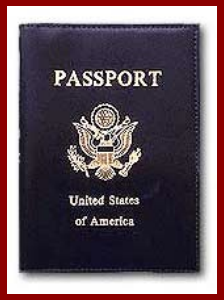
Matching Electronic Fingerprints of RFID Tags Using the Hotelling's Algorithm

Presented to: IEEE Sensors Applications Symposium, Feb. 17, 2009

Nurbek Saparkhojayev and Dale R. Thompson, Ph.D., P.E.
Computer Science and Computer Engineering Dept.
University of Arkansas

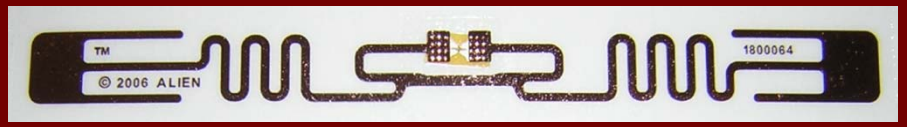
This material is based upon work supported by the National Science Foundation, Cyber Trust area, under Grant No. CNS-0716578.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.



Problem

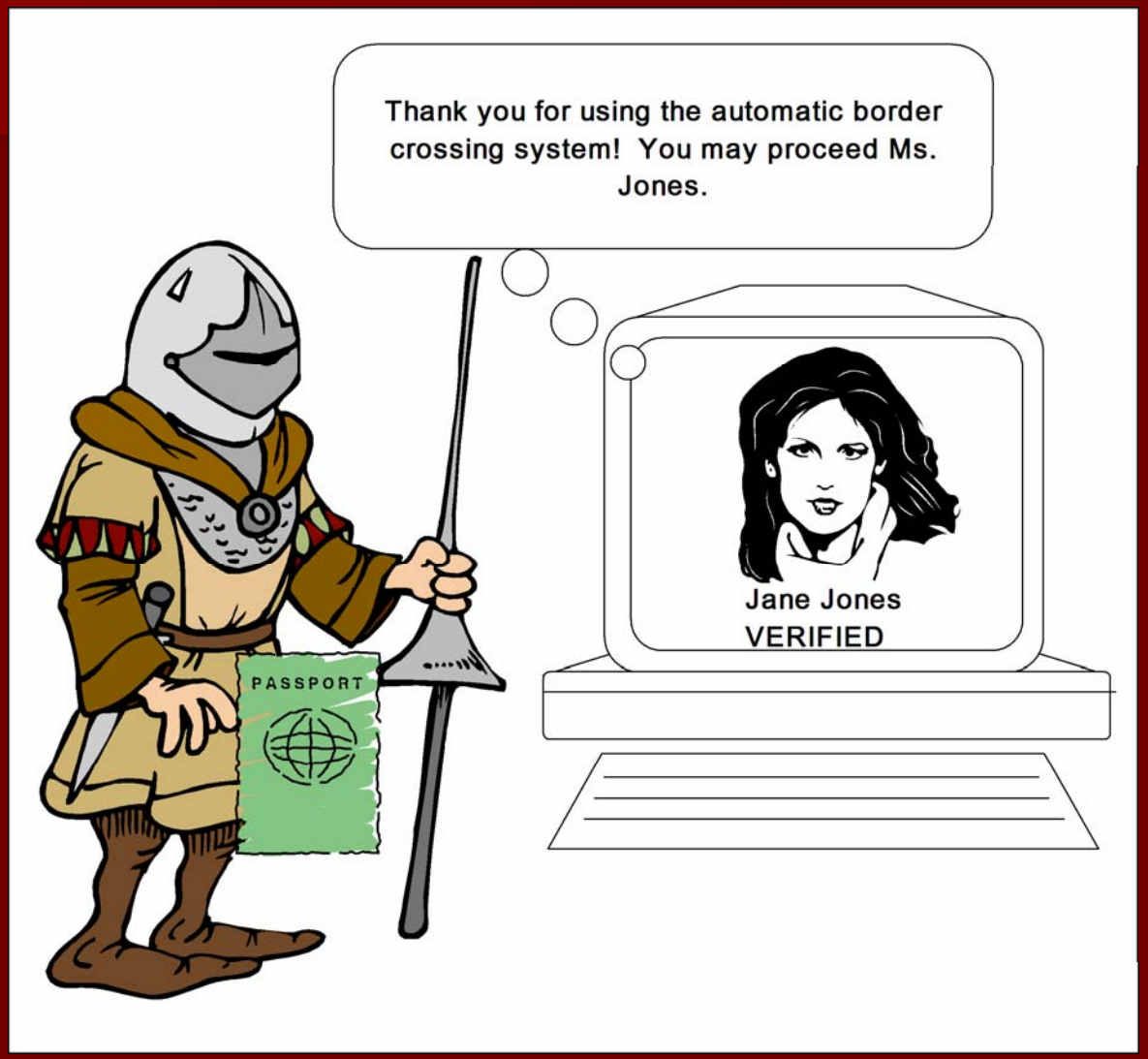
- Counterfeiting travel documents such as ePassport, DHS PASS card, and future drivers licenses
- Travel documents contain radio frequency identification (RFID) tags



Threats to RFID tags

- Cloning the tag
  - Copy contents of tag to another tag
- Side-channel (non-invasive) attacks
  - Monitor certain external parameters such as power consumption, timing delay, or electromagnetic emission
  - Inject noise/faults to the target to cause irregular behaviors

Tag Counterfeiting/Cloning (Spoofing Identity)



Manipulating Data on Passport

- The Hacker's Choice (Oct. 2, 2008)
  - Copied passport
  - Replaced picture with Elvis's picture
  - Turned off active verification
  - Tested on boarding pass machine
  - http://freeworld.thc.org/thc-epassport/
  - http://www.youtube.com/watch?v=4HngStyEm4s
- Used Jeroen van Beek method presented at Black Hat conference

Counterfeiting Mitigation

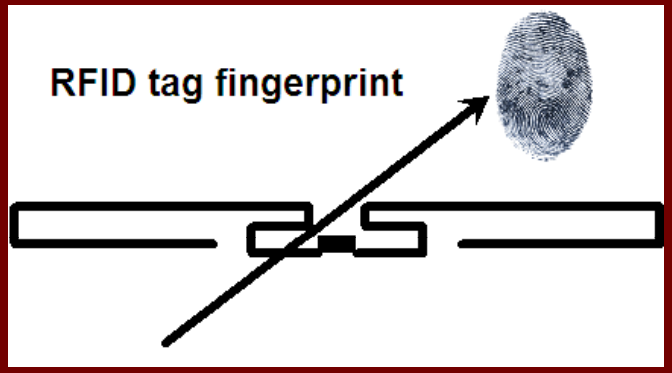
- Tag authentication using cryptography
  - Store secrets on the tag that can be verified
  - Secret keys, symmetric key and public key cryptography
- Physical unclonable functions (PUFs)
- Electronic fingerprint (E-Fingerprint)

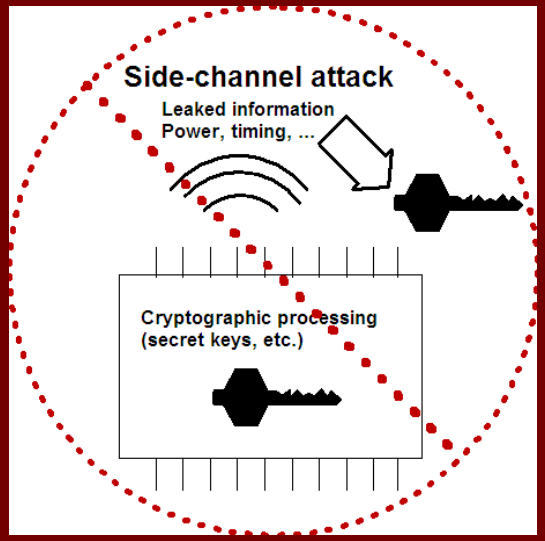
Objective

- Prevent counterfeiting of RFID tags
  - Methods for creating electronic fingerprint based on physical characteristics of tag
  - Digital integrated circuit (IC) design methodology that mitigates power- and timing-based side-channel attacks

Approach

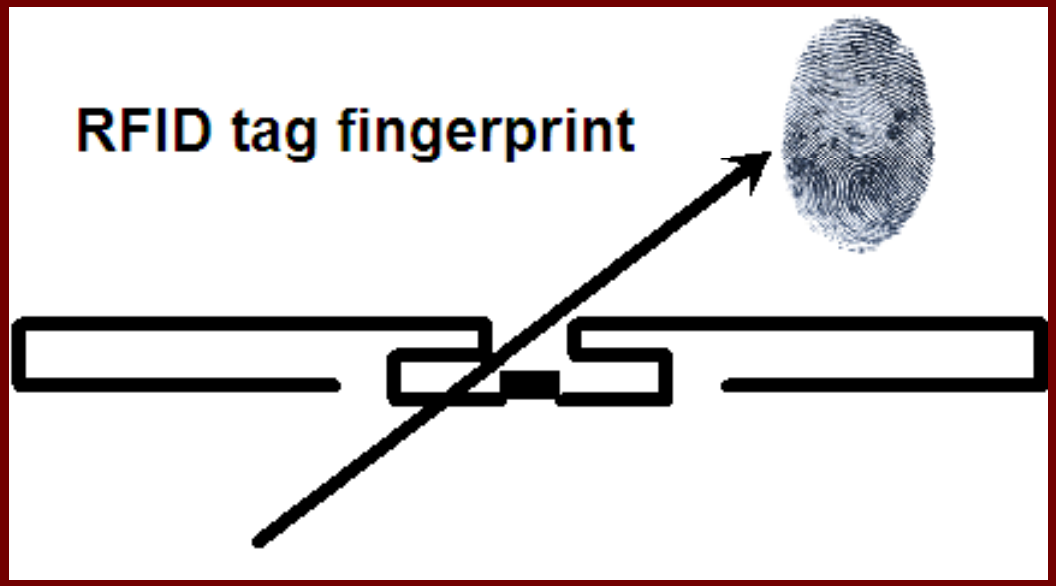
- Electronic fingerprint (e-fingerprint)
  - Authentication becomes a function of what the device "is" in addition to a secret it "knows."
- Digital integrated circuit (IC) design methodology that mitigates power- and timing-based side-channel attacks

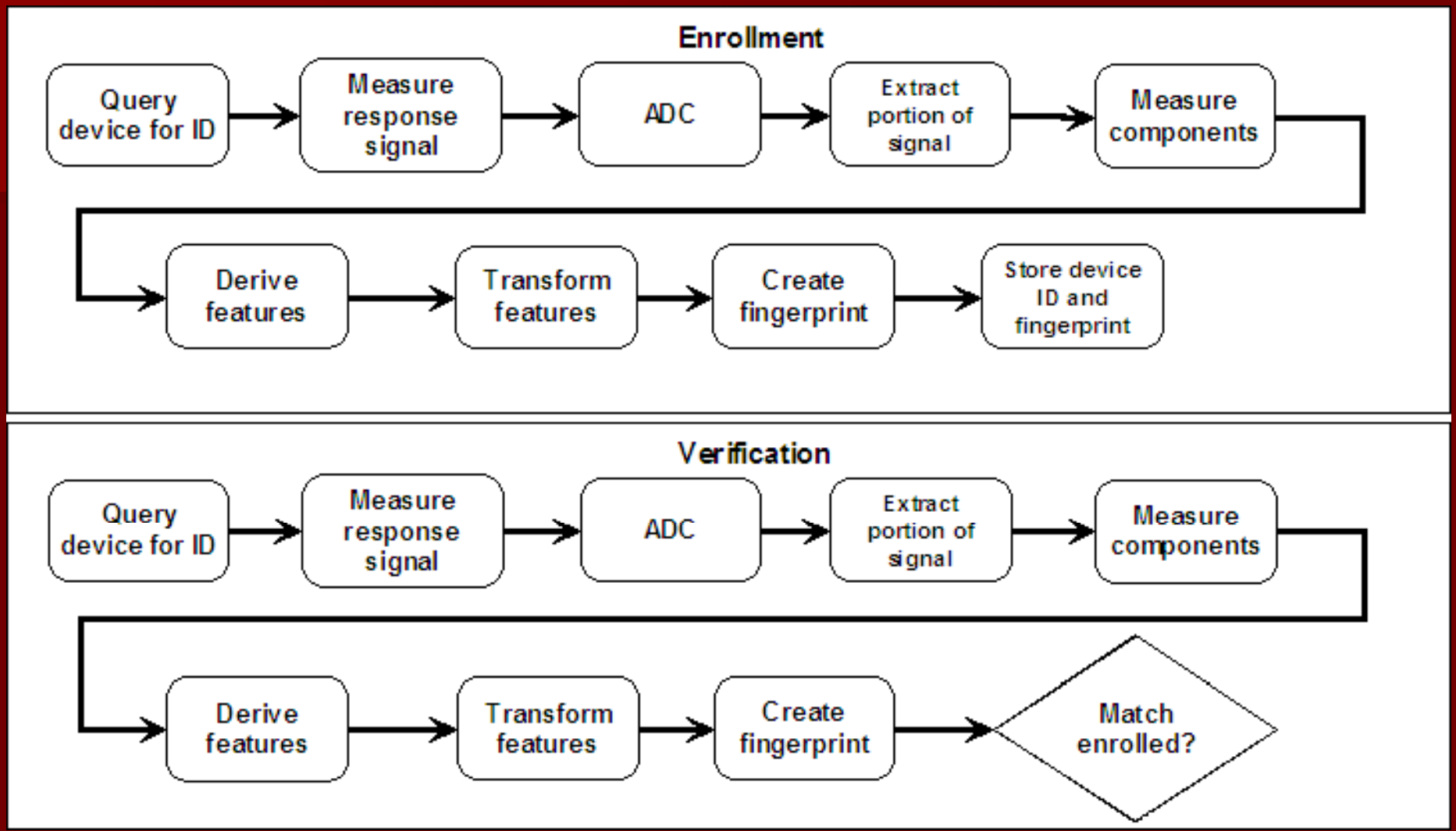




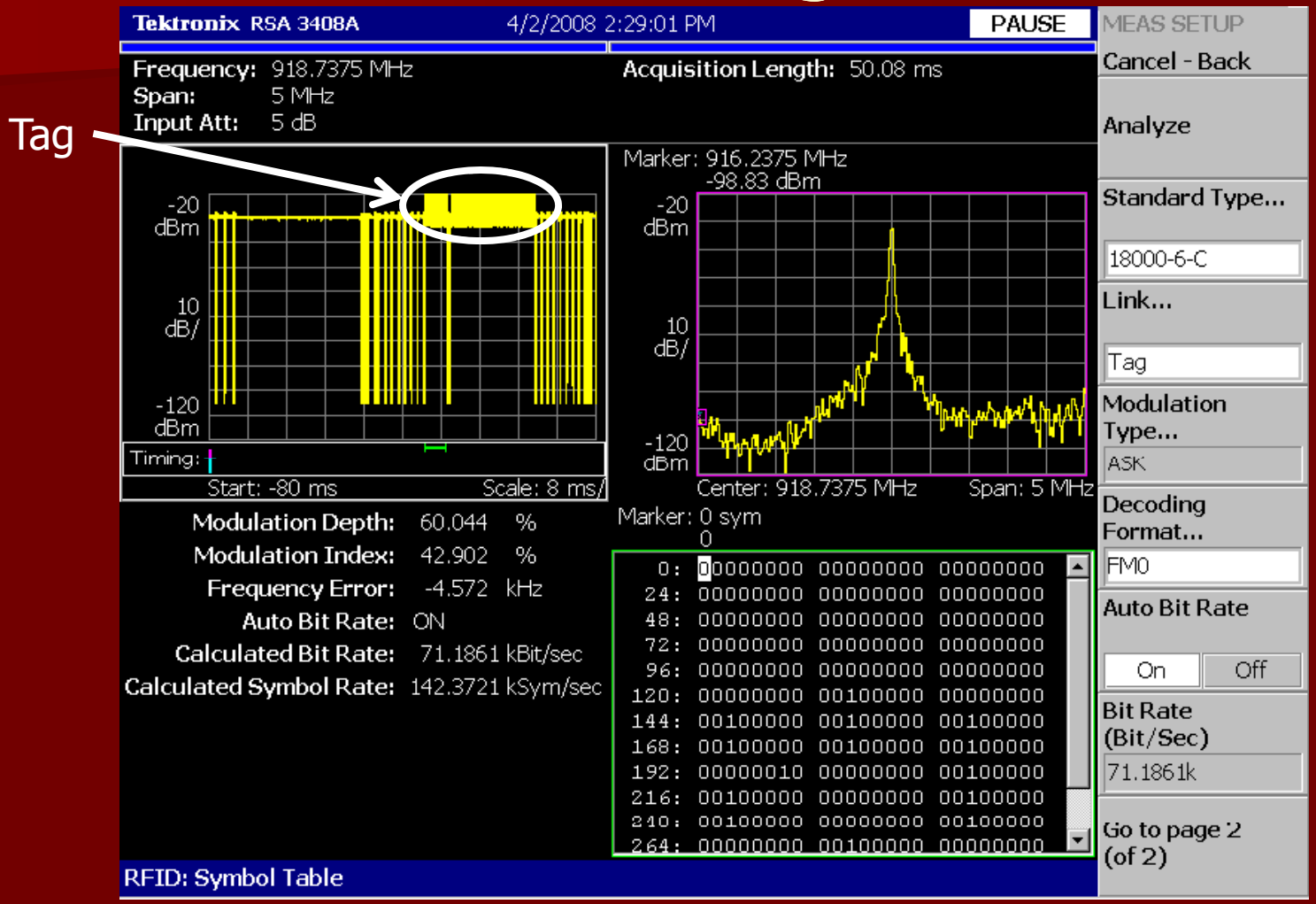
Two-layer security

- Authentication becomes a function of what the device "is" in addition to a secret it "knows."
- Two-layers
  - Cryptography
  - Electronic fingerprint (E-fingerprint)




Enrollment
Query device for ID
Measure response signal
ADC
Extract portion of signal
Measure components
Derive features
Transform features
Create fingerprint
Store device ID and fingerprint
Verification
Query device for ID
Measure response signal
ADC
Extract portion of signal
Measure components
Derive features
Transform features
Create fingerprint
Match enrolled?

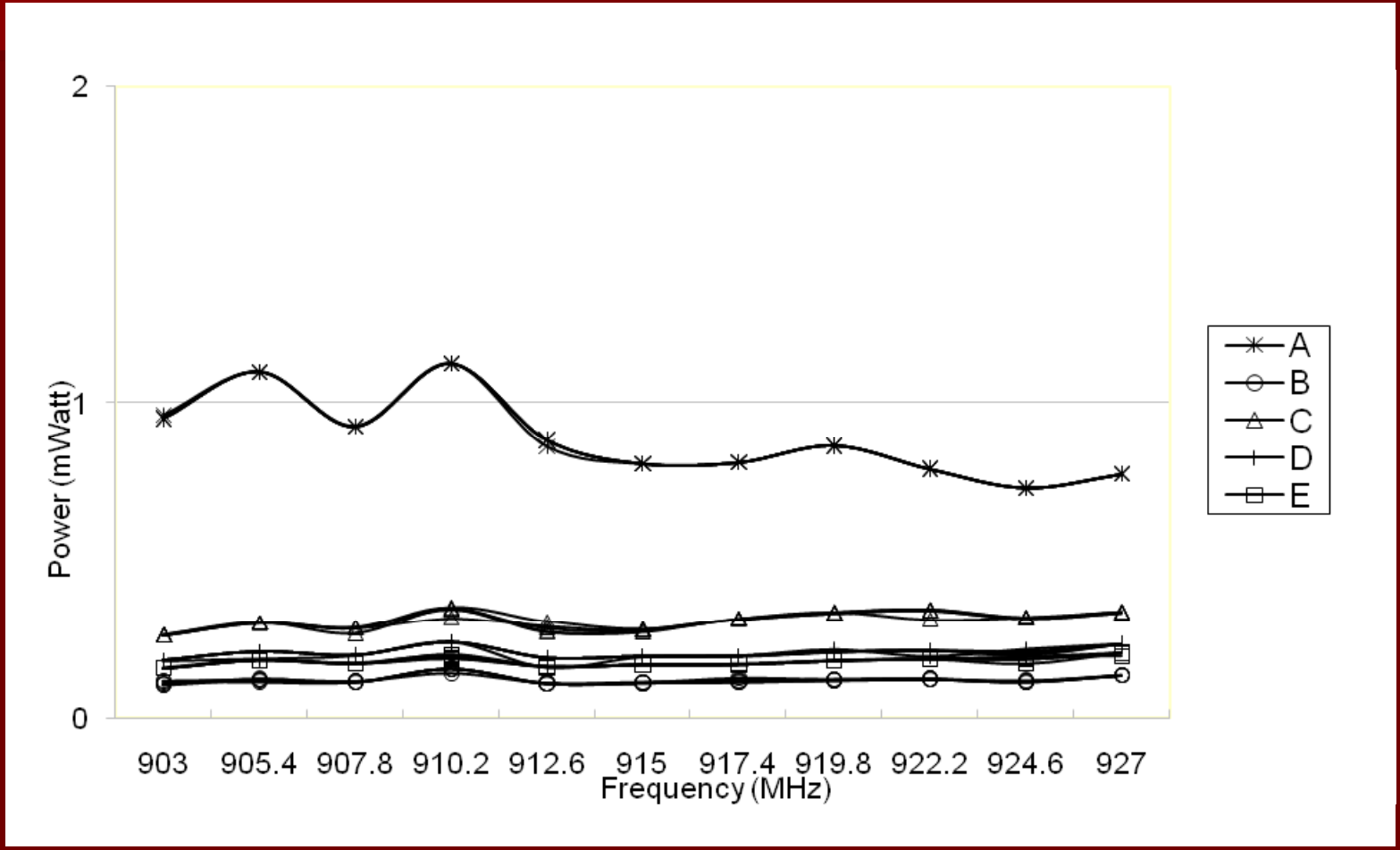
Communication between reader and tag



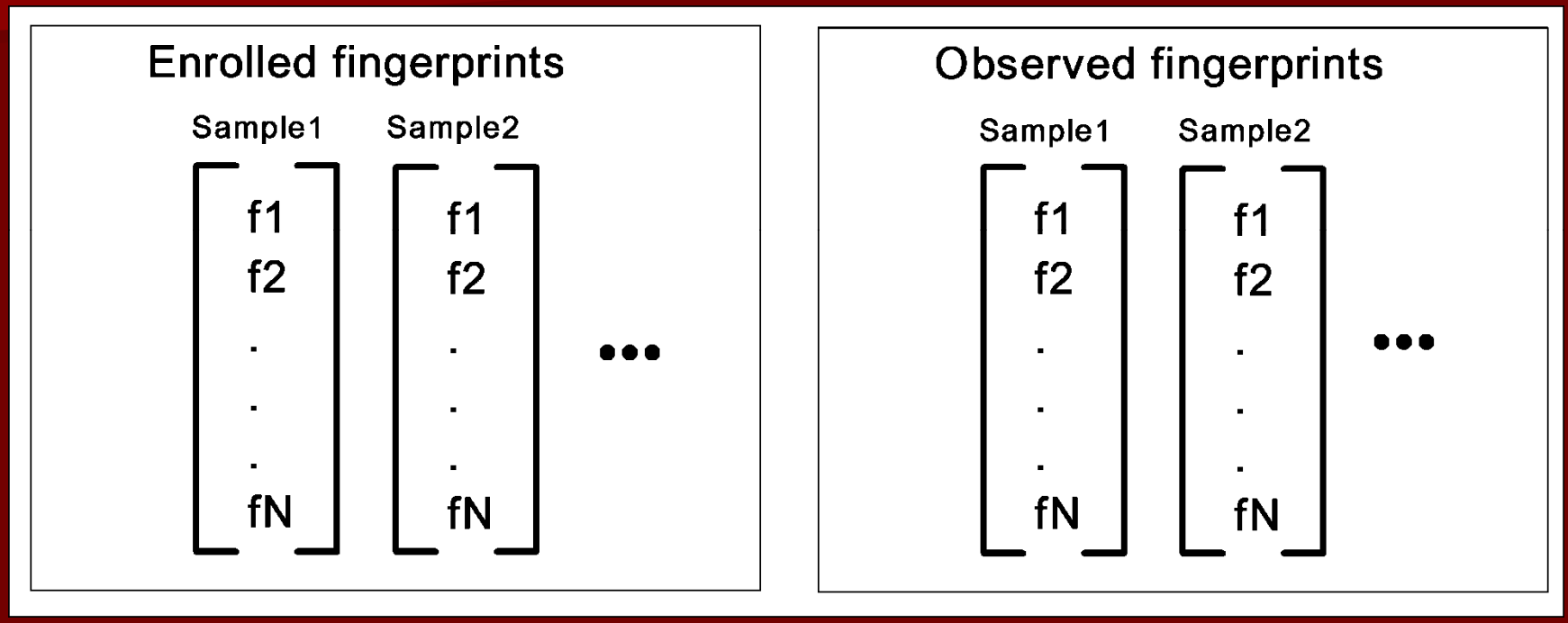
Features

- Minimum power response at multiple frequencies (MPRMF)
- Timing
- Frequency
- Phase
- Transients

Minimum power response measured at multiple frequencies



What will the fingerprint look like?



FAR and FRR

False acceptance rate (FAR)

- Probability that a false identity claim will be accepted
- Type II error
- **Like biometrics, most serious type of error**

False rejection rate (FRR)

- Probability that a true identity claim is falsely rejected
- Type I error

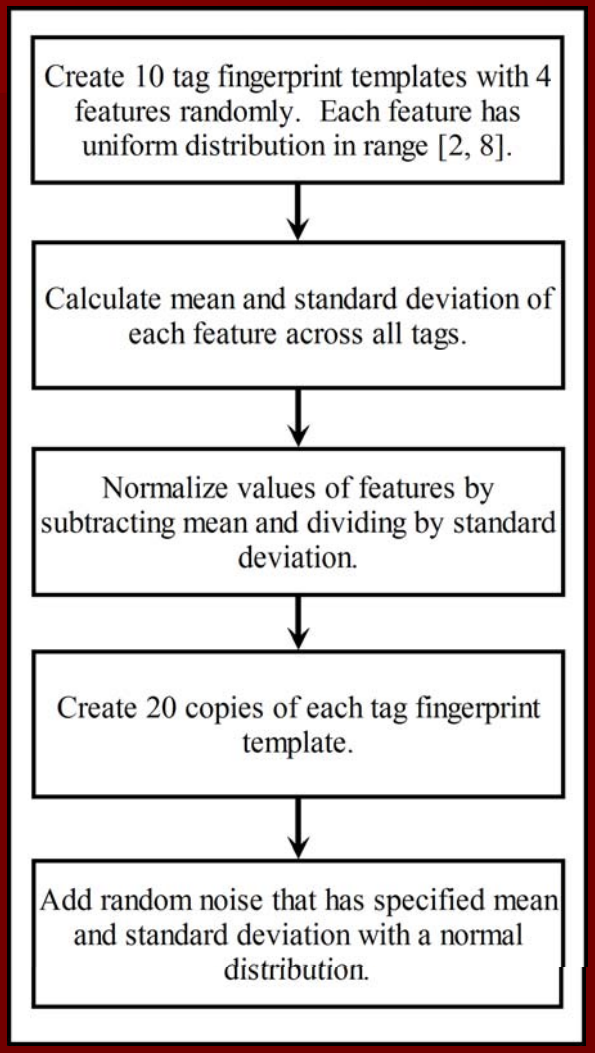
Hotelling's Two-sample T^2 Algorithm

$$T^2 = \frac{n_1 n_2}{n_1+n_2}(\overline{y_1} - \overline{y_2})' S_{pl}^{-1}(\overline{y_1} - \overline{y_2})$$

$$S_{pl} = \left(\frac{1}{n_1+n_2-2}\right)[(n_1-1)S_1 + (n_2-1)S_2]$$

$$\left[\frac{n_1+n_2-p-1}{(n_1+n_2-2)p}\right] T^2 = F_\alpha(p, n_1+n_2-p-1)$$

Create synthetic tag fingerprints



Parameters

- p = 4 = number of features
- n1 = n2 = 20 = number of samples
- alpha = 0.025 (95% confidence level)
- If T^2 > 13.81, assume fingerprints are different

$$T^2 > \left[\frac{(n_1+n_2-2)p}{n_1+n_2-p-1}\right] F_\alpha(p, n_1+n_2-p-1)$$

Case 1: Compare fingerprint of tag 0 with all other fingerprints at varying noise levels (mean = 0)

Comparison of tag 0 with tag#	T^2 for std. dev. 0.5	T^2 for std. dev. 0.75	T^2 for std. dev. 1.0	T^2 for std. dev. 1.25	T^2 for std. dev. 1.5
1	230.85	127.28	73.85	49.06	35.76
2	611.34	262.72	145.38	91.55	62.74
3	129.35	86.51	50.91	34.30	25.08
4	218.95	65.28	38.89	26.61	19.87
5	23.13	28.10	16.86	11.96	9.51
6	122.02	134.23	84.94	61.22	47.66
7	109.31	31.58	15.84	11.13	8.11
8	403.14	145.35	82.72	53.72	38.02
9	242.76	105.05	50.98	27.80	16.31

Table 6. Matching the fingerprint of tag 0 against other tag fingerprints with noise of mean 0 and standard deviation equal to 1.25.

Tag0 against Tag#	T^2 and $\sigma = 1.25$	$\left[\frac{(38)4}{35}\right] F_{\alpha=0.025}(4,35)$	Match
1	49.06	13.81	No
2	91.55	13.81	No
3	34.30	13.81	No
4	26.61	13.81	No
5	11.96	13.81	Yes
6	61.22	13.81	No
7	11.13	13.81	Yes
8	53.72	13.81	No
9	27.80	13.81	No

Table 8. FAR for noise levels with zero mean and five standard deviation values

Standard deviations, σ	False Acceptance Rate (FAR)
0.50	0%
0.75	0%
1.00	0%
1.25	22%
1.50	22%

Case 2: A single tag fingerprint with std. dev. 1.50 compared against itself at noise levels with different means

Noise level mean	T^2 values for six different random fingerprints	$\left[\frac{(38)4}{35}\right] F_{\alpha=0.025}(4,35)$	Average matching rate, %
0.25	2.00, 5.93, 3.27, 3.27, 4.92, 6.16	13.81	100
0.50	7.98, 12.61, 4.29, 8.77, 12.77, 7.96	13.81	100
0.75	17.97, 22.71, 7.29, 17.45, 25.11, 12.29	13.81	33
1.00	31.90, 36.25, 12.25, 29.29, 41.95, 19.17	13.81	17

Table 10. FRR of tag0's fingerprint against itself in noise levels with varying means and standard deviation 1.50 averaged over six runs.

Mean	False Rejection Rate (FRR)
0.25	0%
0.50	0%
0.75	67%
1.00	83%

Conclusions

- Hotelling's performs well across a large range of standard deviations IF the noise has zero mean
- Modest computations

Future Work

- Apply the algorithm to the measured features instead of the synthetic features
- Apply the algorithm across a much larger set of parameters

Contact Information

Dale R. Thompson, Ph.D., P.E.
Associate Professor
Computer Science and Computer Engineering Dept.
JBHT – CSCE 504
1 University of Arkansas
Fayetteville, Arkansas 72701-1201

Phone: +1 (479) 575-5090
FAX: +1 (479) 575-5339
E-mail: d.r.thompson@ieee.org
WWW: http://comp.uark.edu/~drt/