

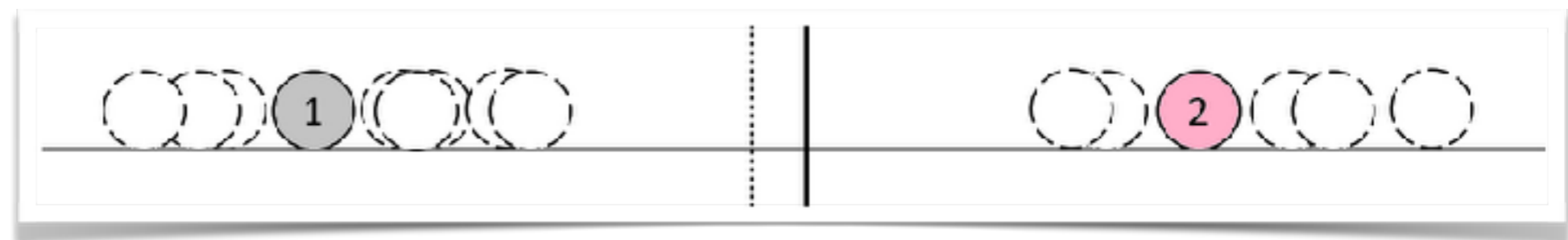
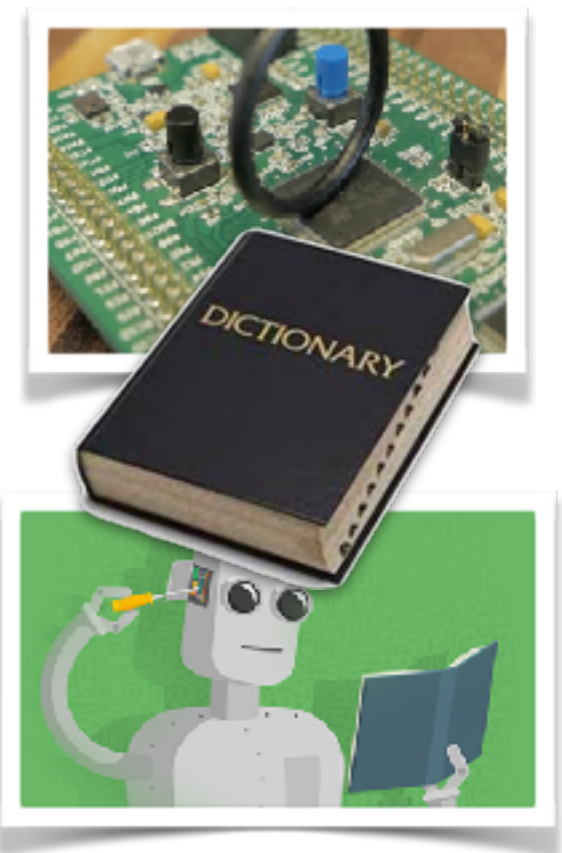
Machine learning techniques for side- channel analysis

Annelie Heuser

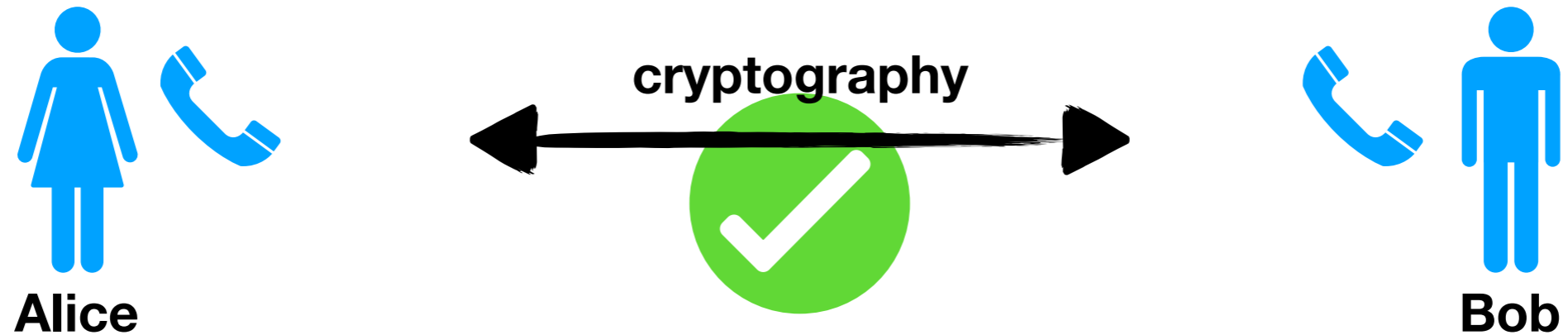


Outline

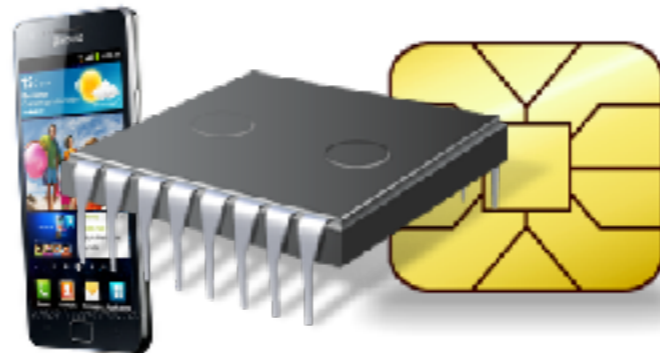
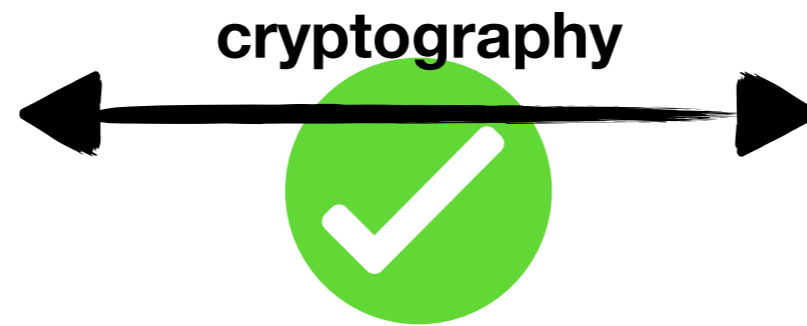
- Side-channel analysis and its terminology
- Dictionary: Side-channel to Machine learning
- When can machine learning be helpful?
- New application: semi-supervised learning



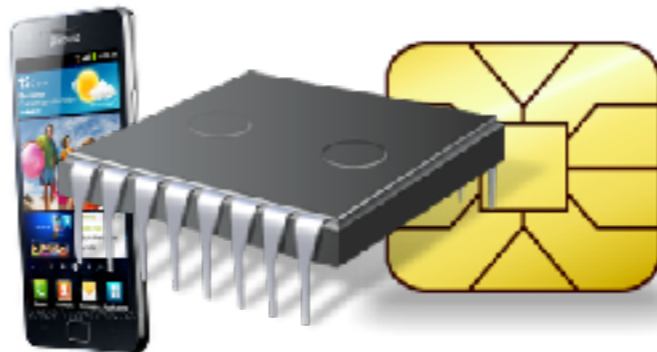
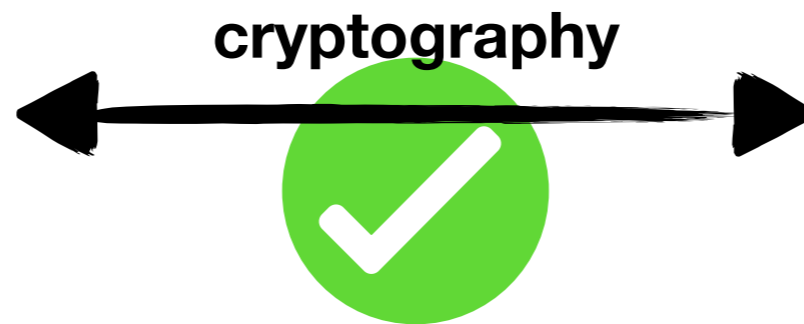
Side-channel analysis



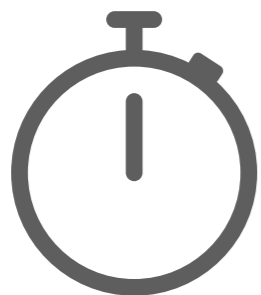
Side-channel analysis



Side-channel analysis



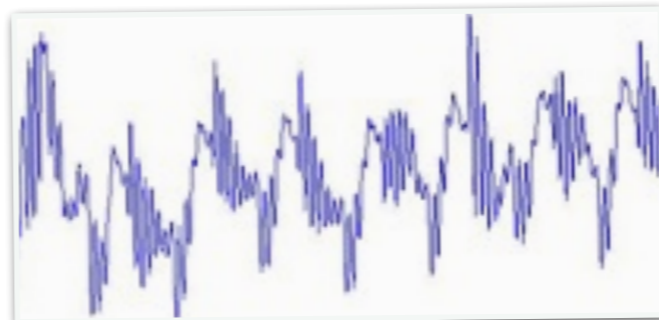
Side-channel information



Time

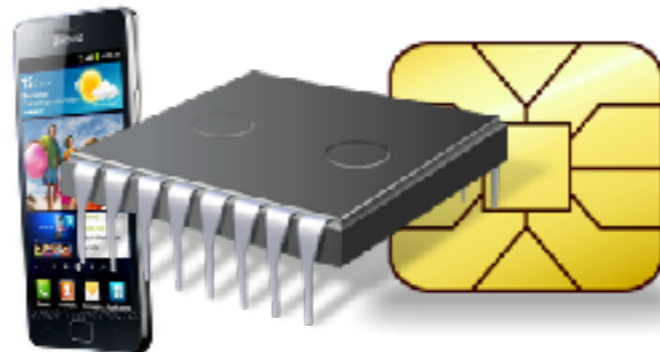
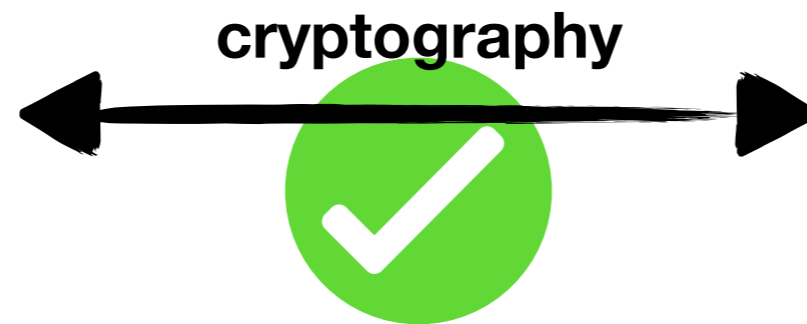


Sound



electromagnetic emanation

Side-channel analysis



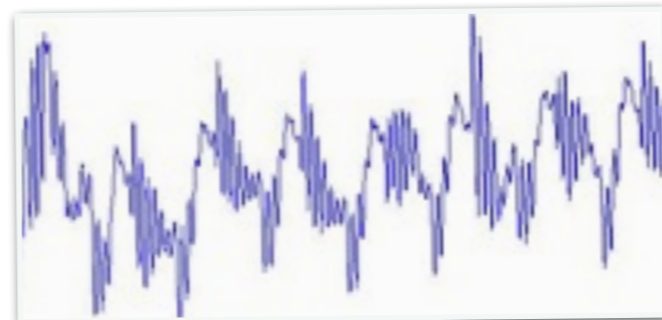
Side-channel information



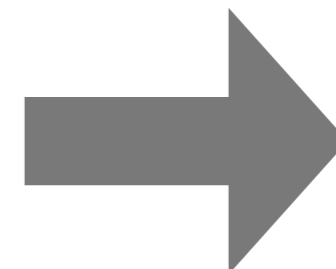
Time



Sound



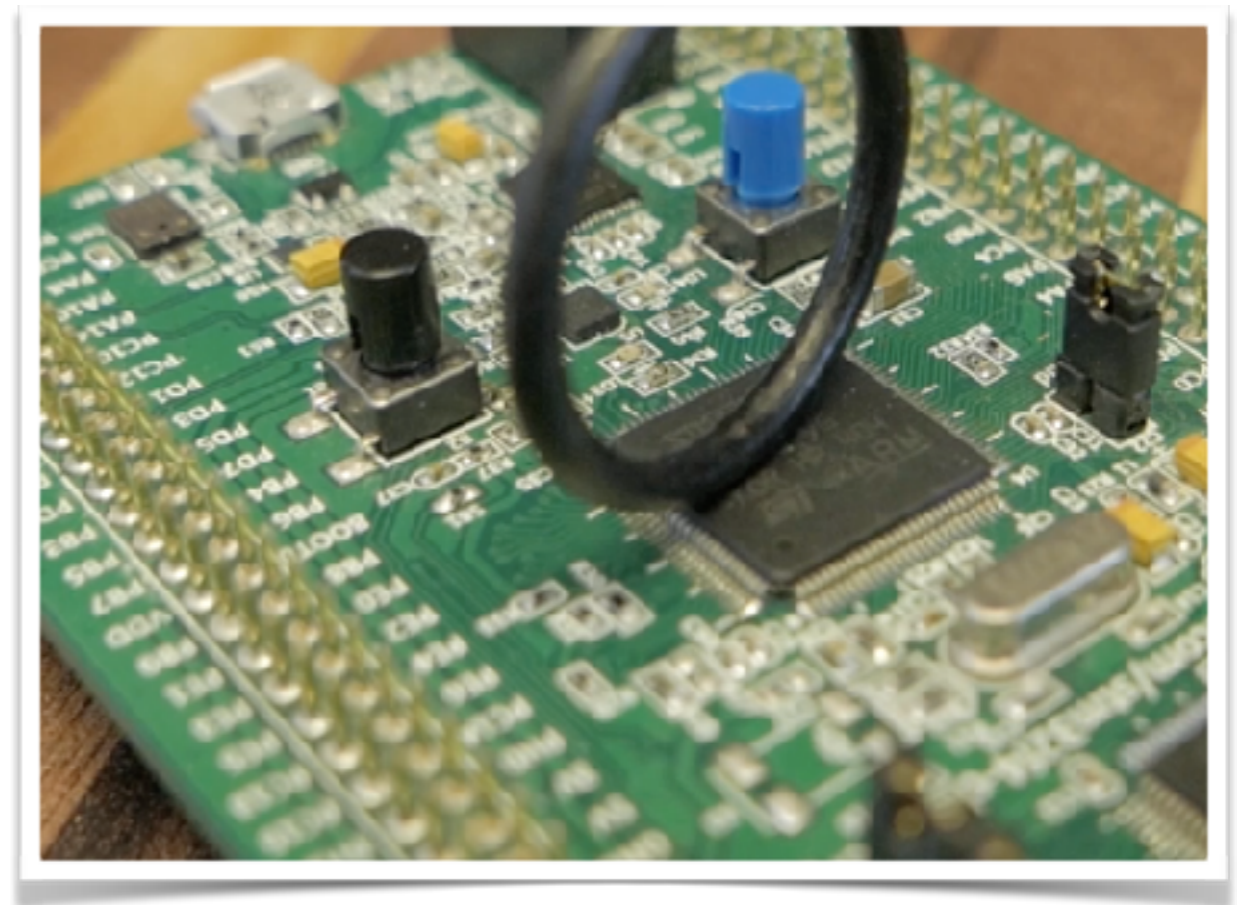
electromagnetic emanation



secret key /
sensitive data

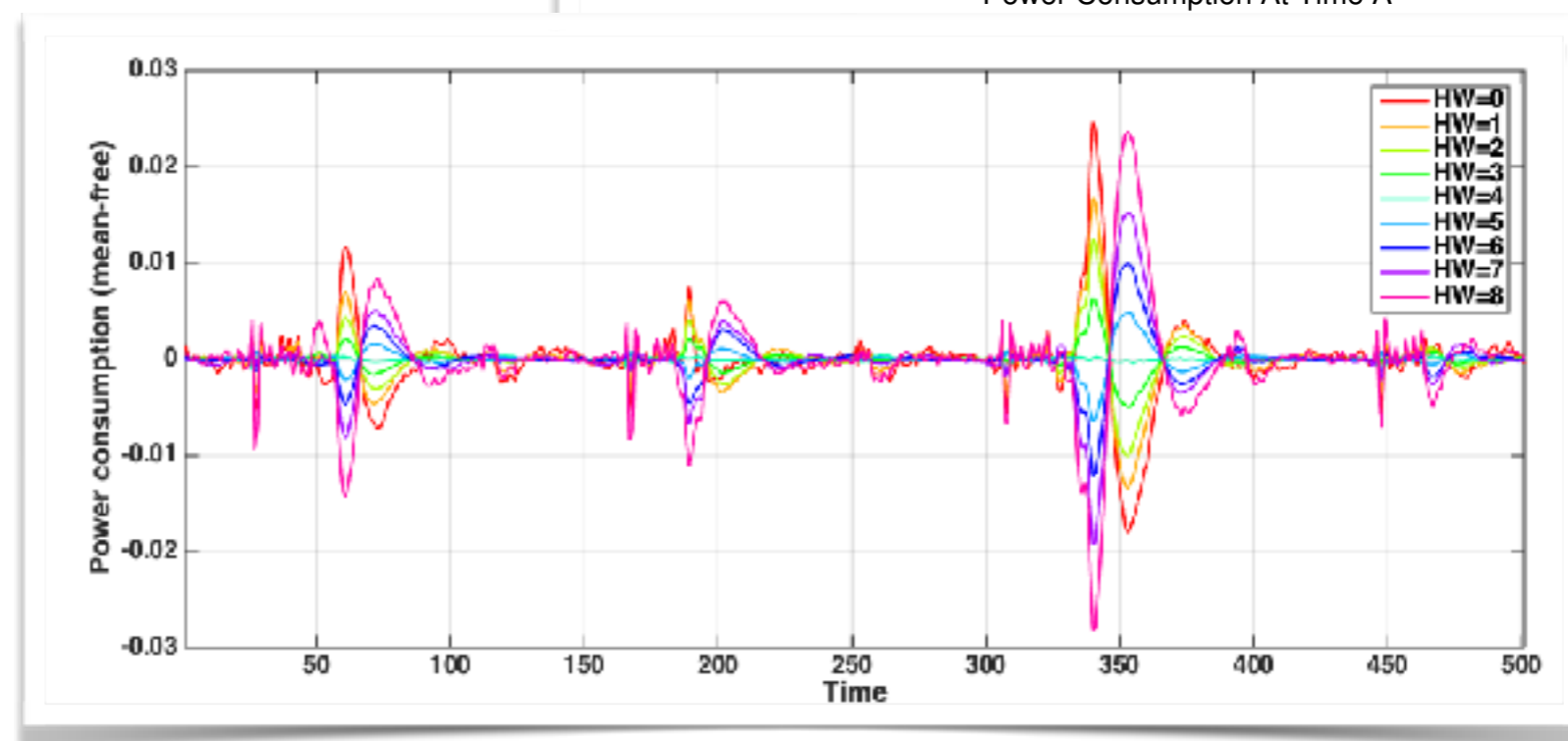
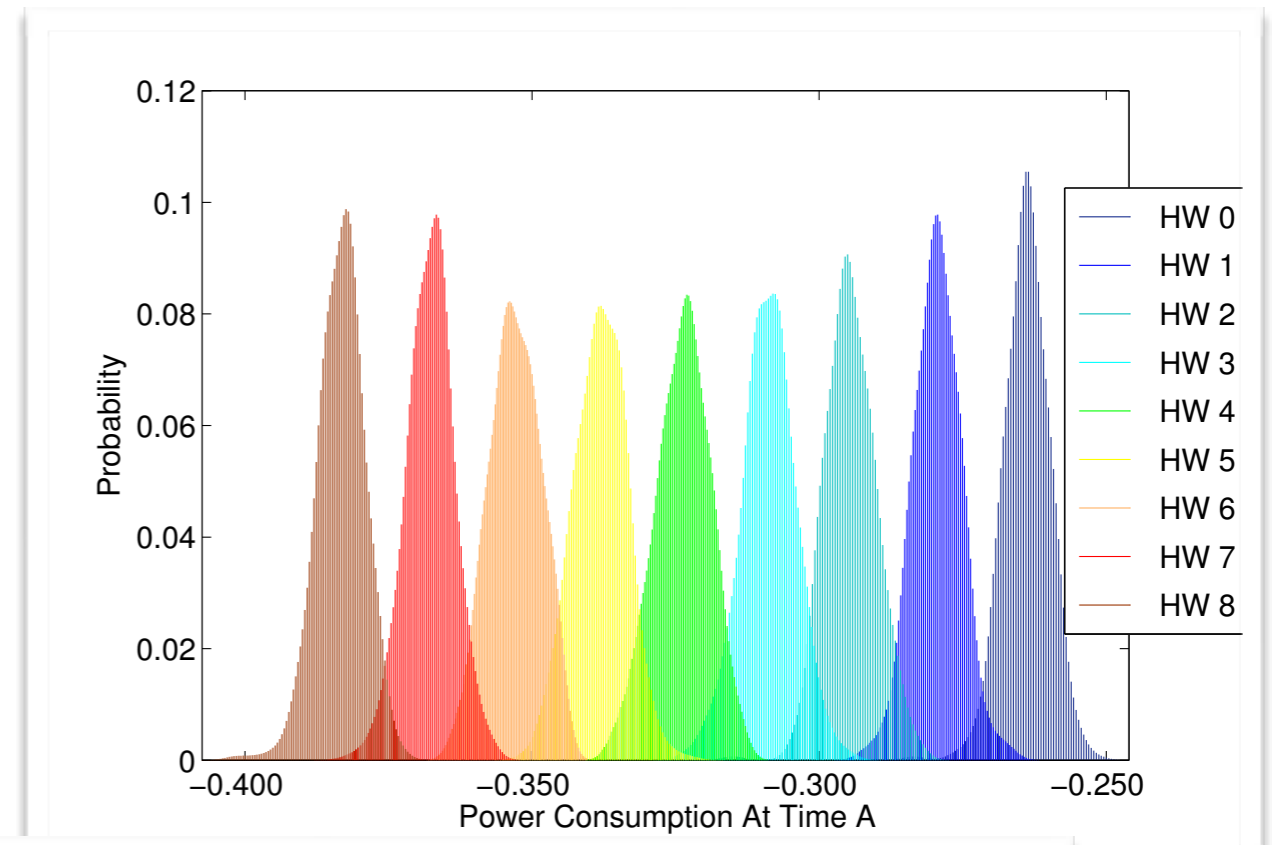
Side-channel analysis

- Measurement setup
 - AES 128
 - attacking SBox operation in the first round
 $S_{\text{box}}(\text{plaintext} \oplus k^*)$
 - key enumeration feasible



Side-channel analysis

- Hamming weight model
- Electromagnetic emanation easily distinguishable regarding HW of intermediate operation



Side-channel attacks

- ...are real in practice



- Beginning 2016: FBI asks Apple to bypass their encryption
- Handful methods to break into the encrypted iPhone
 - software bugs
 - side-channel attacks
 - glitch attack
 - invasive attacks

[edit] (S//NF) Secure key extraction by physical de-processing of Apple's A4 processor

(U) Presenters: [REDACTED] AES cryptographic key "iDevices". This GID key is stored in system non-volatile memory and is used for execution through an exploit that is available with each new release of firmware and hardware.

(S//NF) The Intelligence Community (IC) is highly dependent on a very small number of security flaws, many of which are public, which Apple eventually patches. The following presentation will discuss a method to noninvasively extract the GID key from the A4 silicon. If successful, it would enable decryption and analysis of the boot firmware for vulnerabilities, and development of associated exploits across the entire A4-based product-line, which includes the iPhone® 4, the iPod touch® and the iPad®.

(S) Apple relies on component manufacturers to supply design and manufacturing engineering reports for their products. Their data is used to develop and test products.

[edit] (S//NF) Differential Power Analysis on the Apple A4 Processor

(U) Presenters: [REDACTED], and [REDACTED] (U) The Apple A4 processor contains an on-board, AES cryptographic key called the Global ID (GID) that is believed to be shared across all current "iDevices". This GID key is used to un-wrap the keys that decrypt the corresponding boot firmware code stored in system non-volatile memory. Currently, the only way to examine unencrypted boot code is to gain execution through an exploitable software security flaw. However, Apple is quick to address these flaws with each new release of firmware and hardware.

(S//NF) The Intelligence Community (IC) is highly dependent on a very small number of security flaws, many of which are public, which Apple eventually patches. The following presentation will discuss a method to noninvasively extract the GID key from the A4 silicon. If successful, it would enable decryption and analysis of the boot firmware for vulnerabilities, and development of associated exploits across the entire A4-based product-line, which includes the iPhone® 4, the iPod touch® and the iPad®.

(S//NF) Power analysis techniques have proven effective in extracting hardware resident cryptographic information, such as cryptographic keys, from secure processors noninvasively through side-channel methods. We have worked to develop an environment within the iPhone 4 that assists analysts in performing differential power analysis (DPA) attacks against the A4 processor while preserving the functionality of the device. We have studied electromagnetic (EM) emissions that occur during AES operations with the intent of extracting information about the on-chip AES keys. We will discuss the methods used to acquire various measurements from the system and the progress we've made in attempting to extract the GID key from the devices.

Documents released by Snowden: NSA is studying the use of side-channel attacks to break into iPhones

Side-channel attacks

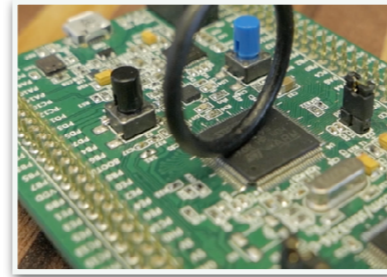
- ...are real in practice
- attacking Philips Hue smart lamps
- side-channel attack revealed the global AES-CCM key used to encrypt and verify firmware updates
- insert malicious update: lamps infect each other with a worm that has the potential to control the device



Paper: Eyal Ronen et al, IoT Goes Nuclear: Creating a ZigBee Chain Reaction

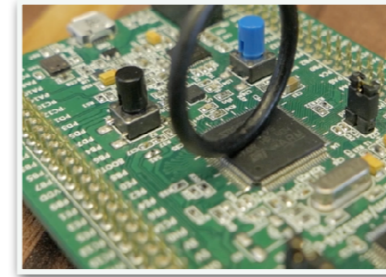
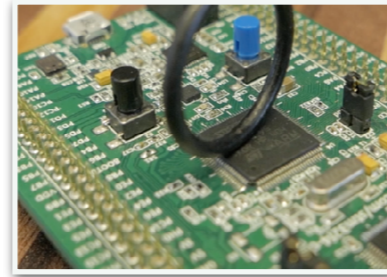
Side-channel analysis

- unprofiled / profiled
- measurement traces
- point in time / point of interest
- intermediate operations / sensitive variable / leakage model
- distinguisher / attack
- success rate / guessing entropy



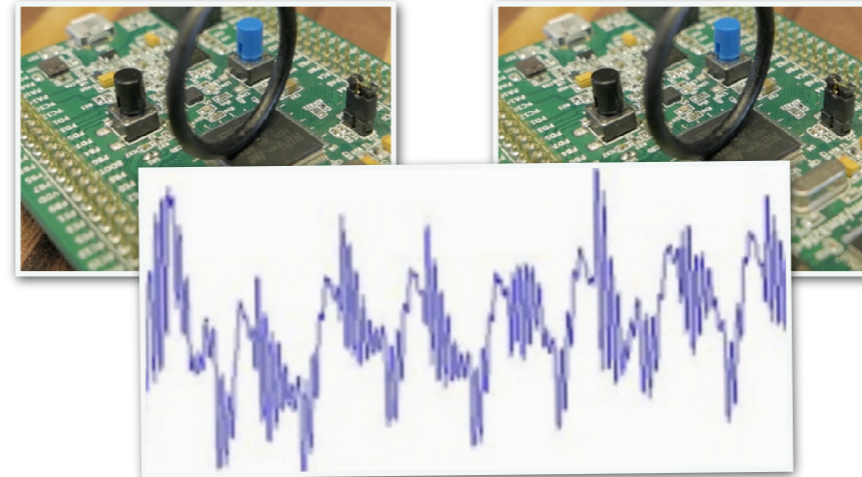
Side-channel analysis

- unprofiled / profiled
- measurement traces
- point in time / point of interest
- intermediate operations / sensitive variable / leakage model
- distinguisher / attack
- success rate / guessing entropy



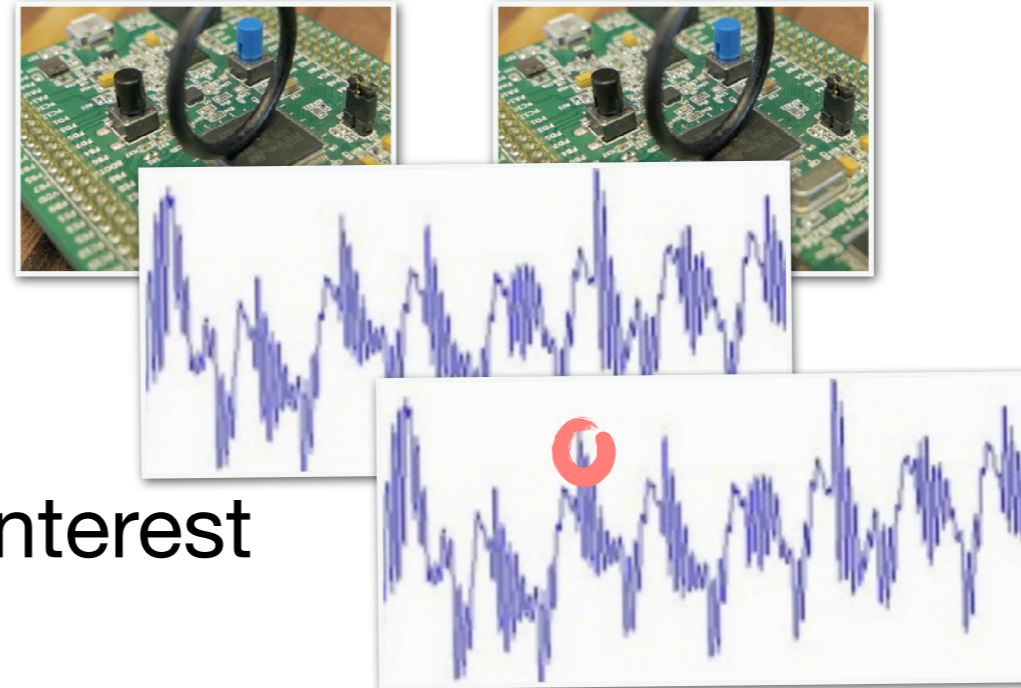
Side-channel analysis

- unprofiled / profiled
- measurement traces
- point in time / point of interest
- intermediate operations / sensitive variable / leakage model
- distinguisher / attack
- success rate / guessing entropy









Side-channel analysis

- unprofiled / profiled
- measurement traces
- point in time / point of interest
- intermediate operations / sensitive variable / leakage model
- distinguisher / attack
- success rate / guessing entropy



Side-channel analysis to machine learning

- unprofiled / profiled  unsupervised / supervised
- measurement trace  data
- point in time / point of interest  feature
- intermediate operations / sensitive variable / leakage model  label
- distinguisher / attack  classification algorithm
- success rate / guessing entropy  accuracy

Machine learning techniques as side-channel attacks

- Input: data, labels
 - points of interest from the measurement trace
 - leakage models (intermediate operations)
- Mainly in supervised scenarios:
support vector machines, random forest, Naive Bayes, deep learning

Machine learning techniques as side-channel attacks

- Input: data, labels
 - points of interest from the measurement trace
 - leakage models (intermediate operations)
- Mainly in supervised scenarios:
support vector machines, random forest, Naive Bayes, deep learning
- Nature of side-channel leakage is still unknown

Machine learning techniques as side-channel attacks

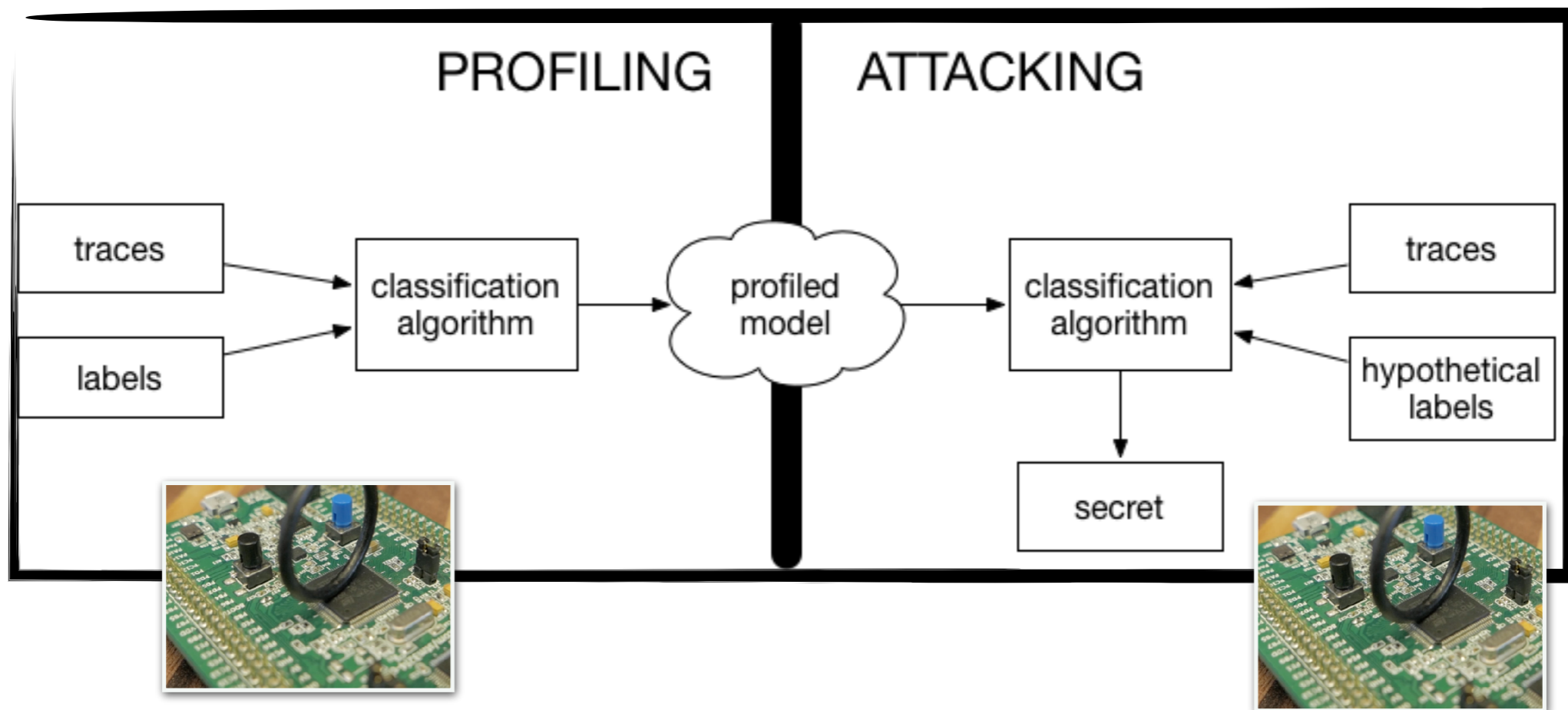
- Input: data, labels
 - points of interest from the measurement trace
 - leakage models (intermediate operations)
- Mainly in supervised scenarios:
support vector machines, random forest, Naive Bayes, deep learning
- Nature of side-channel leakage is still unknown
- Advantages:
 - suitable in “unperfect scenarios”
 - more resistant to imprecisions

Machine learning techniques as side-channel attacks

- Input: data, labels
 - points of interest from the measurement trace
 - leakage models (intermediate operations)
- Mainly in supervised scenarios:
support vector machines, random forest, Naive Bayes, deep learning
- Nature of side-channel leakage is still unknown
- Advantages:
 - suitable in “unperfect scenarios”
 - more resistant to imprecisions
- Disadvantages:
 - time / computational complexity (additional tuning)
 - community is not yet trusting (“only empirical results”)

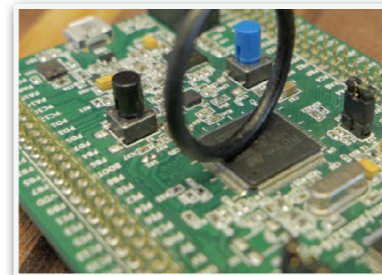
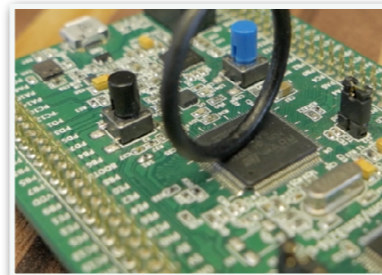
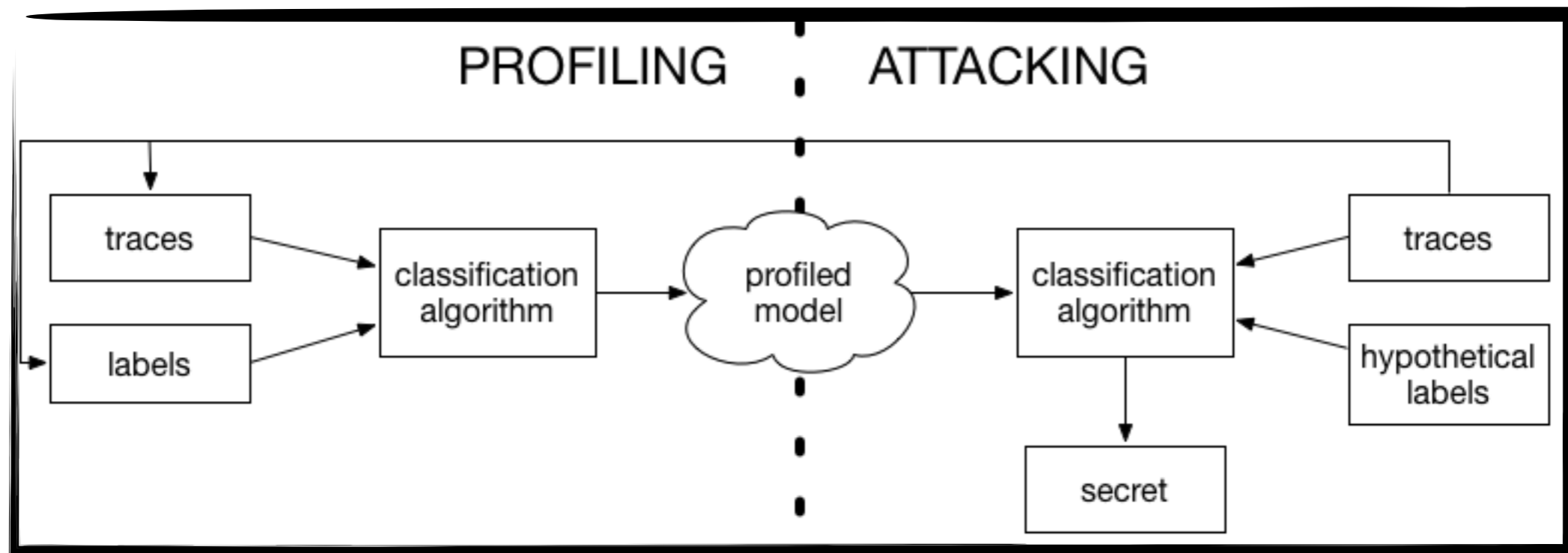
New perspective

- Traditional profiled scenario: realistic?



New perspective

- Semi-supervised learning: a more realistic assessment



Semi-supervised learning

- Techniques for label prediction:
 - self-training
 - label spreading
- Classification algorithms:
 - Support vector machines
 - Naive Bayes
 - Template attack (standard + pooled version)

Semi-supervised learning

- Techniques for label prediction:
 - self-training
 - label spreading
- Classification algorithms:
 - Support vector machines
 - Naive Bayes
 - Template attack (standard + pooled version)
- Datasets (13 k in total)
 - 100 labeled + 12.9k unlabeled
 - 500 labeled + 12.5k unlabeled
 - 1k labeled + 12k unlabeled
 - 3k labeled + 10k unlabeled
 - 5k labeled + 8k unlabeled
 - 10k labeled + 3k unlabeled

Semi-supervised learning

- Techniques for label prediction:
 - self-training
 - label spreading
- Classification algorithms:
 - Support vector machines
 - Naive Bayes
 - Template attack (standard + pooled version)
- Datasets (13 k in total)
 - 100 labeled + 12.9k unlabeled
 - 500 labeled + 12.5k unlabeled
 - 1k labeled + 12k unlabeled
 - 3k labeled + 10k unlabeled
 - 5k labeled + 8k unlabeled
 - 10k labeled + 3k unlabeled

Semi-supervised learning

- Supervised

Size	NB	SVM	TA	TA _p
100	61.51	69.07	0.30	45.41
500	65.93	82.70	0.34	68.93
1k	64.81	86.56	1.33	73.14
3k	67.20	90.81	5.23	74.86
5k	67.86	92.00	2.83	75.79
10k	68.09	93.26	0.39	77.24
13k	68.36	93.71	75.31	77.74

- Semi-supervised

Size	NB	SVM	TA	TA _p	NB	SVM	TA	TA _p
	self-training				label spreading			
100+12.9k	59.04	69.02	58.89	67.55	29.66	24.96	18.76	21.08
500+12.5k	66.15	82.81	56.62	76.86	65.51	81.13	58.77	74.49
1k+12k	68.13	87.10	44.20	78.28	67.73	84.06	7.10	76.55
3k+10k	68.32	90.54	53.04	78.09	68.66	91.83	66.60	77.41
5k+8k	68.08	92.28	46.44	78.35	68.79	91.83	3.24	77.95
10k+3k	68.67	93.58	73.76	77.91	68.7	93.53	49.64	77.97

Semi-supervised learning

- *Influence of noise*: in high noise scenarios this approach may not be beneficial, optimal signal-to-noise ratio?
- *Number of measurements*: in which restricted (practical) scenarios semi-supervised learning is beneficial?
- *Number of classes*: what is the amount of classes where label predictions can be beneficial?
- *Misclassification of labels*: how to limit misclassification of labels? which algorithms cope best with misclassification?
- *Generalisation of models*: What are the benefits when considering leakage measurements from different devices and therefore with different leakage distributions?

Questions?

Machine learning techniques for side- channel analysis

Annelie Heuser



annelie.heuser@irisa.fr

Countermeasures

Countermeasures

- Implementation level countermeasures:
 - ◉ masking: adding additional randomness
 - ◉ hiding: adding additional noise, decreasing signal-to-noise ratio
 - ◉ drawbacks: high implementation overhead, depending on cryptographic primitive

Countermeasures

- Implementation level countermeasures:
 - ◉ masking: adding additional randomness
 - ◉ hiding: adding additional noise, decreasing signal-to-noise ratio
 - ◉ drawbacks: high implementation overhead, depending on cryptographic primitive
- Protocol level: Leakage-Resilience
 - ◉ modelling attackers with the capability to monitor side-channel information
 - ◉ require a side-channel secure initialization in order to obtain a fresh session key for every cryptographic operation
 - ◉ drawback: mostly theoretical, not been tested (thoroughly) in practice yet