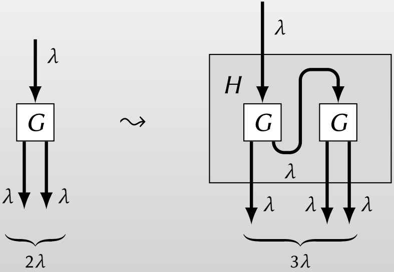
Extending the stretch of a PRG:

$H(s)$:
  $x := G(s)$
  $y := G(x_{\text{right}})$
  return $x_{\text{left}} \| y$



Claim:

If G is a secure length-doubling PRG then H is a secure length-*tripling* PRG. That is, $\mathcal{L}^{H}_{\text{prg-real}} \approx \mathcal{L}^{H}_{\text{prg-rand}}$.

Overview:

Want to show:

$\mathcal{L}^{H}_{\text{prg-real}}$		$\mathcal{L}^{H}_{\text{prg-rand}}$
QUERY(): $s \leftarrow \{0,1\}^{\lambda}$ return $H(s)$	$\approx$	QUERY(): $z \leftarrow \{0,1\}^{3\lambda}$ return z

Standard hybrid technique:

- Starting with $\mathcal{L}^{H}_{\text{prg-real}}$, make a sequence of small modifications
- Each modification has *negligible* effect on calling program
- Sequence of modifications ends with $\mathcal{L}^{H}_{\text{prg-rand}}$

Overview:

Want to show:

$\mathcal{L}^{H}_{\text{prg-real}}$		$\mathcal{L}^{H}_{\text{prg-rand}}$
$\underline{\text{QUERY}():}$ $s \leftarrow \{0,1\}^{\lambda}$ return $H(s)$	$\approx$	$\underline{\text{QUERY}():}$ $z \leftarrow \{0,1\}^{3\lambda}$ return z

The proof will **use** the fact G is a secure PRG. In other words,

$\mathcal{L}^{G}_{\text{prg-real}}$		$\mathcal{L}^{G}_{\text{prg-rand}}$
$\underline{\text{QUERY}():}$ $s \leftarrow \{0,1\}^{\lambda}$ return $G(s)$	$\approx$	$\underline{\text{QUERY}():}$ $z \leftarrow \{0,1\}^{2\lambda}$ return z

$\mathcal{L}^{H}_{\text{prg-real}}$
QUERY():
$s \leftarrow \{0,1\}^\lambda$
return $H(s)$

Starting point is $\mathcal{L}^{H}_{\text{prg-real}}$.

Security proof

$\mathcal{L}^{H}_{\text{prg-real}}$

$\underline{\text{QUERY}():}$

$\quad s \leftarrow \{0,1\}^\lambda$

$\quad \text{return } H(s)$

Starting point is $\mathcal{L}^{H}_{\text{prg-real}}$. Fill in details of H

Security proof

$\mathcal{L}^{H}_{\text{prg-real}}$

<u>QUERY()</u>:

$s \leftarrow \{0,1\}^\lambda$
$x := G(s)$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

Starting point is $\mathcal{L}^{H}_{\text{prg-real}}$. Fill in details of H

$$\mathcal{L}^{H}_{\text{prg-real}}$$

QUERY():
  $s \leftarrow \{0,1\}^\lambda$
  $x := G(s)$
  $y := G(x_{\text{right}})$
  return $x_{\text{left}} \| y$

Starting point is $\mathcal{L}^{H}_{\text{prg-real}}$. Fill in details of H

$\mathcal{L}^{H}_{\text{prg-real}}$
QUERY():
$s \leftarrow \{0,1\}^\lambda$
$x := G(s)$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

These statements appear in $\mathcal{L}^{G}_{\text{prg-real}}$.

Security proof

QUERY(): $x :=$ QUERY$'()$ $y := G(x_{\text{right}})$ return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^{G}_{\text{prg-real}}$
QUERY$'()$: $s \leftarrow \{0,1\}^\lambda$ return $G(s)$

Factor out in terms of $\mathcal{L}^{G}_{\text{prg-real}}$.

$\textsc{query}()$:
$x := \textsc{query}'()$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^{G}_{\text{prg-real}}$
$\textsc{query}'()$:
$s \leftarrow \{0,1\}^{\lambda}$
return $G(s)$

Factor out in terms of $\mathcal{L}^{G}_{\text{prg-real}}$.

Security proof

$$\begin{array}{|l|}\hline \underline{\text{QUERY}():} \\ \quad x := \text{QUERY}'() \\ \quad y := G(x_{\text{right}}) \\ \quad \text{return } x_{\text{left}} \| y \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^G_{\text{prg-rand}} \\ \hline \underline{\text{QUERY}'():} \\ \quad z \leftarrow \{0,1\}^{2\lambda} \\ \quad \text{return } z \\ \hline \end{array}$$

Security of PRG allows to replace $\mathcal{L}^G_{\text{prg-real}}$ with $\mathcal{L}^G_{\text{prg-rand}}$.

Security proof

$$\begin{array}{|l|}\hline \underline{\textsc{query}():} \\ \quad x := \textsc{query}'() \\ \quad y := G(x_{\text{right}}) \\ \quad \text{return } x_{\text{left}} \| y \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{G}_{\text{prg-rand}} \\ \hline \underline{\textsc{query}'():} \\ \quad z \leftarrow \{0,1\}^{2\lambda} \\ \quad \text{return } z \\ \hline \end{array}$$

Security of PRG allows to replace $\mathcal{L}^{G}_{\text{prg-real}}$ with $\mathcal{L}^{G}_{\text{prg-rand}}$.

$\textsc{query}()$:
$x := \textsc{query}'()$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^{G}_{\text{prg-rand}}$
$\textsc{query}'()$:
$z \leftarrow \{0,1\}^{2\lambda}$
return z

Inline call to $\textsc{query}'$.

Security proof

```
QUERY():
  x ← {0,1}^{2λ}
  y := G(x_right)
  return x_left || y
```

Inline call to QUERY′.

QUERY():

$x \leftarrow \{0,1\}^{2\lambda}$

$y := G(x_{\text{right}})$

return $x_{\text{left}} \| y$

Inline call to QUERY′.

Security proof

$\textsc{query}()$:
$x \leftarrow \{0,1\}^{2\lambda}$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

Sampling 2λ uniform bits is the same as sampling λ and then λ more.

QUERY():

$x_{\text{left}} \leftarrow \{0,1\}^\lambda$

$x_{\text{right}} \leftarrow \{0,1\}^\lambda$

$y := G(x_{\text{right}})$

return $x_{\text{left}} \| y$

Sampling 2λ uniform bits is the same as sampling λ and then λ more.

QUERY():
$x_{\text{left}} \leftarrow \{0,1\}^\lambda$
$x_{\text{right}} \leftarrow \{0,1\}^\lambda$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

Sampling 2λ uniform bits is the same as sampling λ and then λ more.

$\textsc{query}()$:
$x_{\text{left}} \leftarrow \{0,1\}^\lambda$
$x_{\text{right}} \leftarrow \{0,1\}^\lambda$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

These statements appear in $\mathcal{L}^G_{\text{prg-real}}$.

Security proof

QUERY():
$x_{\text{left}} \leftarrow \{0,1\}^\lambda$
$y :=$ QUERY$'()$
return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^G_{\text{prg-real}}$
QUERY$'()$:
$s \leftarrow \{0,1\}^\lambda$
return $G(s)$

Factor out in terms of $\mathcal{L}^G_{\text{prg-real}}$.

$$\begin{array}{|l|}\hline \underline{\text{QUERY}():} \\ \quad x_{\text{left}} \leftarrow \{0,1\}^\lambda \\ \quad y := \text{QUERY}'() \\ \quad \text{return } x_{\text{left}} \| y \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}^{G}_{\text{prg-real}} \\ \hline \underline{\text{QUERY}'():} \\ \quad s \leftarrow \{0,1\}^\lambda \\ \quad \text{return } G(s) \\ \hline \end{array}$$

Factor out in terms of $\mathcal{L}^{G}_{\text{prg-real}}$.

Security proof

QUERY():
$x_{\text{left}} \leftarrow \{0,1\}^\lambda$
$y := \text{QUERY}'()$
return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^G_{\text{prg-rand}}$
QUERY$'$():
$z \leftarrow \{0,1\}^{2\lambda}$
return z

Security of PRG allows to replace $\mathcal{L}^G_{\text{prg-real}}$ with $\mathcal{L}^G_{\text{prg-rand}}$.

QUERY():	$\diamond$	$\mathcal{L}^{G}_{\text{prg-rand}}$
$x_{\text{left}} \leftarrow \{0,1\}^{\lambda}$		QUERY′():
$y :=$ QUERY′()		$z \leftarrow \{0,1\}^{2\lambda}$
return $x_{\text{left}} \| y$		return z

Security of PRG allows to replace $\mathcal{L}^{G}_{\text{prg-real}}$ with $\mathcal{L}^{G}_{\text{prg-rand}}$.

Security proof

QUERY():
$x_{\text{left}} \leftarrow \{0,1\}^{\lambda}$
$y :=$ QUERY$'()$
return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^{G}_{\text{prg-rand}}$
QUERY$'()$:
$z \leftarrow \{0,1\}^{2\lambda}$
return z

Inline the call to QUERY$'$.

Security proof

QUERY():

$x_{\text{left}} \leftarrow \{0,1\}^{\lambda}$

$y \leftarrow \{0,1\}^{2\lambda}$

return $x_{\text{left}} \| y$

Inline the call to QUERY′.

$\underline{\textsc{query}():}$
$x_{\text{left}} \leftarrow \{0,1\}^{\lambda}$
$y \leftarrow \{0,1\}^{2\lambda}$
return $x_{\text{left}} \| y$

Inline the call to QUERY′.

Security proof

```
QUERY():
  x_left ← {0,1}^λ
  y ← {0,1}^{2λ}
  return x_left || y
```

$\textsc{query}()$:

$x_{\text{left}} \leftarrow \{0,1\}^{\lambda}$

$y \leftarrow \{0,1\}^{2\lambda}$

return $x_{\text{left}} \| y$

Uniform 2λ bits concatenated with λ bits = Uniform 3λ bits.

QUERY():

$z \leftarrow \{0,1\}^{3\lambda}$
return z

2λ uniform bits concatenated with λ uniform bits = 3λ uniform bits.

```
QUERY():
  z ← {0,1}^{3λ}
  return z
```

2λ uniform bits concatenated with λ uniform bits = 3λ uniform bits.

$\mathcal{L}^{H}_{\text{prg-rand}}$

QUERY():

$z \leftarrow \{0,1\}^{3\lambda}$

return z

This is just $\mathcal{L}^{H}_{\text{prg-rand}}$.

Summary

We showed:

$\mathcal{L}^{H}_{\text{prg-real}}$		$\mathcal{L}^{H}_{\text{prg-rand}}$
$\underline{\text{QUERY}():}$ $s \leftarrow \{0,1\}^{\lambda}$ return $H(s)$	$\approx \dots \approx$	$\underline{\text{QUERY}():}$ $z \leftarrow \{0,1\}^{3\lambda}$ return z

So H is a secure PRG when G is a secure PRG.

A question

H contains two calls to G. We applied the security of G (replacing $\mathcal{L}^G_{\text{prg-real}}$ with $\mathcal{L}^G_{\text{prg-rand}}$) separately to each call to G.

Does the proof still work if we apply security in the other order?

Attempted security proof

$\mathcal{L}^{H}_{\text{prg-real}}$

```
QUERY():
  s ← {0,1}^λ
  x := G(s)
  y := G(x_right)
  return x_left ‖ y
```

Starting point.

Attempted security proof

$\mathcal{L}^{H}_{\text{prg-real}}$
$\underline{\text{QUERY}()}$:
$s \leftarrow \{0,1\}^\lambda$
$x := G(s)$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

Starting point. Can we write this call to G in terms of $\mathcal{L}^{G}_{\text{prg-real}}$?

Attempted security proof

$$\mathcal{L}^{H}_{\text{prg-real}}$$

$\underline{\text{QUERY}():}$
  $s \leftarrow \{0,1\}^\lambda$
  $x := G(s)$
  $y := G(x_{\text{right}})$
  return $x_{\text{left}} \| y$

$\diamond$

$$\mathcal{L}^{G}_{\text{prg-real}}$$

$\underline{\text{QUERY}'():}$
  $s' \leftarrow \{0,1\}^\lambda$
  return $G(s')$

??

Starting point. Can we write this call to G in terms of $\mathcal{L}^{G}_{\text{prg-real}}$?

Attempted security proof

$\mathcal{L}^{H}_{\text{prg-real}}$

QUERY():
$s \leftarrow \{0,1\}^\lambda$
$x := G(s)$
$y := G(x_{\text{right}})$
return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^{G}_{\text{prg-real}}$

QUERY′():
$s' \leftarrow \{0,1\}^\lambda$
return $G(s')$

??

Argument to G must be chosen *uniformly*

Attempted security proof

$\mathcal{L}^{H}_{\text{prg-real}}$

QUERY():
- $s \leftarrow \{0,1\}^\lambda$
- $x := G(s)$
- $y := G(x_{\text{right}})$
- return $x_{\text{left}} \| y$

$\diamond$

$\mathcal{L}^{G}_{\text{prg-real}}$

QUERY$'$():
- $s' \leftarrow \{0,1\}^\lambda$
- return $G(s')$

??

Argument to G must be chosen *uniformly* but x_{right} is not!