Information Security – Theory vs. Reality

0368-4474-01, Winter 2011

Lecture 2: Crypto review, fault attacks

Eran Tromer

(This lecture was given mostly on the whiteboard.)

Administrative

- Course website:
  http://cs.tau.ac.il/~tromer/courses/infosec11
- Lecture slides after talk
- Tentative list of topics
- Mailing list
- Questionnaire
- Registration
  To: tromer@cs.tau.ac.il
  Subject: ISTvR registration

Crypto review

- Encryption
  - Security defined as indistinguishability game
  - Chosen plaintext attack
  - Chosen message attack
- Digital signatures and message authentication codes
  - Unforgeability
- Hash functions
  - Collision-resistance
  - Heuristic pseudorandomness

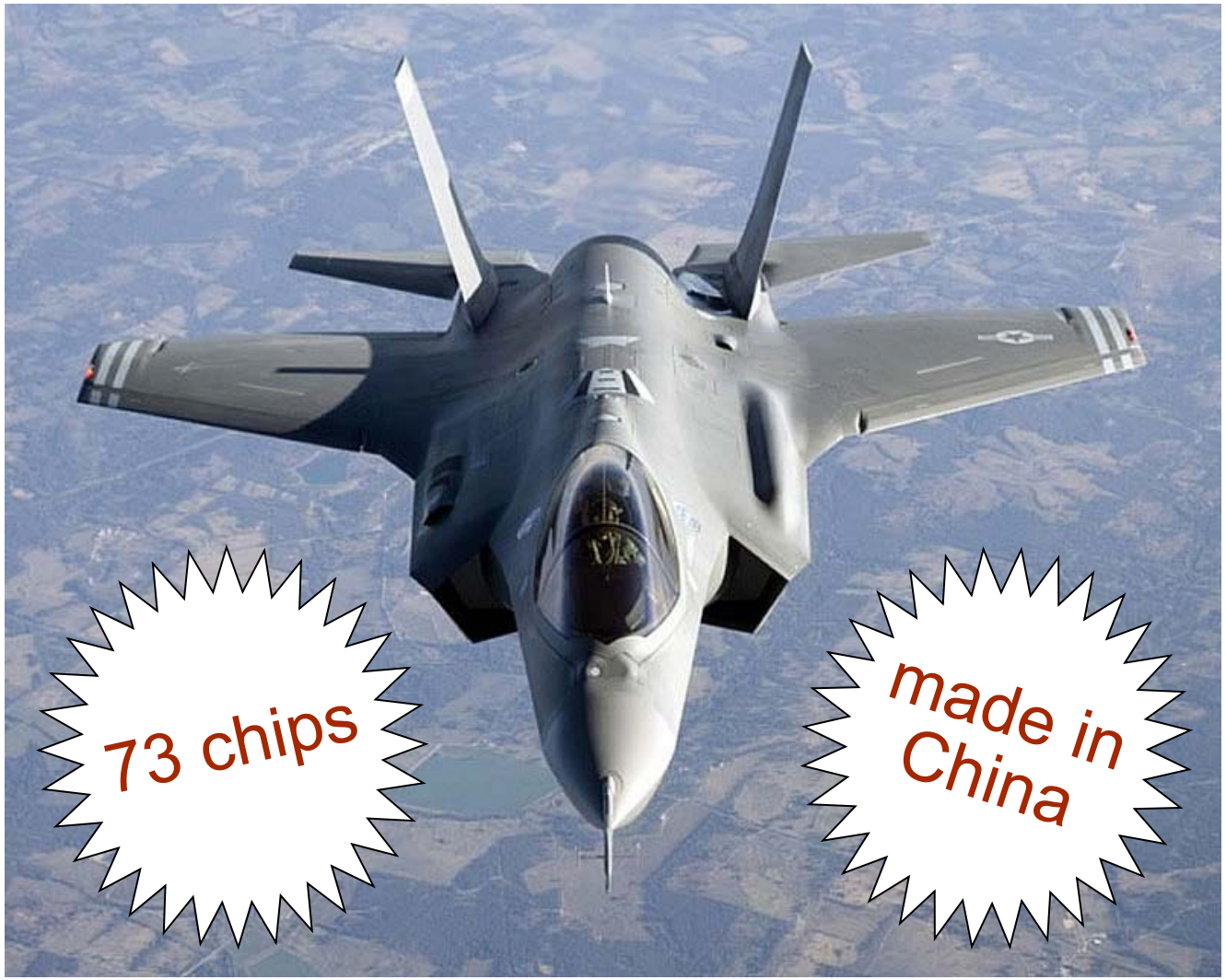
Hardware faults

- Differential Fault Analysis of Arbitrary Ciphers
  Biham, Shamir, *Differential Fault Analysis of Secret Key Cryptosystems* (section 3)

- RSA via Chinese Remainder Theorem
  DeMillo, Lipton, *On the importance of eliminating errors in cryptographic protocols*
  (section 2)

- JVM single memory error

F-35 Joint Strike Fighter



Information technology supply chain: headlines

The New York Times (May 9, 2008)

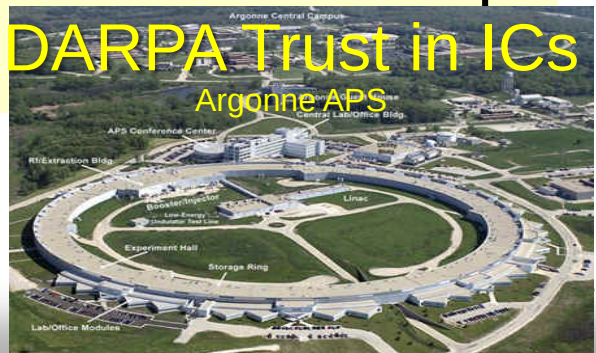
"F.B.I. Says the Military Had Bogus Computer Gear"

ars technica (October 6, 2008)

"Chinese counterfeit chips causing military hardware crashes"

The New York Times (May 6, 2010)

"A Saudi man was sentenced [...] to four years in prison for selling counterfeit computer parts to the Marine Corps for use in Iraq and Afghanistan."



High-level goal

Ensure properties of a distributed computation when parties are mutually untrusting, faulty, leaky & malicious.

Proof-Carrying Data