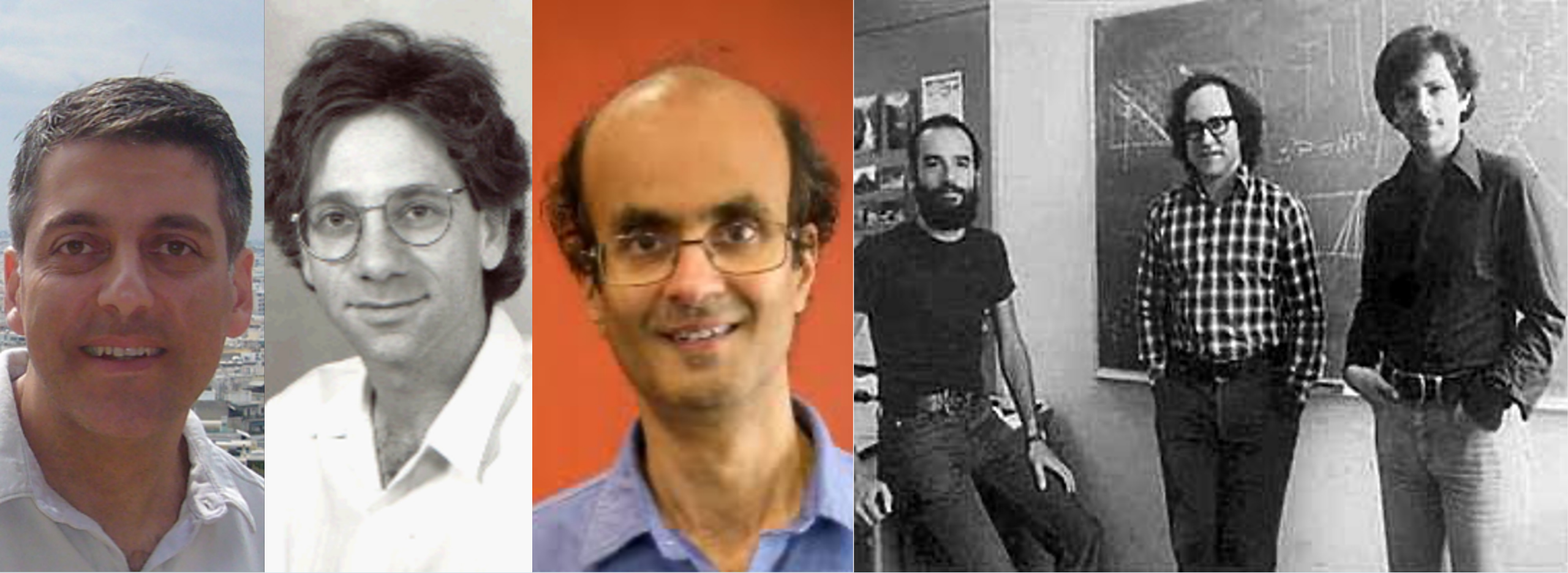


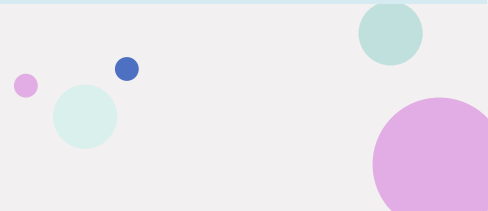


Lecture 15

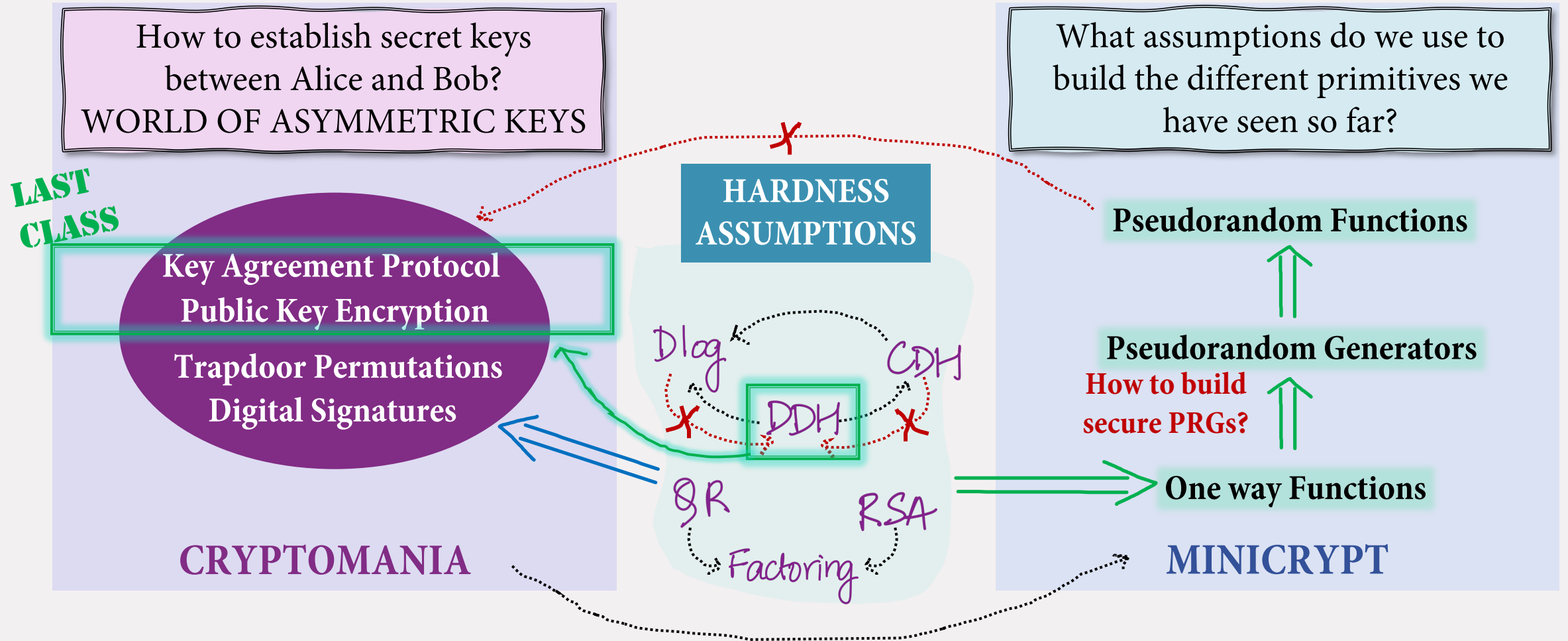
Trapdoor Permutations, Public Key Encryption Continued

CS409: Introduction to Cryptography

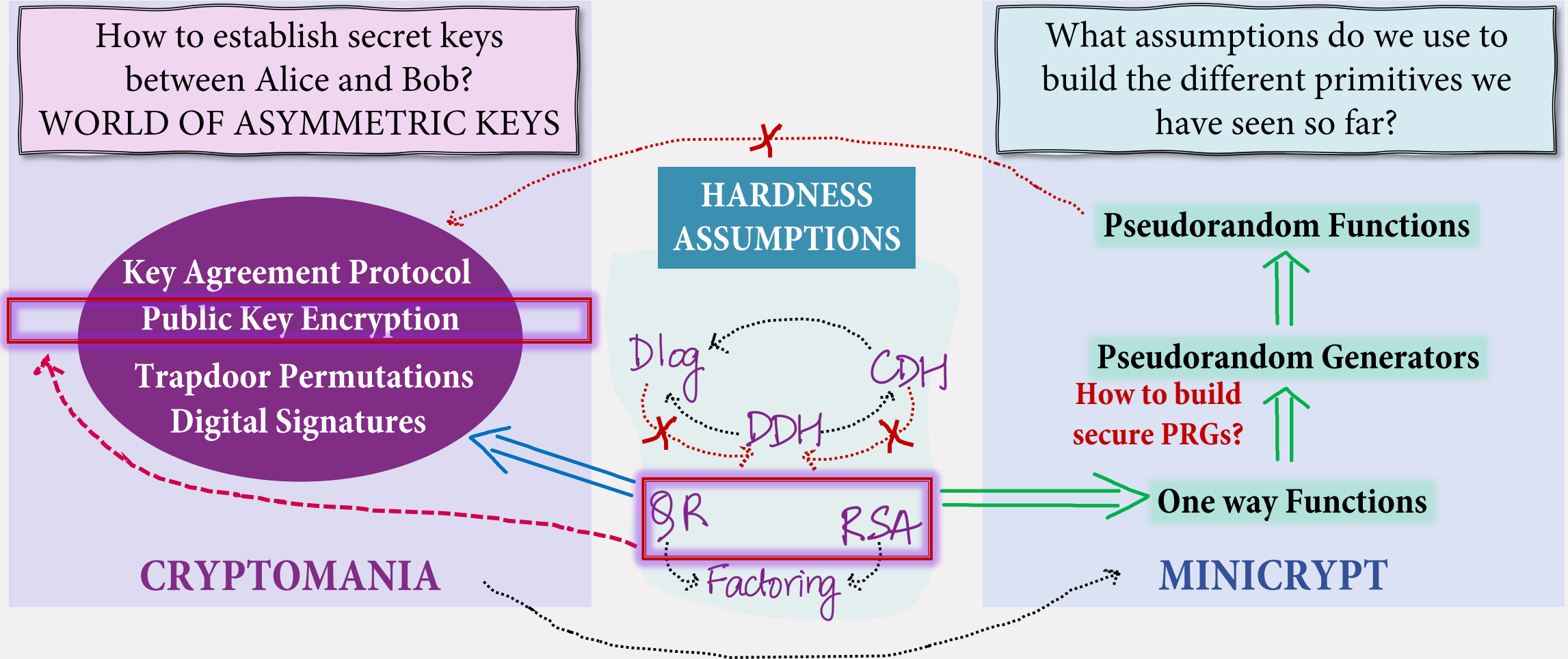
Sruthi Sekar



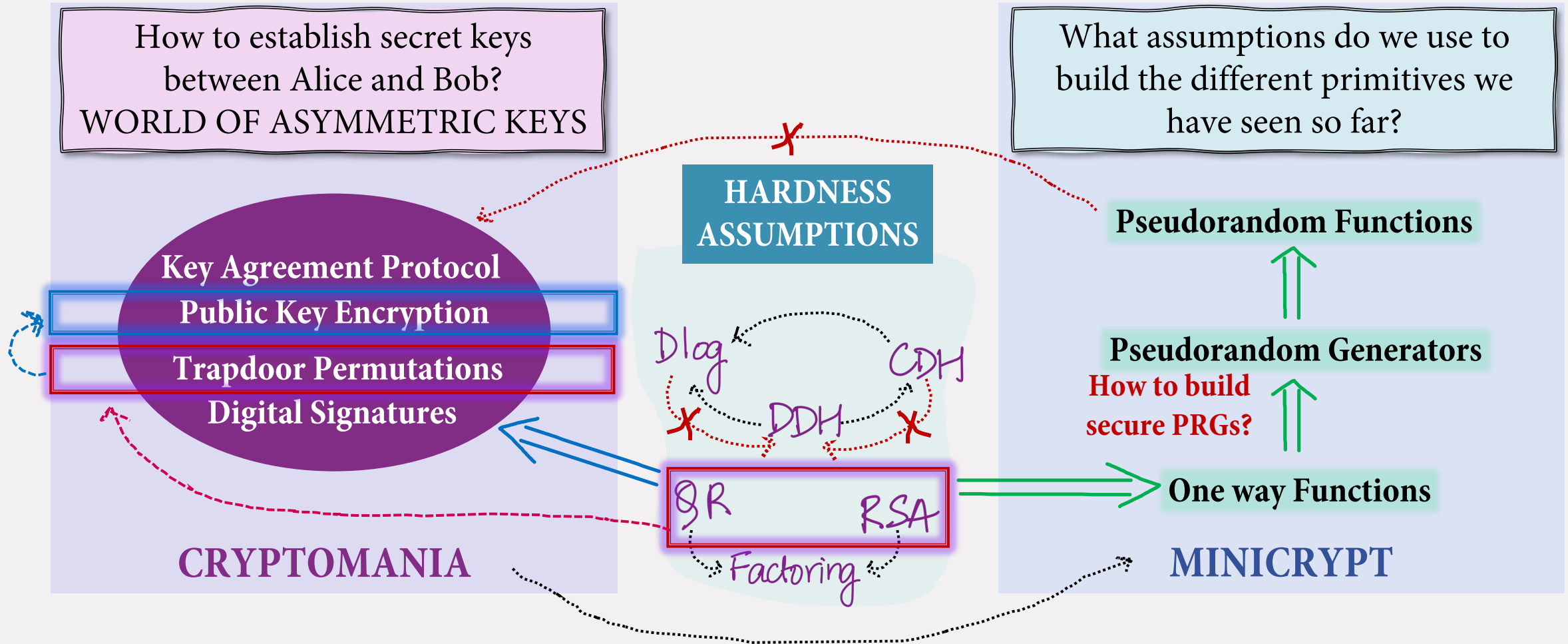
Recall



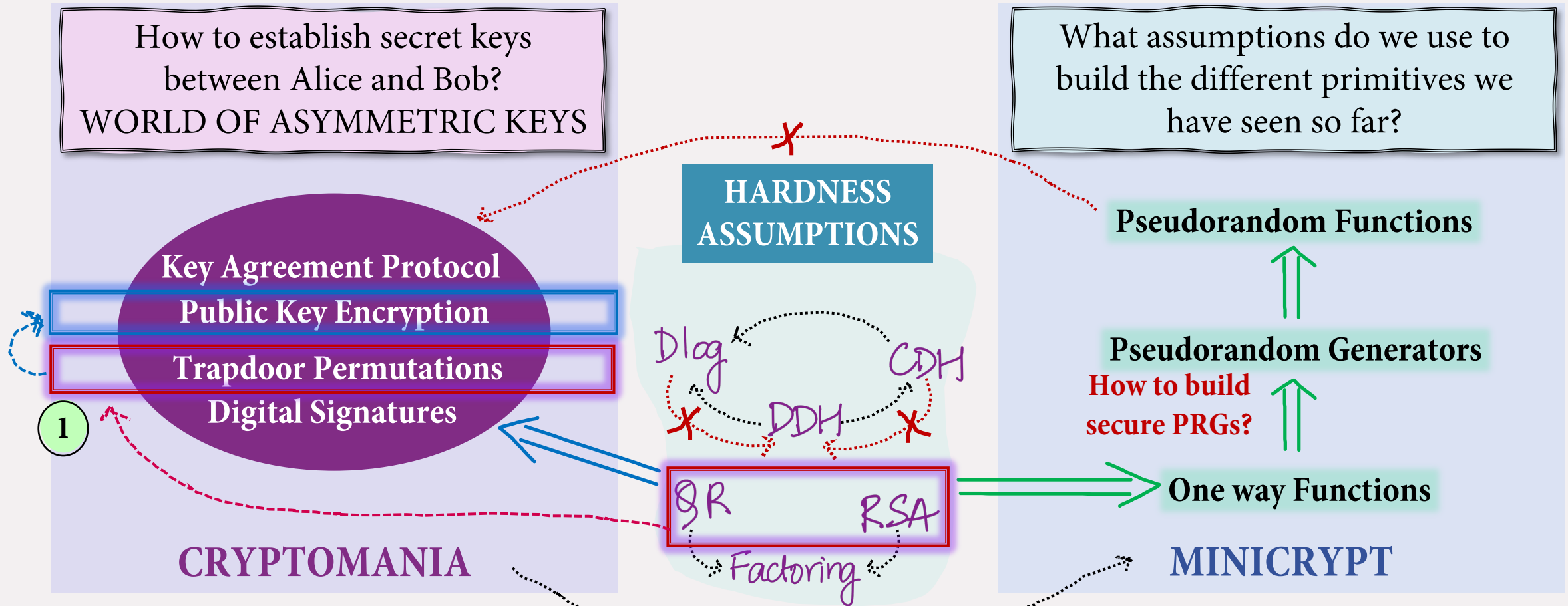
Today



Today



Today



2 IND-CCA Security against Mallory

Recall: One-way Functions

One-way Function Family

$$\{f_n: \{0,1\}^n \rightarrow \{0,1\}^{m(n)}\}_{n \in \mathbb{N}}, \quad \text{Gen}(1^n) \rightarrow f_n$$

- $\exists$ an efficient deterministic algorithm f such that $\forall x, f(n, x) = f_n(x)$

- $\forall$ PPT **Inv**, $\exists$ negl s.t. $\forall n$

$$\Pr_{x \in_R \{0,1\}^n} [\text{Inv}(1^n, f_n(x)) \in f_n^{-1}(f_n(x))] \leq \text{negl}(n)$$

- **Length-preserving OWF**: $m(n) = n$
- **One-way permutation Family**: for each $f_n \leftarrow \text{Gen}(1^n)$, f_n is length-preserving and bijective.

Examples

1. $\mathcal{G}(1^n) \rightarrow (\mathbb{G}, q, g)$, $f_{p,g}(x) := g^x \bmod p$, where $x \in \mathbb{Z}_q$ (**Exponentiation mod prime**)

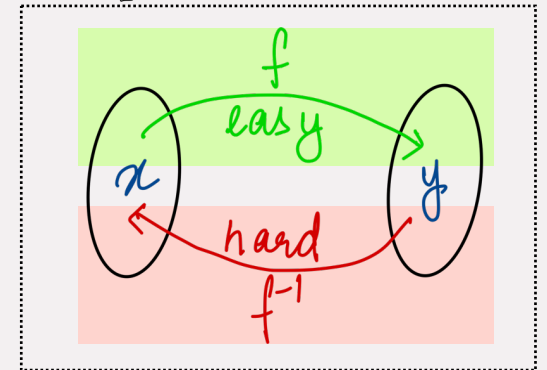
(If **Dlog** problem is hard relative to $\mathcal{G}$ then, $\{f_{p,g}\}$ is a OWF family)

2. $f_N(x) := x^2 \bmod N$, where $x \in \mathbb{Z}_N^*$ and $N = pq$ (large primes p and q). (**Squaring mod composite**)

(If factoring N is hard (factoring assumption), then $\{f_N\}$ is a OWF family)



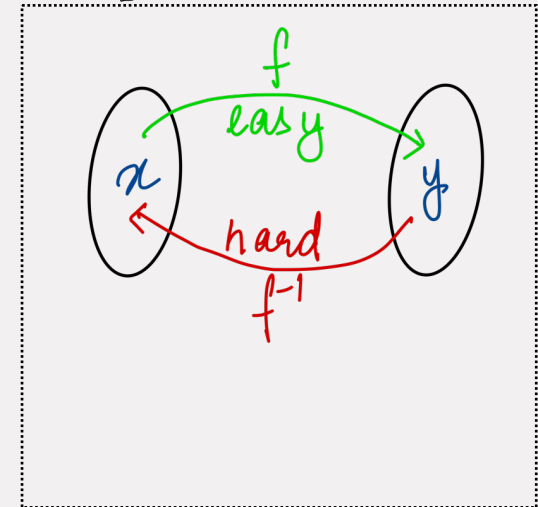
INTUITIVELY



Trapdoor Permutations



INTUITIVELY



Trapdoor Permutations

Definition 1: Trapdoor Permutation Family $\Pi = (\text{Gen}, f, \text{Inv})$

$\text{Gen}(1^n) \rightarrow I, \text{td}$

- $\exists$ an efficient deterministic algorithm f such that $\forall x, f(I, x) = f_I(x)$
- $\exists$ an efficient deterministic algorithm Inv_{td} such that

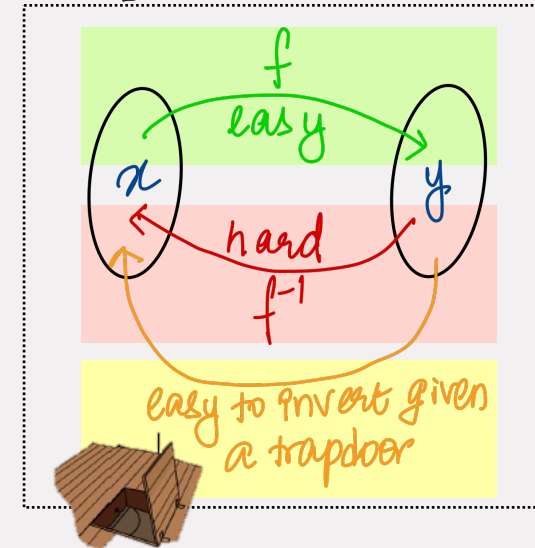
$$\Pr_{x \in_R \{0,1\}^n} [\text{Inv}_{\text{td}}(f_I(x)) \neq x] \leq \text{negl}(n)$$

- $\forall$ PPT $\text{Inv}, \exists \text{negl}$ s.t.

$$\Pr_{x \in_R \{0,1\}^n} [\text{Inv}(I, f_I(x)) \in f_I^{-1}(f_I(x))] \leq \text{negl}(n)$$



INTUITIVELY



Examples

RSA TDP: (from lec 14)

$$f_{N,e}(x) := x^e \bmod N, \text{ where } x \in \mathbb{Z}_N^*$$

(under RSA assumption)

Rabin TDP:

$$f_N(x) := x^2 \bmod N, \text{ where } x \in \text{QuadraticResidue}(\mathbb{Z}_N^*)$$

(under Factoring assumption)

➔ Let's formalize

RSA And Factoring Assumptions

$\text{GenModulus}(1^n) \rightarrow (N, p, q)$ such that $N = pq$, p and q are n -bit primes except with probability $\text{negl}(n)$.

Factoring Assumption

Factoring is hard relative to **GenModulus** if $\forall$ PPT, **Fac**, $\exists$ negl such that $\forall n$

$$\Pr_{(N,p,q) \leftarrow \text{GenModulus}(1^n)} [\text{Fac}(1^n, N) \rightarrow p', q' \text{ s.t. } (p', q' > 1) \wedge (p' \cdot q' = N)] \leq \text{negl}(n)$$

$\exists$ **GenModulus** relative to which factoring is hard

$\text{GenRSA}(1^n) \rightarrow (N, e, d)$ such that $N = pq$ (p, q : n -bit primes), $e, d > 0$: $\gcd(e, \phi(N)) = 1, ed = 1 \bmod \phi(N)$

RSA Assumption

The **RSA problem** is hard relative to **GenRSA** if $\forall$ PPT, **Inv**, $\exists$ negl such that $\forall n$

$$\Pr_{\substack{(N,e,d) \leftarrow \text{GenRSA}(1^n) \\ y \in_R \mathbb{Z}_N^*}} [\text{Inv}(1^n, N, e, y) \rightarrow x \text{ s.t. } (x \in \mathbb{Z}_N^*) \wedge (x^e = y \bmod N)] \leq \text{negl}(n)$$

$\exists$ **GenRSA** relative to which RSA is hard

? OPEN

Trapdoor Permutations

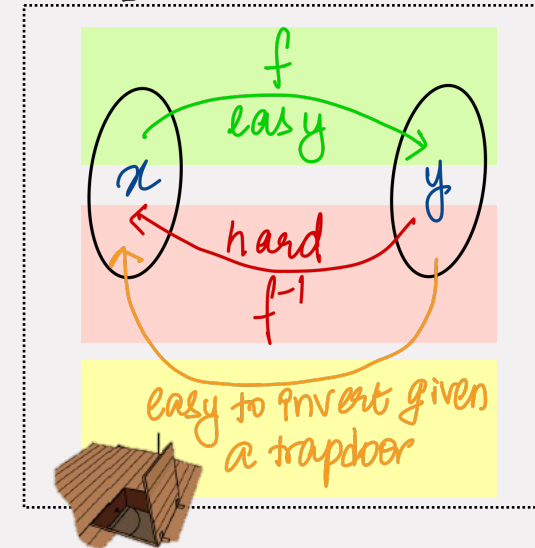
Definition 1: Trapdoor Permutation Family $\Pi = (\text{Gen}, f, \text{Inv})$

$\text{Gen}(1^n) \rightarrow I, \text{td}$

- ✓ $\exists$ an efficient deterministic algorithm f such that $\forall x, f(I, x) = f_I(x)$
- ? $\bullet \exists$ an efficient deterministic algorithm Inv_{td} such that
$$\Pr_{x \in_R \{0,1\}^n} [\text{Inv}_{\text{td}}(f_I(x)) \neq x] \leq \text{negl}(n)$$
- ✓ $\bullet \forall \text{PPT } \text{Inv}, \exists \text{negl s.t.}$
$$\Pr_{x \in_R \{0,1\}^n} [\text{Inv}(I, f_I(x)) \in f_I^{-1}(f_I(x))] \leq \text{negl}(n)$$



INTUITIVELY



Examples

RSA TDP: (from lec 14)

$f_{N,e}(x) := x^e \bmod N$, where $x \in \mathbb{Z}_N^*$

(under RSA assumption)

Rabin TDP:

$f_N(x) := x^2 \bmod N$, where $x \in \text{QuadraticResidue}(\mathbb{Z}_N^*)$

(under Factoring assumption)



Trapdoor?

Inv_{td} ?

Hard-Core Predicates

RECALL FROM LECTURE 13

Definition 2 Hard-core predicate of function family $\Pi = (\text{Gen}, f, \text{Inv})$

$$\text{Gen}(1^n) \rightarrow I, \text{td}$$

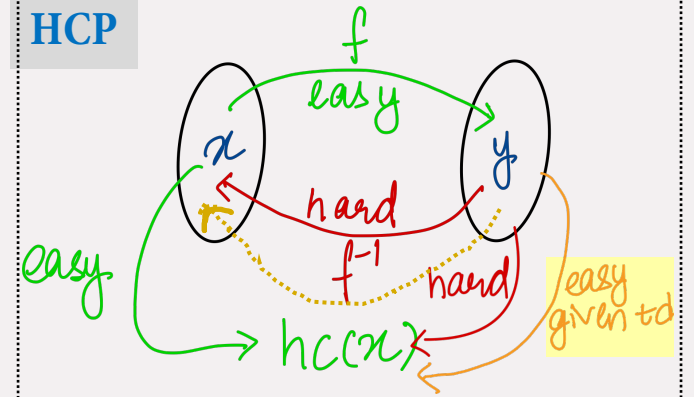
A predicate $hc_I: \{0,1\}^n \rightarrow \{0,1\}$ is a **hard-core predicate** for the above function family if for every **PPT** predictor **Pred**, $\exists \text{negl}$ such that $\forall n$

$$\Pr_{x \in_R \{0,1\}^n} [\text{Pred}(I, f_I(x)) = hc_I(x)] \leq \frac{1}{2} + \text{negl}(n)$$



INTUITIVELY

HCP



Example

RSA TDP:

$$f_{N,e}(x) := x^e \bmod N, \text{ where } x \in \mathbb{Z}_N^* \quad (\text{under RSA assumption})$$

HCP for RSA TDP:

$$\text{lsb}(x) := \text{least significant bit of } x, \text{ where } x \in \mathbb{Z}_N^*$$



Why? [Katz and Lindell, second edition, Theorem 11.31]

TDPs to IND-CPA PKE

Given: A TDP family $\Pi = (\text{Gen}^{\text{td}}, f, \text{Inv})$ and its hard-core predicate hc , how to encrypt a single bit?

$\text{Gen}(1^n)$: $\text{Gen}^{\text{td}}(1^n) \rightarrow I, \text{td}$, output $\text{pk} = I, \text{sk} = \text{td}$

$\text{Enc}(\text{pk}, m)$: For the bit, $m \in \{0,1\}$, choose $r \in_R \{0,1\}^n$ and output $c = (f_I(r), hc_I(r) \oplus m)$

$\text{Dec}(\text{sk}, c = (y, b))$: $\because \text{sk} = \text{td}$, compute $x := \text{Inv}_{\text{td}}(y)$ and the message $m = b \oplus hc_I(x)$

Construction 1

Theorem 1: IND-CPA Security of Construction 1

If $\Pi = (\text{Gen}^{\text{td}}, f, \text{Inv})$ is a TDP family with HCP hc , then **Construction 1** is an IND-CPA secure PKE.

****Therefore, you now have an IND-CPA PKE under the RSA assumption!**

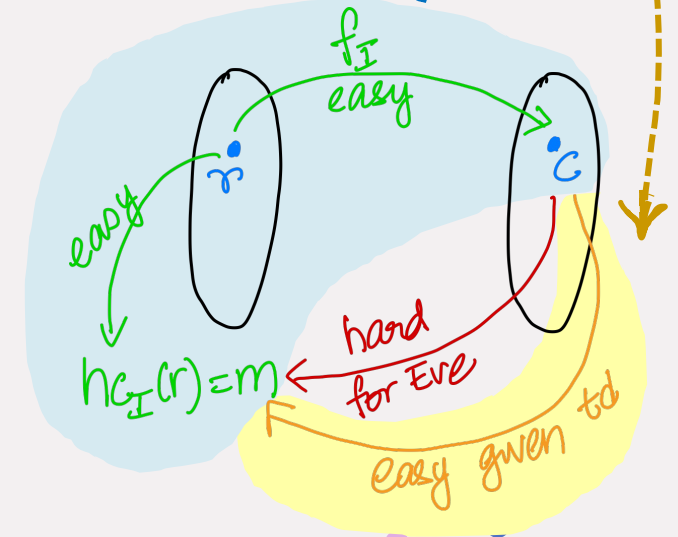
Discuss intuition on board..

HW1

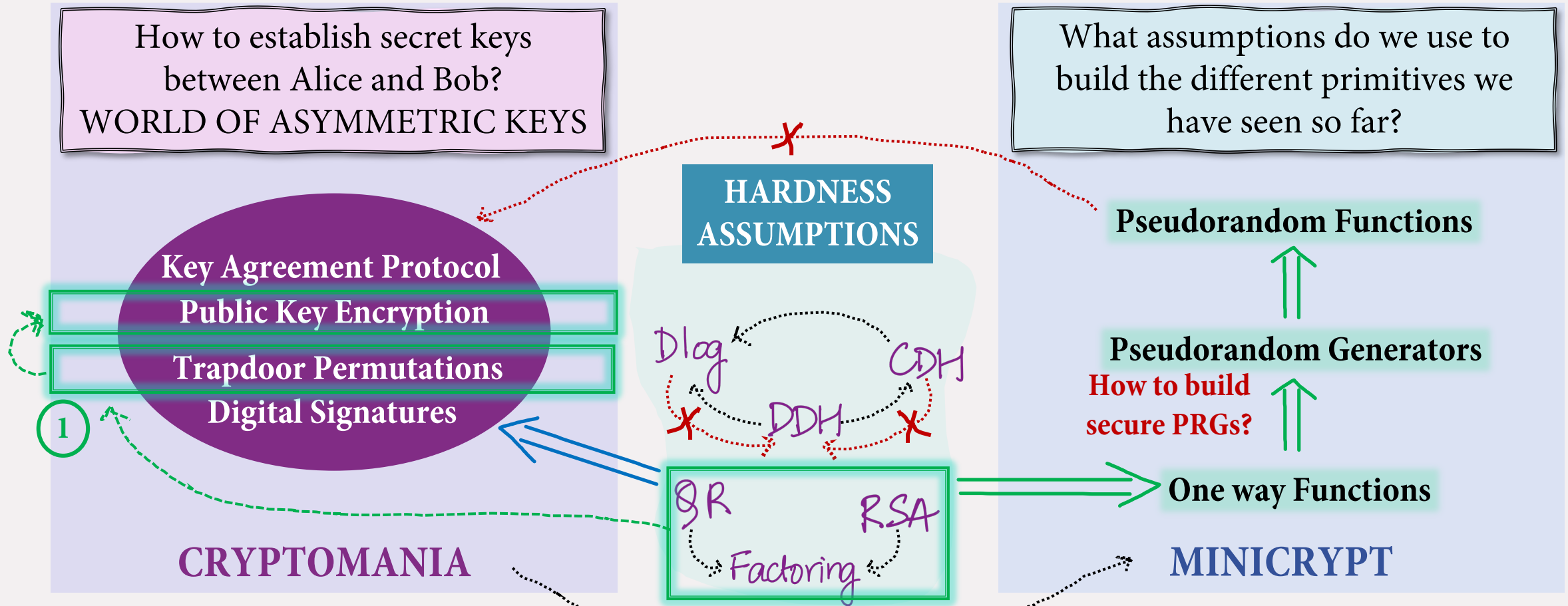
Prove Theorem 1 via a security reduction

HW2

What about encrypting multiple bits?

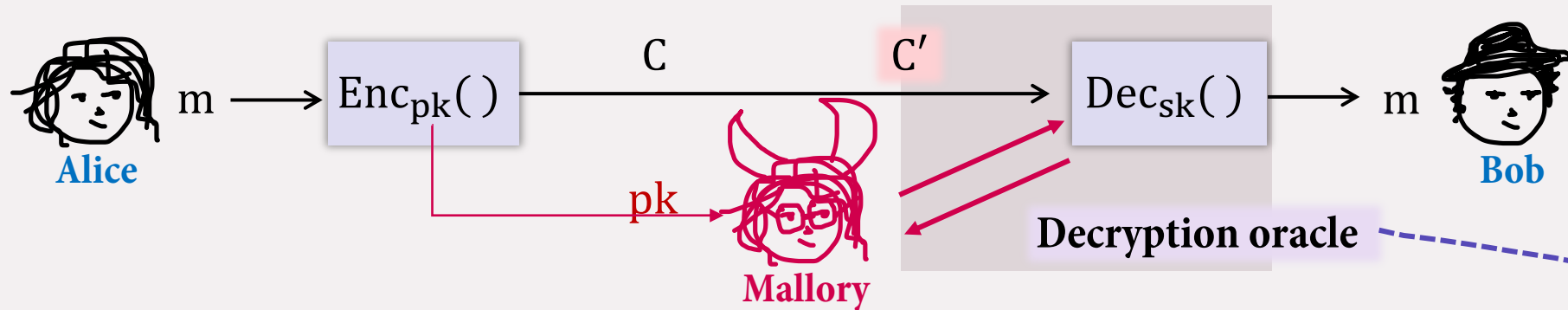


Today



2 IND-CCA Security against Mallory

Malleability Attacks on PKE



What if **Mallory** “malleates” C to produce a new ciphertext C' , that would decrypt to a “related” message m' ?

Malleability of ElGamal Encryption

$\text{Gen}(1^n): \mathcal{G}(1^n) \rightarrow (\mathbb{G}, q, g), x \in_R \mathbb{Z}_q$
 $\text{pk} = (\mathbb{G}, g, X = g^x), \text{sk} = (\mathbb{G}, g, x)$

$\text{Enc}(\text{pk}, m): y \leftarrow \mathbb{Z}_q$
 $C = (C_1 = Y = g^y, C_2 = mX^y)$

$\text{Dec}(\text{sk}, C): C_2 Y^{-x}$

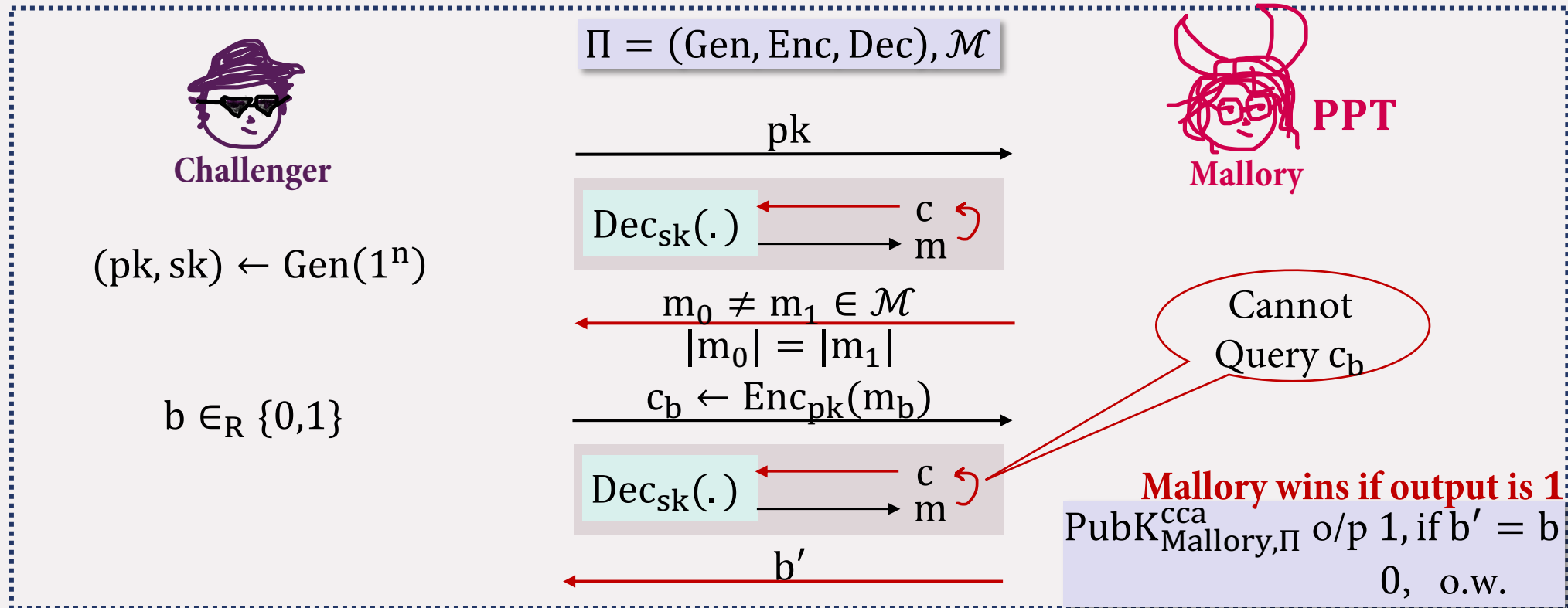
$C' = (Y = g^y, TmX^y) \quad \text{Dec}_{sk}(C') = Tm$

Mallory

Chosen Ciphertext Attack (CCA)

Mallory can get Tm and hence m ! **BREAK!**

IND-CCA Security for PKE



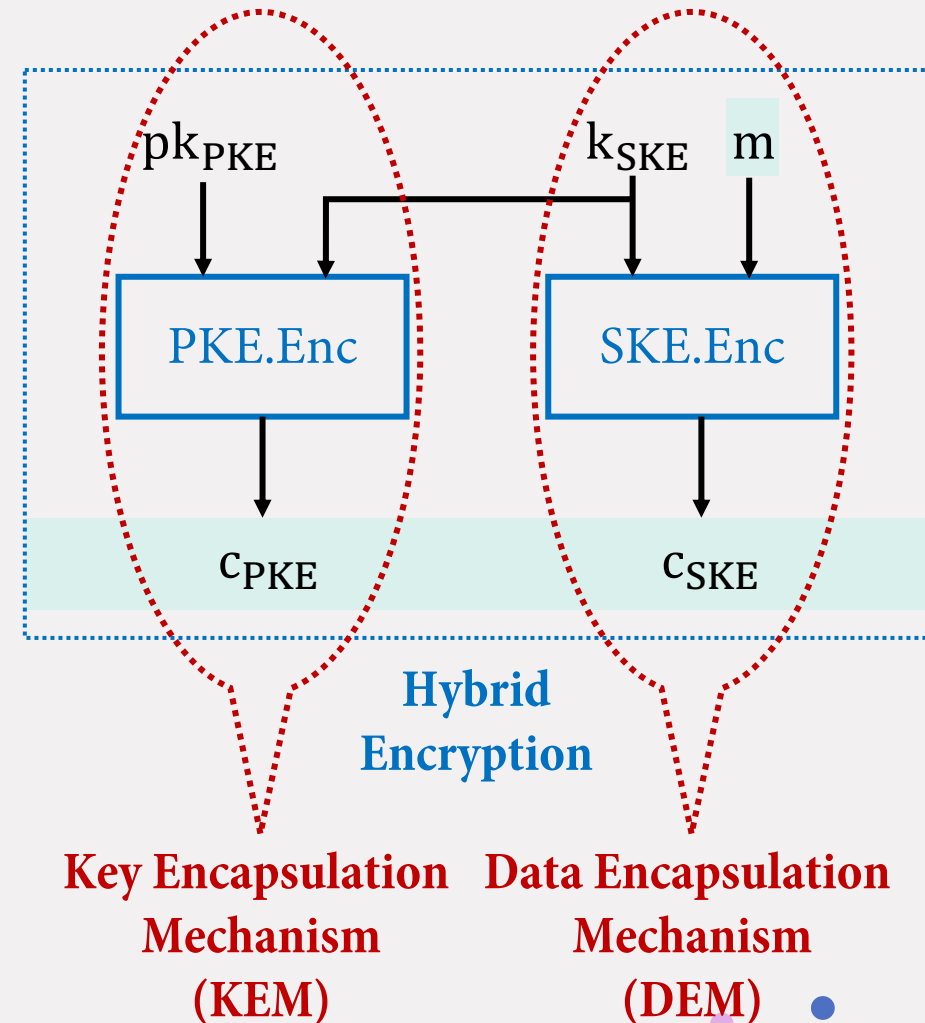
Definition 3: IND-CCA Security (Chosen Ciphertext Attack)

Π is **CCA secure** if, for all **PPT** adversary **Mallory**, there exists a negligible function **negl** such that $\forall n$

$$\Pr[\text{PubK}_{\text{Mallory}, \Pi}^{\text{cca}}(n) = 1] \leq 1/2 + \text{negl}(n)$$

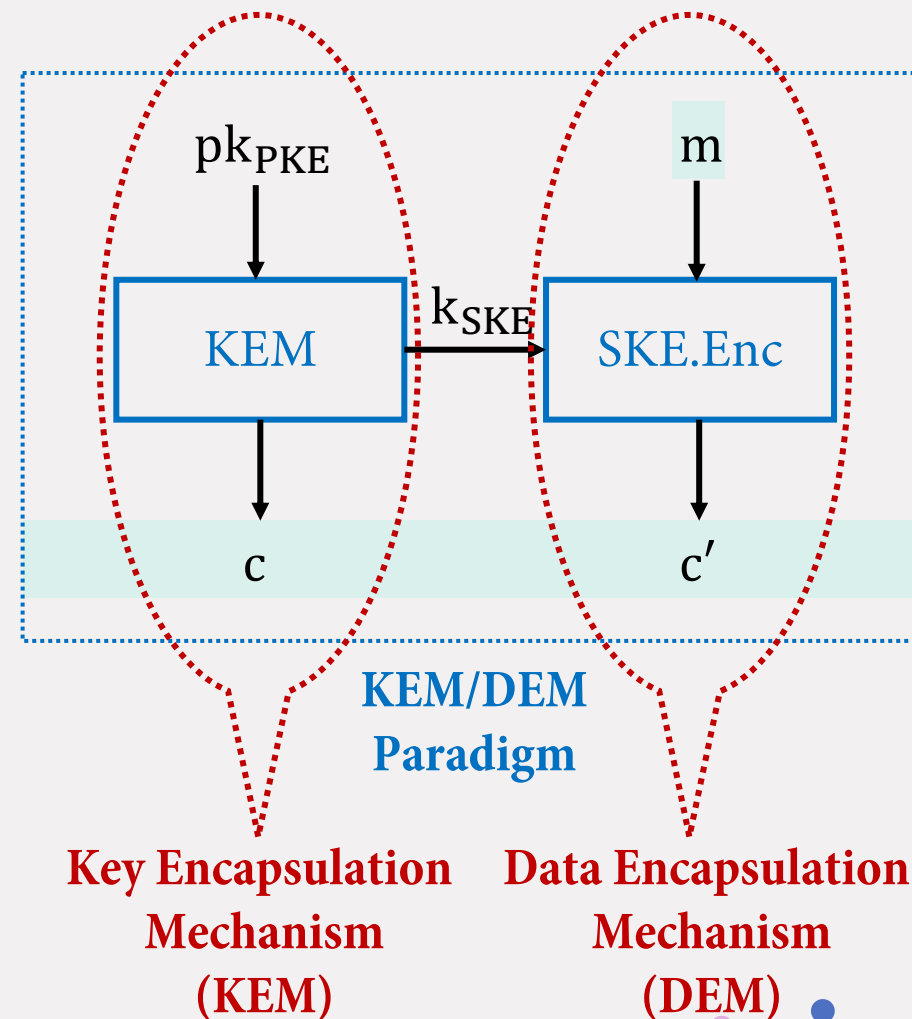
Hybrid Encryption

- **PKE is far less efficient than SKE.**
E.g., DDH-based and RSA CCA encryptions all use exponentiations in group, etc.
- **SKE and MAC are very fast in practice.**
(e.g., using block ciphers like AES)
- **Hybrid Encryption:** Use CCA PKE to transfer k_{SKE} for CCA SKE. The CCA SKE is used to encrypt the message m .
- **Why is this cost-saving?**
PKE is only used to encrypt short k_{SKE} !



KEM/DEM Paradigm

- **Key Encapsulation Method (KEM):** The Encapsulation process takes only the public key pk_{PKE} (no message) and directly outputs the ciphertext c and a key k_{SKE} .
- **Data Encapsulation Method (DEM):** The symmetric encryption used to encrypt the data/message.



Hybrid Encryption Syntax

$$\Pi^{\text{hybrid}} = (\text{Gen}, \text{Enc}, \text{Dec})$$

$$\Pi^{\text{KEM}} = (\text{Gen}^{\text{K}}, \text{Encap}, \text{Decap}); \Pi^{\text{SKE}} = (\text{Gen}^{\text{SKE}}, \text{Enc}^{\text{SKE}}, \text{Dec}^{\text{SKE}})$$

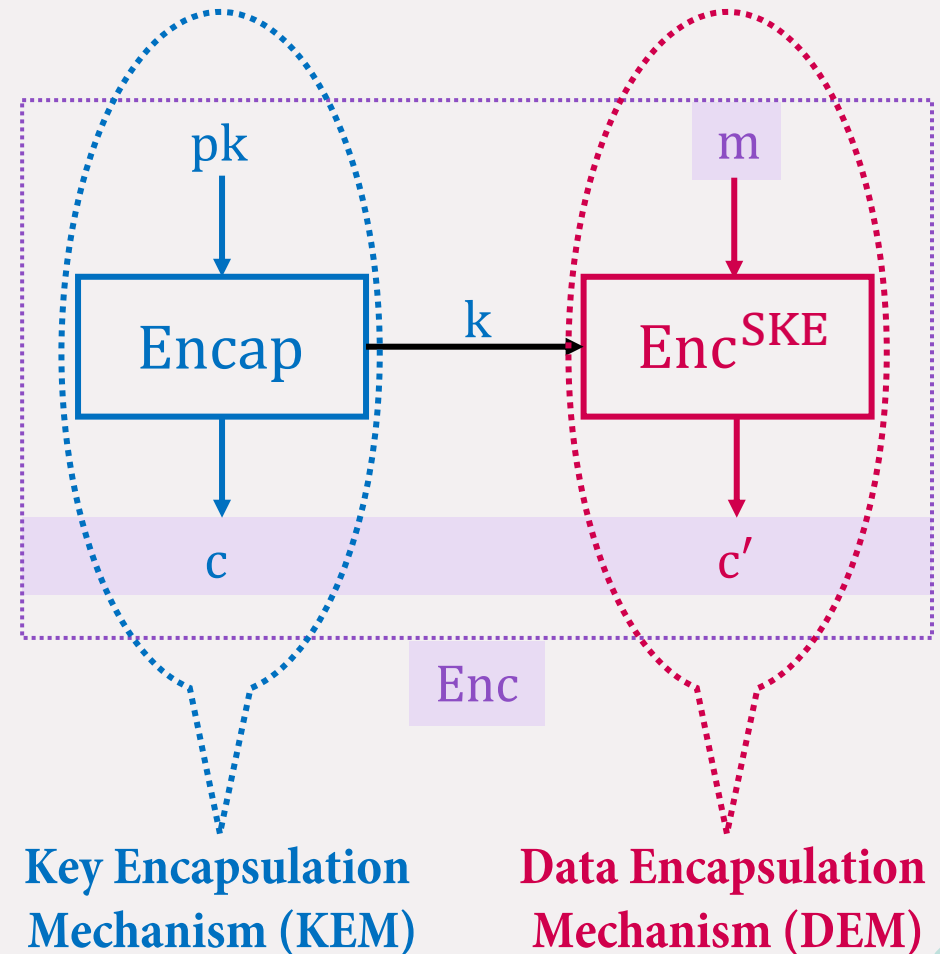
- $\text{Gen}(1^n): (\text{pk}, \text{sk}) \leftarrow \text{Gen}^{\text{K}}(1^n)$
- $\text{Enc}(\text{pk}, m)$: compute $(c, k) \leftarrow \text{Encap}(1^n)$
compute $c' \leftarrow \text{Enc}^{\text{SKE}}(k, m)$
output (c, c')
- $\text{Dec}(\text{sk}, (c, c'))$: compute $k \leftarrow \text{Decap}(\text{sk}, c)$
output $m = \text{Dec}^{\text{SKE}}(k, c')$



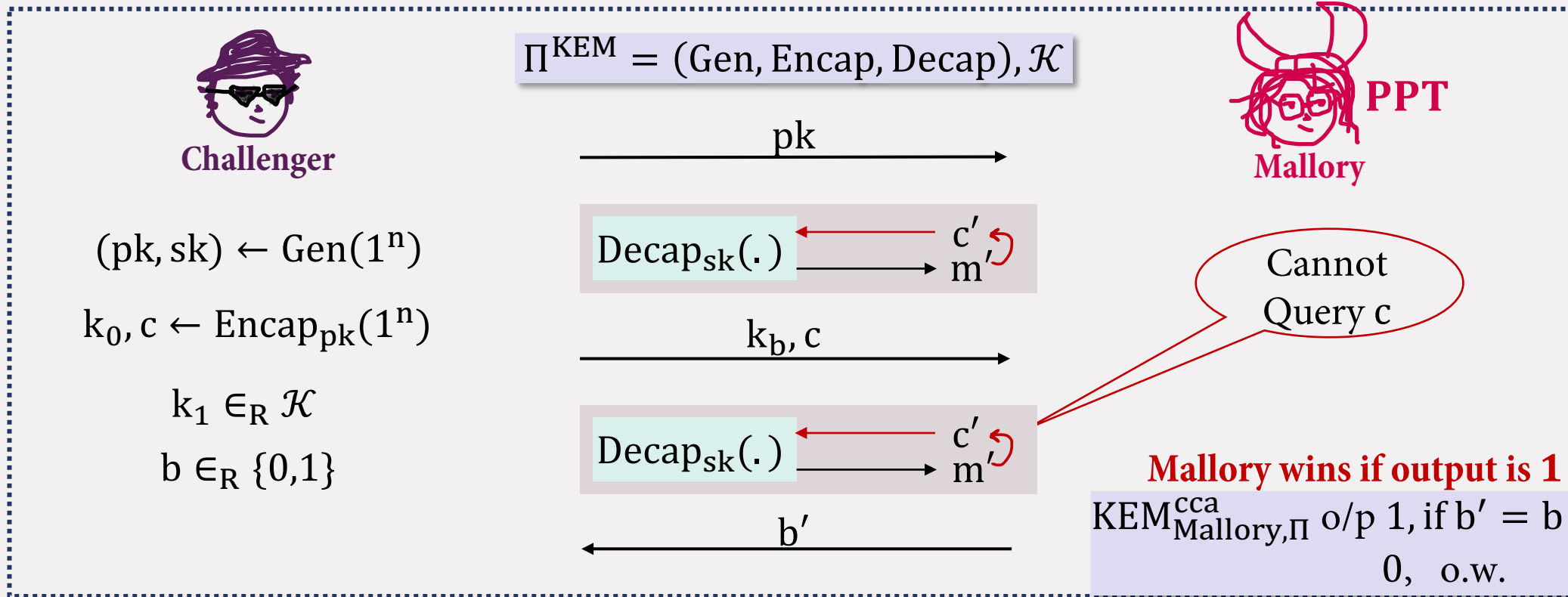
When is a hybrid encryption IND-CCA Secure?

CCA KEM + CCA SKE $\Rightarrow$ CCA PKE

Let's formalize!



IND-CCA Security for KEM



Definition 4: IND-CCA Security (Chosen Ciphertext Attack) of KEM

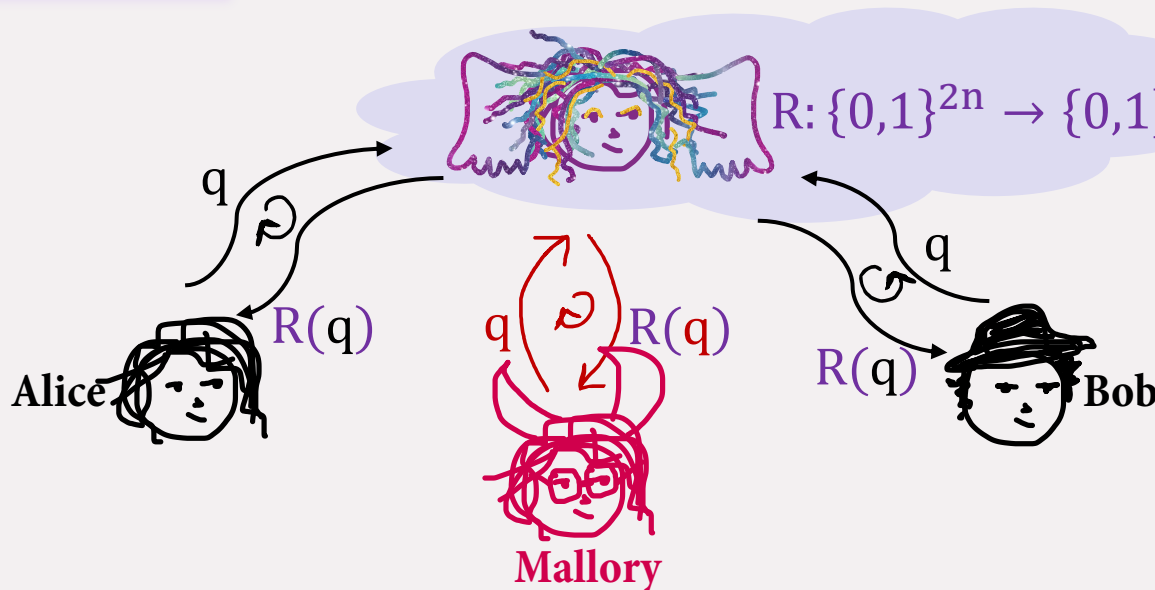
Π^{KEM} is **CCA secure** if, for all **PPT** adversary **Mallory**, there exists a negligible function **negl** such that $\forall n$

$$\Pr[\text{KEM}_{\text{Mallory}, \Pi}^{\text{cca}}(n) = 1] \leq 1/2 + \text{negl}(n)$$

Random Oracle Model

THE POWER: Random Function Oracle in the Sky accessible to all

**RECALL
FROM
LECTURE 6**



Everyone (including **Mallory**) has access to a random function oracle $R: \{0,1\}^{2n} \rightarrow \{0,1\}^n$

- **Queries Private:** **Mallory** will not know **Alice** and **Bob**'s queries, x .
- **R implements a truly random function:** On fresh input x by anyone, R outputs $y \in_R \{0,1\}^n$ and adds (x, y) to the queried list Q . If the query x is already in Q , then return the corresponding y .

Diffie-Hellman Integrated Encryption Scheme

(DHIES) IND-CCA Hybrid Encryption

Gen(1^n): $\mathcal{G}(1^n) \rightarrow (\mathbb{G}, q, g)$, $x \in_R \mathbb{Z}_q$, $X = g^x$, specify a function $H: \mathbb{G} \rightarrow \{0,1\}^{2n}$
output $pk = (\mathbb{G}, q, g, X, H)$, $sk = (\mathbb{G}, q, g, x, H)$

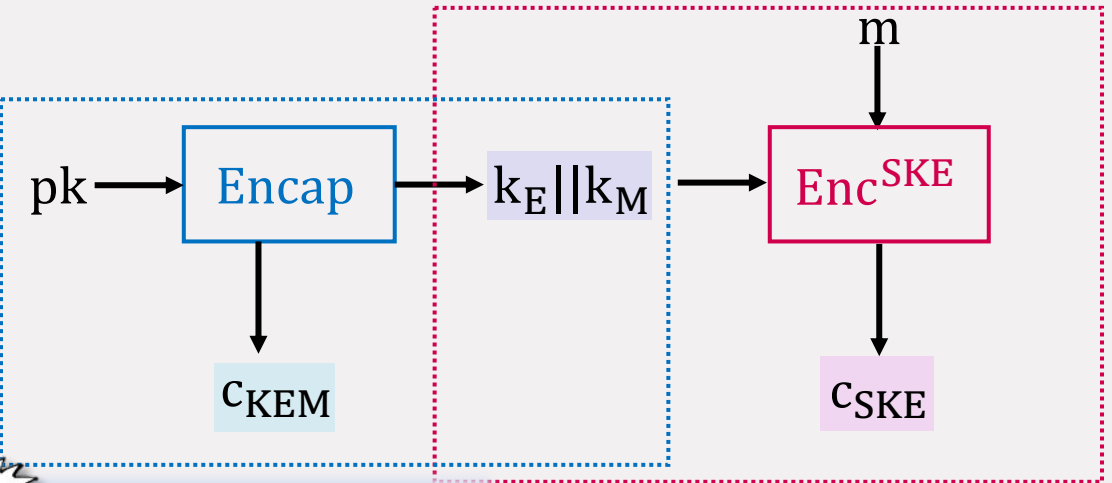
Enc(pk, m):

Encap(pk): $y \in_R \mathbb{Z}_q$
 $k_E || k_M \leftarrow H(X^y)$
 $c_{KEM} = g^y$

Enc^{SKE}($k_E || k_M, m$):
 $c_{SKE} = (c = \text{Enc}_{k_E}(m), \text{MAC}_{k_M}(C))$

Encrypt-then-authenticate

Output: (c_{KEM}, c_{SKE})



Is this a CCA KEM?

CCA Secure SKE
 [Lec 9]



CCA Security of $\Pi^{\text{hybrid}} = (\text{Gen}, \text{Enc}, \text{Dec})?$

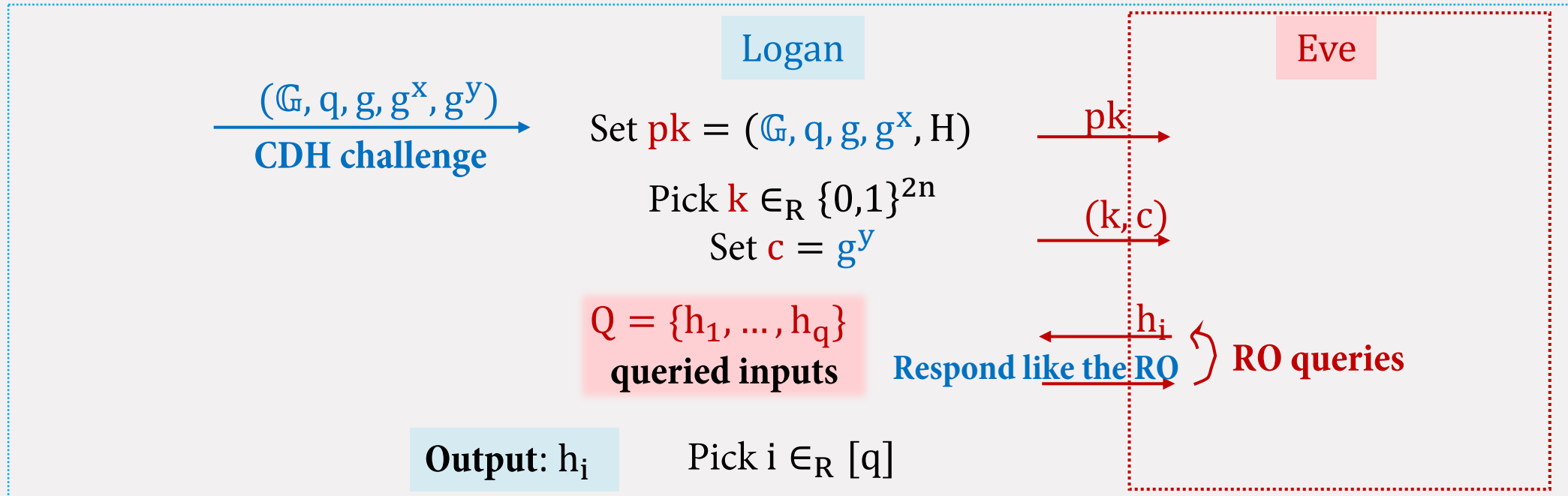
CCA KEM + CCA SKE $\Rightarrow$ CCA Hybrid Encryption

DHIES: IND-CPA Security

Theorem 2: IND-CPA Security of DHIES KEM

If **CDH** is hard relative to $\mathcal{G}$ and $H: \mathbb{G} \rightarrow \{0,1\}^{2n}$ is an **RO**, then the DHIES KEM is **IND-CPA-secure**.

Proof Sketch: $\exists$ **Eve** against the CPA security $\Rightarrow \exists$ **Logan** breaking CDH



If **Eve** did query g^{xy} then
CDH is broken w.p. $1/q$!

If **Eve** didn't query g^{xy} then, **k** is uniform from **Eve's** perspective!
Hence, can guess **b** w.p. $1/2$

■

DHIES: IND-CCA Security

Theorem 3: IND-CCA Security of DHIES KEM

If **gap-CDH** is hard relative to $\mathcal{G}$ and $H: \mathbb{G} \rightarrow \{0,1\}^{2n}$ is a **RO**, then the DHIES KEM is **IND-CCA-secure**.

Proof Sketch- Bird's eye view

CCA Security?

- IND-CCA adversary has access to $\text{Decap}_{\text{sk}}(\cdot)$, which means it has access to a **DDH solver!**
- Excluding the $\text{Decap}_{\text{sk}}(\cdot)$, the **IND-CCA** adversary is like an **IND-CPA** adversary (secure based on **CDH**).
- Thus, if **CDH** is hard, even given a DDH solver (called **gap-CDH**), DHIES is **IND-CCA-secure!**

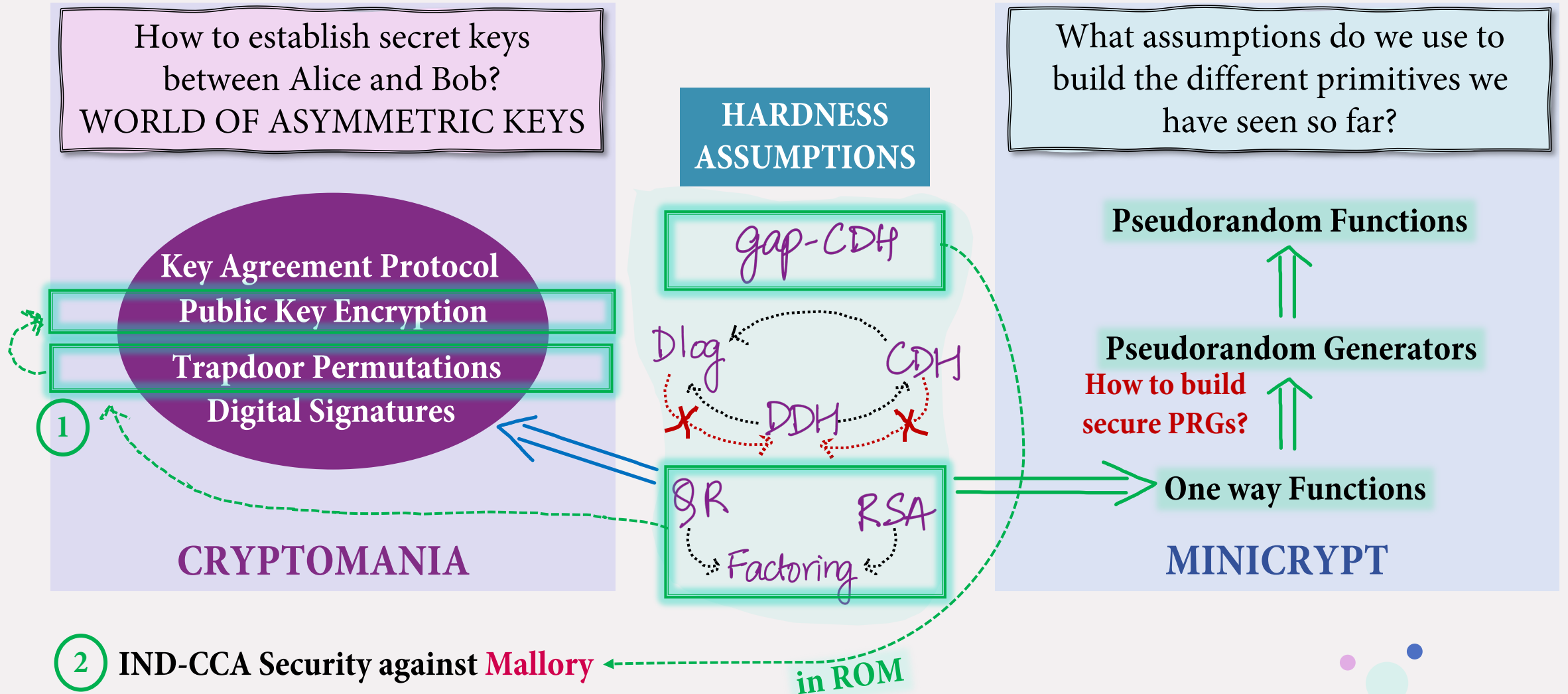


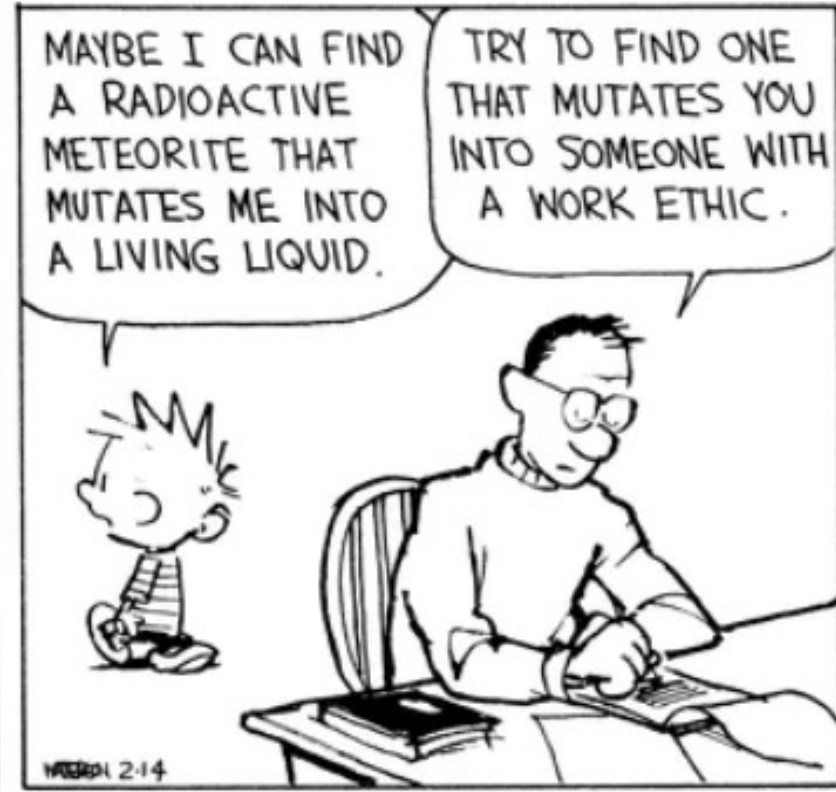
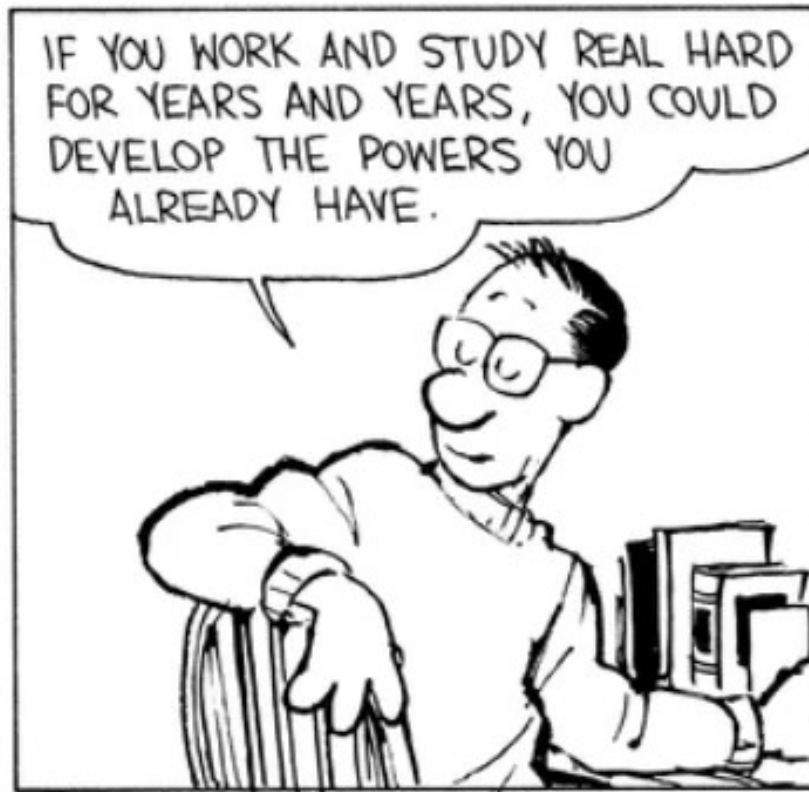
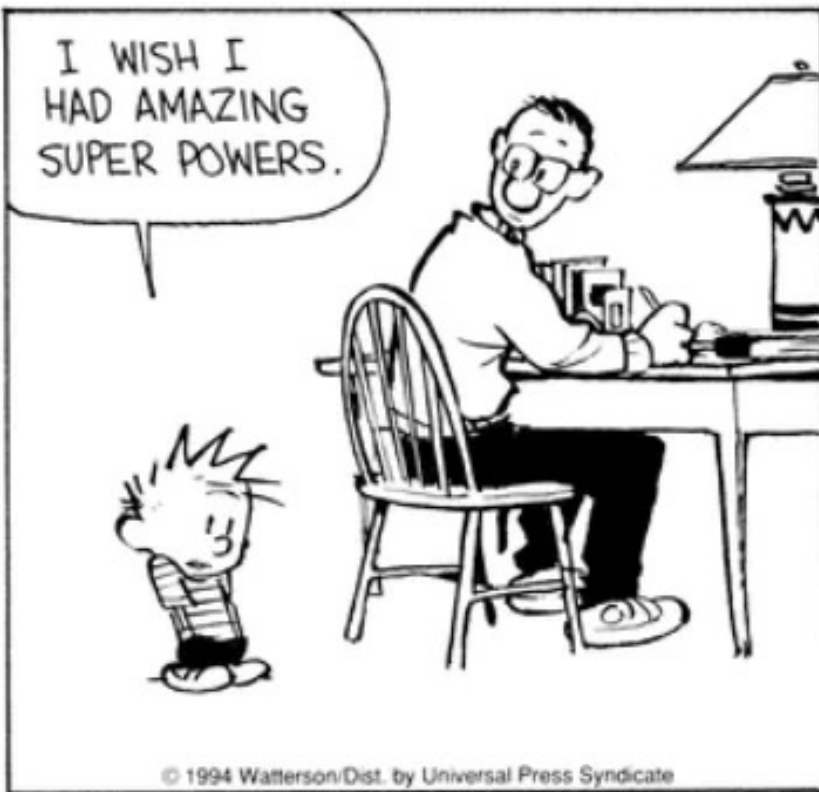
Why?

****This proof is hard, hence you can skip it..**

On the board

Summary





THANK YOU