Information Theoretic Cryptography

Introduction

Benny Applebaum
Tel Aviv University

BIU Winter-School of Information-Theoretic Cryptography
February 2020
Cryptography

Communication and Computation in the presence of adversary

Honest party --- Adversary --- Honest party
Cryptography

- Encryption
- Authentication
Cryptography

- Commitments
- Coin Tossing
- ZK-Proofs
- Secure Computation
Computational Cryptography

Exploit **computational limitation** to achieve privacy/authenticity/...
Information-Theoretic Cryptography

Exploit information gaps to achieve privacy/authenticity/...
Information-Theoretic Cryptography

Exploit **information gaps** to achieve privacy/authenticity/…

Computationally unbounded  Adversary
Information-Theoretic Cryptography

Exploit information gaps to achieve privacy/authenticity/...
## (Shallow) Comparison

<table>
<thead>
<tr>
<th>Computational Cryptography</th>
<th>IT Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp-limited adversary</td>
<td>Comp-unbounded adversary</td>
</tr>
<tr>
<td>Unproven assumptions</td>
<td>Unconditional (no assumptions)</td>
</tr>
<tr>
<td>Composability issues</td>
<td>Good closure properties</td>
</tr>
<tr>
<td>Complicated def’s</td>
<td>Easy to define and work with (concretely)</td>
</tr>
<tr>
<td>Allows magic (PRG/PKC/OT/)</td>
<td>No magic (useless w/o information gaps)</td>
</tr>
<tr>
<td>Short keys</td>
<td>Long keys/large communication</td>
</tr>
<tr>
<td>May be comp. expensive</td>
<td>Typically fast (for short messages)</td>
</tr>
</tbody>
</table>
The Crypto Tower

- Obfustopia
- Secure Computation
- Public-Key
- Symmetric
- Information Theoretic

Assumption
The Crypto Tower: Realistic View

Obfustopia

Secure Computation

Public Key

Symmetric

Information Theoretic
The Crypto Tower: Realistic View

Obfustopia
- MMAPS-based obfuscation

Secure Computation
- GMW-MPC
- GMW-ZK
- Yao-GC

Public Key
- FDH-RSA
- RSA-OAEP
- DDH-KA

Symmetric
- HILL
- GL
- GGM

Information Theoretic
The best of all worlds

Obfustopia

Secure Computation

Public-Key

Symmetric

Information Theoretic
Obfustopia
Secure Computation
Public-Key
Symmetric
Information Theoretic

The best of all worlds

Problem
Problem
Two Case Studies:

Perfect Encryption & Error Correcting Codes

Image credits:
Photo: CC BY SA 4.0, by DobriZheglov, https://commons.wikimedia.org/wiki/File:Claude_Shannon_1776.jpg
Ali Baba's cave: CC BY 2.5, by Dake, https://commons.wikimedia.org/wiki/File:Zkip_alibaba{1,2,3}.png
Case Study 1: Perfect Encryption [Shannon 48]

Message $M \in \{0,1\}^n$
Case Study 1: Perfect Encryption [Shannon 48]

Secrecy: For every $X, Y \in \{0,1\}^n$

where $K \in_R K$

$E_K(X) \equiv E_K(Y)$

$M \in \{0,1\}^n$ → Encryption → Ciphertext $E_K(M)$ → Decryption → $M \in \{0,1\}^n$

Private key $K \in K$
Perfect Secrecy

**Secrecy:** For every $X, Y \in \{0,1\}^n$

where $K \in_R K$

$$\forall C, \Pr[K \in \{0,1\}^n \mid E_K(X) = C] = \Pr[K \in \{0,1\}^n \mid E_K(Y) = C]$$
**Statistical Secrecy**

**Secrecy:** For every $X, Y \in \{0,1\}^n$

where $K \in_R K$

\[
\forall \text{ set of ciphertexts } S, \Pr_K [E_K(X) \in S] \approx_\delta \Pr_K [E_K(Y) \in S]
\]
Statistical Secrecy

**Secrecy:** For every $X, Y \in \{0,1\}^n$

where $K \in_R K$

\[ E_K(X) \approx E_K(Y) \]

\[ \forall \text{ unbounded } Adv, \left| \Pr_K[Adv(E_K(X)) = 1] - \Pr_K[Adv(E_K(Y)) = 1] \right| \leq \delta \]
Computational Secrecy [GM’82]

**Secrecy:** For every $X, Y \in \{0,1\}^n$
where $K \in_R K$

$$E_K(X) \approx E_K(Y)$$

\[
\forall \text{comp} - \text{bounded Adv}, \left| \Pr_K[\text{Adv}(E_K(X)) = 1] - \Pr_K[\text{Adv}(E_K(Y)) = 1] \right| \leq \delta
\]
One-Time Pad is Perfectly Secure

\[ M \in [0, 1]^n \]

Private key \( K \in [0, 1]^n \)

\[ E_K(M) = K \oplus M \]

\[ \forall X, Y, \quad E_K(X) \equiv E_K(Y) \]

\[ D_K(C) = C \ominus K \]
Proof

\[ \forall X, Y, \quad E_K(X) \equiv E_K(Y) \]

Claim: \[ \forall X, C, \Pr[K \cdot E_K(X) = C] = 1/|G| \]

\[ \Pr[K + M = C] = \Pr[K = C - M] = 1/|G| \]

Put differently: For every \( X \) the mapping \( K \mapsto E_K(X) \) is a bijection from randomness space to ciphertext space.

In fact, non-degenerate linear mapping
Efficiency Measures

Communication, Randomness, Round complexity

• OTP: Optimal!

Message $M \in \{0,1\}^n$

Encryption:

$E_K(M) = K \oplus M$

Decryption:

$D_K(C) = C \oplus K$

Alice

Private key $K \in_R \{0,1\}^n$

Bob

Private key $K \in \{0,1\}^n$
Riddle: Broadcast Encryption [Fiat-Naor94]

Message $M \in \{0,1\}$
Subset $S$

Keys $K_1, \ldots, K_N$

Alice

Subset $S$

$E_K(M, S)$

Can decrypt iff $i \in S$

$K_1$

Bob 1

$i$

Bob $i$

$K_i$

Bob N

$K_N$
Riddle: Broadcast Encryption [Fiat-Naor94]

Communication?
Randomness (length of each key)?
Best tradeoffs?

Message $M \in \{0, 1\}$
Subset $S$

Communication?
Randomness (length of each key)?
Best tradeoffs?

E$_K(M, S)$
Subset $S$

Can decrypt iff $i \in S$

Alice

Keys $K_1, \ldots, K_N$

Bob 1

Bob $i$

Bob $N$
Case Study 2: Error Correction/Detection
[Hamming47, Shannon48]

Shannon: Solutions with optimal communication overhead
• Random linear mapping is optimal [Varshamov]
• Later efficient constructions

\[ M \in \{0,1\}^k \rightarrow \text{Encode} \rightarrow \text{Decode} \rightarrow M \in \{0,1\}^n \]

Can tamper (erase/corrupt) up to \( \delta \)-fraction of symbols

\[ C = (C_1, \ldots, C_N) \]
Unified view: Distributed Storage

Coding setting:
Adv. actively corrupts/erase servers

Message $M \in \{0,1\}^k$

Alice

Encoding

Bob N

Decoding

$M \in \{0,1\}^k$
Unified view: Distributed Storage

Secrecy setting:
Adversary passively corrupts servers

Message $M \in \{0,1\}^k$

Encoding $C_1$

Decoding $M \in \{0,1\}^k$

Alice

Bob $N$
Unified view: Distributed Storage

Secrecy setting:
Adversary passively corrupts servers

Message $M \in \{0,1\}^k$

Encoding

$E_K(M) = K + M$

Decoding

$M \in \{0,1\}^k$
Unified view: Distributed Storage

Secrecy setting:
Adversary passively corrupts servers

Message $M \in \{0,1\}^k$

Encoding

$K_i$

Decoding

$M + K_1 + \cdots + K_N$

$M \in \{0,1\}^k$
Can we achieve privacy & resiliency?

Secrecy setting:
Adversary passively corrupts servers

Message $M \in \{0,1\}^k$

Encoding

$M + K_1 + \cdots + K_N$

Decoding

$M \in \{0,1\}^k$
Secret-Sharing (Gilad’s talk)

Threshold setting:
Corruption bounds
\[ T_{active}, T_{erasure}, T_{passive} \]

Message \( M \in \{0,1\}^k \)

Alice

Encoding

\[ C_1, C_i, C_N \]

Decoding

\[ M \in \{0,1\}^k \]
Secret-Sharing (Gilad’s talk)

Threshold setting:
Corruption bounds $T_{active}, T_{erasure}, T_{passive}$

Message $M \in \{0,1\}^k$

Encoding

$C_1$

Bob N

Decoding

$M \in \{0,1\}^k$

Alice

$C_i$

$C_N$
General Secret-Sharing (Benny’s talk)

General corruption patterns:
• Related to Broadcast encryption problem
• Huge gaps between LBs and UBs

Message $M \in \{0,1\}^k$

Alice

Encoding

$C_1$

Bob N

Decoding

$M \in \{0,1\}^k$
Private Information Retrieval (Yuval+Klim)

Message $M \in \{0,1\}^k$

Alice

Encoding

$C_1$

$C_i$

$C_N$

Decoding

$M \in \{0,1\}^k$

Bob N
Private Information Retrieval (Yuval+Klim)
Private Information Retrieval (Yuval+Klim)

$\index i \in \{1, \ldots, k\}$

Bob N

Hide access pattern $i$

Alice
Private Information Retrieval (Yuval+Klim)

Hide access pattern $i$
- Power of non-linearity
- Huge gaps between LBs and UPs

Bob N

index $i$

$M[i]$

Alice
Computation: Beyond Storage

\[ x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \]

Trusted Party
Consensus (Ittai’s talk)
Achieving Agreement at the presence of failures/corruptions/delays

Only correctness requirement
No privacy requirements
General Secure Computation (Yuval’s talk)

Compute joint function of the parties inputs

Passive adversaries
• Privacy
Active adversaries
• Correctness & Privacy

$F(x_1, ..., x_5)$
General Secure Computation (Yuval’s talk)

Compute joint function of the parties inputs

\[ x_1 + \ldots + x_5 \]

Challenge:
Design 1-private protocol for sum over \( G \)
Proofs in Non-Interactive Setting (Niv’s Talk)

\[ F(x_1, \ldots, x_5) = 1 \]
Randomized Encoding & Constant-Round MPC
(Benny’s Talk)

\[ F(x_1, \ldots, x_5) \]
Summary: Information Theoretic Cryptography

• Cool questions

• Exciting connections with
  • Coding, Information-theory, Communication Complexity, Computational complexity, Theory of Computation

• Relevant to computational crypto as well

• Many open problems

• New conference: ITC 2020, June 17-19, 2020 in Boston
  • PC: Daniel Wichs, General Chairs: Adam Smith & Yael Kalai

Have a Good Time!