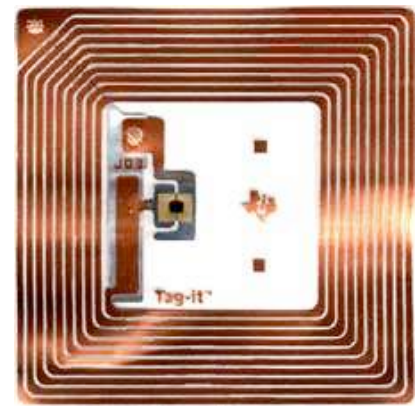
RFID
Security and Privacy

Stephen A. Weis
Massachusetts Institute of Technology
Computer Science and Artificial Intelligence Lab

Today's Talk

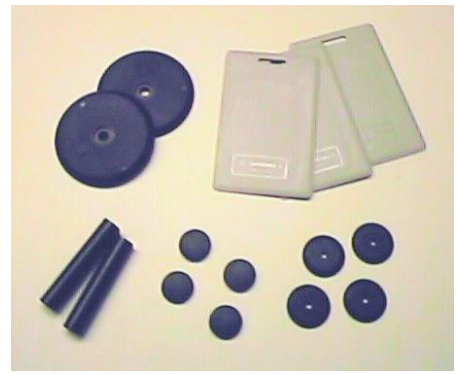
- What are the security and privacy risks?
- How can we address these risks?
- What are the open problems?



Foil Inlay Tag

Why RFID?

- Supply Chain Management
- Inventory Control
- Retail Systems
- Access Control Systems
- Payment Systems
- *What if implemented insecurely?*



Active Tags

Espionage and Theft

- Corporate spies could track inventory changes and extrapolate sales data
- Spies could anticipate strategy by tracking components through a supply chain
- Thieves can locate high-value items

Implantable Tag

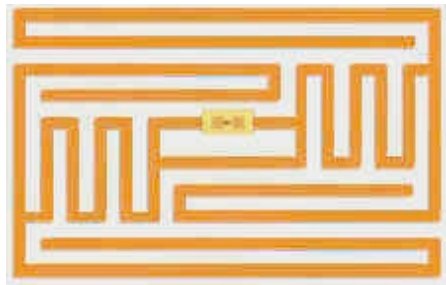
Forgery

- Proximity cards for building access
- Public transit and toll systems
- Payment and token systems
- “Skimming” valid data to produce clones
- Swapping products for tagged decoys

Keychain Tag

Denial of Service

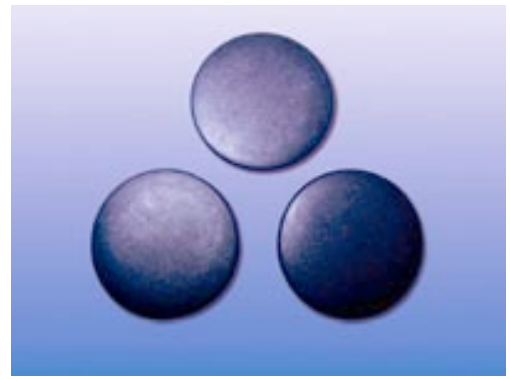
- Jamming readers
- Seeding fake tags
- Disabling or destroying tags



Foil Inlay Tag

Privacy

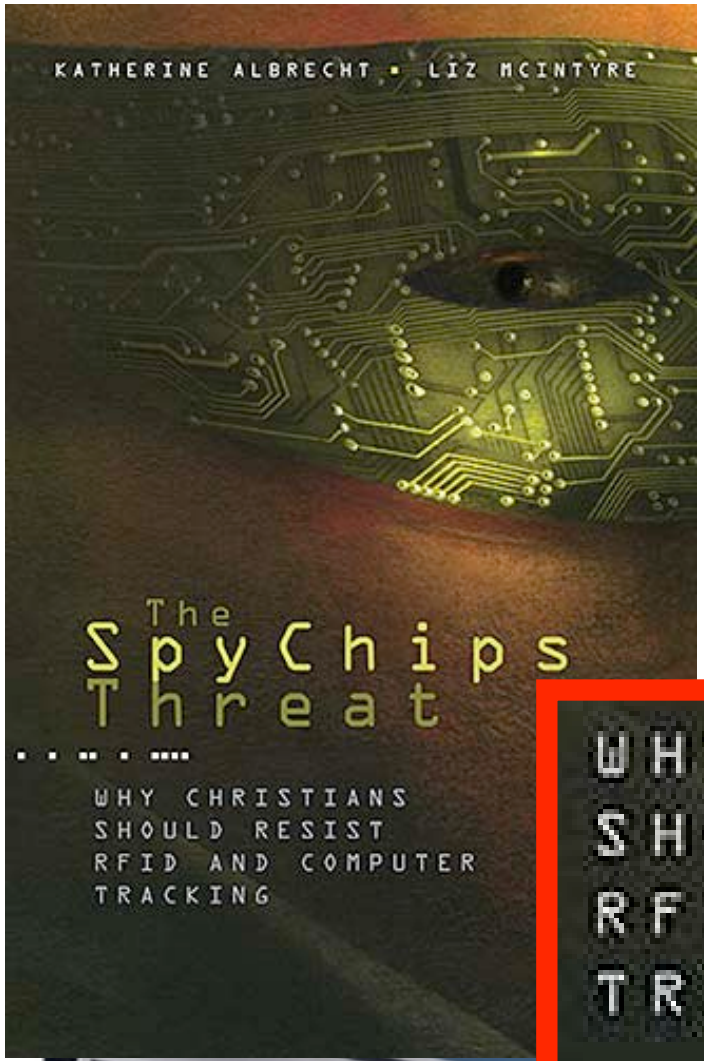
- Clothes, drugs, books, currency, passports
- Snooping on individuals
- Targeting certain groups
- Location privacy

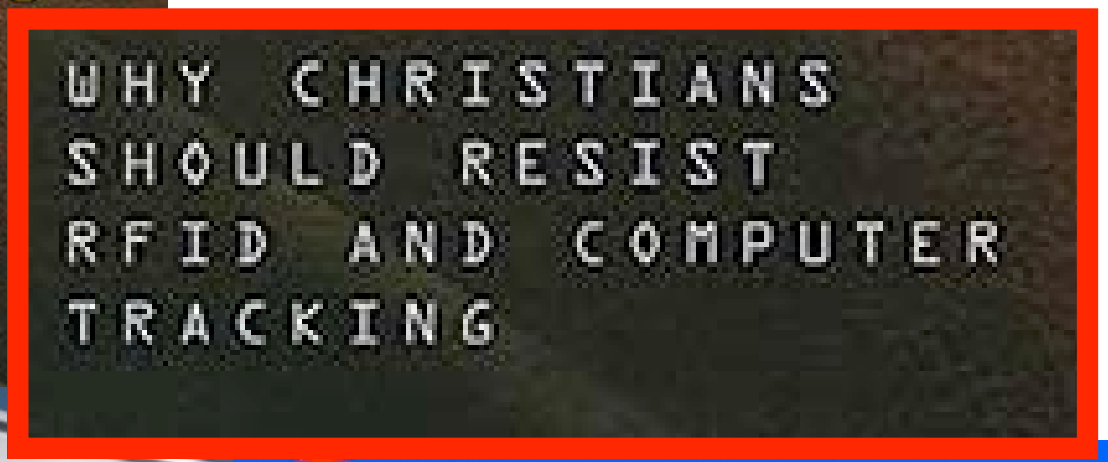


Laundry Tags

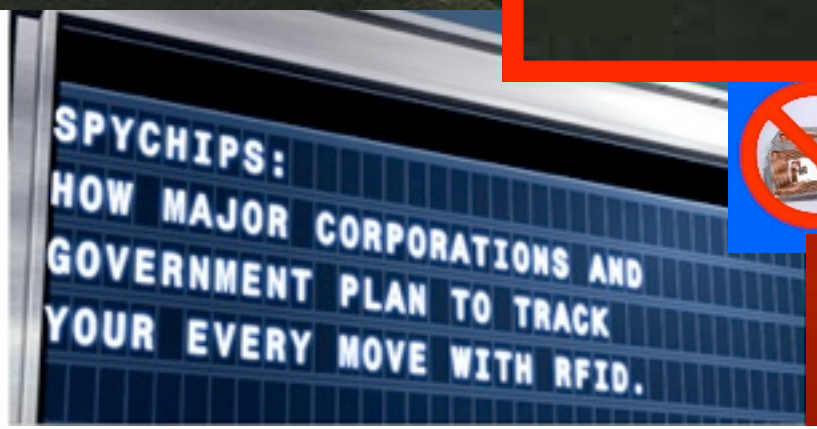
RFID...

- ...Big Brother's spychip?
- ...terrorist targeting device?
- ...work of the anti-Christ?





RFID
NINETEEN EIGHTY-FOUR

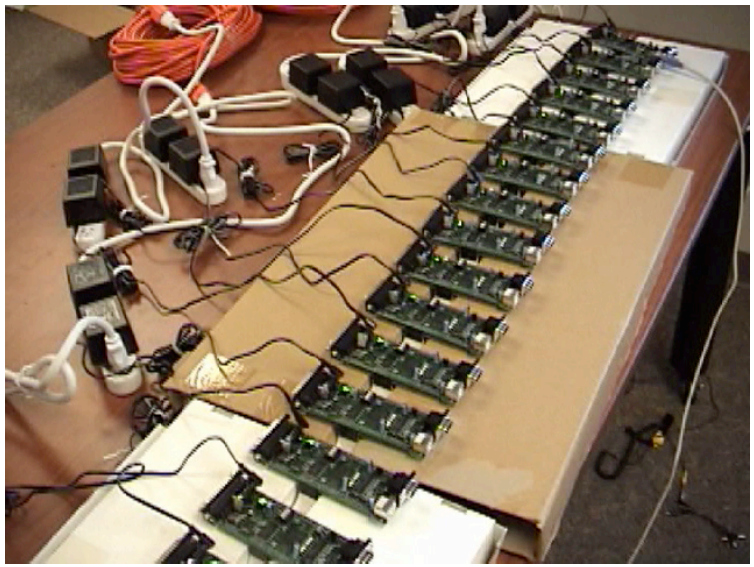


Notags.co.uk

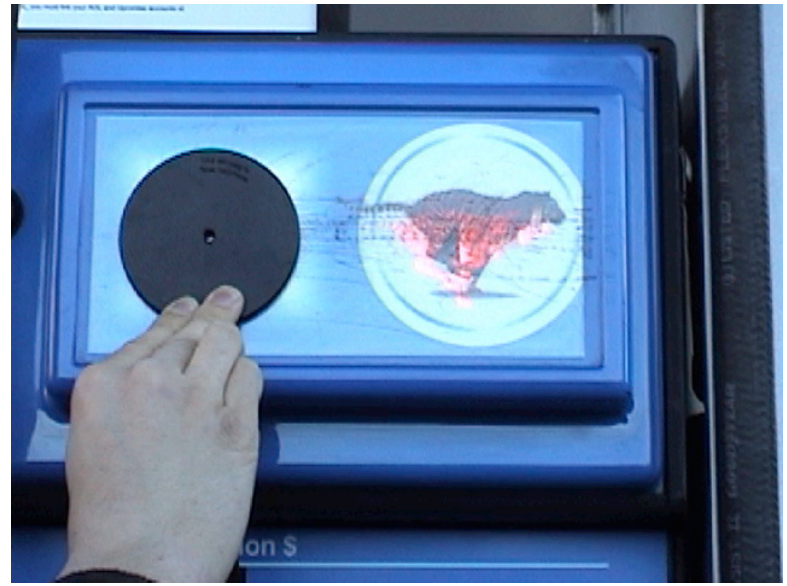
RFID Kills.com

ExxonMobil SpeedPass

Skimming Equipment



Cracking the TI DST

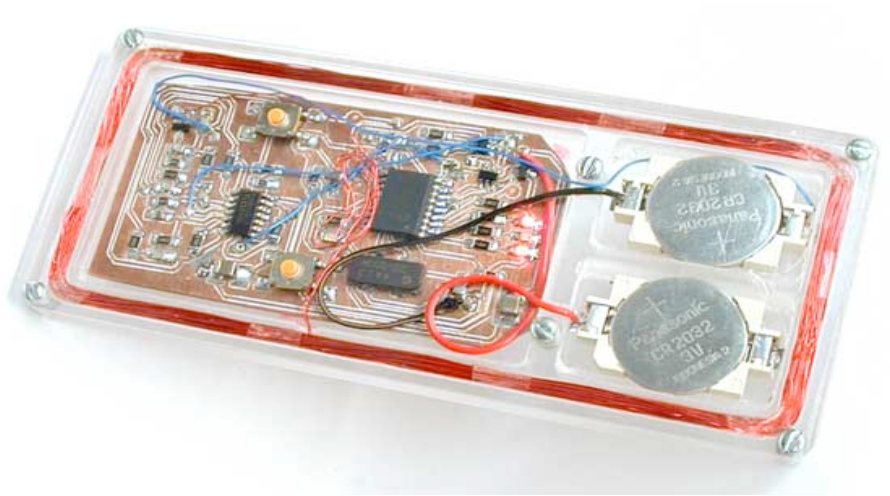


Buying gas with a clone

Images courtesy of rfidanalysis.org

Proximity Card Attack

MIT RFID Proximity Card



A proximity card emulator

Digression: RFID Passports?

- What biometrics are stored on passports?
- Why? Who is authorized to read it?
- How can the data be abused?
- Revocation? What if I lose my passport?
- Why wireless? Why not contact?

Adversaries

- Passive: Eavesdropping only
- Active: Participate in tag-reader protocols
- Physical: Extract secrets from tag circuits
- May differ on “forward” and “backward”

Security Challenges

- Low cost ⇒ Limited gates and storage
- Vulnerable packaging ⇒ No shared keys
- "Passive" power ⇒ Limited power, no clock, no pre-computation, few rounds
- Minimum performance ⇒ Limited time

Cryptography Costs

- Standard DES and AES take 4-20K gates
- SHA-1 hash function takes ~20K gates
- Most tags couldn't even hold an RSA key
- Some hope: Low-cost AES, ECC, NTRU, low-cost authentication (more later)

To kill or not to kill?

- Why not destroy RFID tags at checkout?
- Only addresses individual privacy issues
- Removable RFID price tag works well
- Does not allow end-user applications:

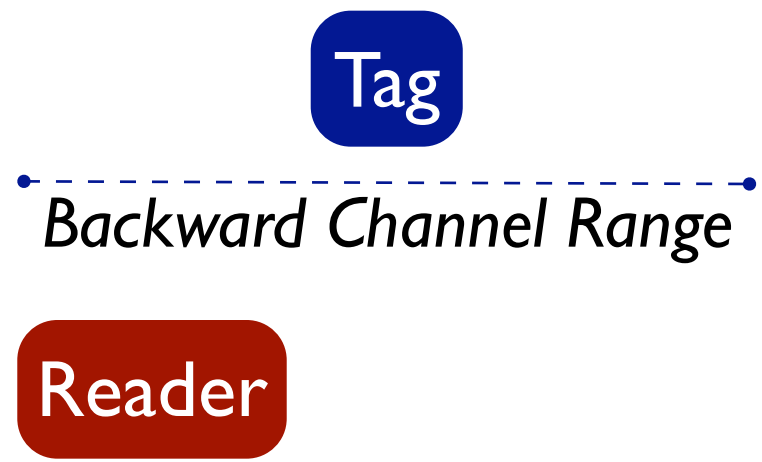
SIMPill

Back-End Access Control

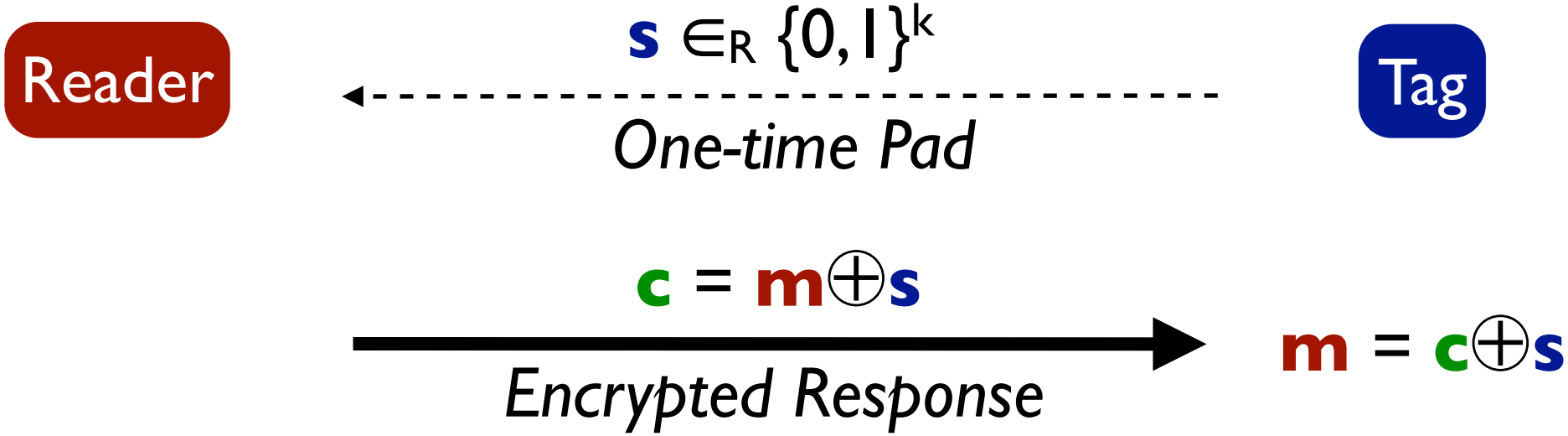
- Object Naming Service (ONS) -- look up ID numbers and returns product codes
- Why not restrict access to ONS?
- Still allows tracking of predictable tags
- Centralized lookups are too slow
- Could change tag IDs. How to manage?

Channel Asymmetry

- "Forward": Reader-to-tag channel
- "Backward": Tag-to-reader channel
- Passive power sent on forward channel



Backwards One-time Pad



Backwards One-time Pad

- Used in EPCGlobal Class-1, Gen-2
- Open research problem: How to cheaply generate random bits with digital logic?
- Manufacturers may use LFSRs

Hash-Based Schemes

- Several ideas rely on one-way functions
- Access Control (aka Hash Locks):
  Reader locks tag with *H(x)*, unlocks with *x*
- Private Identification:
  Tag sends (*r*, *H(ID,r)*), reader hashes its IDs
- How do we build cheap one-way functions?

Blocker Tags

- Juels, Rivest & Szydlo (2003)
- Device for enhancing personal privacy
- Injects itself in anti-collision protocol to restrict access to tags a person carries
- An idea is to put blocker tags in bags
- Not a commercial product

Privacy Bits

- Juels and Brainard
- Tag responses contain an access control policy: "It's okay/not okay to read me"
- Readers may choose to obey policy
- Corrupt readers risk being caught

Caveat Emptor

Can Zero-Knowledge Tags Protect Privacy?

A Danish startup is developing an RFID system that uses a zero-knowledge authentication protocol to protect consumer privacy, while allowing an item's tag to remain alive.

By Farhat Khan, RFID Journal, Sept. 27, 2005

...

A Danish startup named RFIDSec, however, is developing Zeroleak, a new approach to tag security. Zeroleak aims to protect consumers' privacy while allowing a tag to function after the item is purchased. Zeroleak tags will use a zero-knowledge authentication protocol which, can verify that an RFID reader has the proper authority to read it but does not require the tag to reveal any identifying information during the authentication process.

"Zeroleak tags will use a zero-knowledge authentication protocol."

Tag Authentication

- What about protecting against forgeries?
- Payment systems, designer goods, drugs, passports, access control systems
- Traditional authentication is too expensive
- Can't trust tags with shared secrets

Hopper-Blum Protocol

- Secure Human-to-Computer Authentication
- Secure against passive eavesdroppers
- Not secure against active adversaries
- Security based on a hard learning problem

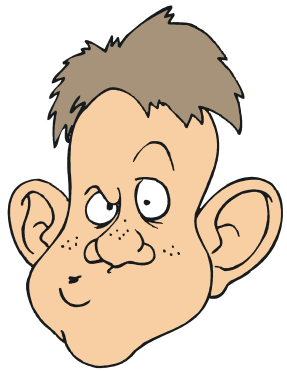
HB+ Authentication

- With Ari Juels, Crypto '05
- A new authentication protocol that handles active malicious attacks.
- Extremely hardware-efficient
- Secure under same assumption as HB

Hopper-Blum Authentication

Computer(**x**)

Bob(**x**, η)



$\mathbf{a} \in \{0,1\}^k$

Challenge

$z=(\mathbf{a}\cdot\mathbf{x})\oplus\nu$

Response

$z=(\mathbf{a}\cdot\mathbf{x})$?

$\nu \in_R \{0,1\}$

Repeat for q rounds.

Authenticate Bob if he passes $(1-\eta)q$ rounds.

Security Against Bad Bob

Computer(**x**)

$\mathbf{a} \in \{0,1\}^k$

Challenge

$z=(\mathbf{a} \cdot \mathbf{?})$

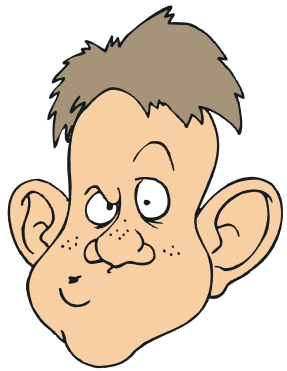
Guess Response

Adversary

Security Against Passive Eavesdroppers

Computer(**x**)

Bob(**x**, η)



Eavesdropper

$(\mathbf{a_0}, z_0), (\mathbf{a_1}, z_1), \ldots, (\mathbf{a_q}, z_q)$

$\nu \in_R \{0,1\}$

Find an **x'** that allows you to answer a
(1- η) fraction of **a** challenges

Learning Parity with Noise

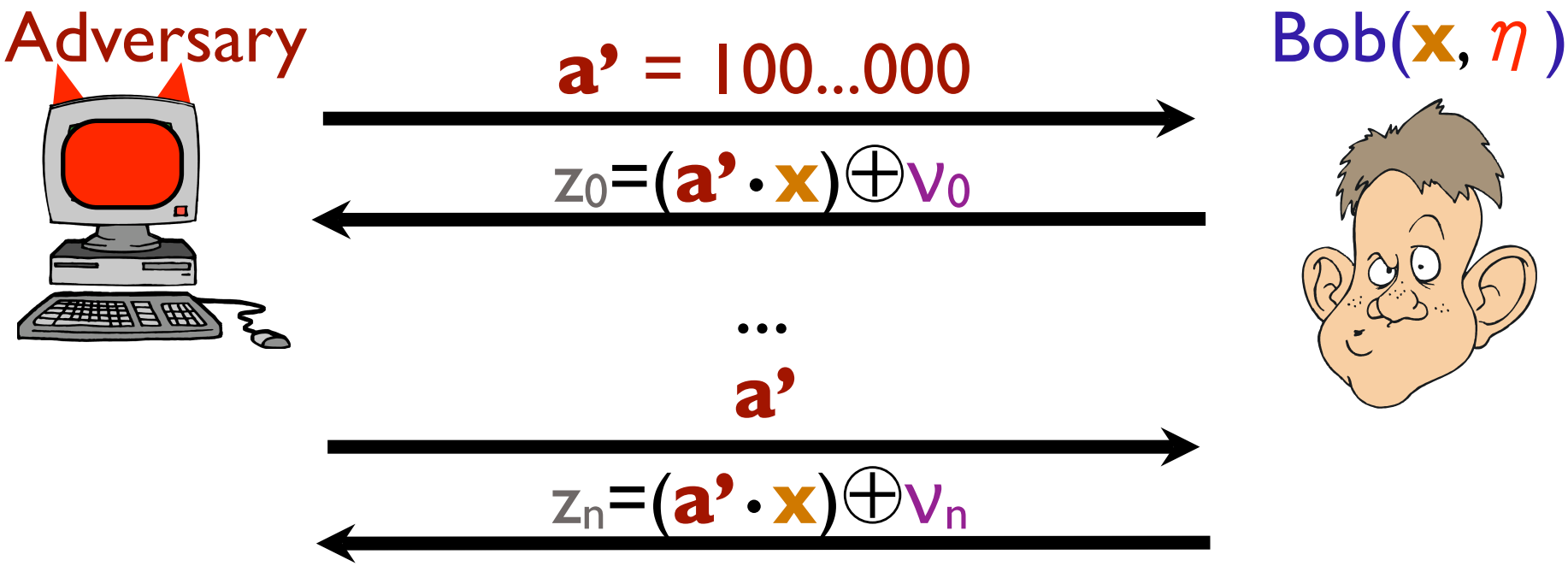
- Related Cryptosystems:
  - McEliece, 1978, Niederreiter, 1986, Stern, 1996
- Crypto and learning problems:
  - A. Blum, Furst, Kearns, Lipton, 1993
- $O\left(2^{\frac{k}{\lg k}}\right)$ LPN algorithm:
  - A. Blum, Kalai, Wasserman, 2003
- Shortest Vector Problem: Regev, 2005

Concrete Security

Key Size (k)	Best Attack
64	2^{35}
128	2^{56}
192	2^{72}
224	2^{80}
256	2^{88}
288	2^{96}

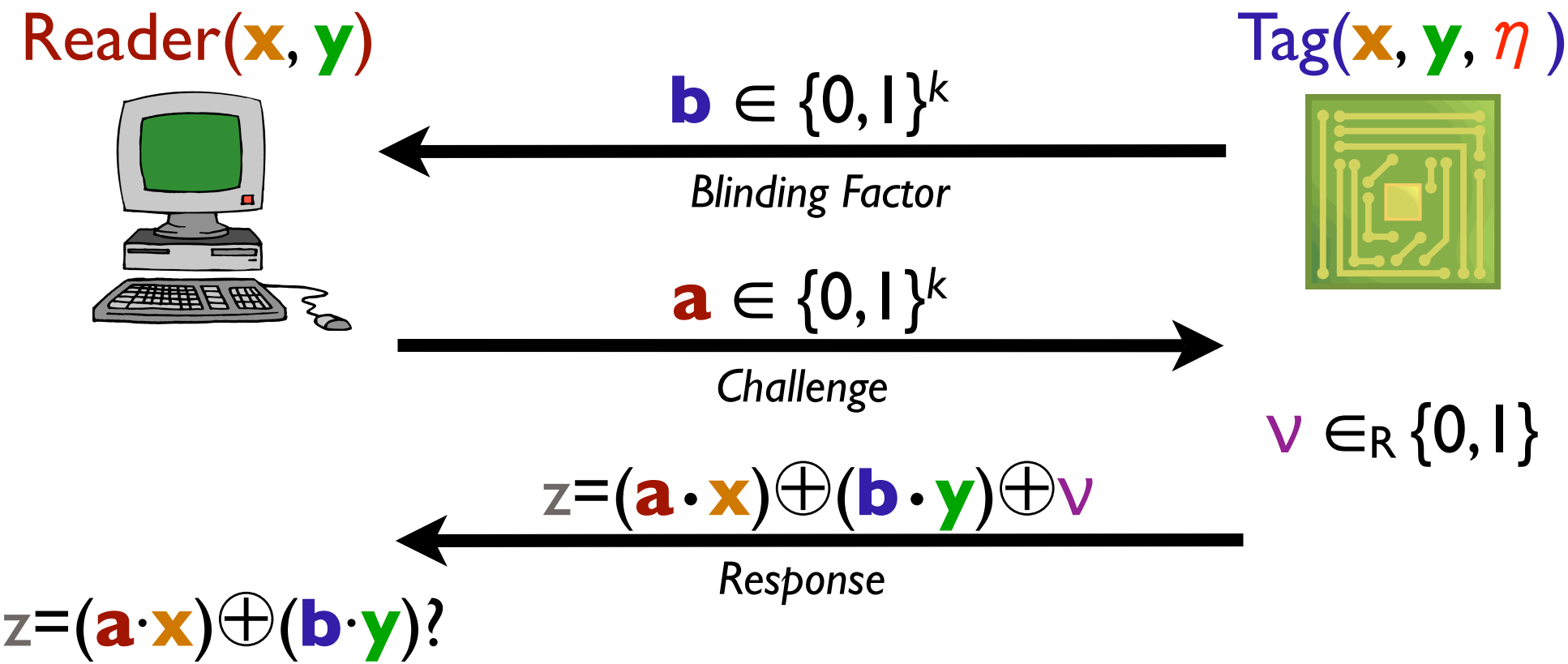
Obligatory grain of salt → □

Active Attack against HB

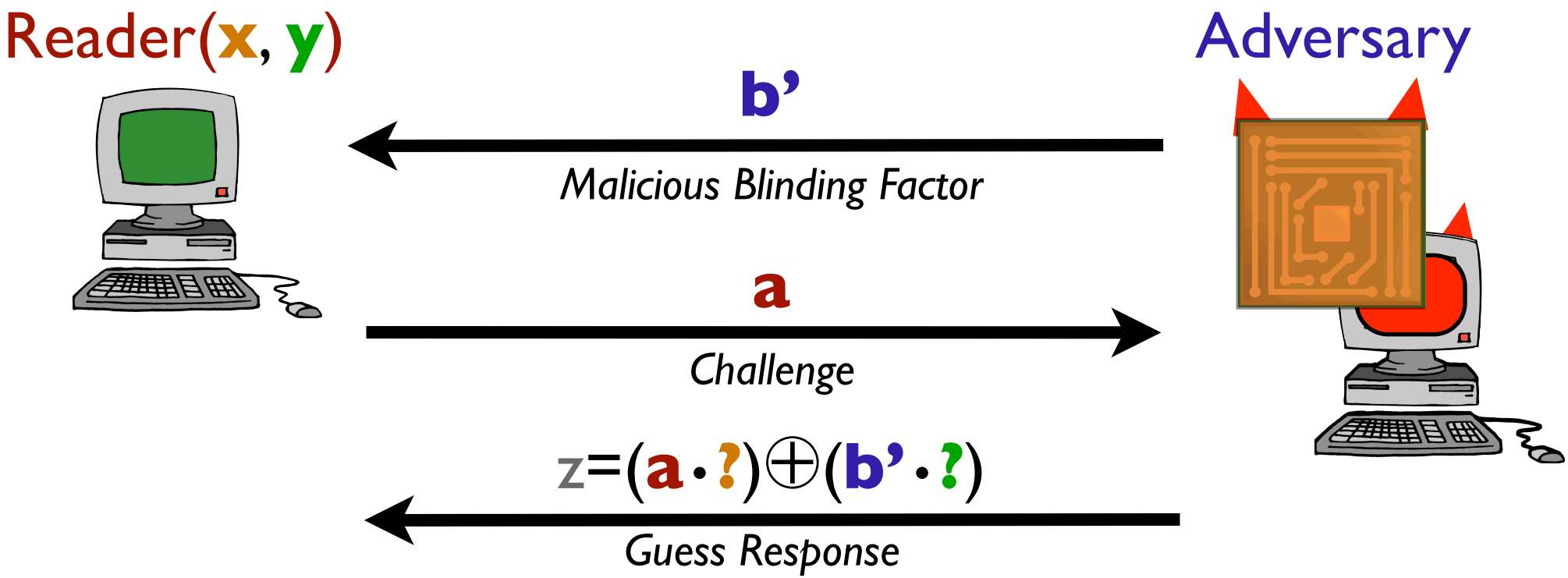


Adversary takes majority of z_i values to get noise-free parity bit. Extract all k bits in $\Omega(k/(1-2\eta)^2)$ trials

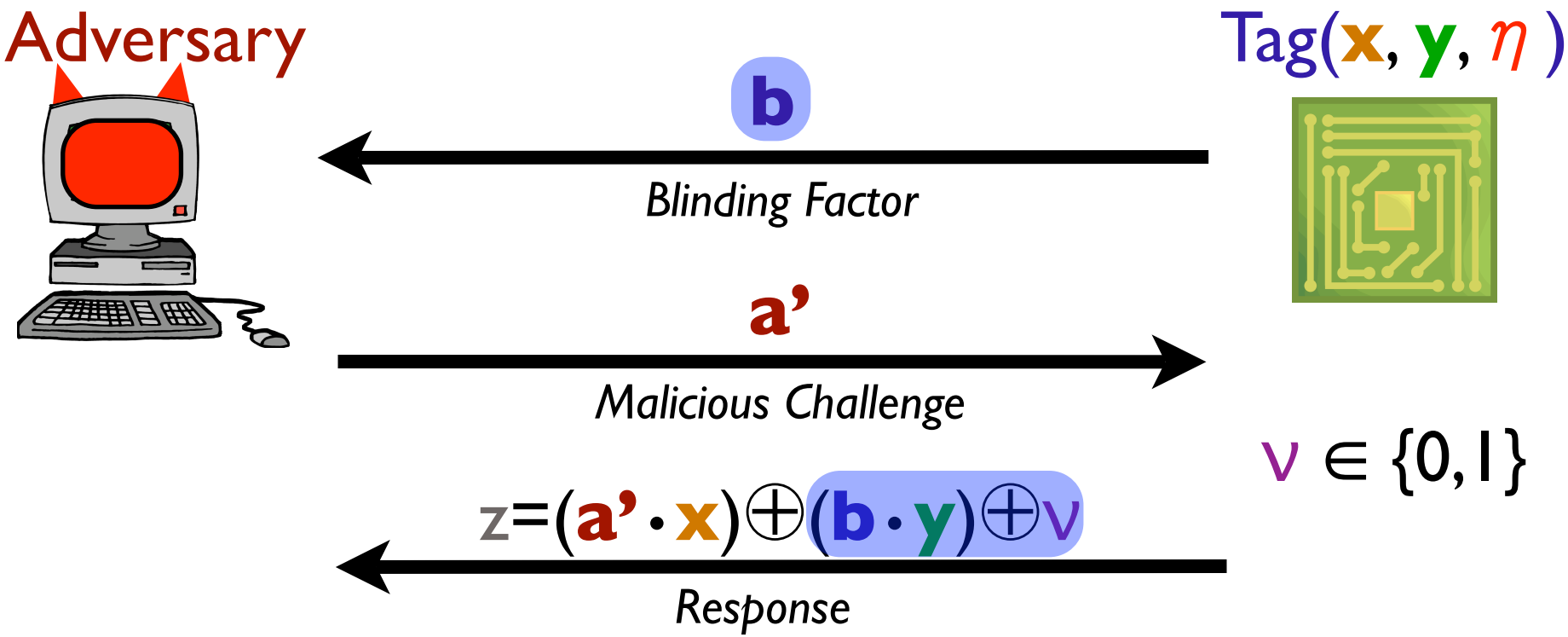
Our New Protocol: HB+



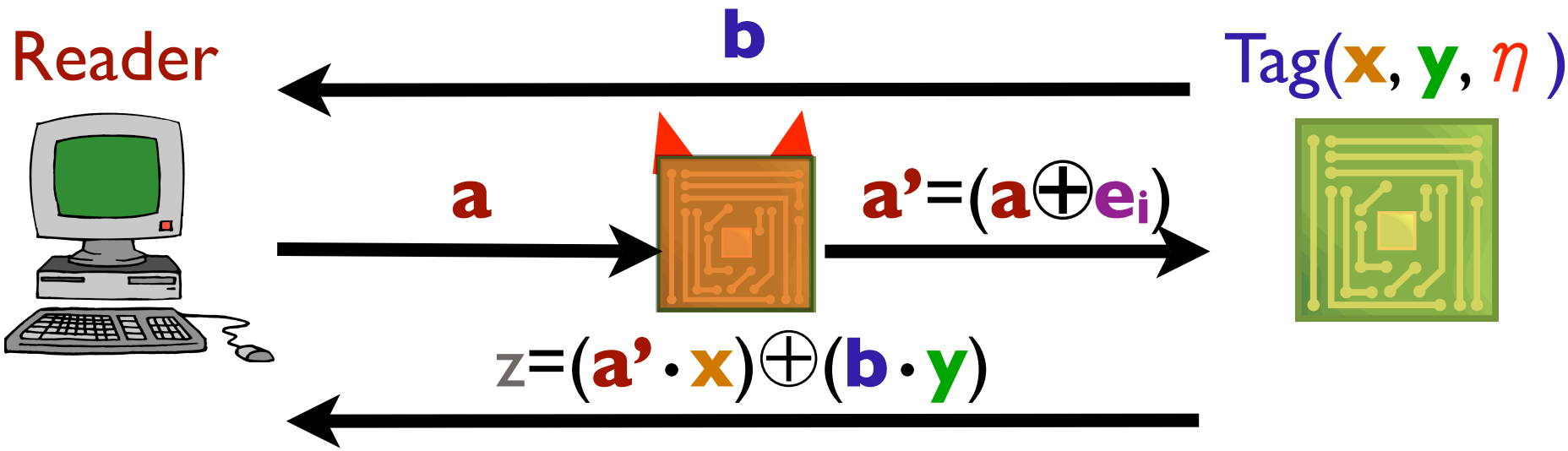
Security against Bad Bob



Security against Active Attacks



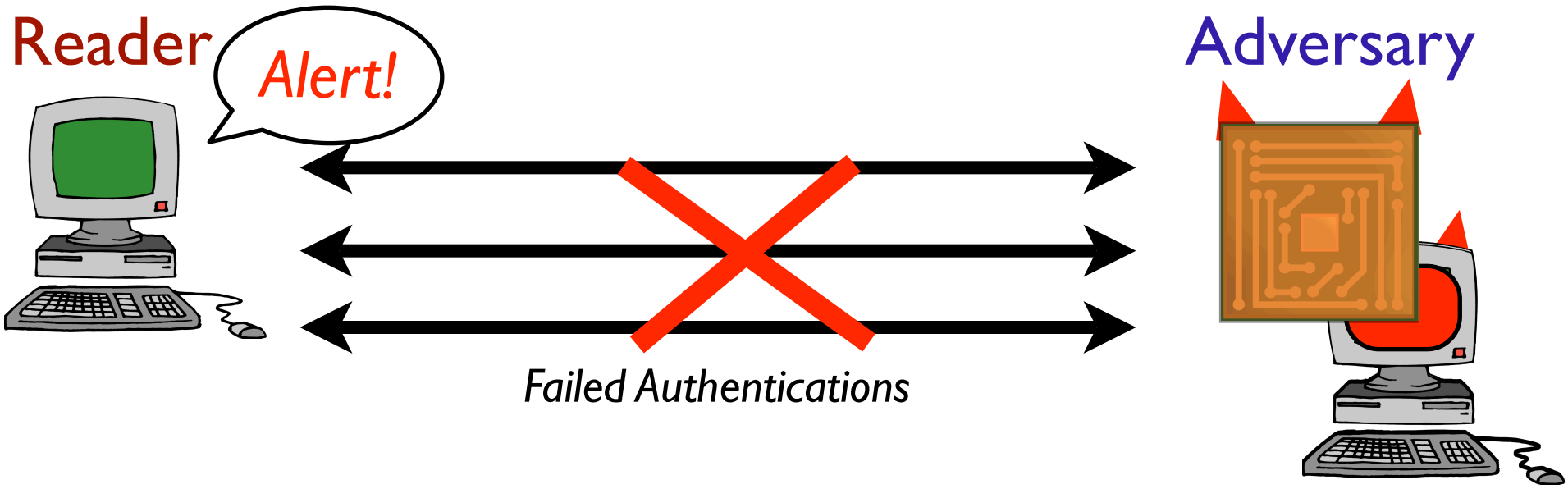
Man-in-the-Middle Attack



Adversary picks a standard basis vector e_i.

If tag is authenticated, x_i is zero.

Detection Security Model



Assume valid readers will detect suspicious failures:
No Reader oracles.

EM and Side-Channel

Skew random number generator with EM signal or monitor energy consumption in a side-channel attack?

Future Work

- ~~Parallel~~ HB+ *(Katz)*
- Two-round HB+
- Real implementation costs
- Random number generation
- Electromagnetic & side-channel attacks
- Key management
- RFID policies

Questions?

- Thanks to Alon and Salil for the invite
- E-mail: sweis@mit.edu
- URL: http://crypto.csail.mit.edu/~sweis