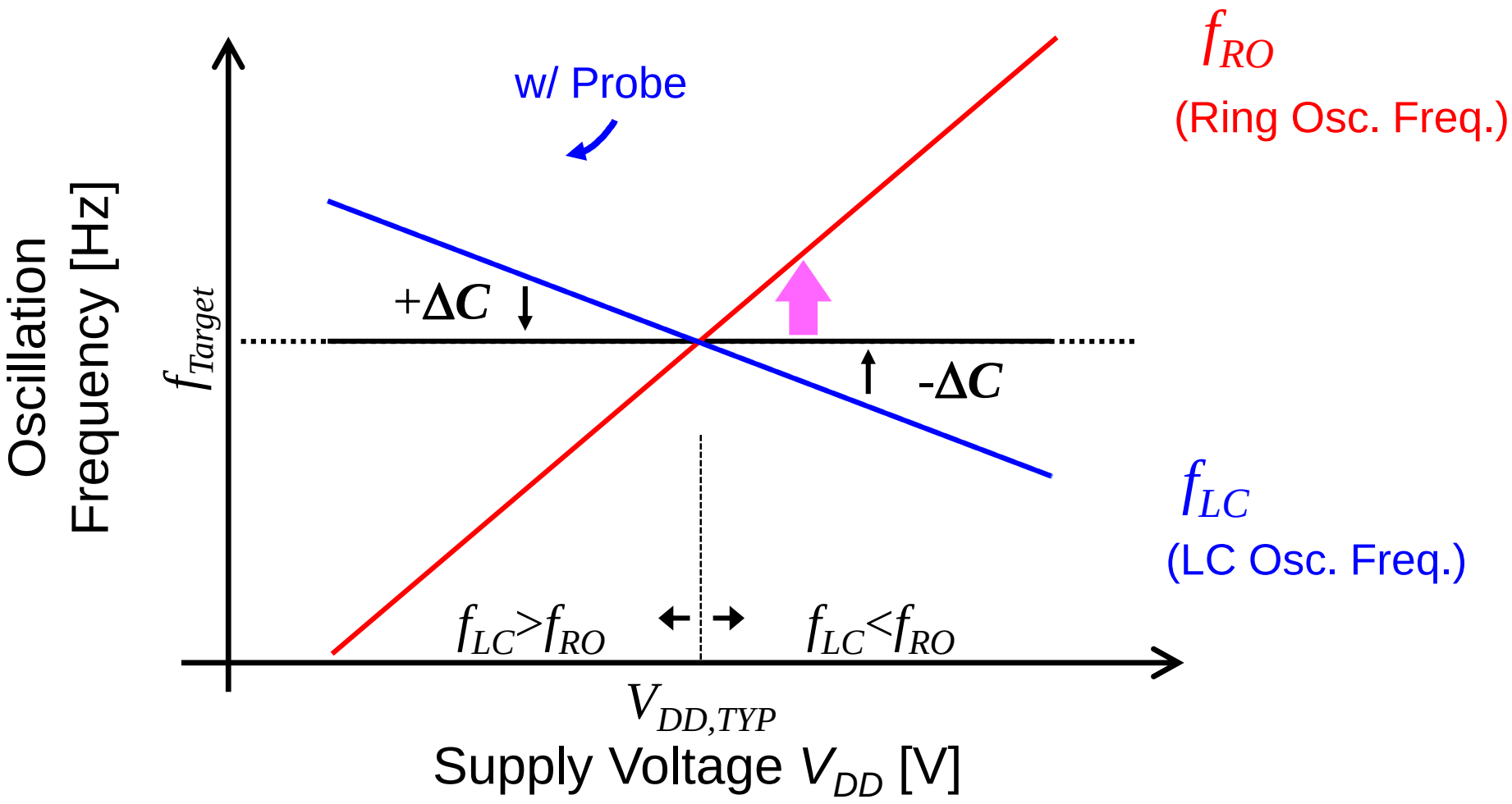
Calibration scheme



f_{Target} : Target frequency after calibration

ΔC : Capacitance change for calibration (Decided by $|f_{RO}-f_{LC}|$)

Calibration scheme

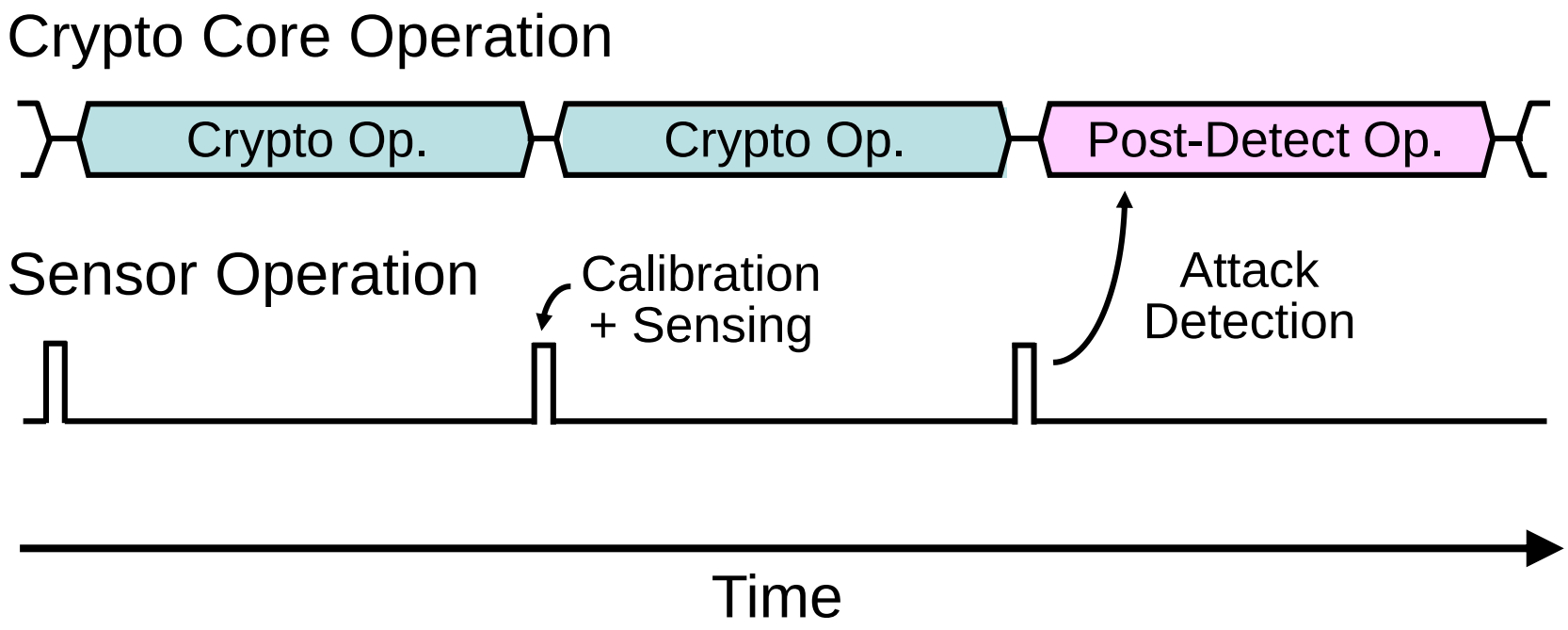


f_{Target} : Target frequency after calibration

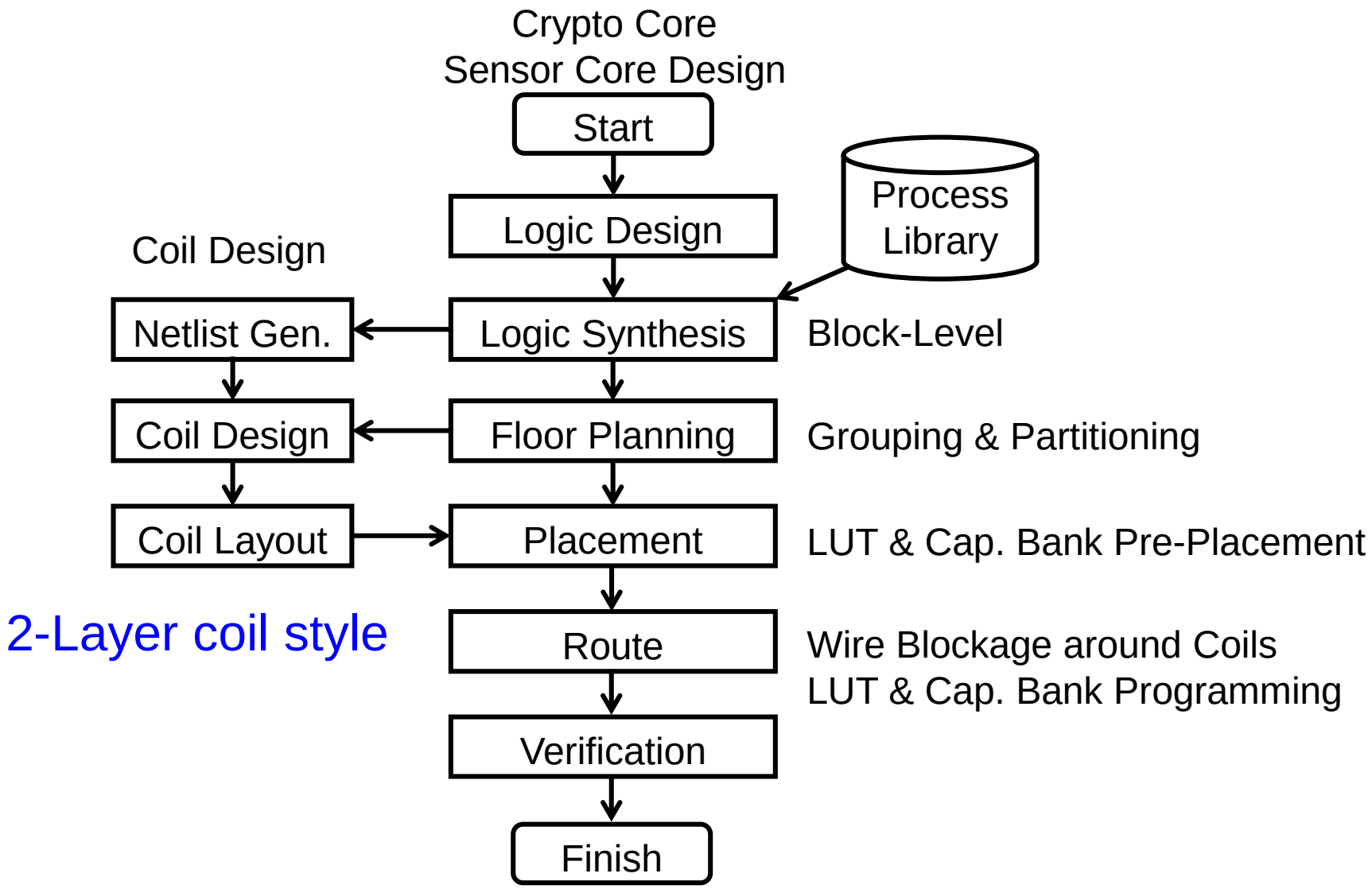
ΔC : Capacitance change for calibration (Decided by $|f_{RO}-f_{LC}|$)

Intermittent sensor operation

- Save power and performance overheads
- No interference between crypto core and sensor
  - Two circuits are activated exclusively

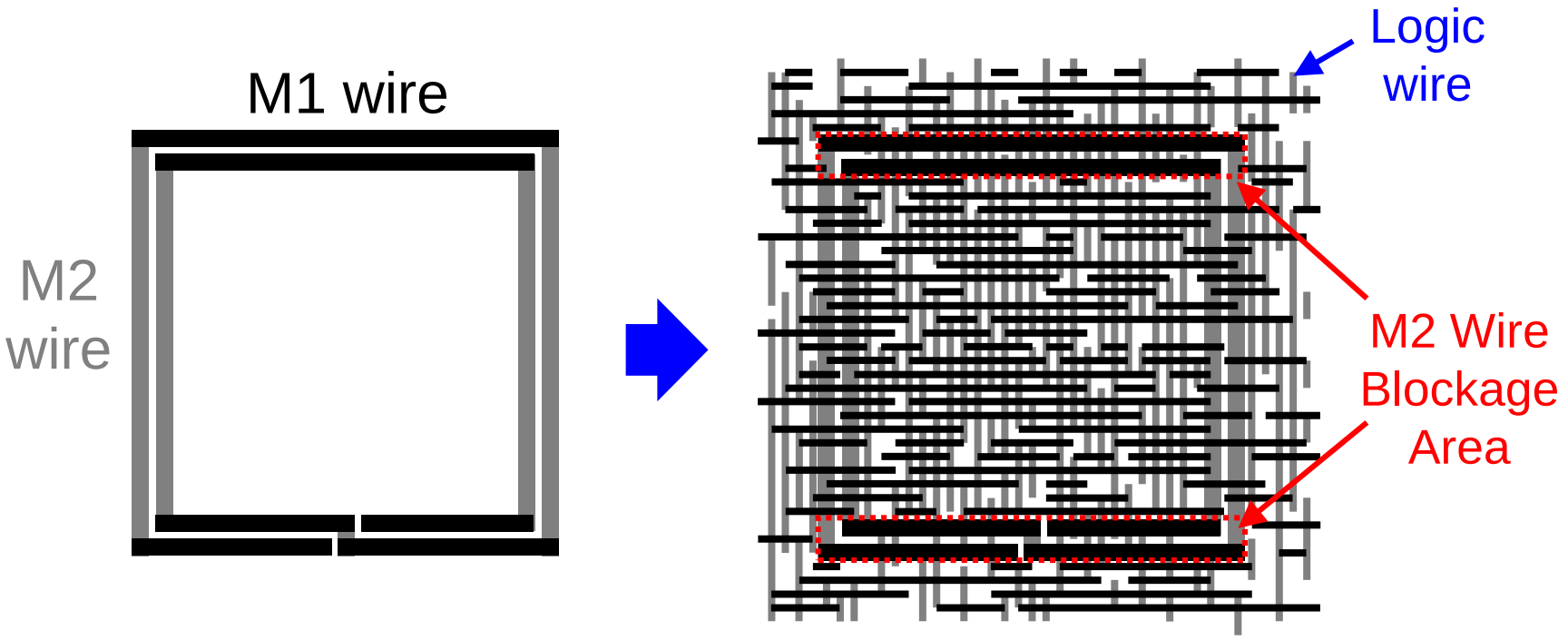


Design flow


Crypto Core
Sensor Core Design
Start
Logic Design
Process Library
Coil Design
Netlist Gen.
Logic Synthesis
Block-Level
Coil Design
Floor Planning
Grouping & Partitioning
Coil Layout
Placement
LUT & Cap. Bank Pre-Placement
2-Layer coil style
Route
Wire Blockage around Coils
LUT & Cap. Bank Programming
Verification
Finish

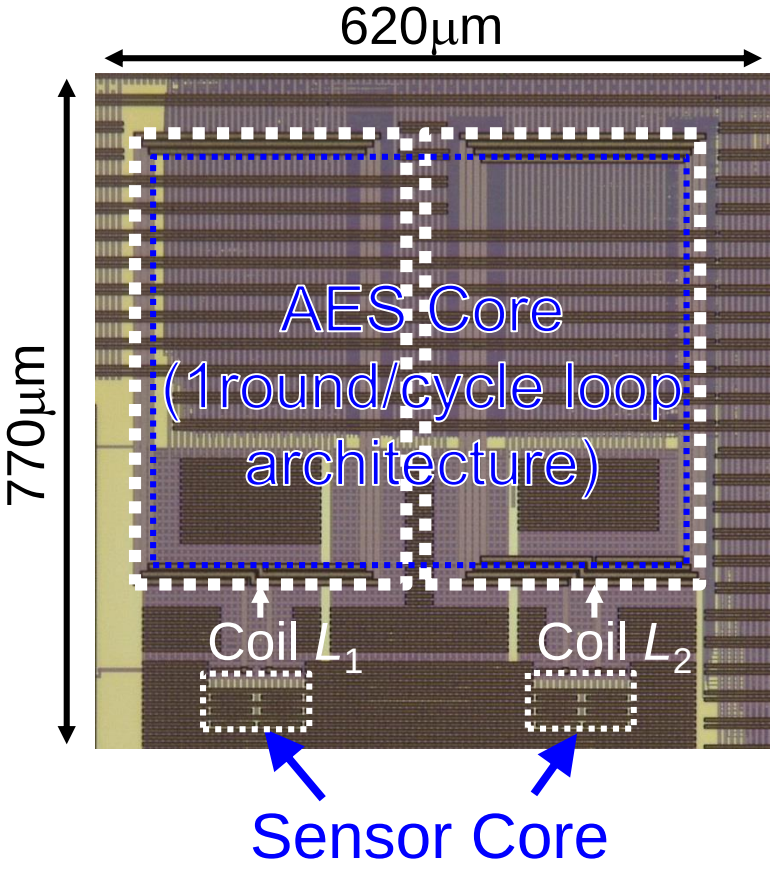
Sensor coil layout

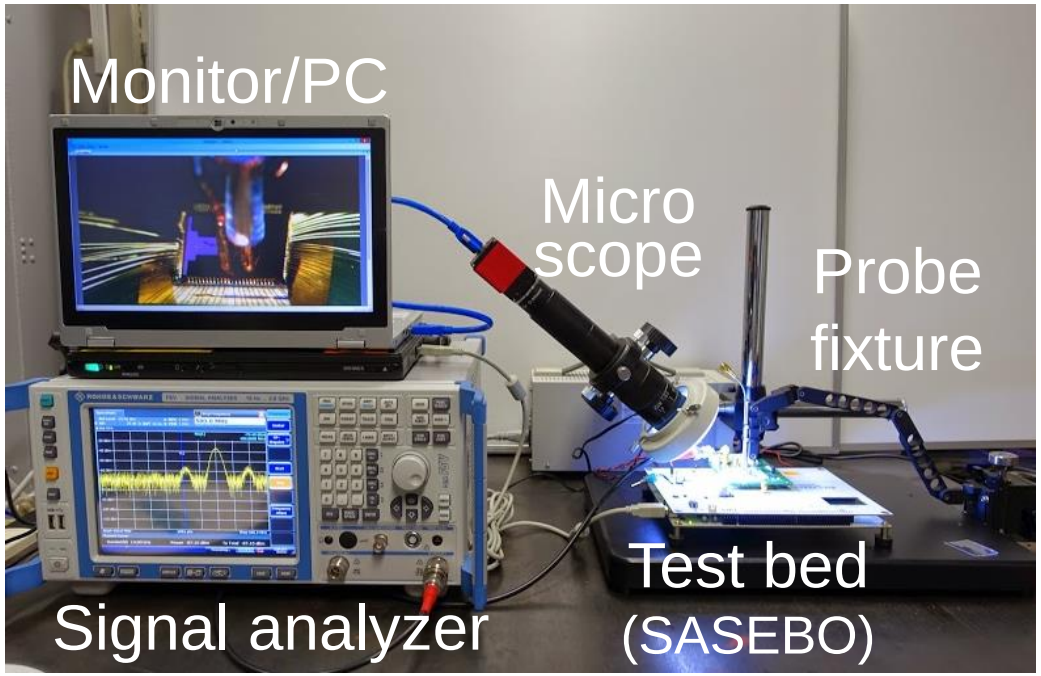
- Two different metal layers for orthogonal edges
  - Coils embedded in sea of logic interconnections
  - Save wire resources for logic circuits



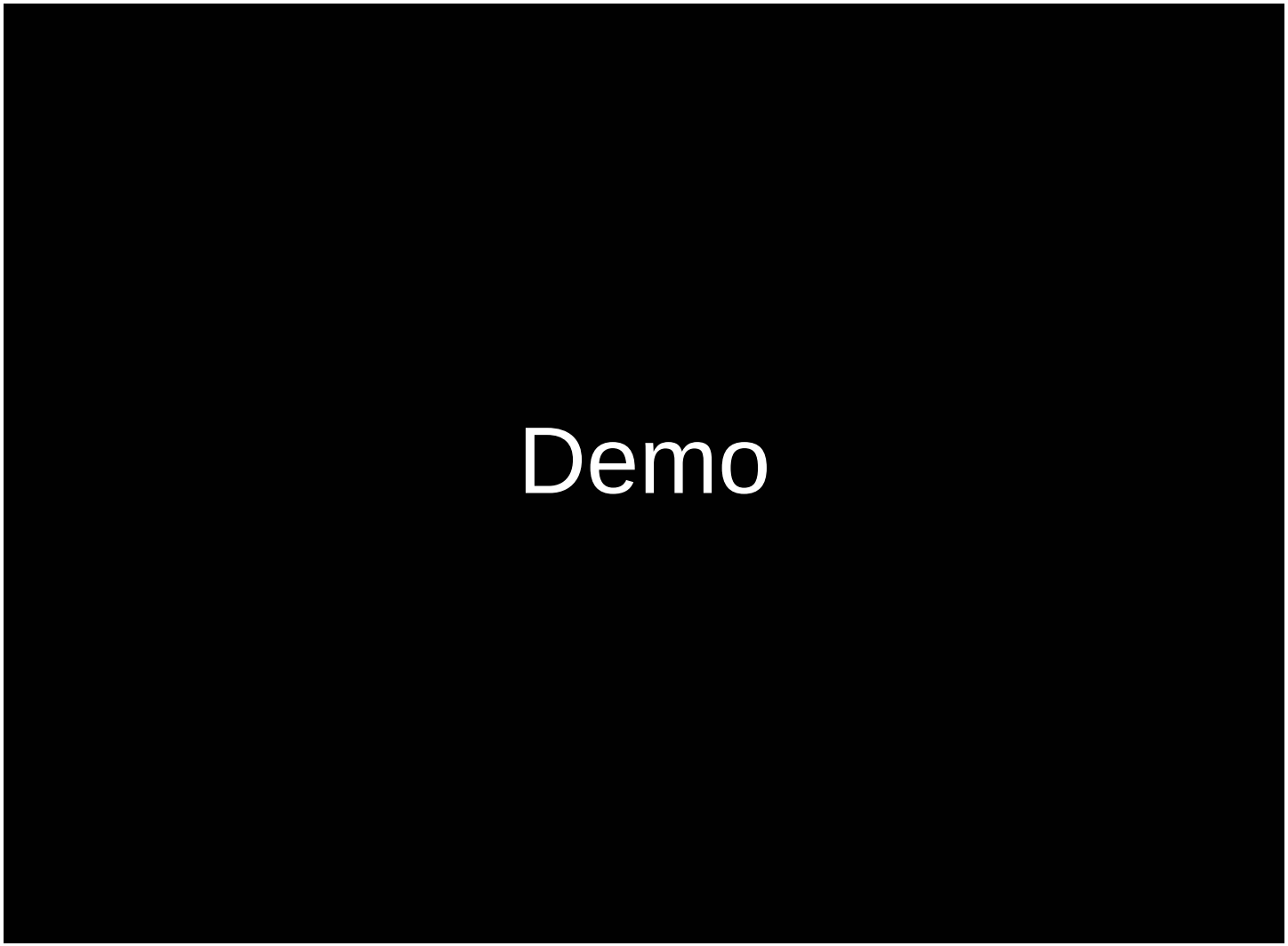
Experimental setup

- 128bit-Key AES processor with EM attack sensor fabricated in 0.18μm Logic CMOS
- Experiments of typical and prospective attack scenarios

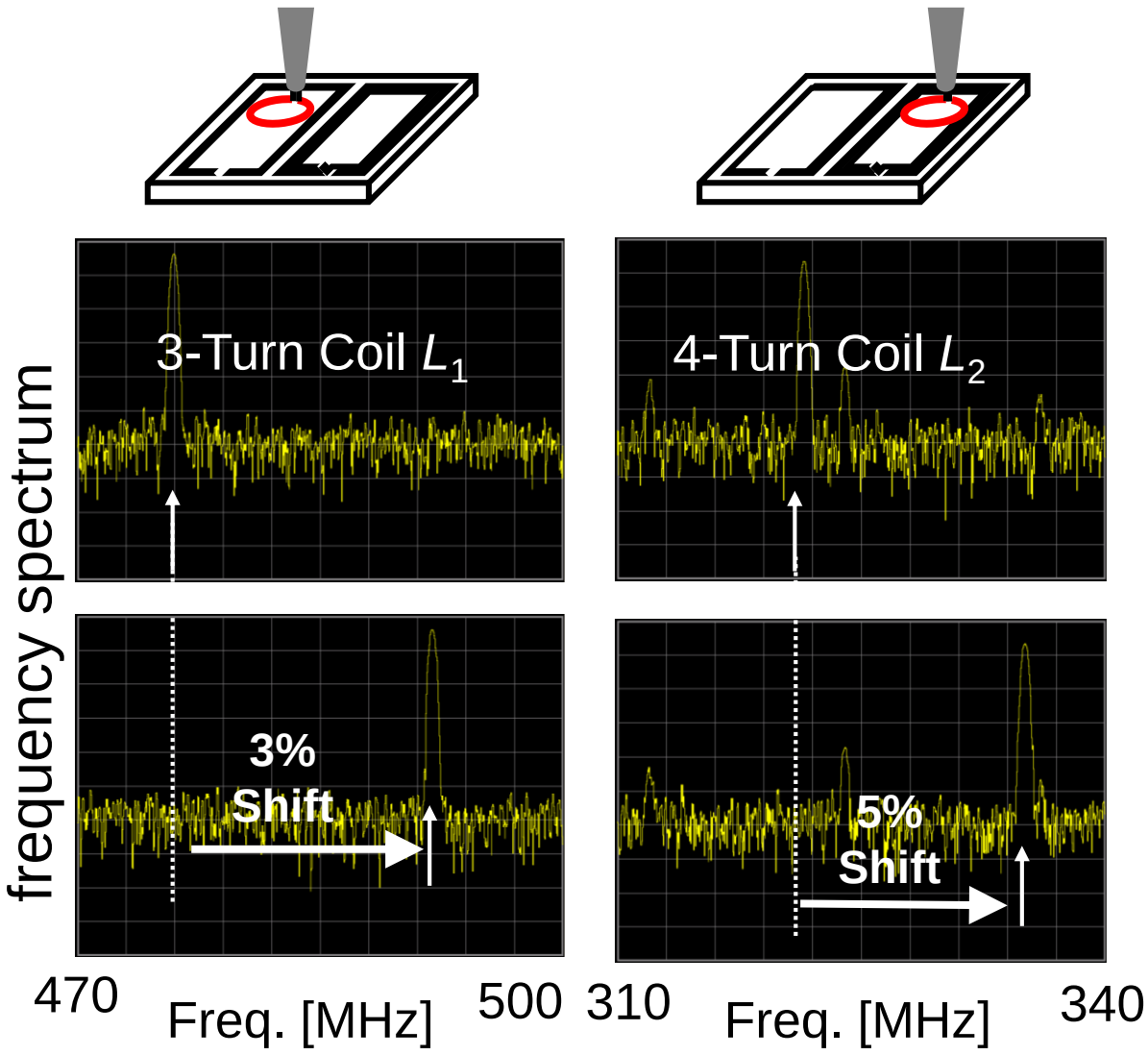




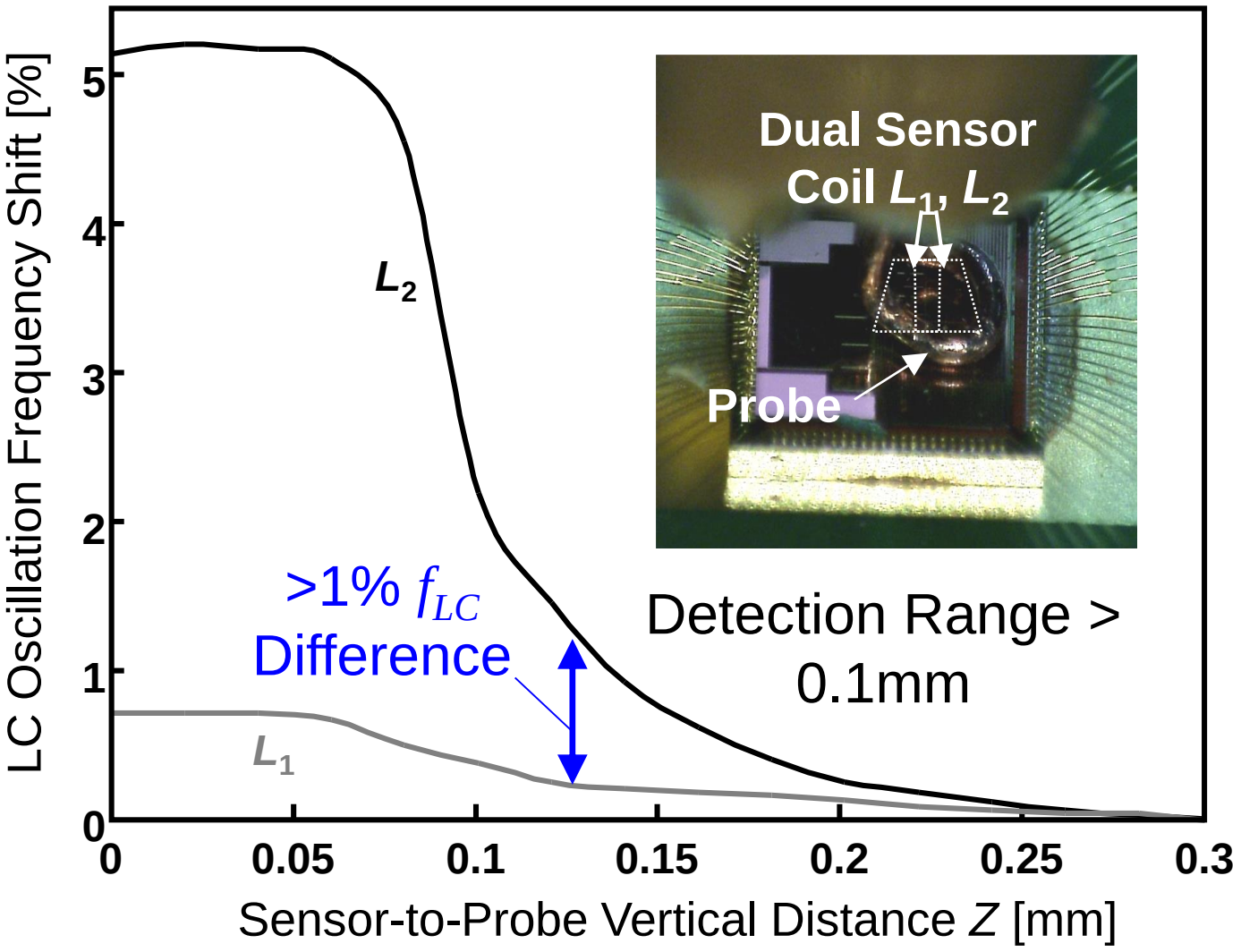
Typical attack with single micro probe



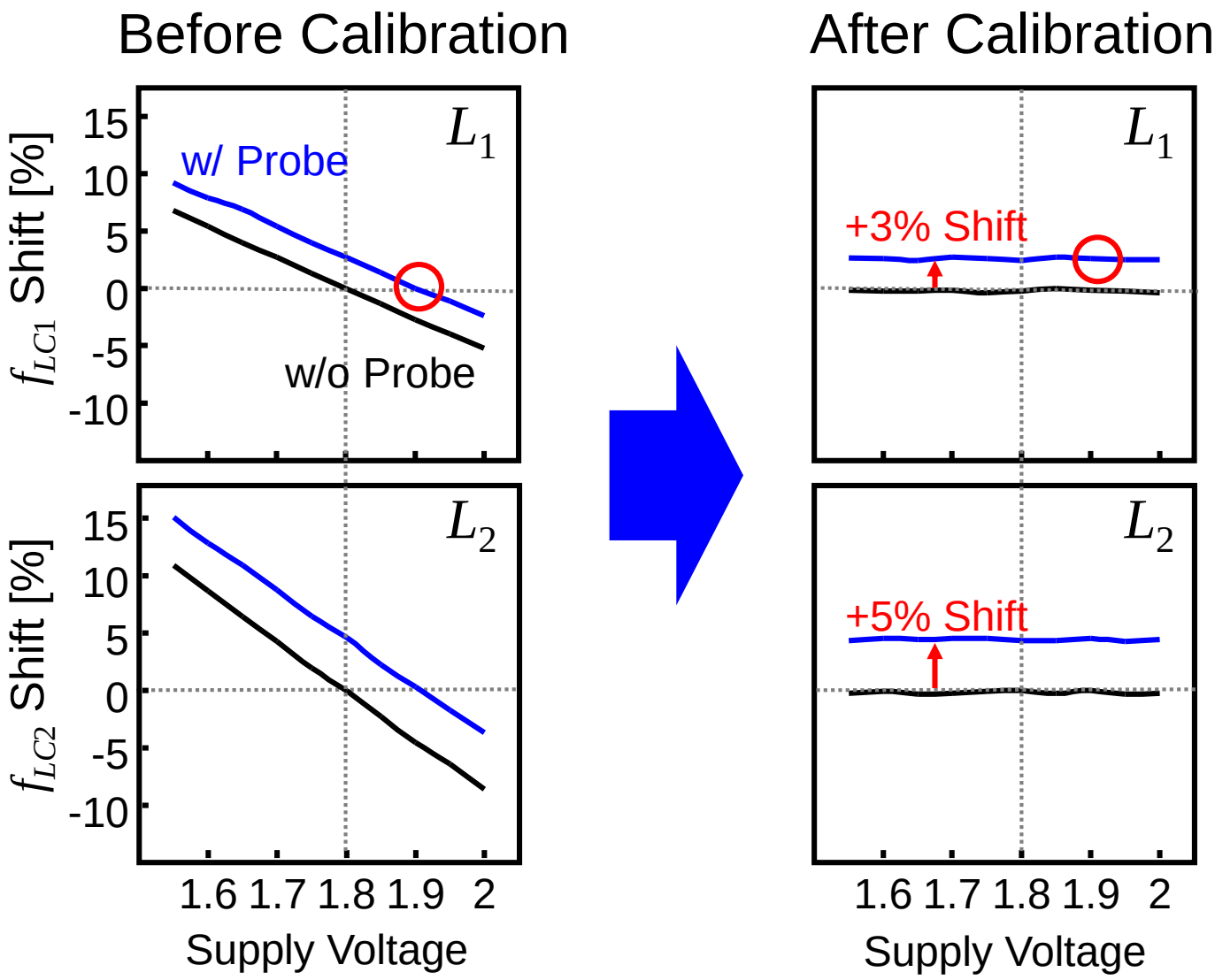
Typical attack with single micro probe



Attack with larger probe



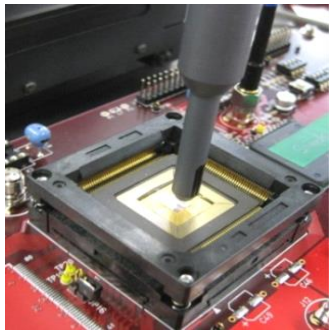
Changing PVT condition and presetting probe



Overhead of sensor

	AES core	Sensor	Total (Sensor Overhead)
2NAND Gate Count	24.3k	0.3k	24.6k (+1.2%)
Wire Resource	0.40mm^2	0.05mm^2	0.45 (+11%)
Layout Area	0.48mm^2	0.01mm^2	0.49mm^2 (+2%)
Performance	125μs/Enc	0.3μs/Sense	125.3μs (-0.2%)
Power Consumption	0.23mW	0.02mW	0.25mW (+9%)

Discussion



- Proposed sensor is effective for various probing attacks in addition to EM analysis and EM fault injection attacks
- One possible attack may be to keep the difference of LC oscillation frequencies during measurement
  - Difficulty level is high since attacker cannot see oscillation freq.
- Detection distance between probe and sensor is at most 0.1 mm so far
  - Conventional EMAs on chip package are still possible
  - Combination of existing and proposed countermeasures is practical

Conclusion

- New reactive countermeasure “EM attack sensor”
  - Sense EM field variation caused by probe approach
  - Prevent microprobe-based EMAs performed on chip surface
- Design methodology and validity verification
  - Standard-cell-based design methodology
  - Showed low cost and performance overhead
  - Demonstrated detection of typical and prospective attacks
- Future works
  - Extension of maximum detection distance
  - Effective combination with existing countermeasures
  - Further validation based on other possible attack scenarios

Thank you