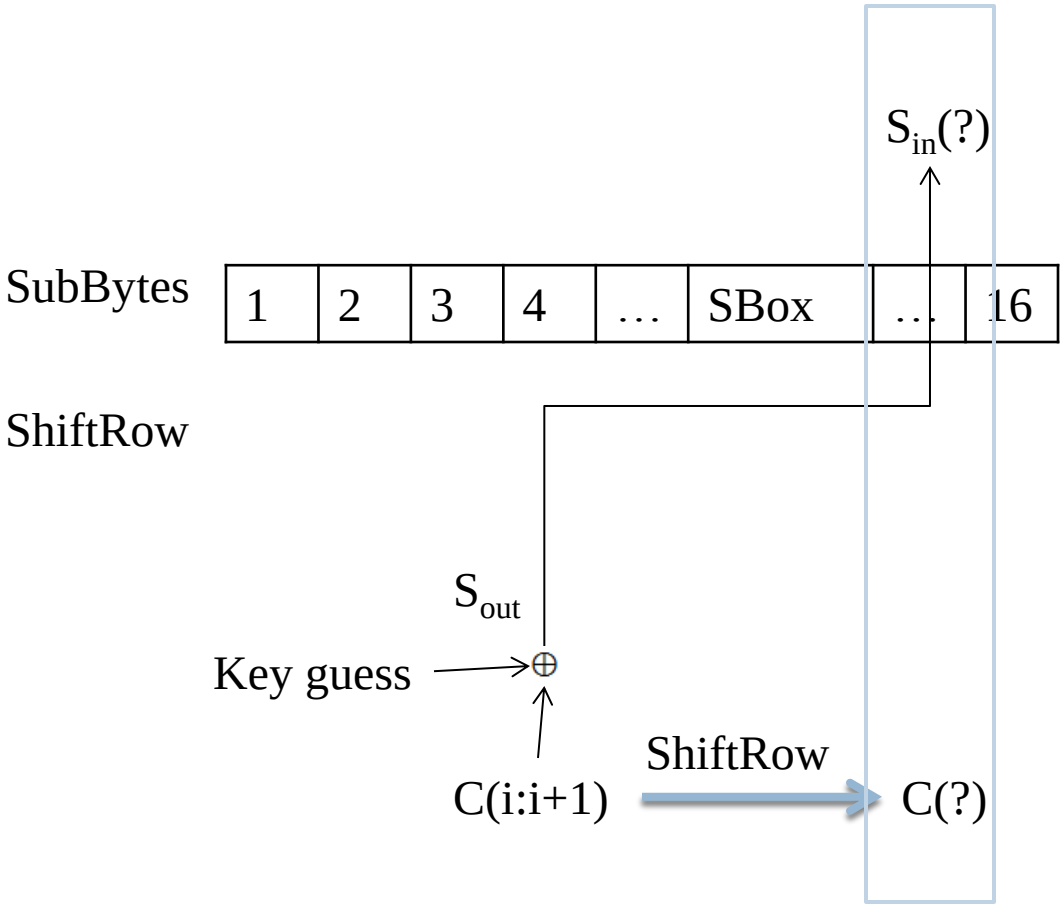
Correlation Power Analysis

Computer Science and Engineering Department
University of Connecticut

Power Analysis

- Simple Power Analysis (SPA)
  - different operations consume different power
- Differential Power Analysis (DPA)
  - different data consume different power
- Correlation Power Analysis (CPA)
  - more advanced than DPA
  - there is correlation between data and power

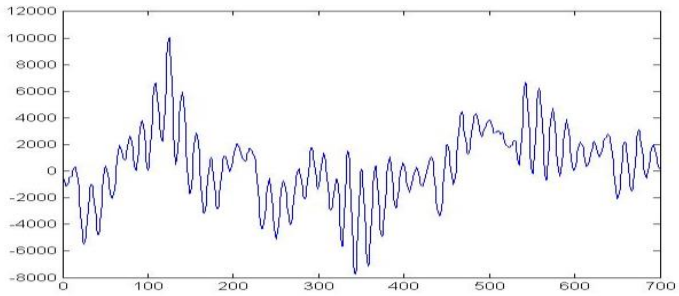
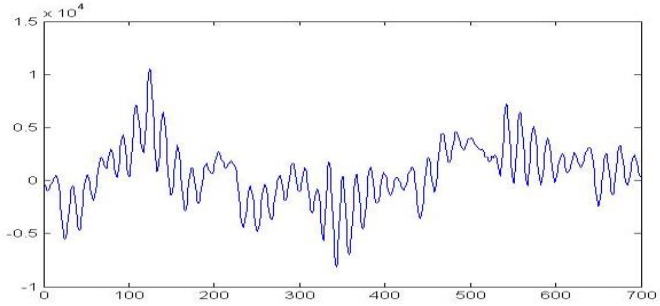
Bit Transitions



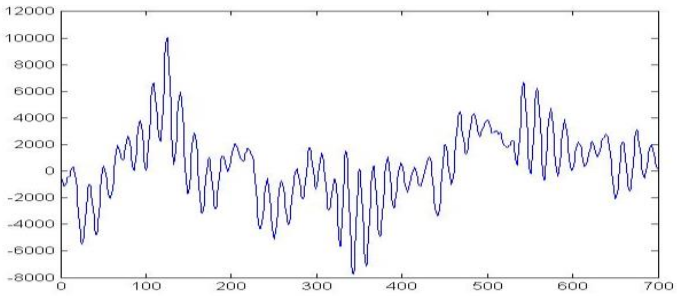
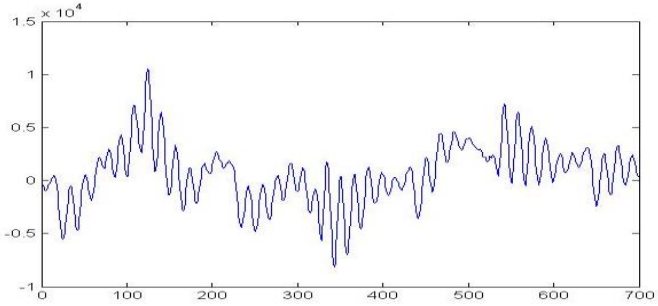
- Sin(?) ⊕ C(?)
  - 0 → no transition
  - 1 → yes transition

- DPA output: 00110110

DPA

Ciphertext	HW	Power trace
`e6a636e30c85f35e 980f3546a04daff7`	0001 1001	
`e9f7a9d7d2387d7e e8c7c5235c354dd`	1001 1110	

CPA

Ciphertext	HW	Power trace
e6a636e30c85f35e980f3546a04daff7	25	
e9f7a9d7d2387d7ee8c7c5235c354dd	158	

CPA

- Hamming weight model: Power dissipation of an operation at a specific time is proportional to the hamming weight of the processing data

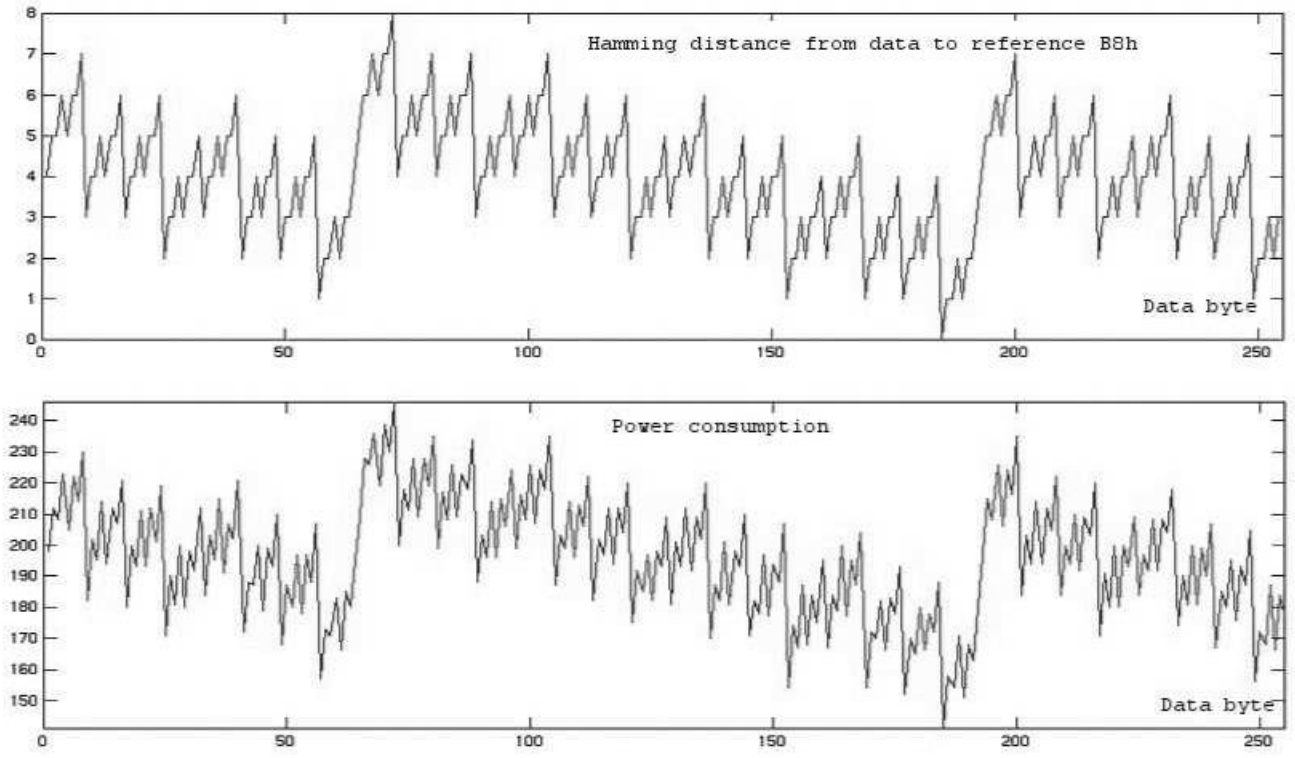
- Correlation coefficient: $W = aH(D) + b$

$$\rho_{W,H} = \frac{Cov(W,H)}{\sigma_W \sigma_H} = \frac{E((W-\mu_W)(H-\mu_H))}{\sqrt{D(W)}\sqrt{D(H)}}$$

- The correlation coefficient indicates how two random variables (Power and Data) matches each other.

Power Trace

- Power dissipation of operation is proportional to the hamming weight of the data.



Brier et al. 2004

Correlation Analysis

- Pearson's coefficient
  - obtained by dividing the covariance of the two variables by the product of their standard deviations.

$$\hat{\rho}_{W\,H}(R) = \frac{N\sum W_i H_{i,R} - \sum W_i \sum H_{i,R}}{\sqrt{N\sum W_i^2 - (\sum W_i)^2}\sqrt{N\sum H_{i,R}^2 - (\sum H_{i,R})^2}}$$

  - W = power traces
  - H = Hamming distance

  - Values between 1 and -1 (perfect linear correlation). No linear dependency produce value of 0.

Correlation Analysis

- Rank correlation coefficient
  - extent to which, as one variable increases, the other variable increases/decreases, without being represented by a linear relationship.
- For data (x, y), if an increase in x is always accompanied by an increase in y, then it is a perfect rank correlation.
  - If (x, y) are not in a straight line, Pearson coefficient may be much lower.

CPA vs. DPA

CPA

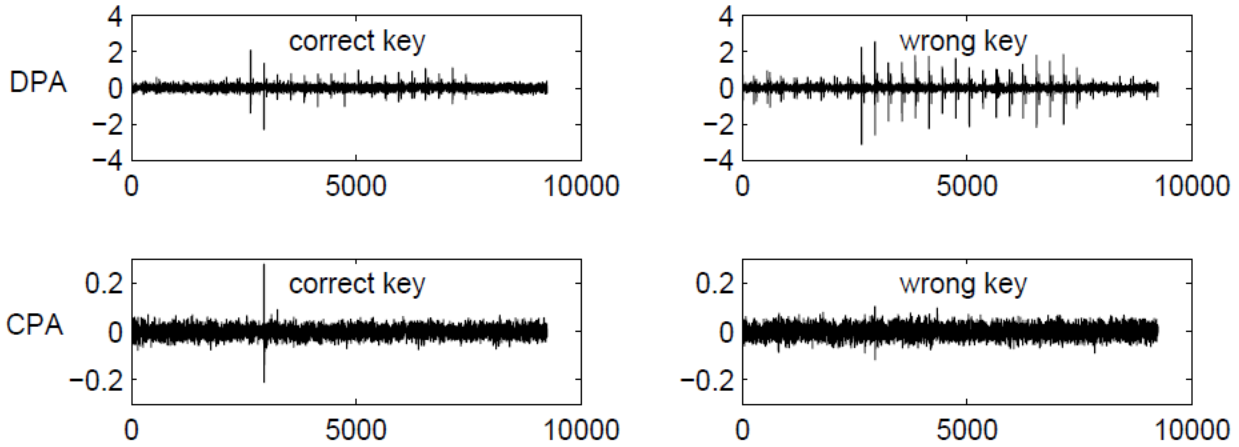
- Attack using relationship between data and power
- Looks at correlation between all key guesses
- Faster, more accurate than DPA

DPA

- Attack using relationship between data and power
- Looks at difference of category averages for all key guess
- Slower and less efficient than CPA

CPA vs. DPA results

- CPA generally have less noise and require less traces to guess the correct key.



Le et al. 2006

Key Guess Correlation

- 1st round: sub-keys are 24, 19, 8, 8, 5, 50, 43, 2

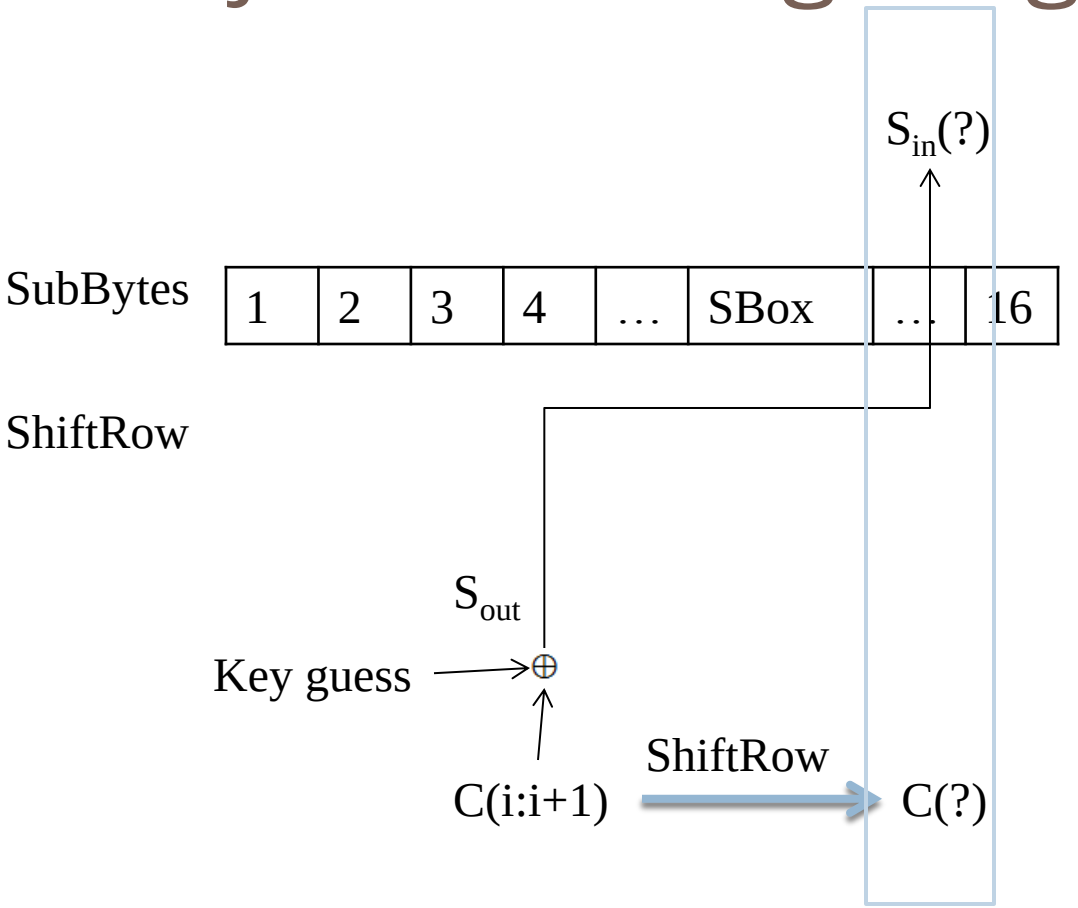
$SBox_1$		$SBox_2$		$SBox_3$		$SBox_4$		$SBox_5$		$SBox_6$		$SBox_7$		$SBox_8$	
K	ρ_{max}	K	ρ_{max}	K	ρ_{max}	K	ρ_{max}	K	ρ_{max}	K	ρ_{max}	K	ρ_{max}	K	ρ_{max}
24	92%	19	90%	8	87%	8	88%	5	91%	50	92%	43	89%	2	89%
48	74%	18	77%	18	69%	44	67%	32	71%	25	71%	42	76%	28	77%
01	74%	57	70%	05	68%	49	67%	25	70%	05	70%	52	70%	61	76%
33	74%	02	70%	22	66%	02	66%	34	69%	54	70%	38	69%	41	72%
15	74%	12	68%	58	66%	29	66%	61	67%	29	69%	0	69%	37	70%
06	74%	13	67%	43	65%	37	65%	37	67%	53	67%	30	68%	15	69%

Brier et al. 2004

Citation

- Eric Brier and Christophe Clavier and Francis Olivier. “Correlation Power Analysis with a Leakage Model.” Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop. 16-29. 2004. http://www.iacr.org/archive/ches2004/31560016/31560016.pdf
- Thanh-Ha Le and Jessy Clédière and Cécile Canovas and Bruno Robisson and Christine Servière and Jean-Louis Lacoume. “A Proposition for Correlation Power Analysis Enhancement.” Cryptographic Hardware and Embedded Systems - CHES 2006. 174-186. http://www.iacr.org/cryptodb/archive/2006/CHES/14/14.pdf
- Fan Zhang, Zhijie Jerry Shi. "Differential and Correlation Power Analysis Attacks on HMAC-Whirlpool.” Eighth International Conference on Information Technology: New Generations, 2011. 359-365. http://www.engr.uconn.edu/~zshi/publications/zhang11dpa_hmac.pdf

Proj 4: Hamming Weight



- Sin(?) ⊕ C(?)
  - 0 → no transition
  - 1 → yes transition

- DPA output: 00110110

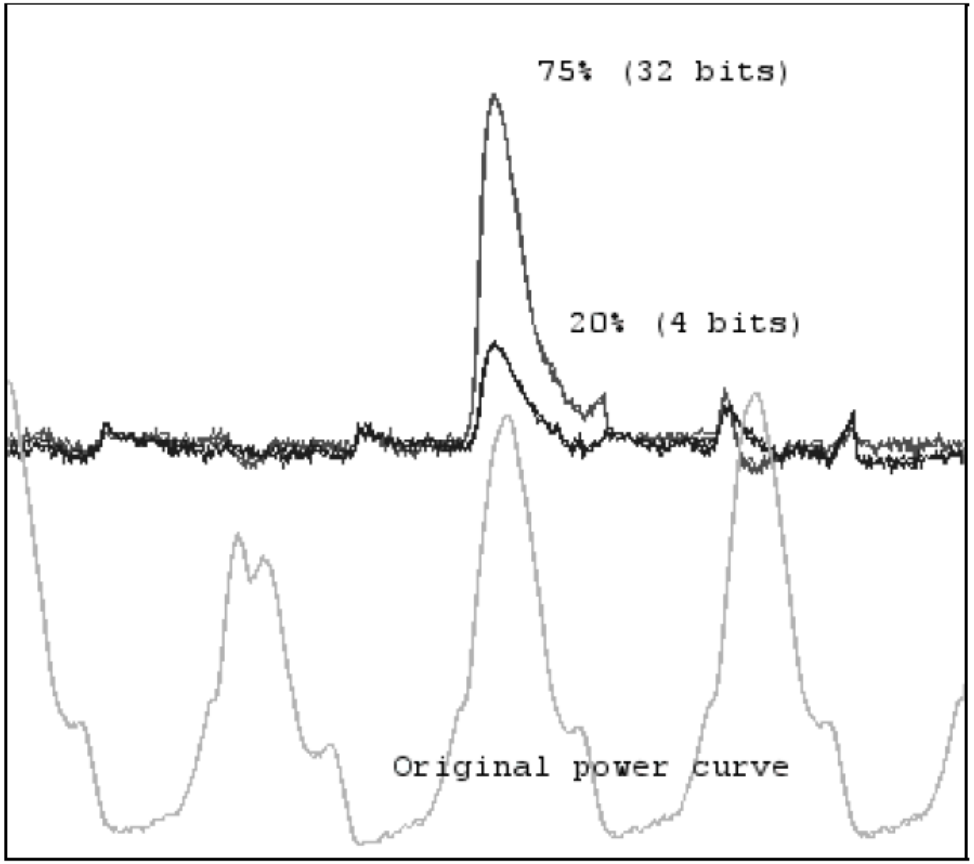
- **CPA output: sum(00110110)**

Proj 4: CPA

- Loop through key guess and ciphertext/trace
  - Find Hamming Weight
  - Find Pearson's correlation coefficient
  - Find max of the array of coefficient

Correlation Curve?

- The highest absolute value of ρ suggests the correct key guess



Brier et al. 2004