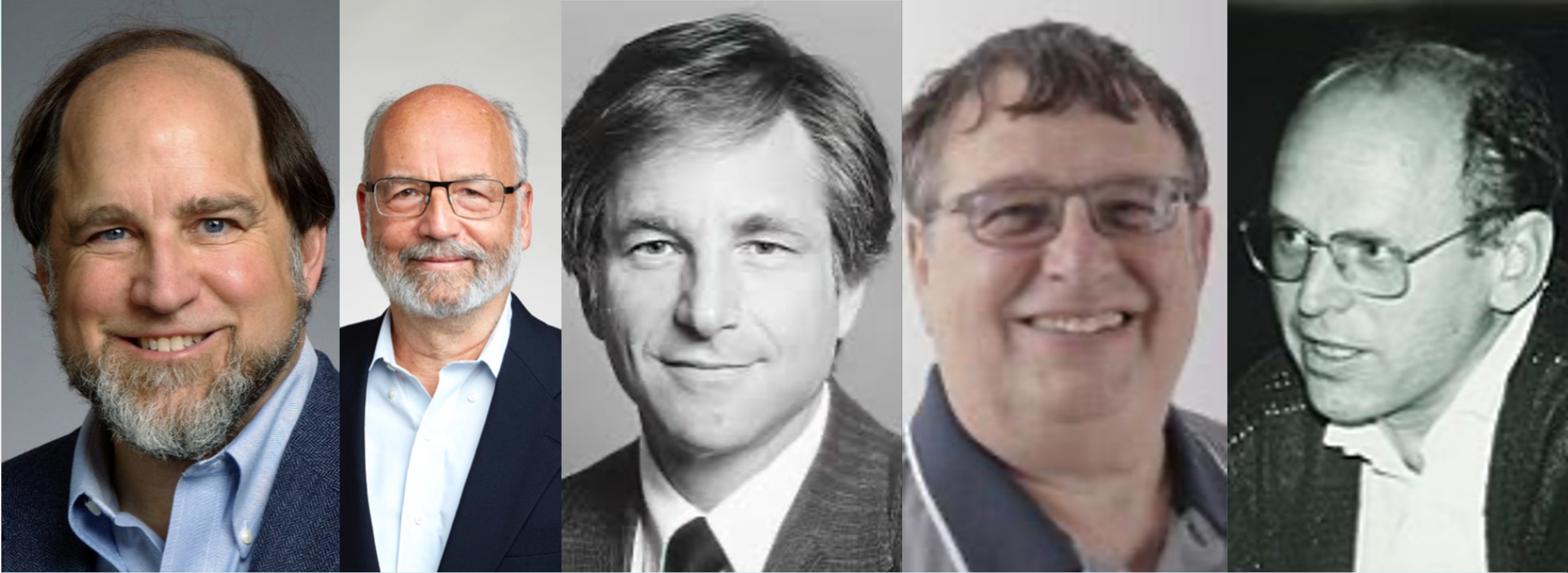


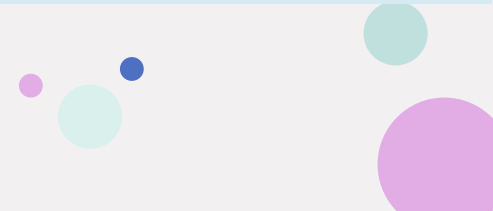


Lecture 17

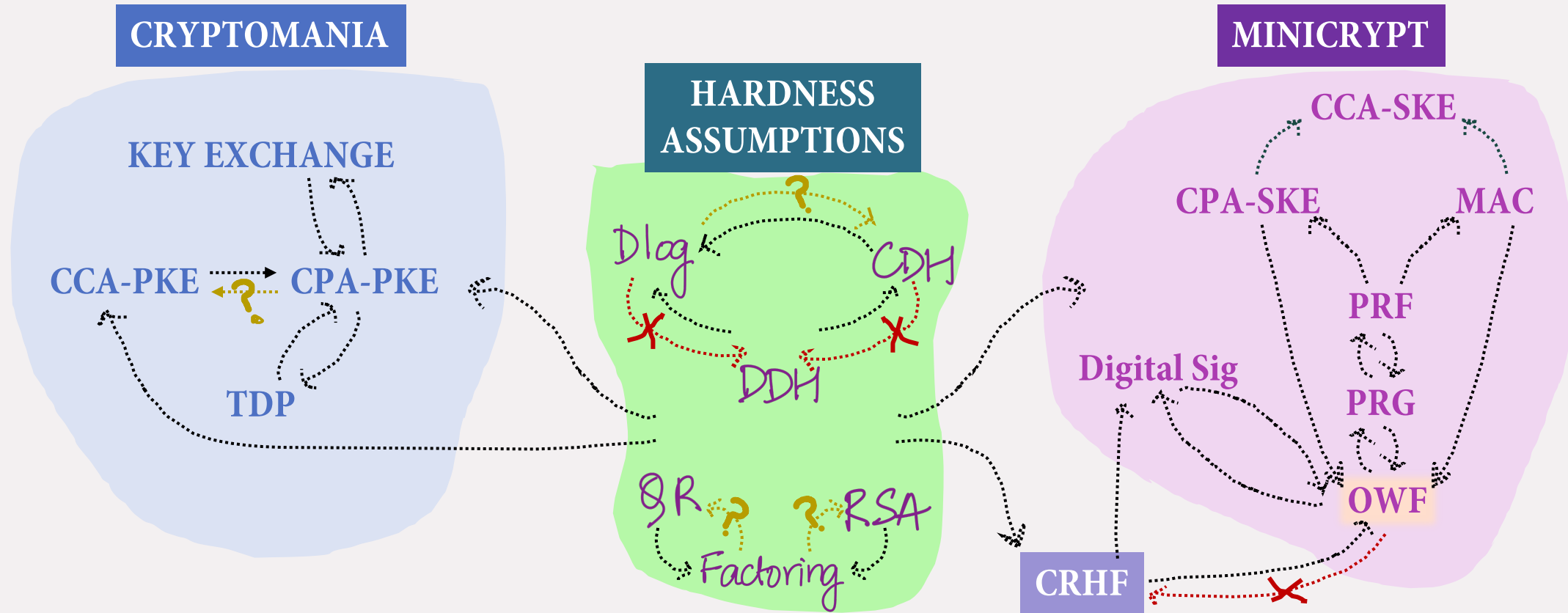
Digital Signatures cont., Identification Schemes, Fiat-Shamir

CS409: Introduction to Cryptography

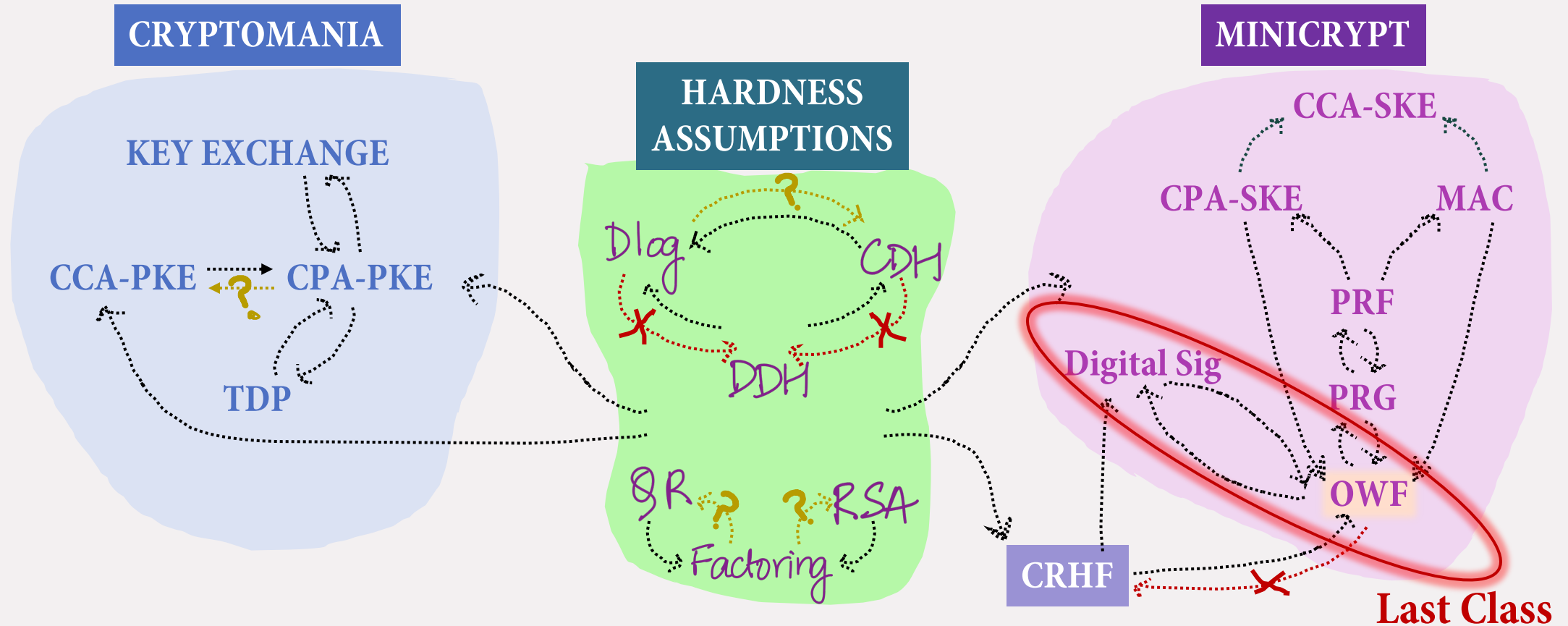
Sruthi Sekar



Big Picture so far



Big Picture so far

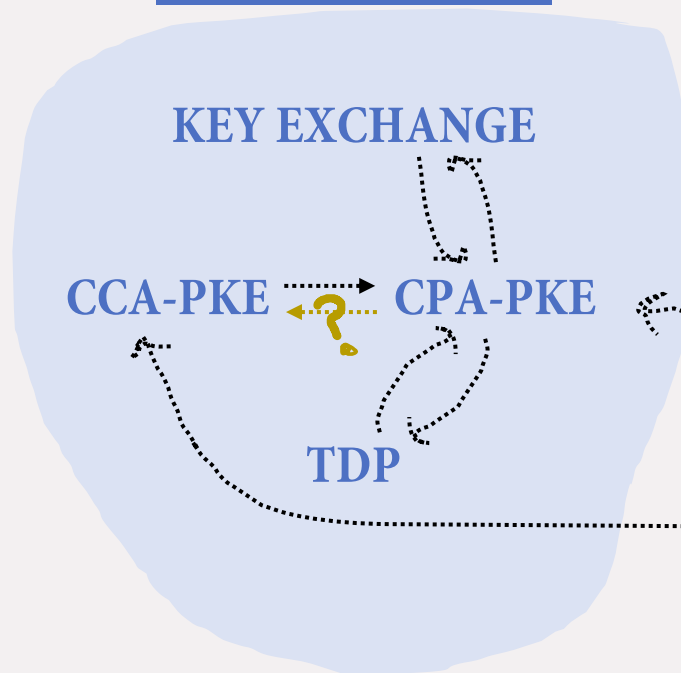


Last Class

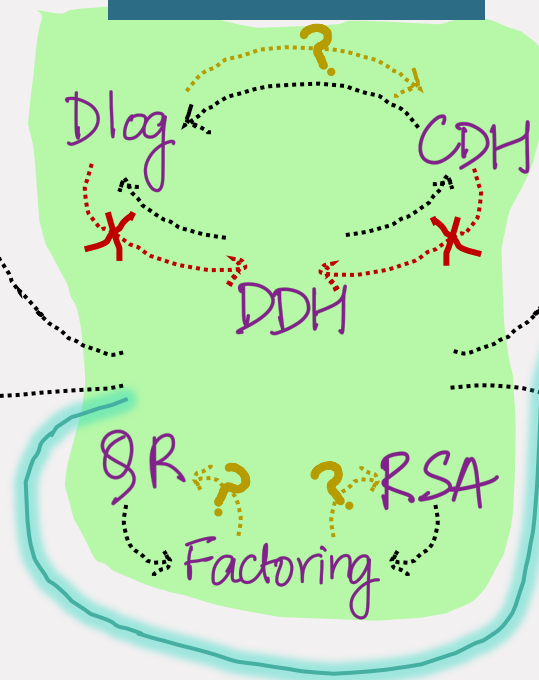
...? open ...X doesn't imply implies

Today

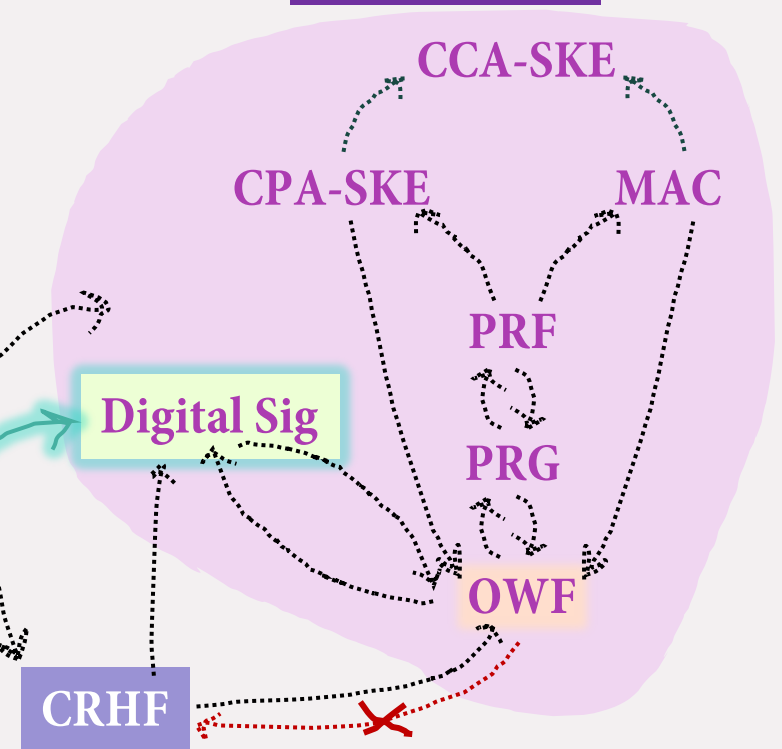
CRYPTOMANIA



HARDNESS ASSUMPTIONS



MINICRYPT



① RSA-based

② Dlog-based: Identification Scheme + Fiat-Shamir

...? open ...X doesn't imply implies

Plain RSA Signature

$\text{GenRSA}(1^n) \rightarrow (N, e, d)$: $N = pq$, $e > 1$ such that $\gcd(e, \varphi(N)) = 1$, $d := e^{-1} \bmod \varphi(N)$
 $\text{pk} = (N, e)$ $\text{sk} = (N, d)$

$\text{Sign}(\text{sk} = (N, d), m)$: compute $\sigma := m^d \bmod N$

$\text{Vrfy}(\text{pk} = (N, e), m, \sigma)$: output 1 if and only if $\sigma^e = m \bmod N$

Plain RSA Signature



SECURE OR NOT?

FORGERY JUST GIVEN pk ?

Yes, pick a random $x \in_R \mathbb{Z}_N^*$ and compute $y = x^e \bmod N$

Output $(m = y, \sigma = x)$



FORGERY ON A TARGET MESSAGE m^* ?



Yes, query $m_1, m_2 = (m^*/m_1) \bmod N$, get $\sigma_1 = m_1^d \bmod N, \sigma_2 = m_2^d \bmod N$

Output $(m^*, \sigma^* = \sigma_1 \sigma_2 \bmod N)$

RSA Full-Domain Hash Signature

Gen(1^n): $\text{GenRSA}(1^n) \rightarrow (N, e, d)$: $N = pq$,
 $e > 1$ such that $\gcd(e, \varphi(N)) = 1$, $d := e^{-1} \bmod \varphi(N)$
 $\text{pk} = (N, e)$ $\text{sk} = (N, d)$

A function $H: \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$ picked by Gen (implicitly)

Sign($\text{sk} = (N, d), m$): compute $\sigma := H(m)^d \bmod N$

Vrfy($\text{pk} = (N, e), m, \sigma$): output 1 if and only if $\sigma^e = H(m) \bmod N$

RSA-FDH Signature



What property from H ?

FORGERY JUST GIVEN pk ?

FORGERY ON A TARGET MESSAGE m^* ?

RSA Full-Domain Hash Signature

Theorem 1: EU-CMA Security of RSA-FDH

If RSA is **hard** relative to GenRSA and H is **modeled** as an RO, then the RSA-FDH is EU-CMA secure.

Proof Sketch: $\exists$ **Mallory** breaking EU-CMA-security of RSA-FDH $\Rightarrow \exists$ **Solver** against **GenRSA**

In RO model

Given: (N, e, y) for
 $(N, e, d) \leftarrow \text{GenRSA}(1^n)$
 and $y \in_R \mathbb{Z}_N^*$

Observations:

- signatures are $\sigma = H(m)^d$
- which means $H(m) = \sigma^e$

If $m' = m_i$ then output σ'
 Else $\perp$

Solver
 (Acts like the RO)

$pk = (N, e)$

$Q^{RO} = \{m_1, m_2, \dots, m_q\}$
 $i \in_R [q]$: to plug challenge

WLOG, assume $m'_j \in Q^{RO} \forall j$

pk

Mallory

RO Queries

$h_i = y$
 $j \neq i: h_j = \sigma_j^e, \sigma_j \in_R \mathbb{Z}_N^*$

Sign Queries

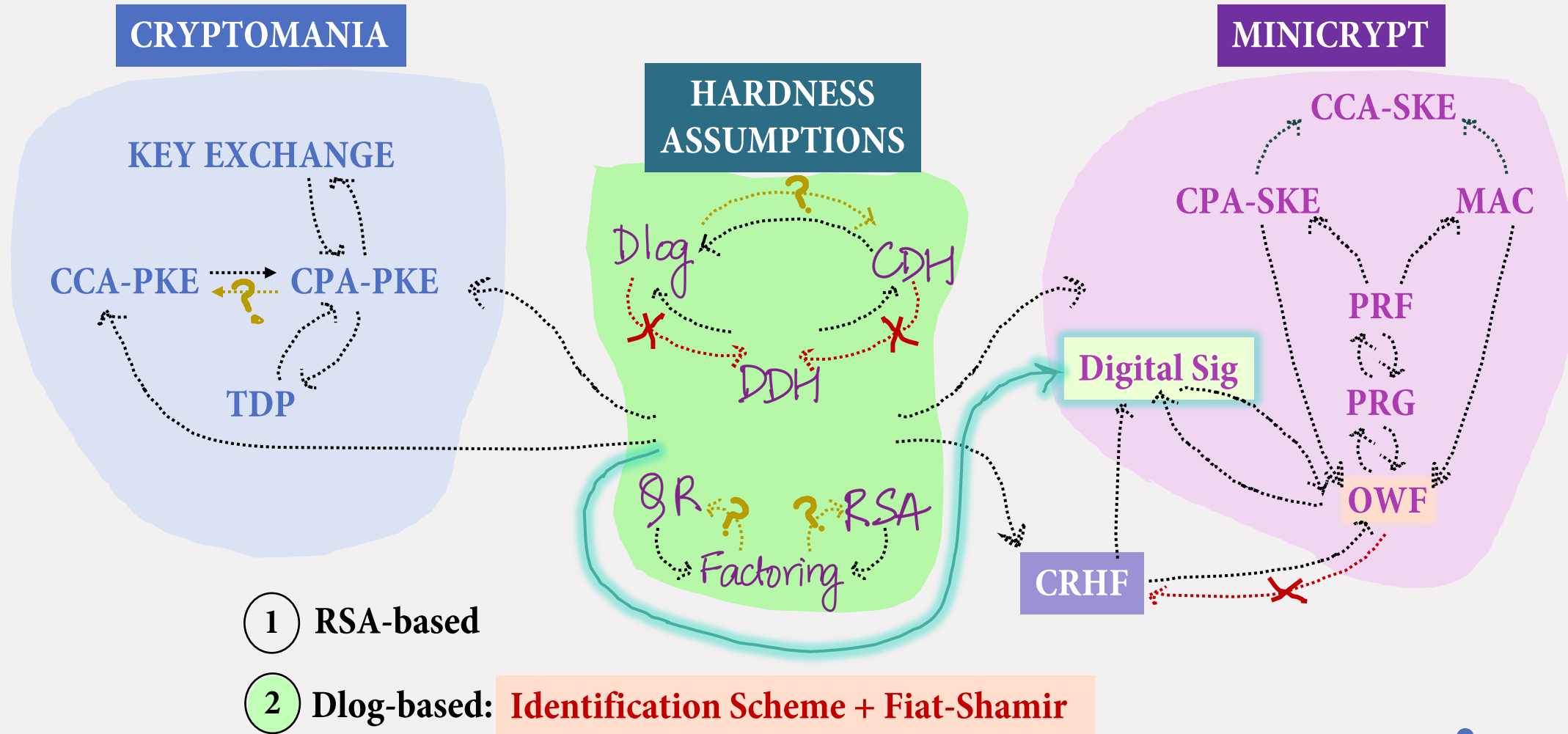
If $j = i: \perp$
 Else σ_j from above

m', σ'

Full analysis: discuss on board

$$\Pr[\text{Solver wins}] = \frac{\Pr[\text{Mallory wins}]}{q}$$

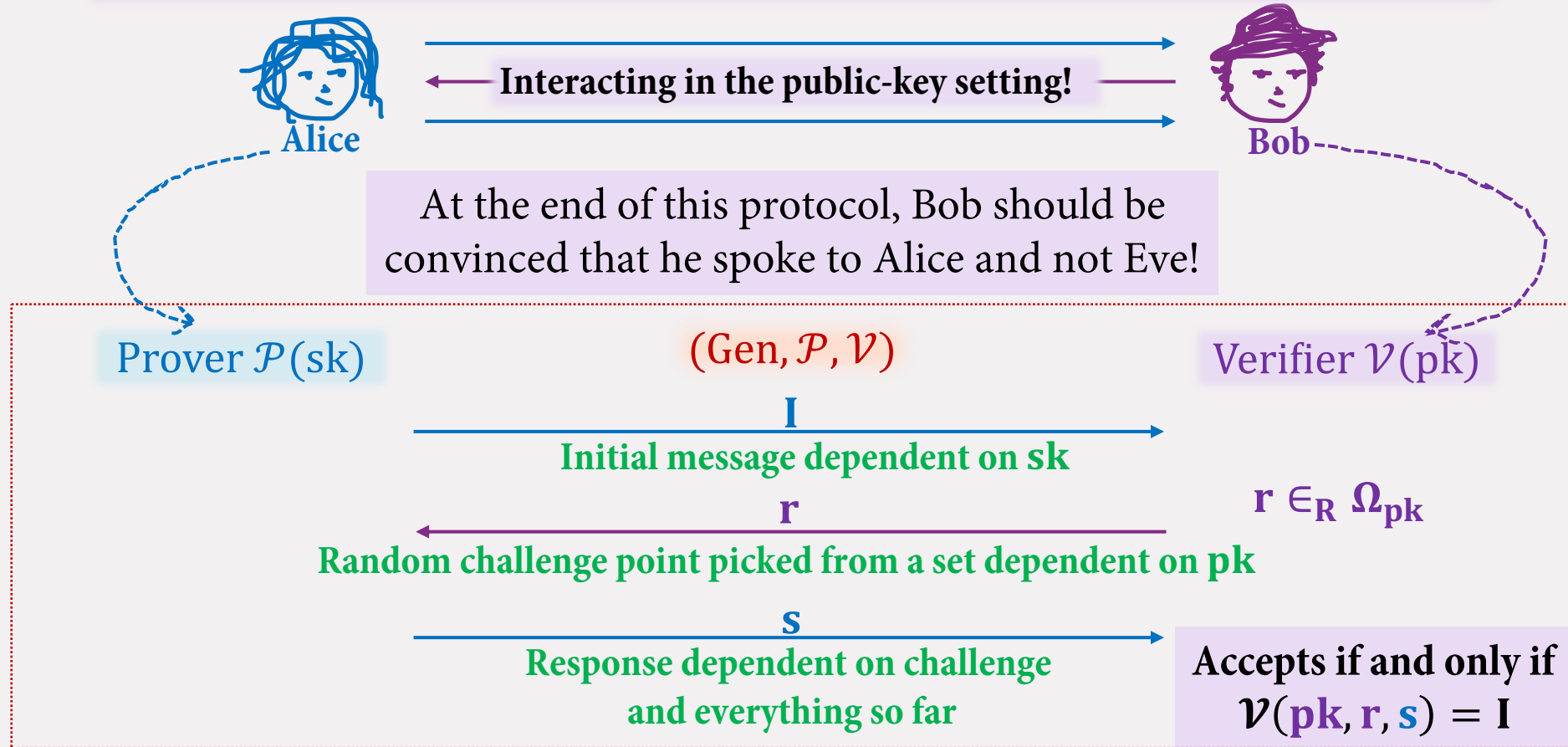
Today



$\cdots \rightarrow$ open $\cdots \nrightarrow$ doesn't imply $\cdots \rightarrow$ implies

Identification Protocol

How does Alice identify (authenticate) herself in her communication with Bob?

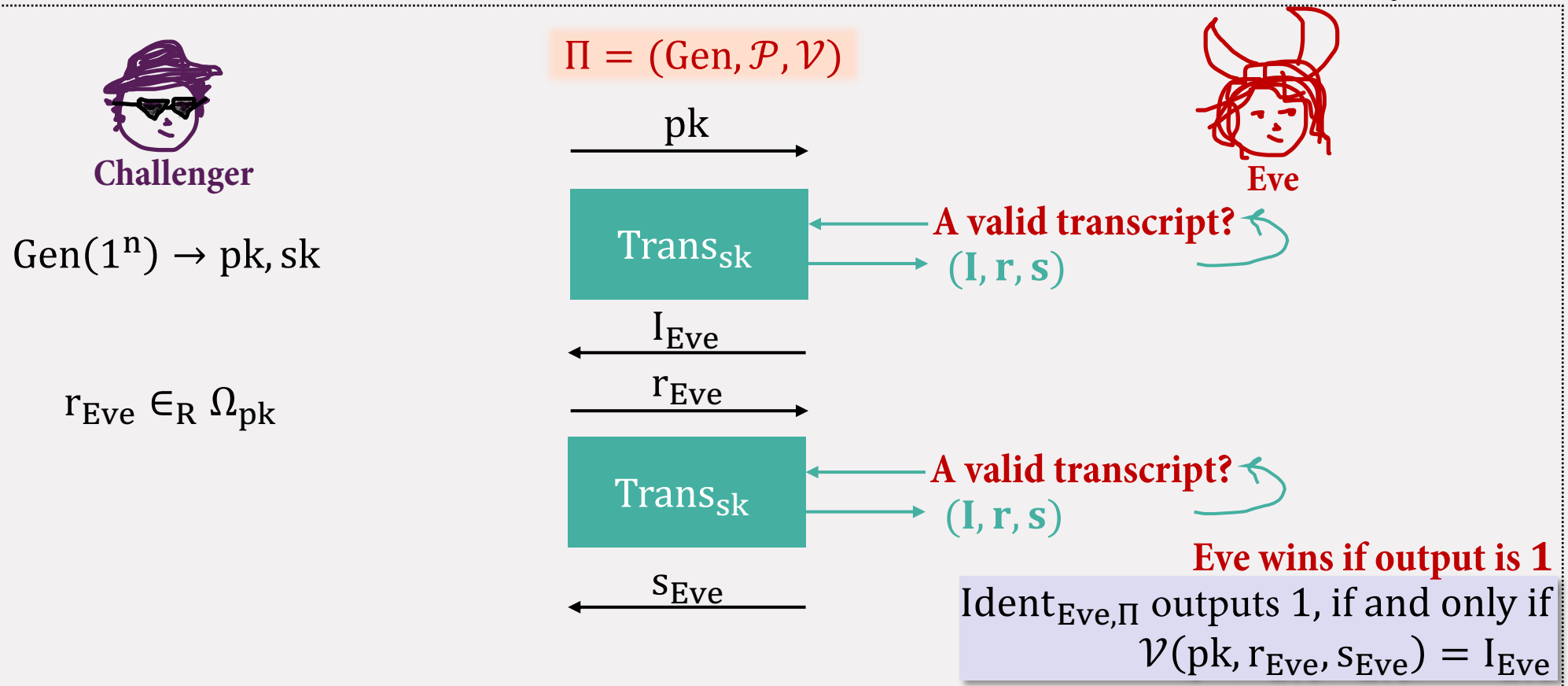


A three-round identification scheme



Security? Eve watching the transcript (many times also), should not fool Bob!

Identification Protocol: Security



Definition 1 (Identification scheme)

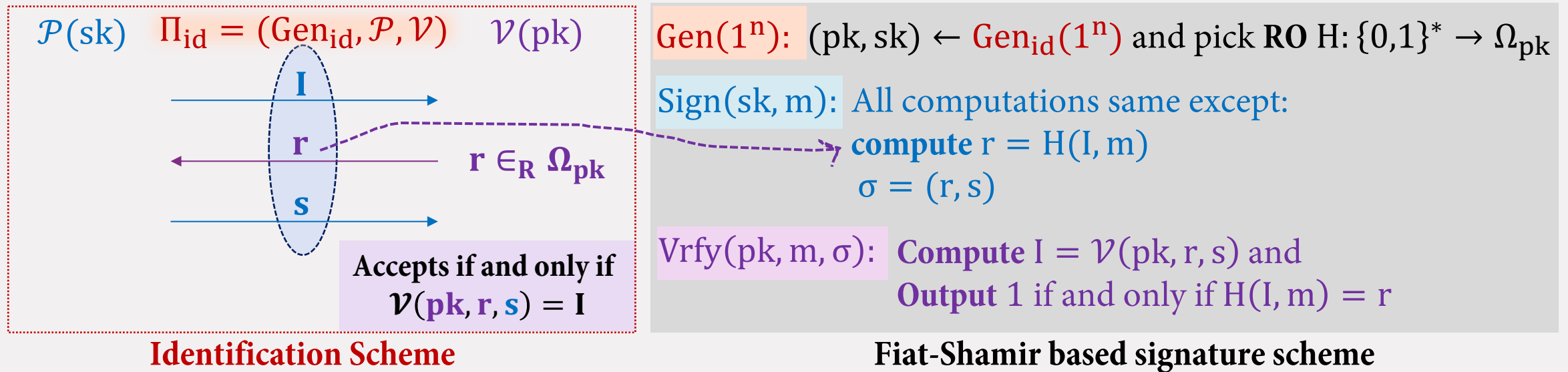
An identification scheme Π is **secure against a passive attack** if, for all **PPT Eve**, $\exists$ negligible **negl**: $\forall n$

$$\Pr[\text{Ident}_{\text{Eve}, \Pi}(n) = 1] \leq \text{negl}(n)$$

Identification to Signatures



FIAT-SHAMIR: Replace the verifier with a random oracle H , and Sign is just the prover algorithm.



Theorem 2: Fiat-Shamir gives EU-CMA secure DS

If Π_{id} is a secure identification scheme and H is modeled as an RO, then $(\text{Gen}, \text{Sign}, \text{Vrfy})$ is EU-CMA secure

****Proof is advanced! If interested, see Katz and Lindell, second edition, Theorem 12.10.**

Schnorr Identification Scheme

Discrete Log Assumption (RECALL)

The **discrete log problem is hard relative to $\mathcal{G}$** if for all PPT **Logan**, there exists a negligible negl s.t. $\forall n$

$$\Pr_{\substack{\mathcal{G}(1^n) \rightarrow \mathbb{G}, q, g \\ h \in_R \mathbb{G}}} [\mathbf{Logan}(\mathbb{G}, q, g, h) \rightarrow x \text{ such that } x \in \mathbb{Z}_q \wedge g^x = h] \leq \text{negl}(n)$$



Alice

Alice wants to use her ElGamal keys and convince Bob that he is talking to her and not Eve!



Bob

$$\begin{aligned} \text{pk}_{\text{Elgamal}} &= g^x \\ \text{sk}_{\text{Elgamal}} &= x \end{aligned}$$

$\xrightarrow{\text{pk}_{\text{Elgamal}}}$
and proof that she “knows” the x corresponding to $\text{pk}_{\text{Elgamal}}$

This proof should convince Bob!

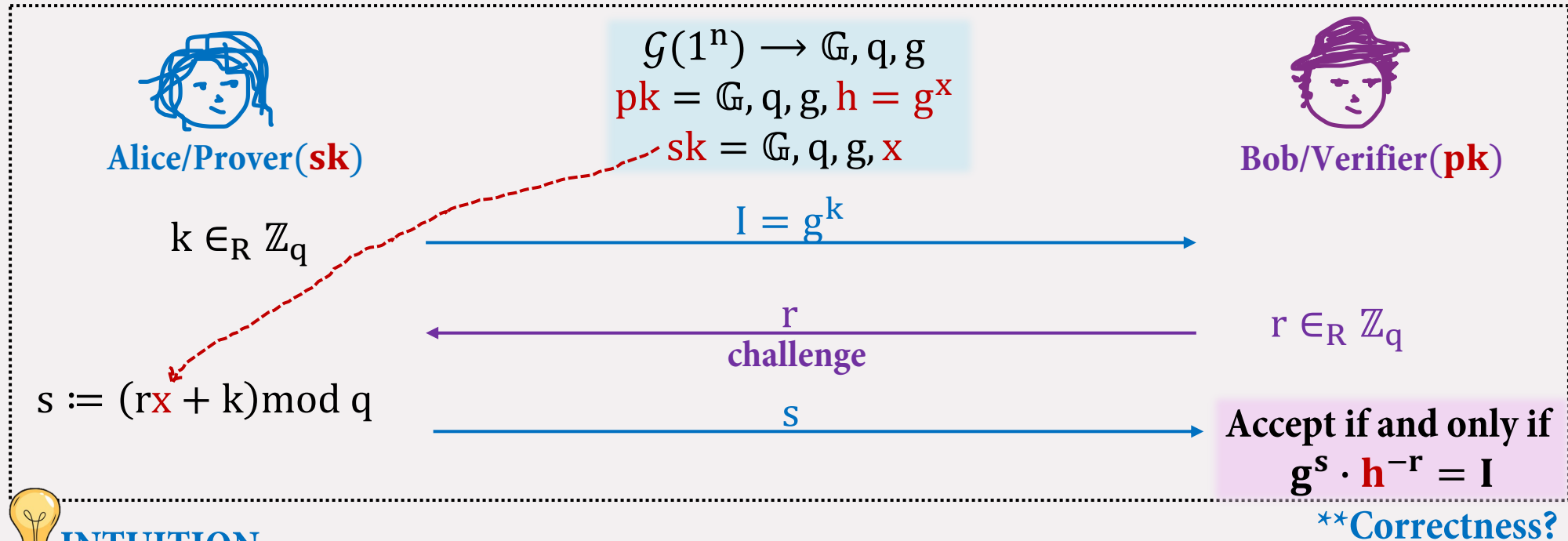
Proof of Knowledge

- This proof is something **Eve, the impersonator, shouldn't** be able to give and **convince Bob!**
- This proof **should not reveal x** itself (otherwise, all security is lost!)

Zero-knowledge proof

*** Next few lectures

Schnorr Identification Scheme



INTUITION



Can impersonator Eve compute the response s (correctly) without knowing $\mathbf{x}$?



Is the interaction revealing the secret $\mathbf{x}$?

No, Why?

Real transcript

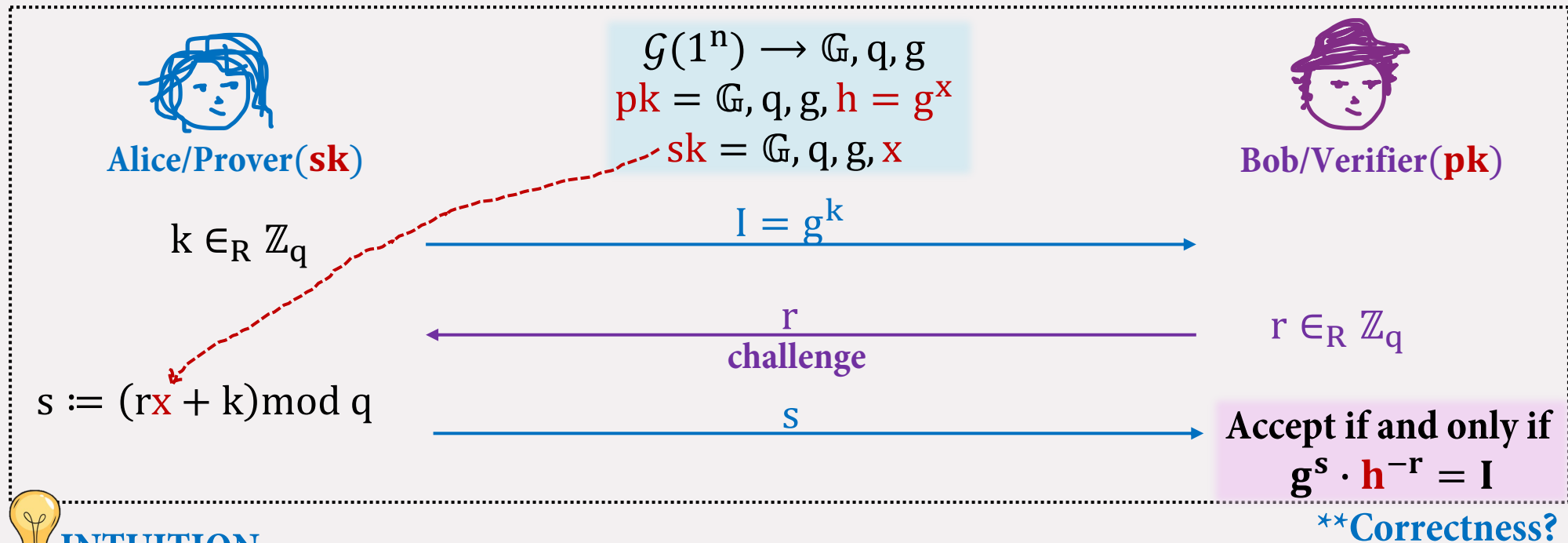
$r \in_R \mathbb{Z}_q$
 $(g^k, r, s = rx + k \bmod q)$

$\approx$

Simulated transcript

$r, s \in_R \mathbb{Z}_q$
Output: $(g^s \cdot \mathbf{h}^{-r}, r, s)$

Schnorr Identification Scheme



INTUITION



Can impersonator Eve compute the response s (correctly) without knowing $\mathbf{x}$?

Is the interaction revealing the secret $\mathbf{x}$?

Given pk , Eve sends some I , gets r , and can correctly respond with s such that $g^s \cdot \mathbf{h}^{-r} = I$

$\Rightarrow$ Eve could compute correct s_1, s_2 for at least two different r_1, r_2 , i.e.,
 $g^{s_1} \mathbf{h}^{-r_1} = g^{s_2} \mathbf{h}^{-r_2}$

$\Rightarrow$ Eve can implicitly compute $\mathbf{x} = (s_1 - s_2)(r_1 - r_2)^{-1} \bmod q$

Schnorr Identification: Security

Theorem 3: Dlog implies security of Schnorr

If **Dlog** is hard relative to $\mathcal{G}$, then the Schnorr identification scheme is secure against **Eve**.

Proof Sketch: $\exists$ **Eve** against Schnorr $\Rightarrow$ **Logan** against **Dlog**

Challenge: $(\mathbb{G}, q, g), h$
for $h \in_R \mathbb{G}$

Logan

Set $pk = ((\mathbb{G}, q, g), h)$

SimTrans:

$r, s \in_R \mathbb{Z}_q$
set $I = g^s \cdot h^{-r}$

$r_{\text{Eve}} \in_R \mathbb{Z}_q$

$r_{\text{Eve}}^* \in_R \mathbb{Z}_q$

◀◀ Rewind and re-run Eve to get
her response on one more r_{Eve}^*

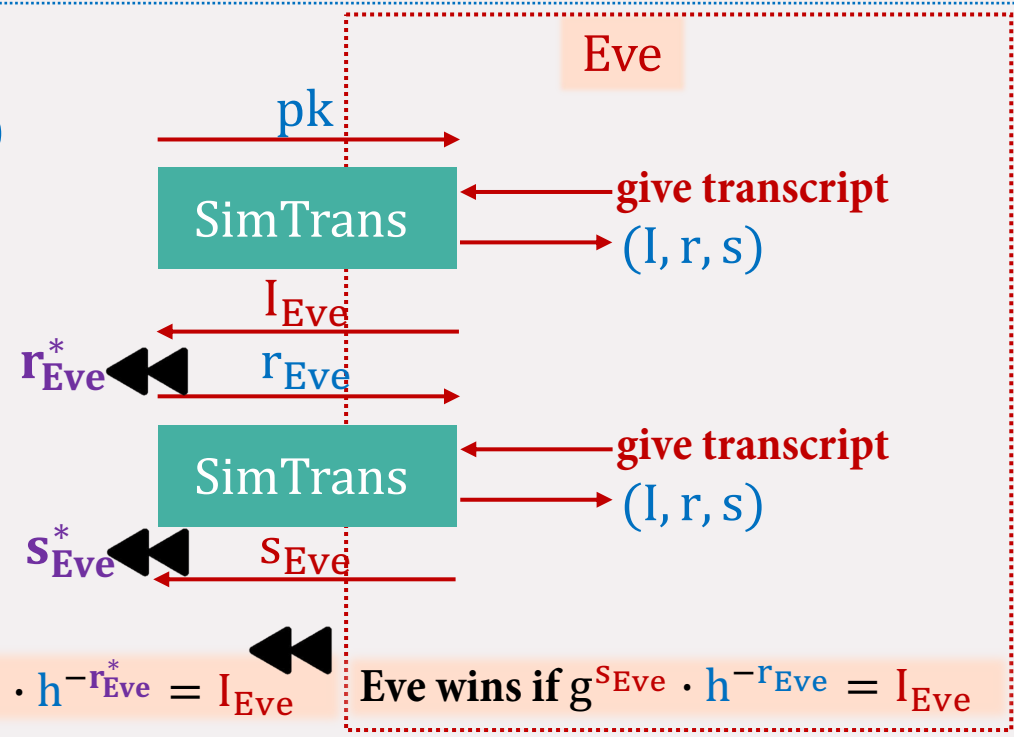
Output:

$[(s_{\text{Eve}} - s_{\text{Eve}}^*)(r_{\text{Eve}} - r_{\text{Eve}}^*)^{-1} \bmod q]$

Eve wins if $g^{s_{\text{Eve}}^*} \cdot h^{-r_{\text{Eve}}^*} = I_{\text{Eve}}$

Eve wins if $g^{s_{\text{Eve}}} \cdot h^{-r_{\text{Eve}}} = I_{\text{Eve}}$

$\Pr[\text{Logan wins}] \geq (\Pr[\text{Eve wins}])^2 - 1/q$ winning in both events $r_{\text{Eve}} \neq r_{\text{Eve}}^*$ (otherwise useless)



Schnorr Signature

Gen(1^n): $\mathcal{G}(1^n) \rightarrow \mathbb{G}, q, g$ A function $H: \{0,1\}^* \rightarrow \mathbb{Z}_q$ picked by Gen (implicitly)

$x \in_R \mathbb{Z}_q$ and set $y = g^x$

$pk = (\mathbb{G}, q, g, h), sk = (\mathbb{G}, q, g, x)$

Sign(sk, m): choose $k \in_R \mathbb{Z}_q$, set $I = g^k$, compute $r = H(I, m)$, and $s := rx + k \bmod q$

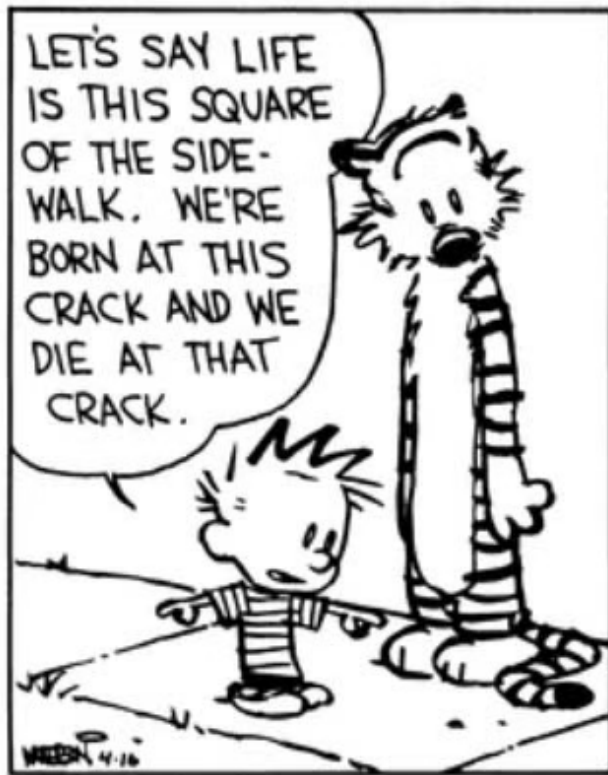
output $\sigma = (r, s)$

Vrfy(pk, m, σ): output 1 if and only if $H(g^s \cdot h^{-r}, m) = r$

Schnorr Signature

Schnorr Identification Protocol + Fiat-Shamir transform

READING EXERCISE: Another **Dlog-based** widely used signature is **DSA**: [Katz-Lindell, 12.5.2]



IS OUR QUICK EXPERIENCE HERE POINTLESS? DOES ANYTHING WE SAY OR DO IN HERE REALLY MATTER? HAVE WE DONE ANYTHING IMPORTANT? HAVE WE BEEN HAPPY? HAVE WE MADE THE MOST OF THESE PRECIOUS FEW FOOTSTEPS??



THANK YOU