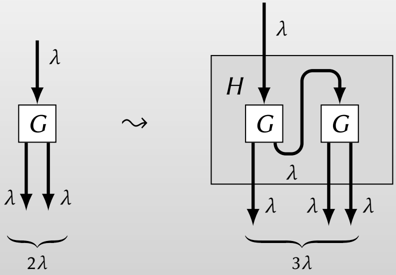
Extending the stretch of a PRG:

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



Claim:

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

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

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:

$$\begin{array}{|l|}\hline \mathcal{L}^{H}_{\text{prg-real}} \\ \hline \underline{\textsc{query}():} \\ \quad s \leftarrow \{0,1\}^{\lambda} \\ \quad \text{return } H(s) \\ \hline \end{array} \approx \begin{array}{|l|}\hline \mathcal{L}^{H}_{\text{prg-rand}} \\ \hline \underline{\textsc{query}():} \\ \quad z \leftarrow \{0,1\}^{3\lambda} \\ \quad \text{return } z \\ \hline \end{array}$$

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

$$\begin{array}{|l|}\hline \mathcal{L}^{G}_{\text{prg-real}} \\ \hline \underline{\textsc{query}():} \\ \quad s \leftarrow \{0,1\}^{\lambda} \\ \quad \text{return } G(s) \\ \hline \end{array} \approx \begin{array}{|l|}\hline \mathcal{L}^{G}_{\text{prg-rand}} \\ \hline \underline{\textsc{query}():} \\ \quad z \leftarrow \{0,1\}^{2\lambda} \\ \quad \text{return } z \\ \hline \end{array}$$

Security proof

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

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

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

$$\begin{array}{|l|}\hline \quad \mathcal{L}^{H}_{\text{prg-real}} \\ \hline \underline{\textsc{query}():} \\ \quad s \leftarrow \{0,1\}^{\lambda} \\ \quad \text{return } \boxed{H(s)} \\ \hline \end{array}$$

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

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

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

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

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

Security proof

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

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

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

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

Security proof

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

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

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

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

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

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′.

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

Inline call to QUERY′.

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

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

Security proof

$\underline{\textsc{query}()}$:

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

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

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

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

$$\begin{array}{|l|}\hline \underline{\textsc{query}():} \\ \quad x_{\text{left}} \leftarrow \{0,1\}^{\lambda} \\ \quad x_{\text{right}} \leftarrow \{0,1\}^{\lambda} \\ \quad y := G(x_{\text{right}}) \\ \quad \text{return } x_{\text{left}} \| y \\ \hline \end{array}$$

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

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

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

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

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

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

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

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

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

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

Inline the call to QUERY′.

Security proof

$$\begin{array}{l} \underline{\text{QUERY}():} \\ \quad x_{\text{left}} \leftarrow \{0,1\}^{\lambda} \\ \quad y \leftarrow \{0,1\}^{2\lambda} \\ \quad \text{return } x_{\text{left}} \| y \end{array}$$

Inline the call to QUERY′.

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

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

$$
\boxed{\begin{array}{l}
\textsc{query}():\\
\quad x_{\text{left}} \leftarrow \{0,1\}^{\lambda}\\
\quad y \leftarrow \{0,1\}^{2\lambda}\\
\quad \text{return } x_{\text{left}} \| y
\end{array}}
$$

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

Security proof

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

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

QUERY():
$z \leftarrow \{0,1\}^{3\lambda}$
return z

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

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

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

Summary

We showed:

$$\begin{array}{|l|}\hline \mathcal{L}^{H}_{\text{prg-real}} \\ \hline \underline{\textsc{query}():} \\ \quad s \leftarrow \{0,1\}^{\lambda} \\ \quad \text{return } H(s) \\ \hline \end{array} \approx \ldots \approx \begin{array}{|l|}\hline \mathcal{L}^{H}_{\text{prg-rand}} \\ \hline \underline{\textsc{query}():} \\ \quad z \leftarrow \{0,1\}^{3\lambda} \\ \quad \text{return } z \\ \hline \end{array}$$

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

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

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

Starting point.

Attempted security proof

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

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

Attempted security proof

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

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

Attempted security proof

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

Argument to G must be chosen *uniformly*

Attempted security proof

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

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