Recall that we have $G : \{0,1\}^k \rightarrow \{0,1\}^{2k}$ a PRA.
$G(s) = G_0(s) \cdot G_1(s)$

$F_0(x) = S_x$, where for any prefix $a$ of $x$, and bit $b$,$S_b = S$
$S_{ab} = G_b(S_a)$

Fix $\mathcal{U}$, $k$. Say $\mathcal{U}$ makes $\leq q(k)$ queries.

Experiment with $F$:
Pick $s \in \{0,1\}^k$.
Run $\mathcal{U}_F(s) (1^k)$.
$\mathcal{U}$ outputs $a$.

Experiment with a truly random function:
Pick a random function $R : \{0,1\}^k \rightarrow \{0,1\}^k$.
Run $\mathcal{U}_R(s) (1^k)$.
$\mathcal{U}$ outputs $a$. 
Hybrid experiment corresponding to $0 \leq i \leq k$, $0 \leq j \leq q(k)$:

When $A$ issues its $l^{th}$ query $x_l$:

For $l \leq j$: Let $x_{(i+1)}$ denote the $(i+1)$-bit prefix of $x_l$.

Pick $S_{x_{(i+1)}}$ at random.

Compute $S_{x_l}$ using $G$.

For $l > j$: Pick a $k$-bit value corresponding to $x_l x_{(i+1)} \ldots x_{(i+1)}$, unless already defined. (Store it.)

Compute $S_{x_l}$ using $G$; i.e.

$$S_{x_l} = G_{x_{(i+1)}} (S_{x_{(i+1)}}),$$

unless already defined.

The picture of Hybrid $(i, 0)$ and $(i+1, 0)$ is:

<table>
<thead>
<tr>
<th>Hybrid $(i, 0)$</th>
<th>Hybrid $(i+1, 0)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ not defined }</td>
<td>{ not defined }</td>
</tr>
<tr>
<td>Depth $i$</td>
<td>Depth $i + 1$</td>
</tr>
<tr>
<td>$S_{x(i)}$, $S_{x(i)} \ldots S_{x(i)}$</td>
<td>$S_{x(i+1)} \ldots S_{x(i+1)}$</td>
</tr>
</tbody>
</table>

Note: Hybrid $(0, 0)$ = Experiment with $F$

Hybrid $(i, q)$ = Hybrid $(i+1, 0)$

Hybrid $(k, 0)$ = Experiment with truly random function

It is sufficient to show that $\exists$ negligible $\nu$ s.t.

$\forall 0 \leq i < k$, $\forall 0 \leq j < q$,

$A$'s advantage in distinguishing Hybrid $(i, j)$ from Hybrid $(i, j+1)$

is $\leq \nu(k)$. 
Reduction: Given as input $S = S_0 \cdot (\ldots) S_i$ s.t. either $S = G(s)$ or $S$ is random.

Invoke $A$ and respond to $A$'s $q^{th}$ query by:

For $q \leq j$: Identical behavior to Hybrid $(i, j)$ / Hybrid $(i, j+1)$.

For $q = j+1$: Let the unknown $S_j$ if it exists, correspond to $S_{x_0^q}$

Then $S_{x_{(q+1)}} = S_{x_0^q}$, unless it has already been defined.

Compute $S_{x^q}$ from there.

For $q > j+1$: Identical behavior to Hybrid $(i, j)$ / Hybrid $(i, j+1)$.

"Analysis" of reduction:

If $S$ is truly random, then $A$'s view is computed identically to Hybrid $(i, j+1)$.

If $S = G(s)$, then $A$'s view is computed identically to Hybrid $(i, j)$.

OWF
\[ \Rightarrow (\text{HILL}) \]
\[ \Rightarrow (\text{GL}) \]
PRG
OWP with hardcore bit
\[ \Rightarrow (\text{GGM}) \]

PRF

Symmetric encryption against an active adversary