One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

$\underline{\mathsf{Invert}_{\mathcal{A},f}(n)}$:

One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

$\underline{\text{Invert}_{\mathcal{A},f}(n)}$:
Challenger chooses $x \leftarrow \{0,1\}^n$, and computes $y = f(x)$.

One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

$\underline{\text{Invert}_{\mathcal{A},f}(n)}$:
Challenger chooses $x \leftarrow \{0,1\}^n$, and computes $y = f(x)$.
$\mathcal{A}$ is given $(1^n, y)$ and outputs x'.

One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

$\underline{\mathsf{Invert}_{\mathcal{A},f}(n)}$:
Challenger chooses $x \leftarrow \{0,1\}^n$, and computes $y = f(x)$.
$\mathcal{A}$ is given $(1^n, y)$ and outputs x'.
The output of the experiment is 1 if $f(x') = y$, and 0 otherwise.

One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

$\underline{\text{Invert}_{\mathcal{A},f}(n)}$:
Challenger chooses $x \leftarrow \{0,1\}^n$, and computes $y = f(x)$.
$\mathcal{A}$ is given $(1^n, y)$ and outputs x'.
The output of the experiment is 1 if $f(x') = y$, and 0 otherwise.

Definition

A function $f : \{0,1\}^* \to \{0,1\}^*$ is *one-way* if the following two conditions hold:

- (Easy to compute:) There exists a polynomial-time algorithm M_f computing f; that is, $M_f(x) = f(x)$ for all x.
- (Hard to invert:) For every probabilistic polynomial-time algorithm $\mathcal{A}$, there is a negligible function negl such that $\Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \leq \text{negl(n)}$.

One Way Functions

$f : \{0,1\}^* \to \{0,1\}^*$ is a owf, if it is easy to compute and "hard to invert."

$\underline{\text{Invert}_{\mathcal{A},f}(n)}$:
Challenger chooses $x \leftarrow \{0,1\}^n$, and computes $y = f(x)$.
$\mathcal{A}$ is given $(1^n, y)$ and outputs x'.
The output of the experiment is 1 if $f(x') = y$, and 0 otherwise.

Definition

A function $f : \{0,1\}^* \to \{0,1\}^*$ is *one-way* if the following two conditions hold:

- (Easy to compute:) There exists a polynomial-time algorithm M_f computing f; that is, $M_f(x) = f(x)$ for all x.
- (Hard to invert:) For every probabilistic polynomial-time algorithm $\mathcal{A}$, there is a negligible function negl such that $\Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \leq \text{negl(n)}$.

Candidate owf: $f_{p,g}(x) = g^x \bmod p$

Hard-Core Predicates

Hard-Core Predicates

A function $\mathsf{hc} : \{0,1\}^* \to \{0,1\}$ is *a hard-core predicate of a function f* if hc can be computed in polynomial time, and for every probabilistic polynomial-time adversary $\mathcal{A}$ there is a negligible function negl such that

$$\Pr_{x \leftarrow \{0,1\}^*}[\mathcal{A}(1^n, f(x)) = \mathsf{hc}(x)] \leq \frac{1}{2} + \mathsf{negl}(n)$$

Hard-Core Predicates

Hard-Core Predicates

A function hc : $\{0,1\}^* \to \{0,1\}$ is *a hard-core predicate of a function f* if hc can be computed in polynomial time, and for every probabilistic polynomial-time adversary $\mathcal{A}$ there is a negligible function negl such that

$$\Pr_{x \leftarrow \{0,1\}^*}[\mathcal{A}(1^n, f(x)) = \mathrm{hc}(x)] \leq \frac{1}{2} + \mathrm{negl(n)}$$

$\mathrm{hc}(x) = \bigoplus_{i=1}^{n} x_i$ is *not* a hard-core predicate for every one-way function.

Hard-Core Predicates

Hard-Core Predicates

A function hc : $\{0,1\}^* \to \{0,1\}$ is *a hard-core predicate of a function f* if hc can be computed in polynomial time, and for every probabilistic polynomial-time adversary $\mathcal{A}$ there is a negligible function negl such that

$$\Pr_{x \leftarrow \{0,1\}^*}[\mathcal{A}(1^n, f(x)) = \mathrm{hc}(x)] \leq \frac{1}{2} + \mathrm{negl}(n)$$

$\mathrm{hc}(x) = \bigoplus_{i=1}^{n} x_i$ is *not* a hard-core predicate for every one-way function.

Let $g(x)$ be a owf, and define $f(x) = (g(x), \oplus x_i)$. It is easy to show that f is a owf. (Try it!)

Hard-Core Predicates

Hard-Core Predicates

A function hc : $\{0,1\}^* \to \{0,1\}$ is *a hard-core predicate of a function f* if hc can be computed in polynomial time, and for every probabilistic polynomial-time adversary $\mathcal{A}$ there is a negligible function negl such that

$$\Pr_{x \leftarrow \{0,1\}^*}[\mathcal{A}(1^n, f(x)) = \mathrm{hc}(x)] \leq \frac{1}{2} + \mathrm{negl}(n)$$

$\mathrm{hc}(x) = \bigoplus_{i=1}^{n} x_i$ is *not* a hard-core predicate for every one-way function.

Let $g(x)$ be a owf, and define $f(x) = (g(x), \oplus x_i)$. It is easy to show that f is a owf. (Try it!) Clearly hc is not a hard-core function for f described above.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] = 1$,
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = 1$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] = 1$,
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = 1$.

Proof: On input $(1^n, y)$, $\mathcal{A}_r$ sends n different challenges to $\mathcal{A}$: $\{(1^n, (y, e^i))\}_{i=1}^{n}$, where e^i is the vector of length n, containing a 1 in location i, and 0 everywhere else.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] = 1$,
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = 1$.

Proof: On input $(1^n, y)$, $\mathcal{A}_r$ sends n different challenges to $\mathcal{A}$: $\{(1^n, (y, e^i))\}_{i=1}^n$, where e^i is the vector of length n, containing a 1 in location i, and 0 everywhere else. Since $\mathcal{A}$ always succeeds, note that it will output x_i in response to the ith challenge:

$$\bigoplus_{j=1}^{n} (x_j \wedge e_j^i) = x_i.$$

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] \geq \frac{3}{4} + \frac{1}{\mathrm{poly}(n)}$
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = \frac{1}{4\mathrm{poly}(n)}$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] \geq \frac{3}{4} + \frac{1}{\mathrm{poly}(n)}$
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = \frac{1}{4\mathrm{poly}(n)}$.

Proof idea: On input $(1^n, y)$, $\mathcal{A}_r$ sends many challenges to $\mathcal{A}$:
$\{(1^n, (y, r \oplus e^i))\}_{i=1}^n$, and $\{(1^n, (y, r))\}_{i=1}^n$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] \geq \frac{3}{4} + \frac{1}{\mathrm{poly}(n)}$
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = \frac{1}{4\mathrm{poly}(n)}$.

Proof idea: On input $(1^n, y)$, $\mathcal{A}_r$ sends many challenges to $\mathcal{A}$:
$\{(1^n, (y, r \oplus e^i))\}_{i=1}^n$, and $\{(1^n, (y, r))\}_{i=1}^n$.
Intuitively, each of these look random. (Though, they are correlated!)
So $\mathcal{A}$ should succeed on most.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] \geq \frac{3}{4} + \frac{1}{\mathrm{poly}(n)}$
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = \frac{1}{4\mathrm{poly}(n)}$.

Proof idea: On input $(1^n, y)$, $\mathcal{A}_r$ sends many challenges to $\mathcal{A}$:
$\{(1^n, (y, r \oplus e^i))\}_{i=1}^n$, and $\{(1^n, (y, r))\}_{i=1}^n$.
Intuitively, each of these look random. (Though, they are correlated!)
So $\mathcal{A}$ should succeed on most.
Note that $\mathrm{gl}(x, r) \oplus \mathrm{gl}(x, r \oplus e^i) = x_i$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] \geq \frac{1}{2} + \frac{1}{\mathrm{poly}(n)}$
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = \frac{1}{\mathrm{poly}'(n)}$.

Goldreich-Levin

Theorem

Assume that one-way functions exist. Then there exists a one-way function g, and a hard-core predicate gl of g.

Let f be a owf. Define owf $g(x, r) = (f(x), r)$, for $|x| = |r|$.
(Prove to yourself that if f is a owf, then g is a owf!)
Define $\mathrm{gl}(x, r) = \bigoplus_{i=1}^{n} (x_i \wedge r_i)$.

Claim: $\exists p.p.t.\ \mathcal{A}$ s.t. $\Pr[\mathcal{A}(1^n, (f(x), r)) = \mathrm{gl}(x, r)] \geq \frac{1}{2} + \frac{1}{\mathrm{poly}(n)}$
$\Rightarrow \exists p.p.t.\ \mathcal{A}_r$ s.t. $\Pr[\mathcal{A}_r(1^n, f(x)) \in f^{-1}(f(x))] = \frac{1}{\mathrm{poly}'(n)}$.

Proof: see book.

PRGs

Thereom

Let f be a one-way permutation with hard-core predicate hc. Then $G(s) = f(s)||\text{hc}(s)$ is a PRG with expansion factor $\ell(n) = n + 1$.

PRGs

Thereom

Let f be a one-way permutation with hard-core predicate hc. Then $G(s) = f(s)||\text{hc}(s)$ is a PRG with expansion factor $\ell(n) = n + 1$.

Proof sketch:
$\mathcal{A}_r$ receives challenge $f(x)$ and must output $\text{hc}(x)$.
Choose $r \leftarrow \{0, 1\}$, and send $f(x)||r$ to $\mathcal{A}$.
If $\mathcal{A}$ outputs 0, $\mathcal{A}_r$ outputs r. Otherwise, $\overline{r}$.

PRGs

Thereom

Let f be a one-way permutation with hard-core predicate hc. Then $G(s) = f(s)||\text{hc}(s)$ is a PRG with expansion factor $\ell(n) = n + 1$.

Proof sketch:
$\mathcal{A}_r$ receives challenge $f(x)$ and must output $\text{hc}(x)$.
Choose $r \leftarrow \{0,1\}$, and send $f(x)||r$ to $\mathcal{A}$.
If $\mathcal{A}$ outputs 0, $\mathcal{A}_r$ outputs r. Otherwise, $\overline{r}$.

Key observation in the analysis: note that $f(x)$ is uniformly distributed, since x is uniform, and f is a permutation.

Increasing the Expansion in a PRG

Theorem

If there exists a PRG with expansion factor $n + 1$, then, for any poly(n), there exists a PRG with expansion factor poly(n).

Increasing the Expansion in a PRG

Theorem

If there exists a PRG with expansion factor $n + 1$, then, for any poly(n), there exists a PRG with expansion factor poly(n).

Construction (informally):
Evaluate the PRG, save the last output bit, and feed the first n bits back in.

Increasing the Expansion in a PRG

Theorem

If there exists a PRG with expansion factor $n + 1$, then, for any poly(n), there exists a PRG with expansion factor poly(n).

Construction (informally):
Evaluate the PRG, save the last output bit, and feed the first n bits back in.
Save the last output bit again, and feed the first n bits back in....

Increasing the Expansion in a PRG

Theorem

If there exists a PRG with expansion factor $n+1$, then, for any poly(n), there exists a PRG with expansion factor poly(n).

Construction (informally):
Evaluate the PRG, save the last output bit, and feed the first n bits back in.
Save the last output bit again, and feed the first n bits back in....
Output it all.

PRF from PRG

Theorem

Let G be a PRG with expansion factor $\ell(n) = 2n$. Then there exists a fixed-length PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

PRF from PRG

Theorem

Let G be a PRG with expansion factor $\ell(n) = 2n$. Then there exists a fixed-length PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

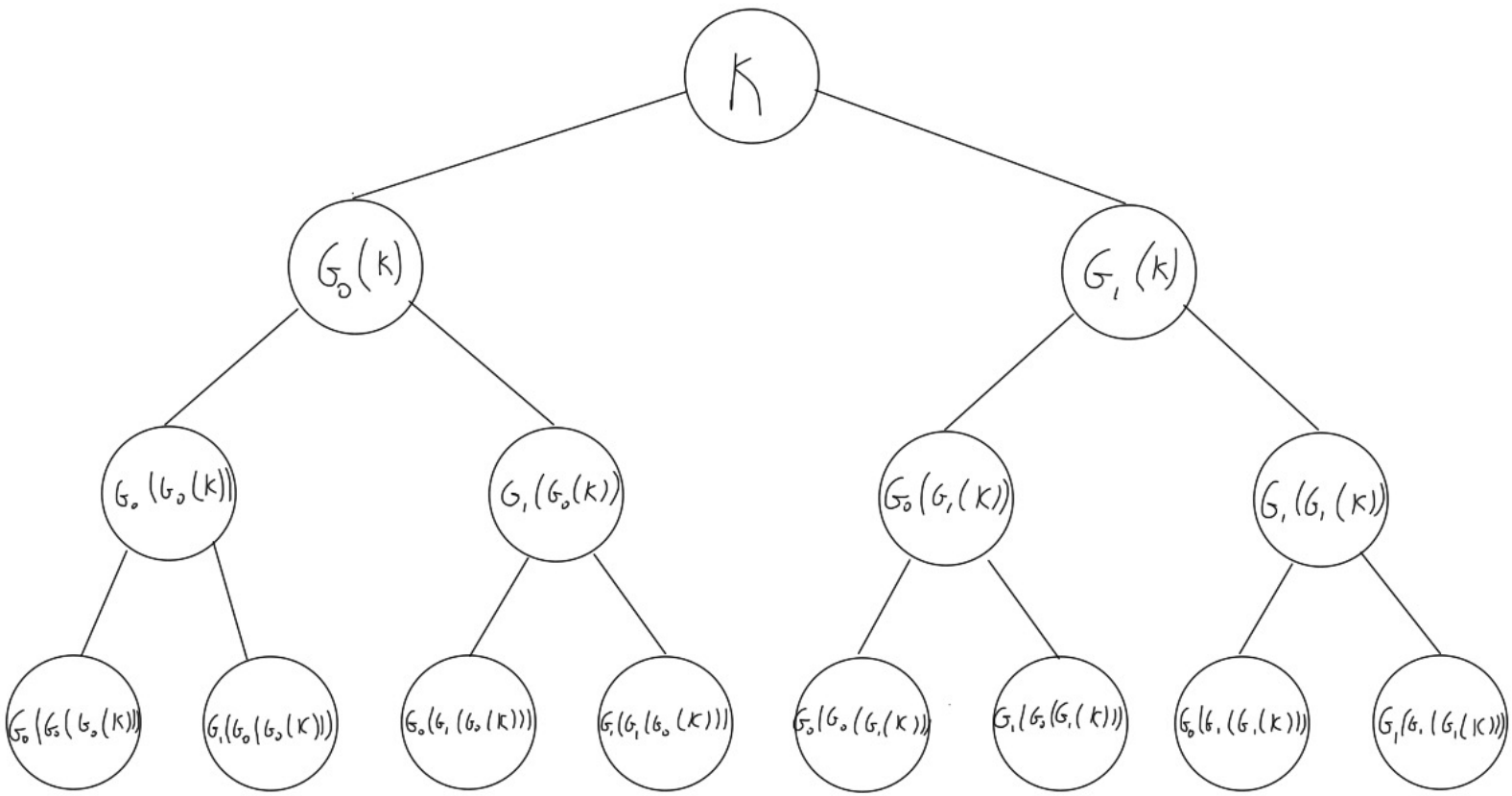
Construction:
Define G_0 and G_1 such that $G(s) = G_0(s)||G_1(s)$.
For key k, and input $x = x_1, \ldots, x_n$,
$F_k(x) = G_{x_n}(G_{x_{n-1}}(\cdots(G_{x_2}(G_{x_1}(k)))\cdots))$

PRF from PRG

Theorem

Let G be a PRG with expansion factor $\ell(n) = 2n$. Then there exists a fixed-length PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

Construction:
Define G_0 and G_1 such that $G(s) = G_0(s)||G_1(s)$.
For key k, and input $x = x_1, \ldots, x_n$,
$F_k(x) = G_{x_n}(G_{x_{n-1}}(\cdots(G_{x_2}(G_{x_1}(k)))\cdots))$



Strong PRP from PRF

Theorem

If F is a PRF, then for $k_1, k_2, k_3 \leftarrow \{0,1\}^n$, the 3-round Feistel network using $F_{k_1}, F_{k_2}, F_{k_3}$ as round functions is a strong pseudorandom permutation.

Tying it all together

Corollary

If one way functions exist, then so do PRGs, PRFs, and strong PRPs.

Tying it all together

Corollary

If one way functions exist, then so do PRGs, PRFs, and strong PRPs.

Corollary

If one way functions exist, then so does CCA-secure private-key encryption, and secure message authentication codes.

Tying it all together

Corollary

If one way functions exist, then so do PRGs, PRFs, and strong PRPs.

Corollary

If one way functions exist, then so does CCA-secure private-key encryption, and secure message authentication codes.

Theorem

If non-trivial private-key encryption exists, then one way functions exist.

Tying it all together

Corollary

If one way functions exist, then so do PRGs, PRFs, and strong PRPs.

Corollary

If one way functions exist, then so does CCA-secure private-key encryption, and secure message authentication codes.

Theorem

If non-trivial private-key encryption exists, then one way functions exist.

Theorem

If MACs exist (supporting an unbounded, polynomial number of queries), then one way functions exist.