1A)

SHANNON DEFINED "PERFECT SECRECY", i.e., THE FACT THAT THE CYPHERTEXT CARRIES NO INFORMATION ABOUT THE PLAINTEXT.

FROM DEF1:

LET M BE A RANDOM VARIABLE OVER $\mathcal{M}$, AND K BE A UNIFORM DISTRIBUTION OVER $\mathcal{K}$. (ENC, DEC) HAS PERFECT SECRECY IF:

$\forall M, \forall m \in \mathcal{M}, c \in \mathcal{C}$:

$$Pr[M = m] = Pr[M = m \mid \mathcal{C} = c]$$

I REFUTE THIS SENTENCE SHOWING AN ENCRYPTION SCHEME WITH NON-UNIFORM DISTRIBUTION $\mathcal{C}$, BUT PERFECT SECRECY IS STILL VALID.

ASSUME Π IS A PERFECT SECRET ENCRYPTION SCHEME.

I BUILD $\Pi'(Enc', Dec')$ AS: (KEYSPACE = $\mathcal{K}$, MESSAGE SPACE $\mathcal{M}$, CYPHERTEXT $\mathcal{C}$, M R.V. OVER $\mathcal{M}$.)

$Enc'(k, M)$:

$c \leftarrow \Pi_{Enc}(k, M)$

$b \leftarrow \$\{0,1\}^{10}$

IF $b \bmod 3 == 0$:

RETURN $c \| 01$

ELSE RETURN $c \| 00$

$Dec'(k, \mathcal{C})$:

$c' \leftarrow$ FIRST $M-2$ bit OF c

RETURN $\Pi_{Dec}(K, c)$

THIS ENCRYPTION SCHEME PRODUCES A NON-UNIFORM CYPHERTEXT DISTRIBUTION. THE PROBABILITY A CYPHERTEXT ENDS WITH 00 IS $3/4$ AND 01 IS $1/4$. STILL THIS ENCRYPTION SCHEME CARRIES NO INFO ABOUT THE MESSAGE, AND THE DECRYPTION DOES NOT DEPEND ON THE 2 LAST BITS OF CYPHERTEXT. SO, Π' IT'S PERFECTLY SECURE EVEN IF IT HAS A NON-UNIFORM CYPHERTEXT DISTRIBUTION.

SO, THE SENTENCE IS WRONG.

1b

(i)

$\mathcal{M} = \{0, 1, 2, 3, 4\}$ Enc $\Rightarrow c = k + m \bmod 5$

$K = \{0, 1, 2, 3, 4, 5\}$ Dec $\Rightarrow m = c - k \bmod 5$

ENC K \ M	0	1	2	3	4	
0	0	1	2	3	4	
1	1	2	3	4	0	
2	2	3	4	0	1	
3	3	4	0	1	2	
4	4	0	1	2	3	
5	0	1	2	3	4	

$Pr(c=0) = 6/30$

$Pr(c=1) = 6/30$

$Pr(c=2) = 6/30$

$Pr(c=3) = 6/30$

$Pr(c=4) = 6/30$

$$Pr(c=x) = 6/30 \quad \forall x \in \{0, 4\}$$

HENCE THE CYPHERTEXT CARRIES NO INFORMATION ABOUT THE MESSAGE, SO:

$$Pr[M = m] = Pr[M = m \mid C = c]$$

AND THE PERFECT SECRECY IS VALID.

1b

(ii)

$\mathcal{M} = \{m \in \{0,1\}^{\ell} : \text{LAST BIT OF } m \text{ IS } 0\}$

K UNIFORM OVER THE KEY SPACE $\mathcal{K} = \{0,1\}^{\ell-1}$

$Enc(K, m) \Rightarrow c = m \oplus (K \| 0)$

$Dec(k, c) \Rightarrow m = c \oplus (K \| 0)$

CLEARLY THIS ENC. SCHEME IS PERFECTLY SECURE BECAUSE IS A OTP WITH AN IRRELEVANT MODIFICATION. BY THE WAY, LET'S FORMALIZE THIS:

I HAVE TO SHOW $Pr[M = m] = Pr[M = m \mid C = c]$

- $Pr[M = m \mid C = c] = \dfrac{Pr[C = c \mid M = m] \cdot Pr[M = m]}{Pr[C = c]}$ (1)

- $Pr[C = c \mid M = m] = Pr[Enc(k, m) = c] =$

$Pr[c = m \oplus (K \| 0)] = \dfrac{1}{2^{\ell-1}}$

THIS BECAUSE THE PROBABILITY ONLY DEPENDS ON $\ell - 1$ BITS m AND k. SINCE THEY ARE IN UNIFORM DISTRIBUTIONS $1/2^{\ell-1}$ IS THE Pr.

- $Pr[C = c] = \sum_{m \in \mathcal{M}} Pr[C = c \wedge M = m] = \{\text{by SATURATION}\}$

$$= \sum_{m \in \mathcal{M}} Pr[C = c \mid M = m] \cdot Pr[M = m] = \text{(by BAYES)}$$

$$= \sum_{m \in \mathcal{M}} Pr[Enc(k, M) = c \mid M = m] \cdot Pr[M = m] =$$

$$= \sum_{m \in \mathcal{M}} Pr[Enc(k, m) = c] \cdot Pr[M = m] =$$

$$= Pr[Enc(k, m) = c] \cdot \underbrace{\sum_{m \in \mathcal{M}} Pr[M = m]}_{1} =$$

$$\Downarrow \; 1/2^{l-1}$$

So, I HAVE $P[C = c] = 1/(2^{l-1})$,

REPLACING THE FORMULA (1) WITH VALUES I GET:

$$Pr[M = m \mid C = c] = \frac{Pr[C = c \mid M = m] \cdot Pr[M = m]}{Pr[C = c]} =$$

$$= \frac{\left(\frac{1}{2^{l-1}}\right) \cdot Pr[M = m]}{\left(\frac{1}{2^{l-1}}\right)} = Pr[M = m] \quad \checkmark$$

2A

$\mathcal{H} = \{h_s : X \to Y\}_{s \in S}$ t-WISE INDEPENDENT $\forall$ SEQUENCES OF DISTINCT INPUTS $x_1, \ldots, x_t \in X$, $\forall$ OUTPUT SEQUENCE $y_1, \ldots, y_t \in Y$

$$Pr[h_s(x_1) = y_1 \wedge \ldots \wedge h_s(x_t) = y_t : s \leftarrow \$ S] = \frac{1}{|Y|^t}$$

(i)

$\forall t \geq 2$:

$\mathcal{H}$ t-WISE INDEPENDENT $\Rightarrow$ $(t-1)$-WISE INDEPENDENT

SINCE $\mathcal{H}$ IS t-WISE INDEPENDENT, I CAN WRITE THIS AS:

$$Pr[h_s(x_1) = y_1 \wedge \ldots \wedge h_s(x_{t-1}) = y_{t-1}] \cdot Pr[h_s(x_t) = y_t] =$$

$$= \underbrace{Pr[h_s(x_1) = y_1 \wedge \ldots \wedge h_s(x_{t-1}) = y_{t-1}]}_{(t-1)\text{-WISE INDEPENDENT}} \cdot \frac{1}{|Y|} =$$

$\frac{1}{|Y|}$ ← Probability of t-th element

(ii)

I SHOULD PROVE THAT (FOR A UNIFORMLY RANDOM S)

$$Pr[h_s(x_1) = y_1 \wedge h_s(x_2) = y_2 \wedge h_s(x_3) = y_3] = \frac{1}{|Y|^3}$$

$$Pr[h_s(x_1) = y_1 \wedge h_s(x_2) = y_2 \wedge h_s(x_3) = y_3] =$$

CONTINUE

$$= P_r\left[\begin{cases} s_0 + s_1 \cdot x_1 + s_2 \cdot x_1^2 = y_1 \\ s_0 + s_1 x_2 + s_2 x_2^2 = y_2 \\ s_0 + s_1 x_3 + s_2 x_3^2 = y_3 \end{cases}\right] =$$

$$= P_r\left[\begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\right] =$$

$$= P_r\left[\begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix}^{-1} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\right] =$$

THE RIGHT PART OF THE EQUAL IS CONSTANT, SO LET'S REPLACE IT FOR SOME COSTANTS k_0, k_1, k_2

$$= P_r\left[\begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} k_0 \\ k_1 \\ k_2 \end{pmatrix}\right] = \frac{1}{|y|^3}$$

S UNIFORMLY RANDOM

THIS IS VALID ONLY IF I CAN INVERT THE MATRIX, SO LET'S COMPUTE THE DETERMINANT.

$$\det\begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} = (x_2 x_3^2) + (x_1 x_2^2) + (x_1^2 x_3) - (x_1^2 \cdot x_2) - (x_1 x_3^2)$$

$$- (x_2^2 \cdot x_3) =$$

$$= x_2 x_3 (x_3 - x_2) + x_1 x_2 (x_2 - x_1) + x_1 x_3 (x_1 - x_3) \neq 0$$

✓

INPUTS DISTINCT

2b)

SAY THAT $X \Rightarrow (k,n)$-SOURCE IF $X \in \{0,1\}^n$, MIN-ENTROPY $(X) \geq k$.

(i) $l = 128$

MINIMAL AMOUNT OF MIN ENTROPY NEEDED TO OBTAIN $\varepsilon = 2^{-80}$

- MIN ENTROPY $\Rightarrow 2\log_2\left(\frac{1}{\varepsilon}\right) - 2 + l = 286 \quad (k)$
- ENTROPY LOSS $\Rightarrow k \geq l + \delta \Rightarrow 286 \geq 128 + \delta \Rightarrow \delta = 158$

(ii)

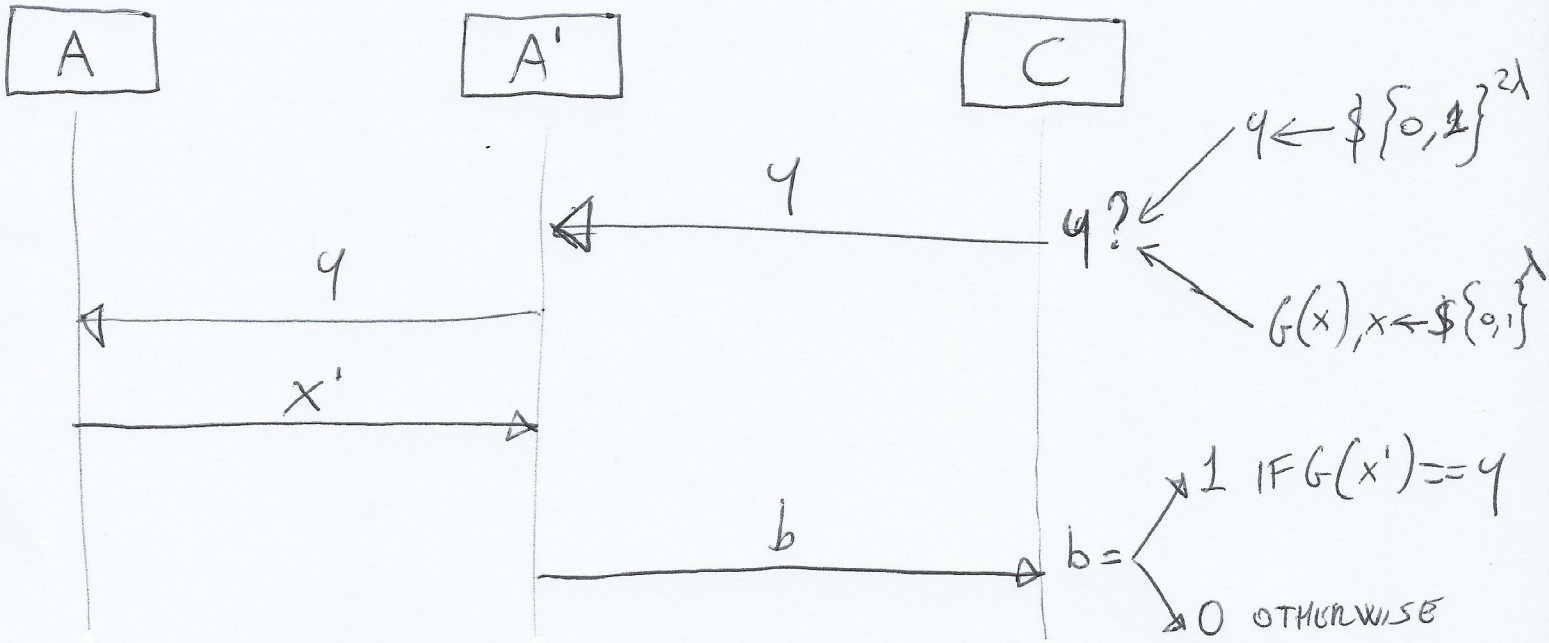
$\delta = 158$

$238 \geq l + 158 \Rightarrow l \leq 238 - 158 = 80 = l$

3A

$G: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ PRG with λ-bit stretch.

G is OWF?



Let's assume G is not a OWF. So, there exists a PPT attacker A able to find pre-images of G with pr. non negl.

$$Pr\left[A(y) = 1, x \leftarrow \$ \{0,1\}^\lambda, y = G(x)\right] \geq \frac{1}{poly(\lambda)} \quad (A)$$

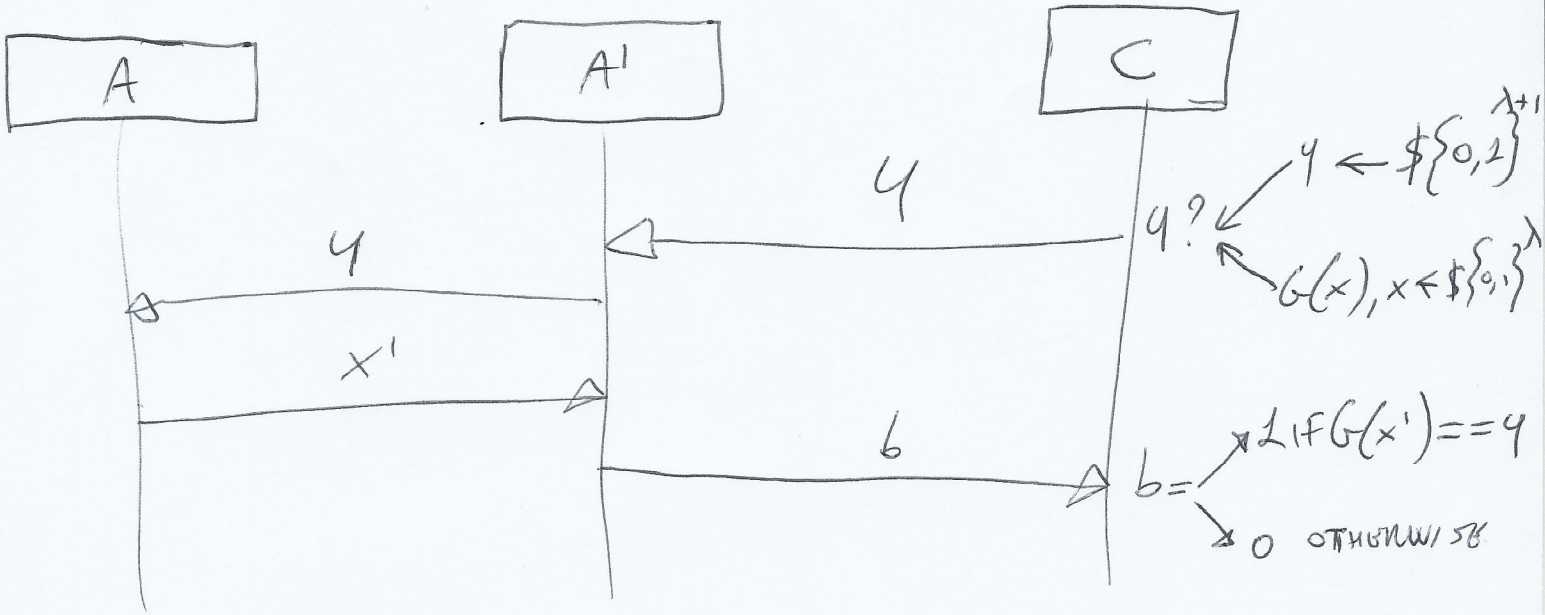
$$Pr\left[A(y) = 1, y \leftarrow \$ \{0,1\}^{2\lambda}\right] \leq \frac{2^\lambda}{2^{2\lambda}} = \frac{1}{2^\lambda} \left(\frac{\text{VALID INPUTS}}{\text{POSSIBLE INPUTS}}\right) \quad (B)$$

Let's take the first element (A) and the second (B).

$$\left| Pr[(A)] - Pr[(B)] \right| \geq \frac{1}{poly(\lambda)} - \frac{1}{2^\lambda} \not\in negl(\lambda).$$

3b)

As I did in the previous solution, I assume G is not a OWF. There exists a PPT attacker A able to find pre-images of G with Pr. non negl.



$$Pr\left[A(y)=1, x \leftarrow \$\{0,1\}^{\lambda}, y=G(x)\right] \geq 1/poly(\lambda) \qquad (A)$$

$$Pr\left[A(y)=1, y \leftarrow \{0,1\}^{2\lambda}\right] = \frac{2^{\lambda}}{2^{\lambda+1}} = \frac{1}{2}\left(\frac{\text{VALID INPUTS}}{\text{POSSIBLE INPUTS}}\right) \qquad (B)$$

$$\left|Pr[(A)] - P[(B)]\right| \geq \frac{1}{poly(\lambda)} - \frac{1}{2} \notin NEGL(\lambda).$$

4A

$G_1, G_2 : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ WITH $\ell \geq 1$.

AT LEAST ONE OF G_1, G_2 IS SECURE PRG.

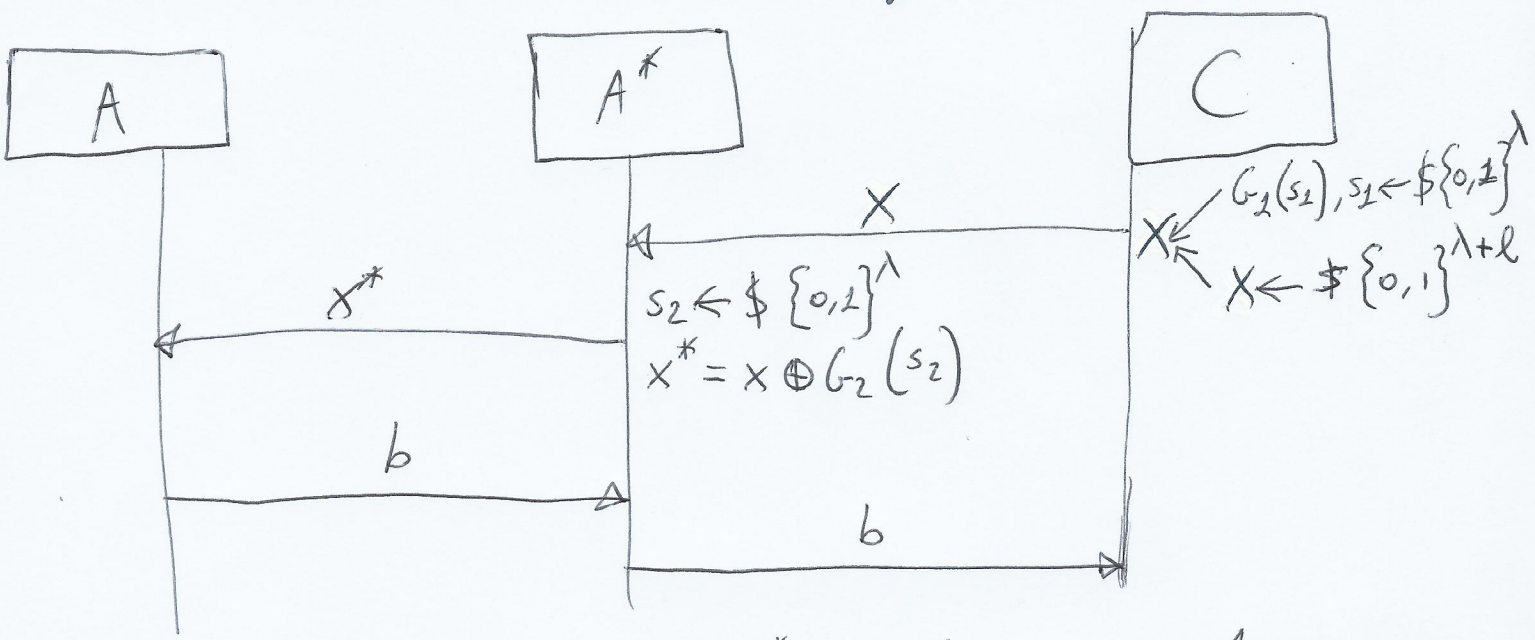
SHOW $G^* : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda+\ell}$ SECURE PRG COMBINING G_1 and G_2.

$G^* = G_1(s_1) \oplus G_2(s_2)$, WITH $s_1, s_2 \leftarrow \$ \{0,1\}^\lambda$

I ASSUME G^* ISN'T A SECURE PRG.

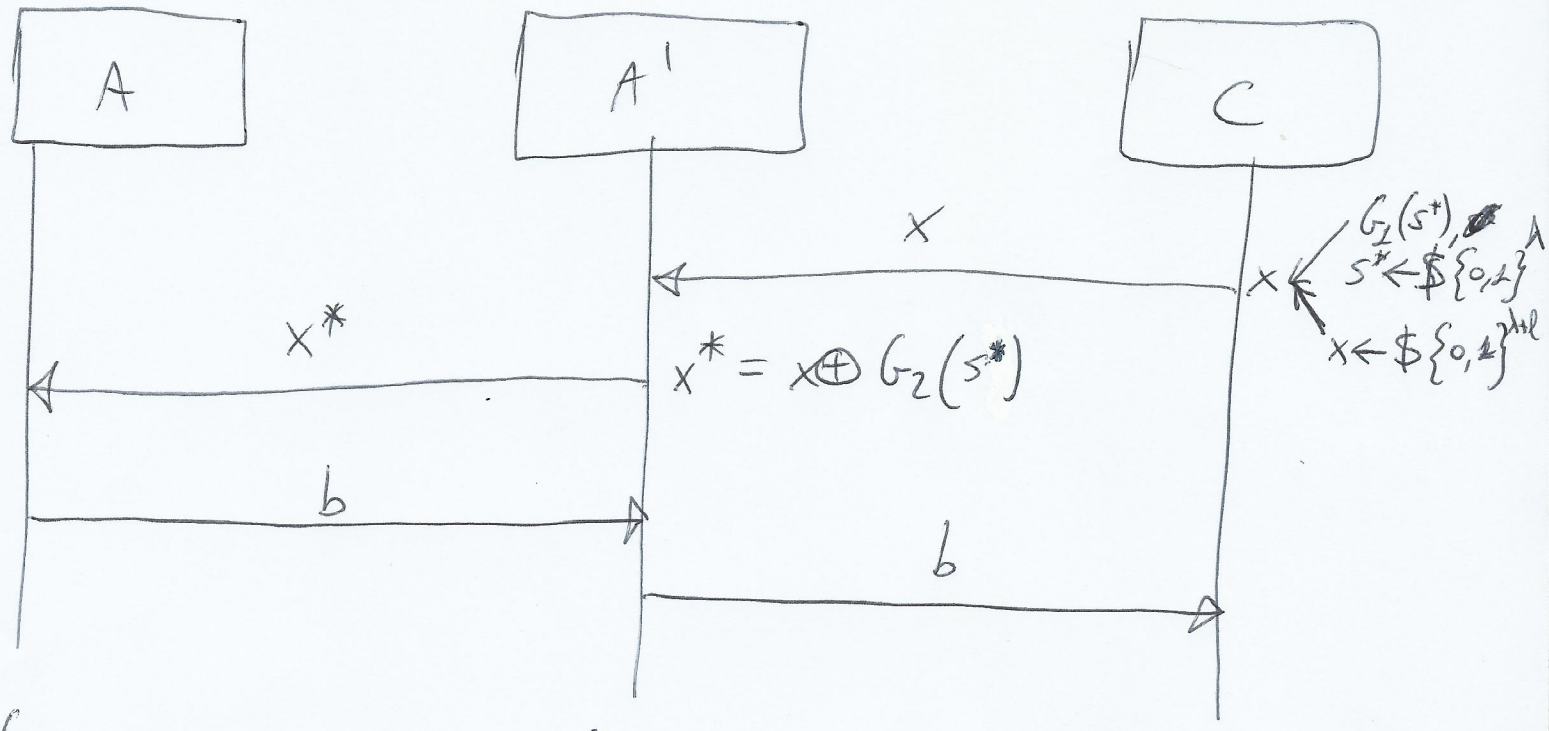
I ASSUME ALSO THAT G_1 IS A SECURE PRG AND EXISTS A PPT ATTACKER A ABLE TO DISTINGUISH BETWEEN G^* AND $U_{\lambda+\ell}$.

I CAN BUILD AN ATTACKER A^* THAT BREAKS G_1.



IF A CAN DISTINGUISH BETWEEN G^* AND $U_{\lambda+\ell}$, THEN A CAN DISTINGUISH BETWEEN G_1 AND $U_{\lambda+\ell}$ BUT THIS IS IMPOSSIBLE.

4b)



GIVEN THE FACT THAT G_1 IS A SECURE PRG, IT PRODUCES A COMPUTATIONALLY INDISTINGUISHABLE OUTPUT (RANDOM).
THEN x^* IS THE RESULT OF x (RANDOM) AND $G_2(s^*)$.
IT WORKS, THE ONLY COUNTEREXAMPLE I CAN GIVE IS WHEN $G_2 = G_1 \oplus a$, for $a \in \{0,1\}^{\lambda+l}$.
IN THAT CASE THE OUTPUT WILL BE $a, \forall s$.
HOWEVER, IF THE SEEDS ARE CHOOSEN BOTH RANDOMLY IT'S A NEGLIGIBLE PROBABILITY.

5A

Let consider any PRF family $F_k : \{0,1\}^n \to \{0,1\}^\ell, k \in \{0,1\}^\lambda$ with $n, \ell \in poly(\lambda)$.

The computationally unbounded distinguisher can brute force F_k. This means that A (the distinguisher) can queries the challenger C with all inputs x_i.

A will return 1 if $\exists k : \forall i \; F_k(x_i) = y_i$.

If the challenger computes values with PRF, A will return 1 (forever, so w.p. 1).

So, $Pr[A(y) = 1, y = F_k(x), k \leftarrow \$ \{0,1\}^\ell] = 1$ (A)

Instead, the probability that the challenger will take a function inside F_k is $\frac{2^\lambda}{(2^\ell)^{2^n}} \left(\frac{\text{valid inputs}}{\text{possible inputs}} \right)$ (B)

So, $Pr[A(y) = 1, y = G(x), G \leftarrow \$ \text{Functions}(n, \ell)] \leq \frac{2^\lambda}{(2^\ell)^{2^n}}$

I have then:

$$\left| P[(A)] - P[(B)] \right| \geq 1 - \frac{2^\lambda}{(2^\ell)^{2^n}} \notin \text{NEGL}.$$

5b

(i) THIS DOESNOT WORK. LET'S TAKE TWO INPUTS x AND x'.

$$x \oplus x' = F_k(x) \oplus F_k(x')$$

IF I TAKE TWO INPUTS AND A DISTINGUISHER A, A QUERIES C WITH THOSE INPUTS. IF C COMPUTES F_k, I GET:

$$x \oplus x' = F_k(x) \oplus F_k(x') \Rightarrow x \oplus x' = G'(k) \oplus x \oplus G'(k) \oplus x' \Rightarrow$$

$$x \oplus x' = x \oplus x'.$$

OBVIOUSLY A WILL DISTINGUISH WITH PROBABILITY 1.

IF, INSTEAD, C COMPUTES A RANDOM FUNCTION, A WILL RETURN 1 WITH PROBABILITY $1/2^{\lambda}$.

THEN SO,

$$\left| Pr\left[A(y_1, y_2) = 1, y_1 = F_k(x_1), y_2 = F_k(x_2), k \leftarrow \$\{0,1\}^{\lambda}\right] - Pr\left[A(y_1, y_2) = 1, y_1 = G(x_1), y_2 = G(x_2), G \leftarrow \text{FUNCTIONS}(\lambda, \lambda+\ell)\right] \right|$$

$$\geq 1 - \frac{1}{2^{\lambda}} \notin \text{NEGL}.$$

5b

(ii)

$$F_k(x) := F_x(k), \quad F: \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\ell;$$

LET'S ASSUME A BAD CASE k^*:

$$F_{k^*}(x) = 0^\ell$$

THIS HAPPENS WITH NEGLIGIBLE PROBABILITY IF THE KEY IS CHOOSEN RANDOMLY.

SINCE THE ATTACKER A CAN QUERY THE INPUT (IT'S x), A CAN FIX THE INPUT.

WITH THIS:

- IF THE FUNCTION IS REAL $\to Pr = 1$
- IF THE FUNCTION IS RANDOM $\to Pr = 1/2^\lambda$

$$\left| Pr\left[A(y) = 1, y = F_k(x), k^*\right] - Pr\left[A(y) = 1, y = G(x), G \leftarrow R\,\text{FUNCTIONS}(\lambda, \lambda, \ell)\right] \right| \geq 1 - \frac{1}{2^\lambda}$$

$\notin$ NEGL.

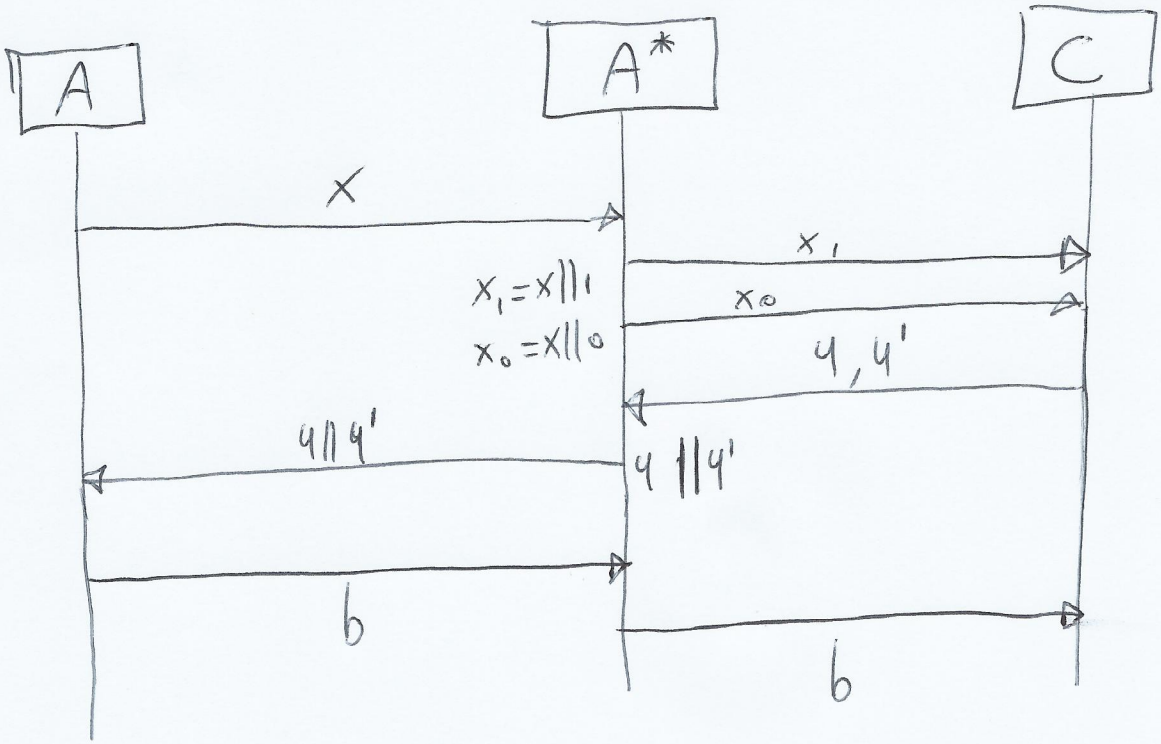
5b

(iii)

$$F'_k(x) = F_k(x||0) || F_k(x||1), \quad x \in \{0,1\}^{n-1}$$

LET'S ASSUME THIS IS NOT A PRG.

SO IT HAS TO EXIST A PPT ATTACKER A ABLE TO BREAK THE SECURITY OF F'_k.



A CAN DISTINGUISH BETWEEN F'_k AND A TRUE RANDOM FUNCTION

$R_{FUNCTIONS}(n-1, 2n)$.

A QUERIES WITH x, THEN A^* FORWARDS $x_1 = x||1$ AND $x_0 = x||0$.

C RETURNS BACK y AND y', AND THEN A^* RETURNS $y||y'$.

A^* FORWARDS THIS VALUE TO A, THAT CAN DISTINGUISH BETWEEN F'_k AND $R_{FUNCTIONS}$.

SO A^* JUST RETURNS BACK THE OUTPUT b.