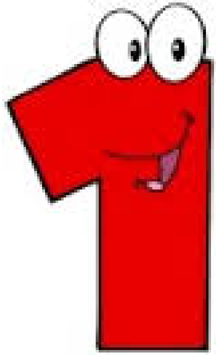
Theoretical constructions of pseudorandom objects

Leanne Streekstra

MSc Logic
ILLC, University of Amsterdam

Okt 20, 2014



One-way functions

- Easy to compute, hard to invert.
  - There exists a PPT algorithm computing f.
  - For all PPT algorithms A, there exists a negligible function:
    $\underset{x \leftarrow \{0,1\}^n}{Pr}[\mathrm{A}(\mathrm{f}(\mathrm{x})) \in \mathrm{f}^{-1}(\mathrm{f}(\mathrm{x}))] \leq \mathrm{negl}(\mathrm{n})$.

Hard-core predicates

- Infeasible to determine hc given f(x)
  - hc(x) can be computed in polynomial time given x.
  - For all PPT algorithms A, there exists a negligible function: $\Pr_{x \leftarrow \{0,1\}^n}[A(f(x)) = hc(x)] \leq 1/2 + negl(n)$.

Constructing hc

- For every one-way function f, there exists a one-way function g with a hard-core predicate hc.
- If f is a permutation, so is g.
- $g(x,r) \overset{def}{=} (f(x),r)$, for $|x|=|r|$.
  - $hc(x,r) \bigoplus_{i=1}^{n} x_i \cdot r_i$

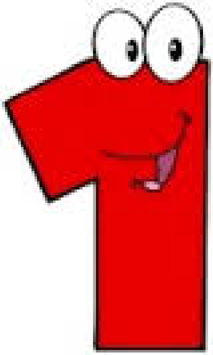
Constructing a PRG with minimal expansion

- If f is a one-way permutation and hc a hard-core predicate for f then G is a PRG:
  - G(x)=(f(x), hc(x))

- G has expansion factor l(n)=n+1

Increasing the expansion factor

- Construct $\widetilde{G}$, with expansion factor $\widetilde{l}$(n)=p(n) for any polynomial p(n), by iteration of G.



Construction

- Construct a PRF from a PRG with expansion factor l(n)=2n.

Construction

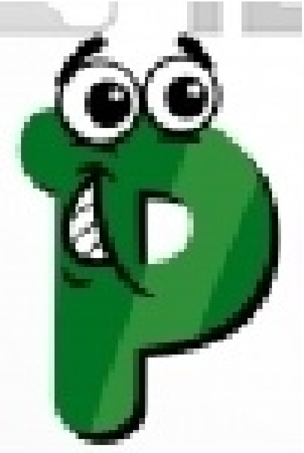
- Construct a PRF from a PRG with expansion factor l(n)=2n.
- $\mathrm{F}_k(x_1 x_2 \ldots x_n) = \mathrm{G}_{x_n}(\ldots(\mathrm{G}_{x_2}(\mathrm{G}_{x_1}(\mathrm{k})))\ )$.

Feistel network

- Combine a PRF with a 3-round Feistel network to get a PRP.

Feistel network

- Combine a PRF with a 3-round Feistel network to get a PRP.
- Strong PRP: combine a PRF with a 4-round Feistel network.



From PRG to one-way function

- If there exists a PRG, there exists a one-way function.

From PRG to one-way function

- If there exists a PRG, there exists a one-way function.
- If there exists a private-key encryption scheme with indistinguishable ecryptions in the presence of an eavesdropper, then there exists a one-way function.

Conclusion

- One-way functions are both sufficient and necessary for all private-key cryptography


#1
#1