Cryptography

Lecture 5

Arkady Yerukhimovich

September 11, 2024

Outline

1. Lecture 4 Review

2. Security of PRG+OTP (Chapter 3.3.3)

Lecture 4 Review

- PRGs
- Proofs by reduction

Outline

Security of PRG+OTP: Intuition

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is PRG

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG
Goal: Prove that $\Pi =$PRG+OTP is secure
Proof:

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is PRG

Goal: Prove that $\Pi =$PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] > 1/2 + 1/\text{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is PRG
Goal: Prove that $\Pi =$PRG+OTP is secure
Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] > 1/2 + 1/\text{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:

Intuition

- $\mathcal{A}_r$ receives either $r \leftarrow \{0,1\}^{l(n)}$ or $r = G(s)$

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that $\Pi =$PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] > 1/2 + 1/\text{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:

Intuition

- $\mathcal{A}_r$ receives either $r \leftarrow \{0,1\}^{l(n)}$ or $r = G(s)$
- IDEA: use r as mask to encrypt (i.e., $c = r \oplus m$)

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is PRG
Goal: Prove that Π =PRG+OTP is secure
Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] > 1/2 + 1/\text{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:

Intuition

- $\mathcal{A}_r$ receives either $r \leftarrow \{0,1\}^{l(n)}$ or $r = G(s)$
- IDEA: use r as mask to encrypt (i.e., $c = r \oplus m$)
- If $r \leftarrow \{0,1\}^{l(n)}$, Π is just OTP ($\Pr[\mathcal{A}_c$ WINS$] = 1/2$)

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG
Goal: Prove that Π =PRG+OTP is secure
Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π ($\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] > 1/2 + 1/\text{poly}(n)$)
- Construct $\mathcal{A}_r$ that breaks G:

Intuition

- $\mathcal{A}_r$ receives either $r \leftarrow \{0,1\}^{l(n)}$ or $r = G(s)$
- IDEA: use r as mask to encrypt (i.e., $c = r \oplus m$)
- If $r \leftarrow \{0,1\}^{l(n)}$, Π is just OTP ($\Pr[\mathcal{A}_c$ WINS$] = 1/2$)
- If $r = G(s)$, Π is PRG+OTP (by assumption, $\Pr[\mathcal{A}_c$ WINS$] > 1/2 + 1/\text{poly}(n)$)

Security of PRG+OTP: Intuition

Assumption: $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is PRG

Goal: Prove that $\Pi =$PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π ($\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] > 1/2 + 1/\text{poly}(n)$)
- Construct $\mathcal{A}_r$ that breaks G:

Intuition

- $\mathcal{A}_r$ receives either $r \leftarrow \{0,1\}^{l(n)}$ or $r = G(s)$
- IDEA: use r as mask to encrypt (i.e., $c = r \oplus m$)
- If $r \leftarrow \{0,1\}^{l(n)}$, Π is just OTP ($\Pr[\mathcal{A}_c$ WINS$] = 1/2$)
- If $r = G(s)$, Π is PRG+OTP (by assumption, $\Pr[\mathcal{A}_c$ WINS$] > 1/2 + 1/\text{poly}(n)$)
- $\mathcal{A}_r$ runs $\mathcal{A}_c$ generating challenge c using r, observes if $\mathcal{A}_c$ wins, and if so outputs "PRG".

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b = 0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b = 1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},n}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},n} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that $\Pi =$PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π ($\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n)$)

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b = 0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b = 1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that $\Pi =$PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π ($\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n)$)
- Construct $\mathcal{A}_r$ that breaks G:

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that Π =PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:
  - $\mathcal{A}_r$ gets $r \in \{0,1\}^{l(n)}$ as its challenge (trying to tell if its random or $G(s)$)

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that Π =PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:
  - $\mathcal{A}_r$ gets $r \in \{0,1\}^{l(n)}$ as its challenge (trying to tell if its random or $G(s)$)
  - $\mathcal{A}_r$ runs $\mathcal{A}_c$ to get (m_0, m_1)

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that $\Pi =$PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:
  - $\mathcal{A}_r$ gets $r \in \{0,1\}^{l(n)}$ as its challenge (trying to tell if its random or $G(s)$)
  - $\mathcal{A}_r$ runs $\mathcal{A}_c$ to get (m_0, m_1)
  - $\mathcal{A}_r$ chooses $b \leftarrow \{0,1\}$ and sets $c = r \oplus m_b$ (challenge)

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that Π =PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:
  - $\mathcal{A}_r$ gets $r \in \{0,1\}^{l(n)}$ as its challenge (trying to tell if its random or $G(s)$)
  - $\mathcal{A}_r$ runs $\mathcal{A}_c$ to get (m_0, m_1)
  - $\mathcal{A}_r$ chooses $b \leftarrow \{0,1\}$ and sets $c = r \oplus m_b$ (challenge)
  - $\mathcal{A}_r$ gives c to $\mathcal{A}_c$ and gets bit b'

Security of PRG+OTP: Building $\mathcal{A}_r$

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$. If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$; if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$. He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Assumption: $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is PRG

Goal: Prove that Π =PRG+OTP is secure

Proof:

- Assume there exists PPT $\mathcal{A}_c$ that breaks Π $(\Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n)] > 1/2 + 1/\mathrm{poly}(n))$
- Construct $\mathcal{A}_r$ that breaks G:
  - $\mathcal{A}_r$ gets $r \in \{0,1\}^{l(n)}$ as its challenge (trying to tell if its random or $G(s)$)
  - $\mathcal{A}_r$ runs $\mathcal{A}_c$ to get (m_0, m_1)
  - $\mathcal{A}_r$ chooses $b \leftarrow \{0,1\}$ and sets $c = r \oplus m_b$ (challenge)
  - $\mathcal{A}_r$ gives c to $\mathcal{A}_c$ and gets bit b'
  - $\mathcal{A}_r$ outputs 1 ("PRG") if $b = b'$ and 0 otherwise

Security of PRG+OTP: Analysis

PRG+OTP Encryption

- Gen(1^n): $k \leftarrow \{0,1\}^n$
- Enc(k, m): $c = G(k) \oplus m$
- Dec(k, c): $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b = 0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b = 1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},n}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow$ Gen, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},n} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Need to analyze $\Pr[\mathcal{A}_r$ WINS$]$ ($\Pr[PRG_{\mathcal{A}_r,G}(n) = 1]$)

Security of PRG+OTP: Analysis

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k, m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k, c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b = 0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b = 1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Need to analyze $\Pr[\mathcal{A}_r \text{ WINS}]$ ($\Pr[PRG_{\mathcal{A}_r,G}(n) = 1]$)

- Case 1: $r \leftarrow \{0,1\}^{l(n)}$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r \leftarrow \{0,1\}^{l(n)}$, this is just OTP

Security of PRG+OTP: Analysis

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b = 0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b = 1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Need to analyze $\Pr[\mathcal{A}_r \text{ WINS}]$ $(\Pr[PRG_{\mathcal{A}_r,G}(n) = 1])$

- Case 1: $r \leftarrow \{0,1\}^{l(n)}$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r \leftarrow \{0,1\}^{l(n)}$, this is just OTP
  - $\Pr[\mathcal{A}_r(r) = 1] = \Pr[\mathcal{A}_c \text{ outputs } b' = b] = 1/2$

Security of PRG+OTP: Analysis

PRG+OTP Encryption

- $\mathrm{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathrm{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathrm{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b = 0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b = 1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathrm{PrivK}^{eav}_{\mathcal{A},n}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathrm{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathrm{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathrm{PrivK}^{eav}_{\mathcal{A},n} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Need to analyze $\Pr[\mathcal{A}_r$ WINS$]$ $(\Pr[PRG_{\mathcal{A}_r,G}(n) = 1])$

- Case 1: $r \leftarrow \{0,1\}^{l(n)}$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r \leftarrow \{0,1\}^{l(n)}$, this is just OTP
  - $\Pr[\mathcal{A}_r(r) = 1] = \Pr[\mathcal{A}_c$ outputs $b' = b] = 1/2$
- Case 2: $r = G(s)$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r = G(s)$, this is OTP+PRG

Security of PRG+OTP: Analysis

PRG+OTP Encryption

- $\text{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\text{Enc}(k,m)$: $c = G(k) \oplus m$
- $\text{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$.
  If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$;
  if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$.
  He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\text{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \text{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \text{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\text{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Need to analyze $\Pr[\mathcal{A}_r \text{ WINS}]$ ($\Pr[PRG_{\mathcal{A}_r,G}(n) = 1]$)

- Case 1: $r \leftarrow \{0,1\}^{l(n)}$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r \leftarrow \{0,1\}^{l(n)}$, this is just OTP
  - $\Pr[\mathcal{A}_r(r) = 1] = \Pr[\mathcal{A}_c \text{ outputs } b' = b] = 1/2$
- Case 2: $r = G(s)$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r = G(s)$, this is OTP+PRG
  - $\Pr[\mathcal{A}_r(r) = 1] = \Pr[\mathcal{A}_c \text{ outputs } b' = b] =$
    $= \Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] \geq 1/2 + 1/\text{poly}(n)$

Security of PRG+OTP: Analysis

PRG+OTP Encryption

- $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k,m)$: $c = G(k) \oplus m$
- $\mathsf{Dec}(k,c)$: $m = G(k) \oplus c$

$PRG_{\mathcal{D},G}(n)$

- The challenger chooses $b \leftarrow \{0,1\}$. If $b=0$, he chooses $r \leftarrow \{0,1\}^{l(n)}$; if $b=1$, he chooses $s \leftarrow \{0,1\}^n$, and computes $r = G(s)$. He gives r to $\mathcal{D}$.
- On input r, the distinguisher $\mathcal{D}$ outputs a guess b'
- $PRG_{\mathcal{D},G}(n) = 1$ (i.e., $\mathcal{D}$ wins) if $b' = b$

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$

- $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathcal{M}$
- The challenger chooses $k \leftarrow \mathsf{Gen}$, $b \leftarrow \{0,1\}$, computes $c \leftarrow \mathsf{Enc}_k(m_b)$ and gives c to $\mathcal{A}$
- $\mathcal{A}$ outputs a guess bit b'
- We say that $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$ (i.e., $\mathcal{A}$ wins) if $b' = b$.

Need to analyze $\Pr[\mathcal{A}_r$ WINS$]$ ($\Pr[PRG_{\mathcal{A}_r,G}(n) = 1]$)

- Case 1: $r \leftarrow \{0,1\}^{l(n)}$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r \leftarrow \{0,1\}^{l(n)}$, this is just OTP
  - $\Pr[\mathcal{A}_r(r) = 1] = \Pr[\mathcal{A}_c$ outputs $b' = b] = 1/2$

$\mathcal{A}_r$ win

0

- Case 2: $r = G(s)$
  - $\mathcal{A}_c$ receives $c = r \oplus m_b$ with $r = G(s)$, this is OTP+PRG
  - $\Pr[\mathcal{A}_r(r) = 1] = \Pr[\mathcal{A}_c$ outputs $b' = b] =$
    $= \Pr[PrivK^{eav}_{\mathcal{A}_c,\Pi}(1^n) = 1] \geq 1/2 + 1/\mathrm{poly}(n)$

1

- Summing these together, we get

$$\begin{aligned}\Pr[PRG_{\mathcal{A}_r,G}(1^n) = 1] &\geq 1/2 \cdot 1/2 + 1/2 \cdot (1/2 + 1/\mathrm{poly}(n)) \\ &= 1/2 + 1/(2\mathrm{poly}(n))\end{aligned}$$

Contradiction!

Where Are We Now

- Features of PRG+OTP encryption
  - Can encrypt messages of arbitrary length, just need PRG with enough stretch.
  - Achieve security against an eavesdropper

Where Are We Now

- Features of PRG+OTP encryption
  - Can encrypt messages of arbitrary length, just need PRG with enough stretch.
  - Achieve security against an eavesdropper
- Limitations of PRG+OTP encryption
  - Can only see one encryption
  - If see two, can tell whether they are equal