Masking and Dual-rail Logic Don't Add Up

Patrick Schaumont
schaum@vt.edu

Secure Embedded Systems Group
ECE Department

Kris Tiri
kris.tiri@intel.com

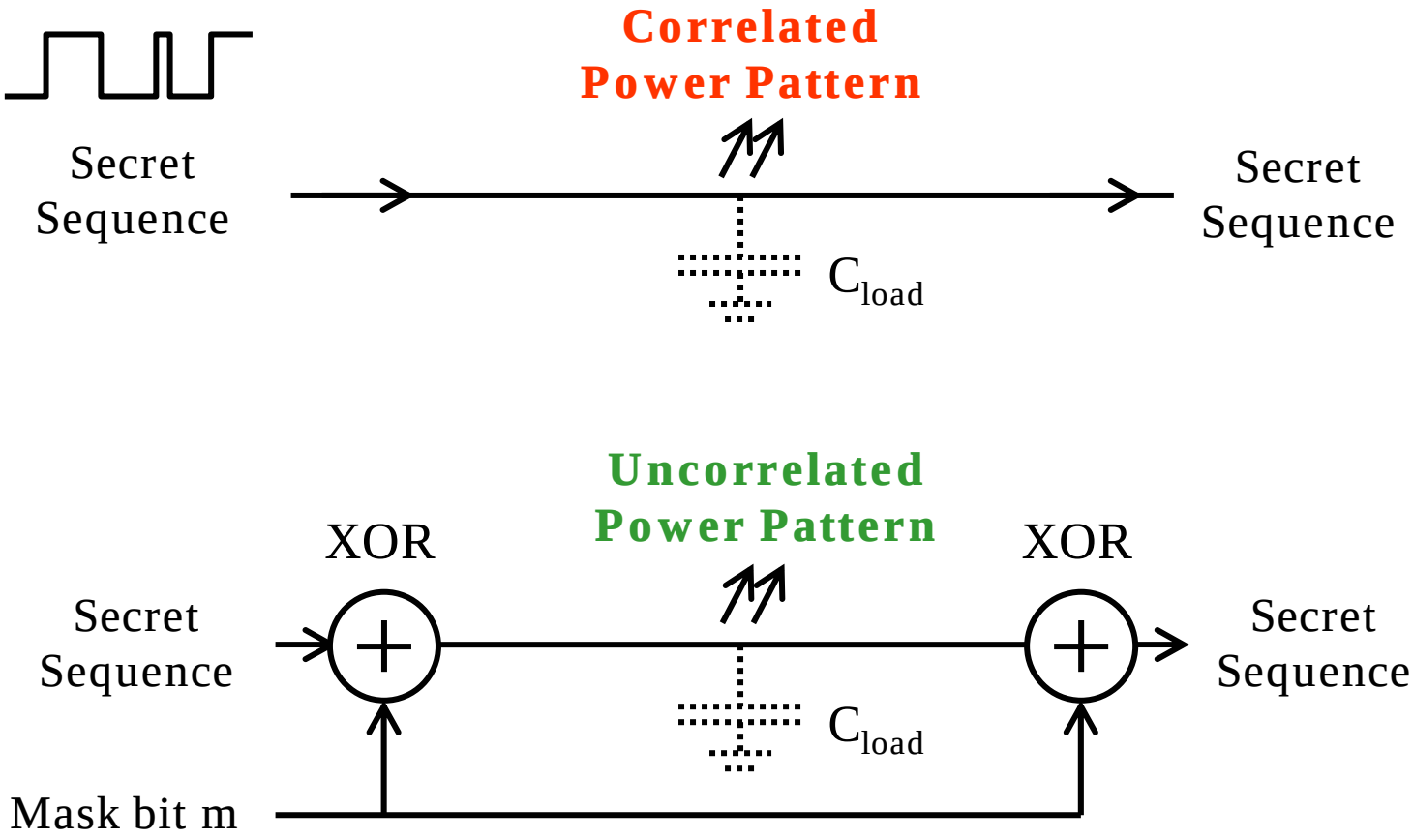
Digital Enterprise Group
Intel Corporation

Our Contributions

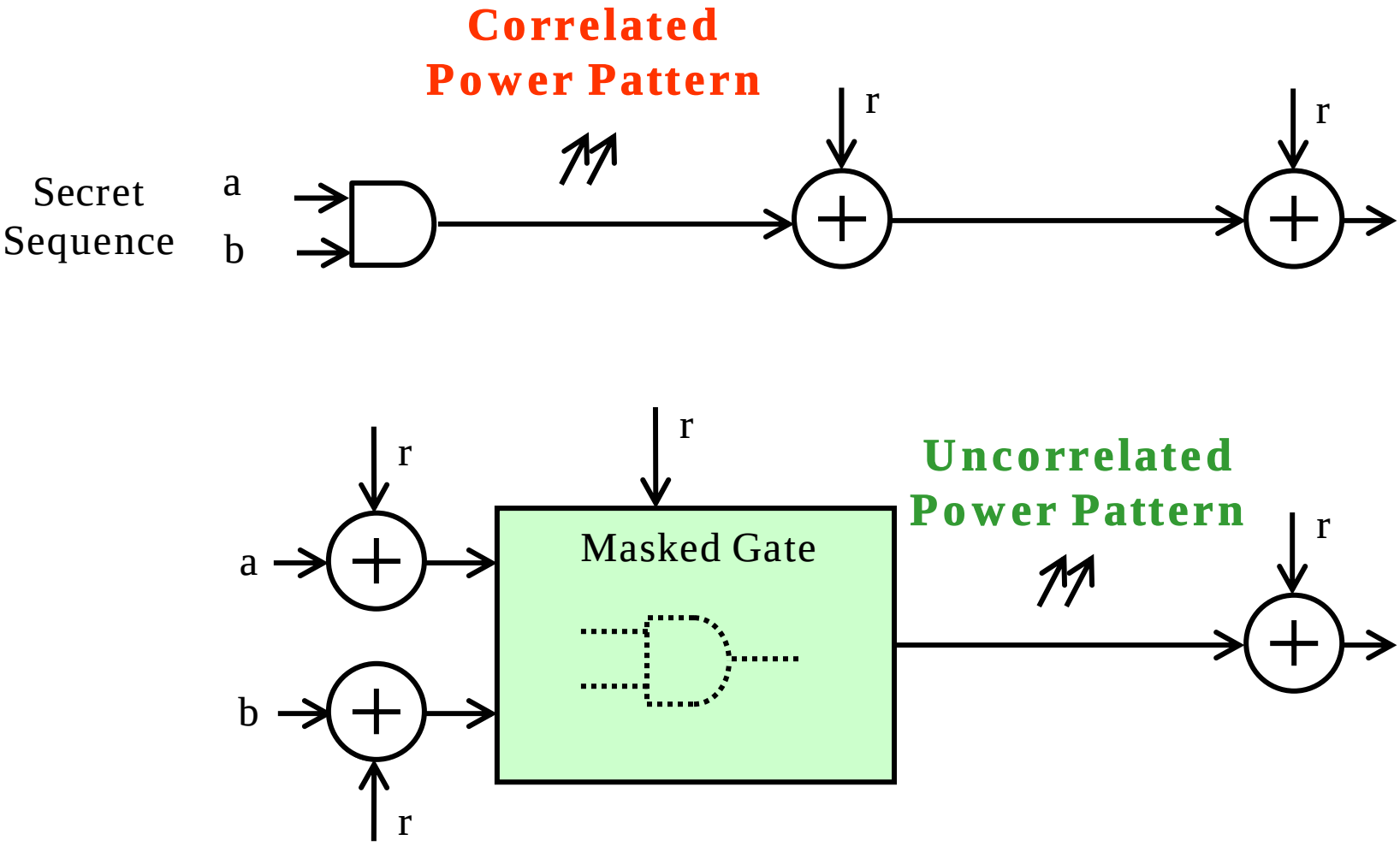
1. Using a simple *statistical* technique, we can break single-bit masked secure logic styles including
    1. RSL [Suzuki 2004]
    2. MDPL [Popp 2005]
    3. DRSL [Chen 2006]

2. Side channel resistance obtained by combining masking and dual-rail logic is not routing-independent

Preliminaries: Masked Hardware Signals

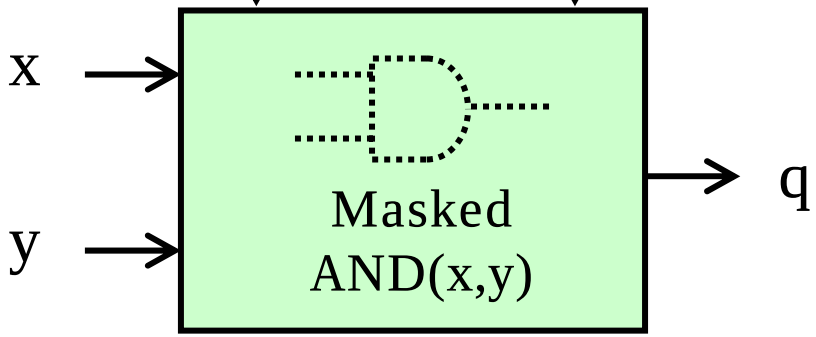


Preliminaries: Masked Logic



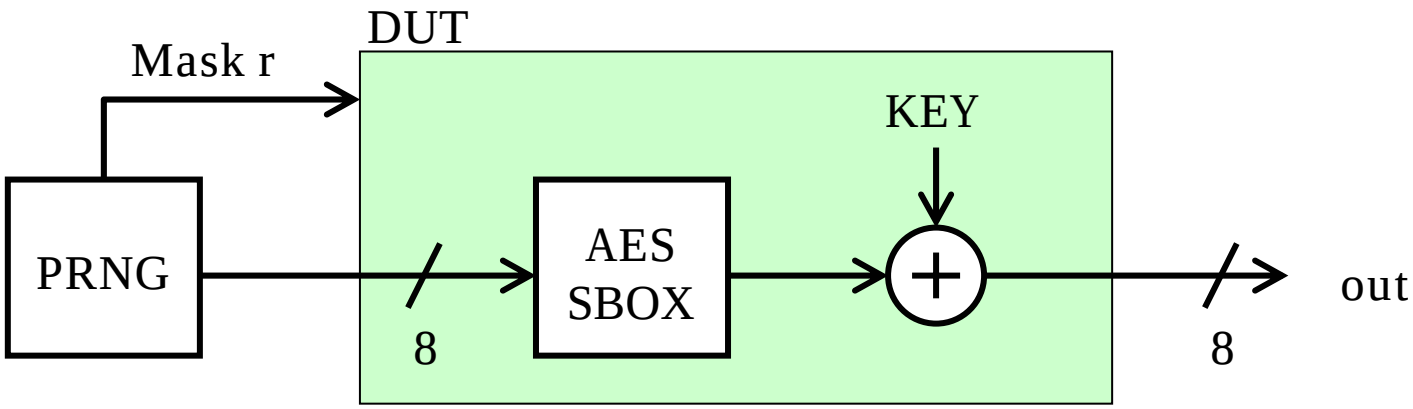
Preliminaries: Random Switching Logic

Precharge Signal e r [Suzuki 2004]



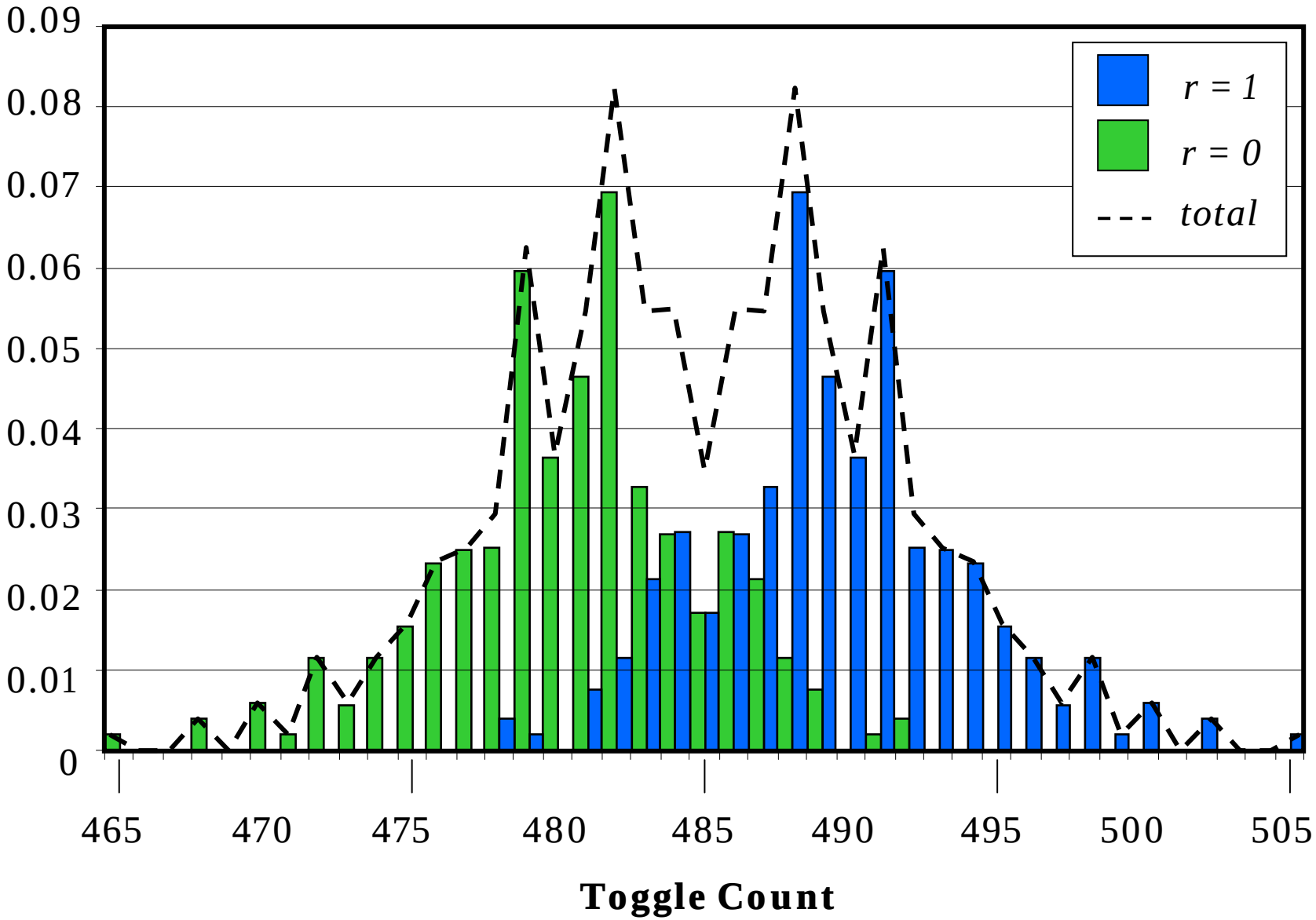
e	r	q	
0	X	0	
1	0	AND(x , y)	= **AND(a, b) = q**
1	1	OR(x , y)	= **OR($\overline{a}$, $\overline{b}$) = $\overline{q}$**

Our Experiment: Sbox in RSL



- Gate-level DUT Implementation - **970 RSL gates**
- Cycle-based simulation, abstracting all timing effects
- Power Model = toggle counting on DUT gate outputs

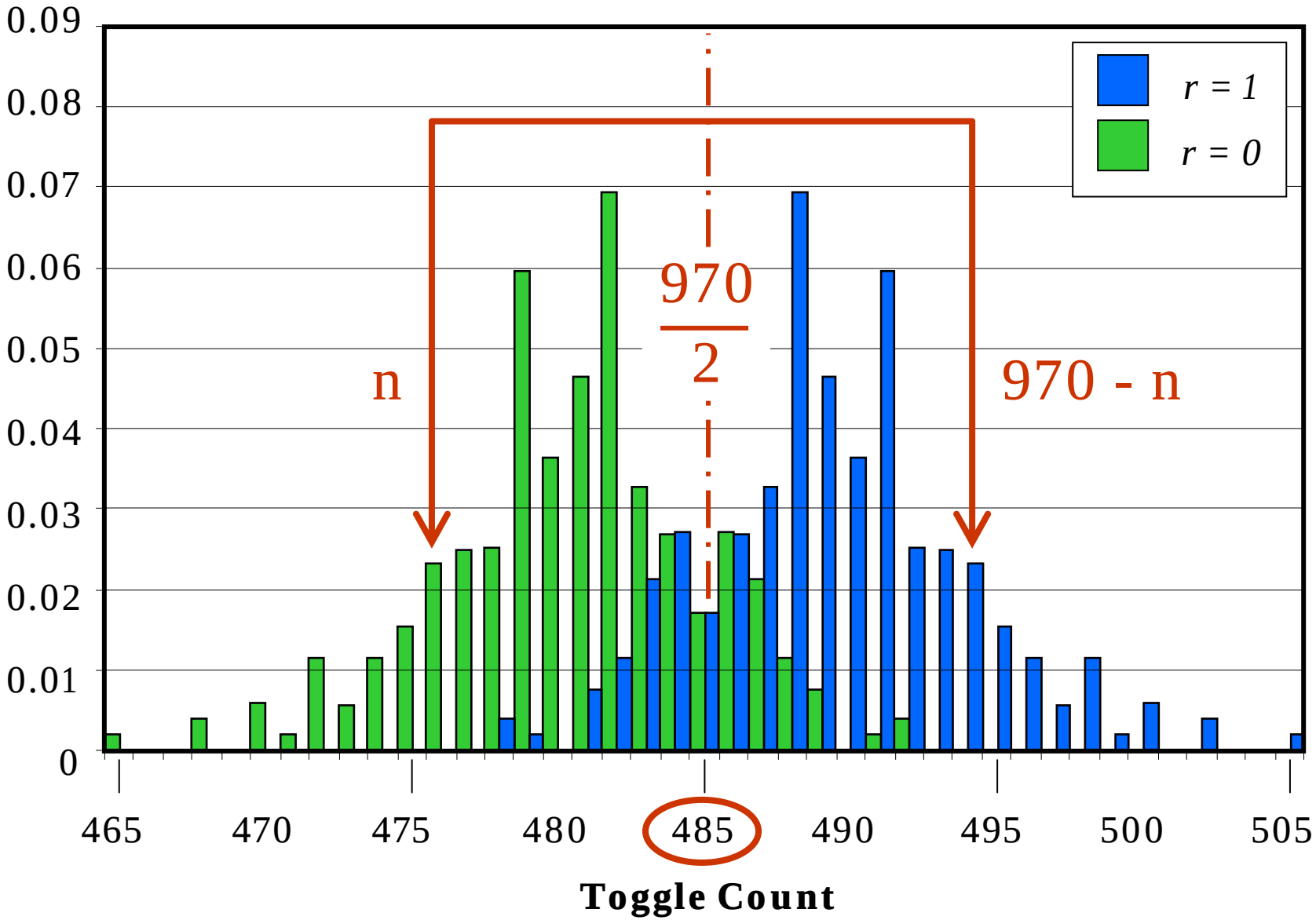
Power Probability Distribution for SBOX



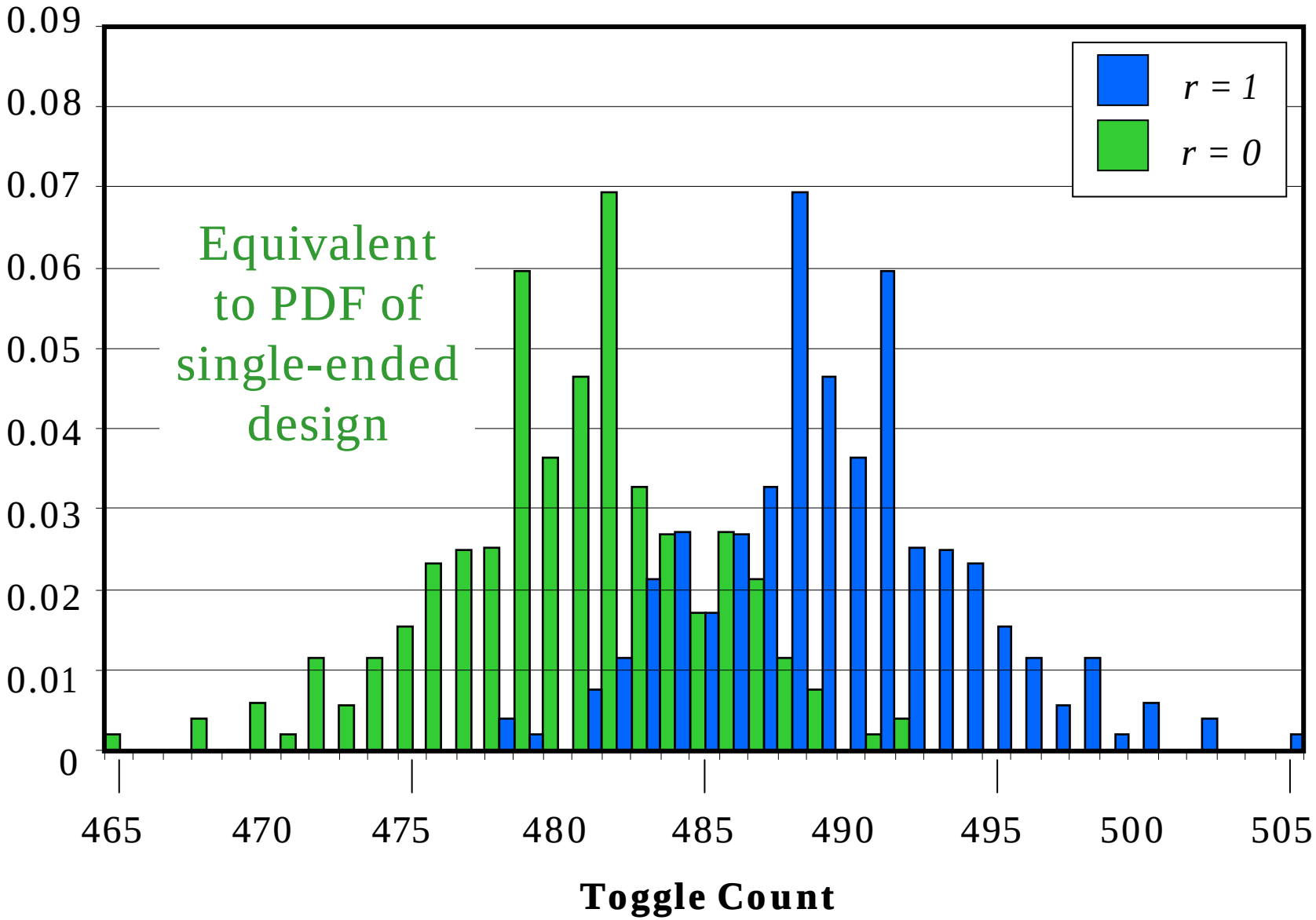
Explaining the Cause of Symmetry

unmasked value	masked value	
	r = 0	**r = 1**
	prechg eval	prechg eval
Transitions in single RSL gate		
'0'		1 toggle
'1'	1 toggle	
Transitions in 970 RSL gates		
970 - n '0'		(970 -n) toggle
n '1'	n toggle	

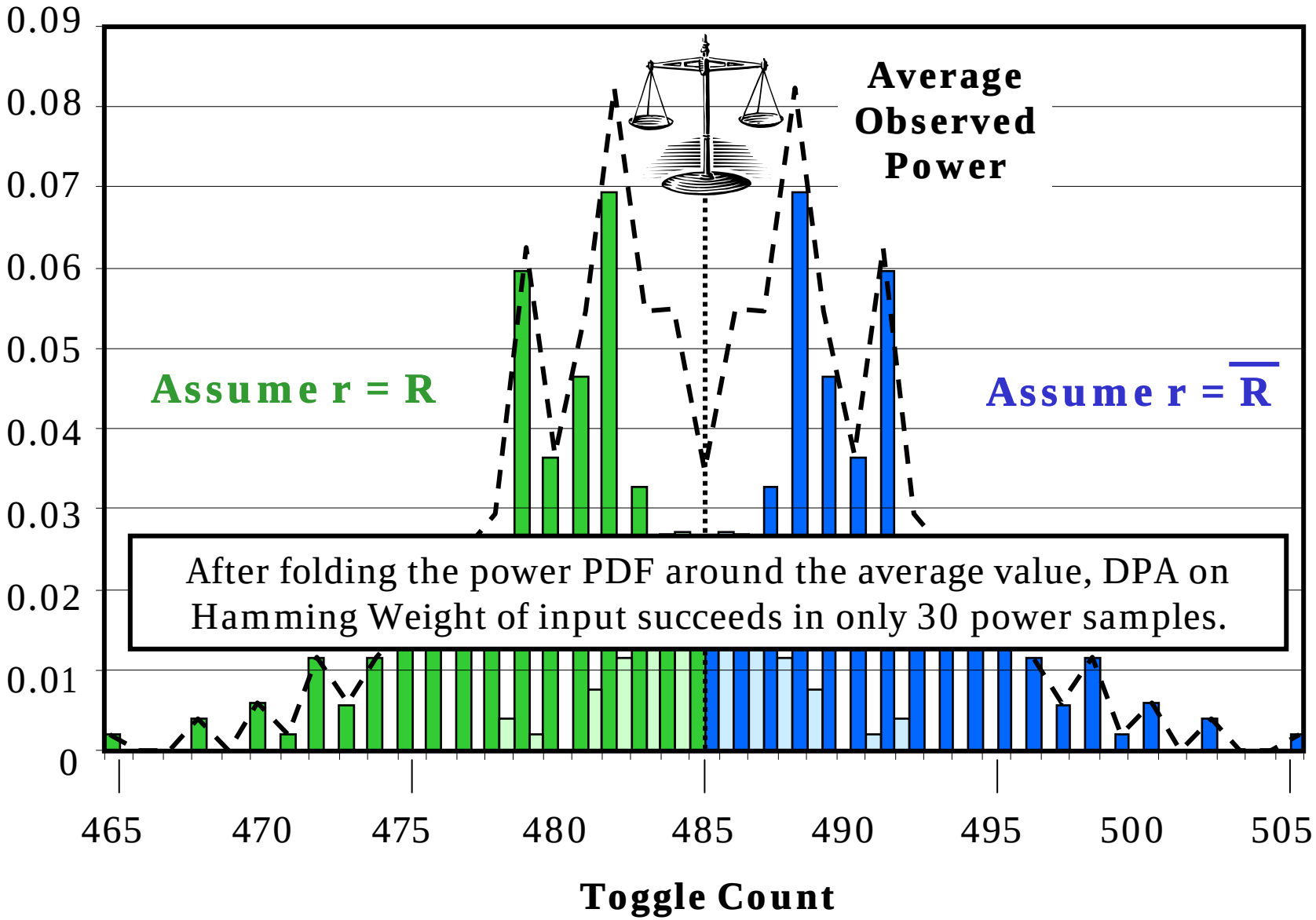
Power Probability Distribution for SBOX



An Attack using the Power PDF



An Attack using the Power PDF



Preliminaries: Masking and DRP

- **D**ual-**R**ail **P**recharge Logic
  encodes each value as a complementary signal pair
- In combination with masking: MDPL [Popp 2005]

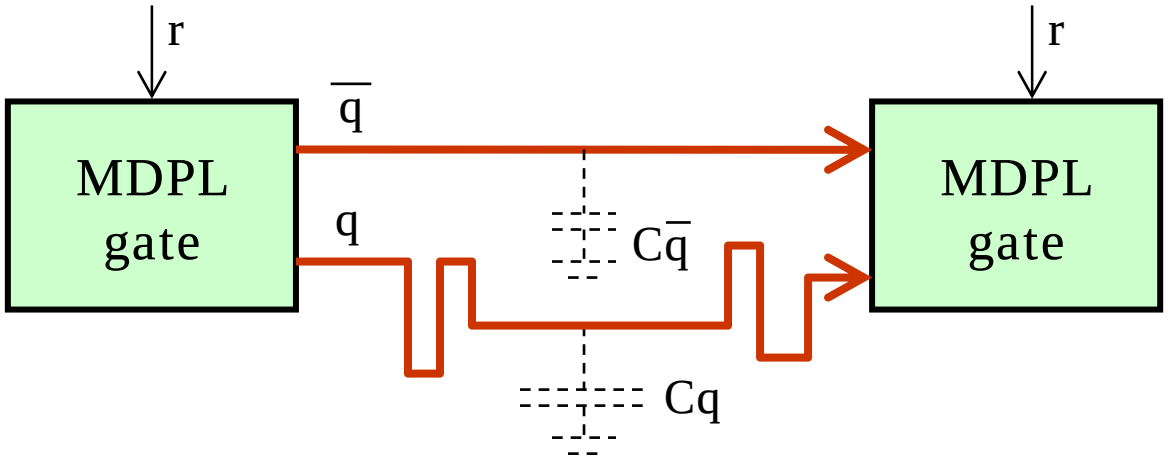
unmasked value	masked value	
	r = 0	**r = 1**
	prechg eval	prechg eval
Transitions in single MDPL gate		
'0'	$\overline{q}$ 0 → 1 q 0 → 0	$\overline{q}$ 0 → 0 q 0 → 1
'1'	$\overline{q}$ 0 → 0 q 0 → 1	$\overline{q}$ 0 → 1 q 0 → 0

Preliminaries: Masking and DRP

- **D**ual-**R**ail **P**recharge Logic
  encodes each value as a complementary signal pair
- In combination with masking: MDPL [Popp 2005]

unmasked value	masked value	
	r = 0	**r = 1**
	prechg eval	prechg eval
Transitions in single MDPL gate		
'0'	$\overline{q}$ toggle	q toggle
'1'	q toggle	$\overline{q}$ toggle

Impact of Routing Imbalances



unmasked value	masked value	
	r = 0	**r = 1**
	prechg eval	prechg eval
Transitions in single MDPL gate		
'0'	Δq toggle	Δq toggle
'1'		

$\Delta q \sim (Cq - C\overline{q})$

Impact of Routing Imbalances

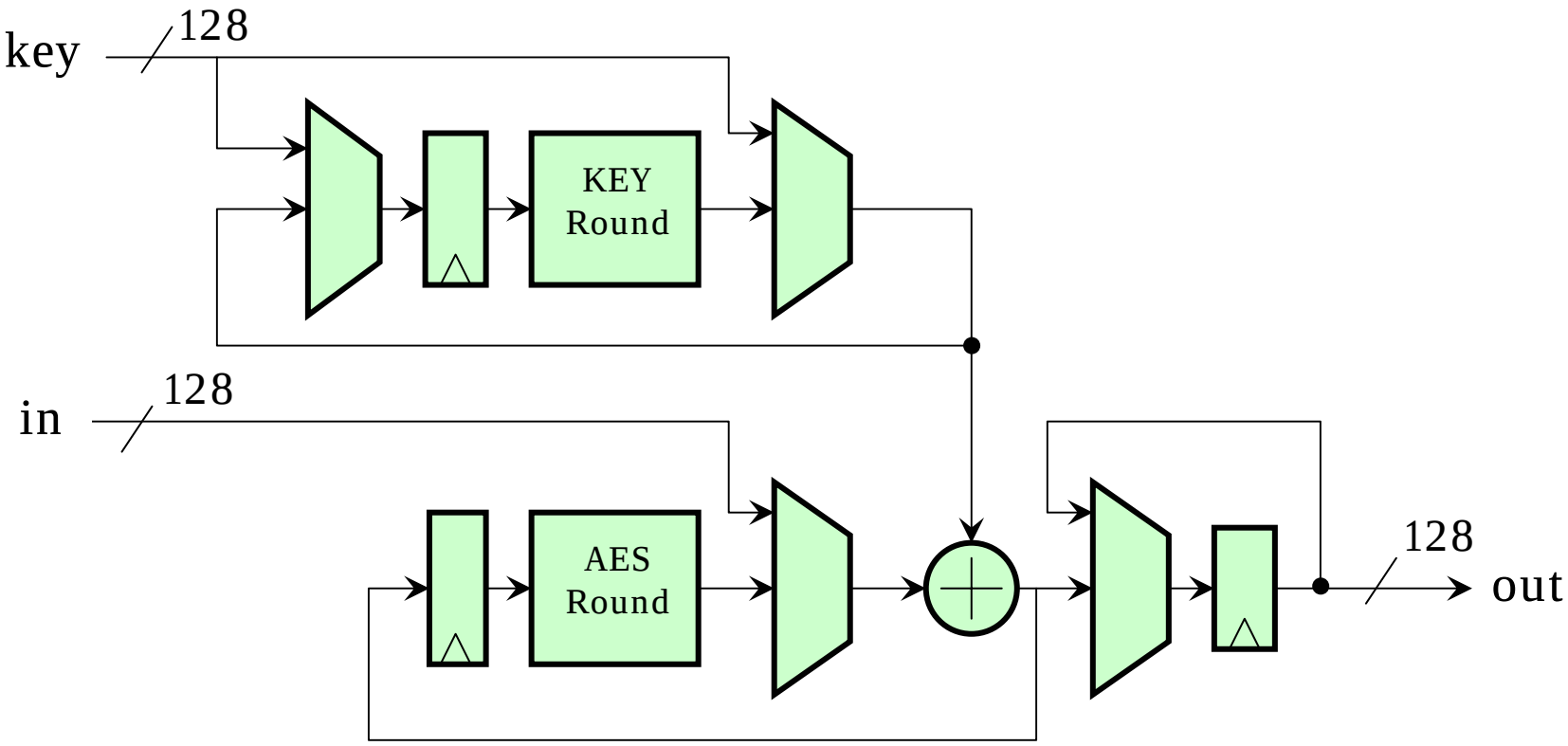
unmasked value	masked value	
	r = 0	**r = 1**
	prechg eval	prechg eval
Transitions in single MDPL gate		
'0'	Δq toggle	Δq toggle
'1'		

$\Delta q \sim (Cq - C\overline{q})$

Impact of Routing Imbalances

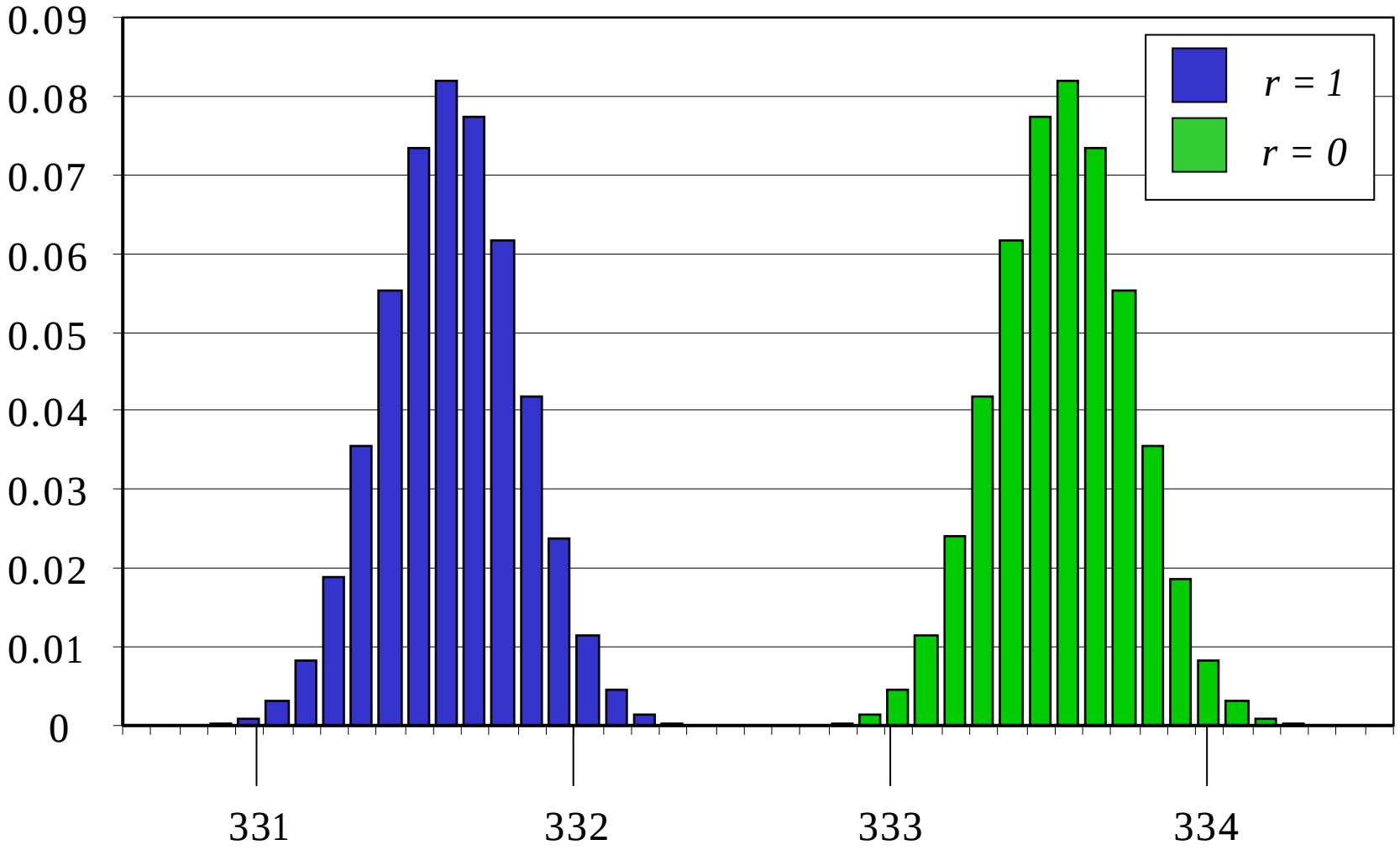
unmasked value	masked value	
	r = 0	**r = 1**
	prechg eval	prechg eval
Transitions in single MDPL gate		
$\Delta q \sim (Cq - C\overline{q})$ '0'	Δq toggle	Δq toggle
$\Delta q \sim (Cq - C\overline{q})$ '1'		
Transitions in 970 MDPL gates		
970 - n '0'	n Δq toggle	970 - n Δq toggle
n '1'		

Evaluation using Actual Layout Data

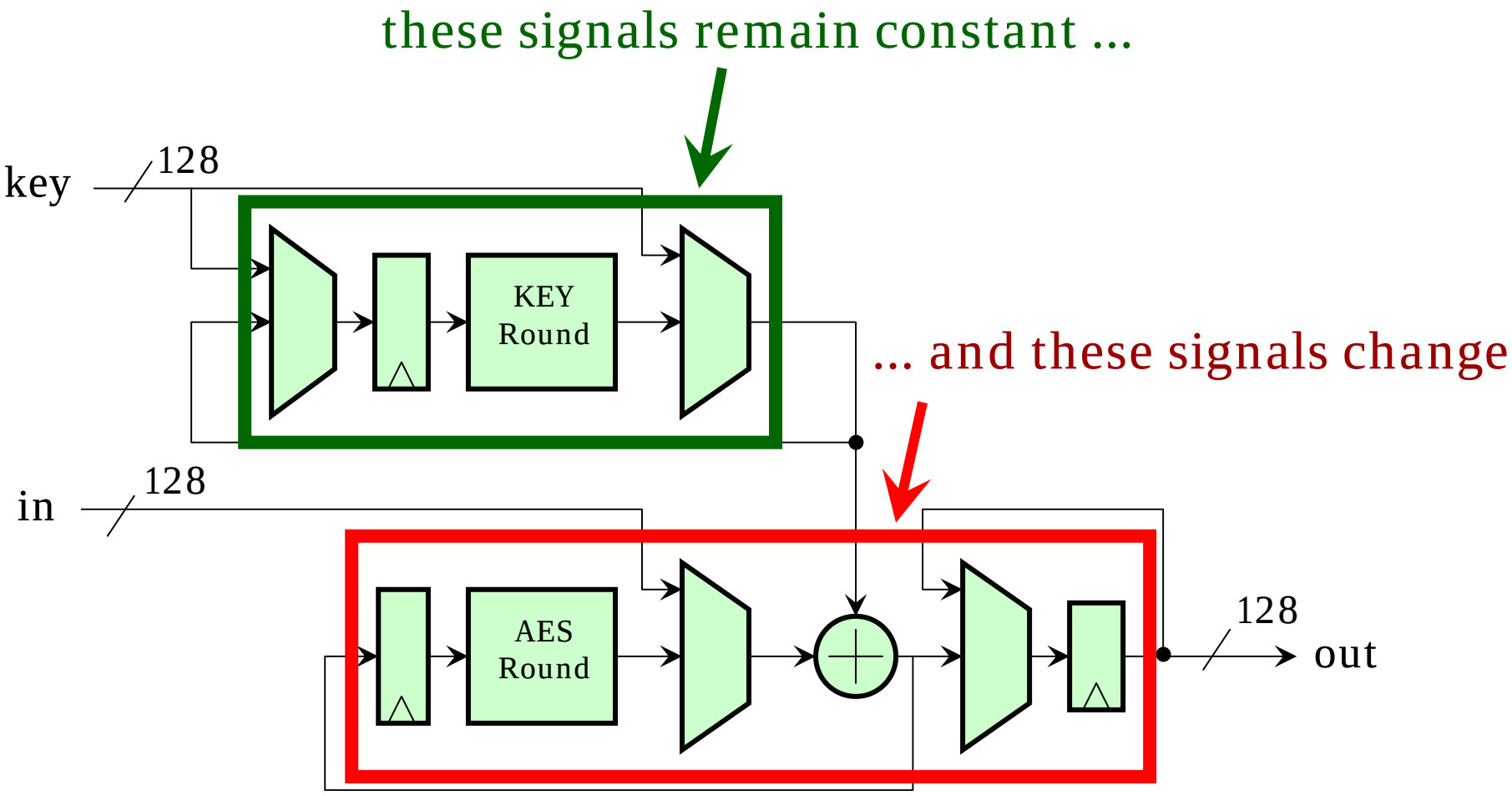


- AES-128 using 16K Dual-rail gates in 0.18 μm CMOS
- Cycle-based simulation using weighted toggle counts
- Weights from layout (no routing constraints)

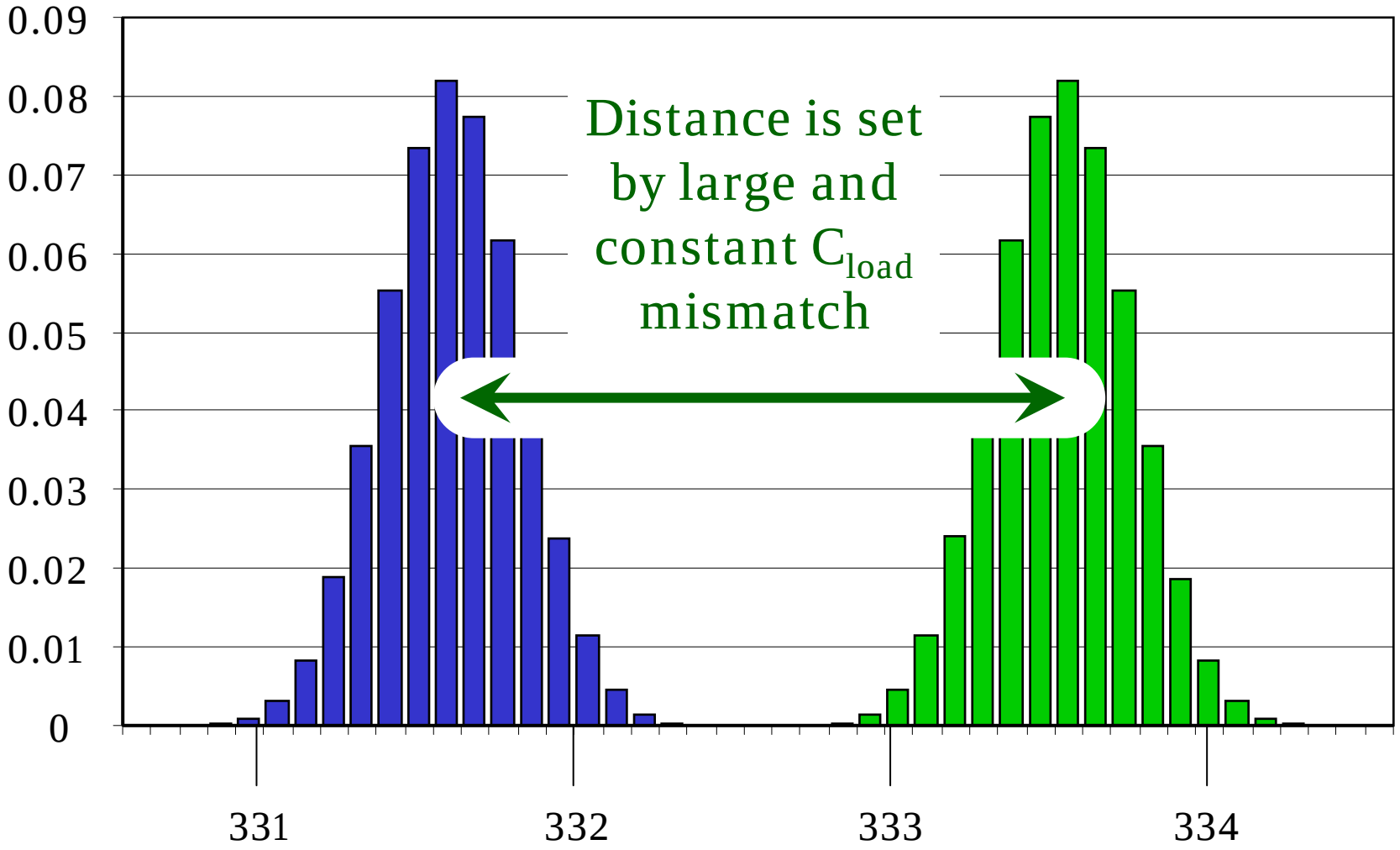
Estimated Power PDF of AES



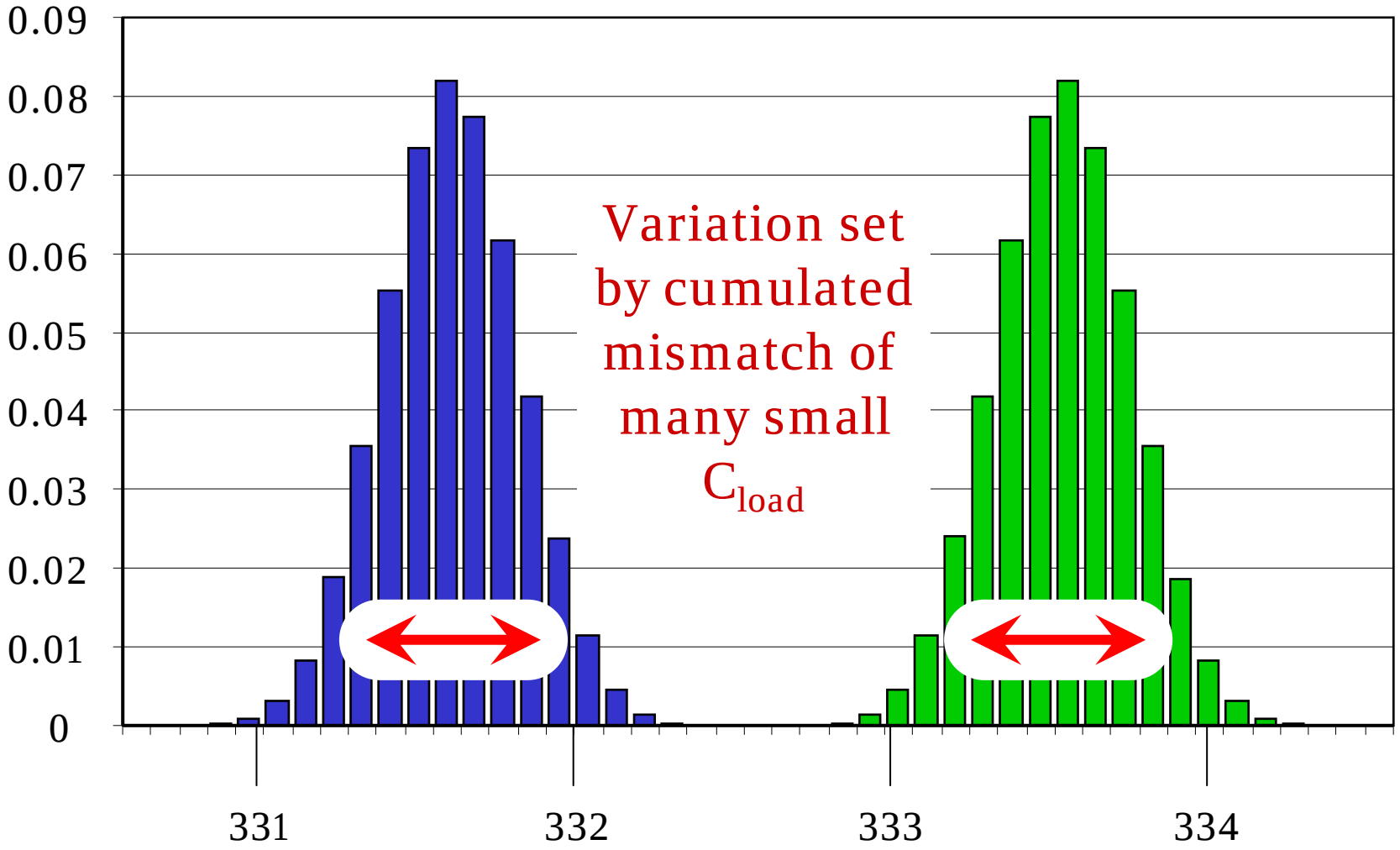
For each power sample in the trace ...



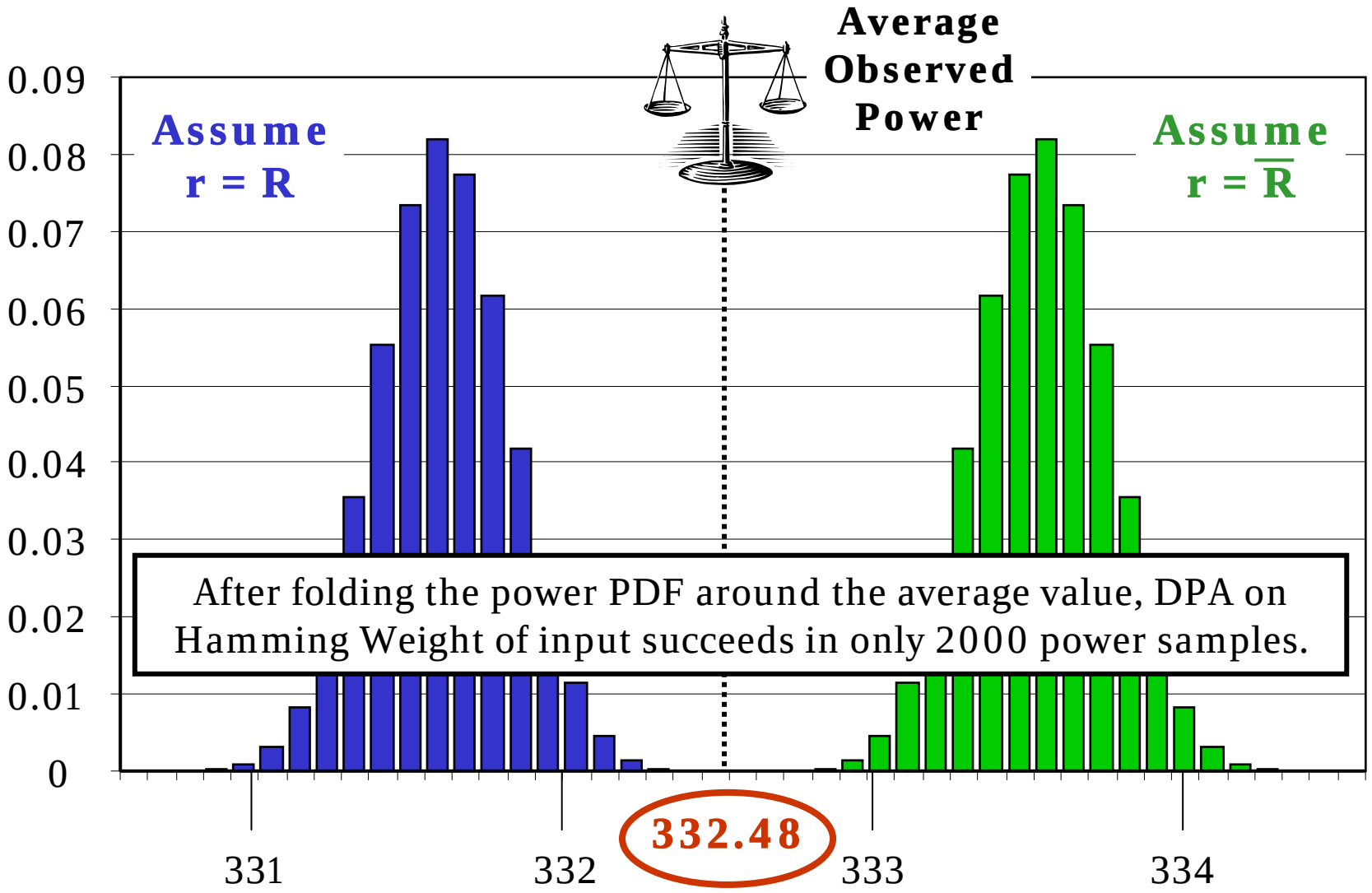
Masking Constant Signals: Binary Effect



Masking Varying Signals: Gaussian Effect



An attack on the AES Power PDF



Related Work

- In software implementations, masking is attacked by combining multiple power samples or by pre-characterization of the implementation
  - [Messerges 2000] Second Order DPA
  - [Peeters 2005] Maximum-likelihood
  - [Oswald 2007] Template Attacks
- For cases where mask and masked signal cannot be observed separately, Waddle proposes the use of squared power samples
  - [Waddle 2004] Zero-Offset DPA
- Our technique demonstrates direct observation of the mask value, without the need for circuit characterization.
  - We have demonstrated this with known masked circuit styles

Conclusions

- Masking and Dual-Rail Logic are not additive for side-channel resistance
- Secure Circuit Styles *cannot* be developed without considering the system-level perspective on security
- Effective countermeasures against our attack will need to address the following question: "How can we add a mask without adding information?"
  - When a mask is used to hide the PDF of a data signal, the masking process itself should not reveal the mask PDF