

# Chosen Ciphertext Security

Kari & Karl

Crypt - 2003

A Good<sup>a</sup> Public Key Cryptosystem

A Good<sup>a</sup>: Practical and Provably Secure against Adaptive Chosen Ciphertext Attacks

# Introduction

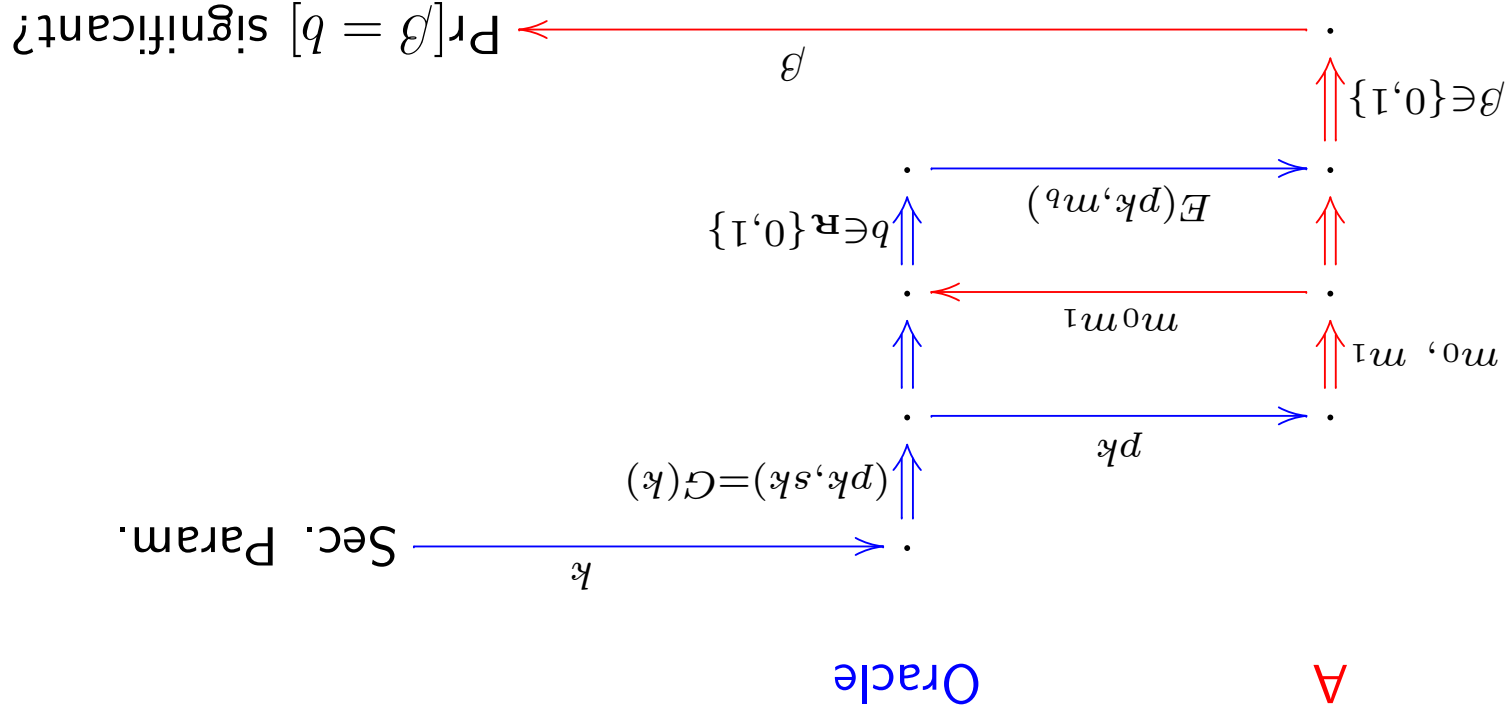
- ◆ Semantic security of public-key cryptosystems
- ◆ Probabilistic cryptosystems
- ◆ Active attacks
  - Provable secure, but impractical systems
  - Practical schemes, but no proofs of security
  - Heuristic methods: OAEP encodes  $m$  in a special way
  - A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, by Ronald Cramer and Victor Shoup, 1998.

# Outline

- ◆ Preliminaries - reminder and new definitions.
  - \* Definitions of Security
  - \* Diffie-Hellman Decision Problem
- ◆ The basic scheme.
- ◆ Security of the scheme
  - \* Outline proof-structure.
- ◆ Summary
- ◆ References

# Preliminaries: Security Definitions

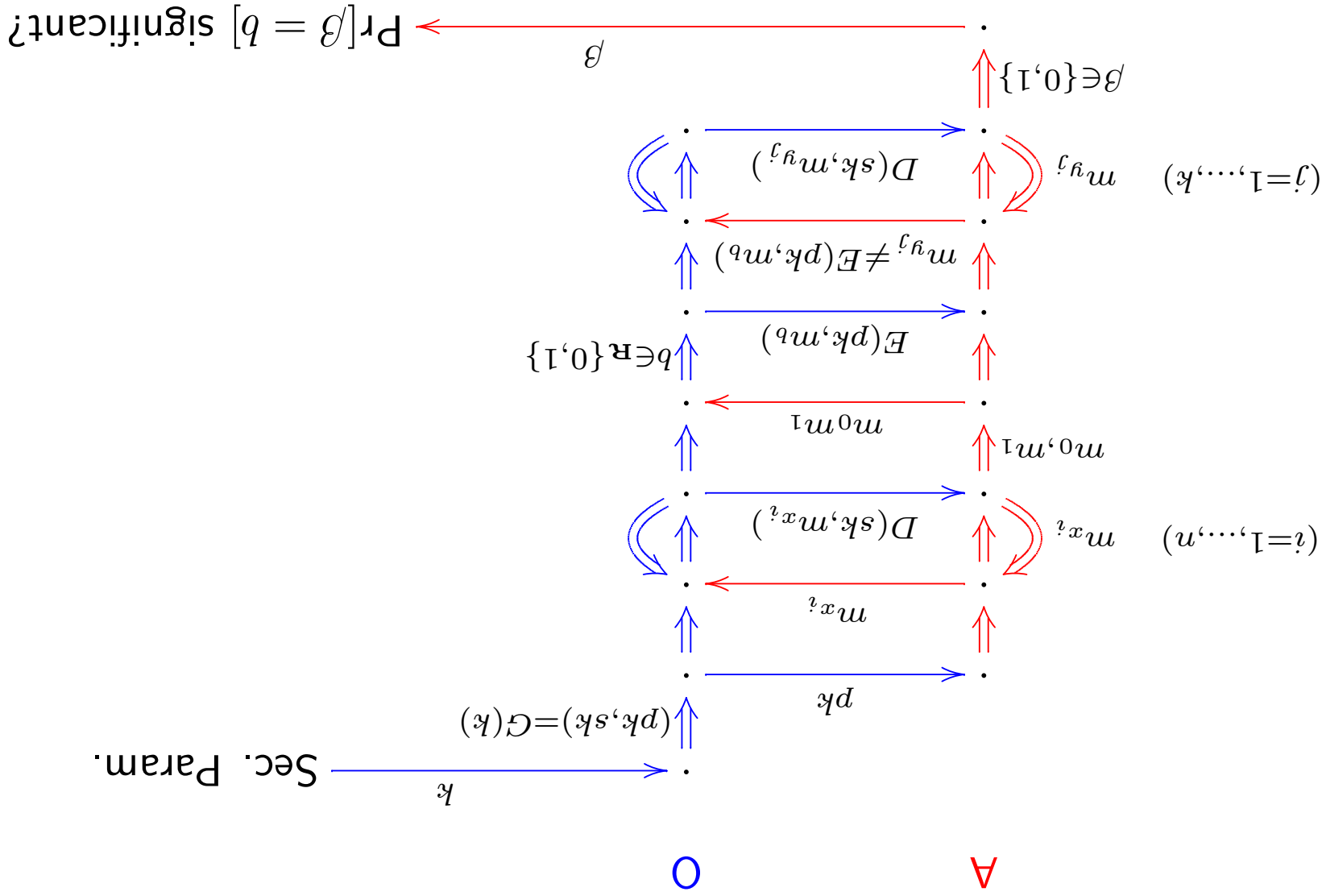
- ◆ Semantic Security: An adversary should not be able to obtain even partial information about an encrypted message.
- ◆ Consider an encryption scheme  $(G, E, D)$ . The SS game is the following:



# Adaptive Chosen Ciphertext Security

- ◆ Semantic security – guess which of  $m_0$  and  $m_1$  was encrypted.
- ◆ Active attacks – use of decryption oracle.
- ◆ Adaptive – decrypt both before and after encryption of  $m_0$  or  $m_1$ .
- ◆ ACC security game.

# ACC Security Game



# Decisional Diffie-Hellman (DDH)

- ◆ Use a slightly different version: Fix a group,  $G$ , of large prime order  $q$ 
  - let  $\mathbf{R}$  be the distribution of random tuples  $(g_1, g_2, u_1, u_2) \in G^4$
  - let  $\mathbf{D}$  be the distribution of tuples  $(g_1, g_2, u_1, u_2) \in G^4$ , where  $g_1, g_2$  are chosen at random, and  $u_1 = g_1^{r_1}, u_2 = g_2^{r_2}$  for some random  $r \in \mathbb{Z}_q$ .

- ◆ An algorithm that solves the DDH is a statistical test that can effectively distinguish  $\mathbf{D}$  from  $\mathbf{R}$ .

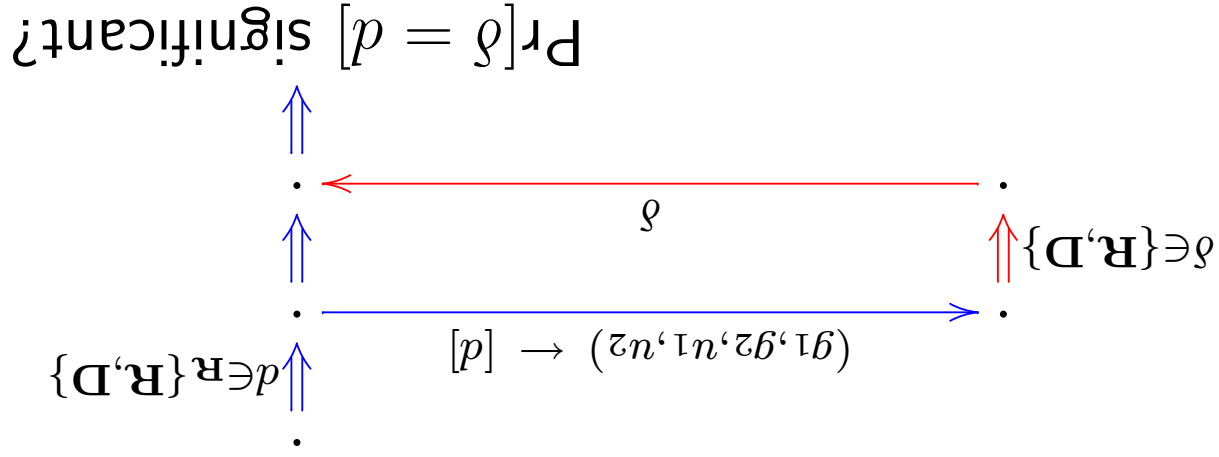
- ◆ DDH is hard in  $G$  if no such algorithm exists.

- ◆ This variant is provably equivalent to the 'standard' DDH.

# DDH - Game

◆ DDH can be thought of as a game:

T
Environment



# Basic Scheme

- ◆ Assume a group  $G$  of large prime order  $q$ .
- ◆ Also assume that any plaintext can be encoded as an element of  $G$ .
- ◆ Finally assume a family of universal one-way hash functions  $\mathcal{H}$ , where each function maps  $G^3$  into  $\mathbb{Z}_q$ .
- ◆ We describe *Key Generation (KeyGen)*, *Encryption (Enc)* and *Decryption (Dec)*.

# Key Generation

- ◆ Select base elements  $g_1, g_2 \in \mathbf{R} G$ , and random numbers  $x_1, x_2, y_1, y_2, z \in \mathbf{R} \mathbb{Z}_q$

- ◆ Now compute elements

$$c = g_1^{x_1} g_2^{x_2} \quad d = g_1^{y_1} g_2^{y_2} \quad h = g_1^z$$

- ◆ Select a hash function at random  $H \in \mathbf{R} \mathcal{N}$ .

- ◆  $\text{KeyGen}(G, \mathcal{N}) = (\mathbf{PK}, \mathbf{SK})$ , where  $\mathbf{PK} = (g_1, g_2, c, d, h, H)$  and  $\mathbf{SK} = (x_1, x_2, y_1, y_2, z)$ .

# Encryption

◆ Recall  $\mathbf{SK} = (x_1, x_2, y_1, y_2, z)$  and  $\mathbf{PK} = (g_1, g_2, c, d, h, H)$

$$c = g_1^{x_1} g_2^{x_2} \quad d = g_1^{y_1} g_2^{y_2} \quad h = g_1^z$$

◆ To encrypt a message  $m \in G$ ,

– Select a number  $r \in \mathbb{R}_{\mathbb{Z}_q}$ .

– Compute

$$u_1 = g_1^r \quad u_2 = g_2^r \quad e = h^r m$$

– then compute

$$\alpha = H(u_1, u_2, e) \quad v = c^r d^{r\alpha}$$

◆  $\mathbf{Enc}(\mathbf{PK}, m) = (u_1, u_2, e, v) = (g_1^r, g_2^r, h^r m, c^r d^{r\alpha})$

# Decryption

◆ Recall  $\mathbf{SK} = (x_1, x_2, y_1, y_2, z)$  and  $\mathbf{PK} = (g_1, g_2, c, d, h, H)$   
 $c = g_1^{x_1} g_2^{x_2}$     $d = g_1^{y_1} g_2^{y_2}$     $h = g_1^z$

$\mathbf{Enc}(\mathbf{PK}, m) = (u_1, u_2, e, v) = (g_1^r, g_2^r, h^r m, c^r d^{r\alpha})$

◆ To decrypt a message  $(u_1, u_2, e, v)$  do the following

– first compute  $\alpha = H(u_1, u_2, e)$

– check if

$$u_1^{x_1 + y_1 \alpha} u_2^{x_2 + y_2 \alpha} = v$$

– if not output **reject** otherwise

– return

$$m = e(u_2^{-1})^{-1}$$

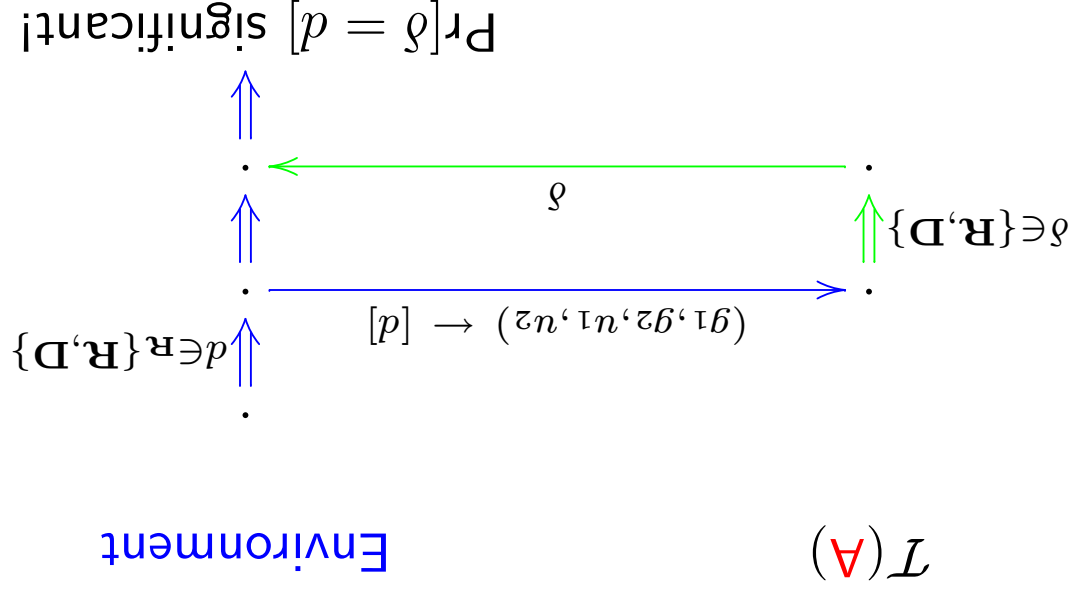
# Security

- ◆ **Theorem 1** *The described cryptosystem is secure against Adaptive Chosen Ciphertext Attacks if the following two conditions are satisfied*
  - $\mathcal{U}$  is a family of universal one-way hash functions.
  - $DDH$  is hard in  $G$

- ◆ **Proof: Standard Technique - Contraposition:** if we have an adversary  $\mathcal{A}$  which attacks the cryptosystem with non-negligible success-probability then we can construct an algorithm that will solve the  $DH$ -test with non-negligible success-probability.
- ◆ Details are more technical so we just outline the structure.

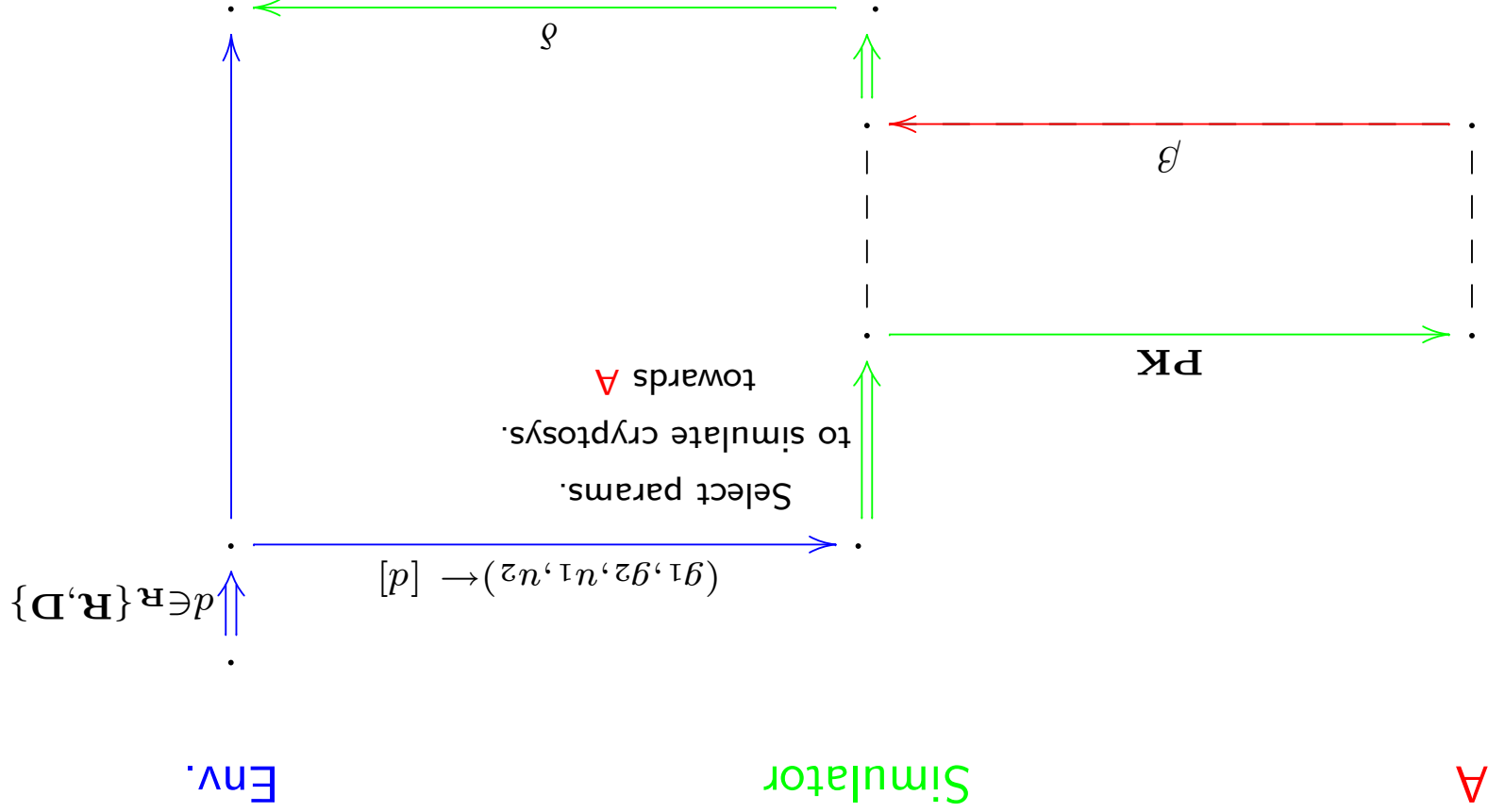
# Construction

- ◆ Assume we have an algorithm  $\mathcal{A}$  for breaking the cryptosystem.
- ◆ We build a fast algorithm  $\mathcal{I}(\mathcal{A})$  that solves DDH.

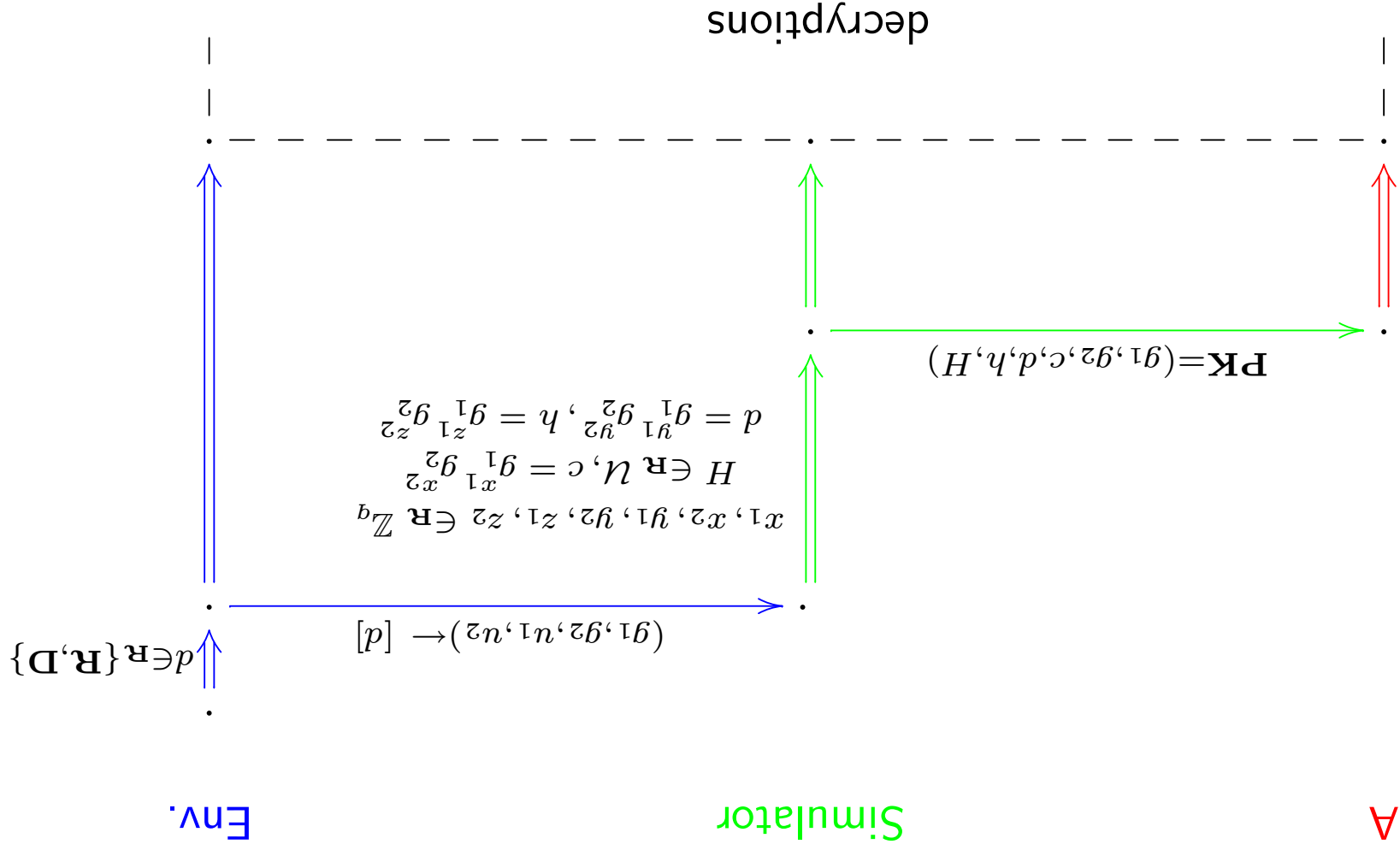


# Overview of $\mathcal{I}(A)$

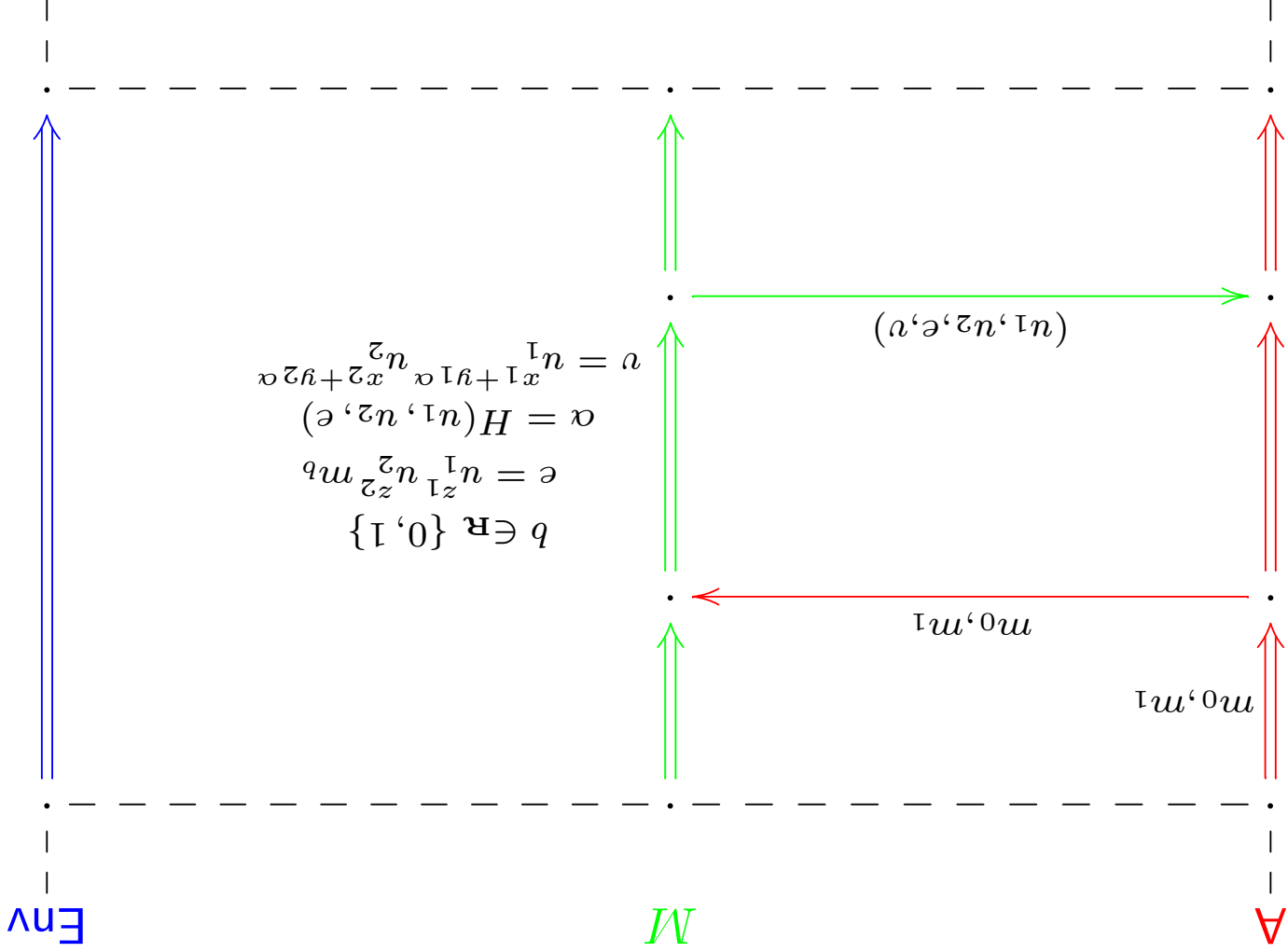
- ◆ Will use a “man in middle” construction



$\mathcal{T}(A) (1/3)$



# $\mathcal{I}(A)$ (ctd. 2/3)





# Correctness

- ◆ The rest of the proof deals with proving the following statements.
- ◆ If  $d = \mathbf{D}$  then the “ $M$ ” component will look like a proper cryptosystem to  $\mathbf{A}$ , and by assumption the probability of  $\mathbf{A}$  guessing  $b$  is  $\frac{1}{2} + K$  with  $K$  non-negligible.
- ◆ If  $d = \mathbf{R}$  then the “ $M$ ” component will essentially look random to  $\mathbf{A}$  (independent of  $b$ ) and we have that the probability of  $\mathbf{A}$  guessing  $b$  is  $\frac{1}{2} + \epsilon$  for a negligible  $\epsilon$ .
- ◆ This means that output of our algorithm (which checks  $\beta = b$ ) is a statistical test for distinguishing  $\mathbf{D}$  and  $\mathbf{R}$ .

# Summary

- ◆ We've looked at a practical cryptosystem.
  - encryption and decryption requires only a few computations
- ◆ We considered Adaptive Chosen Ciphertext Security which models a strong class of attacks.
- ◆ The cryptosystem is provably secure against ACC attacks in any group where DH is hard.

## References

- ◆ Can be found on Victor Shoup's homepage  
<http://shoup.net/papers>
- ◆ Main reference: **A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack**, Ronald Cramer and Victor Shoup, in Proc. Crypto'98.
- ◆ An updated, more formal paper: **Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack**, Ronald Cramer and Victor Shoup, 2003, to appear SIAM Journal of Computing.