Hot Topics 2010: Cryptography

Scott Yilek

What is Cryptography

- One common definition: “Mathematical science of securing digital information.”
- You may have heard of encryption, digital signatures, message authentication codes, hash functions, key exchange,…

What is Cryptography

What is Cryptography

Use mathematical tools to prevent adversary from

-Reading messages
-Modifying messages
-Inserting new messages

What is Cryptography

Use mathematical tools to prevent adversary from

-Reading messages
-Modifying messages
-Inserting new messages

Provable Security: Prove (with NP-Completeness style reductions) that if some well-known problem is hard (e.g., factoring large numbers), then the scheme is secure.

What Do Crypto Researchers Do?

Cryptanalysis:

- Break existing (bad) crypto

- Improve fastest known attacks on cryptographic algorithms or related hard problems (e.g., factoring).

Design new protocols:

- Build fancy new crypto that is more secure/fast/interesting/flexible…

- Prove secure

Theory:

-How do cryptographic primitives relate to each other and to other mathematical objects

- What can and cannot be proven using existing techniques

What is Hot Right Now

Hash functions:

National Institute of Standards and Technology (NIST) is holding world-wide competition to design a new hash function, due to the recent attacks on SHA-1.

Homomorphic Encryption:

Most cryptographers thought impossible for 20-30 years. But…
Craig Gentry just came up with first fully-homomorphic encryption scheme.

Lattices:

Crypto has historically been based on groups, rings, fields, etc.
Now, with homomorphic encryption done with lattices, researchers are building all kinds of cool crypto using lattices.

What are Top Crypto Places (Other than UCSD)

MIT: Ron Rivest ("R" in RSA), Shafi Goldwasser, Silvio Micali

-Developed most of big results in the 80s.
-Almost all top Professors in crypto got PhD at MIT (e.g., both Mihir and Daniele did).

Other good places in US: Stanford, UCLA, NYU, Georgia Tech, …

Outside of US: Weizmann (Israel), CWI (Amsterdam), ETH (Zurich)

Crypto at UCSD

Mihir Bellare:

One of the most prolific authors in all of computer science.
(h-index is 57, highest in our department.)

With Phil Rogaway, started practice-oriented provable security.

Developed HMAC, OAEP, and other standardized cryptographic protocols.

Part of team that developed Skein hash function which is a contender in the on-going NIST competition.

Daniele Micciancio:

Expert on lattices and lattice-based crypto

Does some work on using PL-techniques to prove things in crypto

Also had a hash function submission to the NIST competition
(but it got eliminated ☹)

Crypto at UCSD cont.

Hovav Shacham:

Did a lot of the early work on pairing-based cryptography

Well-known for BLS signature scheme (Boneh, Lynn, Shacham).

Russell Impagliazzo:

Foundational work on computational hardness.

Showed can build pseudorandom generators from one-way functions.