

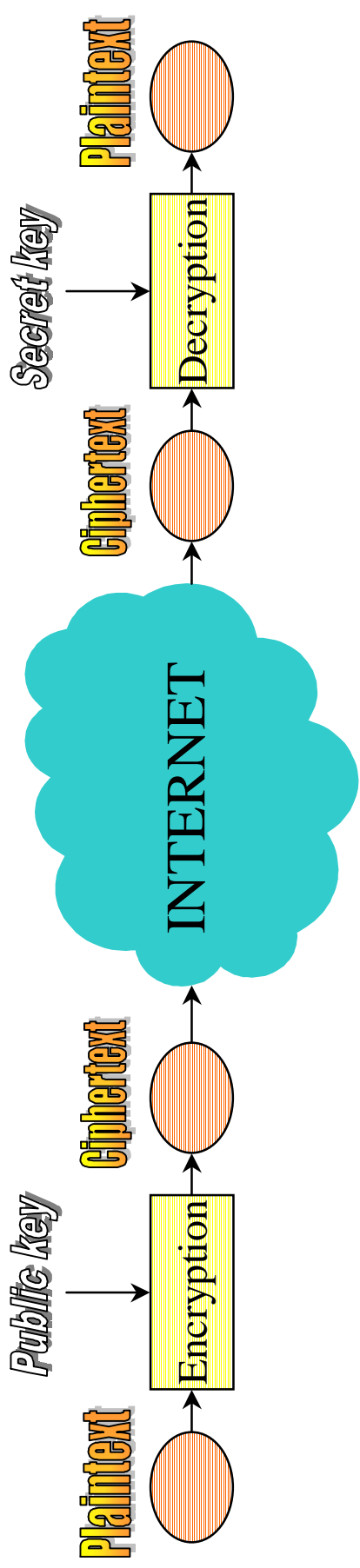
# **DHIES: An Encryption Scheme based on the Diffie-Hellman problem**

**Michel Abdalla (UC San Diego)**

**Mihir Bellare (UC San Diego)**

**Phillip Rogaway (UC Davis)**

# Public-key Encryption



# Diffie-Hellman/Discrete Log based encryption

Why?

- **Low cost:** elliptic curve groups of relatively small size suffice.
- **Alternative to RSA.**

# Diffie-Hellman Key Exchange Protocol

Let  $g$  be a generator for a group  $G = \{g^0, g^1, \dots, g^{|G|-1}\}$

Alice

$$sk_A \xleftarrow{R} \{0, \dots, |G|-1\}$$

$$pk_A \leftarrow g^{sk_A}$$

$$\xrightarrow{pk_A}$$

$$\xleftarrow{pk_B}$$

Bob

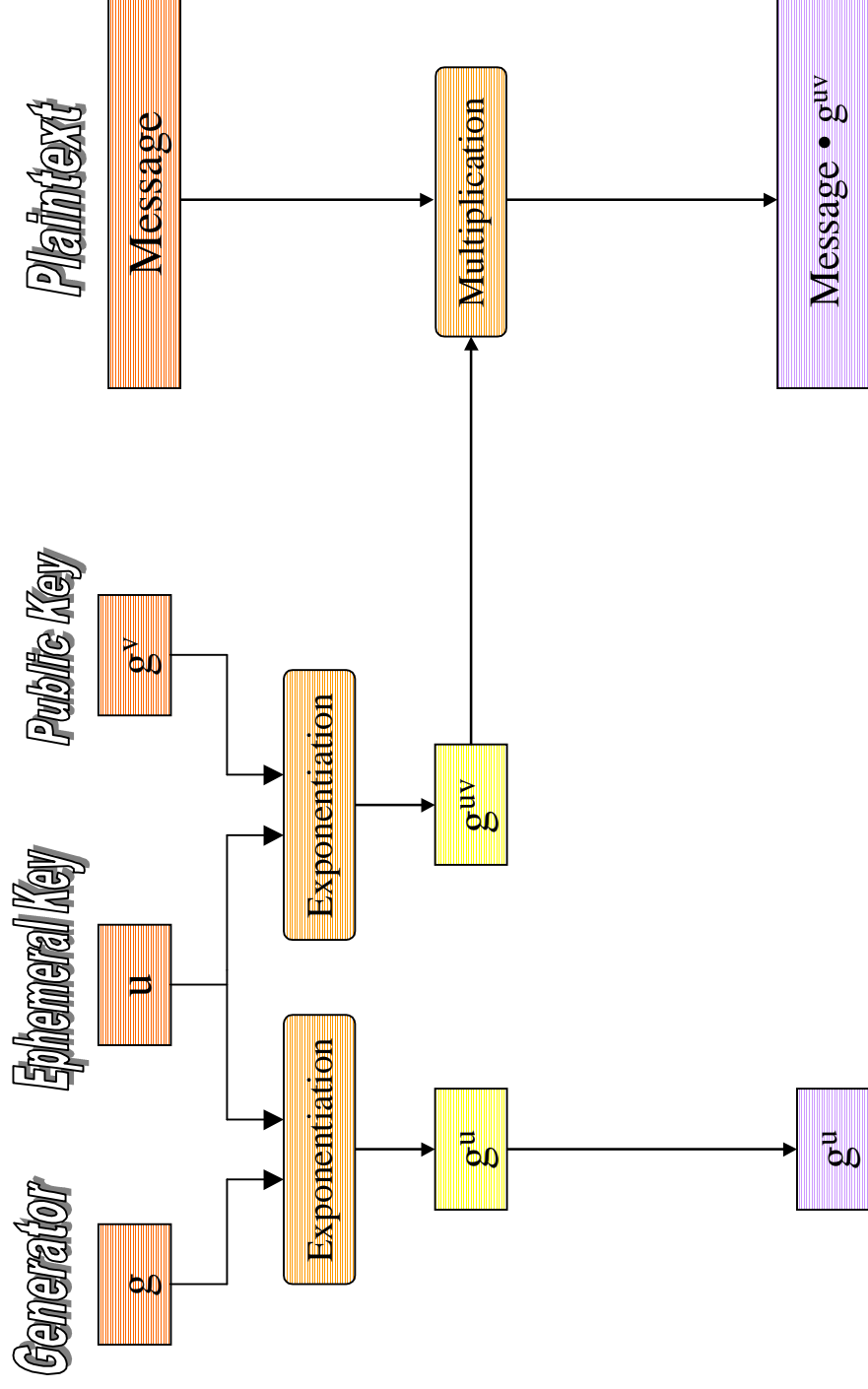
$$sk_B \xleftarrow{R} \{0, \dots, |G|-1\}$$

$$pk_B \leftarrow g^{sk_B}$$

$$S \leftarrow pk_B^{sk_A} = g^{sk_B sk_A}$$

$$S \leftarrow pk_A^{sk_B} = g^{sk_A sk_B}$$

# El Gamal Encryption Scheme



# Deficiencies of the El Gamal Scheme

- Security weakness: susceptible to chosen-ciphertext attacks.
- Functional weakness: requires message to be a group element.

# Our Goal

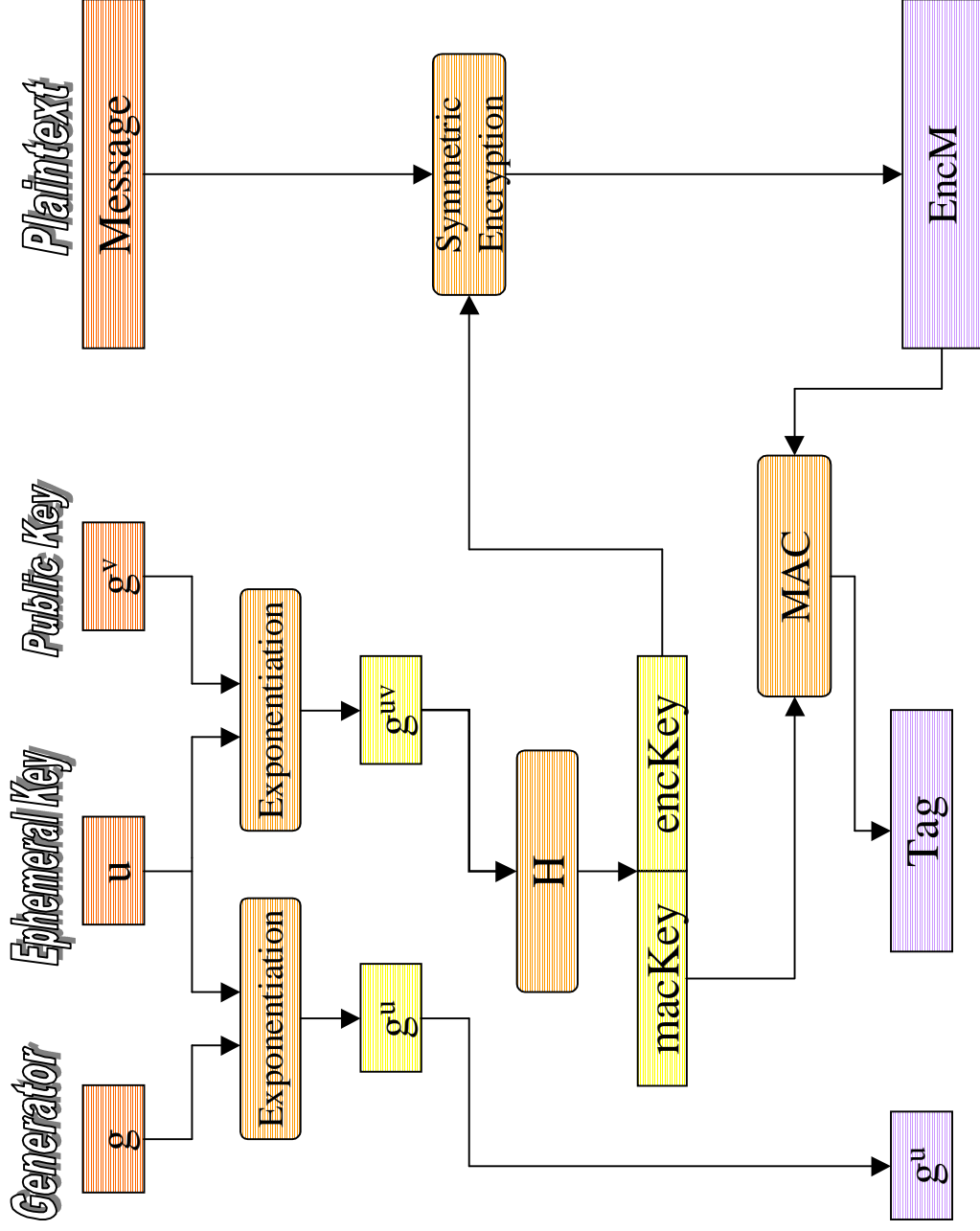
Design a natural, simple extension of the El Gamal scheme.

- **Security attributes:**
  - resistance to chosen-ciphertext attacks.
  - security supported by a proof.
- **Functional attributes:**
  - Can encrypt arbitrary messages
  - Same cost as El Gamal (for public key operations).

# Components of DHIES

- *A Symmetric Encryption Scheme.*  
e.g. DES/CBC encryption.
- *A Message Authentication Scheme.*  
e.g. HMAC.
- *H (Secure Hash Function).*  
e.g. SHA-1/MD5.

# Our scheme: DHIES



# Intuition

- MAC prevents chosen-ciphertext attacks.
- Symmetric encryption enables encryption of arbitrary messages.

# Use of DHIES

- ANSI X9.63EC (draft) standard
- IEEE P1363a (draft) standard
- Corporate (draft) standard SEC

# Comparison of Schemes in Groups of Prime Order

Scheme	IND-CPA	IND-CCA	Underlying Assumption	Cost: Number of Mod. Exp's
El Gamal	✓	X	DDH	2
Cramer-Shoup	✓	✓	DDH	4
DHIES	✓	✓	ODH	2

# Rest of the talk

- Measures of security for public-key encryption schemes
- Assumptions about hardness of discrete log/Diffie-Hellman related problems
- Security of DHIES

# Security Goals

- Indistinguishability (IND)

The encryption of two different plaintexts of the same length should be indistinguishable.

- Types of attack

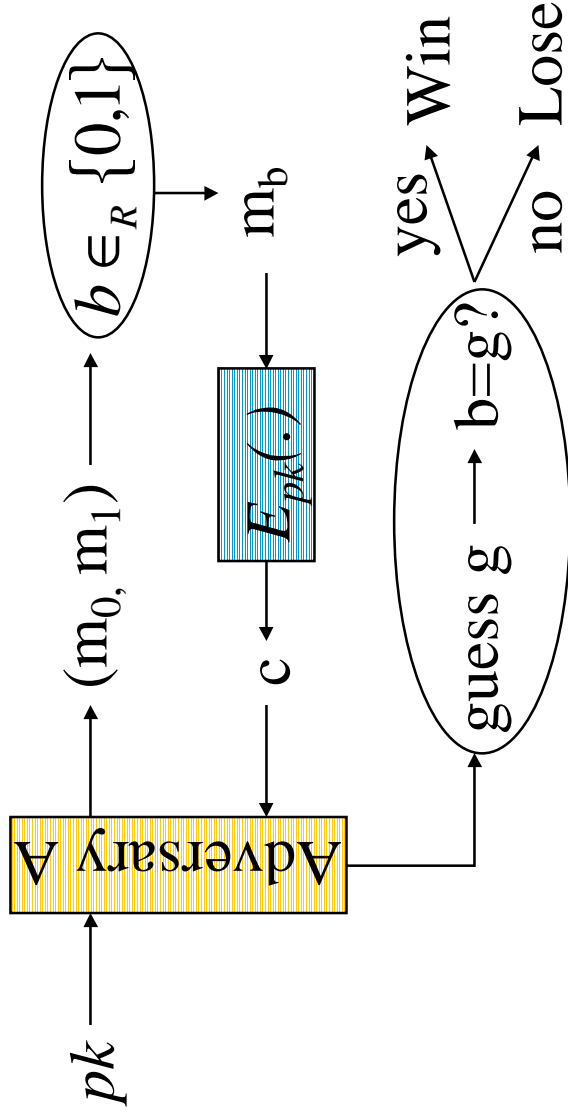
- Chosen-plaintext attack (CPA)

Always possible with PK encryption

- Chosen-ciphertext attack (CCA)

Adversary can make queries to a decryption oracle

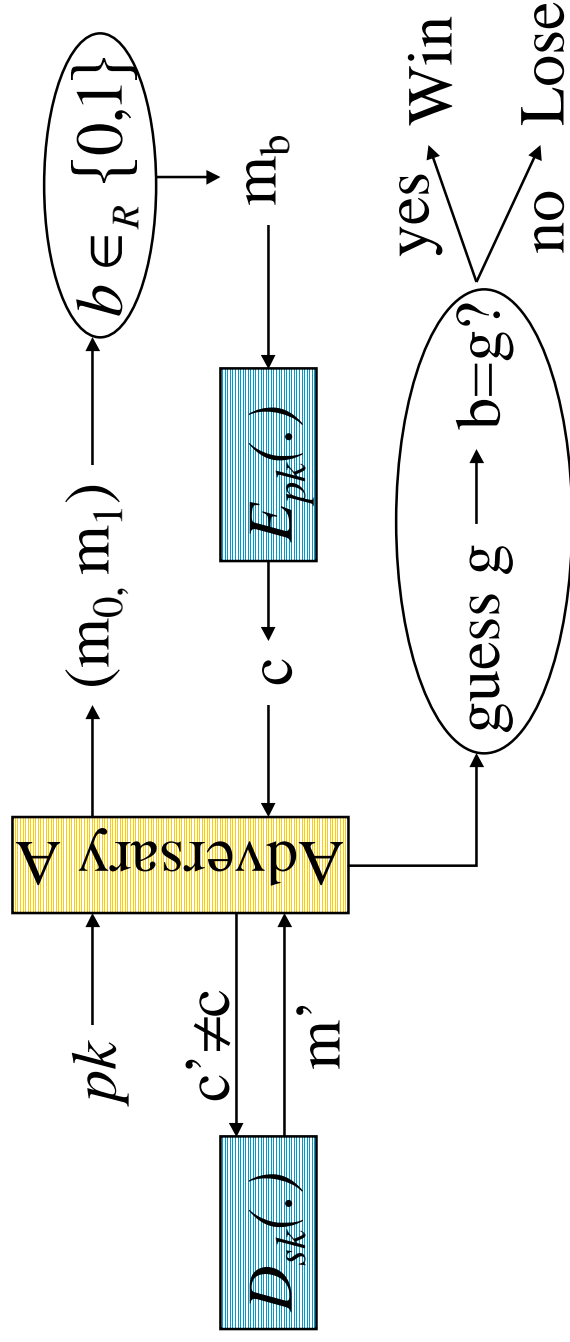
# IND-CPA



$$\text{Adv}_{\text{SCHEME}}^{\text{ind-cpa}}(t) = \max_A \text{Pr}[A \text{ wins}]$$

Scheme is IND-CPA secure if  $\text{Adv}_{\text{SCHEME}}^{\text{ind-cpa}}(t)$  is "small" for "large"  $t$ .

# IND-CCA



$$\text{Adv}_{\text{SCHEME}}^{\text{ind-cca}}(t, q) = \max_{\text{A running in time } t \text{ and making } q \text{ queries}} \{\Pr[A \text{ wins}]\}$$

Scheme is IND-CCA secure if  $\text{Adv}_{\text{SCHEME}}^{\text{ind-cca}}(t)$  is "small" for "large"  $t$ .

# Summary

- Measures of security associated to *SCHEME*,

$$\text{Adv}_{SCHEME}^{\text{ind-cpa}}(t) \quad \text{and} \quad \text{Adv}_{SCHEME}^{\text{ind-cca}}(t, q),$$

- capture **strong** security requirements (much beyond hardness of recovery of secret key) in a **quantitative** way.
- Practice-oriented provable-security approach.

# Rest of the Talk

- ✓ Measures of security for public-key encryption schemes
- Assumptions about hardness of discrete log/Diffie-Hellman related problems
- Security of DHIES

- We seek clear, believable assumptions on the DH problem under which security of **natural**, simple schemes (e.g., **DHIES**) can be **proved**.
- Our assumptions are **new** and **stronger** than previous ones, but this has enabled low-cost schemes with proven security.
- **We do not** use random oracles!

# Assumptions

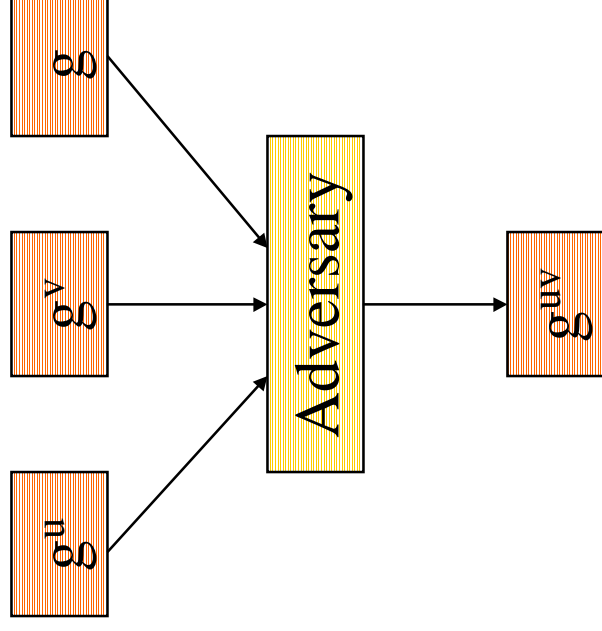
- **CDH** - Computational Diffie-Hellman
- **DDH** - Decisional Diffie-Hellman
- **HDH** - Hash Diffie-Hellman
- **ODH** - Oracle Diffie-Hellman



Increasing Strength

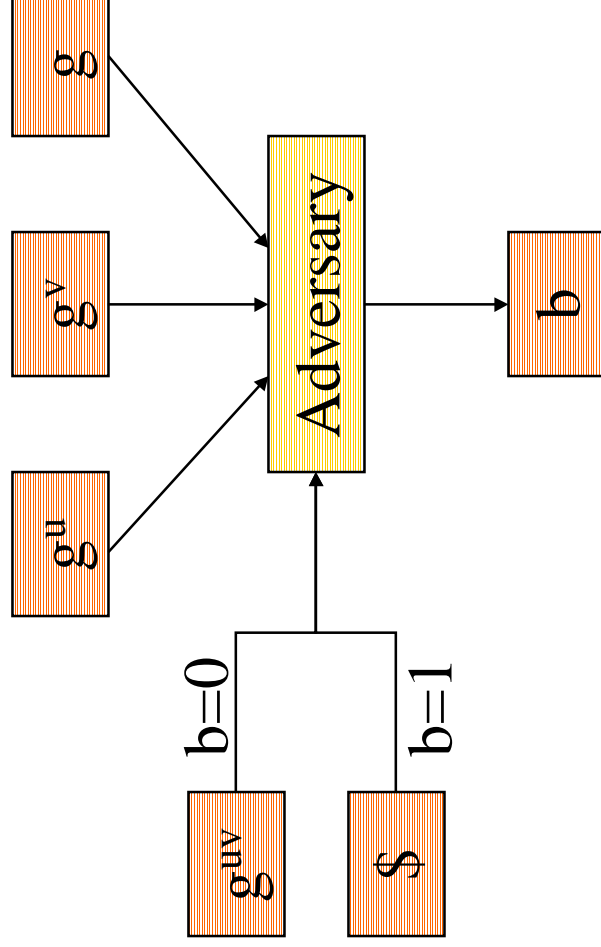
# Computational Diffie-Hellman (CDH)

Let  $g$  be a generator for a cyclic group  $G$ .



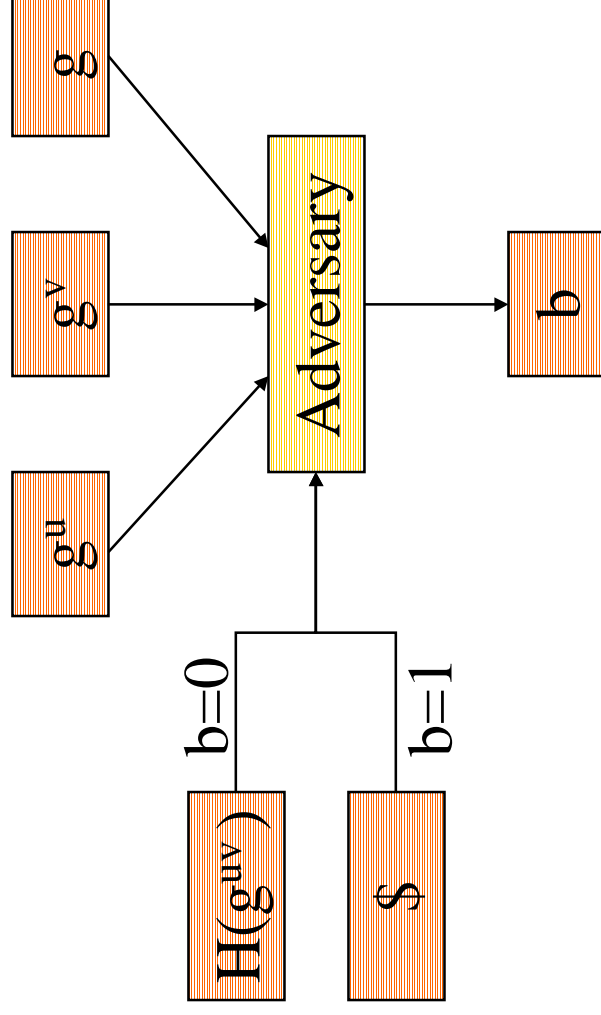
# Decisional Diffie-Hellman (DDH)

Let  $g$  be a generator for a cyclic group  $G$  of prime order.



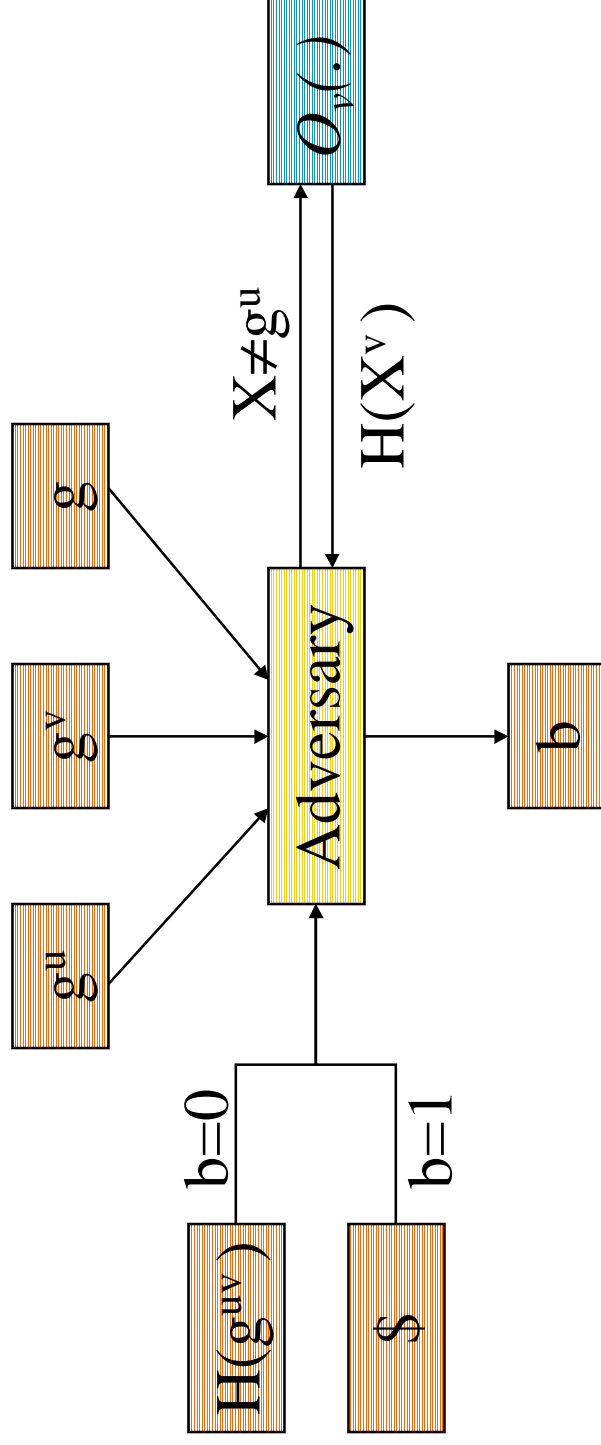
# Hash Diffie-Hellman (HDH)

Let  $g$  be a generator for a cyclic group  $G$  and  $H$  a hash function.



# Oracle Diffie-Hellman (ODH)

Let  $O_v$  be an oracle that, on input  $X$ , returns  $H(X^v)$ .



# Rest of the talk

- ✓ Measures of security for public-key encryption schemes
- ✓ Assumptions about hardness of discrete log/Diffie-Hellman related problems
- Security of DHIES

# IND-CPA of DHIES

- Theorem: If *HDH* holds in a cyclic group  $G$  and the underlying *symmetric encryption scheme* is secure, then *DHIES* is IND-CPA secure.
- Quantitative version:

$$\text{Adv}_{DHIES}^{\text{ind-cpa}}(t) \leq 2 \times \text{Adv}_{G,H}^{\text{hdh}}(t_1) + \text{Adv}_{SYM}^{\text{sym}}(t_2)$$

# IND-CCA of DHIES

- Theorem: If *ODH* holds in a cyclic group  $G$ , the underlying *symmetric encryption scheme* is secure, and the *MAC* is unforgeable, then *DHIES* is IND-CCA secure.

- Quantitative version:  $\text{Adv}_{\text{DHIES}}^{\text{cca}}(t, q) \leq$

$$2 \cdot \text{Adv}_{G,H}^{\text{odh}}(t_1, q) + 2 \cdot q \cdot \text{Adv}_{\text{MAC}}^{\text{mac}}(t_2, q - 1) + \text{Adv}_{\text{SYM}}^{\text{sym}}(t_3)$$

# Intuition for IND-CPA of DHIES

Let  $C = U \parallel Enc_M \parallel Tag$  be the challenge.

- Case 1: Output  $H(U^v)$  does not look random.  
Can break the *HDH assumption*.
- Case 2: Output  $H(U^v)$  looks random  
Can break the *underlying symmetric encryption*.

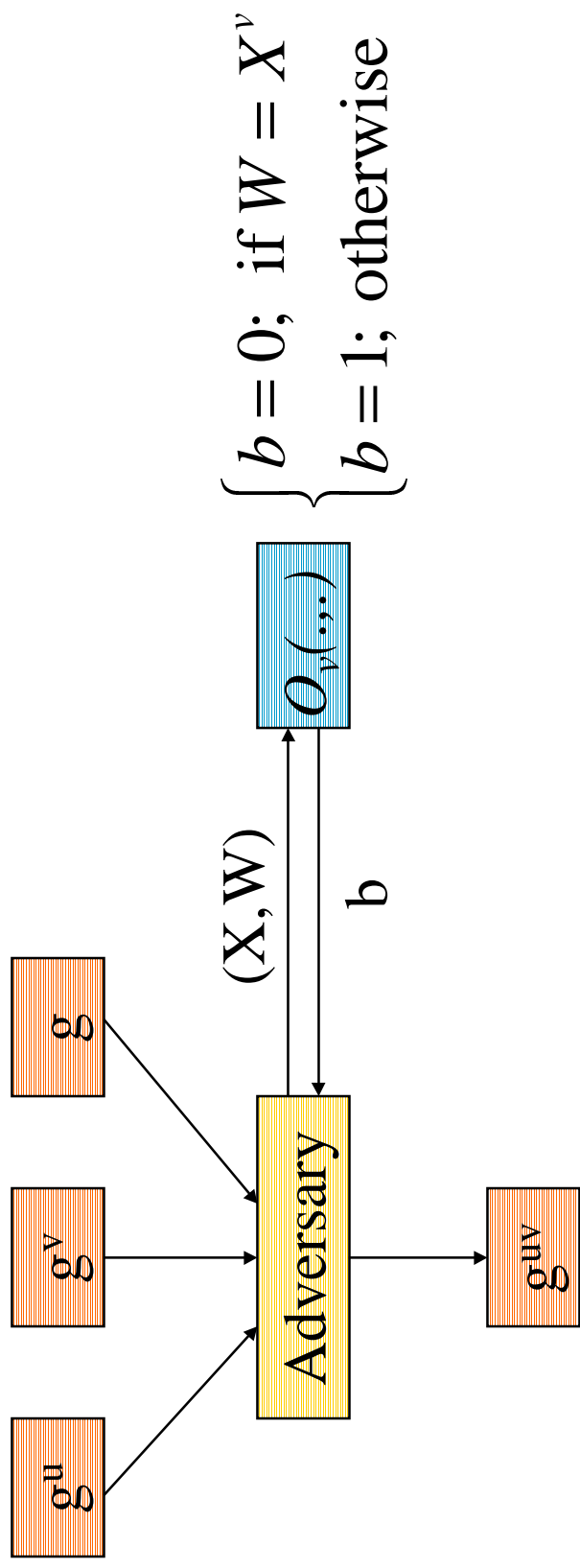
# Intuition for IND-CCA of DHIES

Let  $C = U // EncM // Tag$  be the challenge.

- Case 1: Output  $H(U^v)$  does not look random.
  - Can break the *ODH assumption*.
- Case 2: Output  $H(U^v)$  looks random
  - 2.1: there is a *valid* query to *decryption oracle*.
    - Can break the *underlying MAC*.
  - 2.2: there are no valid queries to *decryption oracle*.
    - Can break the *underlying symmetric encryption*.

# Proof in Random Oracle Model

- DHIES can **alternatively** be proven secure in the RO model based on the assumption that following problem (**SDH**) is hard.



# Proof in Generic Model

- In the generic model [Sh97], a lower bound for the hardness of SDH can be proved.
- Theorem: If  $p$  is the largest prime factor of the group order, then any generic algorithm solving SDH with non-negligible probability runs in time  $o(\sqrt{p})$

# Concluding Remarks

- *DHIES* was proven IND-CPA and IND-CCA.
- *DHIES* is as efficient as the basic El Gamal scheme.
- *DHIES* is more efficient than the Cramer-Shoup scheme [*CS98*], but under stronger assumptions.
- *DHIES* is included in several draft standards: P1363a, ANSI X9.63EC, SEC.