Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

Zhejiang University

23 November 2020

Cryptography Today

We will spend this first class surveying the uses, status, and prospects of cryptography in the current world.

Cryptography

Protection of data by transformations that turn useful and comprehensible plaintext into scrambled and meaningless ciphertext under control of secret keys.

What Drives Cryptography?

- Requirements
- Tools
- Imagination

The Scope of the Issue

Cryptography has gone from being a mysterous, secret, aspect of military, diplomatic, and intelligence communications to something "everyone" uses every day.

Fifty years back: Cryptography in 1970

- Governments
- Banks
- Oil companies

Pivotal Events

- 1967: David Kahn publishes *The Codebreakers*
- 1970: IBM adopts "Lucifer" cryptosystem
- 1975: Development of public-key cryptography
- 1981: First *Crypto* conference

1970s Scale

When the U.S. or NATO military bought a lot of crypto devices that meant a hundred thousand.

(I don't know Russian or Chinese numbers but I suspect that at that era they were smaller.)

Current Scale

- Every browser has *Transport Layer Security* the essential mechanism of internet security.
- Every smart-card has encryption.
- Every mobile phone has encryption.
- Many utility meters have encryption.

By the Numbers

Today there are billions of cryptographic devices, far more complex than those of 1970, used by most people every day whether they know it or not.

Crypto Is an Amplifier

Cryptography amplifies the security or insecurity of the key to be the security or insecurity of the message.

Cryptography Is a Separator

- Separate security from message path

Key Management Systems

- Key production facility
- Staging areas
- Individual users
- Lots of trust required

Key management reflects and affects the structure of the organizations it serves.

Problem of Scale

It is necessary to distinguish carefully between a system of encipherment envisioned for a momentary exchange of letters between several isolated people and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time.

Auguste Kerckhoffs, *La Cryptographie Militaire*, 1883, as quoted in David Kahn: *The Codebreakers*, 1967.

Essential Elements

- Block ciphers
- Public-key cryptography
- Message digests

Long Cycle Systems

- Xored "random" sequence of bits with plaintext
- Simple: transistors were pennies a piece
- Do it one bit at a time

Block Ciphers

- 32-, 64-, or 128-bit blocks
- Many rounds of computation
- Universal building block

Current Standard Block Ciphers

- AES (US and beyond)
- SM4 (China)
- Kuznyechik (Russian Federation)

Public-key Cryptography

- Key Distribution
- Digital Signatures

Key Management

Private Message Requires Unique Key

- 100 subscribers need 10,000 keys.

- Secret keys must be protected.

Digital Signatures

Settle Disputes

Between Sender and Receiver

- Only One Person Can Produce It

- Anyone Can Recognize It

Public Key Cryptography

- Keys Come In Inverse Pairs
- Given One — Can't Find the Other

Fundamental Property

- Public Key
  - In telephone directory
- Secret Key
  - In subscriber's safe

Solves Both Problems

Key Distribution: Encrypt With Public Key

Digital Signature: Encrypt With Secret Key

Signed and Sealed Message

$$\overbrace{\underbrace{\left\{\{message\}^{\text{Sender Private Key}}, SenderID\right\}}_{\text{Signed}}}^{\text{Sealed}}{}^{\text{Receiver Public Key}}$$

RSA* System

$$Message \rightarrow Message^{e} \pmod{p \times q}$$

Public Key is Product $p \times q$

Secret Key is Factors: (p, q)

* Rivest, Shamir, and Adleman

Certificates

- "Phonebook" of certificates
- Certificate is a signed public key.
- Certificate authority

Message Digest

- Small item inseperable from big item.
- Sign the small one.

Message Digests

- MD5
- SHA1, SHA2
- Kechak
- SM9

Cryptographic Standardization

- US Federal Information Processing Standards
- NSA Suite B
- GOST
- IETF

What's New in Cryptography

- Homomorphic Encryption
- Blockchains
- Quantum Computing
- Quantum Key Distribution

Homomorphic Encryption

- Public algorithm on secret data
- User homomorphically encrypt data
- Send to server
- Server computes on encrypted data
- Sends back encrypted results
- User decrypts

Problem: High Cost

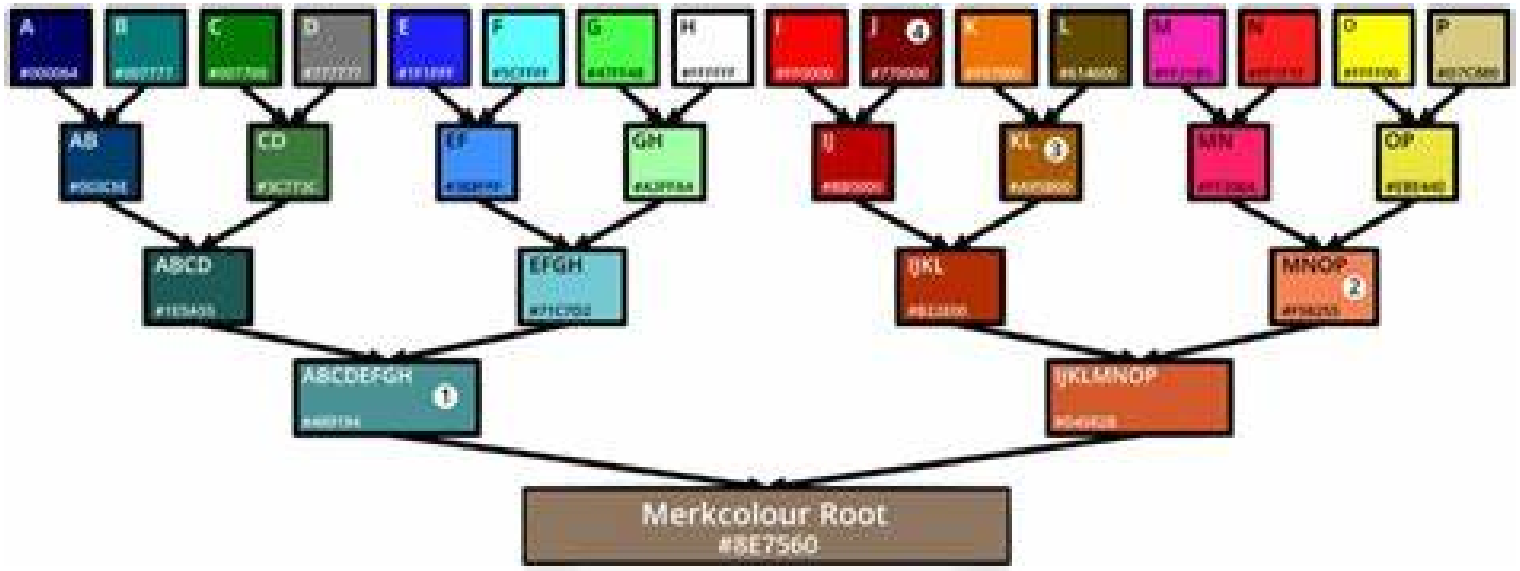
- Factor of billions in inefficiency
- Only useful in certain cases
- Private data queries
- Black conference bridge
- Others?

Block Chains

Secure, distributed, accounting

Ralph Merkle

Merkle Tree


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
AB
CD
EF
GH
IJ
KL
MN
OP
ABCD
EFGH
IJKL
MNOP
ABCDEFGH
IJKLMNOP
Merkcolour Root
#8E7560

Lenstra and Haber Timestamping

- Build Merkle tree of document hashes
- Publish root of tree (current block) in the New York Times every week

Blockchains Eliminate the Physical Element

Replace weekly publication of the current block with a constant discussion among the stakeholders.

Applications of Blockchains

- Money: Bitcoin
- Supply-chain management

Money

- Universal currency (Gold) gave way to
- Fiat currencies
- Maintained by central banks
- Added elasticity

Monetary Objectives

- Trans-national
- Inflation resistant
- Totally digital

Results

- Bitcoin has failed as currency
- Highly volatile commodity
- Inflation resistant ?

Supply-chain management

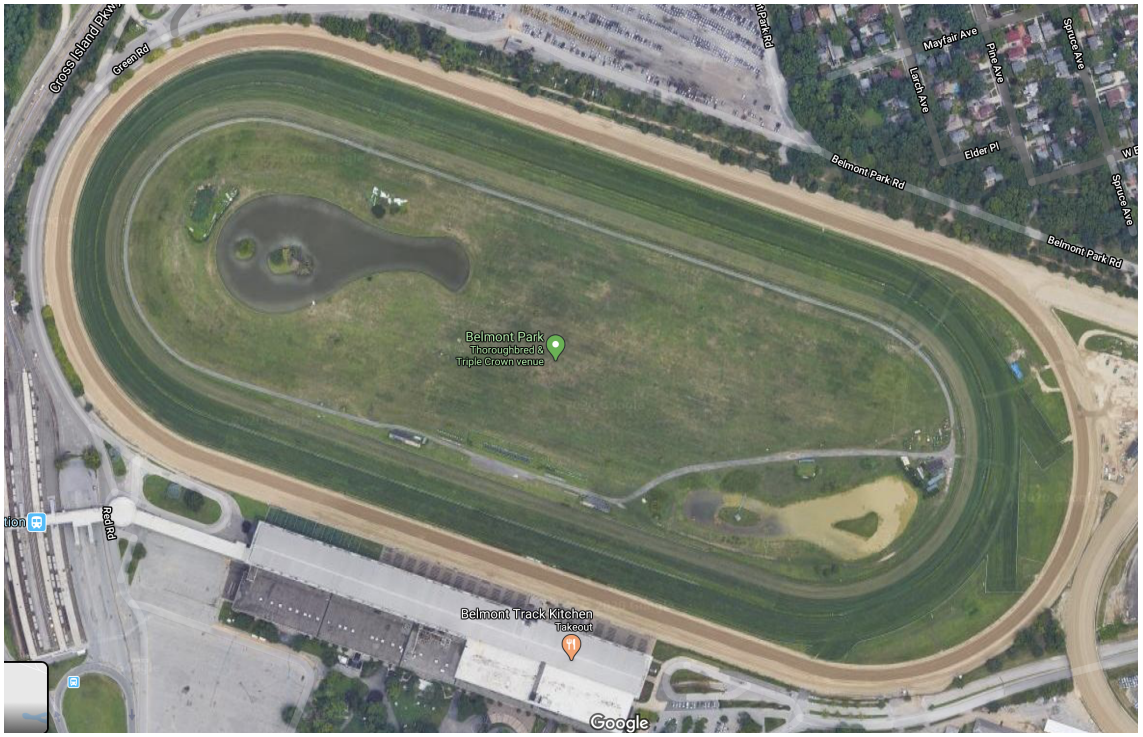
- Diverse players
- Not easily centralized
- Rescales rapidly

Why is Quantum Computing Important for Security?

Quantum computing will break the number theoretic public-key cryptosystems, RSA and both modular and elliptic-curve Diffie-Hellman, we use in internet commerce today.

How Does Quantum Computing Break Public-Key Crypto?

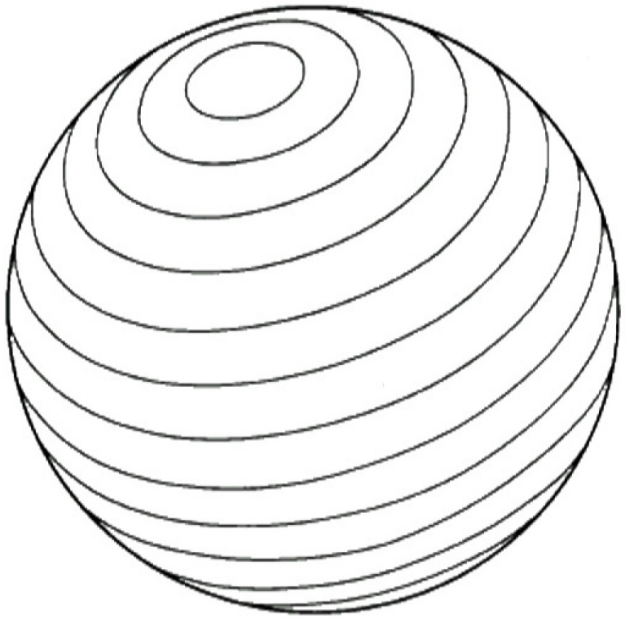
- In a public-key system, anyone can do the forward operation;
- It is going back that is hard.
- Like a race track



- Like walking on a track, if you go forward long enough, you will get back where you started.

- The step just before that is the decryption of what you started with.

- In systems like Diffie-Hellman and RSA, it is easy to move a long way forward very quickley.



You went all the way around a cycle but how long is the cycle? How far do you go? That's the big secret.

How Does Quantum Computing Break Public-Key Crypto?

Shor's Algorithm finds cycle length.

It will tell you how far to go.

Is Quantum Computing Real?
The big money thinks so.

Google

IBM

Intel

Microsoft

PRC

(Have I missed anyone?)

When Will it Happen?

No one knows but when it does it will be sudden by comparison with the rates of change of cybersecurity measures.

It Will Be Sudden

Cryptography will be a small part of the quantum-computing market; when QC come in it will sweep the world.

Quantum Key Distribution

- Channel dependent — not really cryptography
- Usually Runs over optical fiber — already fairly secure
- Intrusion detecting and anti-escrow

Quantum Resistant Algorithms

- Several possibilities for replacement
  - Coding theory (Mcleice) systems
  - Knapsack systems
  - Lattice-based systems