Modern Crypology - Problem Set 2

name: Guy Levy
id: 206865362

1 - PRGs

Answers:

1. Assume (for the sake of contradiction) G' is not a PRG, so there exists an index $i \in [l]$ such that:

$\exists$ PPT D and $\exists p : \mathbb{N} \to \mathbb{N}$ some polynomial:

$$\left| Pr_{x \leftarrow U_n}[D(G'_i(x)) = 1] - Pr_{b \leftarrow U_1}[D(b) = 1] \right| > \frac{1}{2} + \frac{1}{p(n)}$$

But $G'_i(x) = G_{\sigma(j)}(x)$ for one $j \in [l]$ So

$$\left| Pr_{x \leftarrow U_n}[D(G_{\sigma(j)}(x)) = 1] - Pr_{b \leftarrow U_1}[D(b) = 1] \right| > \frac{1}{2} + \frac{1}{p(n)}$$

So there exists index $k = \sigma(j), k \in [l]$ in which

$$\left| Pr_{x \leftarrow U_n}[D(G_k(x)) = 1] - Pr_{b \leftarrow U_1}[D(b) = 1] \right| > \frac{1}{2} + \frac{1}{p(n)}$$

In contradiction to the assumption that G is a PRG. $\Rightarrow\Leftarrow$
So we must conclude G' is a PRG.

2. Denote $n < l$ the numbers for which $G : \{0,1\}^n \to \{0,1\}^l$.

So by definition of G' its of the form $G' : \{0,1\}^{2n} \to \{0,1\}^{2l}$

Assume we have a distinguisher D' for G'.
I will construct a distinguisher D for G and thus prove: G' not a PRG $\Rightarrow$ G not a PRG.
Equivalent to the claim we would like to prove: G is a PRG $\Rightarrow$ G' is a PRG.

D' distinguishes G', so $adv_D(G') \geq \frac{1}{p(n)}$ for $p : \mathbb{N} \to \mathbb{N}$ some polynomial.

Define D:
D, given x as an input generates $b \xleftarrow{\$} \{0,1\}$.
if $b = 0$, D generates $s \xleftarrow{\$} U_n$ and calculates $y \leftarrow G(s)$.
 if $b = 1$, D generates $y \xleftarrow{\$} U_l$.
D runs $D'(x \cdot y)$ and returns the result.

Assessment of Ds advantage:

$$adv_D(G) = \left| Pr_{s \leftarrow U_n}[D(G(s)) = 1] - Pr_{x \leftarrow U_l}[D(x) = 1] \right|$$

$$= \left| Pr_{s \leftarrow U_n}[D'(G(s) \cdot y) = 1] - Pr_{x \leftarrow U_l}[D'(x \cdot y) = 1] \right|$$

Simplify members of equation:
$Pr_{s \leftarrow U_n}[D'(G(s) \cdot y) = 1] =$
$Pr_{s \leftarrow U_n}[D'(G(s) \cdot y) = 1 \wedge y \leftarrow U_l] + Pr_{s \leftarrow U_n}[D'(G(s) \cdot y) = 1 \wedge y \leftarrow G(U_n)] =$
$\frac{1}{2} Pr_{s \leftarrow U_n, s' \leftarrow U_n}[D'(G(s) \cdot G(s')) = 1] + \frac{1}{2} Pr_{s \leftarrow U_n, y \leftarrow U_l}[D'(G(s) \cdot y) = 1]$

$Pr_{x \leftarrow U_l}[D'(x \cdot y) = 1] =$
$Pr_{x \leftarrow U_l}[D'(x \cdot y) = 1 \wedge y \leftarrow U_l] + Pr_{x \leftarrow U_l}[D'(x \cdot y) = 1 \wedge y \leftarrow G(U_n)] =$
$\frac{1}{2} Pr_{x \leftarrow U_l, y \leftarrow U_n}[D'(x \cdot y) = 1] + \frac{1}{2} Pr_{x \leftarrow U_l, s \leftarrow U_n}[D'(x \cdot G(s)) = 1]$

Continue with original assessment:
$adv_D(G) = \ldots =$

$$\left| \frac{1}{2} Pr_{s \leftarrow U_n, s' \leftarrow U_n}[D'(G(s) \cdot G(s')) = 1] + \frac{1}{2} Pr_{s \leftarrow U_n, y \leftarrow U_l}[D'(G(s) \cdot y) = 1] \right.$$
$$\left. - \frac{1}{2} Pr_{x \leftarrow U_l, y \leftarrow U_n}[D'(x \cdot y) = 1] - \frac{1}{2} Pr_{x \leftarrow U_l, s \leftarrow U_n}[D'(x \cdot G(s)) = 1] \right|$$

$$=^{(*)} \left| \frac{1}{2} Pr_{s \leftarrow U_n, s' \leftarrow U_n}[D'(G(s) \cdot G(s')) = 1] - \frac{1}{2} Pr_{x \leftarrow U_l, y \leftarrow U_n}[D'(x \cdot y) = 1] \right|$$
$$= \frac{1}{2} \left| Pr_{s \leftarrow U_n, s' \leftarrow U_n}[D'(G(s) \cdot G(s')) = 1] - Pr_{x \leftarrow U_l, y \leftarrow U_n}[D'(x \cdot y) = 1] \right|$$
$\frac{1}{2} adv_{D'}(G') \geq \frac{1}{2p(n)}$

$(*)$ Here we assume D' symmetric on both halves of input. (if there exists some D' for G' then it achieves the same advantage if we switch between 2 halves of input) in particular, lets build such symmetric distinguisher, run D' and its symmetric opposite and flip a coin as to which result to return.

3. Let $G_0 : \{0,1\}^n \to \{0,1\}^l$ be some PRG.

Assume for the sake of contradiction that the claim is true.
$G_1 = G_0(s) \cdot s_1$ is a PRG.
$G' = G_1(s) \cdot s_1 = G_0(s) \cdot s_1^2$ is a PRG.

I will show that G' is distinguishable from U_{l+2} and this not a PRG, and by that reach a contradiction to the claim.

Define D:
Distinguisher D looks at final 2 bits of its input and outputs 1 if they are equal. else outputs 0.

Assess Ds advantage on G':
$adv_D(G') = \left|Pr_{s\leftarrow U_n}[D(G'(s)) = 1] - Pr_{y\leftarrow U_{l+2}}[D(y) = 1]\right| = |1 - \frac{1}{2}| = \frac{1}{2} > \frac{1}{p(n)}$
when $p(n) = 3$, a polynomial.

2 - PRG implies OWF

Answer:

Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a PRG. Also G is 1:1.
Want to prove G is OWF. So need to prove:

1. $G(x)$ is computable in polynomial time.
2. for any PPT A and all sufficiently large n:

$$Pr_{x\leftarrow\{0,1\}^n}[A(1^n, G(x)) = x' : G(x') = G(x)] \leq negl(n)$$

proving 1. is immediate from the definition of PRG.
proving 2:
Assume G is not a OWF;
$\exists$ PPT A s.t. $Pr_{x\leftarrow\{0,1\}^n}[A(1^n, G(x)) = x' : G(x') = G(x)] \geq \frac{1}{p(n)}$ for some polynomial p
From the assumption that G is 1:1
$\exists$ PPT A s.t. $Pr_{x\leftarrow\{0,1\}^n}[A(1^n, G(x)) = x] \geq \frac{1}{p(n)}$ for some polynomial p

Using A, I will now construct D - a distinguisher for G, and thus show that G is not a PRG. this is a contradiction.
So we conclude G must be OWF and end the proof.

Defining D:
Given input $y \in \{0,1\}^{n+1}$, D calculates $A(y)$, this returns some $x \in \{0,1\}^n$. D checks if $G(x) = y$.
if holds, return 1, else return 0.

Now we estimate $adv_D(G)$:
$\left|Pr_{x\leftarrow U_n}[D(G(x)) = 1] - Pr_{y\leftarrow U_{n+1}}[D(y) = 1]\right|$
$= \left|Pr_{x\leftarrow U_n}[A(G(x)) = x] - Pr_{y\leftarrow U_{n+1}, x\leftarrow U_n}[A(y) = x]\right|$
$\geq Pr_{x\leftarrow U_n}[A(G(x)) = x] - Pr_{y\leftarrow U_{n+1}, x\leftarrow U_n}[A(y) = x]$
$\geq \frac{1}{p(n)} - \Big[Pr_{y\leftarrow U_{n+1}, x\leftarrow U_n}[A(y) = x \wedge G(x) = y] + Pr_{y\leftarrow U_{n+1}, x\leftarrow U_n}[A(y) = x \wedge G(x) \neq y]$

Estimate some members of equation:
$Pr_{y\leftarrow U_{n+1}, x\leftarrow U_n}[A(y) = x \wedge G(x) = y] \leq Pr_{y\leftarrow U_{n+1}, x\leftarrow U_n}[G(x) = y] \leq \frac{1}{2^{n+1}}$

$Pr_{y\leftarrow U_{n+1},x\leftarrow U_n}[A(y)=x\wedge G(x)\neq y]\leq Pr_{y\leftarrow U_{n+1},x\leftarrow U_n}[A(x)=y]\leq \frac{1}{2^n}$

Back to original estimation: $adv_D(G)\geq\ldots\geq \frac{1}{p(n)}-\frac{1}{2^{n+1}}-\frac{1}{2^n}\geq^{(*)}\frac{1}{2p(n)}$
$(*)$ $\frac{1}{2p(n)}-negl(n)\geq 0$ holds for sufficiently high n

3 - Bad Primes for Discrete Log

Answers:

1. Given we have $p, y=g^x$ we can calculate $y^{\frac{p-1}{2}}$.

If the result of this is e, we return $LSB(x)=0$.
Otherwise we return $LSB(x)=1$.

This holds because if x is even, i.e. for some $n\in\mathbb{N}: x=2n$ then:

$$y^{\frac{p-1}{2}}=g^{x\frac{p-1}{2}}=g^{2n\frac{p-1}{2}}=g^{n(p-1)}=g^{n\cdot ord(\mathbb{Z}_p^*)}=e$$

And if we get $y^{\frac{p-1}{2}}=e$ then $g^{x\frac{p-1}{2}}=e$ then for some $m\in\mathbb{N}$ it must hold that:
$x\frac{p-1}{2}=m\cdot ord(\mathbb{Z}_p^*)$
$\Rightarrow x(p-1)=2m(p-1)$
$\Rightarrow x=2m$

Overall Ive shown: x is even $\iff y^{\frac{p-1}{2}}=e$.
And so the algorithm is correct.

2. $ord(\mathbb{Z}_p^*)=2^k$ so $0\leq x\leq 2^k$.

If $k<2$ then x can be encoded by one bit which we already got.
Else, notice that the second LSB of x is $LSB(\frac{x}{2})$.
Compute:
$y^{\frac{p-1}{4}}=g^{\frac{x}{2}\cdot\frac{p-1}{2}}$
Exactly by the proof in (1): $\frac{x}{2}$ is even if and only if the result of this computation is e.
So the second LSB of x is 0 $\iff$ the result is 0.

3. Given y we compute $LSB(x)$ like in (1).

Then if x is even we compute $LSB(\frac{x}{2})$ to get the second LSB (like in 1).
Or if x is odd we compute $LSB(\frac{x-1}{2})$ to get the second LSB.$(*)$

Explaination of $(*)$: $LSB(\frac{x-1}{2})$ is computed by computing $(y\cdot g^{p-2})^{\frac{p-1}{4}}$.
If the result is e then $LSB(\frac{x-1}{2})=0$, otherwise 1.

$$(y\cdot g^{p-2})^{\frac{p-1}{4}}=(g^{x+p-2})^{\frac{p-1}{4}}=(g^{x-1+p-1})^{\frac{p-1}{4}}=(g^{x-1})^{\frac{p-1}{4}}=e\iff LSB(\frac{x-1}{2})=0$$

We continue these steps iterativly to compute x:

In [ ]:
```
def bad_prime_log(y,p,k,g):
    assert(p = 2**k + 1)
    x = 0
    for i in range(k):
        if not y**( (p-1) / (2 * 2**i) ) == 0:
            x = x + 2**i
            y = y * g**(p-2)
    return x
```

4 - Information Theoretic MAC

4.1 Naive Adversary

Answer:

A chooses random $m \in_R \{0,1\}^n$
and random tag $a \in_R \{0,1\}^t$
Given some message m, m has some valid tag $MAC_k(m)$.
So m has at least 1 valid tag.
Assuming $M \sim U_n \to MAC_k(M) \sim U_n$ then A succeeds with probability 2^{-t}

4.2 Pairwise Independent Hashing

Denote $H = \{h_{a,b} : \mathbb{F} \to \mathbb{F}\}_{a,b \in \mathbb{F}}$ (the collection mentioned)
Let there be $x_1, x_2, y_1, y_2 \in \mathbb{F}$

$Pr_{h \leftarrow H}[h(x_1) = y_1 \text{ and } h(x_2) = y_2] =$
$Pr_{a \leftarrow \mathbb{F}, b \leftarrow \mathbb{F}}[h_{a,b}(x_1) = y_1 \text{ and } h_{a,b}(x_2) = y_2] =$
$Pr_{a \leftarrow \mathbb{F}, b \leftarrow \mathbb{F}}[a \cdot x_1 + b = y_1 \text{ and } a \cdot x_2 + b = y_2] =^{(*)}$
$Pr_{a \leftarrow \mathbb{F}}[a \cdot x_1 = y_1 \text{ and } a \cdot x_2 = y_2] =^{(**)}$
$Pr[x_1 = y_1 \text{ and } x_2 = y_2] = \frac{1}{2^m} \cdot \frac{1}{2^m} = 2^{-2m} \Rightarrow H$ is pairwise independent.

Explanation $(*)$:
If b is choosen at random from $\mathbb{F}$ then given some x, I claim that every y is equally probable to be $x + b$.
Denote random variable $B \sim uniform(\mathbb{F}), x \in \mathbb{F}$.
Want to prove $x + B \sim uniform(\mathbb{F})$. That is true because:

$$\{x + b | b \in \mathbb{F}\} = \{x - x + b | b - x \in \mathbb{F}\} = \{b | b - x \in \mathbb{F}\} = \mathbb{F}$$

Explanation $(**)$:
If a is choosen at random from $\mathbb{F}$ then given some x, I claim that every y is equally probable to be $a \cdot x$.

Denote random variable $A \sim uniform(\mathbb{F}), x \in \mathbb{F}$.
Want to prove $A \cdot x \sim uniform(\mathbb{F})$. That is true because:

$$\{a \cdot x | a \in \mathbb{F}\} = \{a \cdot x^{-1} \cdot x | a \cdot x^{-1} \in \mathbb{F}\} = \{a | a \cdot x^{-1} \in \mathbb{F}\} = \mathbb{F}$$

Now assume $|\mathbb{F}_1| = 2^n, |\mathbb{F}_1| = 2^m, n \leq m$
We saw $H = \{h_{a,b} : \mathbb{F} \to \mathbb{F}\}_{a,b \in \mathbb{F}}$ is pairwise independent (with functions of the form : $h : \mathbb{F}_1 \to \mathbb{F}_1$).
To generalize to $h : \mathbb{F}_1 \to \mathbb{F}_2$ we use some function $f : \mathbb{F}_1 \to \mathbb{F}_2$ such that every $y \in \mathbb{F}_2$ has exactly 2^{n-m} sources.
Then $H' = \{h_{a,b}(x) : a \cdot f(x) + b\}_{a,b \in \mathbb{F}_2}$ is pairwise independent.

4.3 One-Time MAC

Assume the messages are the members of te field $\mathbb{F}_1$ s.t. $\mathbb{F}_1$ is the finite field of size 2^n.
Assume keys are $k = k_1 \cdot k_2$ where $k_1, k_2 \in \mathbb{F}_2$.
When $\mathbb{F}_2$ is the finite field of size 2^t.
Let $f : \mathbb{F}_1 \to \mathbb{F}_2$ be some function that for every y there are exactly 2^{n-t} sources.

$$MAC_k(m) = k_1 \cdot f(m) + k_2$$

Let A be some adversary.
From the fact that $\{MAC_k()\}_k$ is pairwise independent: $\forall x_1, x2 \in \mathbb{F}_1, \forall y_1, y_2 \in \mathbb{F}_2$:

$$Pr_{k \leftarrow K}[MAC_k(x_1) = y_1 \text{ and } MAC_k(x_2) = y_2] = 2^{-2m}$$

So $\forall x \in \mathbb{F}_1, \forall y \in \mathbb{F}_2$:
$Pr_{k \leftarrow K}[MAC_k(m) = t \text{ and } MAC_k(x) = y | MAC_k(m) = t]$
$= Pr_{k \leftarrow K}[MAC_k(x) = y] = \frac{2^{-2t}}{2^{-t}} = 2^{-t}$

So there is no information in the fact that $MAC_k(m) = t$ and so the best chance A has is to guess , i.e. 2^{-t}.

In [ ]: