(Computational) Indistinguishability

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

Martin R. Albrecht

Introduction

Assumptions

- We reached the limits of what can be done information-theoretically.
- Most cryptographic constructions give you conditional security: its security properties hold if and only if some computational task is hard.
- Examples
    - inverting AES is hard,
    - factoring large integers is hard, or
    - finding short solutions to a system of linear equations modulo q is hard.

What a proof gives you

The only way for an adversary **with these powers** to break **this specific security goal** is to solve this hard computational problem efficiently.

AES-CTR Mode

IND-CPA	$E(m_0, m_1 \in \{0,1\}^{128 \cdot n})$	$E_k(m \in \{0,1\}^{128 \cdot n})$
1: $k \leftarrow\!\!\$ \{0,1\}^{128}$	1: if $|m_0| \neq |m_1|$ then	1: $iv \leftarrow\!\!\$ \{0,1\}^{128}$
2: $b \leftarrow\!\!\$ \{0,1\}$	2: return $\perp$	2: $m_0, \ldots, m_{n-1} \leftarrow m$
3: $b' \leftarrow \mathcal{D}^E$	3: $c \leftarrow\!\!\$ E_k(m_b)$	3: for $0 \leq i < n$ do
4: return $b = b'$	4: return c	4: $\quad c_i \leftarrow \text{AES-128}(k, iv + i) \oplus m_i$
		5: $c \leftarrow iv, c_0, \ldots, c_{n-1}$
		6: return c

We would like to show that c is indistinguishable from random strings, just like the one-time pad.

1. The One-Time Pad samples $k \leftarrow\!\!\$ \{0,1\}^{n \cdot 128}$, we sample $iv \leftarrow\!\!\$ \{0,1\}^{128}$ and then compute AES-128$(k, iv + i)$ for $0 \leq i < n$.
   - If we obtain $iv_0 + i = iv_1 + j$ then we got a Two-Time Pad:

1. The One-Time Pad samples $k \leftarrow\!\!\!\$\ \{0,1\}^{n \cdot 128}$, we sample $iv \leftarrow\!\!\!\$\ \{0,1\}^{128}$ and then compute AES-128($k, iv + i$) for $0 \leq i < n$.
    - If we obtain $iv_0 + i = iv_1 + j$ then we got a Two-Time Pad:
        Solution Use the Fundamental Lemma of Game Playing to sample without replacement

1. The One-Time Pad samples $k \leftarrow\!\!\$\ \{0,1\}^{n \cdot 128}$, we sample $iv \leftarrow\!\!\$\ \{0,1\}^{128}$ and then compute AES-128$(k, iv + i)$ for $0 \leq i < n$.
   - If we obtain $iv_0 + i = iv_1 + j$ then we got a Two-Time Pad:

     Solution Use the Fundamental Lemma of Game Playing to sample without replacement
   - Need to show that if you can break this scheme, then AES-128 is no PRP

1. The One-Time Pad samples $k \leftarrow_{\$} \{0,1\}^{n \cdot 128}$, we sample $iv \leftarrow_{\$} \{0,1\}^{128}$ and then compute AES-128$(k, iv + i)$ for $0 \leq i < n$.
   - If we obtain $iv_0 + i = iv_1 + j$ then we got a Two-Time Pad:

     Solution Use the Fundamental Lemma of Game Playing to sample without replacement
   - Need to show that if you can break this scheme, then AES-128 is no PRP

     Solution This lecture

1. The One-Time Pad samples $k \leftarrow_\$ \{0,1\}^{n \cdot 128}$, we sample $iv \leftarrow_\$ \{0,1\}^{128}$ and then compute AES-128$(k, iv + i)$ for $0 \leq i < n$.

   - If we obtain $iv_0 + i = iv_1 + j$ then we got a Two-Time Pad:

     Solution Use the Fundamental Lemma of Game Playing to sample without replacement

   - Need to show that if you can break this scheme, then AES-128 is no PRP

     Solution This lecture

   - Even if AES-128 is a PRP, we want a PRF

1. The One-Time Pad samples $k \leftarrow\!\!\$ \{0,1\}^{n \cdot 128}$, we sample $iv \leftarrow\!\!\$ \{0,1\}^{128}$ and then compute AES-128$(k, iv + i)$ for $0 \leq i < n$.

   - If we obtain $iv_0 + i = iv_1 + j$ then we got a Two-Time Pad:

     Solution Use the Fundamental Lemma of Game Playing to sample without replacement

   - Need to show that if you can break this scheme, then AES-128 is no PRP

     Solution This lecture

   - Even if AES-128 is a PRP, we want a PRF

     Solution Use the PRP-PRF Switching Lemma

Proof Step 1: Sampling without Replacement

Game_0	$E(m_0, m_1 \in \{0,1\}^{128 \cdot n})$	$E_k\left((m_0, \ldots, m_{n-1}) \in (\{0,1\}^{128})^n\right)$
1: $\mathcal{I}, bad \leftarrow \emptyset, false$	1: **if** $|m_0| \neq |m_1|$ **then**	1: $iv \leftarrow\!\!\$\ \{0,1\}^{128}$
2: $k \leftarrow\!\!\$\ \{0,1\}^{128}; b \leftarrow\!\!\$\ \{0,1\}$	2: $\quad$ **return** $\perp$	2: **if** $\{iv, \ldots, iv + n - 1\} \cap \mathcal{I} \neq \emptyset$ **then**
3: $b' \leftarrow \mathcal{D}^E$	3: $c \leftarrow\!\!\$\ E_k(m_b)$	3: $\quad bad \leftarrow true$
4: **return** $b = b'$	4: **return** c	4: $\quad$ // Game_1
Game_1		5: $\quad iv \leftarrow\!\!\$\$ w.o. overlap with $\mathcal{I}$
1: $\mathcal{I}, bad \leftarrow \emptyset, false$		6: $\mathcal{I} \leftarrow \mathcal{I} \cup \{iv, \ldots, iv + n - 1\}$
2: $k \leftarrow\!\!\$\ \{0,1\}^{128}; b \leftarrow\!\!\$\ \{0,1\}$		7: **for** $0 \leq i < n$ **do**
3: $b' \leftarrow \mathcal{D}^E$		8: $\quad c_i \leftarrow \text{AES-128}(k, iv + i) \oplus m_i$
4: **return** $b = b'$		9: **return** $(iv, c_0, \ldots, c_{n-1})$

$$\left| \Pr[\text{Game}_0{}^{\mathcal{D}}] - \Pr[\text{Game}_1{}^{\mathcal{D}}] \right| \leq \Pr[\text{Game}_0{}^{\mathcal{D}} \text{ sets bad}] \leq n \cdot q \cdot (n \cdot q + 1)/2^{128+1}.$$

Proof Step 2: PRP Security of AES-128

Game$_1$

1: $\mathcal{I} \leftarrow \emptyset$; $b \leftarrow\!\!\$ \{0,1\}$
2: $k \leftarrow\!\!\$ \{0,1\}^{128}$
3: $b' \leftarrow \mathcal{D}^E$
4: **return** $b = b'$

Game$_2$

1: $\mathcal{I} \leftarrow \emptyset$; $b \leftarrow\!\!\$ \{0,1\}$
2: $\pi \leftarrow\!\!\$$ random permutation
3: $b' \leftarrow \mathcal{D}^E$
4: **return** $b = b'$

$E(m_0, m_1 \in \{0,1\}^{128 \cdot n})$

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

$E_k\left((m_0, \ldots, m_{n-1}) \in \left(\{0,1\}^{128}\right)^n\right)$

1: $iv \leftarrow\!\!\$$ w.o. overlap with $\mathcal{I}$
2: $\mathcal{I} \leftarrow \mathcal{I} \cup \{iv, \ldots, iv + n - 1\}$
3: **for** $0 \leq i < n$ **do**
4:      $c_i \leftarrow$ AES-128$(k, iv + i) \oplus m_i$
5:      $c_i \leftarrow \pi(iv + i) \oplus m_i$ //Game$_2$
6: **return** $(iv, c_0, \ldots, c_{n-1})$

Claim: $\left| \Pr[\text{Game}_1^{\mathcal{D}}] - \Pr[\text{Game}_2^{\mathcal{D}}] \right| \leq \text{Adv}_{\text{AES-128}}^{\text{prp}}(\mathcal{B})$

Proof Sketch

- Assume that there is some adversary $\mathcal{D}$ that detects this change and behaves differently in Game_1 and Game_2 of our main proof.
- We use this adversary as a blackbox subroutine in a new adversary $\mathcal{B}$ to break the PRP security of AES-128.

Game_0	$P(x)$
$\pi \leftarrow \emptyset; k \leftarrow\!\!\$ \; \mathcal{K}$	if $x \notin \pi.\text{keys}$ then
return $\mathcal{D}^P$	$\quad \pi[x] \leftarrow\!\!\$ \; \{0,1\}^n \setminus \pi.\text{values}$
Game_1	$y \leftarrow \pi[x]$
1: $\quad \pi \leftarrow \emptyset$	$y \leftarrow E_k(x)$ //Game_0
2: $\quad$ return $\mathcal{A}^P$	return y

$$\text{Adv}_E^{\text{prp}}(\mathcal{A}) := \left| \Pr[\mathcal{A}^{\text{Game}_0}] - \Pr[\mathcal{A}^{\text{Game}_1}] \right|$$
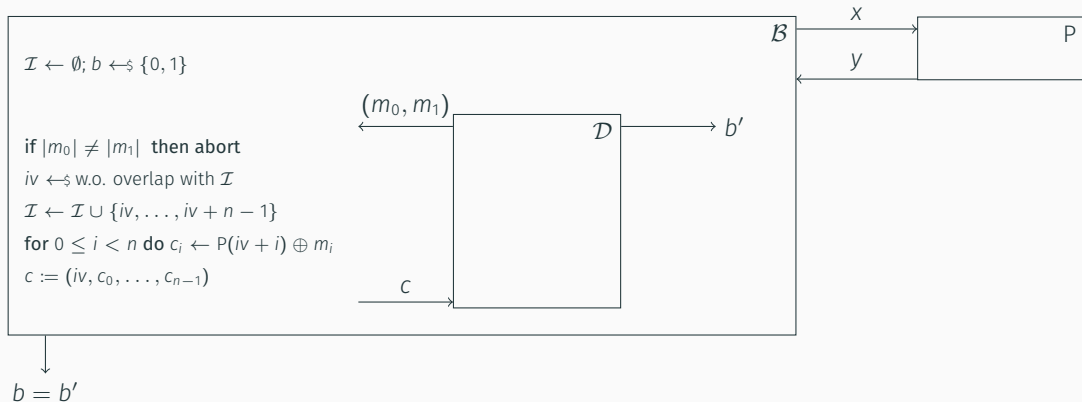
AES-128 Assumption

$\text{Adv}_{\text{AES-128}}^{\text{prp}}(\mathcal{A}) \leq \varepsilon$ for any adversary $\mathcal{A}$ running in time t and $\log(t/\varepsilon) \approx 128$.

$\mathcal{I} \leftarrow \emptyset; b \leftarrow_\$ \{0,1\}$

if $|m_0| \neq |m_1|$ then abort

$iv \leftarrow_\$$ w.o. overlap with $\mathcal{I}$

$\mathcal{I} \leftarrow \mathcal{I} \cup \{iv, \dots, iv + n - 1\}$

for $0 \leq i < n$ do $c_i \leftarrow P(iv + i) \oplus m_i$

$c := (iv, c_0, \dots, c_{n-1})$

(m_0, m_1)

$\mathcal{D}$

$\to b'$

c

$\mathcal{B}$

x

y

P

$b = b'$

PROOF STEP 2: PRP SECURITY

We use this adversary as a blackbox subroutine in a new adversary $\mathcal{B}$ to break the PRP security of AES-128.

$\mathcal{B}^P$	$E(m_0, m_1 \in \{0,1\}^{128 \cdot n})$	$E_k\left((m_0, \ldots, m_{n-1}) \in \left(\{0,1\}^{128}\right)^n\right)$
1: $\mathcal{I} \leftarrow \emptyset; b \leftarrow\!\!\$ \{0,1\}$	1: if $|m_0| \neq |m_1|$ then	1: $iv \leftarrow\!\!\$$ w.o. overlap with $\mathcal{I}$
2: $b' \leftarrow \mathcal{D}^E$	2: return $\bot$	2: $\mathcal{I} \leftarrow \mathcal{I} \cup \{iv, \ldots, iv + n - 1\}$
3: return $b = b'$	3: $c \leftarrow\!\!\$ E_k(m_b)$	3: for $0 \leq i < n$ do
	4: return c	4: $c_i \leftarrow P(iv + i) \oplus m_i$
		5: return $(iv, c_0, \ldots, c_{n-1})$

P is AES-128
$\mathcal{B}^P$ perfectly simulates Game$_1$

P is random permutation
$\mathcal{B}^P$ perfectly simulates Game$_2$

- P is AES-128: $\mathcal{B}^P$ perfectly simulates Game_1
- P is random permutation: $\mathcal{B}^P$ perfectly simulates Game_2

Thus if $\mathcal{D}$ significantly differs in its behaviour between games Game_1 and Game_2, $\mathcal{B}$ significantly differs between AES-128 and a random permutation, i.e. it distinguishes

- We obtain: $\left| \Pr[\text{Game}_1{}^{\mathcal{D}}] - \Pr[\text{Game}_2{}^{\mathcal{D}}] \right| \leq \text{Adv}_{\text{AES-128}}^{\text{prp}}(\mathcal{B})$
- We assumed $\text{Adv}_{\text{AES-128}}^{\text{prp}}(\mathcal{A}) \leq \varepsilon$ for **any** adversary $\mathcal{A}$ running in time t s.t. $\log(t/\varepsilon) \approx 128$.
- Thus: $\left| \Pr[\text{Game}_1{}^{\mathcal{D}}] - \Pr[\text{Game}_2{}^{\mathcal{D}}] \right| \leq \varepsilon$.

Proof Step 3: PRP-PRF Switching Lemma

Game_2	$\text{E}(m_0, m_1 \in \{0,1\}^{128 \cdot n})$	$E_k\left((m_0, \ldots, m_{n-1}) \in \left(\{0,1\}^{128}\right)^n\right)$
1: $\mathcal{I} \leftarrow \emptyset; b \leftarrow\!\!\$ \{0,1\}$	1: if $|m_0| \neq |m_1|$ then	1: $iv \leftarrow\!\!\$ $ w.o. overlap with $\mathcal{I}$
2: $\pi \leftarrow\!\!\$ $ random permutation	2: return $\bot$	2: $\mathcal{I} \leftarrow \mathcal{I} \cup \{iv, \ldots, iv + n - 1\}$
3: $b' \leftarrow \mathcal{D}^{\text{E}}$	3: $c \leftarrow\!\!\$ E_k(m_b)$	3: for $0 \leq i < n$ do
4: return $b = b'$	4: return c	4: $\quad r_i \leftarrow \pi(iv + i)$
Game_3		5: $\quad r_i \leftarrow \rho(iv + i)$ // Game_3
1: $\mathcal{I} \leftarrow \emptyset; b \leftarrow\!\!\$ \{0,1\}$		6: $\quad c_i \leftarrow r_i \oplus m_i$
2: $\rho \leftarrow\!\!\$ $ random function		7: return $(iv, c_0, \ldots, c_{n-1})$
3: $b' \leftarrow \mathcal{D}^{\text{E}}$		
4: return $b = b'$		

$$\left|\Pr[\text{Game}_2^{\mathcal{D}}] - \Pr[\text{Game}_3^{\mathcal{D}}]\right| \leq n \cdot q \cdot (n \cdot q + 1)/2^{128+1}.$$

PROOF: PUTTING IT ALL TOGETHER

$$
\begin{aligned}
\mathrm{Adv}^{\mathrm{ind\text{-}cpa}}_{\text{AES-128-CTR}}(\mathcal{D}) \leq{}& n \cdot q \cdot (n \cdot q + 1)/2^{128+1} && \text{samling w.o. replacment} \\
& + \mathrm{Adv}^{\mathrm{prp}}_{\text{AES-128}}(\mathcal{A}) && \text{PRP security} \\
& + n \cdot q \cdot (n \cdot q + 1)/2^{128+1} && \text{PRP-PRF switching lemma} \\
={}& \frac{2\,n \cdot q \cdot (n \cdot q + 1)}{2^{128+1}} + \mathrm{Adv}^{\mathrm{prp}}_{\text{AES-128}}(\mathcal{A})
\end{aligned}
$$

- If we allow $n \cdot q = 2^{64}$ then AES-128-CTR offers no security guarantees
- If we allow $n \cdot q = 2^{32}$ then AES-128-CTR offers ≈ 64 "bits of security"

¯_(ツ)_/¯

This situation is not unusual![a]

---

[a]AES-256 will not save you here, proof left as homework.

Natural question: is reduction "tight"?
We can **prove** this bound, but is there an attack matching this bound that e.g. breaks IND-CPA with $n \cdot q \approx 2^{64}$ queries?

- If we allow $n \cdot q = 2^{64}$ then AES-128-CTR offers no security guarantees
- If we allow $n \cdot q = 2^{32}$ then AES-128-CTR offers ≈ 64 "bits of security"

¯_("/)_/¯

This situation is not unusual![a]

---
[a] AES-256 will not save you here, proof left as homework.

Natural question: is reduction "tight"?
We can prove this bound, but is there an attack matching this bound that e.g. breaks IND-CPA with $n \cdot q \approx 2^{64}$ queries?

1. Make 2^{64} calls to $E(m_0, m_1)$, call the list of output L_a
2. Make 2^{64} calls to $E(m_0, m_0)$, call the list of output L_b
3. By the "Birthday Paradox" the is a good chance that there exists some $iv_a \in L_a$ and some $iv_b \in L_b$ s.t. $iv_a = iv_b$
4. Check if the matching ciphertexts agree (return $b = 0$) or not (return $b = 1$).

IND-CCA	$E(m_0, m_1)$	$D(c)$
1: $\mathcal{C} \leftarrow \emptyset$	1: **if** $|m_0| \neq |m_1|$ **then**	1: **if** $c \in \mathcal{C}$ **then**
2: $k \leftarrow\!\!\$ \mathcal{K}$	2: **return** $\bot$	2: **return** $\bot$
3: $b \leftarrow\!\!\$ \{0, 1\}$	3: $c \leftarrow\!\!\$ E_k(m_b)$	3: **return** $D_k(c)$
4: $b' \leftarrow \mathcal{D}^{E,D}$	4: **if** $m_0 \neq m_1$ **then** $\mathcal{C} \leftarrow \mathcal{C} \cup \{c\}$	
5: **return** $b = b'$	5: **return** c	

$$\mathrm{Adv}_{E,D}^{\mathrm{ind\text{-}cca}}(\mathcal{D}) = |\Pr[\mathrm{IND\text{-}CCA}^{\mathcal{D}} = 1] - 1/2|.$$

We only proved IND-CPA security, AES-128-CTR (as is) is trivially insecure against an IND-CCA adversary.

Break it!

PRP -> IND-CPA !=> SPRP -> IND-CCA I

Game_0	$P(x)$
1 : $\quad \pi \leftarrow \emptyset$	1 : $\quad$ if $x \in \pi.\text{keys}$ then
2 : $\quad$ return $\mathcal{D}^P$	2 : $\quad\quad y \leftarrow \pi[x]$
Game_1	3 : $\quad$ else
1 : $\quad \pi \leftarrow \emptyset; k \leftarrow\!\!\!\$\; \mathcal{K}$	4 : $\quad\quad y \leftarrow\!\!\!\$\; \{0,1\}^n \setminus \pi.\text{values}$
2 : $\quad$ return $\mathcal{D}^P$	5 : $\quad\quad \pi[x] \leftarrow y$
	6 : $\quad\quad y \leftarrow E_k(x)$ //Game_1
	7 : $\quad$ return y

Figure 1: PRP Security Games.

Game_0	$P(x)$	$P^{-1}(y)$
1: $\pi \leftarrow \emptyset$	1: if $x \in \pi.\text{keys}$ then	1: if $y \in \pi.\text{values}$ then
2: return $\mathcal{D}^{P,P^{-1}}$	2:	2: // Find the x s.t. $\pi[x] = y$
Game_1	3: $\quad y \leftarrow \pi[x]$	3: $\quad x \leftarrow \pi^{-1}[y]$
1: $k \leftarrow\!\!\$\ \mathcal{K}$	4: else	4: else
2: return $\mathcal{D}^{P,P^{-1}}$	5: $\quad y \leftarrow\!\!\$\ \{0,1\}^n \setminus \pi.\text{values}$	5: $\quad x \leftarrow\!\!\$\ \{0,1\}^n \setminus \pi.\text{keys}$
	6: $\quad \pi[x] \leftarrow y$	6: $\quad \pi[x] \leftarrow y$
	7: $\quad y \leftarrow E_k(x)$ // Game_1	7: $\quad x \leftarrow E_k^{-1}(y)$ // Game_1
	8: return y	8: return x

Figure 2: SPRP Security Games.

Our reduction tells us that if AES-128 is a PRP and if we do not allow too many queries then AES-128-CTR is IND-CPA secure

Reduced scope We can focus our efforts on studying AES-128

Wider scope Any result distinguishing AES-128 from a PRP invalidates our proof

Biclique Cryptanalysis of the Full AES

Andrey Bogdanov[*], Dmitry Khovratovich, and Christian Rechberger[*]

K.U. Leuven, Belgium; Microsoft Research Redmond, USA; ENS Paris and Chaire France Telecom, France

August 31, 2011

Abstract. Since Rijndael was chosen as the Advanced Encryption Standard (AES), improving upon 7-round attacks on the 128-bit key variant (out of 10 rounds) or upon 8-round attacks on the 192/256-bit key variants (out of 12/14 rounds) has been one of the most difficult challenges in the cryptanalysis of block ciphers for more than a decade. In this paper, we present the novel technique of block cipher cryptanalysis with bicliques, which leads to the following results:

- The first key recovery method for the full AES-128 with computational complexity $2^{126.1}$.
- The first key recovery method for the full AES-192 with computational complexity $2^{189.7}$.
- The first key recovery method for the full AES-256 with computational complexity $2^{254.4}$.
- Key recovery methods with lower complexity for the reduced-round versions of AES not considered before, including cryptanalysis of 8-round AES-128 with complexity $2^{124.9}$.
- Preimage search for compression functions based on the full AES versions faster than brute force.

In contrast to most shortcut attacks on AES variants, we *do not need to assume related-keys*. Most of our techniques only need a very small part of the codebook and have low memory requirements, and are practically verified to a large extent. As our cryptanalysis is of high computational complexity, it does not threaten the practical use of AES in any way.

Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Berlin, Heidelberg, Dec. 2011, pp. 344–371. DOI: `10.1007/978-3-642-25385-0_19`

Read up on IV reuse attacks!

[BKR11]   Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Berlin, Heidelberg, Dec. 2011, pp. 344–371. DOI: 10.1007/978-3-642-25385-0_19.