Proofs by Reduction

Introduction to Cryptology

2/24/15

Proofs by Reduction

Statement: "If PSEUDORANDOM GENERATOR is secure then ENCRYPTION SCHEME is secure."

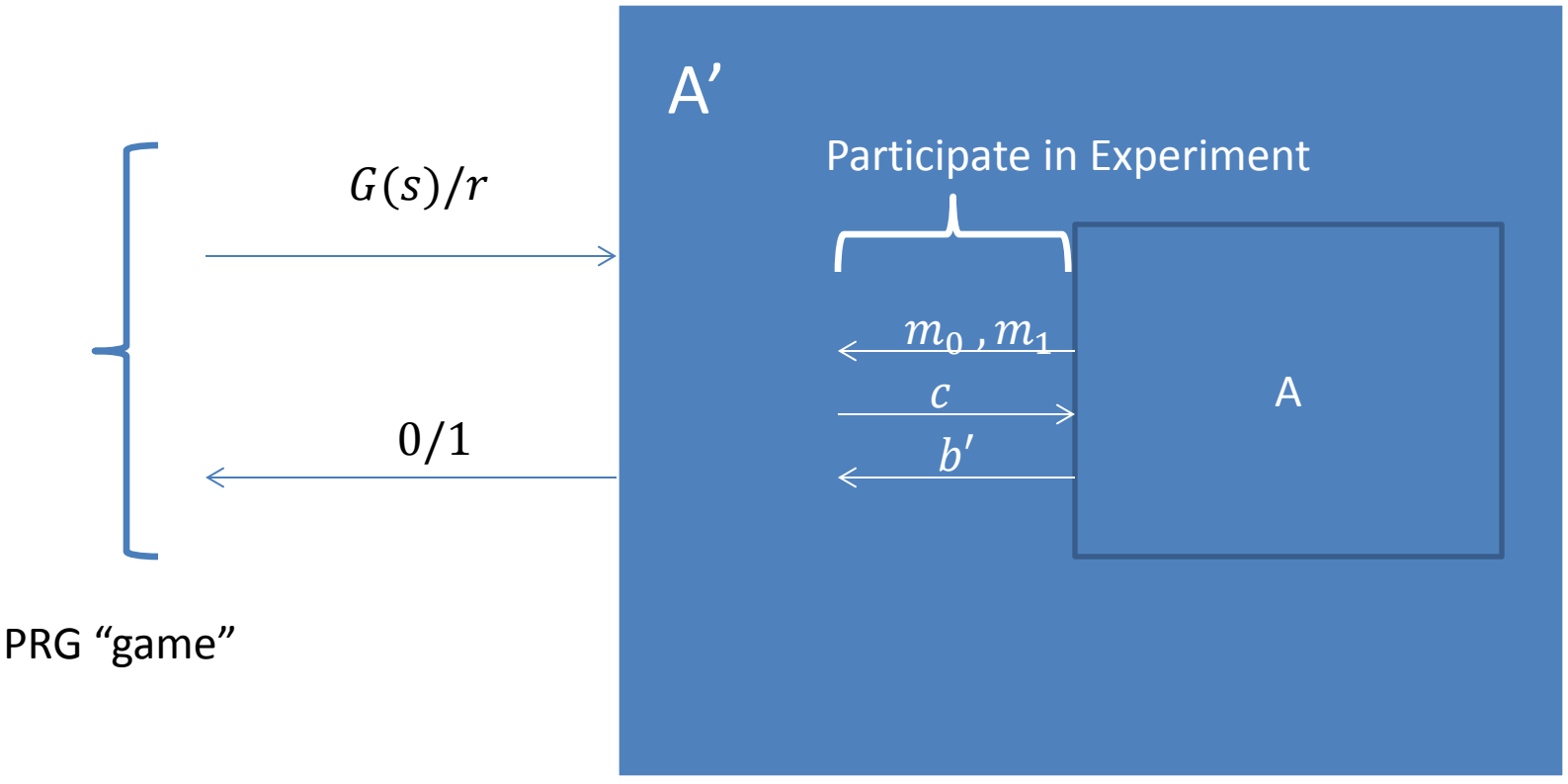
Proof by contrapositive:

Assume ENCRYPTION is not secure.

Then there exists adversary A participating in security experiment such that A breaks security.

We use A to construct A' who breaks PSEUDORANDOM GENERATOR.

Proofs by Reduction

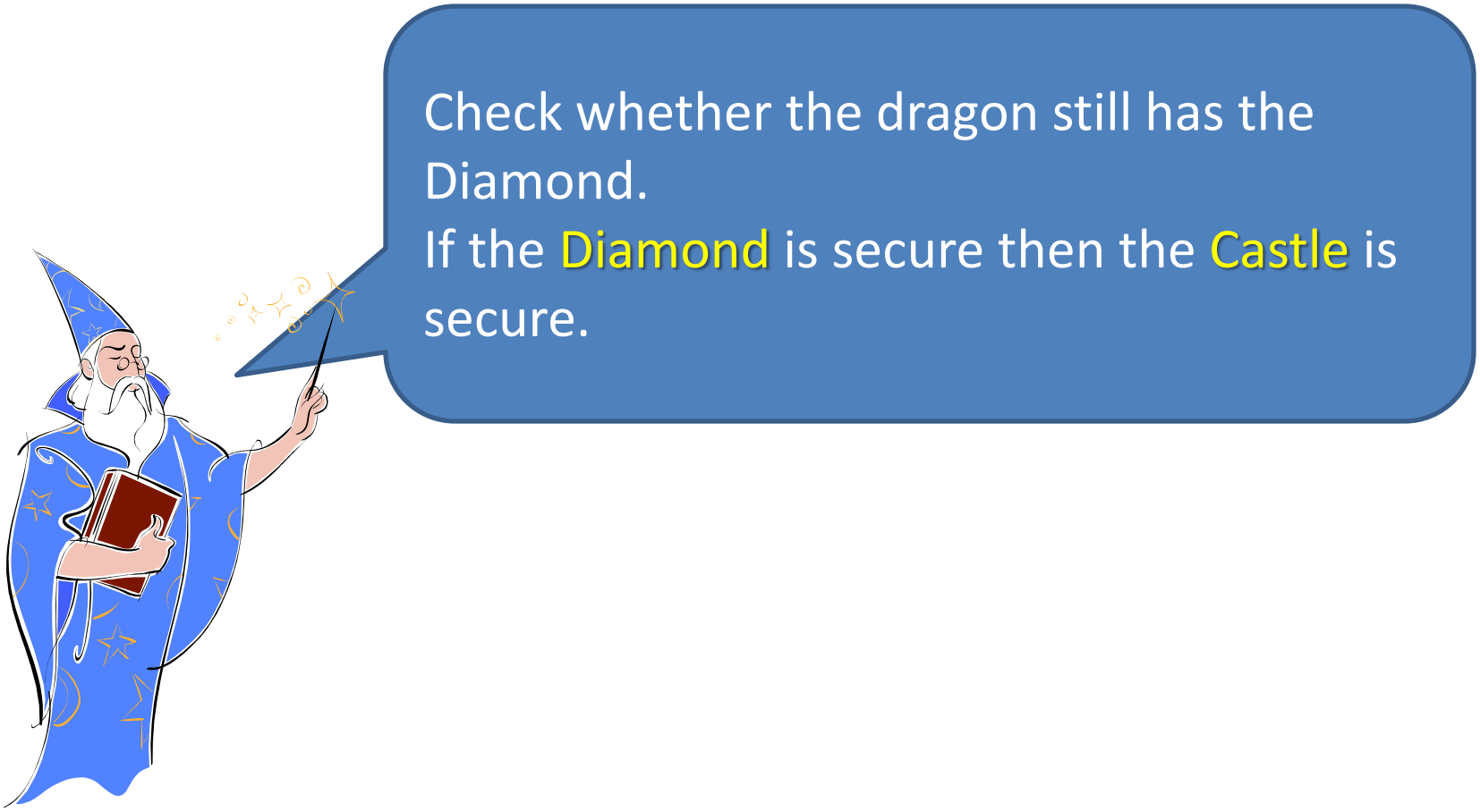


A Non-CS example

Proofs by Reduction

My brother's castle is under attack. I am worried that the walls have been breached.

Proofs by Reduction

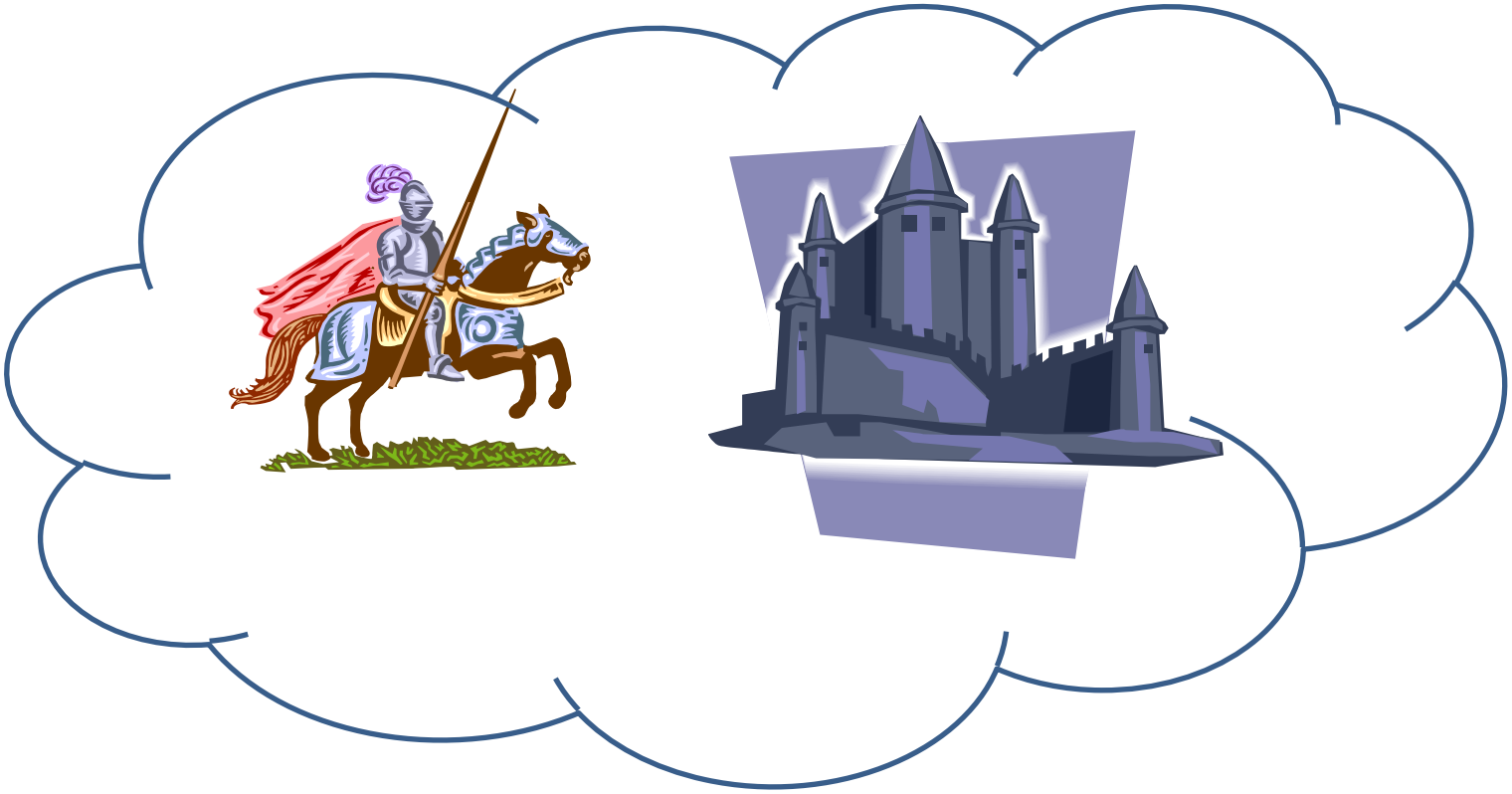


Proofs by Reduction

How do you know?

Proofs by Reduction

Assume the Castle is insecure



Proofs by Reduction

Then the knight has breached the walls and taken the treasure chest

Proofs by Reduction

Then the troll has tricked the knight to hand over the treasure chest

I am a knight of the round table.
I will help you open the chest.

Oh ok. Here you go.

Proofs by Reduction

Then the troll has tricked the knight to hand over the treasure chest

I am a knight of the round table.
I will help you open the chest.

Oh ok. Here you go.

Proofs by Reduction

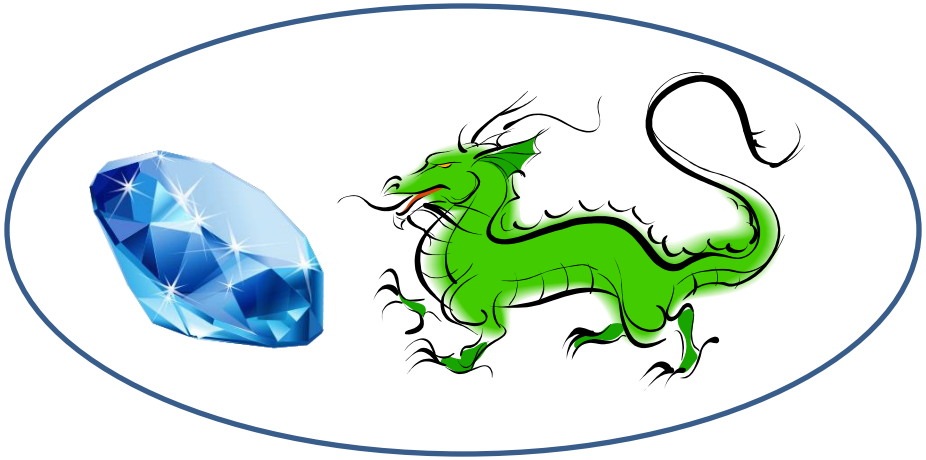
Then the troll has used his key to open treasure chest, has retrieved the gold and has given it to the dragon in exchange for the diamond.

Proofs by Reduction

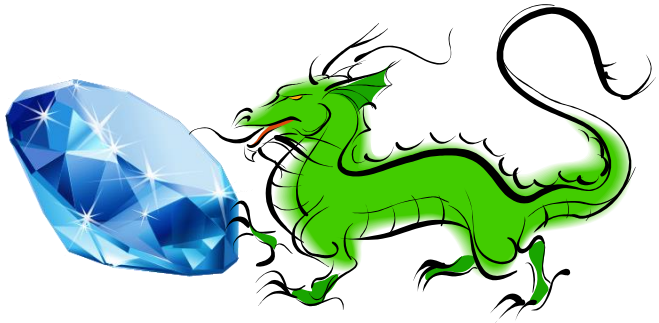
Then the troll has used his key to open treasure chest, has retrieved the gold and has given it to the dragon in exchange for the diamond.

Proofs by Reduction

Now I see. Oh good the castle must be secure since the dragon still has the diamond.



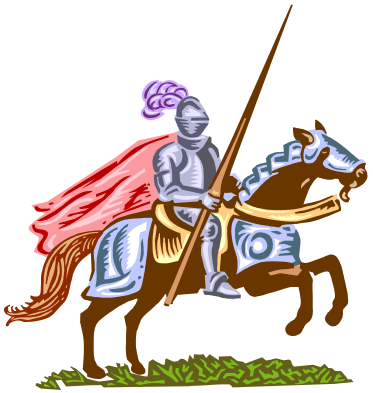
Proofs by Reduction



Getting past the dragon to get the diamond = BREAKING PRG

Breaching the castle walls to get the treasure chest = BREAKING ENCRYPTION

Proofs by Reduction



Knight = ADVERSARY A

BREAKING ENCRYPTION

Troll = ADVERSARY A’

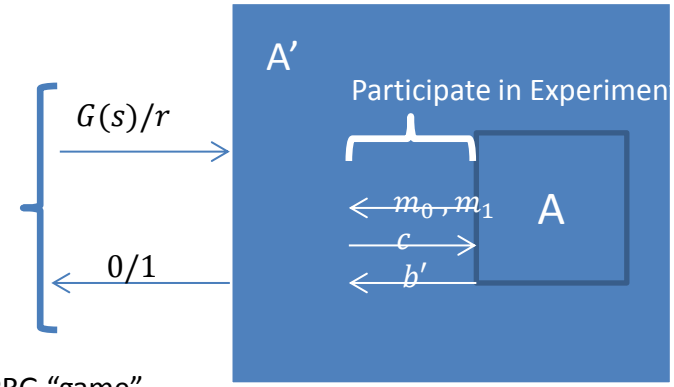
BREAKING PRG

Proofs by Reduction

Troll must

1. Trick  into giving him the chest

2. Uses his  to open the chest and retrieve coins to get the diamond

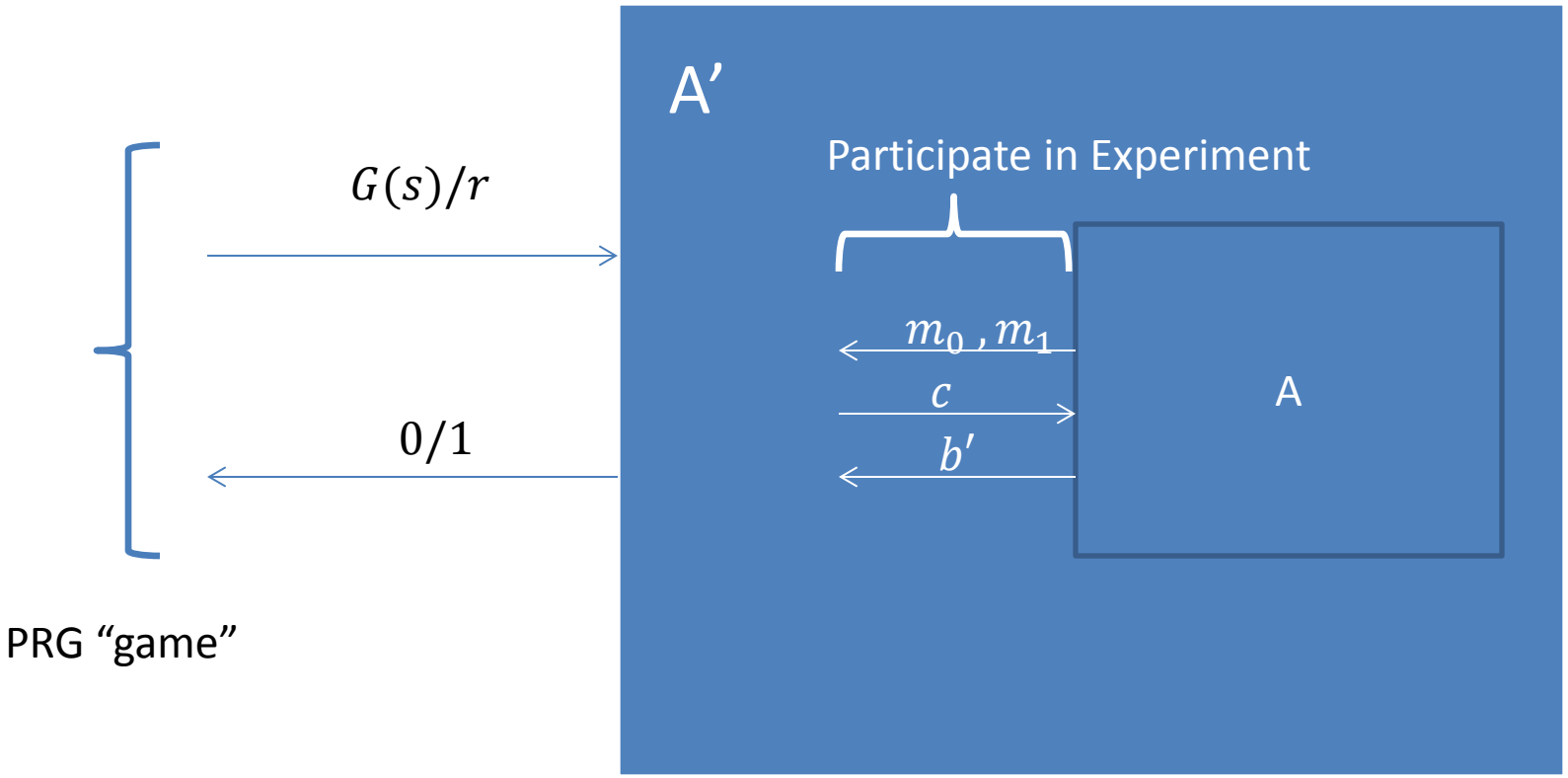


PRG "game"

A' must

1. Interact with A as in the ENCRYPTION security experiment
2. Given A's output b', must transform it to obtain the correct answer $0/1$ and break PRG

Proofs by Reduction—Some Details



- Security parameter n
- A succeeds with probability $\epsilon(n)$
- A' is efficient when A is used as a subroutine
- If A succeeds in "breaking" the instance, A' should succeed with probability is $1/poly(n)$ times A's success probability
- Thus, A' succeeds with non-negligible probability $\epsilon(n)/p(n)$