Game Playing

Advanced Topics in ~~Cybersecurity~~Cryptography (7CCSMATC)

Martin R. Albrecht

Outline

Introduction

Main Reference

Mike Rosulek. The Joy of Cryptography. https://joyofcryptography.com. self published, 2021[1]

- The Joy of Cryptography is an amazing textbook. Read it!
- Mike Rosulek is a cryptographer and associate professor in the School of EECS at Oregon State University
- His research focuses is on cryptographic protocols for secure computation
- NSF CAREER Award in 2013.

[1] Mike proves the result in this lecture using a very nice and intuitive framework. We will focus on traditional game-hopping proofs, because that allows you to digest many research papers in the area of cryptography.

Programme

We have defined security, it is time for us to prove some schemes secure.

IND-CPA Security of the OTP

$E(m)$

1 : $k \leftarrow\$ \{0,1\}^{|m|}$
2 : $c \leftarrow k \oplus m$
3 : **return** c

Figure 1: One-Time Pad

IND-CPA

1 : $k \leftarrow\$ \mathcal{K}$
2 : $b \leftarrow\$ \{0,1\}$
3 : $b' \leftarrow \mathcal{D}^{\mathsf{E}}$
4 : **return** $b = b'$

$\mathsf{E}(m_0, m_1)$

1 : **if** $|m_0| \neq |m_1|$ **then**
2 : **return** $\perp$
3 : $c \leftarrow\$ E_k(m_b)$
4 : **return** c

Figure 2: Indistinguishability under Chosen Plaintext Attacks (IND-CPA)

$$\mathrm{Adv}_{E}^{\text{ind-cpa}}(\mathcal{D}) = \left| \Pr[\text{IND-CPA}^{\mathcal{D}} = 1] - 1/2 \right|.$$

Conceptually, proving insecurity is straight forward

$E(m)$

1 : $k \leftarrow\$ \{0,1\}^{|m|}$
2 : $c \leftarrow k$ & m // bit-wise AND
3 : **return** c, h

IND-CPA

1 : $k \leftarrow\$ \mathcal{K}$
2 : $b \leftarrow\$ \{0,1\}$
3 : $b' \leftarrow \mathcal{D}^{\mathrm{E}}$
4 : **return** $b = b'$

$\mathrm{E}(m_0, m_1)$

1 : **if** $|m_0| \neq |m_1|$ **then**
2 : **return** $\perp$
3 : $c \leftarrow\$ E_k(m_b)$
4 : **return** c

Conceptually, proving insecurity is straight forward

$E(m)$

1 : $k \leftarrow\!\$ \{0,1\}^{|m|}$

2 : $c \leftarrow k$ & m // bit-wise AND

3 : **return** c, h

IND-CPA

1 : $k \leftarrow\!\$ \mathcal{K}$

2 : $b \leftarrow\!\$ \{0,1\}$

3 : $b' \leftarrow \mathcal{D}^{\mathrm{E}}$

4 : **return** $b = b'$

$\mathrm{E}(m_0, m_1)$

1 : **if** $|m_0| \neq |m_1|$ **then**

2 : **return** $\perp$

3 : $c \leftarrow\!\$ E_k(m_b)$

4 : **return** c

Break it!

Conceptually, proving insecurity is straight forward

$E(m)$

1: $k \leftarrow\$ \{0,1\}^{|m|}$
2: $c \leftarrow k$ & m // bit-wise AND
3: **return** c, h

IND-CPA

1: $k \leftarrow\$ \mathcal{K}$
2: $b \leftarrow\$ \{0,1\}$
3: $b' \leftarrow \mathcal{D}^{\mathsf{E}}$
4: **return** $b = b'$

$\mathsf{E}(m_0, m_1)$

1: **if** $|m_0| \neq |m_1|$ **then**
2: **return** $\perp$
3: $c \leftarrow\$ E_k(m_b)$
4: **return** c

Break it!

1. $m_0, m_1 \leftarrow 0^n, 1^n$
2. $c^* \leftarrow \mathsf{E}(m_0, m_1)$
3. if $c^* = 0^n$
   output $b' = 0$
   else $b' = 1$

Conceptually, proving insecurity is straight forward

$E(m)$

1 : $k \leftarrow\$ \{0,1\}^{|m|}$
2 : $c \leftarrow k$ & m // bit-wise AND
3 : **return** c, h

IND-CPA

1 : $k \leftarrow\$ \mathcal{K}$
2 : $b \leftarrow\$ \{0,1\}$
3 : $b' \leftarrow \mathcal{D}^{\mathrm{E}}$
4 : **return** $b = b'$

$\mathrm{E}(m_0, m_1)$

1 : **if** $|m_0| \neq |m_1|$ **then**
2 : **return** $\perp$
3 : $c \leftarrow\$ E_k(m_b)$
4 : **return** c

Break it!

1. $m_0, m_1 \leftarrow 0^n, 1^n$
2. $c^* \leftarrow \mathrm{E}(m_0, m_1)$
3. if $c^* = 0^n$
   output $b' = 0$
   else $b' = 1$

- $\Pr[c^* = 0^n \mid b = 0] = 1$
- $\Pr[c^* = 0^n \mid b = 1] = 1/2^n$

“Conceptually” is the operative word here!

Finding efficient attacks is a key cryptographic research activity and many people, including me, have made a career out of it.

How do we show the absence of attacks?

Game hopping!

How do we show the absence of attacks?

Hybrids!

Game Hopping / Hybrids

Game_0	Game_1	Game_2
1 : Step 1	1 : Step 1	1 : Step 1
2 : Step 2	2 : Step 2a	2 : Step 2a
3 : **return** $\mathcal{A}^P(x)$	3 : **return** $\mathcal{A}^P(x)$	3 : **return** 0

We want to establish that[2]

$$|\Pr[\mathsf{Game}_0{}^{\mathcal{A}}] - 1/2| \leq \mathrm{negl}(\lambda) + \mathrm{poly}(\lambda) \cdot |\Pr[\mathsf{Game}_1{}^{\mathcal{A}}] - 1/2| \text{ and}$$
$$|\Pr[\mathsf{Game}_1{}^{\mathcal{A}}] - 1/2| \leq \mathrm{negl}(\lambda) + \mathrm{poly}(\lambda) \cdot |\Pr[\mathsf{Game}_2{}^{\mathcal{A}}] - 1/2|$$

which implies

$$|\Pr[\mathsf{Game}_0{}^{\mathcal{A}}] - 1/2| \leq \mathrm{negl}(\lambda) + \mathrm{poly}(\lambda) \cdot |\Pr[\mathsf{Game}_2{}^{\mathcal{A}}] - 1/2| .$$

[2] "$\mathrm{negl}(\lambda)$" means $< 1/\mathrm{poly}(\lambda)$, i.e. strictly smaller.

Proof: Game 0

Game_0	$\mathrm{E}(m_0, m_1)$
1 : $k \leftarrow\!\$\ \mathcal{K}$	1 : **if** $\lvert m_0\rvert \neq \lvert m_1\rvert$ **then**
2 : $b \leftarrow\!\$\ \{0,1\}$	2 : **return** $\perp$
3 : $b' \leftarrow \mathcal{D}^{\mathrm{E}}$	3 : $c \leftarrow\!\$\ E_k(m_b)$
4 : **return** $b = b'$	4 : **return** c

$$\mathrm{Adv}_E^{\text{ind-cpa}}(\mathcal{D}) = |\mathrm{Pr}[\text{IND-CPA}^{\mathcal{D}} = 1] - 1/2| = |\mathrm{Pr}[{\mathrm{Game}_0}^{\mathcal{D}} = 1] - 1/2|$$

Proof: Game 1

Game_1	$\mathrm{E}(m_0, m_1)$
1 : $k \leftarrow\!\$\ \mathcal{K}$	1 : **if** $\lvert m_0\rvert \neq \lvert m_1\rvert$ **then**
2 : $b \leftarrow\!\$\ \{0,1\}$	2 : **return** $\perp$
3 : $b' \leftarrow \mathcal{D}^{\mathrm{E}}$	3 : $k' \leftarrow\!\$\ \{0,1\}^{\lvert m\rvert}$
4 : **return** $b = b'$	4 : $c \leftarrow k' \oplus m_b$
	5 : **return** c

We just expanded the definition of the OTP, the two games are identical.

$$\Pr[{\mathrm{Game}_0}^{\mathcal{D}} = 1] = \Pr[{\mathrm{Game}_1}^{\mathcal{D}} = 1]$$

Proof: Game 2

Game_2	$\mathrm{E}(m_0, m_1)$
1 : $k \leftarrow\!\$\ \mathcal{K}$	1 : **if** $\lvert m_0\rvert \neq \lvert m_1\rvert$ **then**
2 : $b \leftarrow\!\$\ \{0,1\}$	2 : **return** $\perp$
3 : $b' \leftarrow \mathcal{D}^{\mathrm{E}}$	3 : $k' \leftarrow\!\$\ \{0,1\}^{\lvert m\rvert}$
4 : **return** $b = b'$	4 : $c \leftarrow k'$
	5 : **return** c

For any $y \in \{0,1\}^n$ and any $m \in \{0,1\}^n$, it holds that
$\Pr[x = y \mid x \leftarrow\!\$\ \{0,1\}^n] = \Pr[x = y \oplus m \mid x \leftarrow\!\$\ \{0,1\}^n] = \Pr[x \oplus m = y \mid x \leftarrow\!\$\ \{0,1\}^n]$.

$$\Pr[\mathrm{Game}_1{}^{\mathcal{D}} = 1] = \Pr[\mathrm{Game}_2{}^{\mathcal{D}} = 1]$$

Proof: Finish

Game_2	$\mathsf{E}(m_0, m_1)$
$k \leftarrow\$ \mathcal{K}$	**if** $\lvert m_0\rvert \neq \lvert m_1\rvert$ **then**
$b \leftarrow\$ \{0,1\}$	**return** $\perp$
$b' \leftarrow \mathcal{D}^{\mathsf{E}}$	$k' \leftarrow\$ \{0,1\}^{\lvert m\rvert}$
return $b = b'$	$c \leftarrow k'$
	return c

We no longer use m_0, m_1, b: $\mathbf{Pr}[\mathsf{Game}_2{}^{\mathcal{D}} = 1] = 1/2$.

$$\begin{aligned}\mathsf{Adv}_E^{\text{ind-cpa}}(\mathcal{D}) &= |\mathbf{Pr}[\text{IND-CPA}^{\mathcal{D}} = 1] - 1/2| = |\mathbf{Pr}[\mathsf{Game}_0{}^{\mathcal{D}} = 1] - 1/2| \\ &= |\mathbf{Pr}[\mathsf{Game}_1{}^{\mathcal{D}} = 1] - 1/2| \\ &= |\mathbf{Pr}[\mathsf{Game}_2{}^{\mathcal{D}} = 1] - 1/2| = |1/2 - 1/2| = 0\end{aligned}$$

Identical Hybrids: Dead Code

$\text{Game}_0(x)$	$\text{Game}_1(x)$
1 : **if** x is even **return** 0	1 : **if** x is even **return** 0
2 : **else if** x is odd **return** 1	2 : **else if** x is odd **return** 1
3 : **else return** -1	3 : **else return** ∞

Identical Hybrids: Unused Variables and Parameters

$\mathrm{Game}_0(\mathrm{x})$	$\mathrm{Game}_1(\mathrm{x})$	$\mathrm{Foo}(a, b)$
1 : $\mathrm{Foo}(x, x)$	1 : $\mathrm{Foo}(x, 0^\lambda)$	1 : $k \leftarrow\!\!\$\ \{0,1\}^\lambda$
		2 : **return** $a \oplus k$

Identical Hybrids: Inlining

$\mathrm{Game}_0(x)$	$\mathrm{Game}_1(x)$
1 : $\mathrm{Foo}(x)$	1 : $k \leftarrow\!\!\$\ \{0,1\}^\lambda$
$\mathrm{Foo}(a)$	2 : **return** $x \oplus k$
1 : $k \leftarrow\!\!\$\ \{0,1\}^\lambda$	
2 : **return** $a \oplus k$	

Identical Hybrids: Loop Unrolling

Game_0(x,n)	Game_1(x,n)
1 : **if** $\lambda < n$ **return** $\perp$	1 : **if** $\lambda < n$ **return** $\perp$
2 : **for** $0 \leq i < \lambda$ **do**	2 : **for** $0 \leq i < n$
3 : $\quad \text{Foo}(x, i)$	3 : $\quad \text{Foo}(x, i)$
	4 : **for** $n \leq i < \lambda$
	5 : $\quad \text{Foo}(x, i)$

Notes on the One-Time Pad

Information-Theoretic Security

- The reduction (aka the proof) establishes that the one-time pad is (t, ε)-secure for any $t < \infty$ and $\varepsilon > 0$.
  - It achieves **information-theoretic security**
- There exists an entire subfield of cryptography for that, aptly named "information-theoretic cryptography"
  - The one-time pad is not the only information-theoretically secure construction, there is also secret sharing, secure multiparty computation, private information retrieval
  - The 10th BIU Winter School on Cryptography was dedicated to it[3]
  - Vinod Vaikuntanathan gave a talk about open problems[4].

[3] `https://web.archive.org/web/20230604034629/https://cyber.biu.ac.il/event/the-10th-biu-winter-school-on-cryptography/`

[4] Vinod Vaikuntanathan. Some Open Problems in Information-Theoretic Cryptography. 37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2017). `https://drops.dagstuhl.de/storage/00lipics/lipics-vol093-fsttcs2017/LIPIcs.FSTTCS.2017.5/LIPIcs.FSTTCS.2017.5.pdf`. 2017.

Brittle

- The proof assumes that for each message a new uniform mask k is chosen
- If that condition is violated, it is easy to break the one-time pad by using $(m_0 \oplus k) \oplus (m_1 \oplus k) = m_0 \oplus m_1$.[5]
- This requires transporting random key material of the same length as the message securely.

[5] Or any stream cipher, see e.g. Christina Garman, Kenneth G. Paterson, and Thyla van der Merwe. **Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS.** In: *USENIX Security 2015*. Ed. by Jaeyeon Jung and Thorsten Holz. USENIX Association, Aug. 2015, pp. 113–128. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/garman

Quantum Key Distribution (QKD)

- There's a big marketing push ongoing to sell QKD: "secured by the laws of physics"
- These systems are point-to-point only, slow, limited to ~100km and not, in fact, guaranteed by the laws of physics[1,2]
- QKD solutions will have to compete with the one-time pad: fill up a 1TB hard-disk with random bits, send a courier to the destination, select random bits by communicating an offset into data

[1] "Quantum key distribution and Quantum cryptography vendors—and the media—occasionally state bold claims based on theory—e.g., that this technology offers 'guaranteed' security based on the laws of physics. Communications needs and security requirements physically conflict in the use of QKD/QC, and the engineering required to balance these fundamental issues has extremely low tolerance for error. Thus, security of QKD and QC is highly implementation-dependent rather than assured by laws of physics." (NSA)

[2] "Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors." (GCHQ)

Fin

Read The Joy of Cryptography!

References I

[GPM15] Christina Garman, Kenneth G. Paterson, and Thyla van der Merwe. Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS. In: *USENIX Security 2015*. Ed. by Jaeyeon Jung and Thorsten Holz. USENIX Association, Aug. 2015, pp. 113–128. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/garman.

[Ros21] Mike Rosulek. The Joy of Cryptography. https://joyofcryptography.com. self published, 2021.

[Vai17] Vinod Vaikuntanathan. Some Open Problems in Information-Theoretic Cryptography. 37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2017). https://drops.dagstuhl.de/storage/00lipics/lipics-vol093-fsttcs2017/LIPIcs.FSTTCS.2017.5/LIPIcs.FSTTCS.2017.5.pdf. 2017.