(Computational) Indistinguishability

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

Martin R. Albrecht

Outline

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

Recap: IND-CPA and AES-128-CTR

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

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

Proof Strategy

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

Proof Strategy

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

Proof Strategy

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

Proof Strategy

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

Proof Strategy

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

Proof Strategy

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

$\mathcal{I}, \mathit{bad} \leftarrow \emptyset, \mathit{false}$
$k \leftarrow\!\!\$\ \{0,1\}^{128};\ b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow \mathcal{D}^{\mathsf{E}}$
$\textbf{return } b = b'$

Game_1

$\mathcal{I}, \mathit{bad} \leftarrow \emptyset, \mathit{false}$
$k \leftarrow\!\!\$\ \{0,1\}^{128};\ b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow \mathcal{D}^{\mathsf{E}}$
$\textbf{return } b = b'$

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

$\textbf{if } |m_0| \neq |m_1| \textbf{ then}$
$\quad \textbf{return } \bot$
$c \leftarrow\!\!\$\ E_k(m_b)$
$\textbf{return } c$

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

$iv \leftarrow\!\!\$\ \{0,1\}^{128}$
$\textbf{if } \{iv, \ldots, iv+n-1\} \cap \mathcal{I} \neq \emptyset \textbf{ then}$
$\quad \mathit{bad} \leftarrow \mathit{true}$
$\quad //\ \mathsf{Game}_1$
$\quad iv \leftarrow\!\!\$\ \text{w.o. overlap with } \mathcal{I}$
$\mathcal{I} \leftarrow \mathcal{I} \cup \{iv, \ldots, iv+n-1\}$
$\textbf{for } 0 \leq i < n \textbf{ do}$
$\quad c_i \leftarrow \text{AES-128}(k, iv+i) \oplus m_i$
$\textbf{return } (iv, c_0, \ldots, c_{n-1})$

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

Proof Step 2: PRP Security of AES-128

Game_1

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

$k \leftarrow\!\!\$\ \{0,1\}^{128}$

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

return $b = b'$

Game_2

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

$\pi \leftarrow\!\!\$$ random permutation

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

return $b = b'$

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

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

  return $\perp$

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

return c

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

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

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

for $0 \leq i < n$ **do**

  $c_i \leftarrow \text{AES-128}(k, iv + i) \oplus m_i$

  $c_i \leftarrow \pi(iv + i) \oplus m_i$ // Game_2

return $(iv, c_0, \ldots, c_{n-1})$

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

Proof Step 2: PRP Security

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

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

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.

AES-128 Assumption

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

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.

$\mathcal{B}^{\mathsf{P}}$

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

$b' \leftarrow \mathcal{D}^{\mathsf{E}}$

return $b = b'$

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

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

  return $\perp$

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

return c

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

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

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

for $0 \leq i < n$ **do**

  $c_i \leftarrow \mathsf{P}(iv + i) \oplus m_i$

return $(iv, c_0, \ldots, c_{n-1})$

P is AES-128

$\mathcal{B}^{\mathsf{P}}$ perfectly simulates Game_1

P is random permutation

$\mathcal{B}^{\mathsf{P}}$ perfectly simulates Game_2

Proof Step 2: PRP Security

- P **is AES-128:** $\mathcal{B}^{\mathsf{P}}$ perfectly simulates Game_1
- P **is random permutation:** $\mathcal{B}^{\mathsf{P}}$ 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: $\left|\Pr[{\text{Game}_1}^{\mathcal{D}}] - \Pr[{\text{Game}_2}^{\mathcal{D}}]\right| \leq \mathrm{Adv}^{\mathrm{prp}}_{\text{AES-128}}(\mathcal{B})$
- We assumed $\mathrm{Adv}^{\mathrm{prp}}_{\text{AES-128}}(\mathcal{A}) \leq \varepsilon$ 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

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

$\pi \leftarrow\!\!\$$ random permutation

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

return $b = b'$

Game_3

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

$\rho \leftarrow\!\!\$$ random function

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

return $b = b'$

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

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

  return $\perp$

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

return c

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

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

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

for $0 \leq i < n$ **do**

  $r_i \leftarrow \pi(iv + i)$

  $r_i \leftarrow \rho(iv + i)$ // Game_3

  $c_i \leftarrow r_i \oplus m_i$

return $(iv, c_0, \ldots, c_{n-1})$

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

Proof: Putting it all together

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

Bounds

- 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?

Bounds

- 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 $\mathsf{E}(m_0, m_1)$, call the list of output L_a
2. Make 2^{64} calls to $\mathsf{E}(m_0, m_0)$, 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 $b = 1$).

Reminder: IND-CPA != IND-CCA

IND-CCA	$\mathrm{E}(m_0, m_1)$	$\mathrm{D}(c)$
$\mathcal{C} \leftarrow \emptyset$	**if** $\lvert m_0 \rvert \neq \lvert m_1 \rvert$ **then**	**if** $c \in \mathcal{C}$ **then**
$k \leftarrow\!\!\$\ \mathcal{K}$	**return** $\perp$	**return** $\perp$
$b \leftarrow\!\!\$\ \{0, 1\}$	$c \leftarrow\!\!\$\ E_k(m_b)$	**return** $D_k(c)$
$b' \leftarrow \mathcal{D}^{\mathrm{E,D}}$	**if** $m_0 \neq m_1$ **then** $\mathcal{C} \leftarrow \mathcal{C} \cup \{c\}$	
return $b = b'$	**return** c	

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

Reminder: IND-CPA != IND-CCA

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

$\pi \leftarrow \emptyset$

$\textbf{return } \mathcal{D}^{\mathsf{P}}$

Game_1

$\pi \leftarrow \emptyset;\ k \leftarrow\$ \mathcal{K}$

$\textbf{return } \mathcal{D}^{\mathsf{P}}$

$\mathsf{P}(x)$

$\textbf{if } x \in \pi.\mathsf{keys} \textbf{ then}$

$\quad y \leftarrow \pi[x]$

$\textbf{else}$

$\quad y \leftarrow\$ \{0,1\}^n \setminus \pi.\mathsf{values}$

$\quad \pi[x] \leftarrow y$

$y \leftarrow E_k(x)$ //Game_1

$\textbf{return } y$

Figure 1: PRP Security Games.

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

Game$_0$

$\pi \leftarrow \emptyset$

return $\mathcal{D}^{\mathsf{P},\mathsf{P}^{-1}}$

Game$_1$

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

return $\mathcal{D}^{\mathsf{P},\mathsf{P}^{-1}}$

$\mathsf{P}(x)$

if $x \in \pi.\mathsf{keys}$ **then**

$\quad y \leftarrow \pi[x]$

else

$\quad y \leftarrow\!\!\$\ \{0,1\}^n \setminus \pi.\mathsf{values}$

$\quad \pi[x] \leftarrow y$

$y \leftarrow E_k(x)$ //Game$_1$

return y

$\mathsf{P}^{-1}(y)$

if $y \in \pi.\mathsf{values}$ **then**

$\quad$ // Find the x s.t. $\pi[x] = y$

$\quad x \leftarrow \pi^{-1}[y]$

else

$\quad x \leftarrow\!\!\$\ \{0,1\}^n \setminus \pi.\mathsf{keys}$

$\quad \pi[x] \leftarrow y$

$x \leftarrow E_k^{-1}(y)$ //Game$_1$

return x

Figure 2: SPRP Security Games.

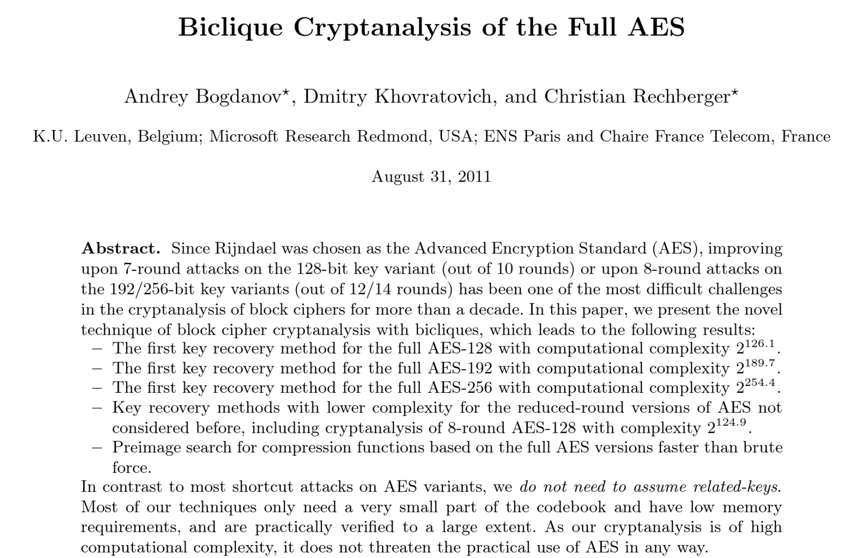
Cryptanalysis Target: $\mathsf{Adv}^{(s)prp}_{\mathsf{AES\text{-}128}}(\mathcal{A})$

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

AES-128 IS NOT SPRP-SECURE FOR $\log(t/\varepsilon) \geq 126.21$


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.

AES-128 is not SPRP-secure for $\log(t/\varepsilon) \geq 126.21$

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

Fin

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.