Simple Power Analysis of Elliptic Curve Cryptography

Yuan-Che Hsu and JPChen

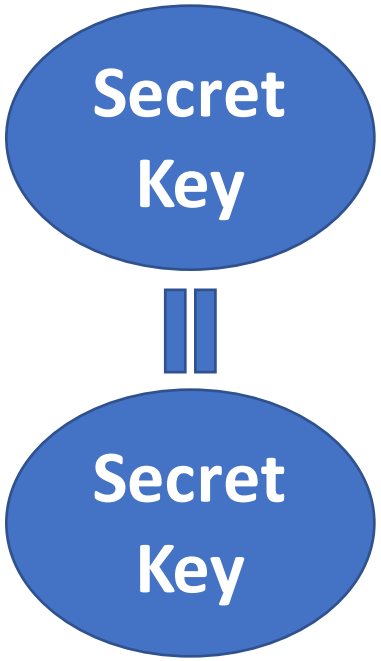
Outline

Outline

- Elliptic Curve Cryptography
- Simple Power Analysis
- Measurement Setup and Implementation
- Conclusions

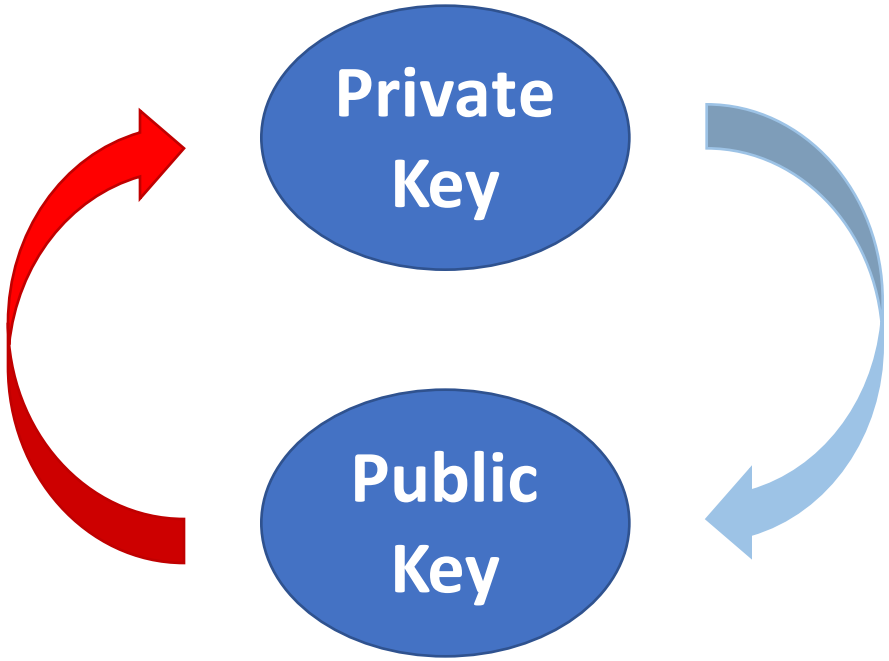
Cryptosystems

Symmetric Cipher



High Speed Encryption
AES / 3-DES

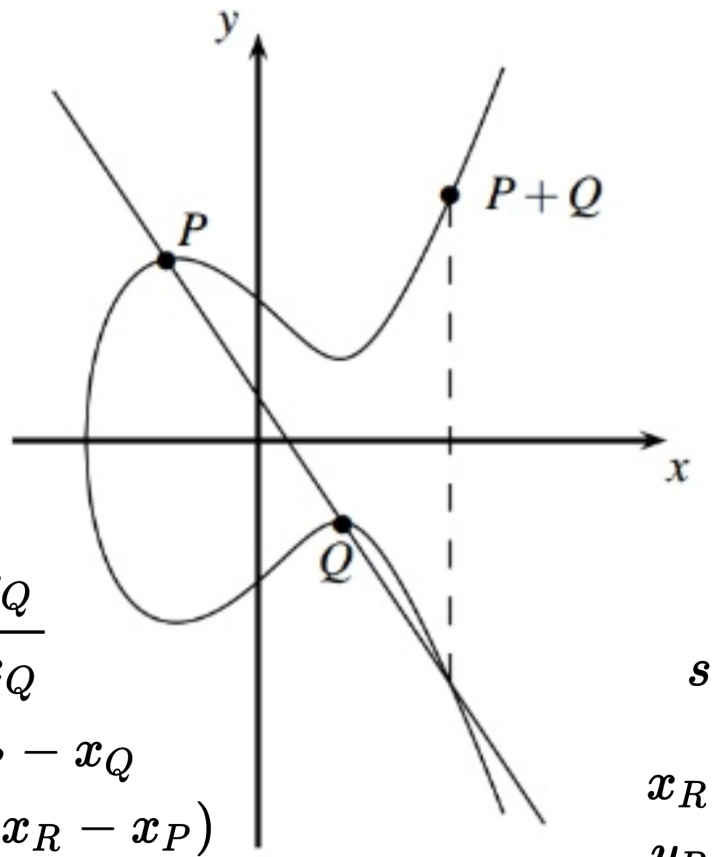
Asymmetric Cipher (PKC)



Key Agreement
RSA / ECC

Elliptic Curve Cryptography (ECC)

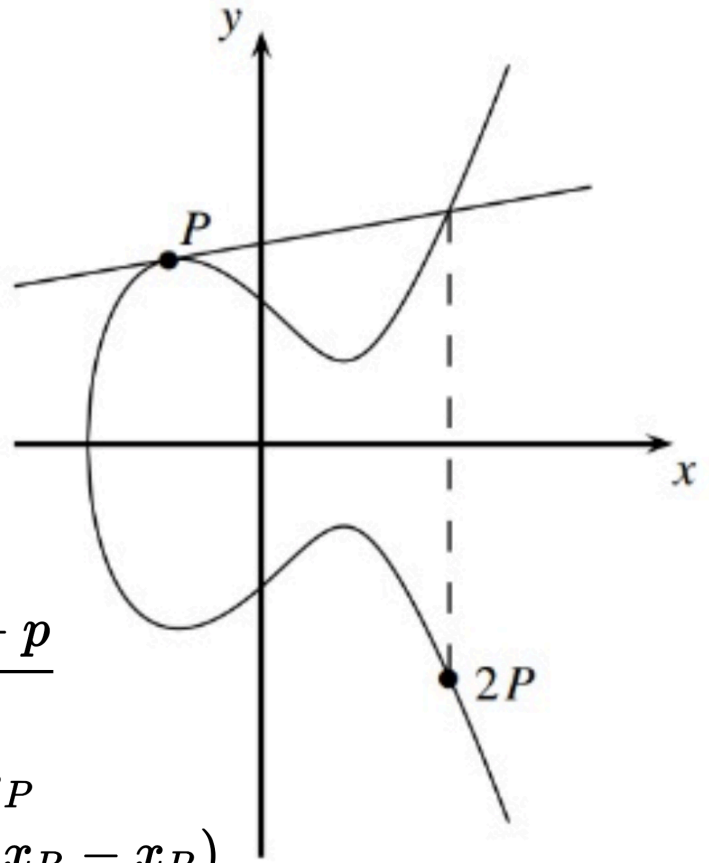
- $y^2 = x^3 + ax + b$
- Private Key: [d]
- Public Key: [d]P



$$s = \frac{y_P - y_Q}{x_P - x_Q}$$

$$x_R = s^2 - x_P - x_Q$$

$$y_R = y_P + s(x_R - x_P)$$



$$s = \frac{3{x_P}^2 - p}{2y_P}$$

$$x_R = s^2 - 2x_P$$

$$y_R = y_P + s(x_R - x_P)$$

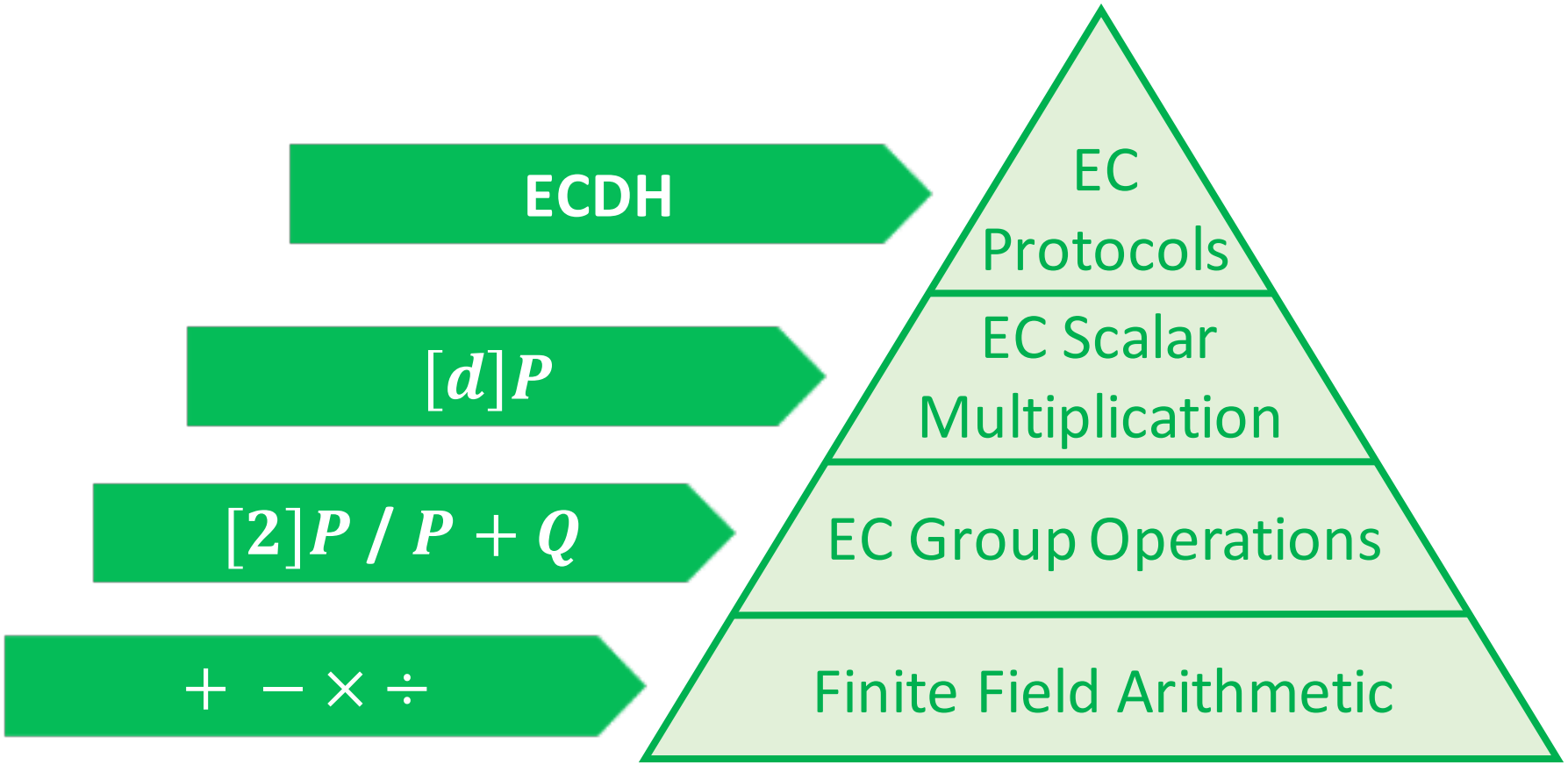
https://www.slideshare.net/KellyBresnahan/elliptic-curve-cryptography-66406021

Scalar Multiplication

- Compute [d]P
- Double-and-Add Algorithm
- 2 Registers

	10101	**10101**	**10101**	**10101**	**10101**	**10101**	**10101**
X	1P	1P	1P	1P	1P	1P	1P
Y	1P	2P	4P	5P	10P	20P	21P

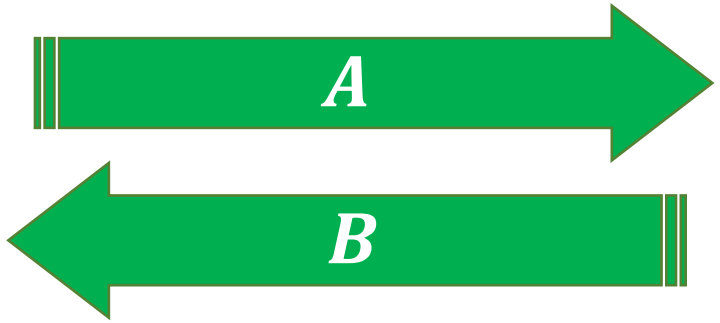
Implementation Hierarchy



ECDH (Key Exchange)

Specified
Field / Curve / Base Point P

Choose secret a
Compute $A = [a]P$



Choose secret b
Compute $B = [b]P$

Compute shared secret $Q = [a]B$

Compute shared secret $Q = [b]A$

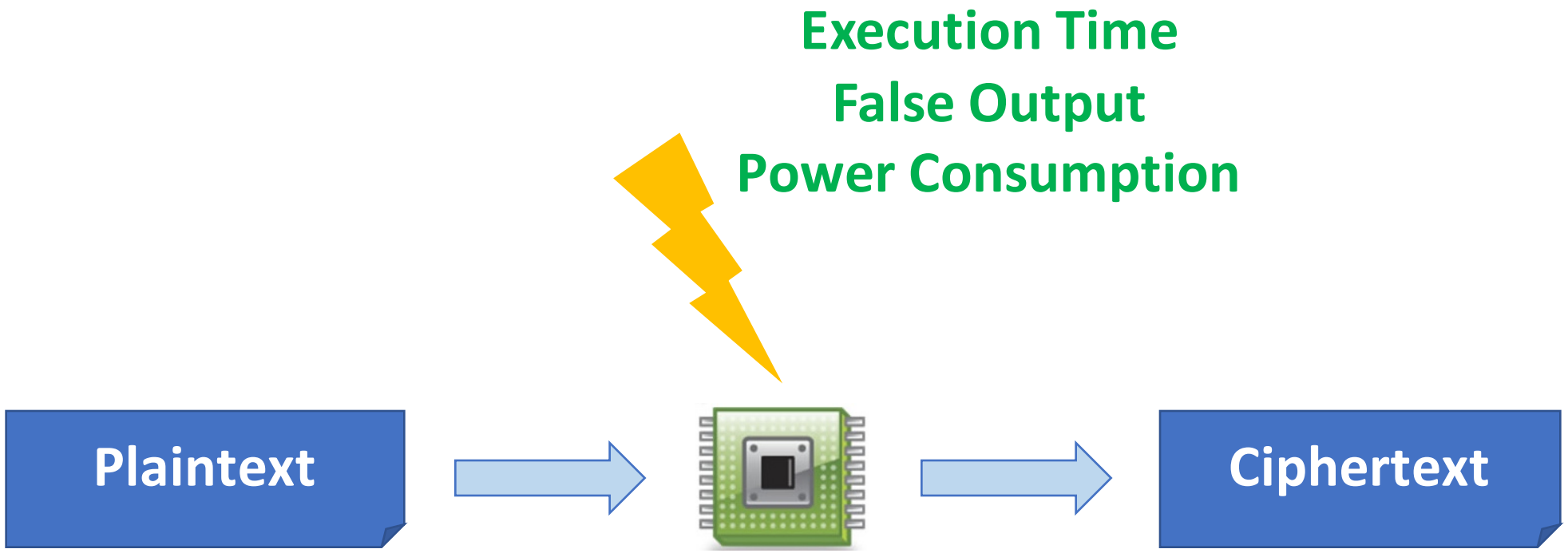
Advantage of ECC

- Small Key Size / Efficient Performance
- Standard of NIST / SECG

Outline

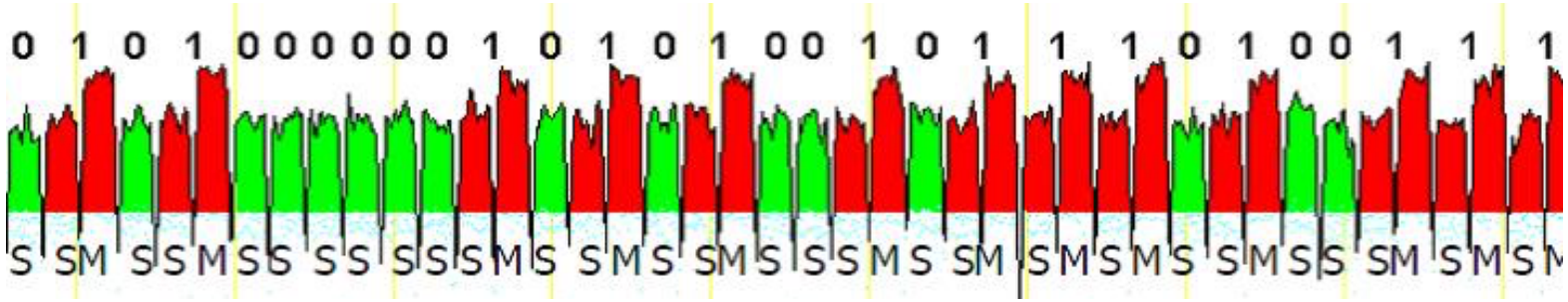
- Elliptic Curve Cryptography
- Simple Power Analysis
- Measurement Setup and Implementation
- Conclusions

Side Channel Attack (SCA)

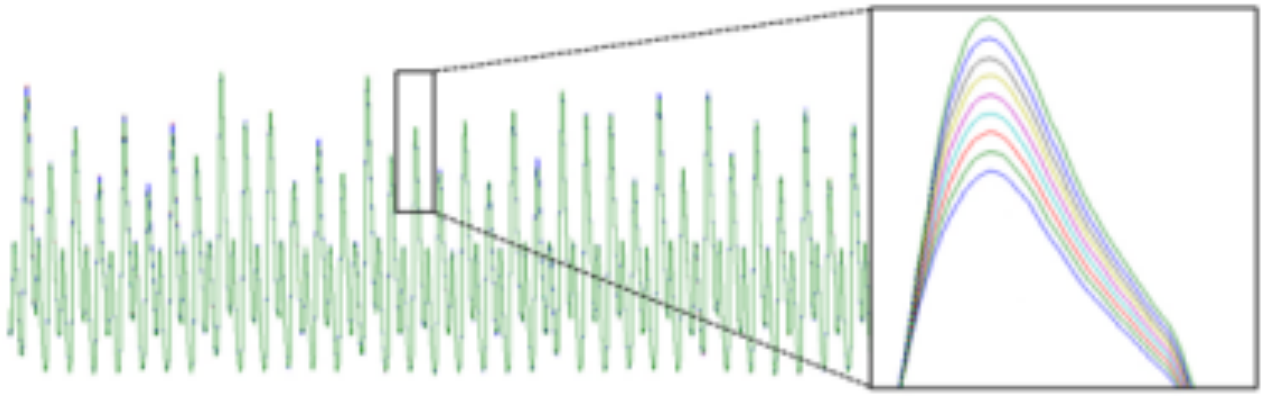


Power Analysis Attack

- Simple Power Analysis
  - Instruction Leakage



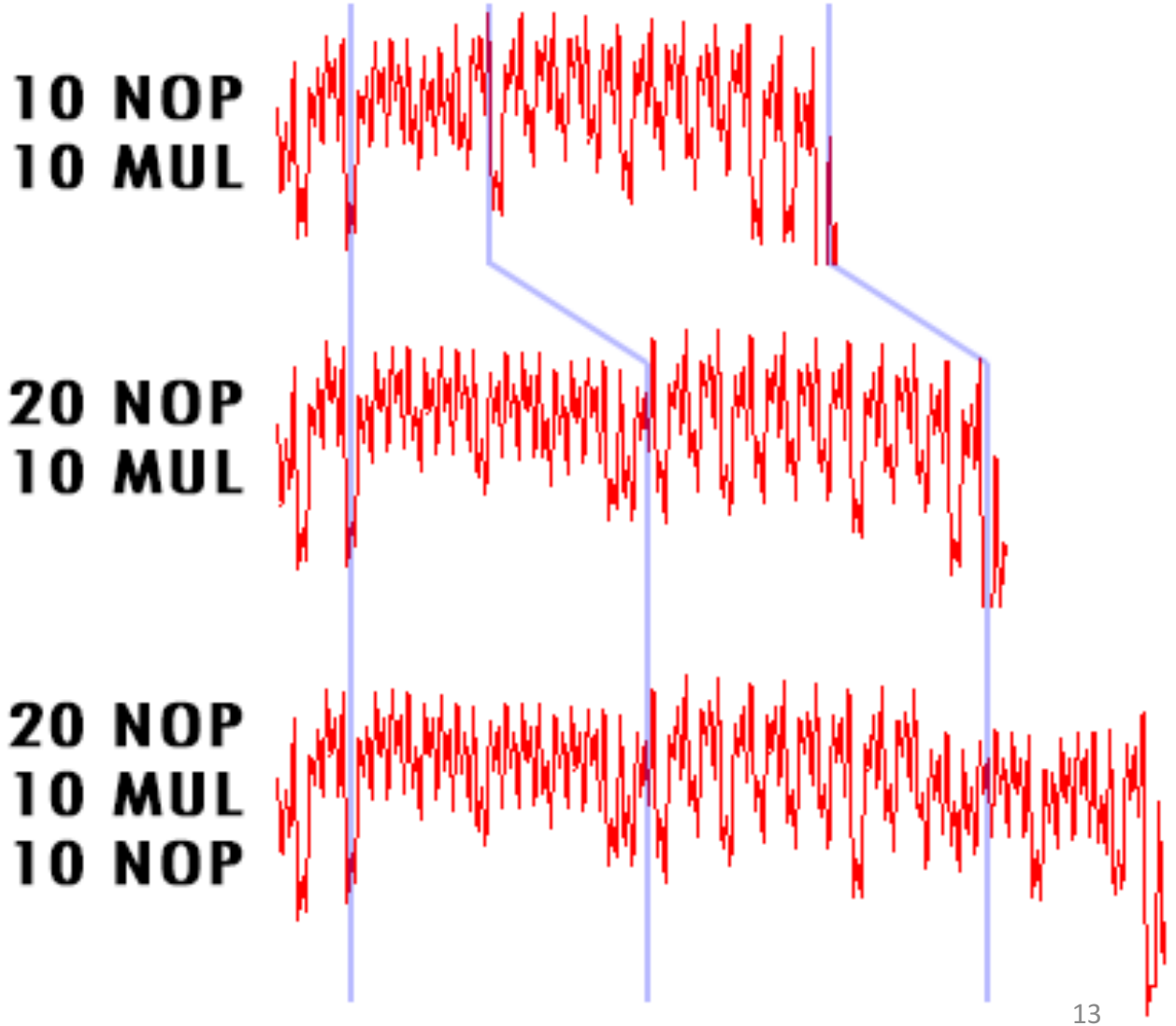
- Differential Power Analysis
  - Data Leakage



http://www.edn.com/Home/PrintView?contentItemId=4410267
https://www.cosic.esat.kuleuven.be/secure-embedded-systems/physical.html

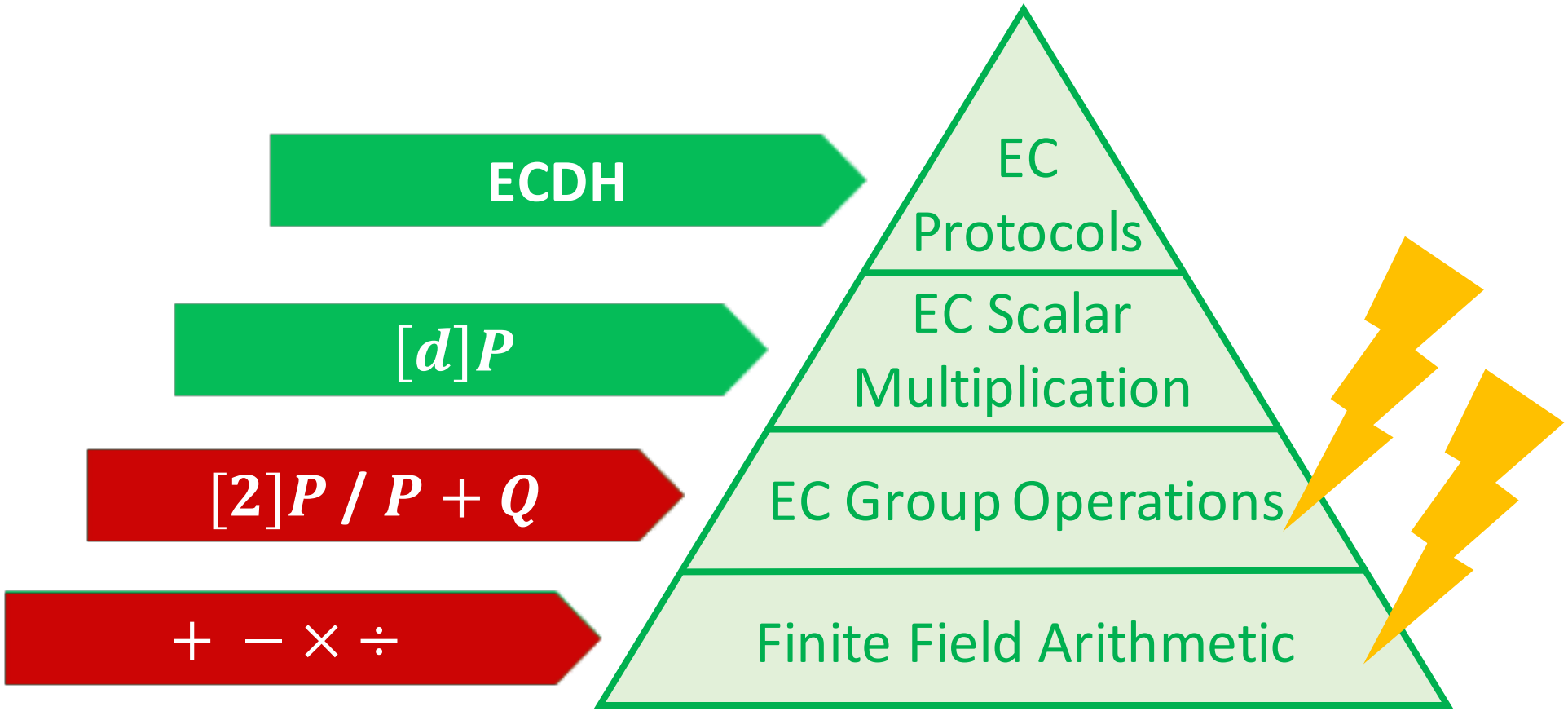
Simple Power Analysis (SPA)

- Key-Dependent Instructions
- Template Profiling
- Pattern Recognition

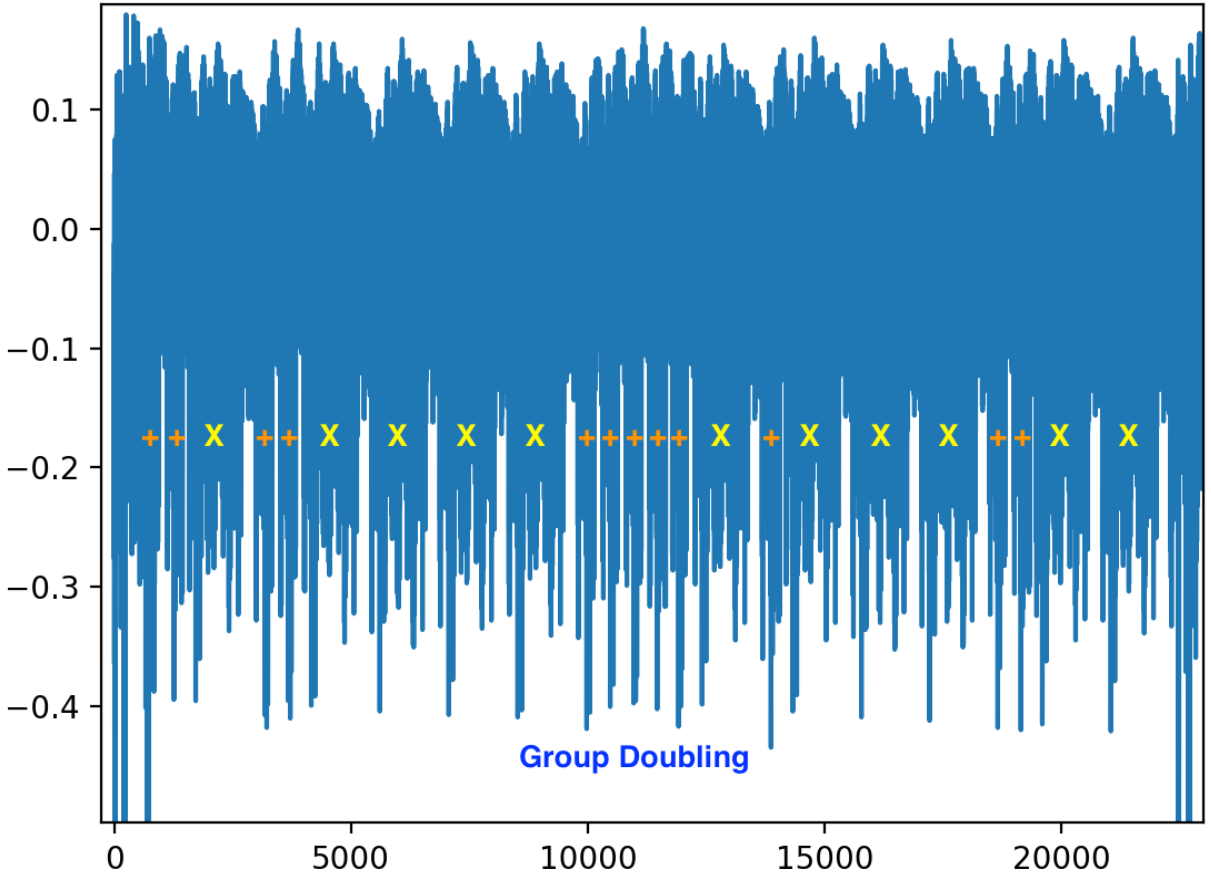


https://wiki.newae.com/Tutorial_B2_Viewing_Instruction_Power_Differences

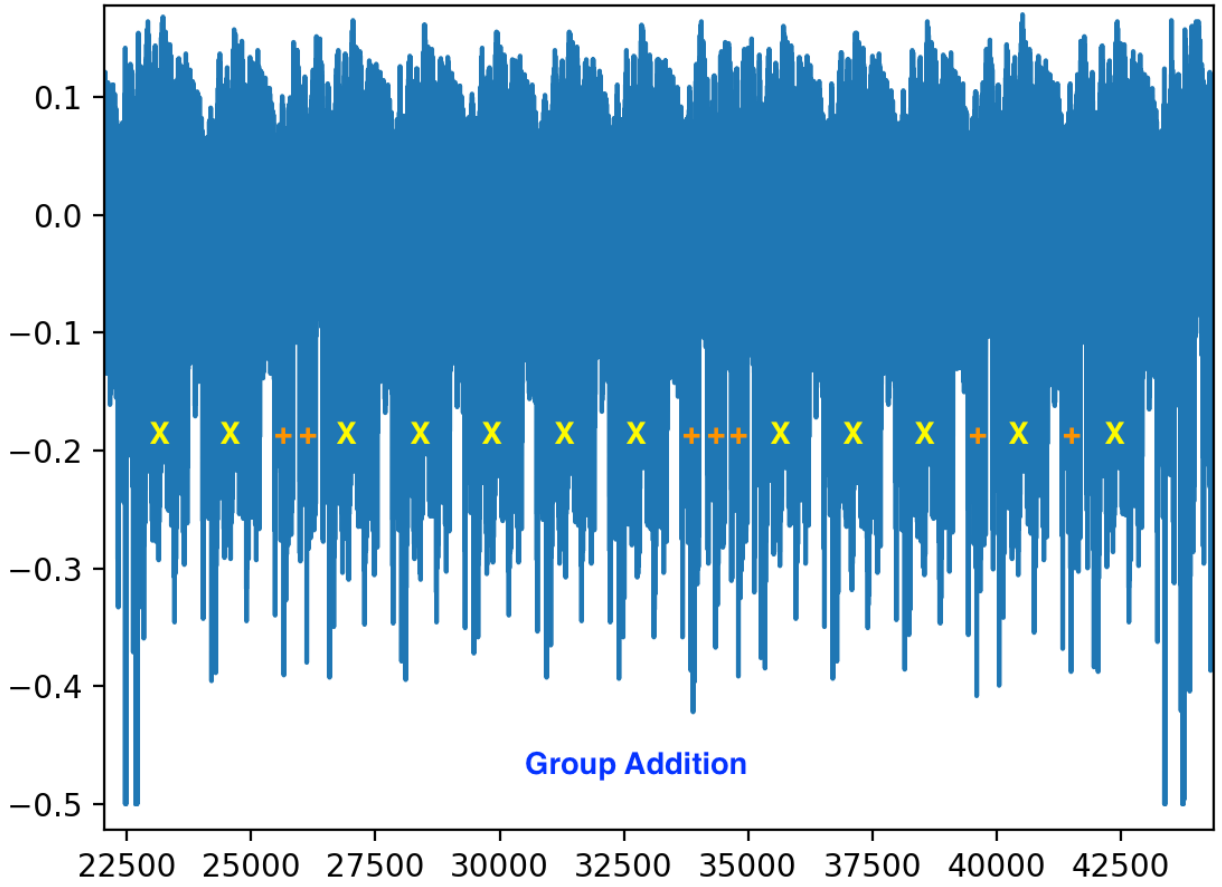
Key-Dependent Instructions



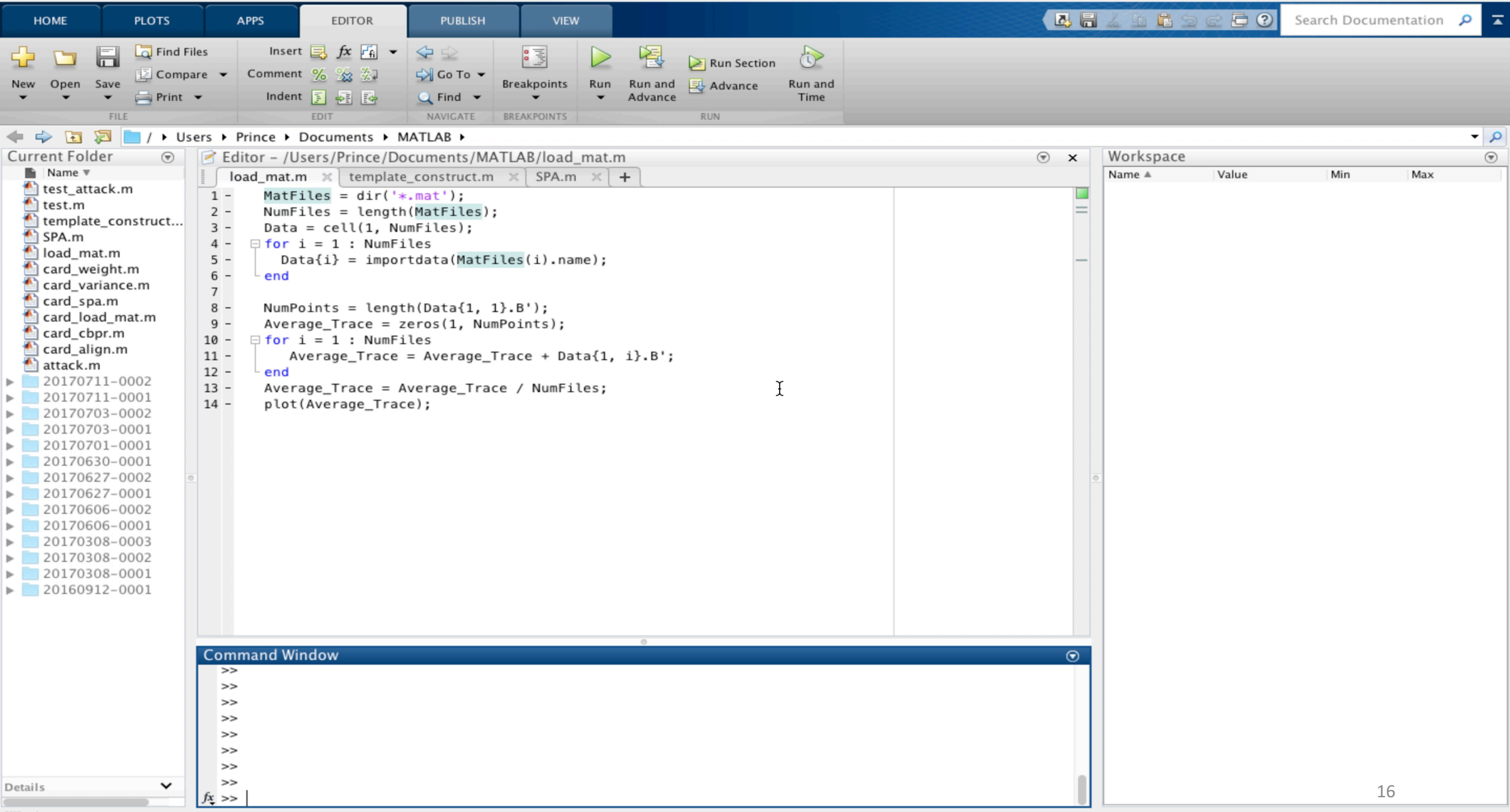
Double and Add in Power Traces



Double



Add


HOME
PLOTS
APPS
EDITOR
PUBLISH
VIEW
Search Documentation
New
Open
Save
Find Files
Compare
Print
FILE
Insert
Comment
Indent
EDIT
Go To
Find
NAVIGATE
Breakpoints
BREAKPOINTS
Run
Run and Advance
Run Section
Advance
Run and Time
RUN
/ ▸ Users ▸ Prince ▸ Documents ▸ MATLAB ▸
Current Folder
Name
test_attack.m
test.m
template_construct...
SPA.m
load_mat.m
card_weight.m
card_variance.m
card_spa.m
card_load_mat.m
card_cbpr.m
card_align.m
attack.m
20170711-0002
20170711-0001
20170703-0002
20170703-0001
20170701-0001
20170630-0001
20170627-0002
20170627-0001
20170606-0002
20170606-0001
20170308-0003
20170308-0002
20170308-0001
20160912-0001
Details
Editor - /Users/Prince/Documents/MATLAB/load_mat.m
load_mat.m
template_construct.m
SPA.m
1 - MatFiles = dir('*.mat');
2 - NumFiles = length(MatFiles);
3 - Data = cell(1, NumFiles);
4 - for i = 1 : NumFiles
5 - Data{i} = importdata(MatFiles(i).name);
6 - end
7
8 - NumPoints = length(Data{1, 1}.B');
9 - Average_Trace = zeros(1, NumPoints);
10 - for i = 1 : NumFiles
11 - Average_Trace = Average_Trace + Data{1, i}.B';
12 - end
13 - Average_Trace = Average_Trace / NumFiles;
14 - plot(Average_Trace);
Command Window
>>
Workspace
Name
Value
Min
Max

Outline

- Elliptic Curve Cryptography
- Simple Power Analysis
- Measurement Setup and Implementation
- Conclusions

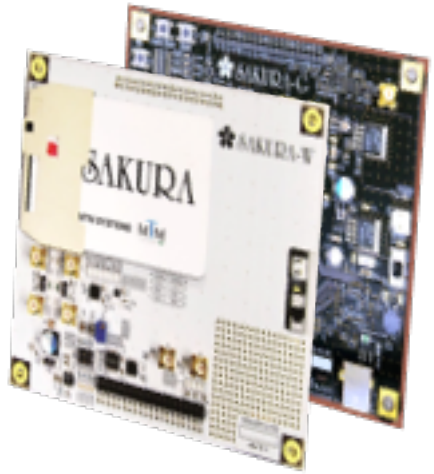
Measurement Setup

Power Traces (USB)

Plaintext (USB)

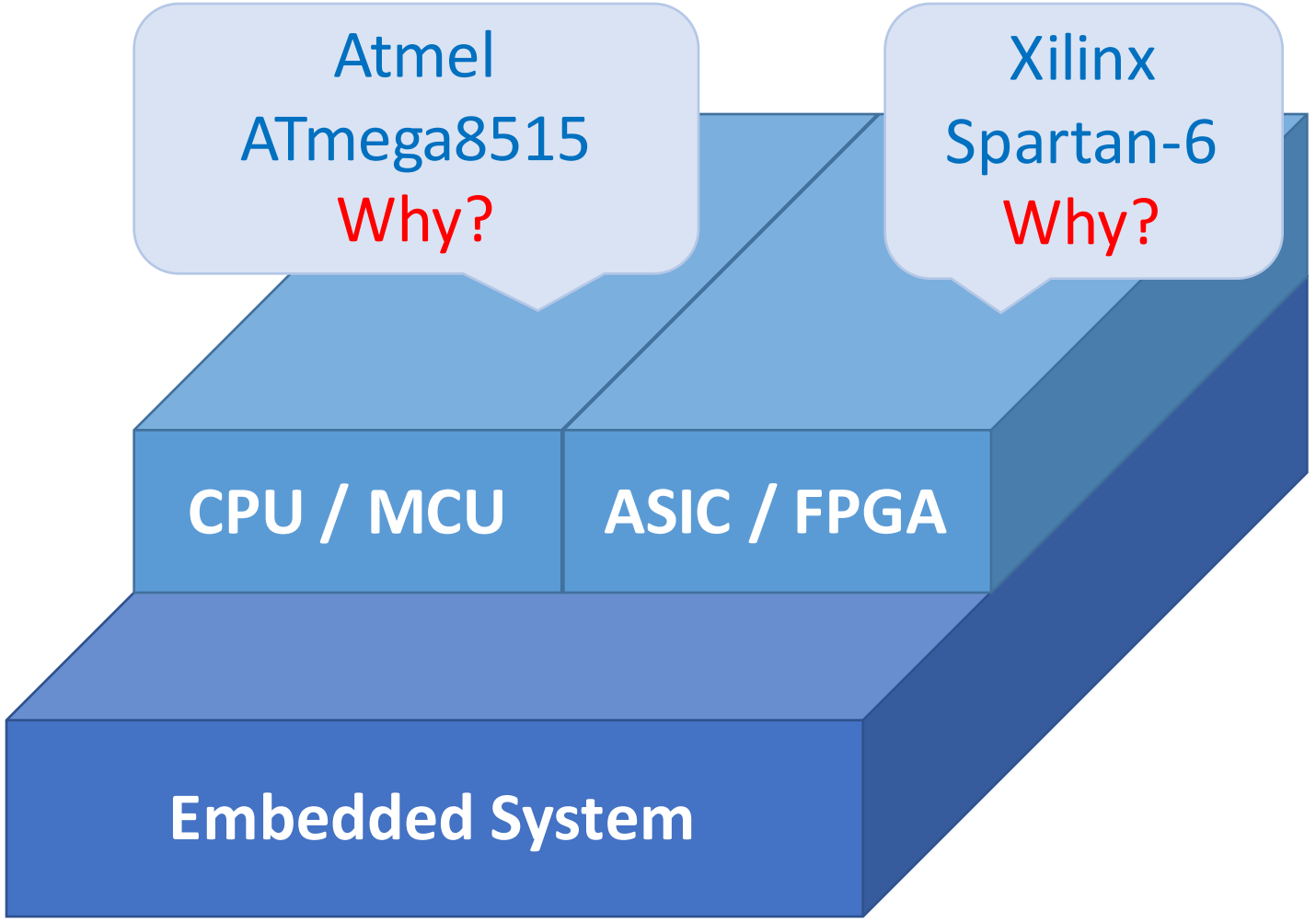
Ciphertext (USB)

Power Consumption (SMA)

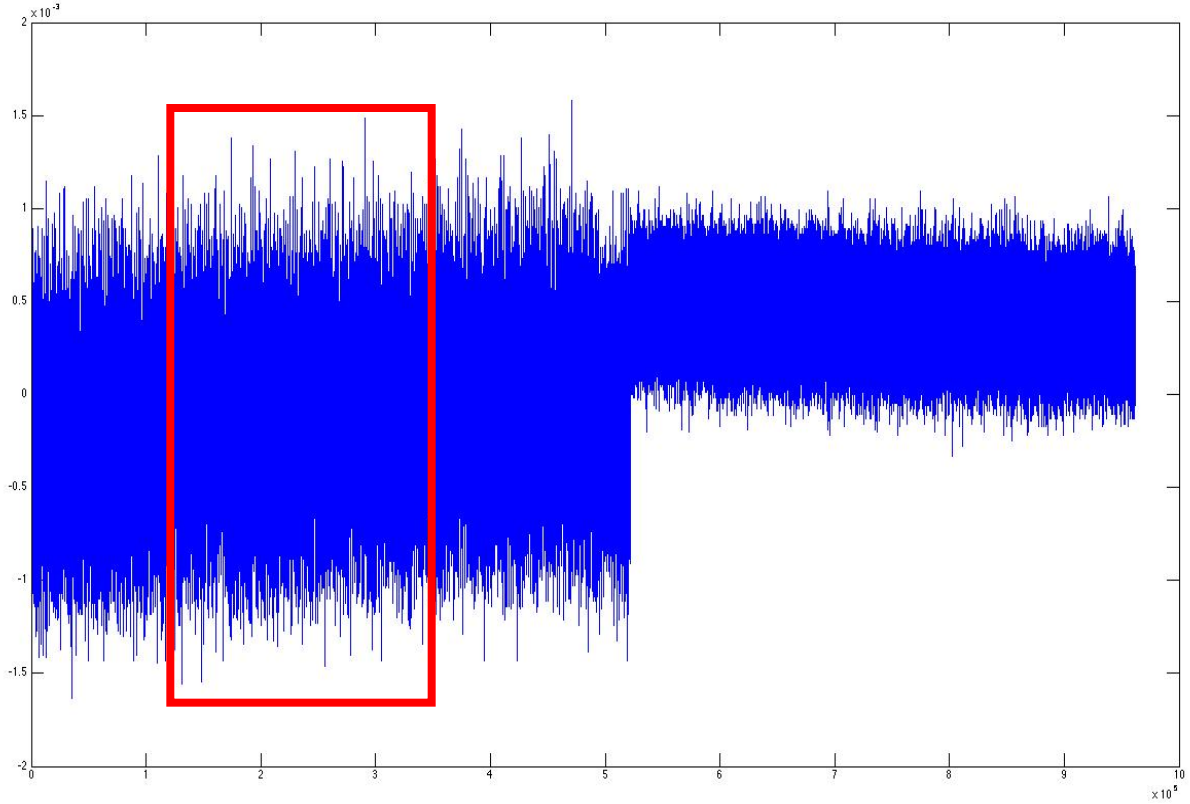


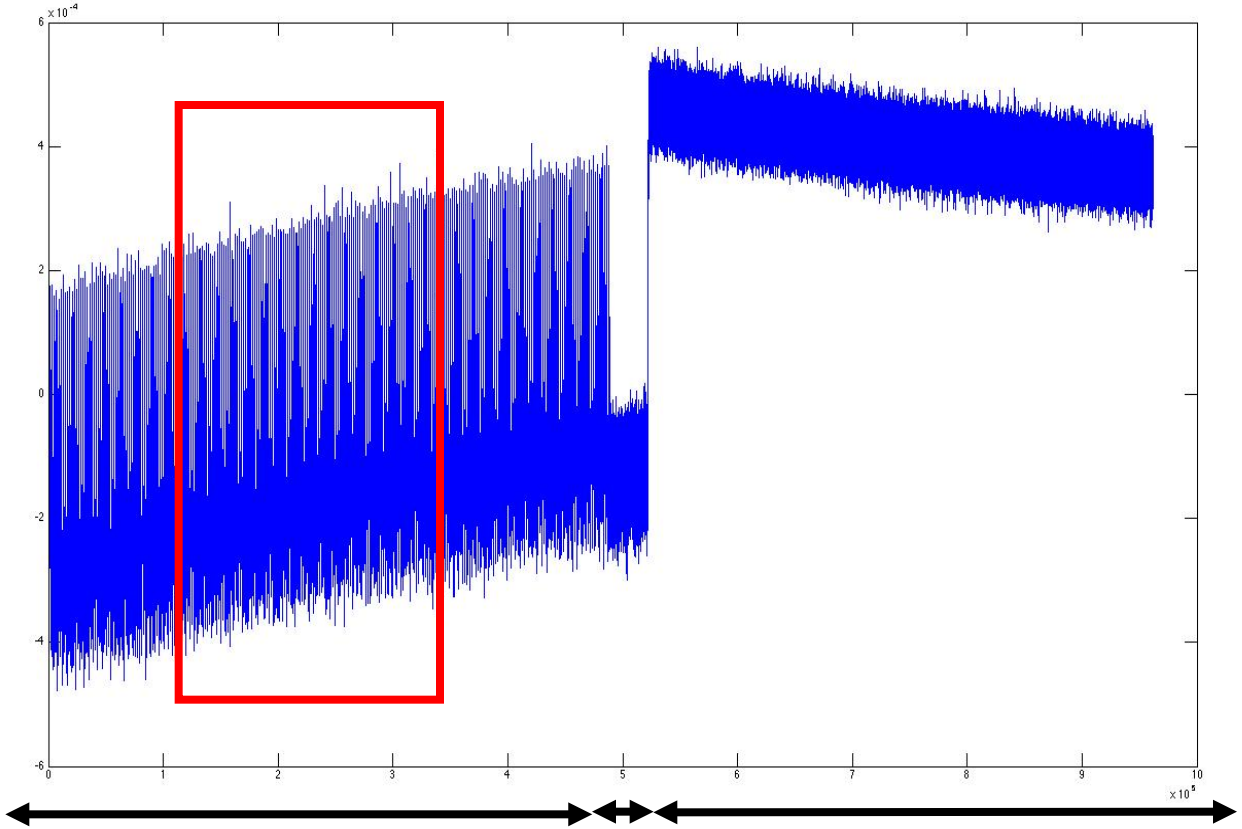
http://en.mtmsystems.jp/sakura.html
http://www.saelig.com/product/PSPC10BIT015.htm
https://www.acer.com/ac/en/IL/content/model/NX.M69ET.008

Target Victims



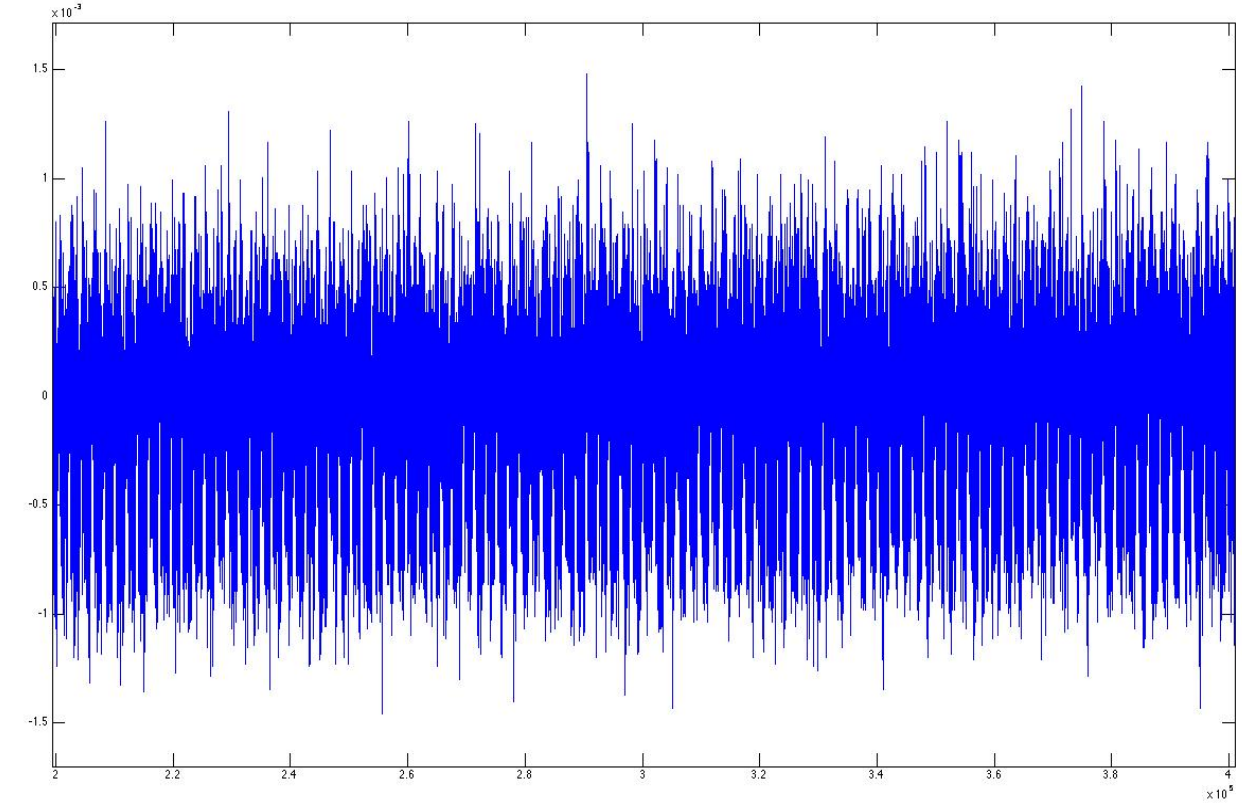
Trace (FPGA)

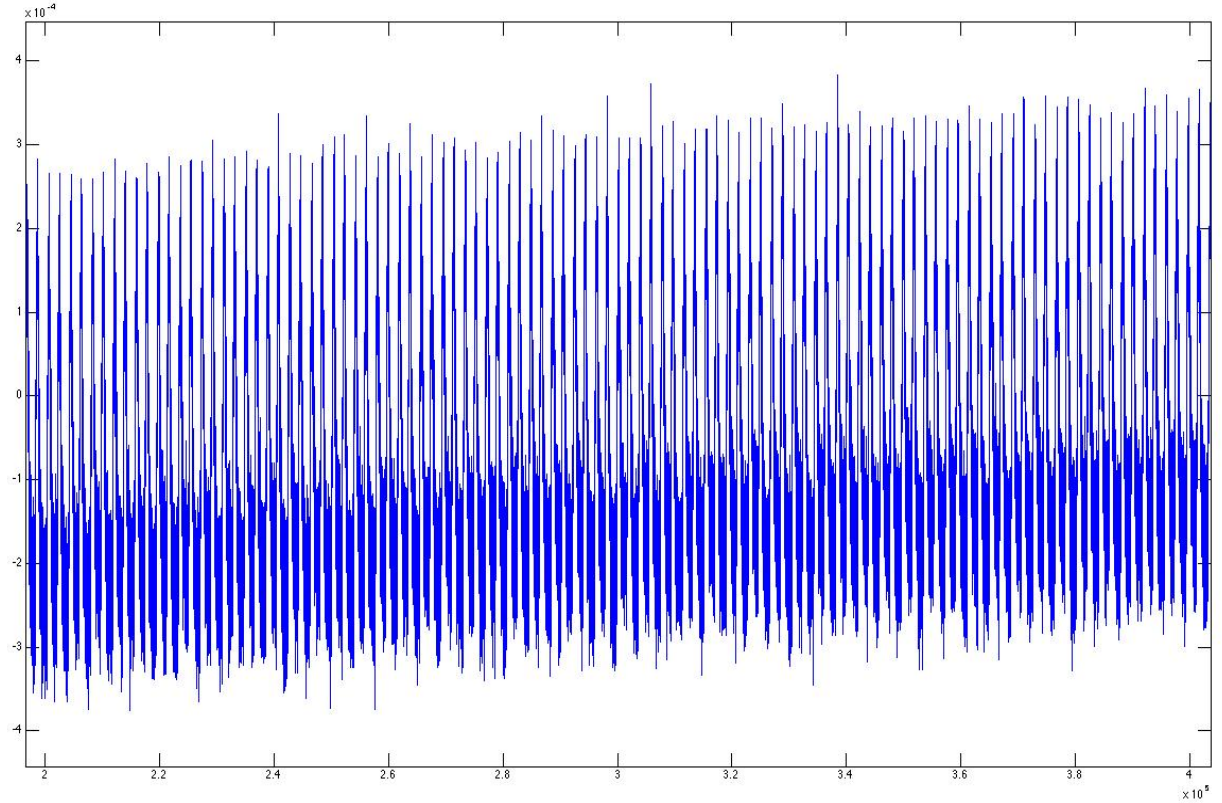




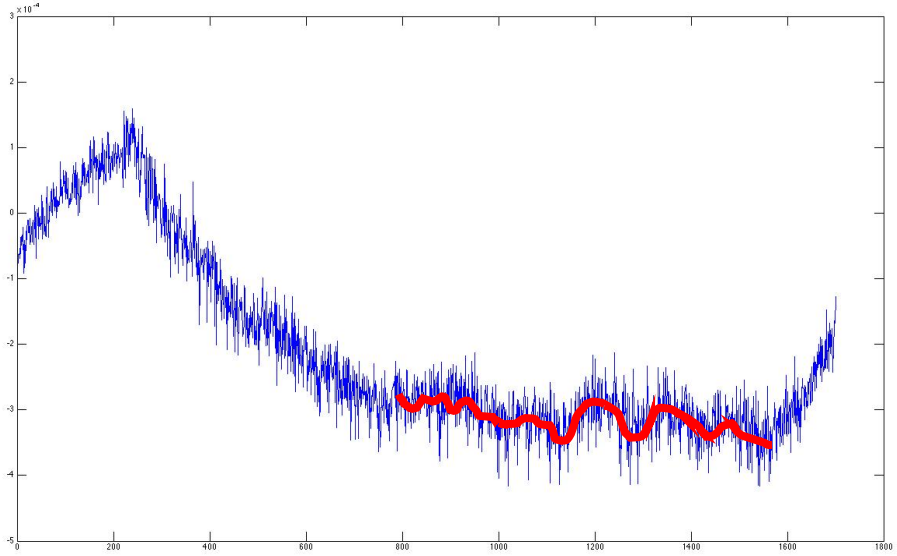
$[2]P$ / $P + Q$ ÷ Idle

Trace Enlarged (FPGA)

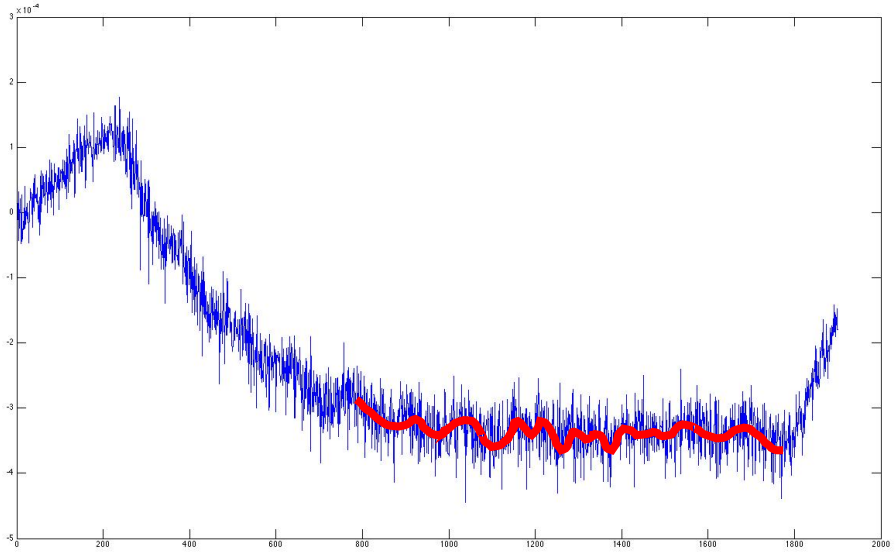




Template Construction (FPGA)



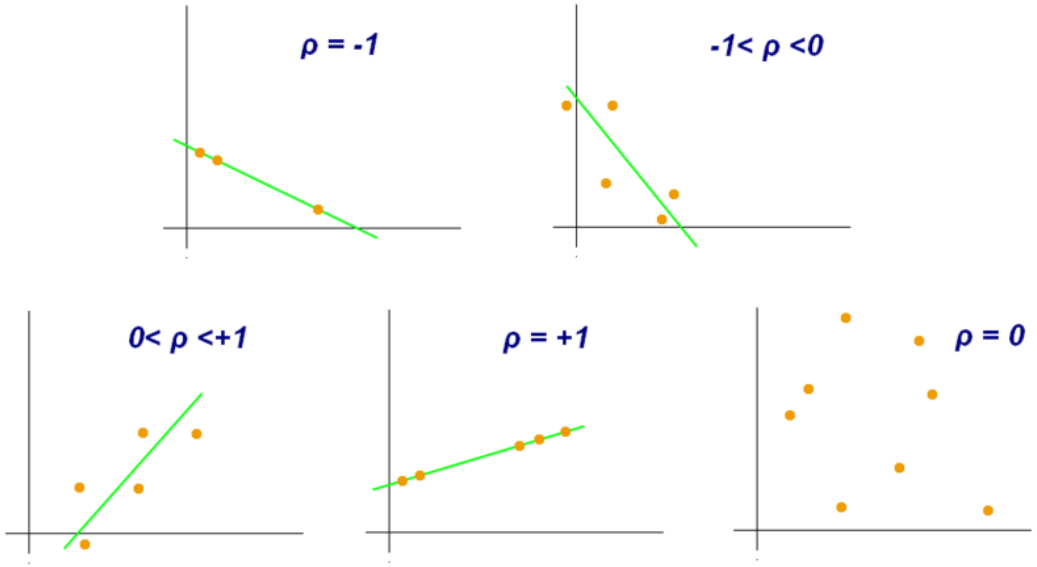
Double

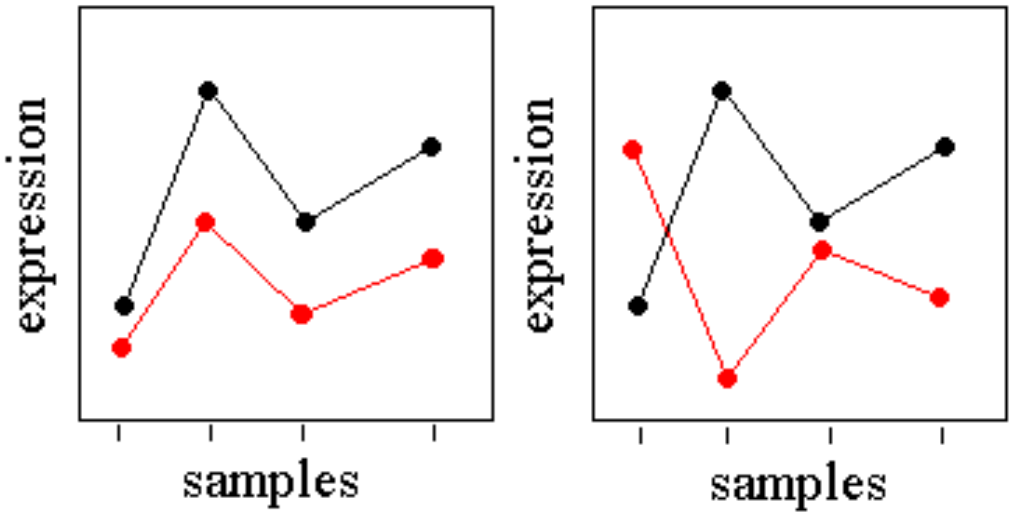


Add

Pearson Correlation Coefficient

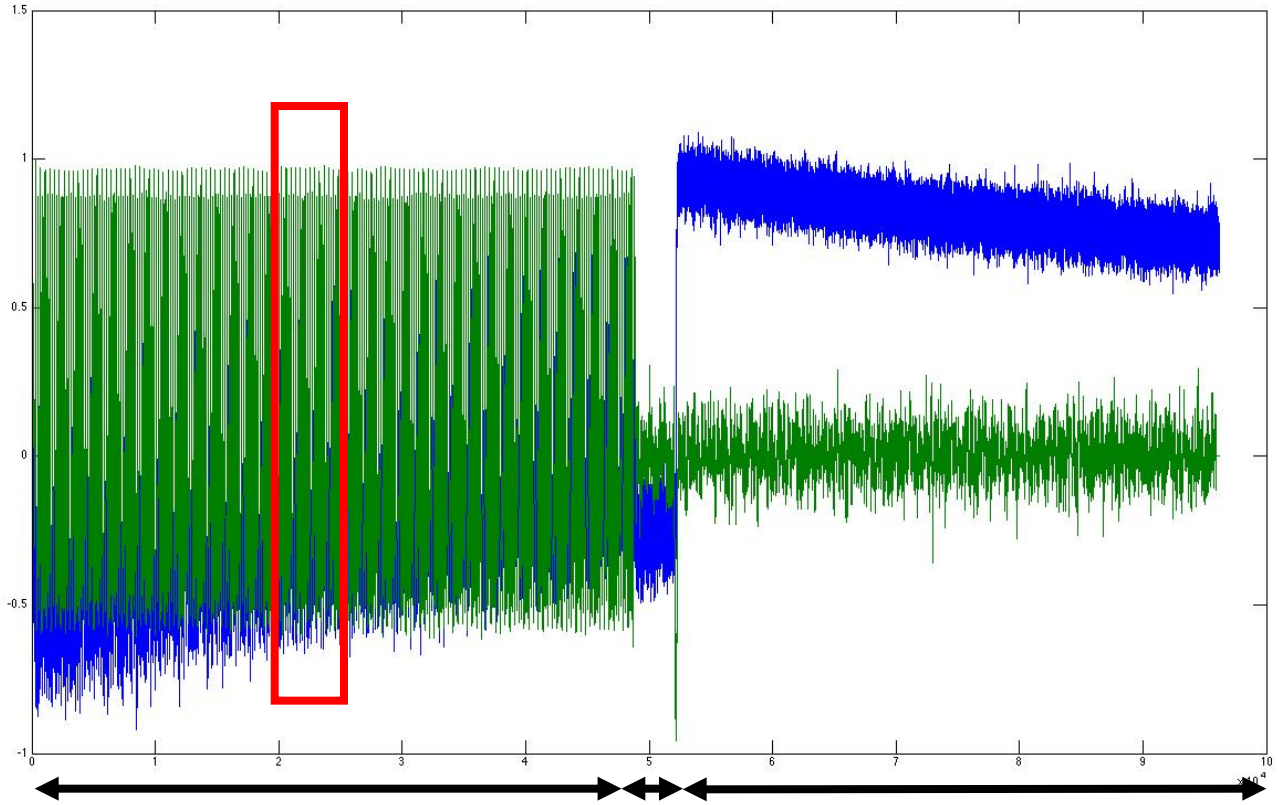
$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}}$$





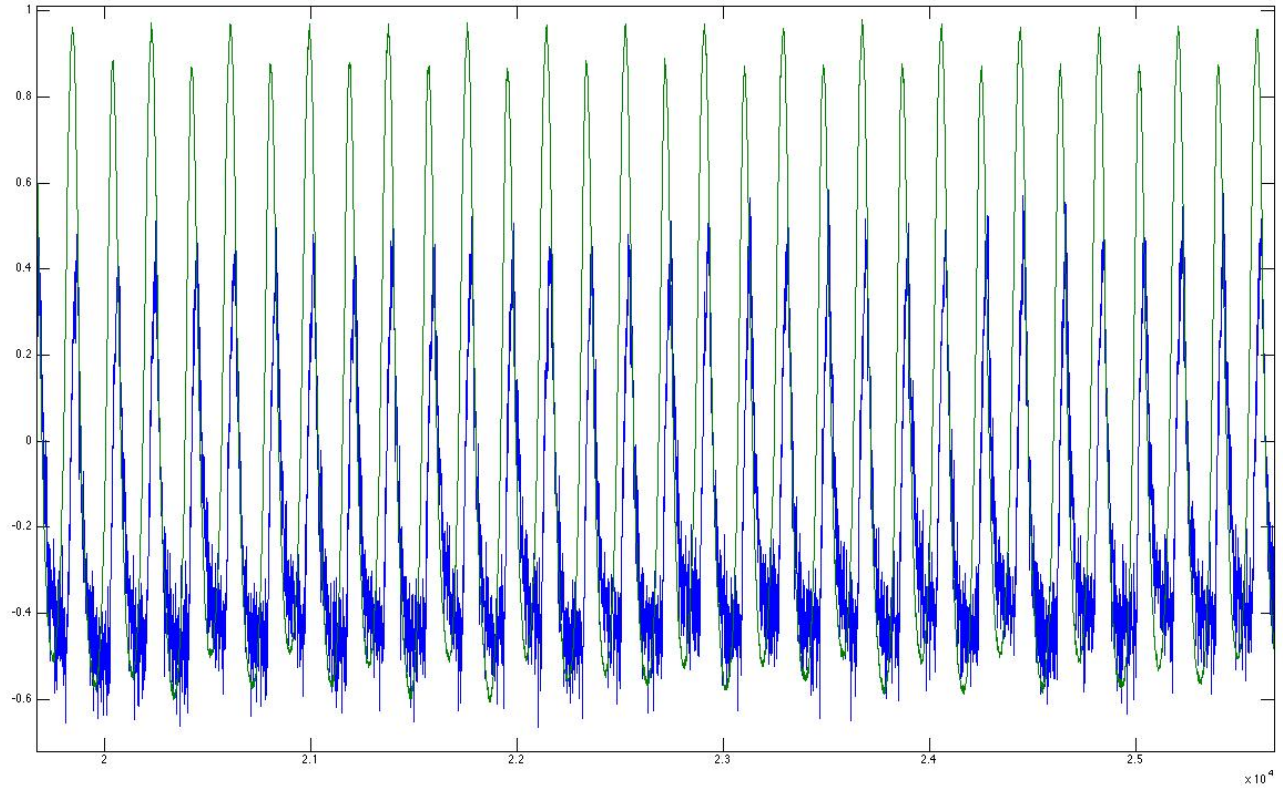
https://en.wikipedia.org/wiki/Pearson_correlation_coefficient
http://www.improvedoutcomes.com/docs/WebSiteDocs/Clustering/Clustering_Parameters/Pearson_Correlation_and_Pearson_Squared_Distance_Metric.htm

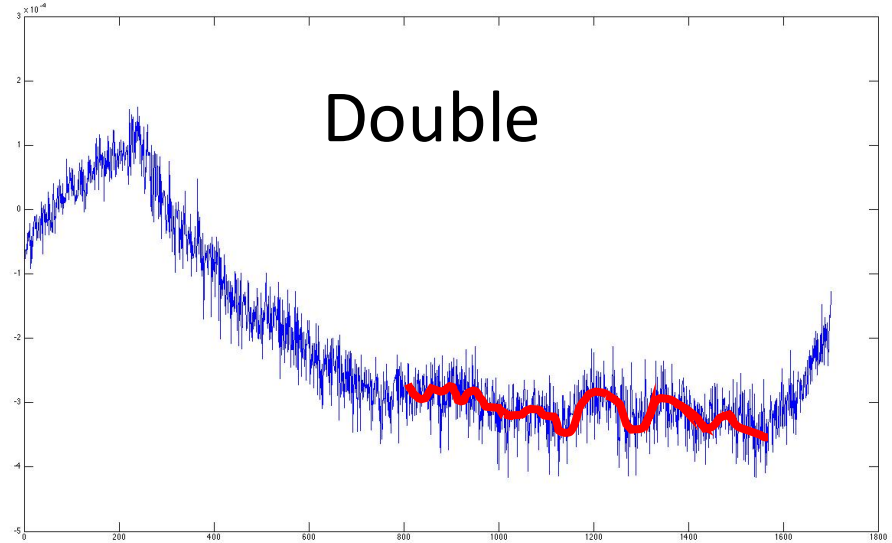
Correlation Trace (FPGA)

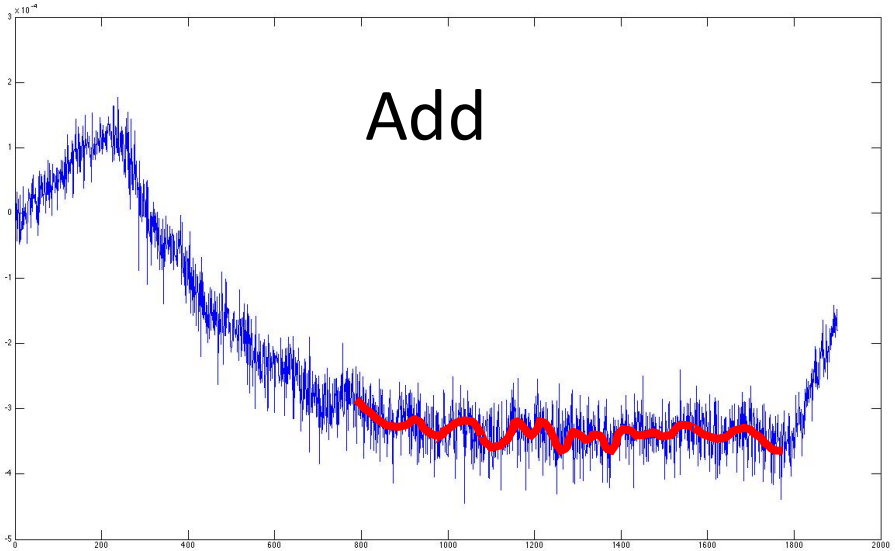


Correlation Trace Zoomed (FPGA)

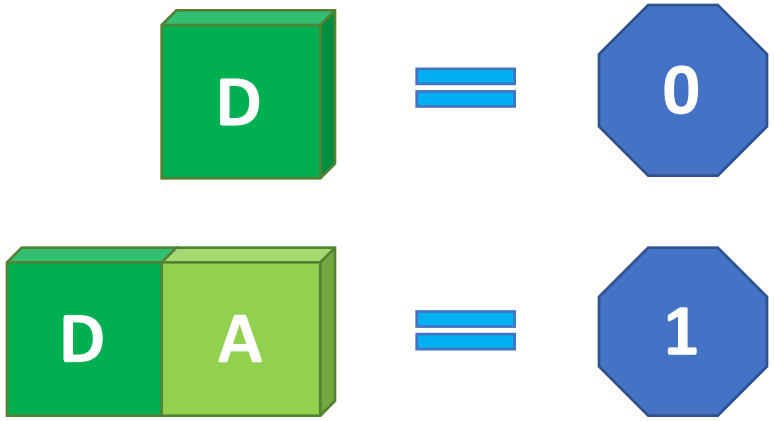
ADADADADADADADADADADADADADADA







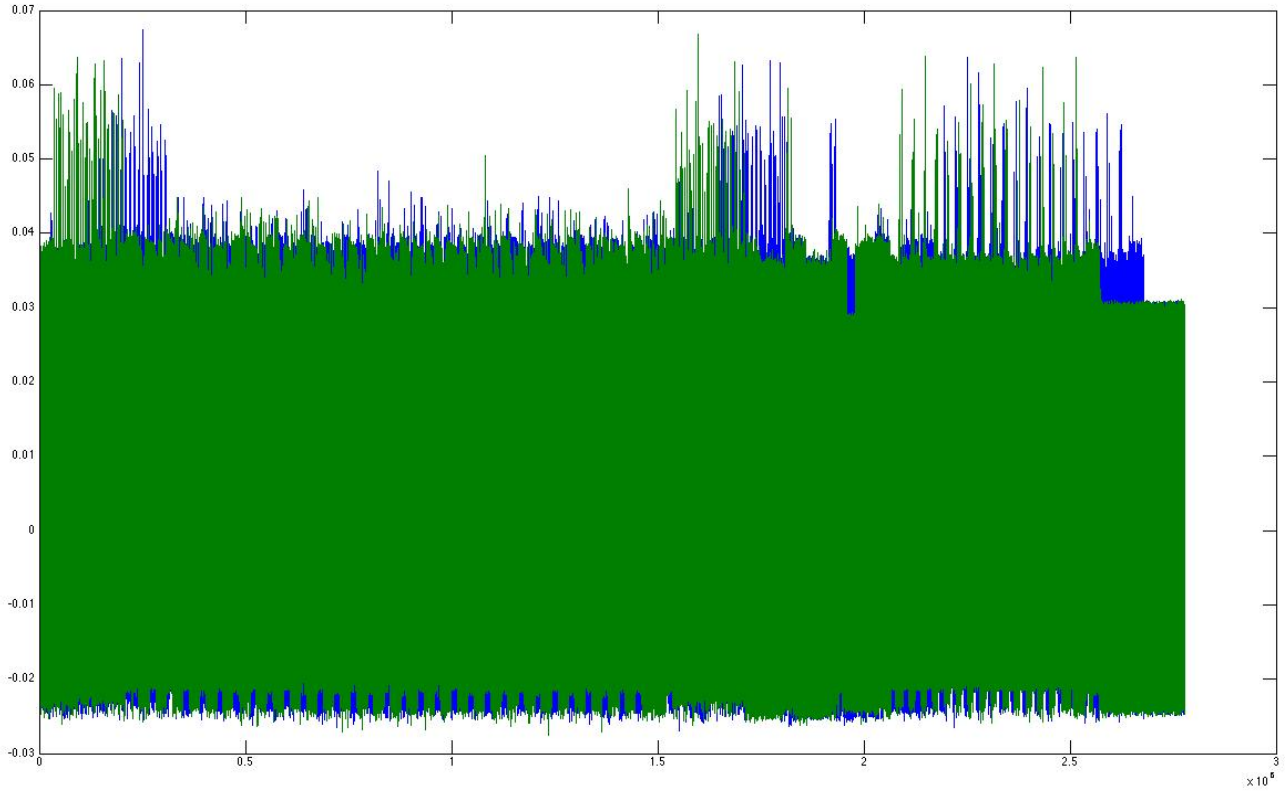
Key Recovery (FPGA)



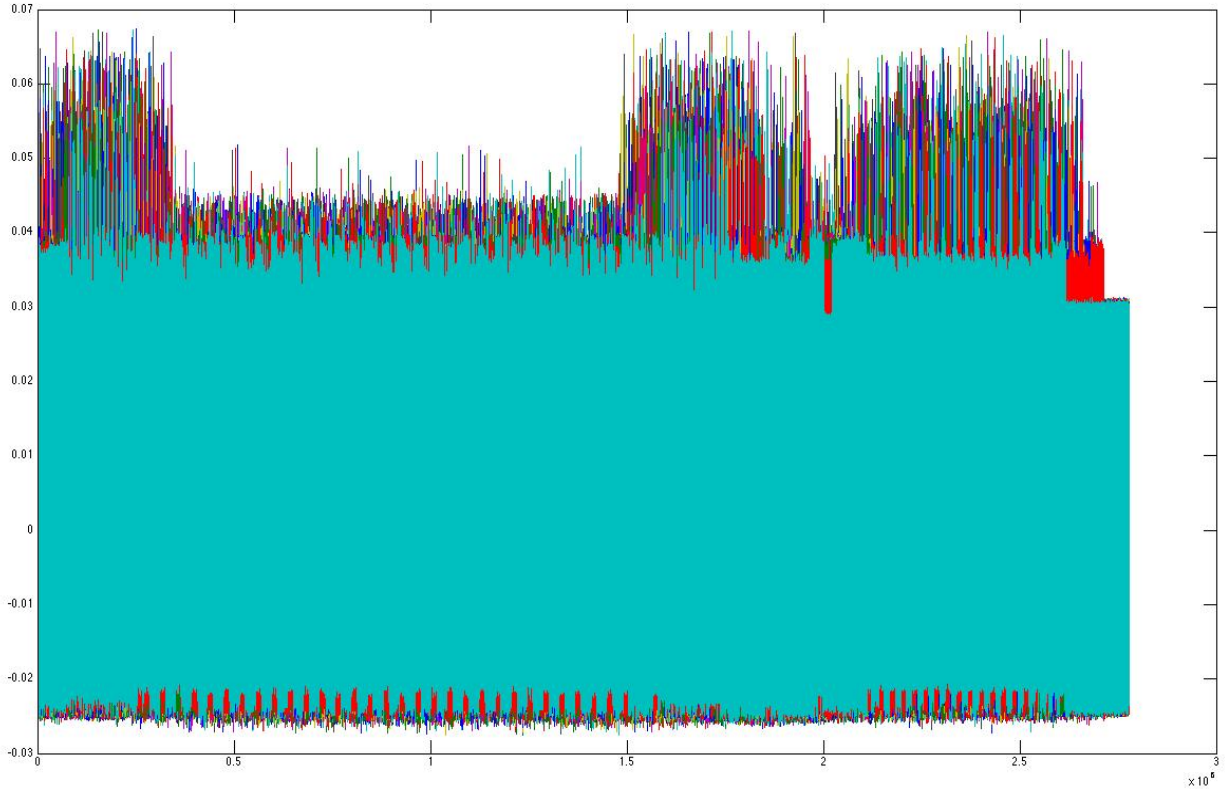
Command Window

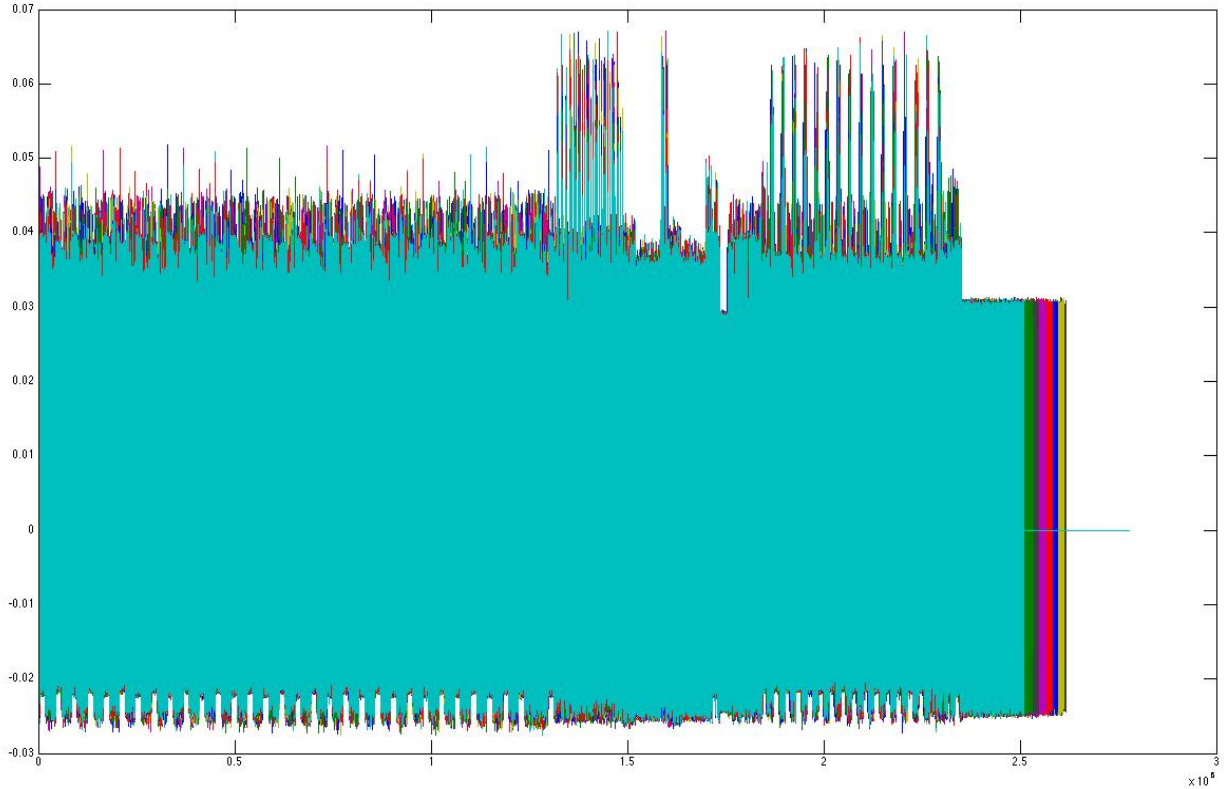
```
>> SPA

Key =

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

>>
```

Two Trace (Smartcard)

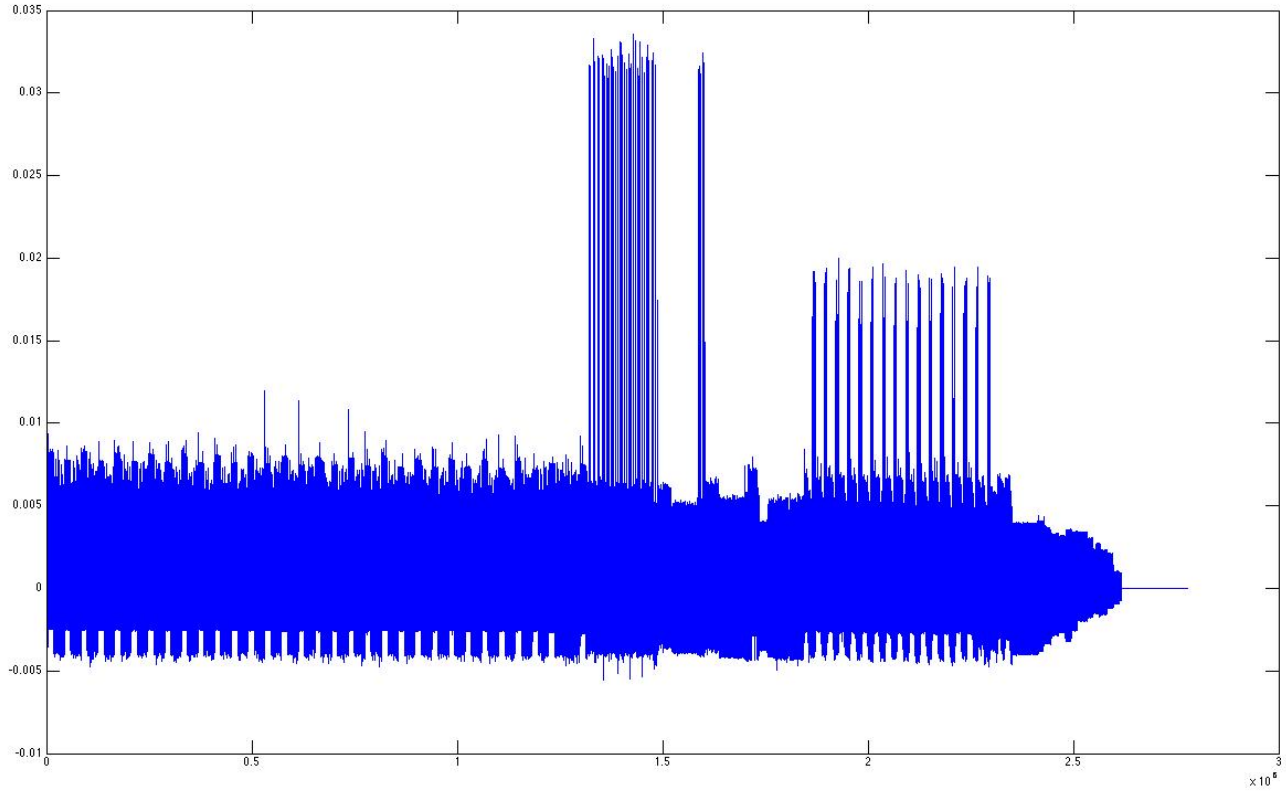


More Traces (Smartcard)

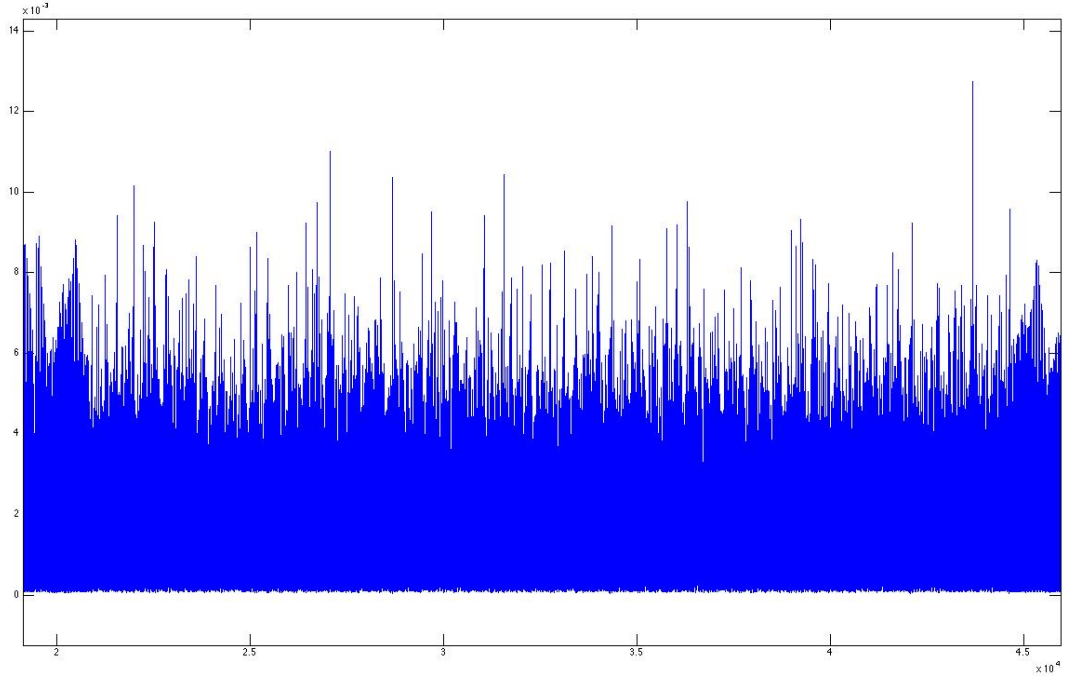


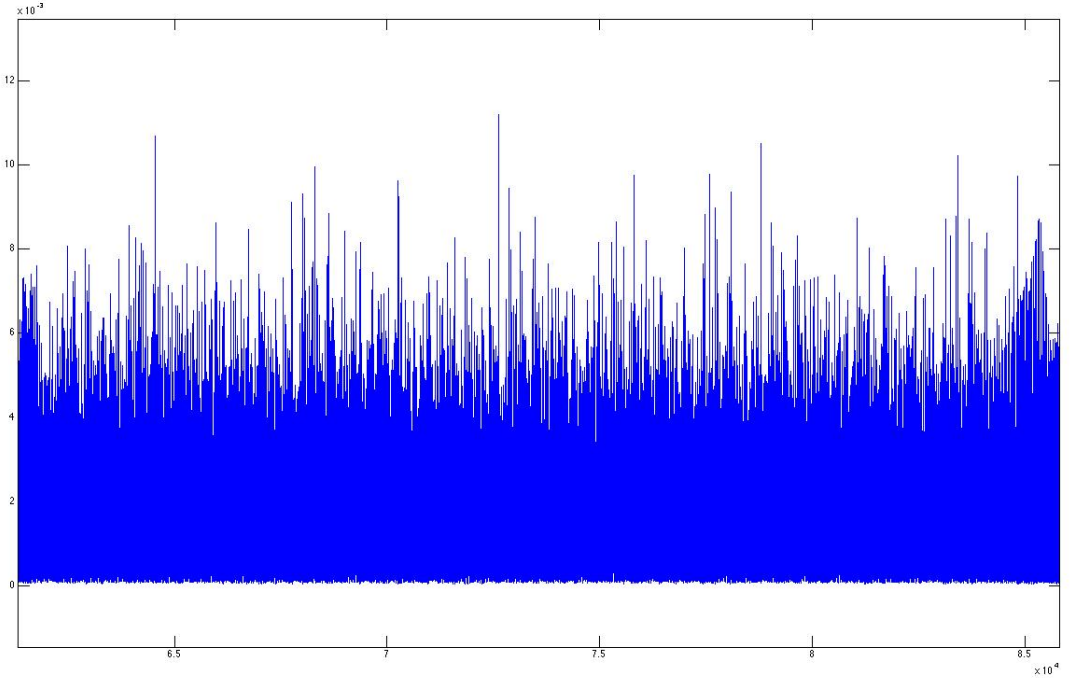


Variance Trace (Smartcard)

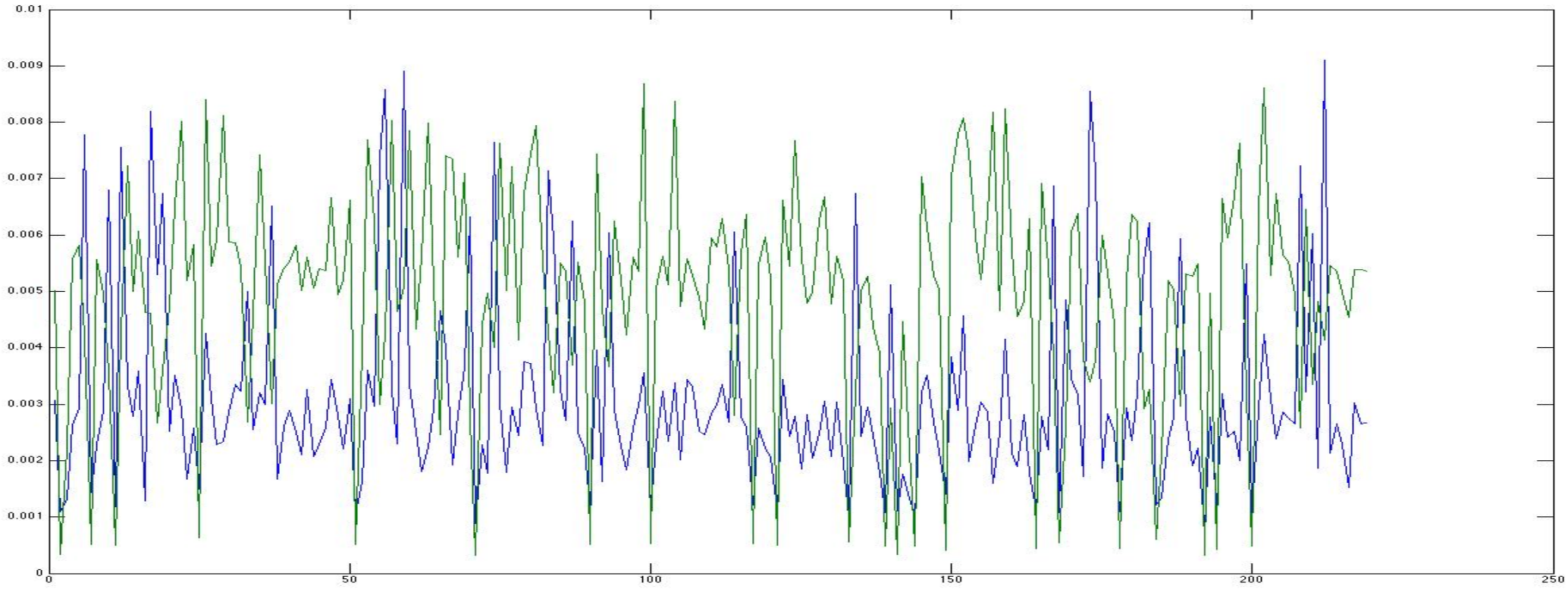


Variance Trace Enlarged (Smartcard)





Extracted Variance Template (Smartcard)



Experiment Results

	Trace #	Base Point	Template Construction	Pattern Recognition
FPGA	32	Fixed	Average	Correlation
Smartcard	30	Random	Alignment Variance	Extraction Correlation

Outline

- Elliptic Curve Cryptography
- Simple Power Analysis
- Measurement Setup and Implementation
- Conclusions

Conclusion

- Algorithmic security is not sufficient anymore
- Hardware security is the main challenge for embedded systems
- Countermeasure exists but trades performance

Thank You for Listening!