CSL759: Cryptography and Computer Security

Ragesh Jaiswal

CSE, IIT Delhi

Minor-1 Exam

Problem 1

- Let $AES: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ be a (t, q, ϵ)-secure PRF. Consider the function family $F: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ defined as $F_K(M) = AES_M(K)$. Is F a secure PRF? Discuss.
- Is F a secure PRF?

Problem 1

- Let $AES: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ be a (t, q, ϵ)-secure PRF. Consider the function family $F: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ defined as $F_K(M) = AES_M(K)$. Is F a secure PRF? Discuss.
- Is F a secure PRF?
  - No.
- How do you show this?

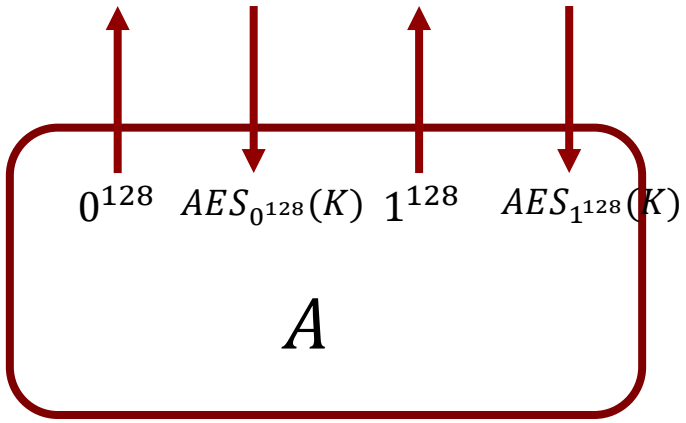
Problem 1

- Let $AES: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ be a (t, q, ϵ)-secure PRF. Consider the function family $F: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ defined as $F_K(M) = AES_M(K)$. Is F a secure PRF? Discuss.
- Is F a secure PRF?
  - No.
- How do you show this?
  - Adversary A
    - Query message 0^{128} and get back C as reply.
    - Query message 1^{128} and get back C' as reply.
    - If $(AES_{0^{128}}^{-1}(C) = AES_{1^{128}}^{-1}(C'))$ then output 1 else output 0.

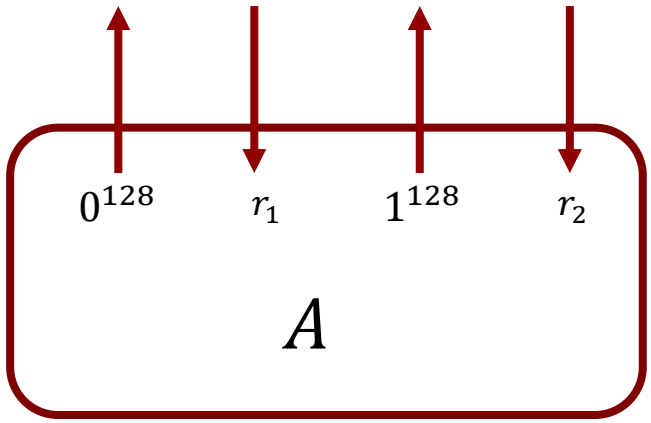
Problem 1

- Adversary A
  - Query message 0^{128} and get back C as reply.
  - Query message 1^{128} and get back C' as reply.
  - If $(AES_{0^{128}}^{-1}(C) = AES_{1^{128}}^{-1}(C'))$ then output 1 else output 0.

$Real_{A,F}$



$Random_A$

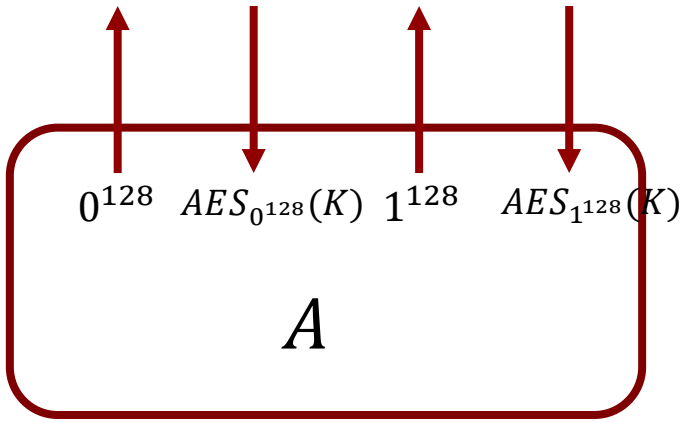


$\Pr[Real_{A,F} = 1] = ?$

Problem 1

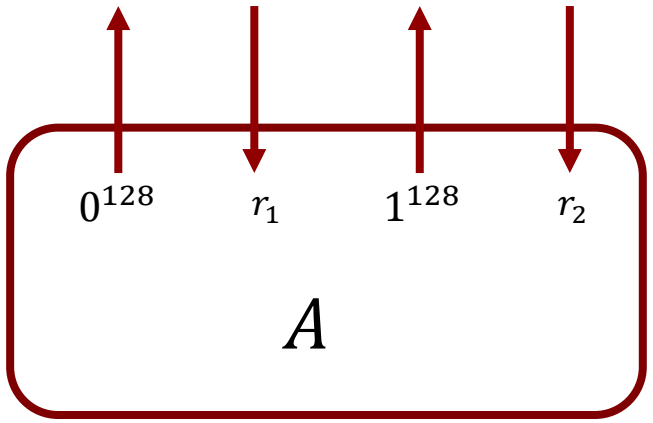
- Adversary A
  - Query message 0^{128} and get back C as reply.
  - Query message 1^{128} and get back C' as reply.
  - If $(AES^{-1}_{0^{128}}(C) = AES^{-1}_{1^{128}}(C'))$ then ourput 1 else output 0.

$Real_{A,F}$



$\Pr[Real_{A,F} = 1] = 1$

$Random_A$

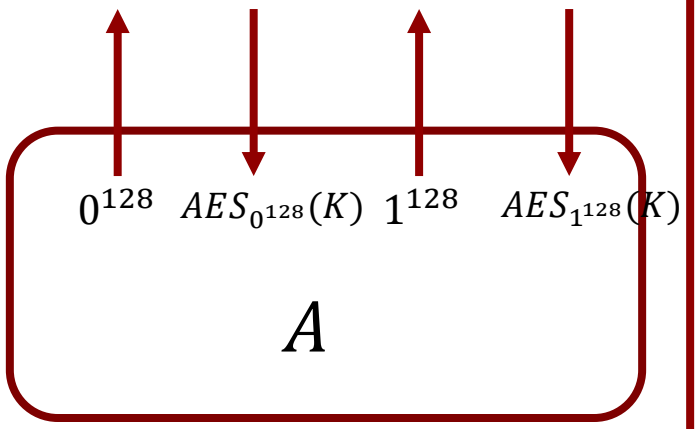


$\Pr[Random_A = 1] = ?$

Problem 1

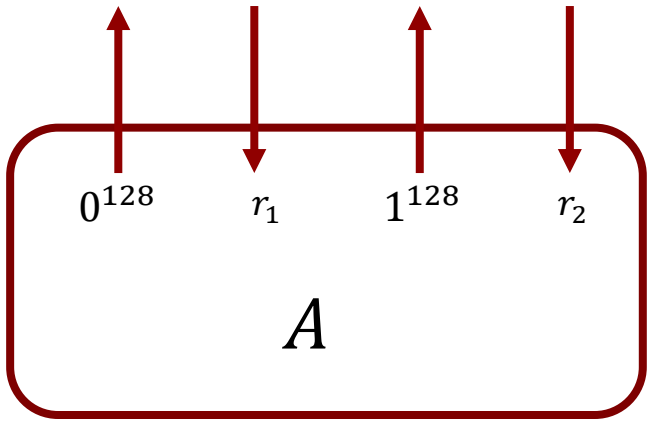
- Adversary A
  - Query message 0^{128} and get back C as reply.
  - Query message 1^{128} and get back C' as reply.
  - If $(AES_{0^{128}}^{-1}(C) = AES_{1^{128}}^{-1}(C'))$ then ourput 1 else output 0.

$Real_{A,F}$



$\Pr[Real_{A,F} = 1] = 1$

$Random_A$



$\Pr[Random_A = 1] = \frac{1}{2^{128}}$

Problem 1

- Adversary A
  - Query message 0^{128} and get back C as reply.
  - Query message 1^{128} and get back C' as reply.
  - If $(AES_{0^{128}}^{-1}(C) = AES_{1^{128}}^{-1}(C'))$ then ourput 1 else output 0.

- $Adv_{PRF}(A, F) = 1 - \frac{1}{2^{128}}$.

Problem 2

- Let $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a (t, q, ϵ)-secure PRF. Consider the function $G: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$ defined as follows:

$$G_K(M) = F_K(M) || F_K(F_K(M))$$

  where $||$ means concatenation. Is G a secure PRF? Discuss.

- Is G a secure PRF?

Problem 2

- Let $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a (t, q, ϵ)-secure PRF. Consider the function $G: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$ defined as follows:

$$G_K(M) = F_K(M) || F_K(F_K(M))$$

  where $||$ means concatenation. Is G a secure PRF? Discuss.

- Is G a secure PRF?
  - Yes.
- How do we show this?

Problem 2

- Let $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a (t, q, ϵ)-secure PRF. Consider the function $G: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$ defined as follows:

$$G_K(M) = F_K(M) || F_K(F_K(M))$$

  where $||$ means concatenation. Is G a secure PRF? Discuss.

- Is G a secure PRF?
  - Yes.
- How do we show this?
  - Theorem: Let A be a PRF adversary for G that runs in time t' and makes q' queries, then there exists a PRF adversary for F that makes $2q'$ queries and runs in time $t' + \theta(qn)$ such that

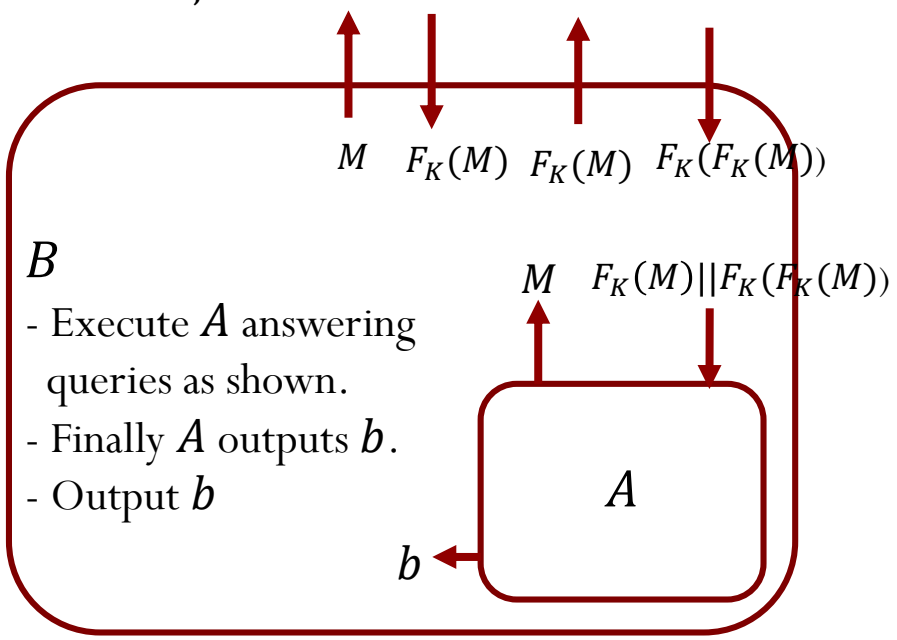
$$Adv_{PRF}(A, G) \leq Adv_{PRF}(B, F)$$

Problem 2

- Theorem: Let A be a PRF adversary for G that runs in time t' and makes q' queries, then there exists a PRF adversary for F that makes $2q'$ queries and runs in time $t' + \theta(qn)$ such that

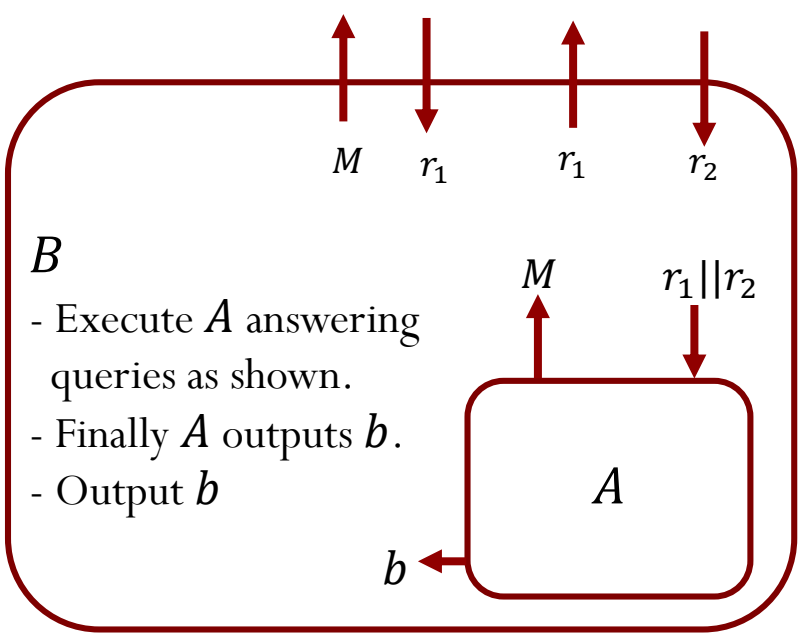
$$Adv_{PRF}(A, G) \leq Adv_{PRF}(B, F)$$

$Real_{B,F}$



$\Pr[Real_{B,F} = 1] = ?$

$Random_B$

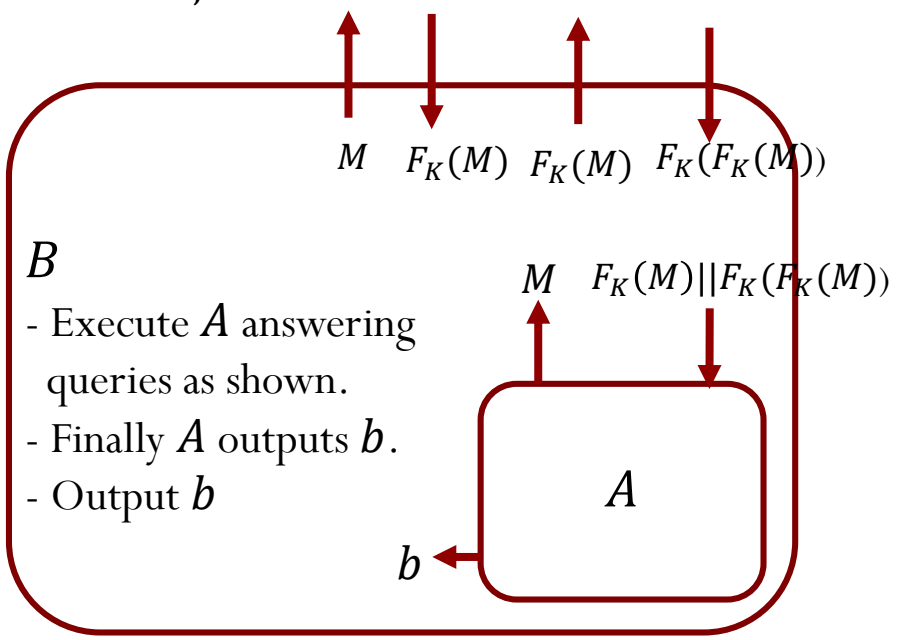


Problem 2

- Theorem: Let A be a PRF adversary for G that runs in time t' and makes q' queries, then there exists a PRF adversary for F that makes $2q'$ queries and runs in time $t' + \theta(qn)$ such that

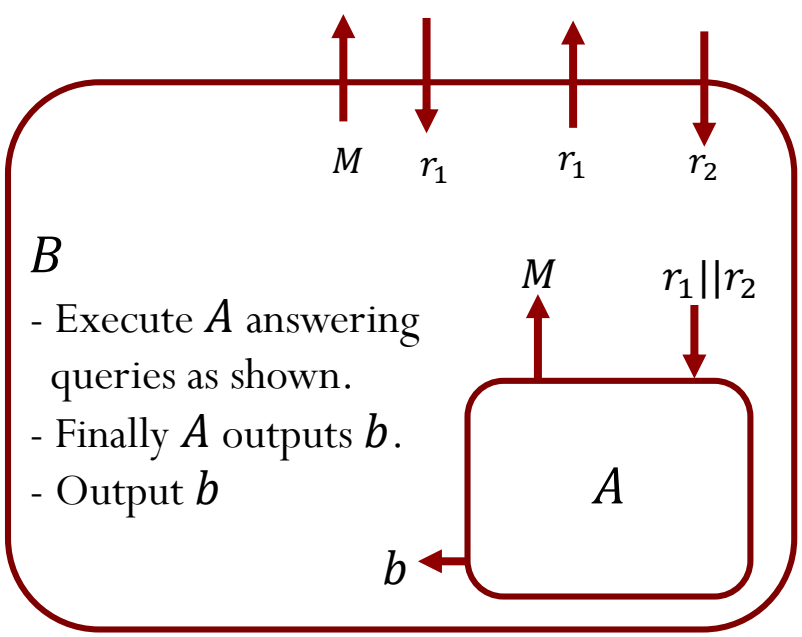
$$Adv_{PRF}(A, G) \leq Adv_{PRF}(B, F)$$

$Real_{B,F}$



$\Pr[Real_{B,F} = 1] = \Pr[Real_{A,G} = 1]$

$Random_B$

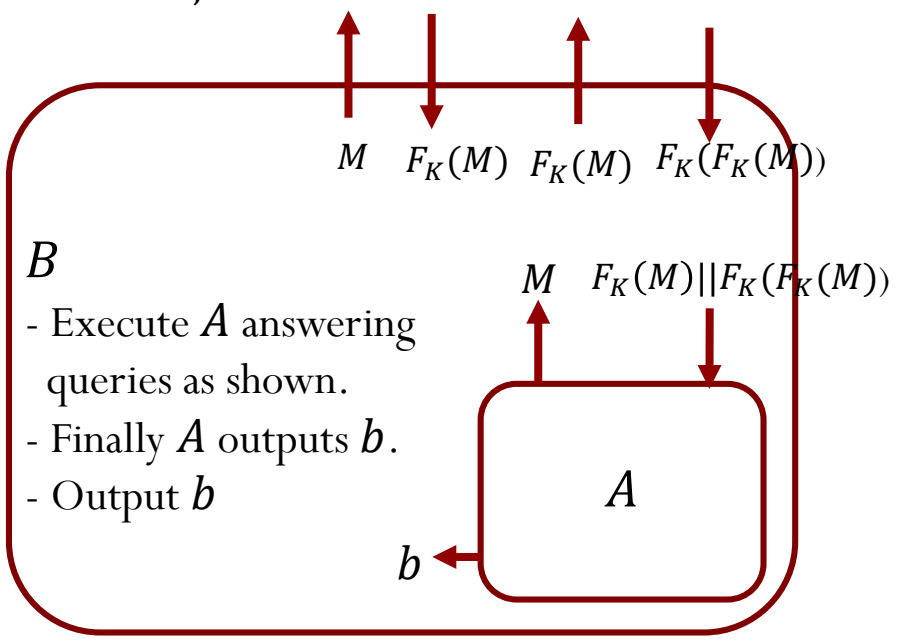


Problem 2

- Theorem: Let A be a PRF adversary for G that runs in time t' and makes q' queries, then there exists a PRF adversary for F that makes $2q'$ queries and runs in time $t' + \theta(qn)$ such that

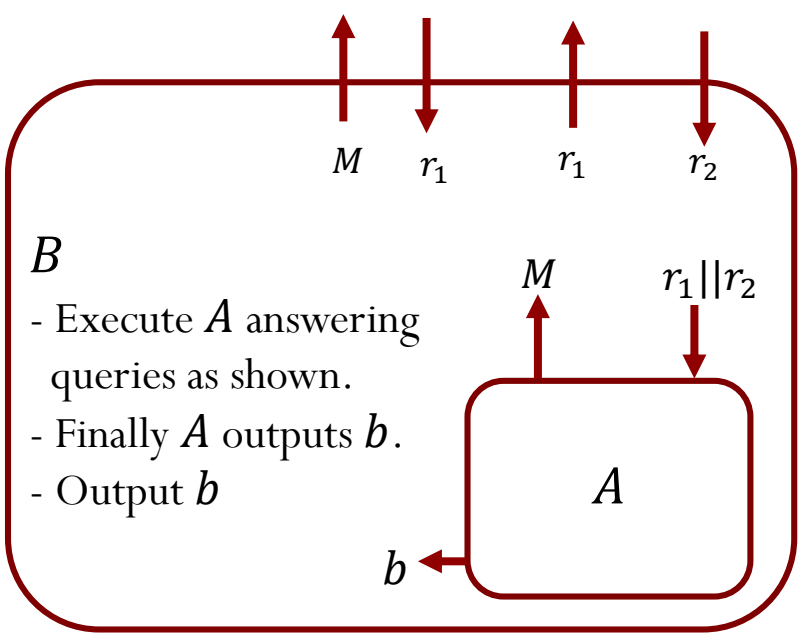
$$Adv_{PRF}(A, G) \leq Adv_{PRF}(B, F)$$

$Real_{B,F}$



$\Pr[Real_{B,F} = 1] = \Pr[Real_{A,G} = 1]$

$Random_B$



$\Pr[Random_B = 1] =? \Pr[Random_A = 1]$

Problem 2

- Let $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a (t, q, ϵ)-secure PRF. Consider the function $G: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$ defined as follows:

$$G_K(M) = F_K(M) || F_K(F_K(M))$$

  where $||$ means concatenation. Is G a secure PRF? Discuss.

- Is G a secure PRF?
  - No. Consider the following adversary:
  - A
    - Make a query 0^{128} and get back $V_1 || V_2$.
    - Make a query V_1 and get back $V_1' || V_2'$.
    - If $(V_2 = V_1')$ then output 1 else output 0.

Problem 2

- A
  - Make a query 0^{128} and get back $V_1||V_2$.
  - Make a query V_1 and get back $V_1'||V_2'$.
  - If $(V_2 = V_1')$ then output 1 else output 0.

- What is $\Pr[Real_{A,G} = 1] = ?$

Problem 2

- A
  - Make a query 0^{128} and get back $V_1||V_2$.
  - Make a query V_1 and get back $V_1'||V_2'$.
  - If $(V_2 = V_1')$ then output 1 else output 0.

- What is $\Pr[Real_{A,G} = 1] = 1$.
- What is $\Pr[Random_A = 1] =?$

Problem 2

- A
  - Make a query 0^{128} and get back $V_1||V_2$.
  - Make a query V_1 and get back $V_1'||V_2'$.
  - If $(V_2 = V_1')$ then output 1 else output 0.

- What is $\Pr[Real_{A,G} = 1] = 1$.
- What is $\Pr[Random_A = 1] = \frac{1}{2^n}$.
- So $Adv_{PRF}(A, G) = 1 - \frac{1}{2^n}$.
- Verdict: G is insecure PRF.

Problem 2

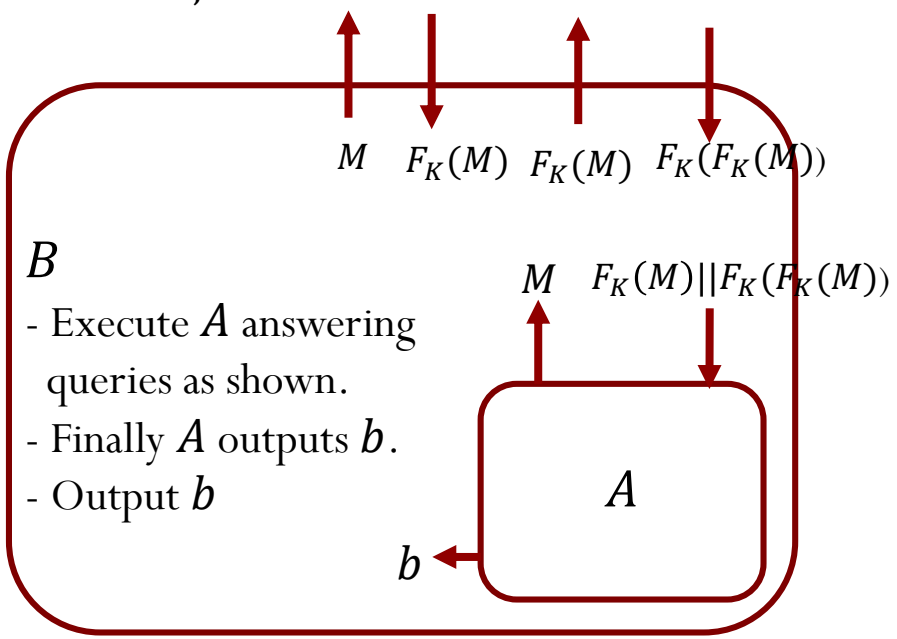
- So where is the fallacy?

Problem 2

- Theorem: Let A be a PRF adversary for G that runs in time t' and makes q' queries, then there exists a PRF adversary for F that makes $2q'$ queries and runs in time $t' + \theta(qn)$ such that

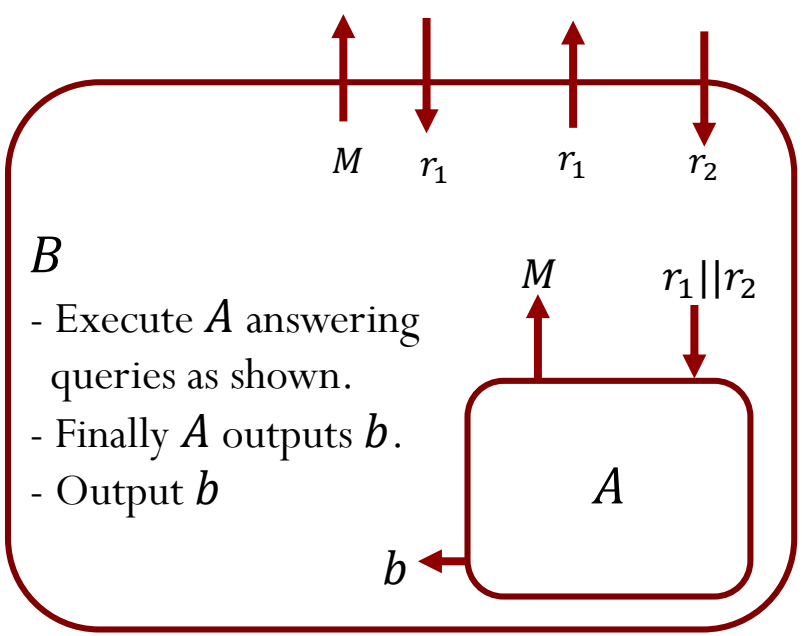
$$Adv_{PRF}(A, G) \leq Adv_{PRF}(B, F)$$

$Real_{B,F}$



$\Pr[Real_{B,F} = 1] = \Pr[Real_{A,G} = 1]$

$Random_B$



$\Pr[Random_B = 1] = \Pr[Random_A = 1]$

Problem 2

- Let $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a (t, q, ϵ)-secure PRF. Consider the function $G: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$ defined as follows:

$$G_K(M) = F_K(M) || F_K(F_K(M))$$

where $||$ means concatenation. Is G a secure PRF? Discuss.

- Is G a secure PRF?
  - Yes.
- How do we show this?
  - Theorem: Let A be a PRF adversary for G that runs in time t' and makes q' queries, then there exists a PRF adversary for F that makes $2q'$ queries and runs in time $t' + \theta(qn)$ such that

$$Adv_{PRF}(A, G) \leq Adv_{PRF}(B, F)$$

End