Towards The Design of Robust Secure Digital Cameras (SDC)

Saraju P. Mohanty

Computer Science and Engineering

University of North Texas.

Outline of The Talk

- Digital Rights Management (DRM)
- Secure Digital Camera (SDC) for real-time DRM
- Robust SDC using AMS-SoC Design Tradeoffs
- Energy-Efficient Watermarking Chip
- Variability-Tolerant Voltage Controlled Oscillator
- Related Research
- Summary and Conclusions

Digital Rights Management (DRM)

Refer:

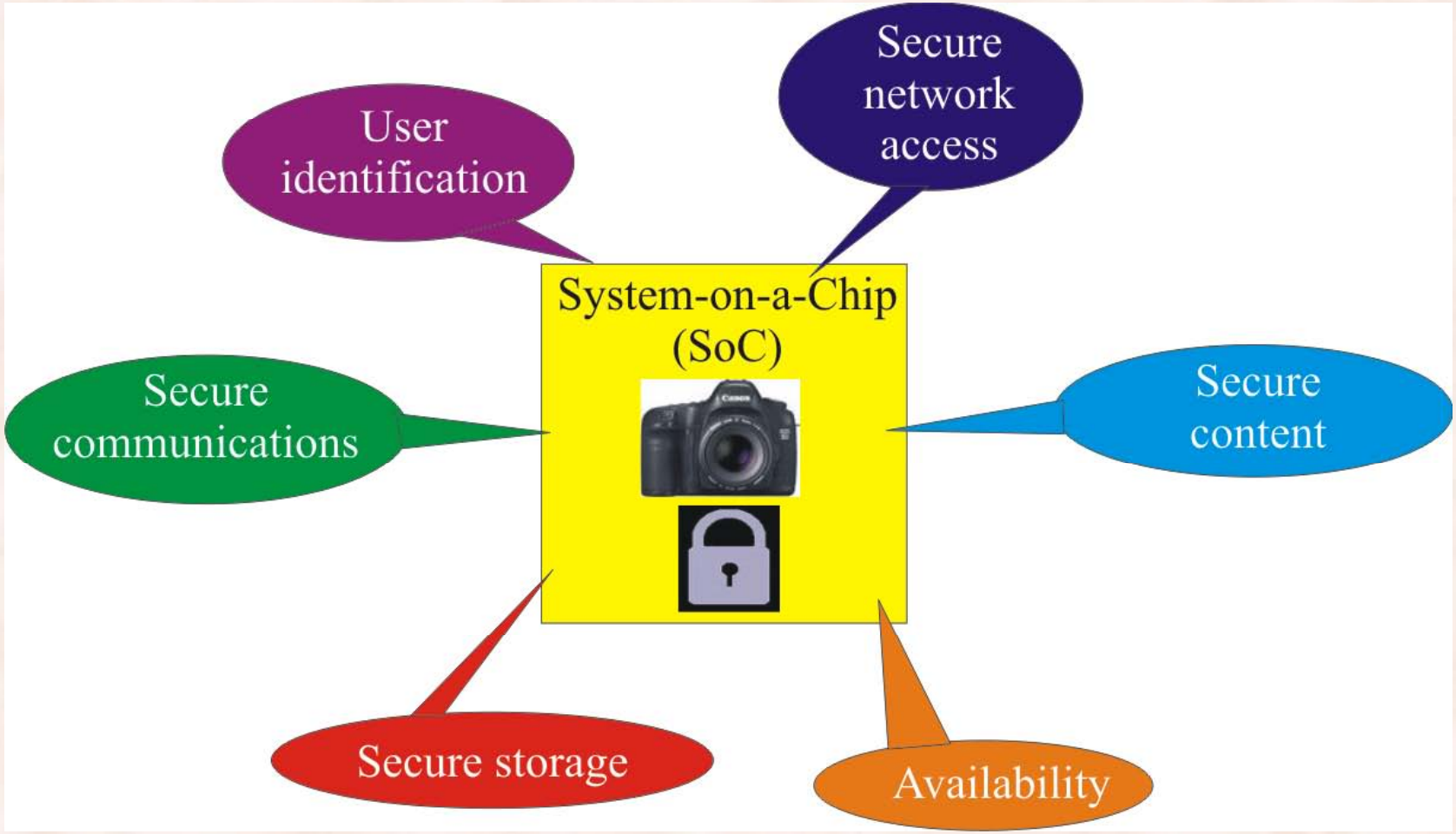
- E. Kougianos, **S. P. Mohanty**, and R. N. Mahapatra, "Hardware Assisted Watermarking for Multimedia", *Special Issue on Circuits and Systems for Real-Time Security and Copyright Protection of Multimedia, Elsevier International Journal on Computers and Electrical Engineering (IJCEE)*, Volume 35, Issue 2, March, 2009, pp. 339-358.

Mobile Consumer Electronics

What are common?

- Access, store, and process multimedia.
- Consume power (energy).
- Designed as Analog/Mixed-Signal System-on-Chips (AMS-SoCs)

Security Requirements in AMS-SoCs: The Big Picture



- Content security is of interest which is handled through digital rights management (DRM) facility.

Digital Rights Management (DRM) : Definition

- DRM is a generic term that refers to any of several technologies used by publishers, creators, or owners to control access and usage of digital data.
- Typically a DRM system:
  - Protects intellectual property by encrypting the data so that it can only be accessed by authorized users.

    and/or

  - Marks the content with a watermark so that the content is distributed with built-in copyright.

DRM : Definition …

Watermarking

Cryptography

- Judicious use of both encryption and watermarking necessary for multilayer protection through DRM.

Secure Digital Camera (SDC) for Efficient DRM

Refer:

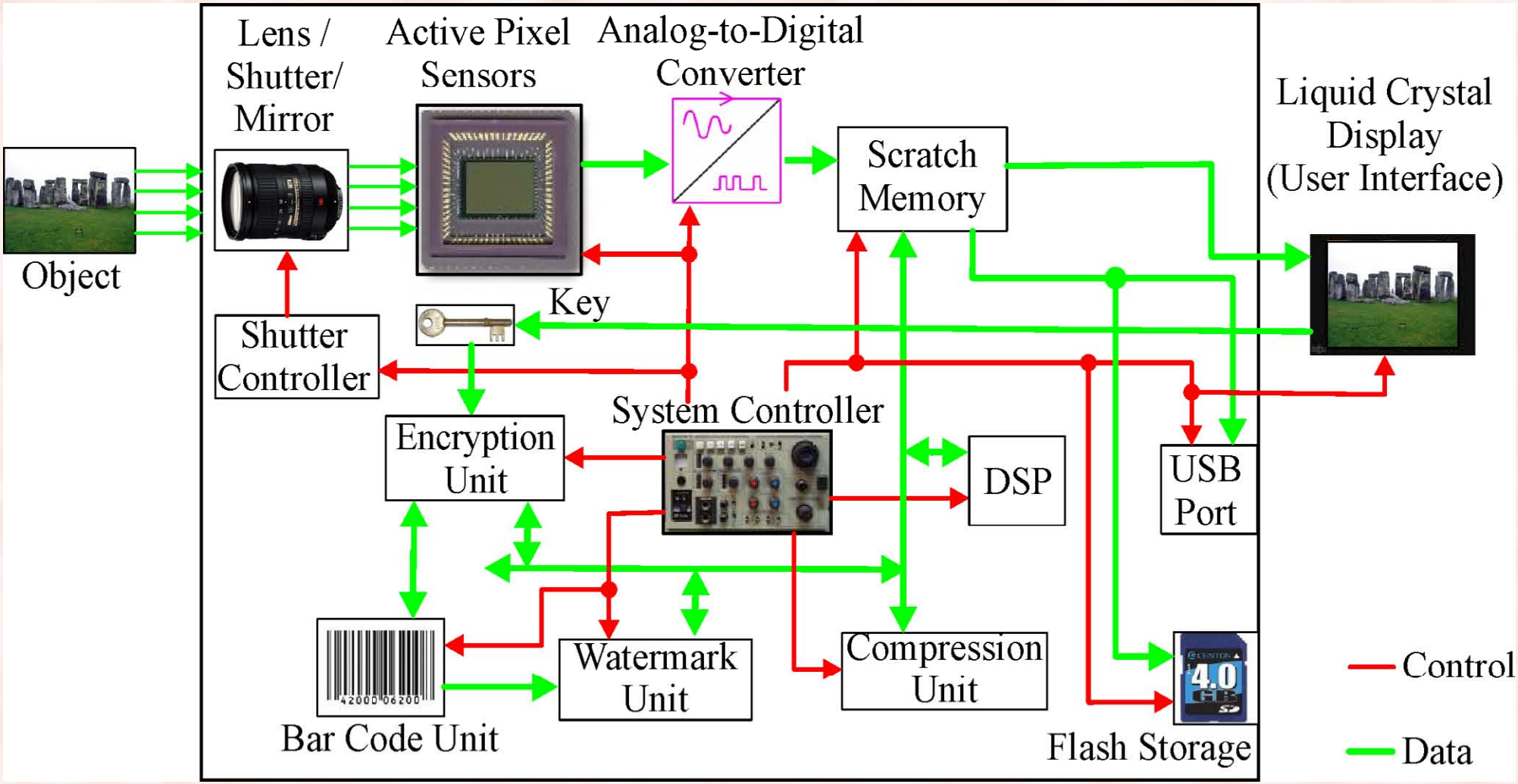
- **S. P. Mohanty**, “A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management”, *Elsevier Journal of Systems Architecture (JSA)*, Vol. 55, No. 10-12, Oct-Dec 2009, pp. 468-480.
- **S. P. Mohanty**, N. Ranganathan, and R. K. Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S^2DC) Design", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 13, No. 8, August 2005, pp. 1002-1012.

Secure Digital Camera (SDC)

- An apparatus built as system-on-a-chip (SoC) with standards features of digital camera and built in facility for real-time, low-cost, energy-efficient DRM.

- For a given image/video SDC needs to prove:
  - Copyright (visible watermarking)
  - Extent of tampering (invisible-fragile watermarking)
  - Source of image i.e. camera information, place, or date (invisible-robust or visible watermarking)
  - Owner's, creator's, or cameraman's information (invisible-robust or visible watermarking)

Secure Digital Camera: AMS-SoC

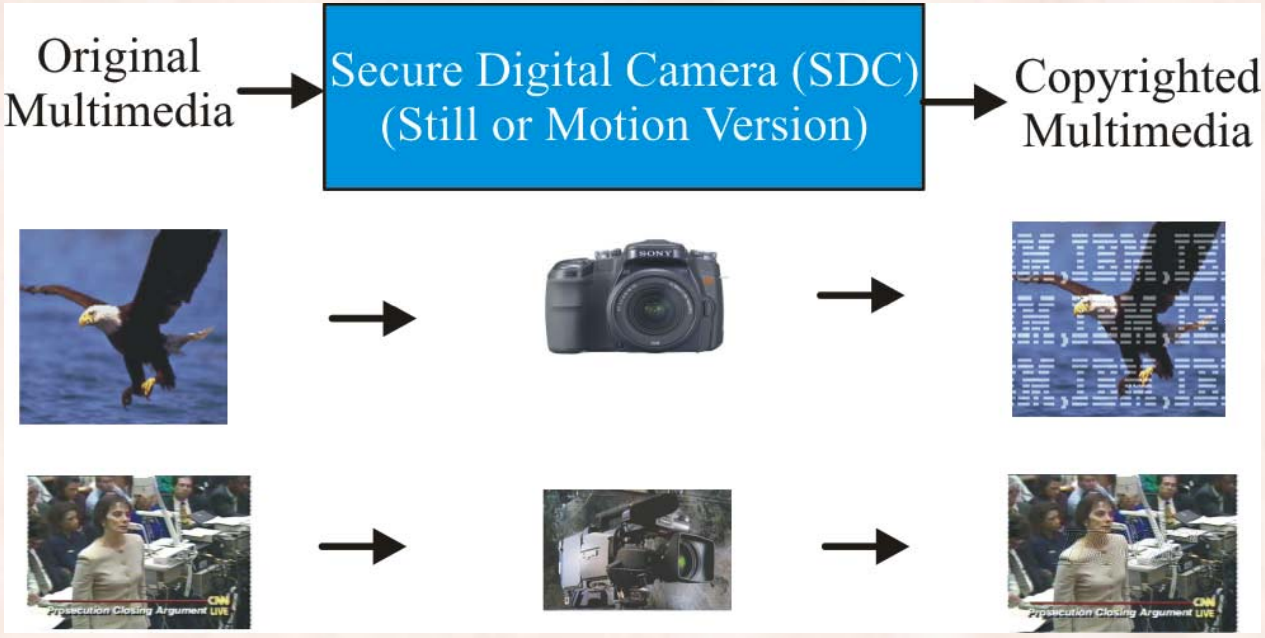


Hardware Based DRM : Advantages

- Easy integration with multimedia hardware, such as digital camera, network processor, GPU, etc.
- Low-power and low-cost compared to software.
- High-performance compared to software.
- Higher reliability/availability compared to software.
- Useful for real-time applications like broadcasting.
- DRM right at the source end will ensure that the information is always protected.
- DRM integrated with multimedia hardware will be more acceptable as legal evidence.

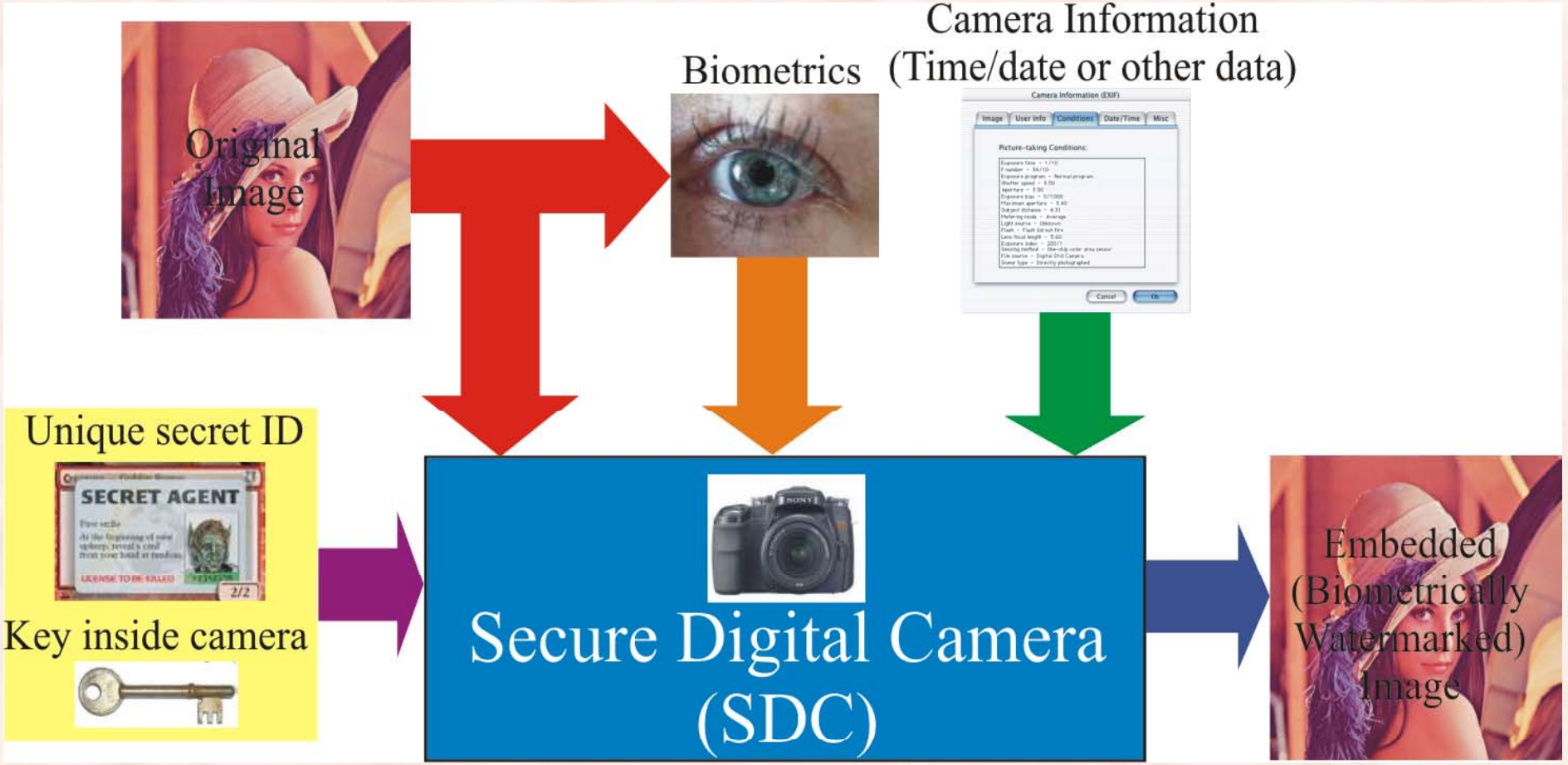
SDC Application: Copyright Protection

- Publicly available images
- Digital Library
- DVD Video
- Digital TV Broadcasting



NOTE: Can enhance revenue of movie/broadcasting industry.

SDC Application: Biometric Based Authentication



NOTE: Can be useful for security, e-passport applications; Refer: Blythe and Fridrich, DFRWS-2004.

Robust SDC Through AMS-SoC Design Tradeoffs

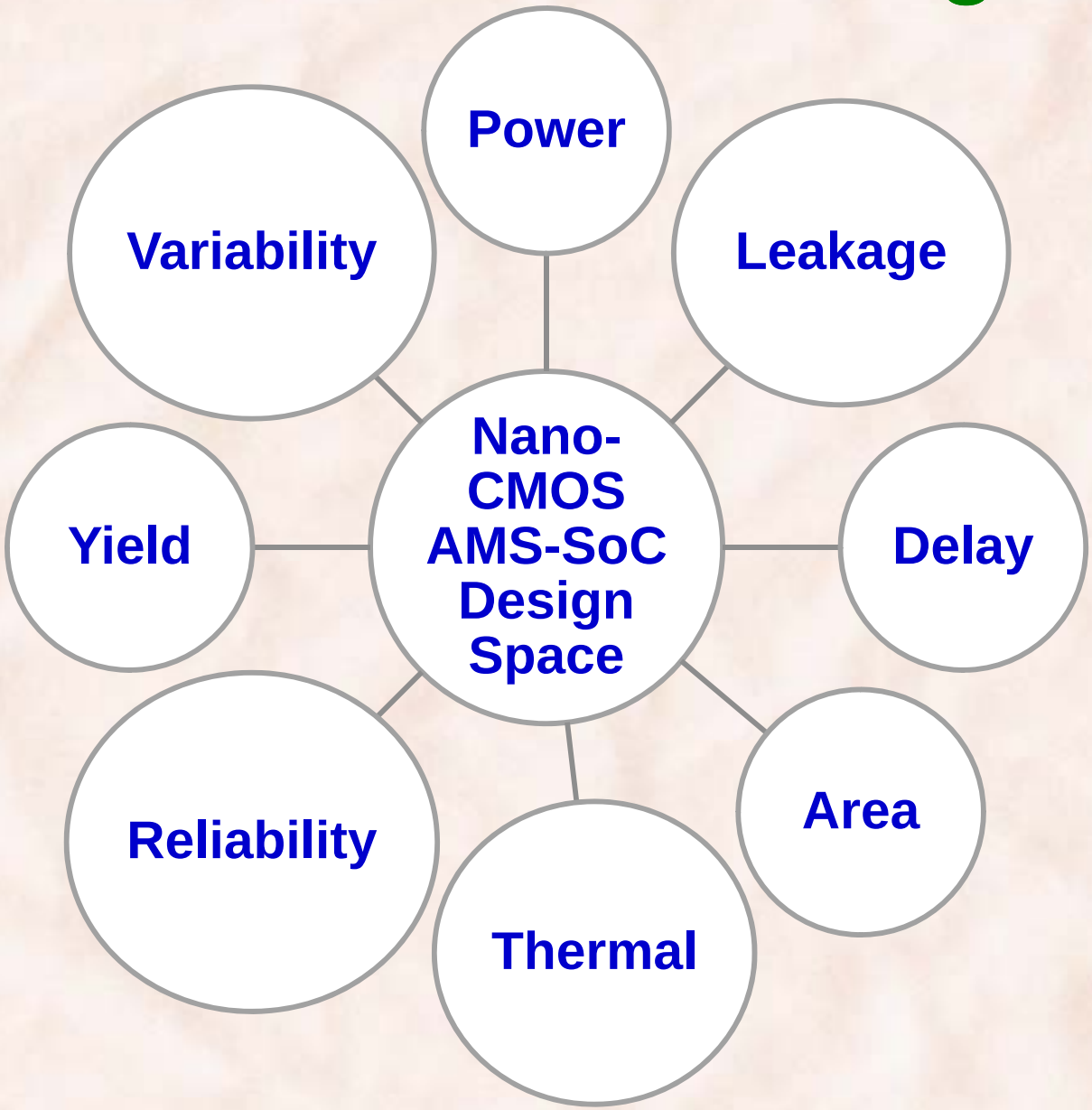
Refer:

- **S. P. Mohanty**, D. Ghai, and E. Kougianos, “A P4VT (Power-Performance-Process-Parasitic-Voltage-Temperature) Aware Dual-V_{Th} Nano-CMOS VCO”, in *Proc. 23rd IEEE International Conference on VLSI Design*, pp. 99-104, 2010
- **S. P. Mohanty**, "Unified Challenges in Nano-CMOS High-Level Synthesis", Abstract, Invited Talk, in *Proceedings of the 22nd IEEE International Conference on VLSI Design*, pp. 531-531, 2009.

Secure Digital Camera : Design Alternatives

- New CMOS sensor with DRM.
- New ADC with DRM.
- Independent DRM processors.
- DRM co-processor for DSP.
- New instruction set architecture for RISC to support DRM at micro-architecture level.

Nano-CMOS AMS-SoC Design of SDC



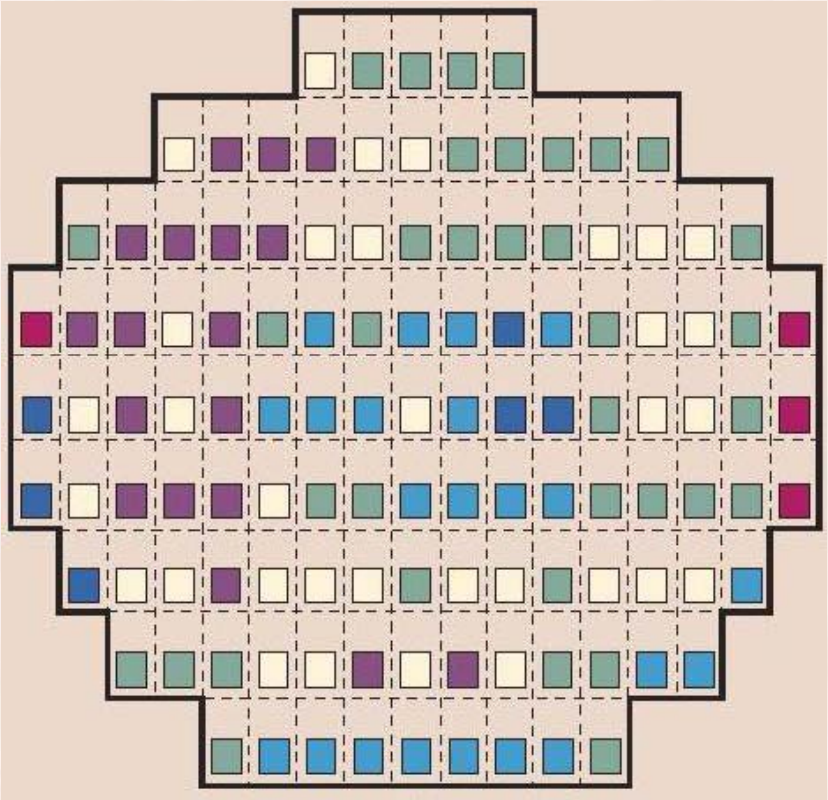
Issues in Nano-CMOS AMS-SoC …

- **Variability**: Variability in process and design parameters has increased. They affect design decisions, yield, and circuit performance.
- **Leakage**: Leakage is increasing. Affects average and peak power metrics. Most significant for applications where system goes to standby mode very often, e.g. PDAs.
- **Power**: Overall chip power dissipation increasing. Affect energy consumption, cooling costs, packaging costs.

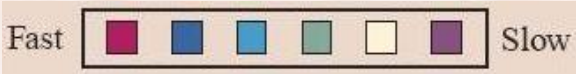
Issues in Nano-CMOS AMS-SoC

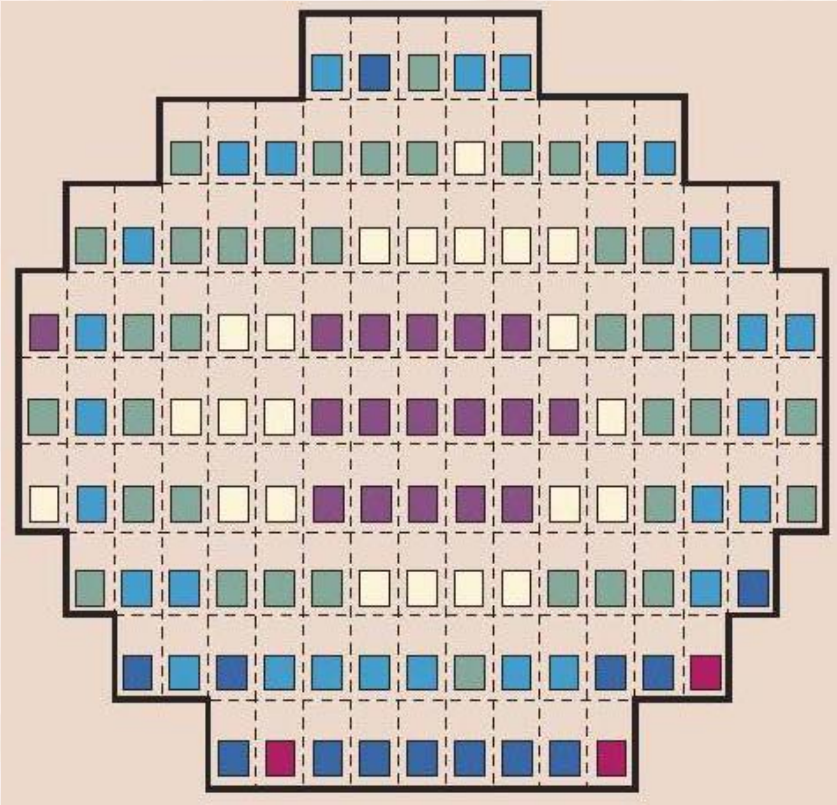
- **Thermals**: Maximum temperature that can be reached by a chip during its operation is increasing. Affects reliability and cooling costs.
- **Reliability**: Circuit reliability is decreasing due to compound effects from variations, power, and thermals.
- **Yield**: Circuit yield is decreasing due to increased variability.

Variability: The Impact in a Wafer



Source–drain resistance is different for different chips in a same die.



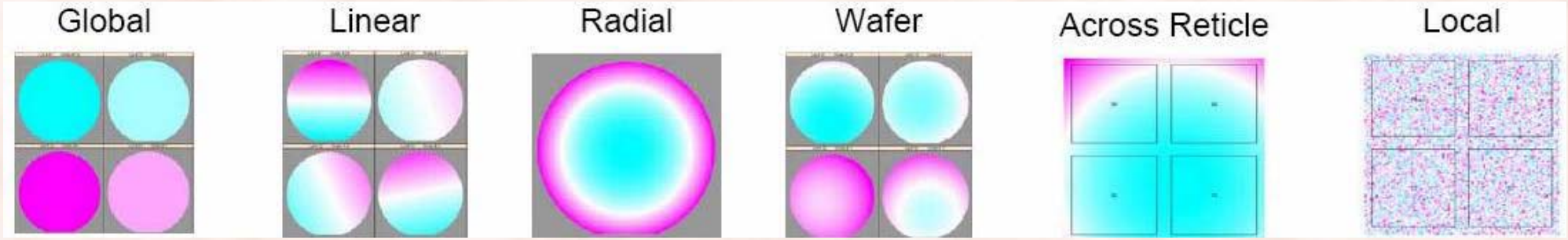


Gate-to-source and gate-to-drain overlap capacitance is different for different chips in a same die.

Source: Bernstein et al., IBM J. Res. & Dev., July/Sep 2006.

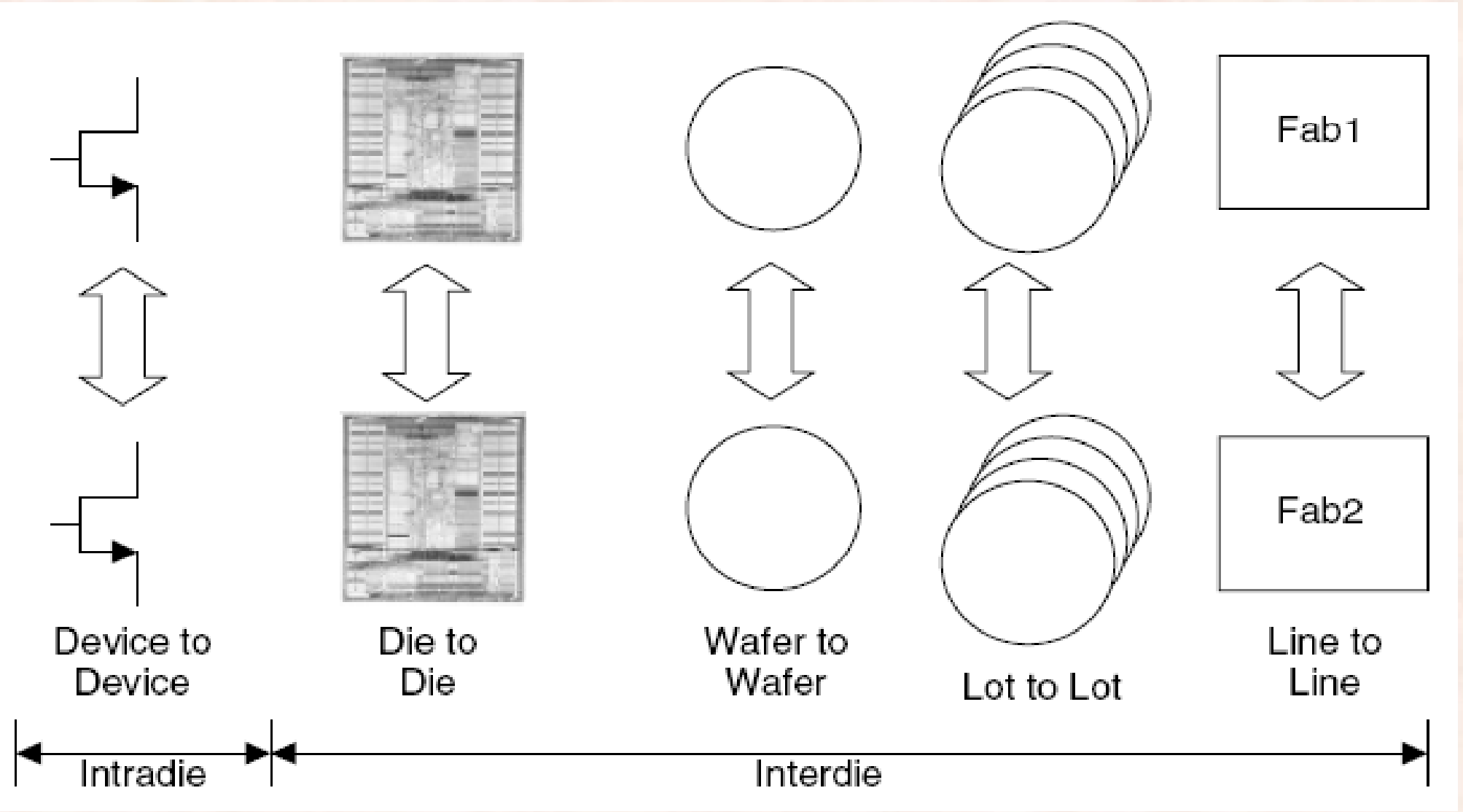
Variability: Types …

- **Parametric Variations**
  - **Wafer**
    - **Global**
    - **Linear**
      - **Caused by Materials/Gas Flow**
    - **Radial**
      - **Caused by Thermal/Spin Processes**
  - **Reticle**
    - **Caused by Photo Processes**
  - **Local**
    - **Caused by Random Microscopic Processes**

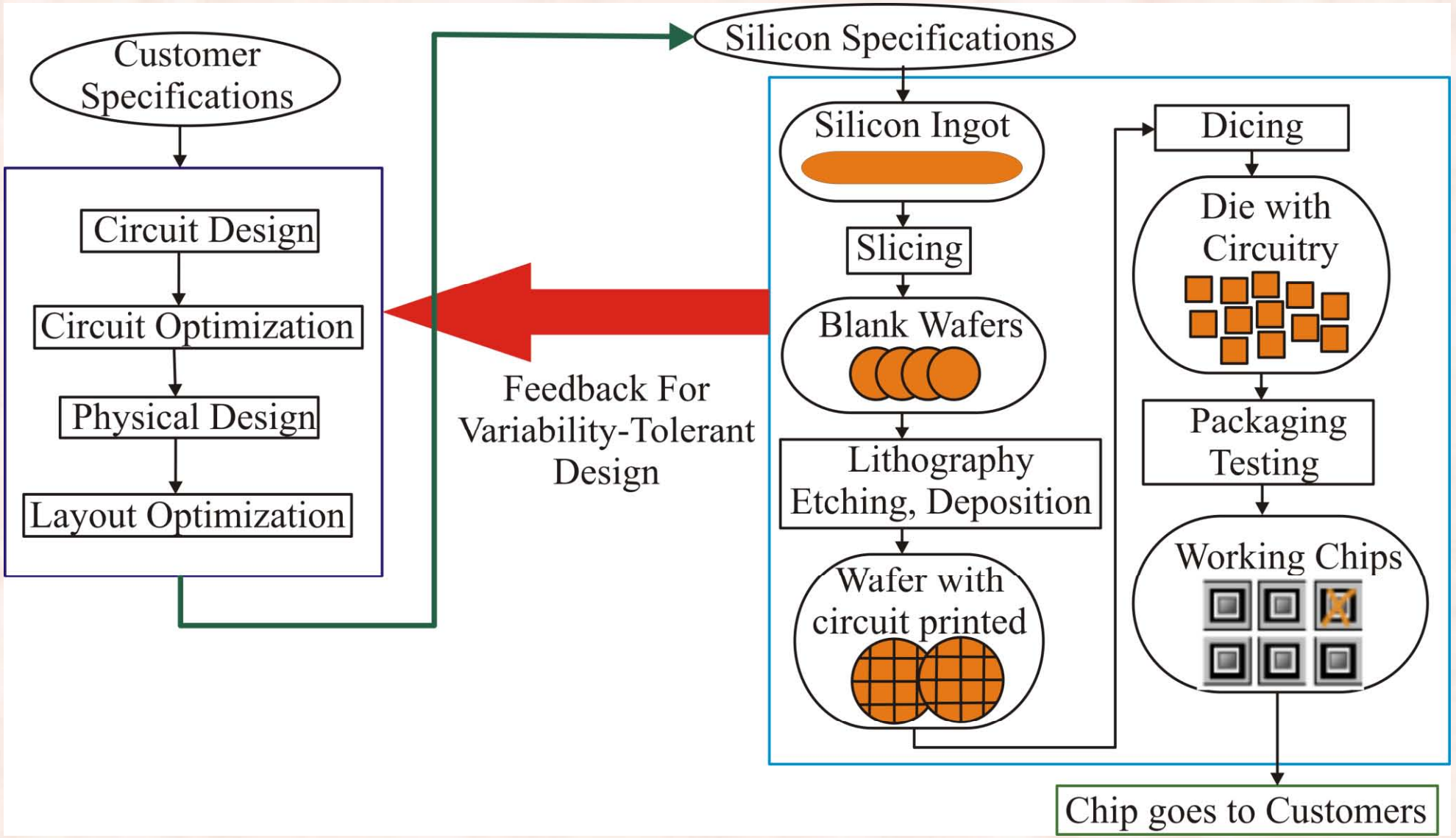


Source: Singhal, DAC Booth 2007

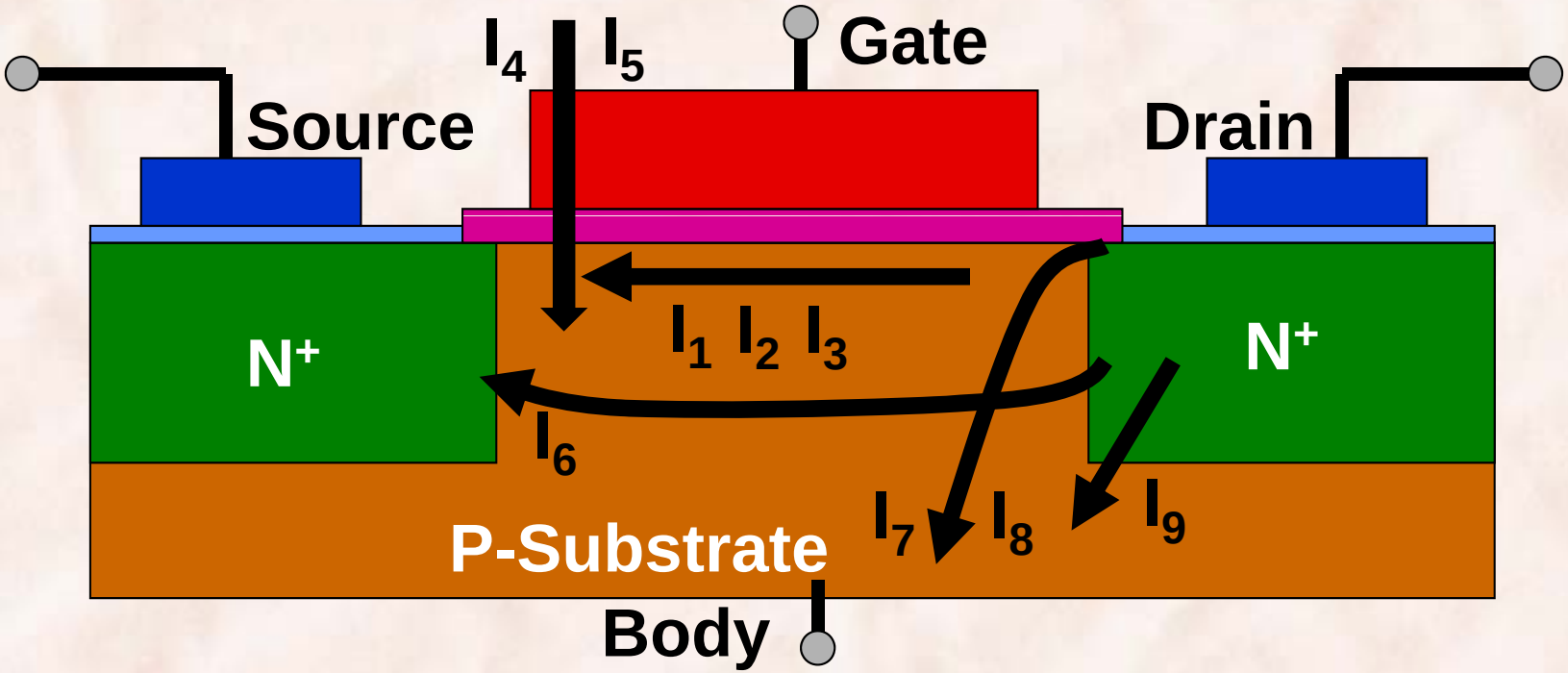
Variability: Types



Variability-Tolerant Design



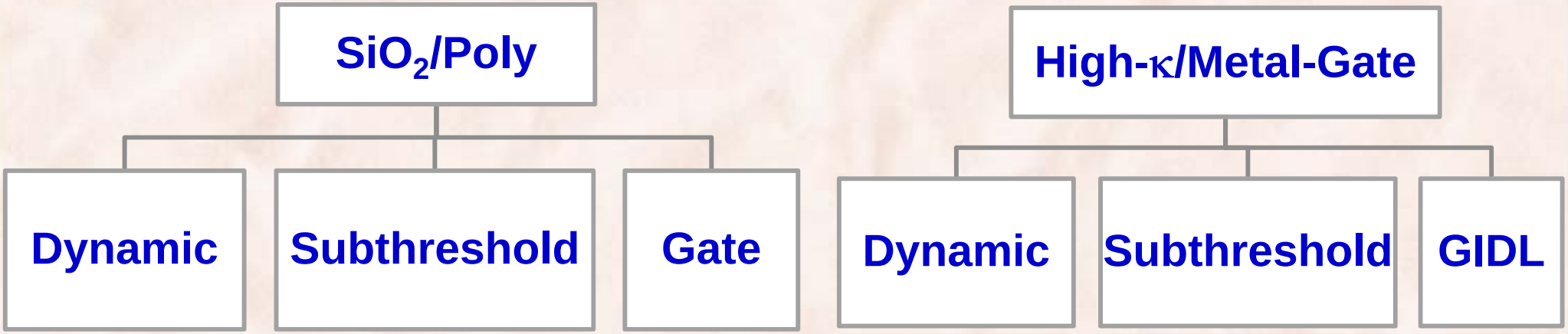
Power and Leakage …



I_1 : drain-to-source active current (ON state)
I_2 : drain-to-source short circuit current (ON state)
I_3 : subthreshold leakage (OFF state)
I_4 : gate Leakage current (both ON & OFF states)
I_5 : gate current due to hot carrier injection (both ON & OFF states)
I_6 : channel punch through current (OFF state)
I_7 : gate induced drain leakage (OFF state)
I_8 : band-to-band tunneling current (OFF state)
I_9 : reverse bias PN junction leakage (both ON & OFF states)

Power and Leakage

- Relative prominence of the components depend on:
  - Technology Node: 65nm, 45nm, or 32nm
  - Process : SiO_2/Poly or High-κ/Metal-Gate



An Energy-Efficient Watermarking Chip

Refer:

- **S. P. Mohanty**, N. Ranganathan, and K. Balakrishnan, "A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain", *IEEE Transactions on Circuits and Systems II (TCAS-II)*, Vol. 53, No. 5, May 2006, pp. 394-398.

A Low-Power Design Approach

Adjust the frequency and supply voltage in a coordinated manner to reduce the power consumption while maintaining performance.

NOTE: Methods for gate-oxide and subthreshold leakage power reduction are also researched.

Highlights of The Watermarking Chip

- DCT domain multimedia processing.
- First to insert both visible and invisible watermarks.
- First low-power design for watermarking using dual voltage and dual frequency.
- Uses selective pipelined and parallelization for better performance.
- Uses decentralized controller scheme to indirectly implement clock gating for power reduction.

Algorithms Selected for The Chip

- Invisible watermarking algorithm:

  I. J. Cox, et al., “Secure Spread Spectrum Watermarking for Multimedia”, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, 1997, pp. 1673-1687.

- Visible watermarking algorithm:

  S. P. Mohanty, et al., "A DCT Domain Visible Watermarking Technique for Images", in *Proceedings of IEEE International Conference on Multimedia and Expo*, 2000, pp. 1029-1032.

NOTE: Highest cited papers in respective category.

Invisible Watermarking Algorithm :
A Modified Version

1. Divide the original image into blocks.
2. Calculate the DCT coefficients of all the image blocks.
3. Consider the 3 largest AC-DCT coefficients of each block for watermark insertion.
4. Compute the watermark $X = \{x_1, x_2, \ldots, x_n\}$, where each x_i is chosen according to $N(0, 1)$, where $N(0, 1)$ denotes a normal distribution with mean 0 and variance 1.
5. Insert the watermark in the DCT domain of the image by setting the frequency components v_i in the original image to v^*_i using the following for scalar factor α:

$$v_i^* = v_i(1 + \alpha x_i)$$

Visible Watermarking Algorithm ...

1. Divide original and watermark image into blocks.
2. Calculate DCT coefficients of all the blocks.
3. Determine the blocks containing edges in the original image.
4. Determine the local and global statistics (μ, σ) of the original image using the DC-DCT and AC-DCT coefficients.
5. Calculate the scaling and embedding factors.
6. Add the original image DCT coefficients and the watermark DCT coefficients block by block.

Visible Watermarking Algorithm

- The α_k and β_k for edge blocks are taken to be α_{max} and β_{min}, respectively.
- For non-edge blocks α_k and β_k are computed as:

$$\alpha_k = \sigma^*_{AC_{Ik}} \left[\exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2\right\}\right]$$

$$\beta_k = \frac{1}{\sigma^*_{AC_{Ik}}} \left[1 - \exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2\right\}\right]$$

- α_k and β_k are then scaled to the ranges (α_{min}, α_{max}) and (β_{min} , β_{max}), respectively.

Visible Watermarking Algorithm :
Modifications

- Use $c_{Iwhite}(0,0)$ for normalization instead of $c_{Imax}(0,0)$.
- Rewrite α_k and β_k equations:

$$\alpha_k = \frac{\sigma_{AC_{Ik}}}{\sigma_{AC_{\max}}}\left[\exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2\right\}\right]$$

$$\beta_k = \frac{\sigma_{AC_{\max}}}{\sigma_{AC_{Ik}}}\left[1 - \exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC_I})^2\right\}\right]$$

- Remove σ_{ACImax}:

$$\alpha^c{}_k = \sigma_{AC_{Ik}}\left[\exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2\right\}\right]$$

$$\beta^c{}_k = \frac{1}{\sigma_{AC_{Ik}}}\left[1 - \exp\left\{-(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2\right\}\right]$$

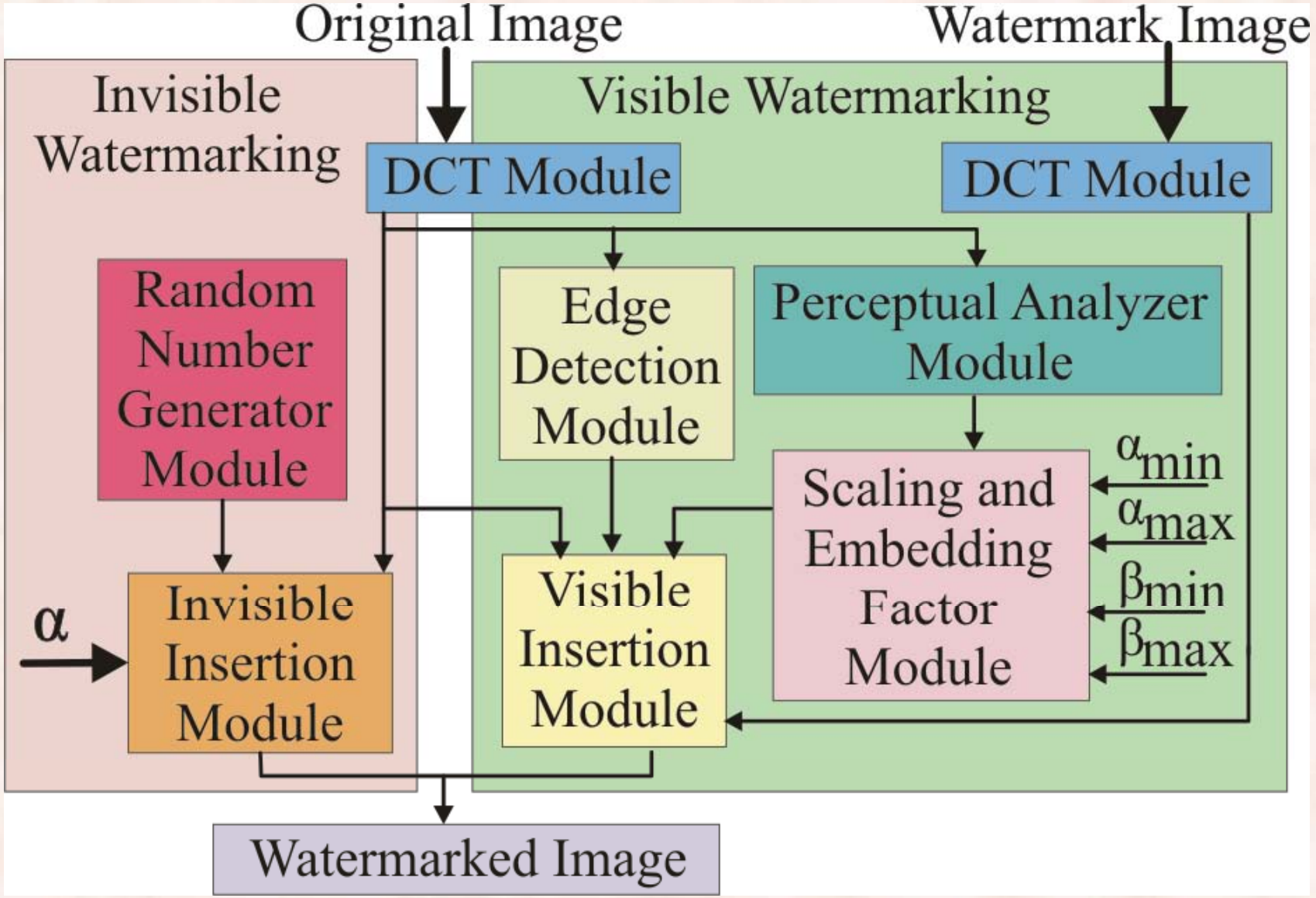
- Remove exponential using Taylor series:

$$\alpha^c{}_k = \sigma_{AC_{Ik}}\left\{1 - (\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2 + (\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^4\right\}$$

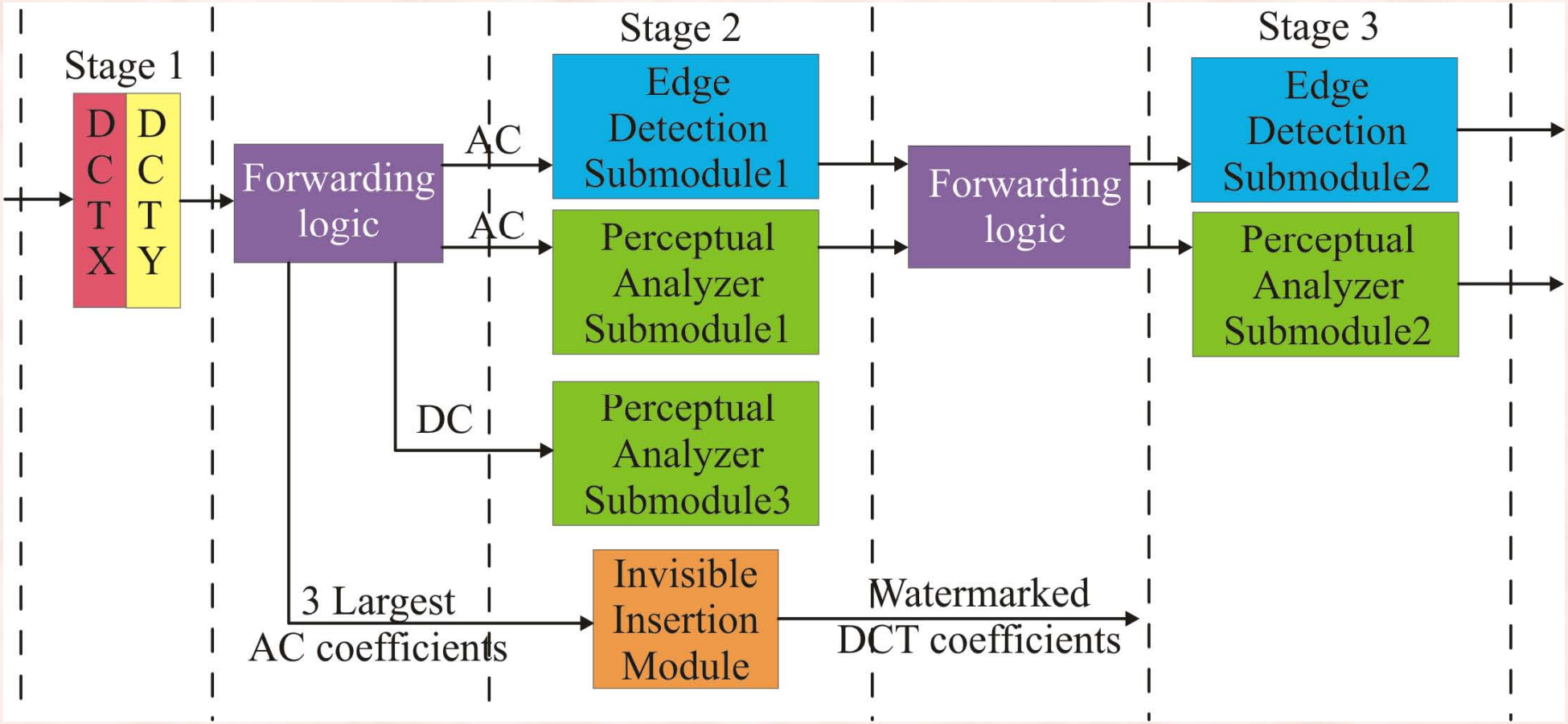
$$\beta^c{}_k = \frac{1}{\sigma_{AC_{Ik}}}\left\{(\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^2 - (\mu^*_{DC_{Ik}} - \mu^*_{DC\,I})^4\right\}$$

- Scale to ranges: (α_{min}, α_{max}) and (β_{min}, β_{max}).

The Proposed Datapath Architecture

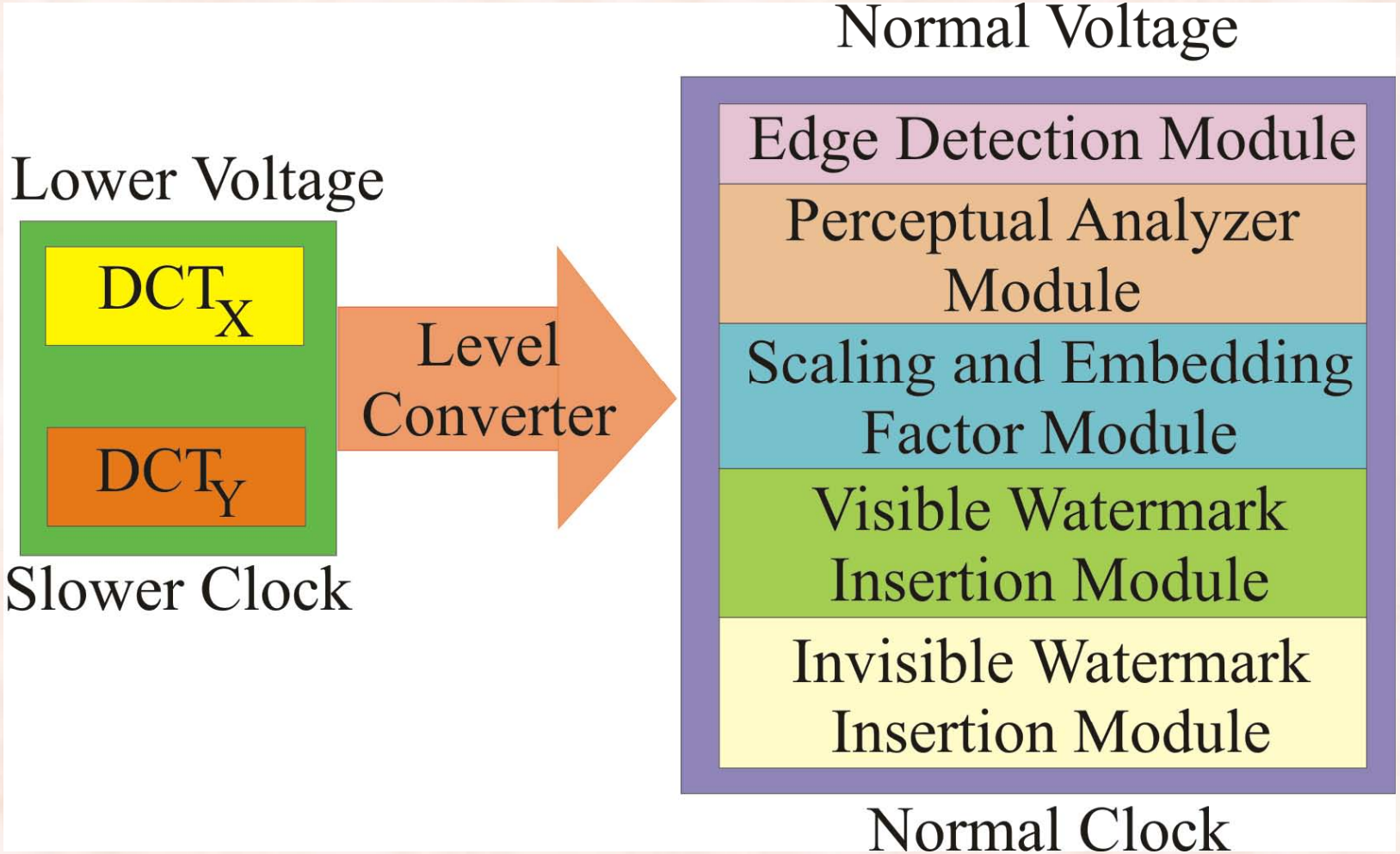


The Proposed Datapath Architecture: Pipeline and Parallelism

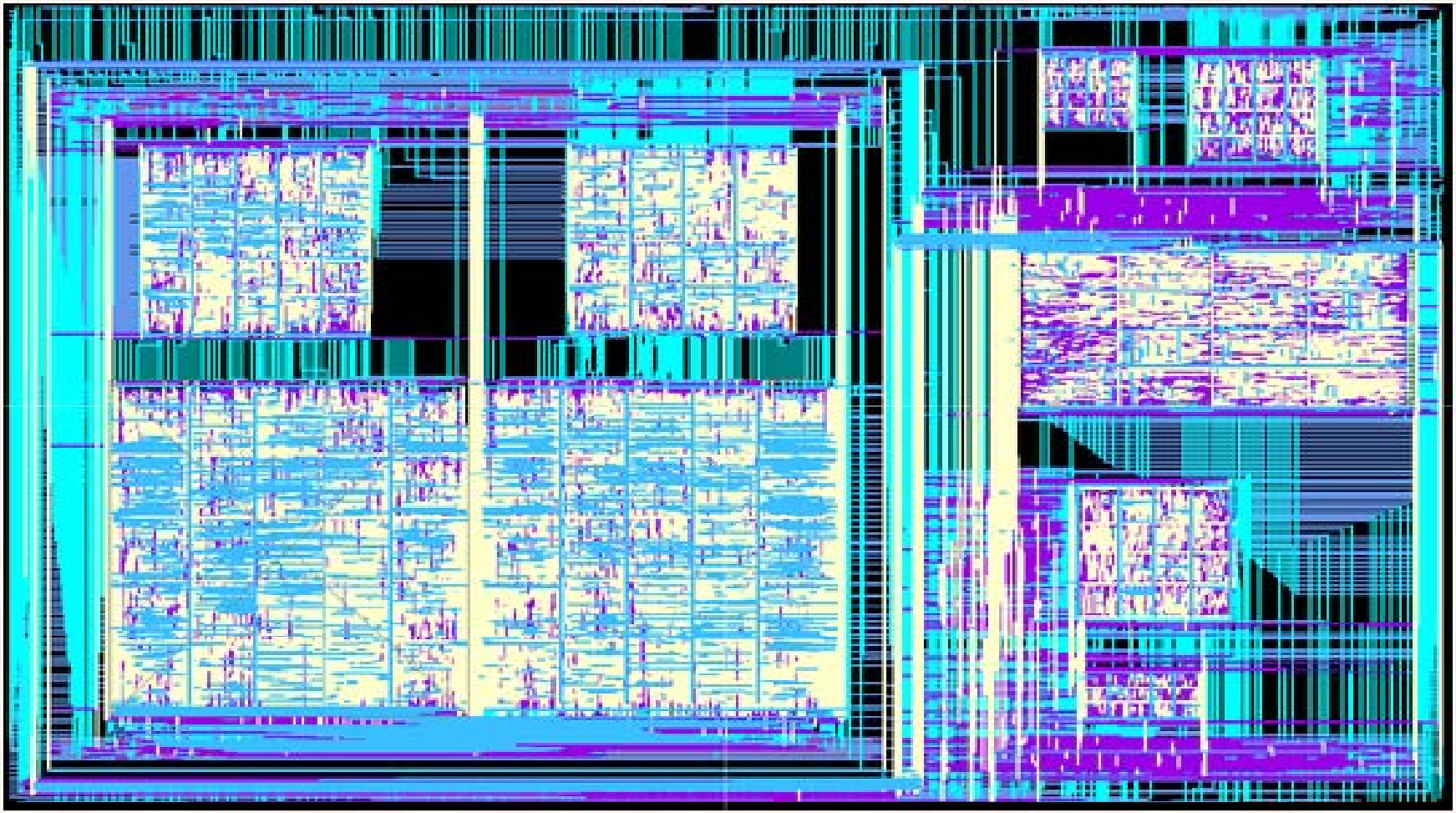


- The visible architecture has 3 stage pipeline and the invisible architecture has 2 stage pipeline.

The Proposed Datapath Architecture: Dual Voltage and Frequency



The Prototype Chip : Layout



NOTE: Standard cell design style adopted. Low-power cells are created based on Virginia Tech: TSMC 0.25µm library.

The Prototype Chip: Statistics

Technology: TSMC 0.25µm

Total Area : 16.2 sq-mm

Dual Clocks: 284MHz and 71MHz

Dual Voltages: 2.5V and 1.5V

No. of Transistors: 1.4million

Power Consumption: 0.3mW

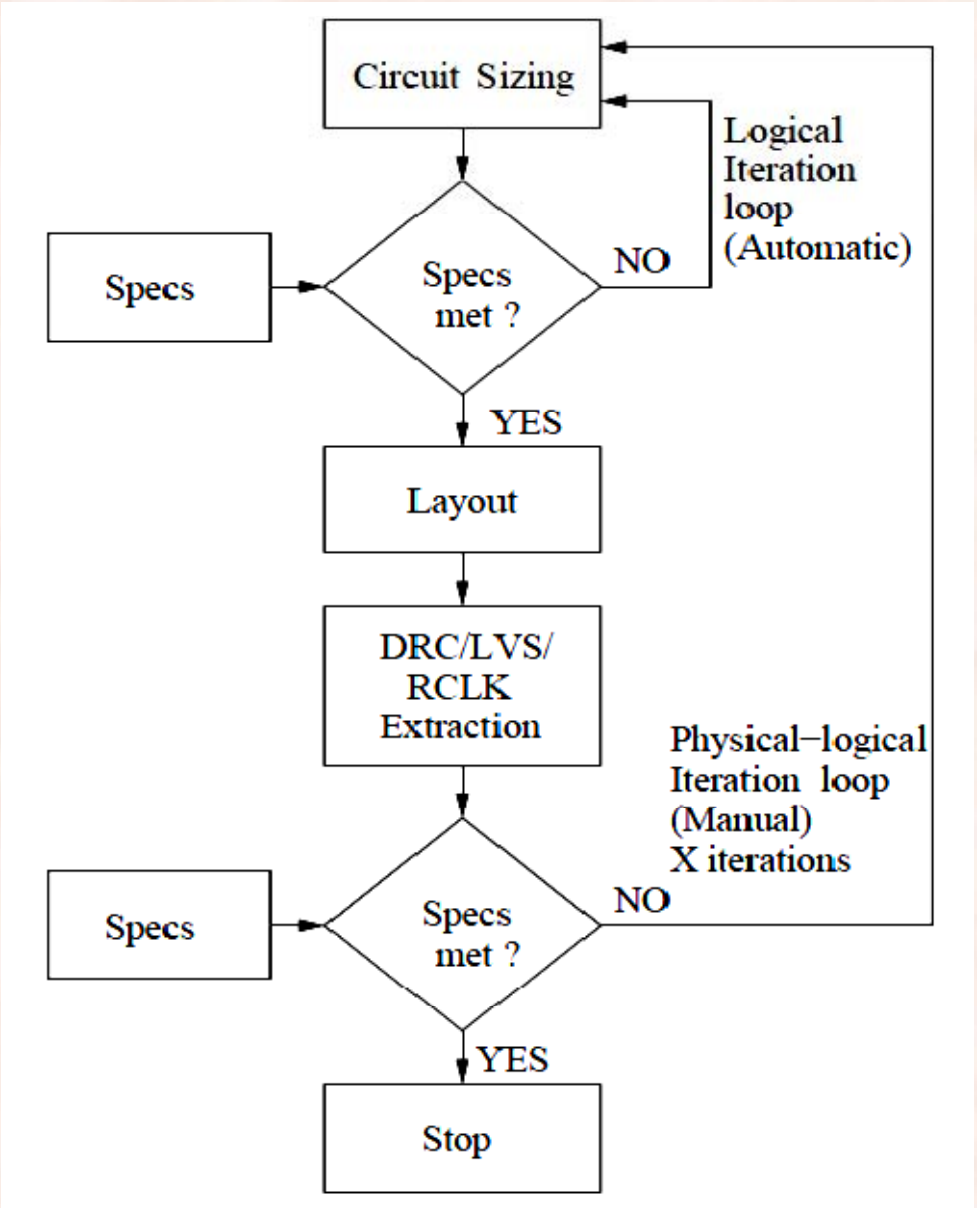
NOTE: One of the lowest power consuming watermarking chip available at present.

Variability-Tolerant Voltage Controlled Oscillator (VCO)

Refer:

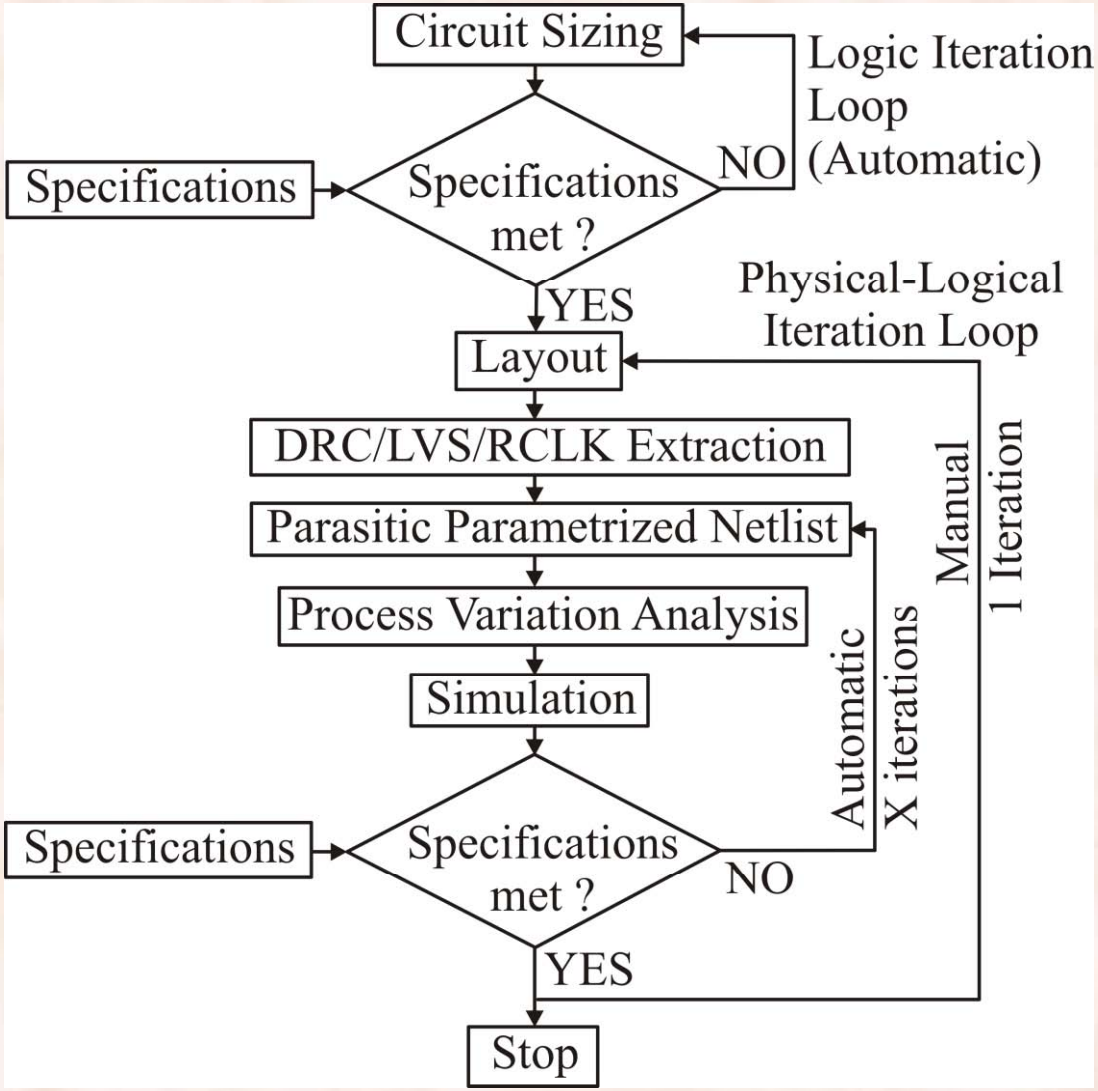
- D. Ghai, **S. P. Mohanty**, and E. Kougianos, "Design of Parasitic and Process Variation Aware RF Circuits: A Nano-CMOS VCO Case Study", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 17, No. 9, September 2009, pp. 1339-1342.

VCO Design Using Standard Flow



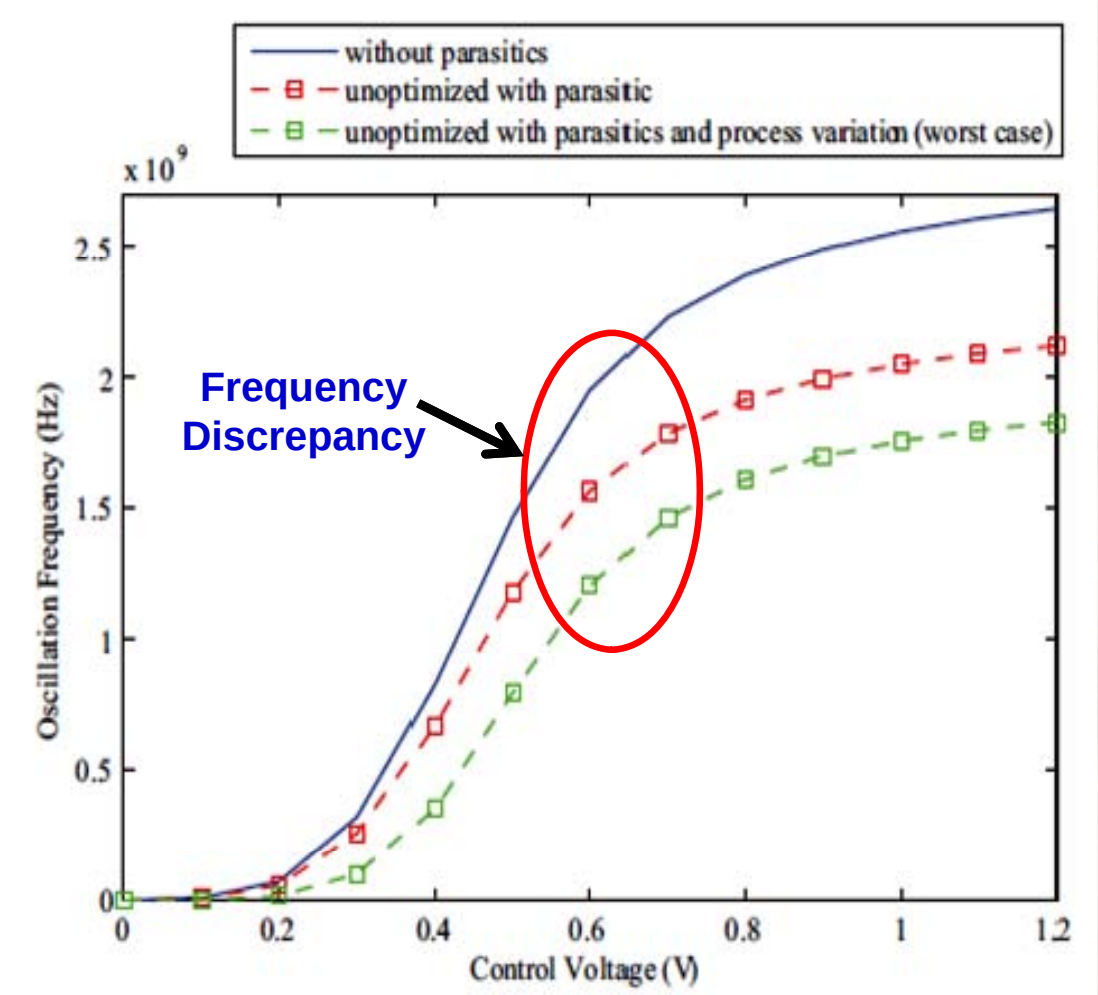
- Standard RFIC design flow requires multiple (X) manual iterations on the back-end layout to achieve parasitic closure between front-end circuit and back-end layout.

Variability-Tolerant VCO Design Using Single Iteration Approach



- The proposed approach performs the multiple (X) iterations automatically on a parasitic parameterized netlist derived from layout.
- The manual iteration is reduced to 1.
- For a process variation tolernat design, process variation analysis and optimization is introduced in the design flow.

VCO Design: Impact of Parasitics and Procession Variations



- Uppermost curve shows the characteristics for logical design; f_c = *2GHz*.
- Middle curve is for layout with parasitic extracted; Discrepancy = 25%.
- Bottom curve is for parasitic extracted layout with *worst case* process variation; f_c = *1.13GHz* and Discrepancy = 43.5%.

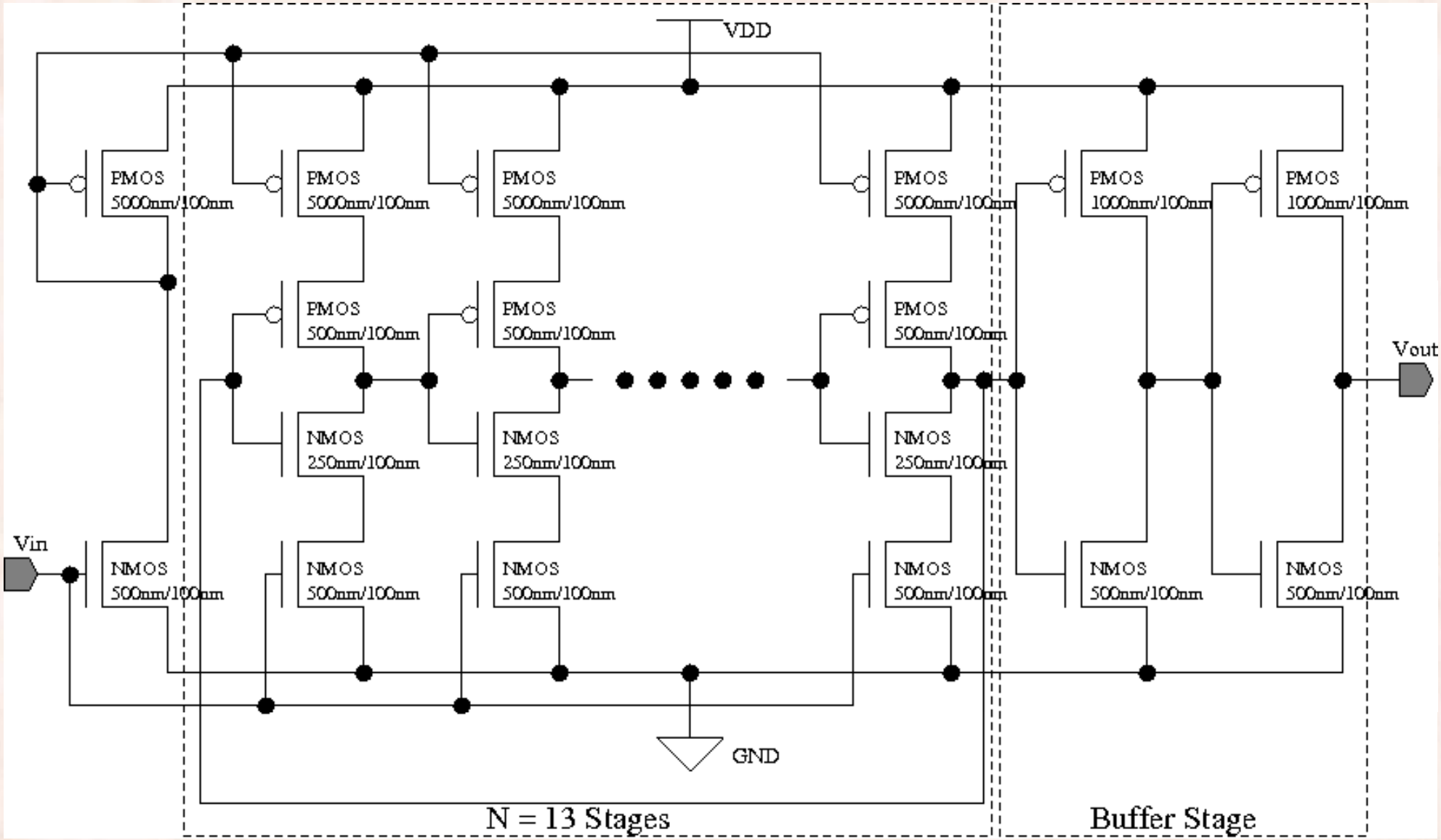
Variability-Tolerant VCO Design: Optimization Algorithm

Input: Parasitic parameterized netlist, Objective set *F*, Stopping criteria *S*, design variable set *D*, Lower design constraint C_{lower}, Upper design constraint C_{upper}.

Output: Optimized objective set $F_{optimal}$, Optimal design variable set $D_{optimal}$ for $S = \pm \sigma$, {where $2\% \leq \sigma \leq 5\%$}.

1. Perform initial simulation to obtain feasible values of design variables for the given specifications.
2. *while* ($C_{lower} < D < C_{upper}$) do
    1. Generate new set of design variables $D' = D \pm \delta D$.
    2. Compute objective set *F*.
    3. if ($S == \pm \sigma$) then return $D_{optimal} = D'$.
    4. end if
3. end while
4. Using design variable set $D_{optimal}$, construct final physical design.
5. Record objective set $F_{optimal}$.

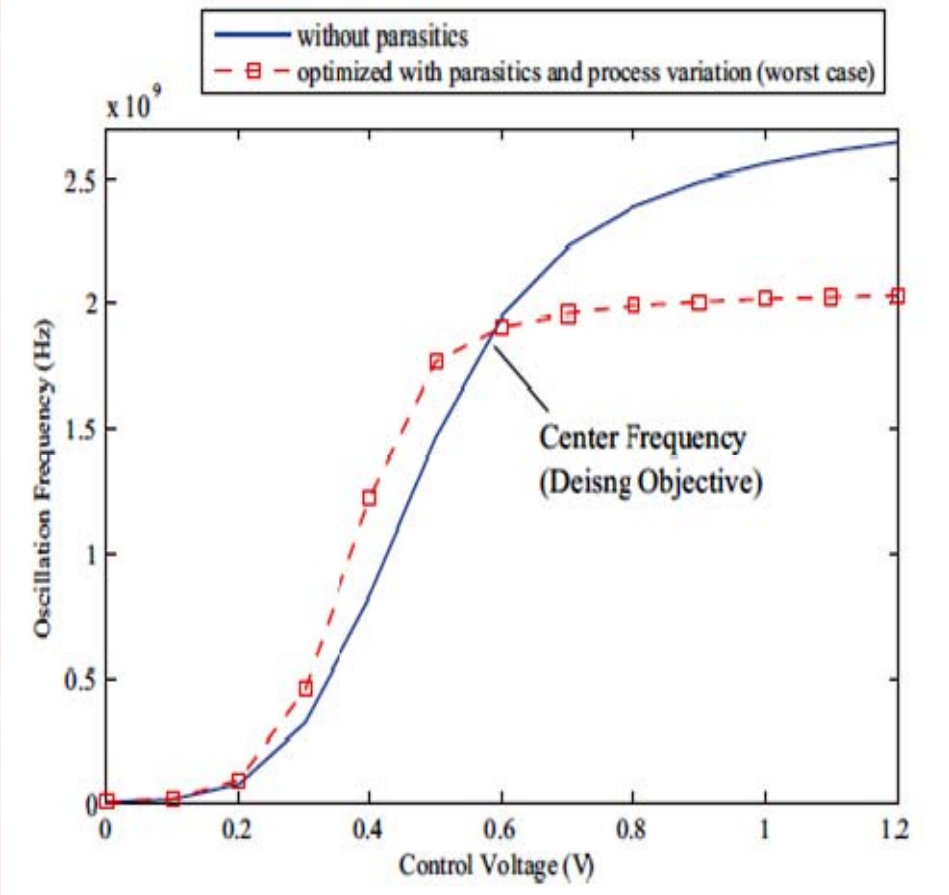
VCO Design: With Baseline Sizes

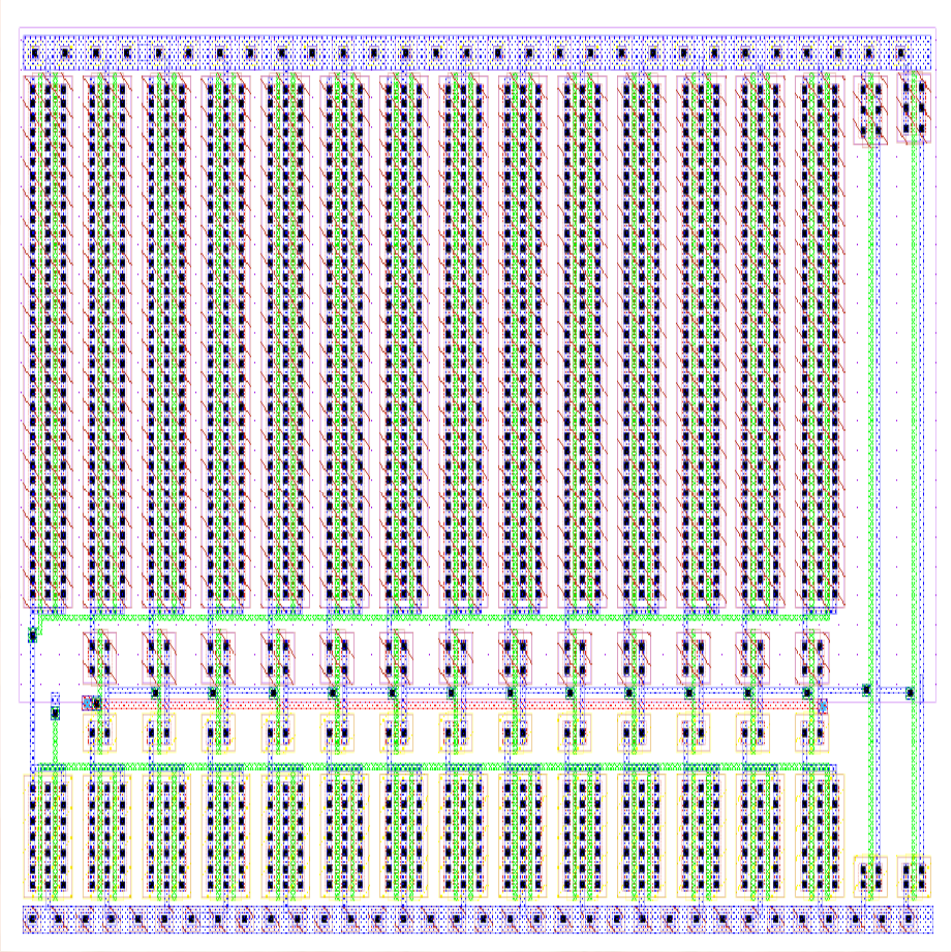


Variability-Tolerant VCO Design: Final Sizes Obtained

Parameter	C_{lower}	C_{upper}	$D_{optimal}$
Wn	200 nm	500 nm	415 nm
Wp	400 nm	1µm	665 nm
Wncs	1 µm	5 µm	4 µm
Wpcs	5 µm	20 µm	19 µm
L	100 nm	110 nm	100 nm

Variability-Tolerant VCO





Related Research

Existing Watermarking Chips

Work	Type	Object	Domain	Tech.	Power
Tsai and Lu 2001	Invisible Robust	Video	DCT	0.35µ	62.8mW
Mathai 2003	Invisible Robust	Video	Wavelet	0.18µ	160mW
Mohanty 2003	Robust Fragile	Image	Spatial	0.35µ	2.05mW
Garimella 2004	Invisible Fragile	Image	Spatial	0.13µ	9.19mW
This Chip	**Visible Invisible**	**Image**	**DCT**	**0.25µ**	**0.3mW**

Variability-Tolerant Nanoscale CMOS Circuit Design

- **Philipp-2007:** Mismatch is analyzed in a pixel.
- **Kim-2006:** A current-controlled oscillator is subjected to process variations.
- **Charan-2008:** A PVT-tolerant humidity sensor.
- **Yang-2008:** A PVT-tolerant PLL.
- **Miyashita-2005:** A PVT-tolerant amplitude controller.
- **Lin-2004:** A PVT-tolerant low-jitter digital PLL.

Sensors With Watermarking

- **Nelson, Jullien, and Yadid-Pecht, ISCAS-2005:** A CMOS APS imager with a pseudorandom generator for invisible watermarking.
- **Shoshan, Fish, Jullien, and Yadid-Pecht, ICECS-2008:** A DCT domain watermarking hardware integrated in the peripheral image processing circuitry of a CMOS image sensor.
- **Lukac and Plataniotis, EL-2006:** The concept of a digital camera that inserts visible watermarks during the colour filter array (CFA).

Summary and Conclusions

Conclusions

- Hardware assisted DRM has several advantages over software only.
- A low-cost, low-power SDC is for real-time DRM.
- A low-power watermarking chip is designed that consumes 0.3mW power.
- SDC to be realized as an AMS-SoC will involve security, power, and performance tradeoffs.
- For nano-CMOS AMS-SoC realization of SDC, the process variations effects need to be considered for its robust design.
- A process variation aware methodology for performance optimization of a VCO circuit components is presented.

Thank You

For more information:

http://www.cse.unt.edu/~smohanty

Email: saraju.mohanty@unt.edu