Cryptography: The art of the impossible

Joshua D. Guttman
Worcester Polytechnic Institute
The MITRE Corporation

March 2013
Bertinoro International Spring School

Thanks to the US National Science Foundation, under grant 1116557

guttman@wpi.edu

Art of the impossible

Or rather: The exceedingly unlikely

- Cryptography is about randomized games between
  - Adversary
  - System, i.e. compliant processes

Art of the impossible

Or rather: The exceedingly unlikely

- Cryptography is about randomized games between
  - Adversary
  - System, i.e. compliant processes
- Criterion of a good cryptosystem:
  - No adversary strategy is better than chance

Art of the impossible

Or rather: The exceedingly unlikely

- Cryptography is about randomized games between
  - Adversary
  - System, i.e. compliant processes
- Criterion of a good cryptosystem:
  - No adversary strategy is better than chance
- Games characterize:
  - Secrecy
  - Message integrity/digital signature
  - Many other functionalities

Computational Style

"No adversary strategy is better than chance"

- "Adversary strategy" means:

  Tractable randomized algorithm $\mathcal{A}$

- $\mathcal{A}$ is "better than chance" means

  Expectation of $\mathcal{A}$ differs little from chance

Computational Style

"No adversary strategy is better than chance"

- "Adversary strategy" means:

  Polynomial-time randomized algorithm $\mathcal{A}$

- $\mathcal{A}$ is "better than chance" means

  Expectation of $\mathcal{A}$ differs little from chance

Computational Style

"No adversary strategy is better than chance"

- "Adversary strategy" means:

  Polynomial-time randomized algorithm $\mathcal{A}$
  Runtime bounded by $p(n)$ for security parameter n

- $\mathcal{A}$ is "better than chance" means

  Expectation of $\mathcal{A}$ differs little from chance

Computational Style

"No adversary strategy is better than chance"

- "Adversary strategy" means:

  Polynomial-time randomized algorithm $\mathcal{A}$
  Runtime bounded by $p(n)$ for security parameter n

- $\mathcal{A}$ is "better than chance" means

  Expectation of $\mathcal{A}$ differs little from chance

$$E_{\mathcal{A}}(n) - E_{chance}(n) < 1/q(n)$$

for all polynomials $q(n)$
and sufficiently large n

Computational Style

"No adversary strategy is better than chance"

- "Adversary strategy" means:

  Polynomial-time randomized algorithm $\mathcal{A}$
  Runtime bounded by $p(n)$ for security parameter n

- $\mathcal{A}$ is "better than chance" means

  Expectation of $\mathcal{A}$ differs little from chance

$$E_{\mathcal{A}}(n) - E_{chance}(n) < 1/q(n)$$

for all polynomials $q(n)$
and sufficiently large n

An asymptotic property

CPA game: Distinguishing ciphertexts

A specification for symmetric-key secrecy

1. System generates key k of length n
2. While adversary requests,
   - System provides $\{\!| s |\!\}_k$ for chosen plaintexts s
3. Adversary chooses two target msgs m_0, m_1
4. System flips coin, obtaining bit b
5. System emits test value $c := \{\!| m_b |\!\}_k$
6. While adversary requests,
   - System provides $\{\!| s |\!\}_k$ for chosen plaintexts s
7. Adversary outputs bit b'

CPA game: Distinguishing ciphertexts

A specification for symmetric-key secrecy

1. System generates key k of length n
2. While adversary requests,
   - System provides $\{\!|\ s\ |\!\}_k$ for chosen plaintexts s
3. Adversary chooses two target msgs m_0, m_1
4. System flips coin, obtaining bit b
5. System emits test value $c := \{\!|\ m_b\ |\!\}_k$
6. While adversary requests,
   - System provides $\{\!|\ s\ |\!\}_k$ for chosen plaintexts s
7. Adversary outputs bit b'

Adversary wins run if $b = b'$

$$E_{chance}(n) = 1/2$$

Corollary: CPA-secure encryption is probabilistic

Consider attacker strategy $\mathcal{A}_1$:

- Request encryptions of m_0, obtaining $c^* := \{\!|\, m_0 \,|\!\}_k$
- If test value $c = c^*$, emit 0
- Otherwise, flip coin

Corollary: CPA-secure encryption is probabilistic

Consider attacker strategy $\mathcal{A}_1$:

- Request encryptions of m_0, obtaining $c^* := \{\!|\, m_0 \,|\!\}_k$
- If test value $c = c^*$, emit 0
- Otherwise, flip coin

Message m_0 can't always yield same value

Corollary: CPA-secure encryption is probabilistic

Consider attacker strategy $\mathcal{A}_1$:

- Request encryptions of m_0, obtaining $c^* := \{\!|\, m_0 \,|\!\}_k$
- If test value $c = c^*$, emit 0
- Otherwise, flip coin

Message m_0 can't always yield same value

$$P[\{\!|\, m_0 \,|\!\}_k = c \mid b = 0] - P[\{\!|\, m_0 \,|\!\}_k = c \mid b = 1] < 1/2q(n)$$

Pseudorandom Expander

Let $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$, where $\ell(n) > n$

Consider the game:

1. System flips a coin, obtaining a bit b
2. If $b = 0$, then return r, where $r \xleftarrow{u} \{0,1\}^{\ell(n)}$ is selected randomly
3. If $b = 1$, then return $G(s)$, where $s \xleftarrow{u} \{0,1\}^n$ is selected randomly
4. Adversary receives this value and returns a bit b'

Adversary wins if $b = b'$

Pseudorandom Expander

Let $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$, where $\ell(n) > n$

Consider the game:

1. System flips a coin, obtaining a bit b
2. If $b = 0$, then return r, where $r \overset{u}{\leftarrow} \{0,1\}^{\ell(n)}$ is selected randomly
3. If $b = 1$, then return $G(s)$, where $s \overset{u}{\leftarrow} \{0,1\}^n$ is selected randomly
4. Adversary receives this value and returns a bit b'

Adversary wins if $b = b'$

G is a pseudorandom expander if no adversary strategy is much better than choosing b' at random

A crypto construction, 1

Let G be a pseudorandom function expander

$$G : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$$

To encrypt m with key k of length n output

$$G(k) \oplus m$$

A crypto construction, 1

Let G be a pseudorandom function expander

$$G : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$$

To encrypt m with key k of length n output

$$G(k) \oplus m$$

Is this construction CPA-secure?

A Game for Construction 1

Indistinguishability under eavesdropping

1. System generates key k of length n
2. While adversary requests,
   - System provides $\{\!|\, s \,|\!\}_k$ for chosen plaintexts s
3. Adversary chooses two target msgs m_0, m_1
4. System flips coin, obtaining bit b
5. System emits test value $c := \{\!|\, m_b \,|\!\}_k$
6. While adversary requests,
   - System provides $\{\!|\, s \,|\!\}_k$ for chosen plaintexts s
7. Adversary outputs bit b'

Adversary wins run if $b = b'$

$E_{chance}(n) = 1/2$

A Game for Construction 1

Indistinguishability under eavesdropping

1. System generates key k of length n
2. While adversary requests,
   - System provides $\{\!| s |\!\}_k$ for chosen plaintexts s
3. Adversary chooses two target msgs m_0, m_1
4. System flips coin, obtaining bit b
5. System emits test value $c := \{\!| m_b |\!\}_k$
6. While adversary requests,
   - System provides $\{\!| s |\!\}_k$ for chosen plaintexts s
7. Adversary outputs bit b'

Adversary wins run if $b = b'$

$$E_{chance}(n) = 1/2$$

Pseudorandom Function Family

Let $F\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{\ell(n)}$ and let

- $F(k,\cdot)$ be the function of its second argument, for $k \xleftarrow{u} \{0,1\}^n$
- f be chosen at random from all functions $f\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$

F is a pseudorandom function family if adversary cannot distinguish between $F(k,\cdot)$ and f

A crypto construction, 2

Let F be a pseudorandom function family

$$F : \{0,1\}^{2n} \rightarrow \{0,1\}^{\ell(n)}$$

To encrypt m with key k

1. select $r \stackrel{u}{\leftarrow} \{0,1\}^{\ell(n)}$ at random
2. output

$$\langle r,\ F(k,r) \oplus m \rangle$$

A crypto construction, 2

Let F be a pseudorandom function family

$$F : \{0,1\}^{2n} \rightarrow \{0,1\}^{\ell(n)}$$

To encrypt m with key k

1. select $r \xleftarrow{u} \{0,1\}^{\ell(n)}$ at random
2. output

$$\langle r,\ F(k,r) \oplus m \rangle$$

Is this construction CPA-secure?

A crypto construction, 2

Let F be a pseudorandom function family

$$F : \{0,1\}^{2n} \to \{0,1\}^{\ell(n)}$$

To encrypt m with key k

1. select $r \stackrel{u}{\leftarrow} \{0,1\}^{\ell(n)}$ at random
2. output

$$\langle r,\ F(k,r) \oplus m \rangle$$

Is this construction CPA-secure?

Proof idea: If there's a good strategy $\mathcal{A}$ in the CPA game, we could use it distinguish $F(k,\cdot)$ from a random f

A crypto construction, 2

Let F be a pseudorandom function family

$$F : \{0,1\}^{2n} \to \{0,1\}^{\ell(n)}$$

To encrypt m with key k

1. select $r \stackrel{u}{\leftarrow} \{0,1\}^{\ell(n)}$ at random
2. output

$$\langle r,\ F(k,r) \oplus m \rangle$$

Is this construction CPA-secure?

Proof idea: If there's a good strategy $\mathcal{A}$ in the CPA game, we could use it distinguish $F(k,\cdot)$ from a random f
Reduce problem of distinguishing $F(k,\cdot)$ to the problem of breaking this construction

Three Elements of Modern Cryptography

- Define crypto functionalities by games
  - Adversary wins by distinguishing
- Assume hard challenges
  - e.g. F a pseudorandom function family
- Prove constructions by reduction:
  - A strategy against the construction yields a strategy against the assumption

Contrast with Strand Space Model

1. Cryptographic model is
   - quantitative
   - probabilistic
   - asymptotic

Contrast with Strand Space Model

1. Cryptographic model is
   - quantitative
   - probabilistic
   - asymptotic
2. Cryptographic model is about games
   - Though: Strand space results also concern all adversary strategies

Contrast with Strand Space Model

1. Cryptographic model is
   - quantitative
   - probabilistic
   - asymptotic
2. Cryptographic model is about games
   - Though: Strand space results also concern all adversary strategies
3. Cryptographic model is about distinguishing runs
   - Strand space results about all bundles (or models) considered each individually

Contrast with Strand Space Model

1. Cryptographic model is
   - quantitative
   - probabilistic
   - asymptotic
2. Cryptographic model is about games
   - Though: Strand space results also concern all adversary strategies
3. Cryptographic model is about distinguishing runs
   - Strand space results about all bundles (or models) considered each individually

Item 3 is the decisive difference