CS 276 Scribe Notes.

Scribe

Daniel Schonberg
dschonbe@eecs.berkeley.edu

Lecturer

David Wagner
daw@cs.berkeley.edu

Abstract

Second half (post-break) of CS276 Lecture on February 2, 2004

1 Pseudo Random Permutations

A study of a sub class of pseudo random functions. For a function to be a permutation, it must be a mapping to strings of equal length. Further, the mapping should be one to one (a bijection). To examine a functions success as a permutation, we must examine the chance of two inputs producing the same output (a collision).

Fact: Given q random n-bit strings

$$0.3\frac{q(q-1)}{2^n} \leq Pr[\text{collision}] \leq 0.5\frac{q(q-1)}{2^n}$$

Knowing this chance of collision, we study the chance an adversary has of finding such a collision given a limitation to at most q queries.

Claim: $|Pr[A^f = 1] - Pr[A^\pi = 1]| \leq 0.5\frac{q(q-1)}{2^n}$
$\forall$ A with less than q queries.

First, note the following result from the homework.

$$d(D, D') \leq d(D|E, D'|E) + Pr[\bar{E}]$$

Proof: Let BAD be the output that there is a collision in the outputs of A's oracle during the running of A.

$$\begin{aligned} Pr[A^f = 1] &= Pr[A^f = 1|B\bar{A}D]Pr[B\bar{A}D] + Pr[A^f = 1|BAD]Pr[BAD] && (1)\\ &\leq Pr[A^\pi = 1] + Pr[BAD] && (2)\\ &\leq Pr[A^\pi = 1] + 0.5\frac{q(q-1)}{2^n} && (3)\end{aligned}$$

The absolute value bars can be achieved with trivial adaptations of this argument. The result then

□

The notation for Pseudo random permutations (PRP) and Pseudo random functions (PRF) is supplied below.

Definition: $f \longleftarrow Fun_{n,n}$ is a $(\infty, q, 0.5\frac{q(q-1)}{2^n})$-PRP.

Definition: $\pi \longleftarrow Perm_n$ is a $(\infty, q, 0.5\frac{q(q-1)}{2^n})$-PRF.
With these definitions, we show the relationship between PRFs and PRPs.

Claim: If $f : Keys \times \{0,1\}^n$ is a (t, q, ϵ)-PRP, it is a $(t, q, \epsilon + 0.5\frac{q(q-1)}{2^n})$-PRF.

Proof:

$$\begin{aligned}
Adv^{PRF}A &= |Pr[A^{F_k} = 1] - Pr_{f \in Functions}[A^f = 1]| && (4)\\
&= |Pr[A^{F_k} = 1] - Pr_{\pi \leftarrow Perms}[A^\pi = 1] + Pr[A^\pi = 1] - Pr[A^f = 1]| && (5)\\
&\leq |Pr[A^{F_k} = 1] - Pr[A^\pi = 1]| + |Pr[A^\pi = 1] - Pr[A^f = 1]| && (6)\\
&\leq Adv^{PRP}A + 0.5\frac{q(q-1)}{2^n} && (7)
\end{aligned}$$

□

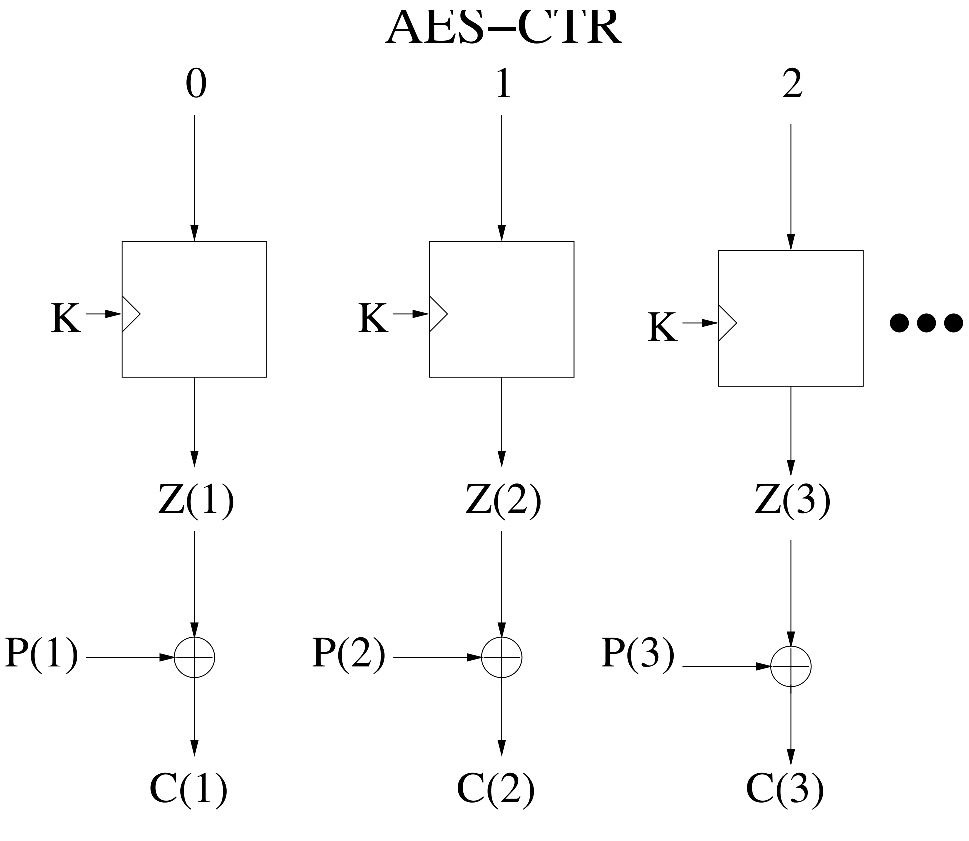

Figure 1: A block diagram of AES blocks used in AES-CTR (counter) mode to act as a pseudo random generator.

We know extend this discussion to Pseudo Random Generators (PRG). We see that is AES is a good PRF, as we take it to be, then AES-CTR (Figure 1) can act as a good PRG for encryption purposes.

Claim: If f is a (t, q, ϵ)-PRF, then $G(k) = (F_k(0), F_k(1), \ldots, F_k(q-1))$ is a (t, ϵ)-PRG.

Proof:

1. If $f = Fun_{n,m}$ (truly random),

$$\begin{aligned} Adv^{PRG}A &= |Pr_{f \in fun_{n,m}}[A(G(f)) = 1] - Pr_{y \in \{0,1\}^{qn}}[A(y) = 1]| && (8) \\ &= |Pr[A(f(0), f(1), \ldots, f(q-1)) = 1] - Pr[A(y) = 1]| && (9) \\ &= |Pr_{y \leftarrow \{0,1\}^n}[A(y) = 1] - Pr[A(y) = 1]| && (10) \\ &= 0 && (11) \end{aligned}$$

2. Replace f by F_k. The resulting Adv only increases by ϵ.

$\square$

Conclusion: AES-CTR (Figure 1) mode is a good PRF, if AES is a good PRF (or good PRP).