Take-home midterm assessment

Fady Youssef

1) PRF $\rightarrow F_k : \{0,1\}^n \mapsto \{0,1\}^l$

$\Rightarrow F_k : 2^n \mapsto 2^l$

$\Rightarrow F_k$: domain $\mapsto$ codomain

where $l \leq n$

In a PRF, the set of possible inputs (domain) is smaller than or equal to the set of possible outputs (codomain). The domain inputs bit strings of length n (size 2^n) that map to the codomain which outputs bit strings of length l (size 2^l). Since the $l \leq n$ this could mean different inputs, may map to the same output.

Given an unconstrained distinguisher, an adversary can observe patterns of outputs or eventually reach all outputs which can be mapped back by the adversary. This mapping from outputs back to inputs by the adversary will allow them to distinguish the PRF from a truly random random function because the PRF would be predictable after being mapped while a random would continue to produce unpredictable outputs.

2) $F: \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^l$

$\Rightarrow F: 2^n \times 2^n \mapsto 2^l$

$\Rightarrow F: 2^{2n} \mapsto 2^l$

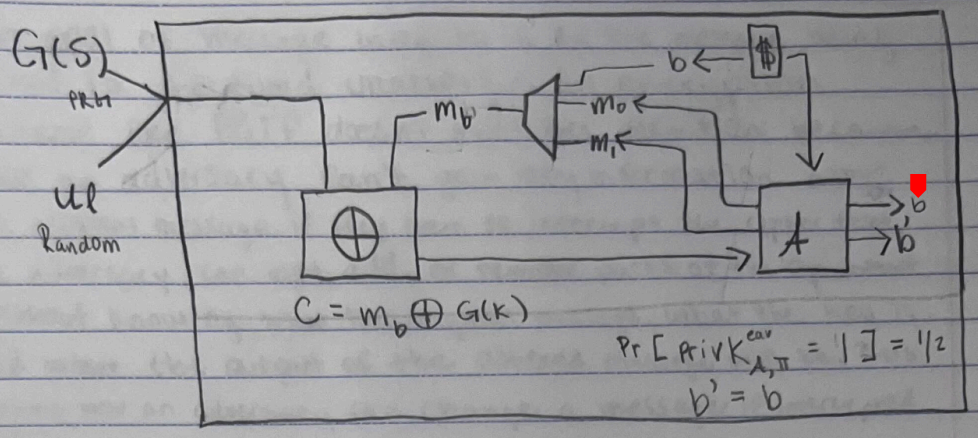
$N_{total} = |C|^{|D|} \Rightarrow (2^l)^{2^{2n}} = \boxed{2^{l \cdot 2^{2n}}}$ ← All possible mappings

2^n possible inputs
2^n possible keys
2^l possible outputs

Since there are 2^n possible inputs and 2^n possible keys, the table would have 2^{2n} input pairs which each map to an output of strings length l.

With a table of 2^{2n} input pairs, it would grow very rapidly in size due to the exponent. This would cause calculating, mapping, and storing infeasible for humans as in computationally bound experiments and protocols, we are often limited by things like lack of resources, time, power, effeciency, etc., which is why we use an oracle. The oracle allows us to negate limitations like time and power, allowing us to use the function without the need of having it.

3)



4) $|Pr[D(G(s)) = 1] - Pr[D(u_l) = 1]| \leq negl(n)$

$|Pr[EAV^{KPA(m)}_{A,\Pi}] - Pr[EAV^{KPA(m)}_{A,\tilde{\Pi}}]| = \alpha$

$Pr[EAV^{KPA}_{A,\tilde{\Pi}} = 1] = 1/2$

$\alpha \leq negl(n)$

$|Pr[EAV^{KPA(m)}_{A,\Pi} = 1] = \frac{1}{2} + \alpha$

$|\frac{1}{2} + \alpha - \frac{1}{2}| = \alpha$

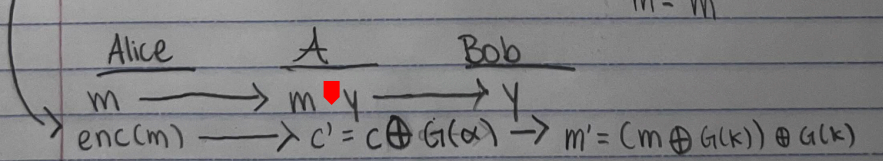
The box diagram shows that for the adversary to break the POTP scheme, they would need a way to distinguish between a deterministic PRF and a truly random function. The probabilitys show the adversarys advantage of breaking the scheme are negligible confirming the security based on the assumed PRF.

5) The goal of message integrity is for the message being sent is received unaltered. An encryption scheme like POTP doesn't meet this definition because while an adversary can't gain any information about the original message if they were to intercept the cipher text, the adversary can edit, add, or remove parts of the ciphertext without knowing what the original message, what the key is, and what the output of the altered message will be. This shows how an adversary can change a message if intercepted during transmission, without the adversary violating security of the POTP scheme. (Adversary can also use own cipher to alter text).

enc: $C = m \oplus G(k)$

dec: $m' = C \oplus G(k)$

$m = m'$



midterm
assessment

PRF $\rightarrow F_k : \{0,1\}^n \mapsto \{0,1\}^l$

$\Rightarrow F_k : 2^n \mapsto 2^l$

$\Rightarrow F_k$: domain $\mapsto$ codomain

where $l \leq n$

In a PRF, the set of possible inputs (domain) is smaller than or equal to the set of possible outputs (codomain). The domain inputs bit strings of length n (size 2^n) that map to the codomain which outputs bit strings of length l (size 2^l). Since the $l \leq n$ this could mean different inputs, may map to the same output.

Given an unconstrained distinguisher, an adversary can observe patterns of outputs or eventually reach all outputs which can be mapped back by the adversary. This mapping from outputs back to inputs by the adversary will allow them to distinguish the PRF from a truly random random function because the PRF would be predictable after being mapped while a random would continue to produce unpredictable outputs.

2) $F: \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^l$

$\Rightarrow F: 2^n \times 2^n \mapsto 2^l$

$\Rightarrow F: 2^{2n} \mapsto 2^l$

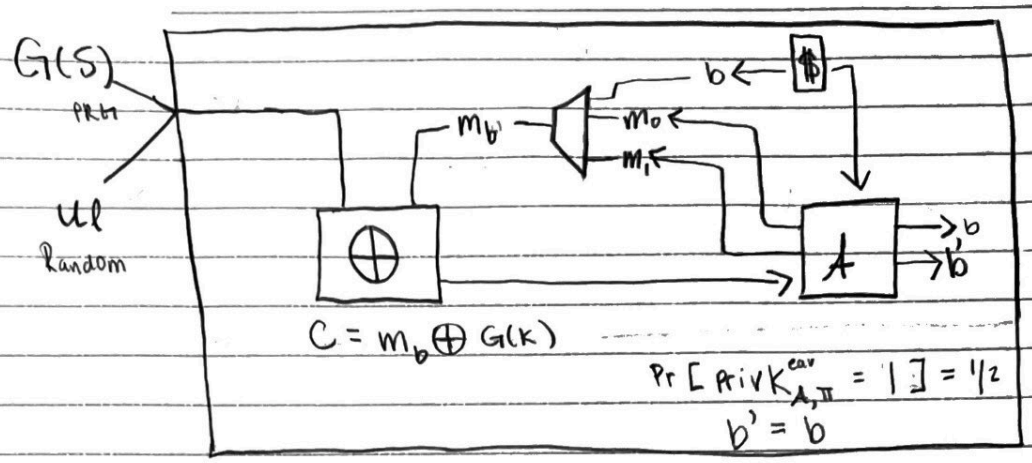
$N_{total} = |C|^{|D|} \Rightarrow (2^l)^{2^{2n}} = \boxed{2^{l \cdot 2^{2n}}}$ ← All possible mappings

2^n possible inputs
2^n possible keys
2^l possible outputs

Since there are 2^n possible inputs and 2^n possible keys, the table would have 2^{2n} input pairs which each map to an output of strings length l.

With a table of 2^{2n} input pairs, it would grow very rapidly in size due to the exponent. This would cause calculating, mapping, and storing infeasible for humans as in computationally bound experiments and protocols, we are often limited by things like lack of resources, time, power, effeciency, etc., which is why we use an oracle. The oracle allows us to negate limitations like time and power, allowing us to use the function without the need of having it.

3



4) $|Pr[D(G(s)) = 1] - Pr[D(U_l) = 1]| \leq negl(n)$

$|Pr[EAV^{KPA(n)}_{A,\Pi}] - Pr[EAV^{KPA(n)}_{A,\tilde{\Pi}}]| = \alpha$

$Pr[EAV^{KPA}_{A,\tilde{\Pi}} = 1] = 1/2$

$\alpha \leq negl(n)$

$|Pr[EAV^{KPA(n)}_{A,\Pi} = 1] = \frac{1}{2} + \alpha$

$|\frac{1}{2} + \alpha - \frac{1}{2}| = \alpha$

The box diagram shows that for the adversary to break the POTP scheme, they would need a way to distinguish between a deterministic PRF and a truly random function. The probabilitys show the adversarys advantage of breaking the scheme are negligible confirming the security based on the assumed PRF.

5) The goal of message integrity is for the message being sent is received unaltered. An encryption scheme like POTP doesn't meet this definition because while an adversary can't gain any information about the original message if they were to intercept the cipher text, the adversary can edit, add, or remove parts of the ciphertext without knowing what the original message, what the key is, and what the output of the altered message will be. This shows how an adversary can change a message if intercepted during transmission, without the adversary violating security of the POTP scheme. (Adversary can also use own cipher to alter text).

enc: $c = m \oplus G(k)$

dec: $m' = c \oplus G(k)$

$m = m'$