



RF-DNA and Anti-Counterfeiting

Darko Kirovski

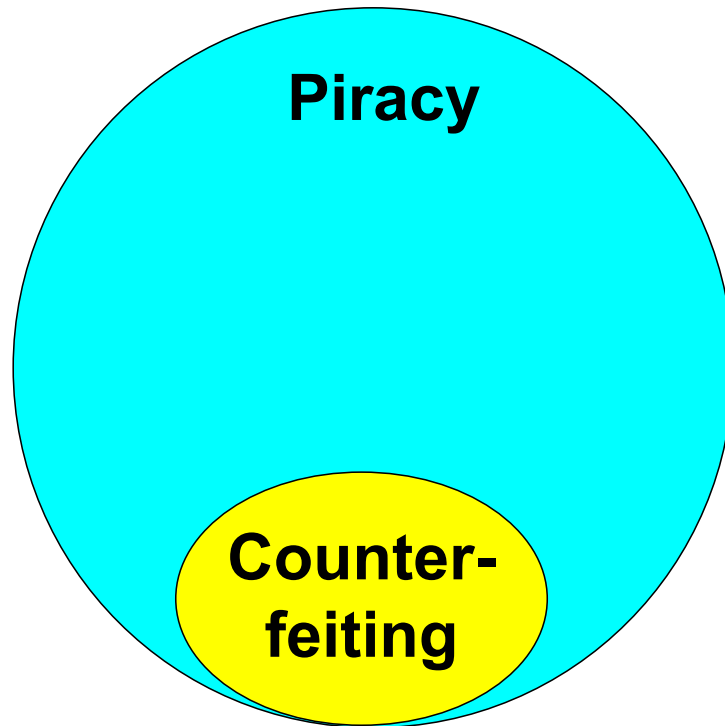
MICROSOFT RESEARCH



Google Scholar entries for a specific year

Source: USPTO

	2006	2005	2004	2003	2002	2001	2000	Patents 2001+
VOIP	107	478	424	285	222	154	117	8105
auction*	98	410	436	319	280	219	221	4421
peer-to-peer	340	1710	1690	1250	765	373	196	9885
sensor network	611	4840	4190	3040	2240	1760	1580	762
transactional memory	43	123	122	120	72	49	39	45
RFID	129	517	324	143	74	36	39	9471
CDMA	167	2190	2740	2430	2120	1740	1820	23827
grid computing	146	824	720	411	187	52	25	678
smart card	34	207	195	183	139	125	102	11270
CMOS	483	4680	4710	3760	3460	2730	2650	43784
video compression	54	447	475	387	411	290	286	4229
NP-hard	138	902	882	709	492	384	321	332
options pricing	62	228	268	262	259	225	176	100
counterfeit	8	47	43	38	28	14	15	2858
piracy	17	76	98	64	57	27	36	1875
public-key	179	912	867	794	558	362	305	2345
operating system	464	2530	2460	2480	1980	1630	1600	93512
compiler	526	1860	1800	1750	1340	1110	1190	10491
buffer overflow	58	308	314	295	216	188	174	1629
race condition	18	79	57	59	37	27	42	722
ddos	36	142	132	125	60	32	15	289
denial of service	112	546	553	556	306	200	168	0
TCP	391	2740	2830	2750	2170	1720	1480	43947
t-cell	328	2230	543	334	195	141	147	19373
cholesterol	264	772	633	414	186	156	277	30957



- ◆ Example of Viral Marketing via piracy:
LOUIS VUITTON
 - 1% authentic
 - 18% of all seized counterfeits in EU

- ◆ **Piracy**

- Both sides know product is not genuine

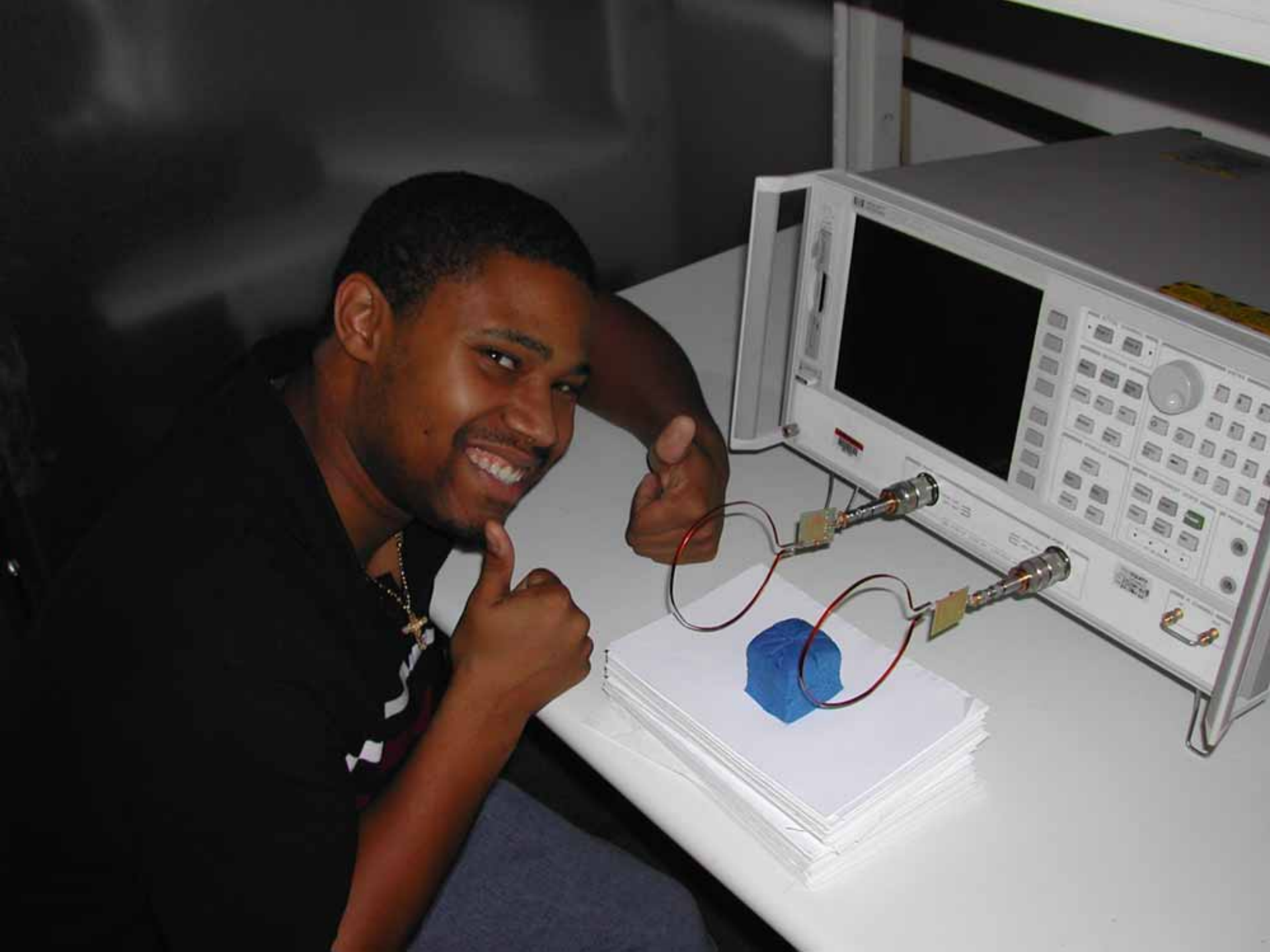
- ◆ **Counterfeiting**

- Seller tricks buyer into believing product is genuine

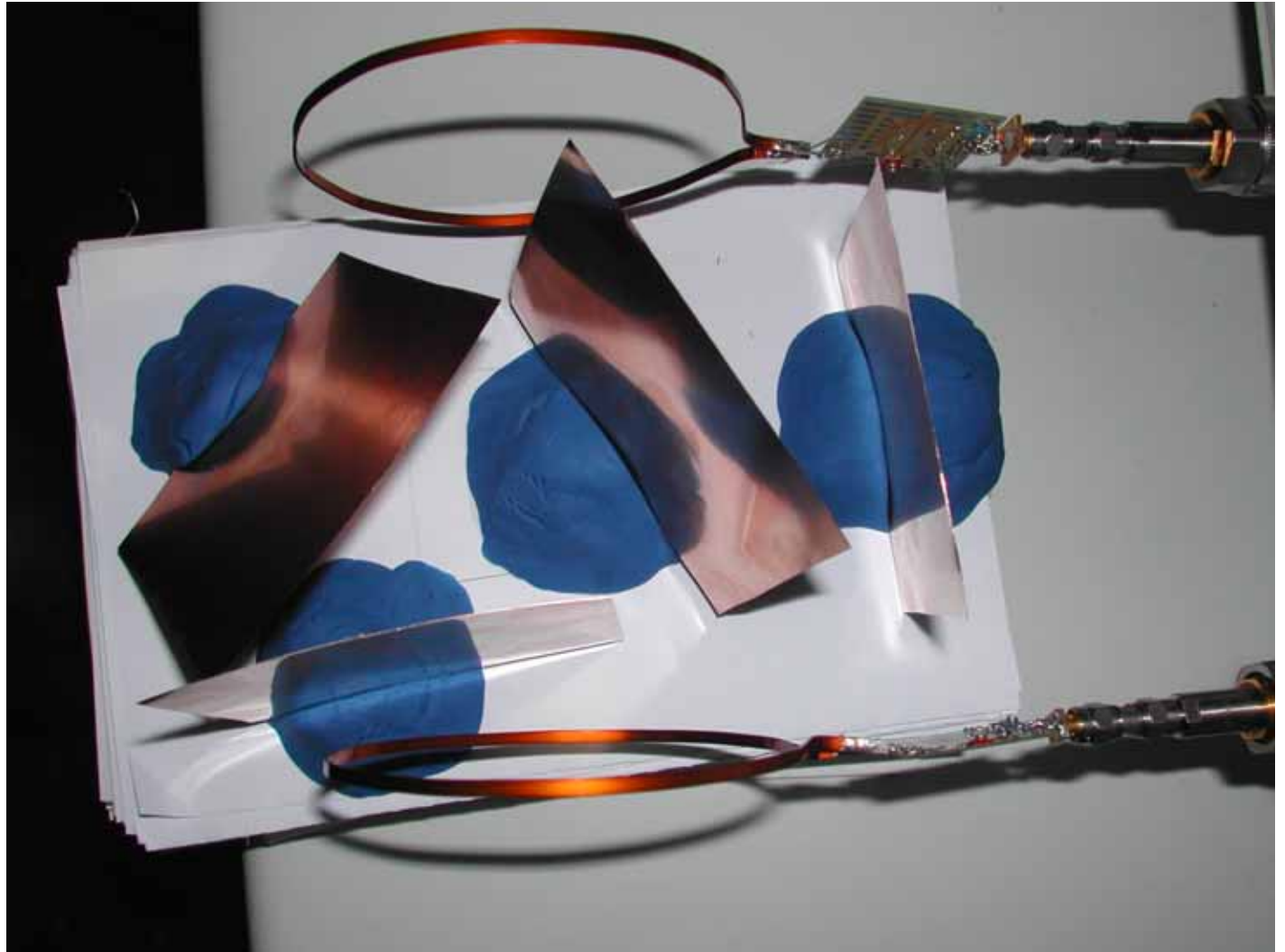


Anti-Counterfeiting Technologies for the Physical World

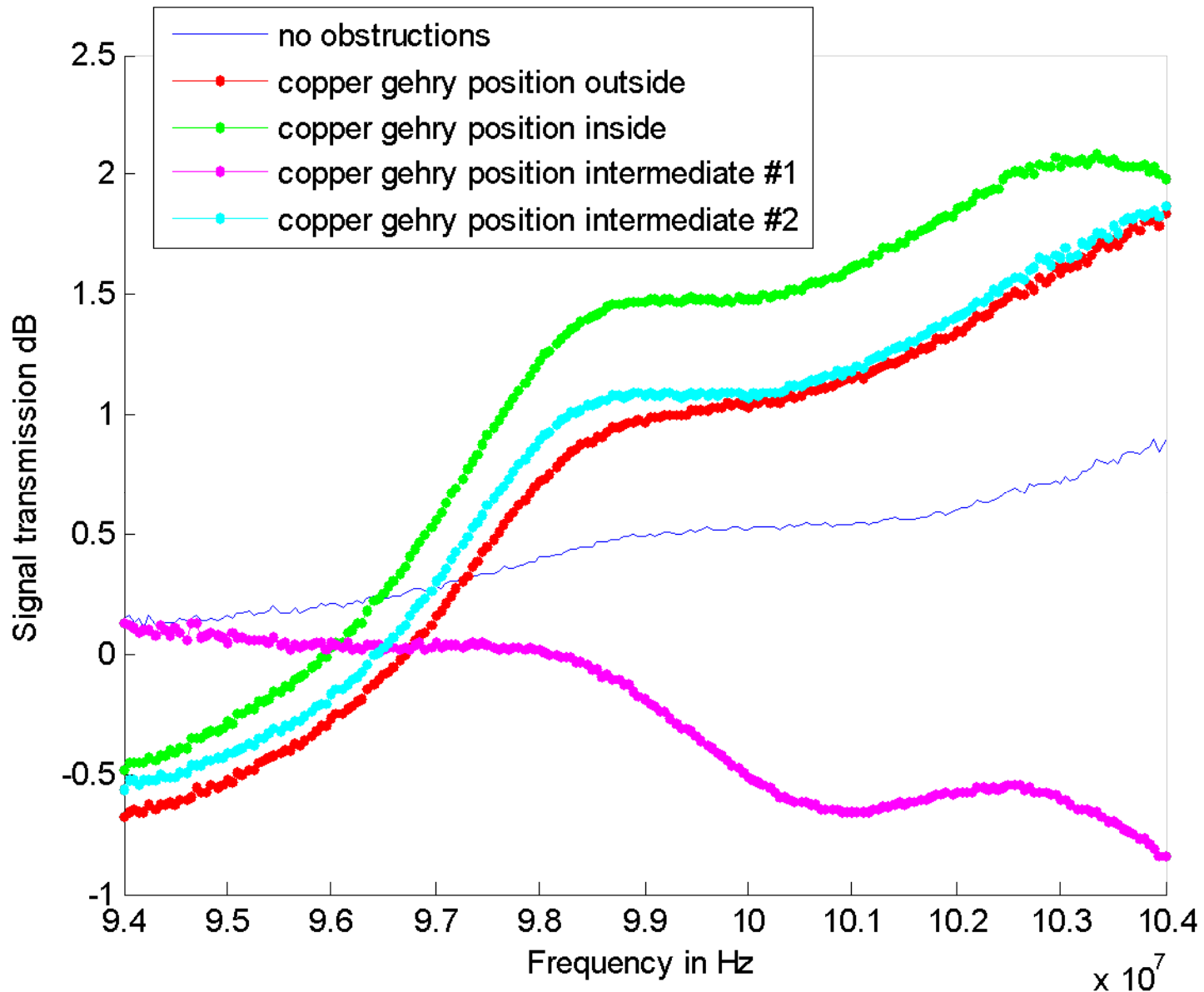


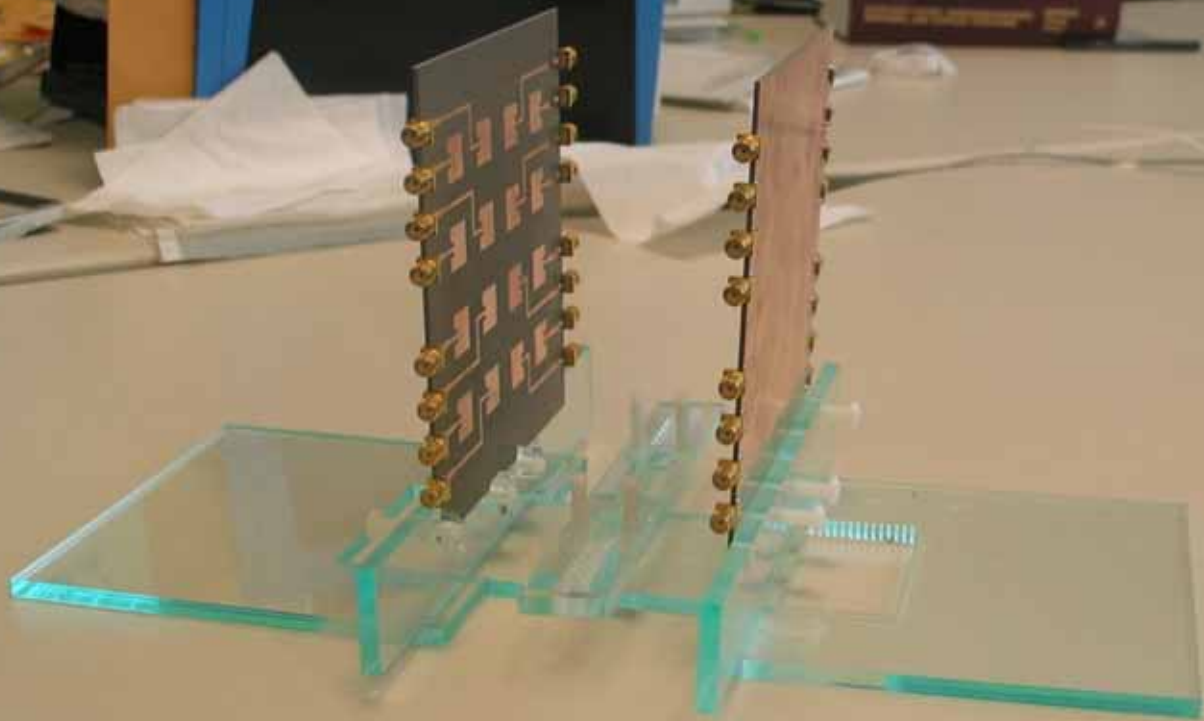


Experimental Design Circular Loop

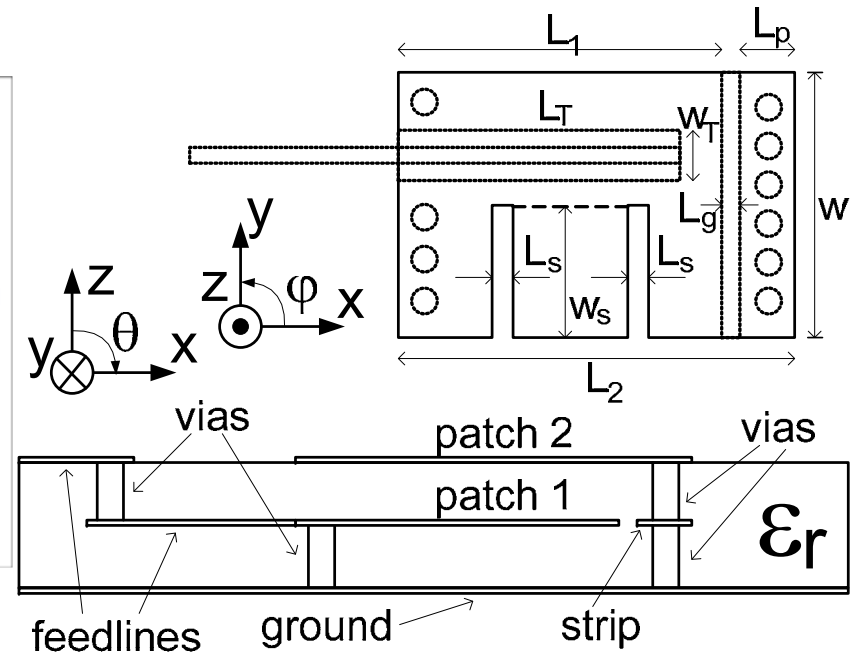
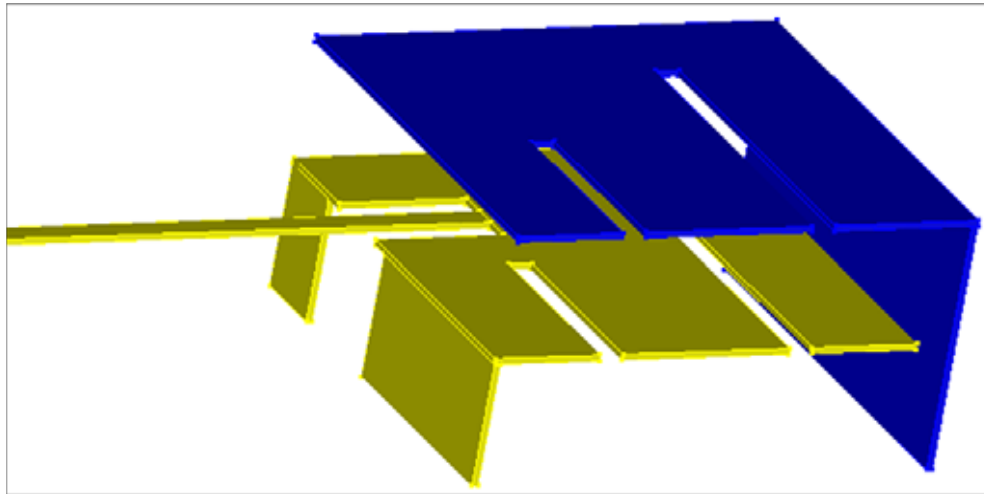


Simulations





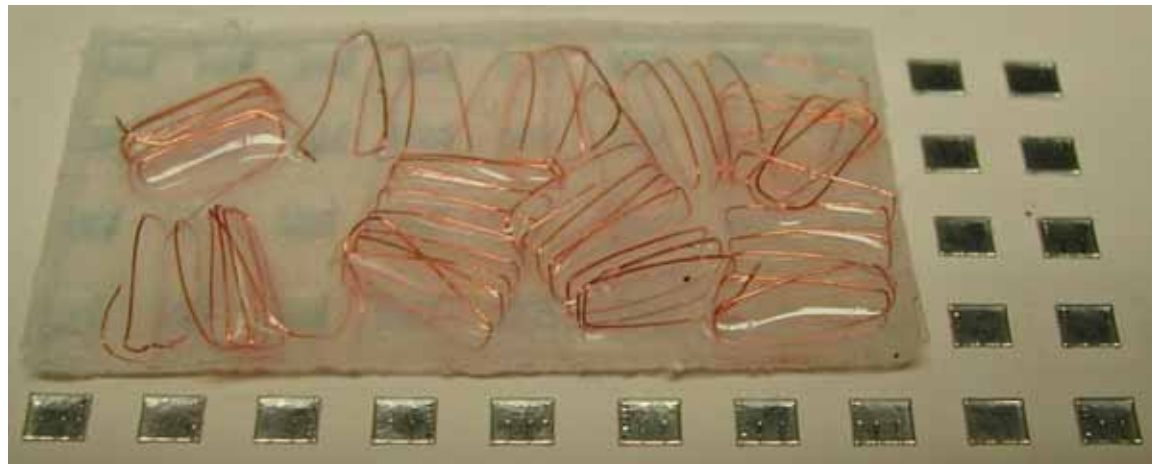
Miniaturized Antenna Structure



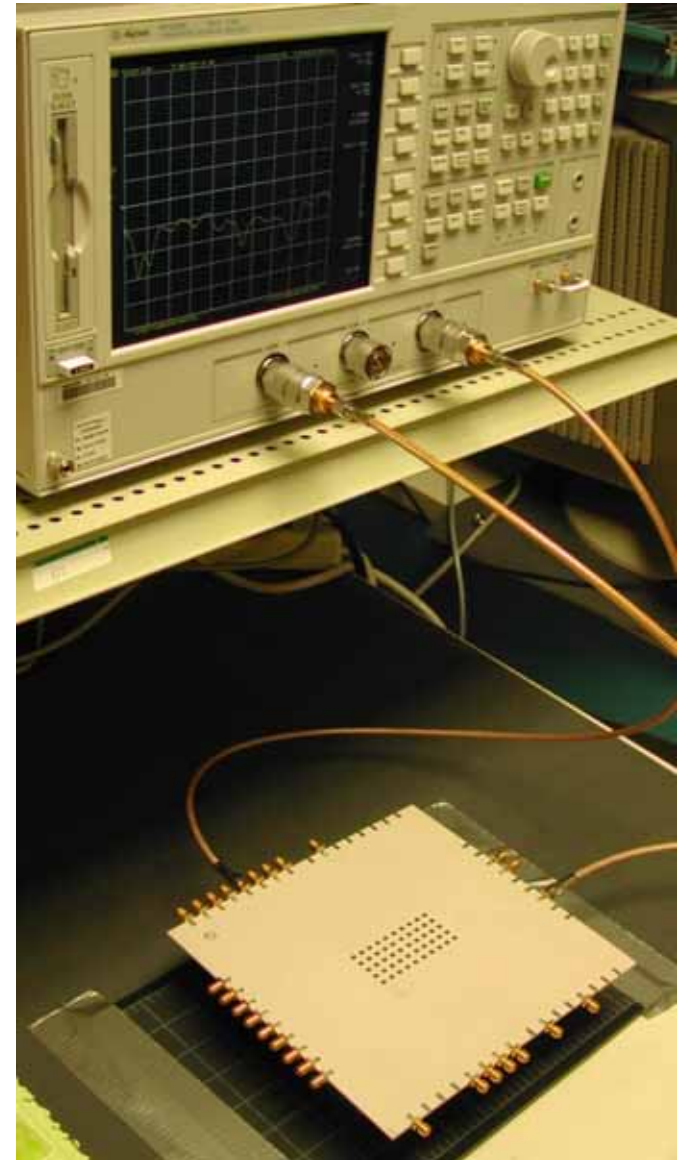
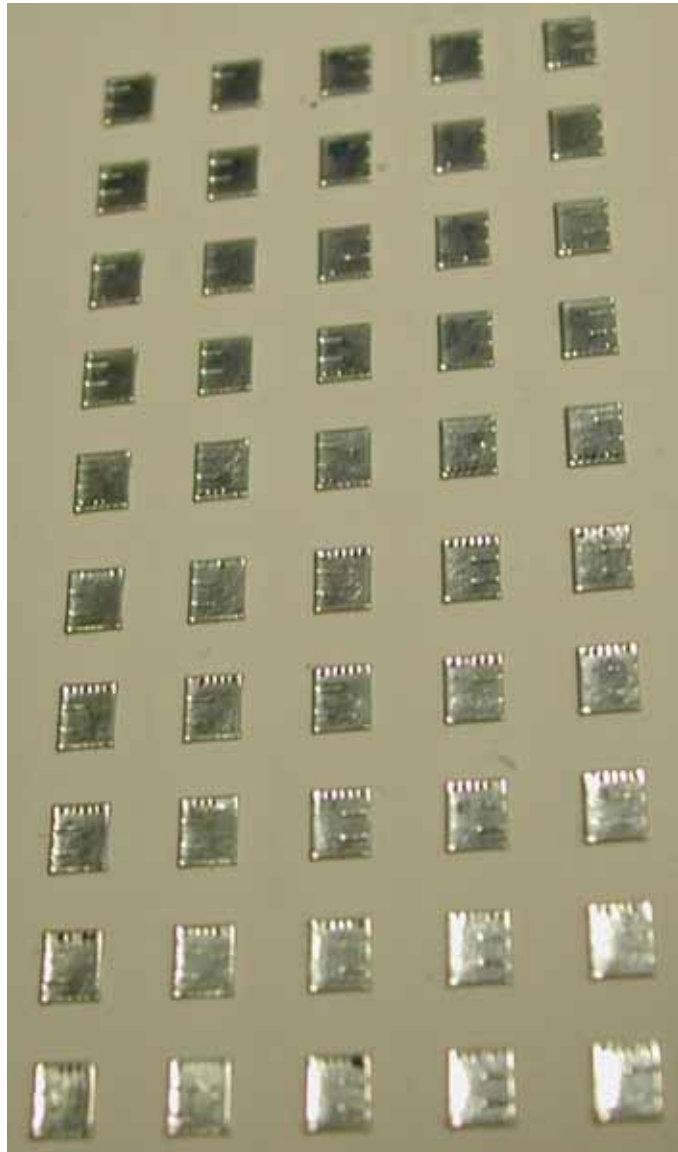
- Design Frequency: 5.25 GHz
- Patch Size: 3.5 x 2.75 mm
- RF35: $\epsilon_r=3.5$, $\tan\delta=0.0018$
- 2 layers, 787 $\mu\text{m}/\text{layer}$
- Larger design, higher efficiency

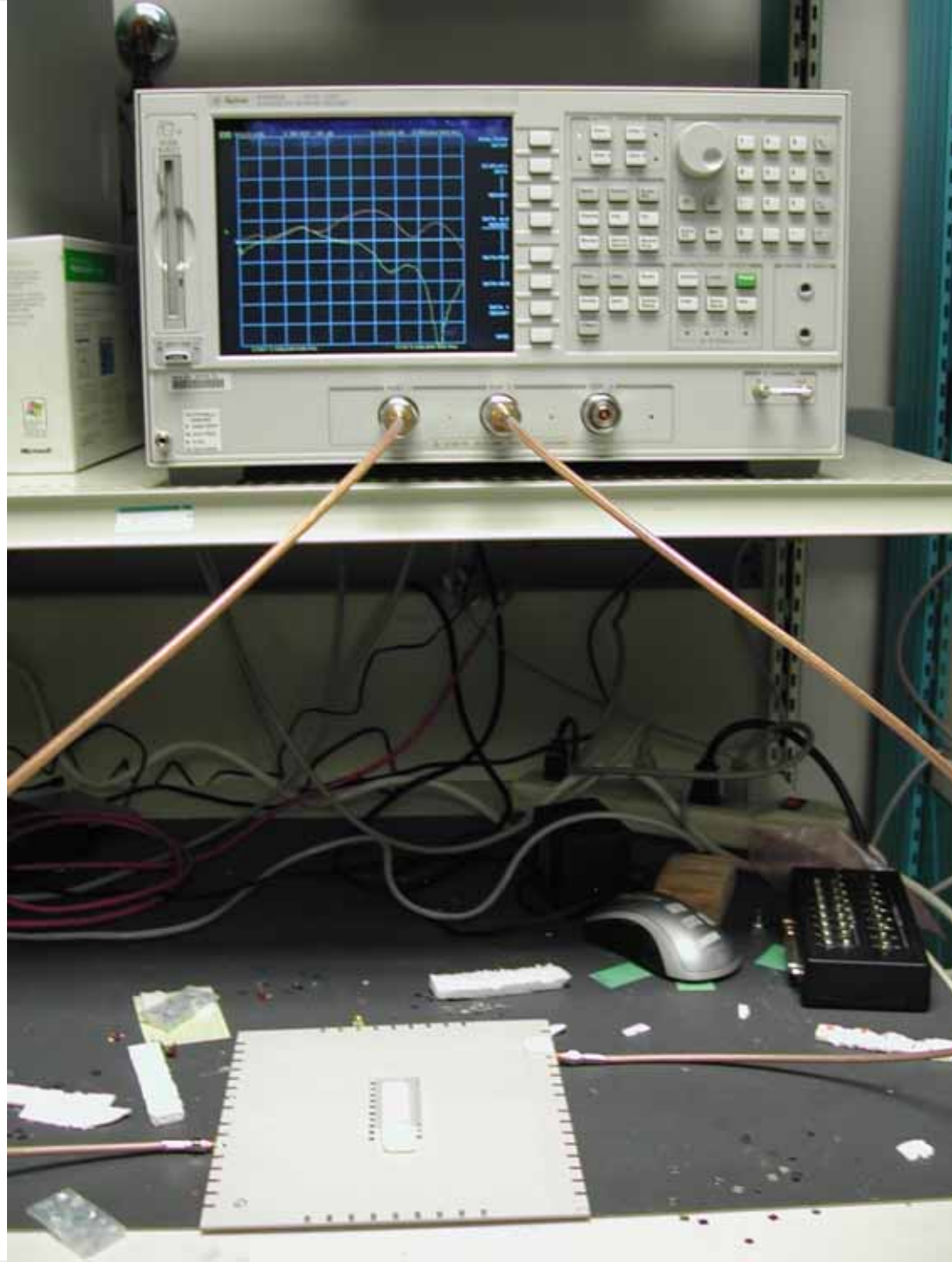
- Design Frequency: 5.32 GHz
- Patch Size: 2.77 x 2.75 mm
- RF60: $\epsilon_r=6.15$, $\tan\delta=0.0028$,
- 2 layers, 787 $\mu\text{m}/\text{layer}$
- Smaller design, lower efficiency

Prototype RF-DNA Instances

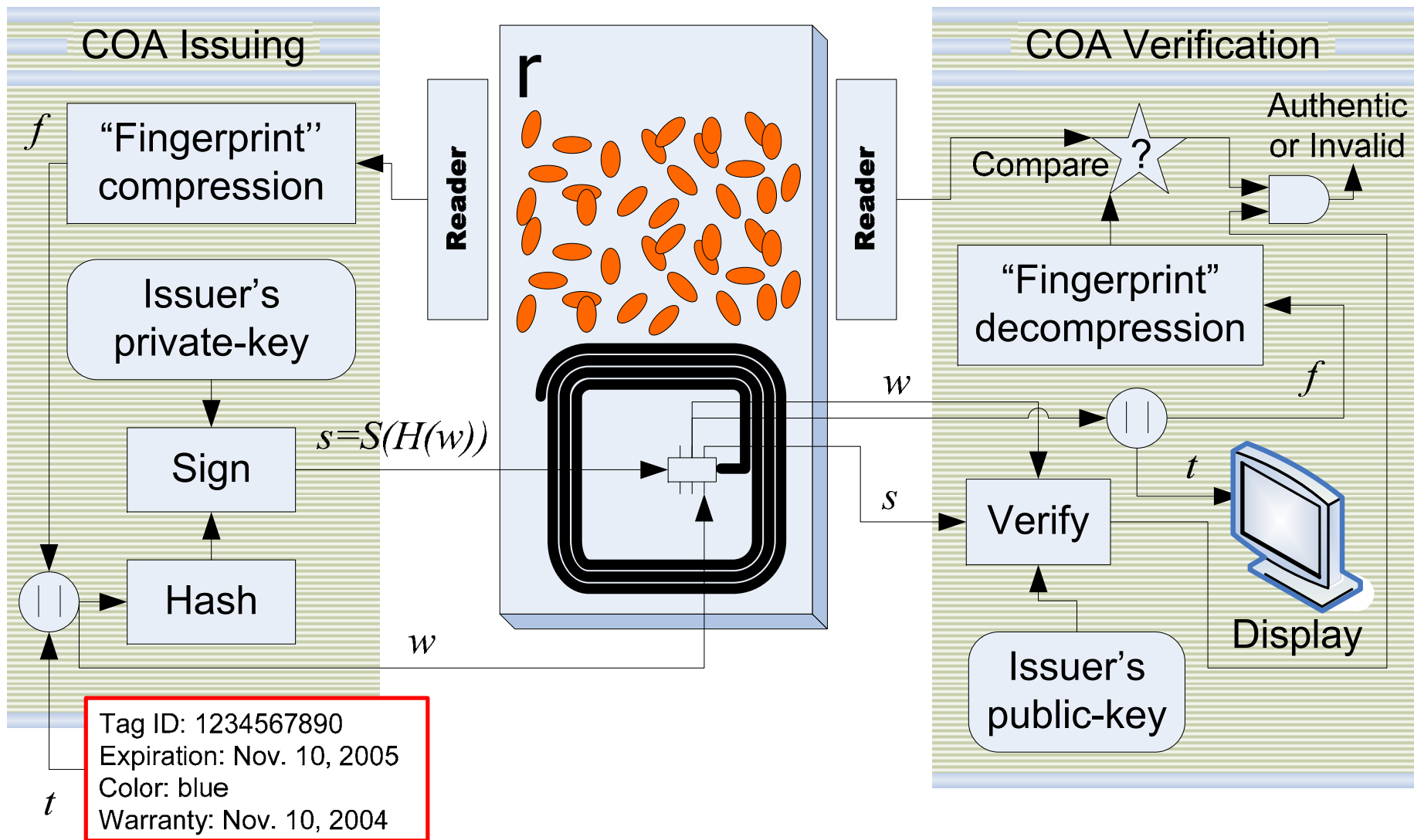


Prototype RF-DNA Reader





The Idea





Desiderata for Anti-Counterfeiting Technologies





Definition of COA

- ◆ Bauder and Simmons – Sandia Labs
- ◆ Desiderata for COA Technologies
 - R1 = Inexpensive to manufacture
 - RF-DNA < US\$0.01 + cost of storage (e.g., RFID)
 - R2 = Expensive to create a near-exact replica
 - RF-DNA requires true 3D manufacturing
 - Cost of R2 = (Adversarial) margin protection limit
 - R3 = Inexpensive to sign/verify
 - RF-DNA reader projected cost US\$100
 - R4 = Robust
 - RF-DNA robust to humidity, temperature, wear-and-tear
 - Proximity of other objects with strong RF effect



Definition of COA

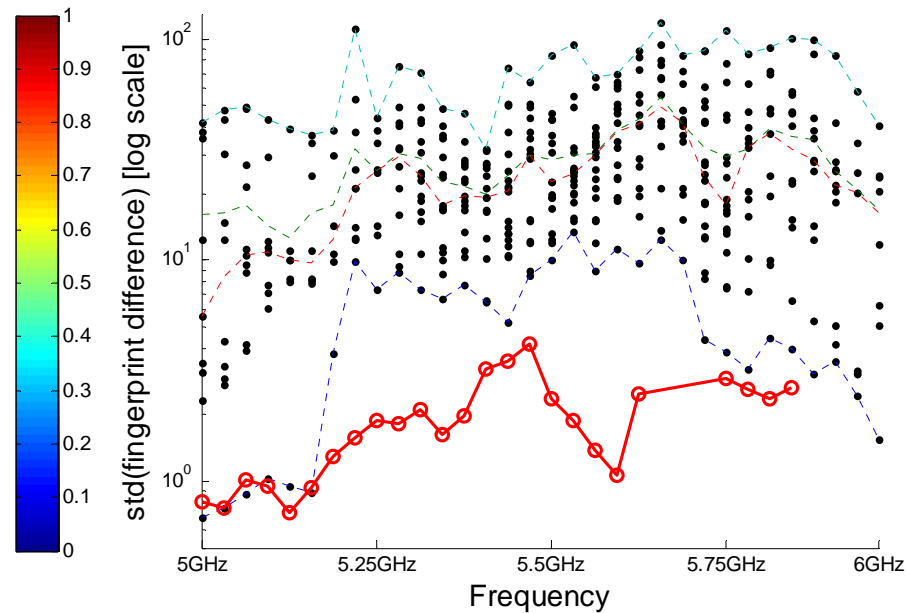
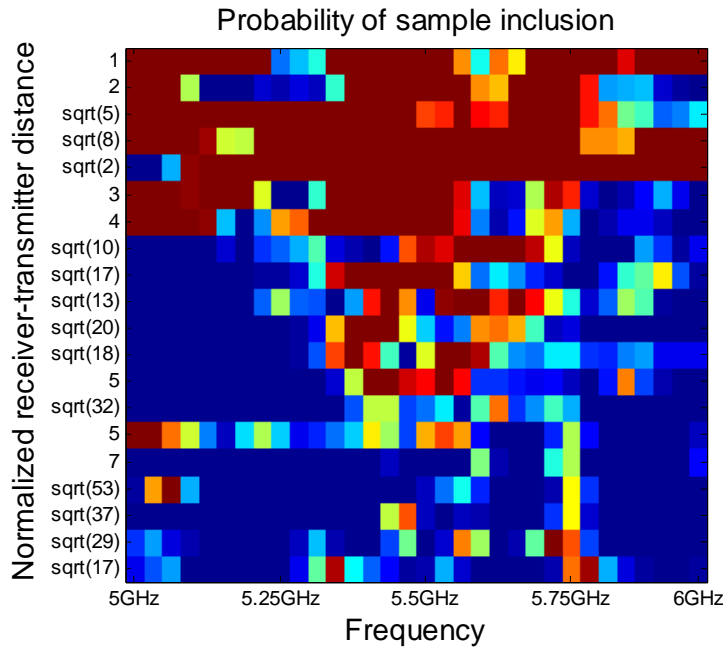
◆ Desiderata for COA Technologies

- R5 = **physical one-way function** – it should be computationally difficult to construct an object of fixed dimensions with a “fingerprint” \mathbf{y} such that $\|\mathbf{x} - \mathbf{y}\| < \delta$, where \mathbf{x} is a given “fingerprint” of an unknown COA instance and δ bounds the proximity of \mathbf{x} and \mathbf{y} with respect to a standardized distance metric $\|\cdot\|$.
- Inverse design over Maxwell equations
- Ill-posed problem
 - Tikhonov regularization
- Even the forward design is difficult
- Linear system
 - Could be non-linear with magnetic materials
 - Hysteresis too slow
- Ultimate anti-skimming tool

Definition of COA

◆ Desiderata for COA Technologies

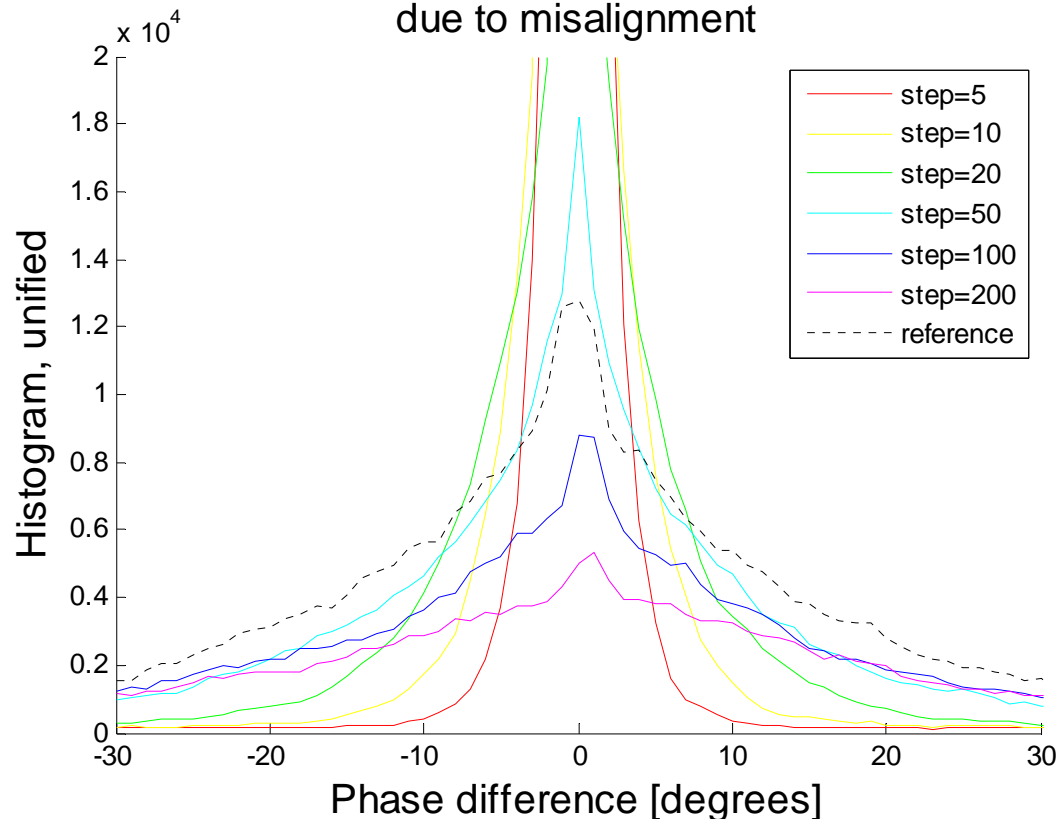
- R6 = repetitiveness
- R7 = non-collision



Definition of COA

- ◆ Desiderata for COA Technologies
 - R8 = fingerprint interdependence

Same-object fingerprint variance
due to misalignment





Definition of COA

- ◆ Desiderata for COA Technologies
 - R10 = visual inspection of the verification path
 - RF-DNA - contactless verification
 - Robust to:
 - jamming
 - signal overpowering



Challenge/Response Systems

- ◆ Prime candidate
 - Variability in semiconductor manufacturing
- ◆ \$\$\$\$\$
 - Need to be on-line
 - Storage vs. lifetime
- ◆ Attack model not clear
 - reverse engineering
 - probing
 - debugging for asynchronous circuits
 - obfuscation
- ◆ Large set of attacks unexplored
- ◆ Need to be on-line
 - Large random number = Product ID
 - Follow IDs through supply chains
 - \$\$\$\$\$ but nearly same effect as with “breakable” C/R systems



Applications

◆ No association with object

- Anti-skimming
 - Credit cards
- Documents of value
 - Money, checks, coupons
 - Travel documents: passports, national IDs, visas
 - Don't talk to readers unless they prove they read your "fingerprint"

◆ Association with object

- Tags, certificates of authenticity, K-th owner
 - Software, hardware, consumer electronics
 - Fashion, jewelry, perfume industry
 - Parts: cars, aircrafts, boats
- Seal
 - Tamper-evident hardware
 - Mail
 - Pharmaceuticals



Summary

- ◆ Bauder and Simmons, Sandia
- ◆ RF-DNA
 - R1-10 ✓
 - Size = inch-by-inch by 1-2mm
 - Materials science
 - Manufacturing optimization
 - Robustness to nearby RF actors
 - Packaging solutions for seals
 - “Fingerprint” compression

Acknowledgments

Yacov Yacobi

Jim Kajiya

Gary Starkweather

Turner Whitted

Mike Sinclair

Gideon Yuval

YuQun Chen (fiber-optic COA)

Josh Benaloh

Microsoft Anti-Piracy

Yasuo Kuga – EE, UW

Manos Tentzeris, Joy Laskar – Georgia Tech

GeorgiaTech Electronic Design Center

Technicolor Labs

Robert Arsov – Credit Suisse

