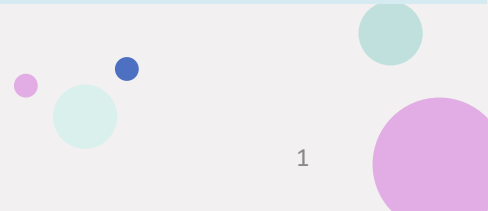




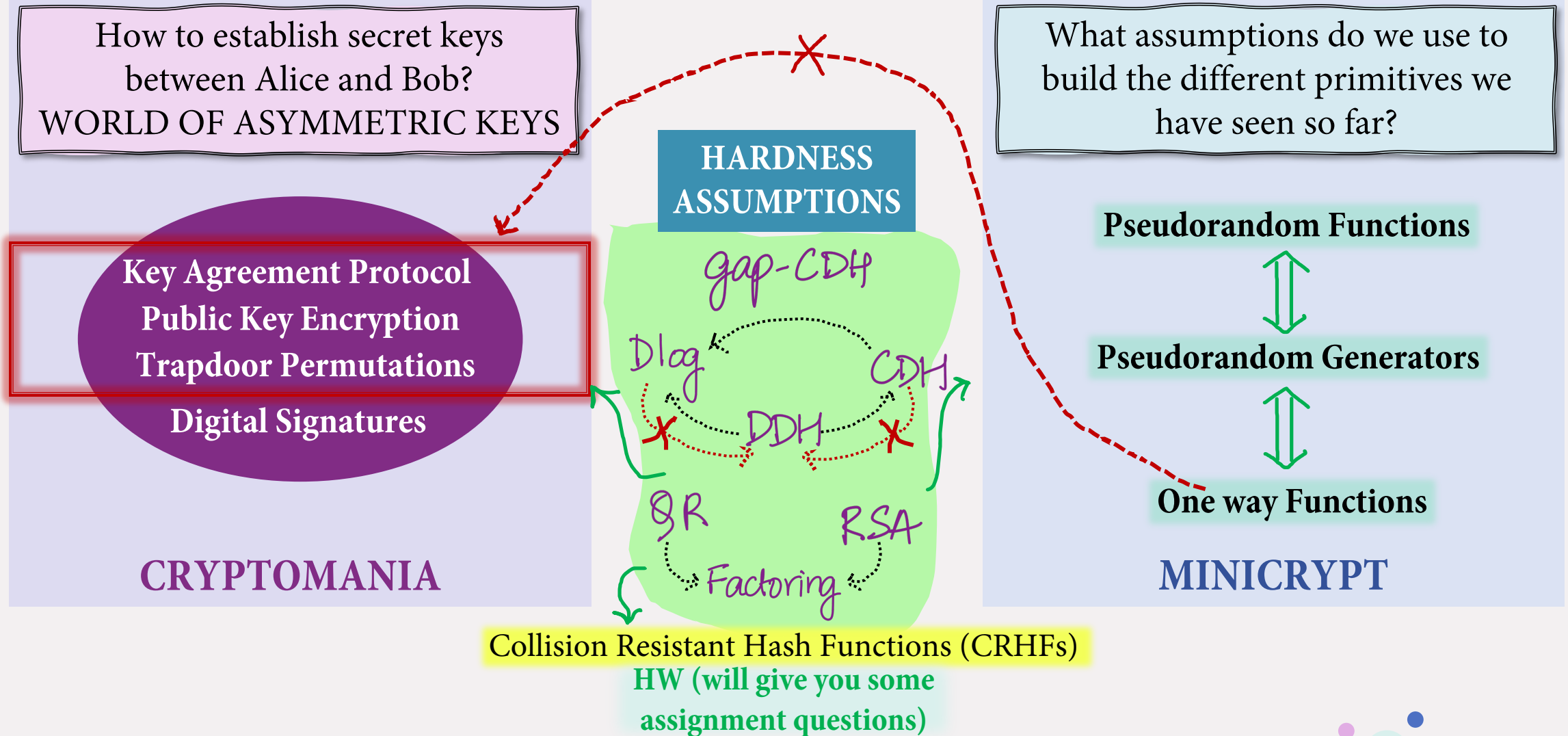
Lecture 17

Digital Signatures

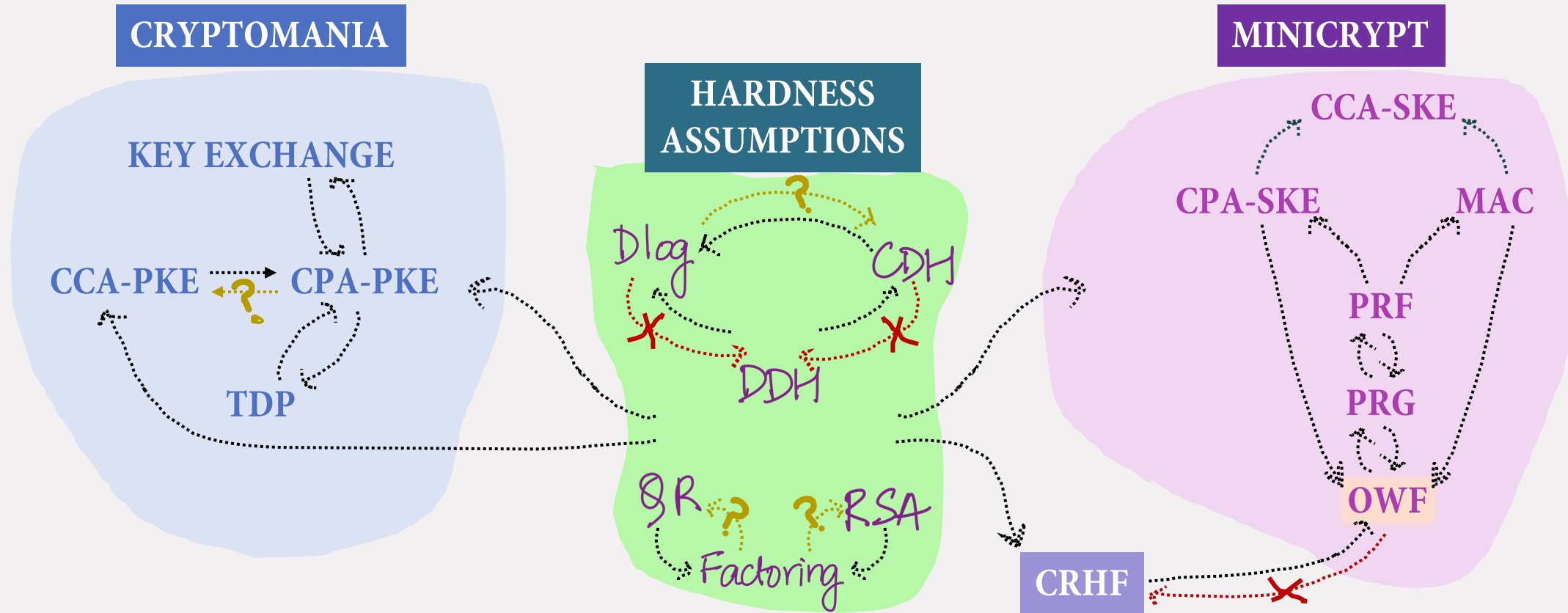
CS409/6011: Introduction to Cryptography
Sruthi Sekar



Big Picture so far

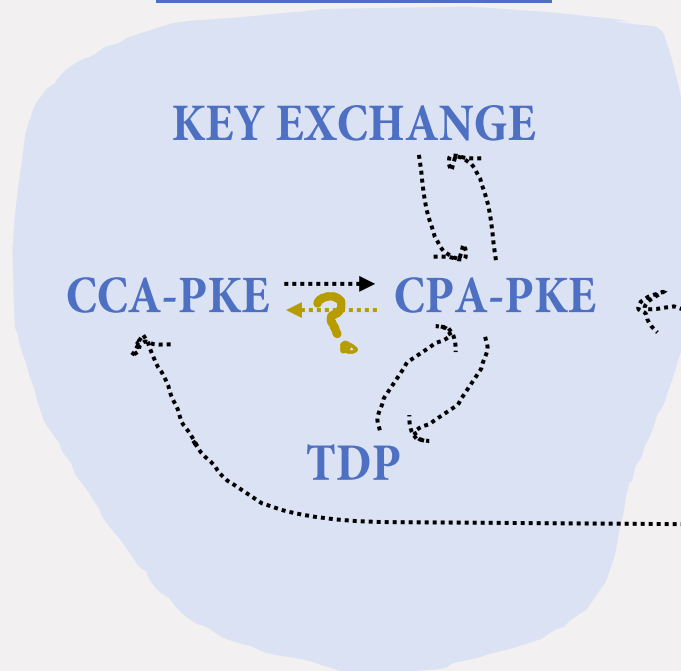


Big Picture so far

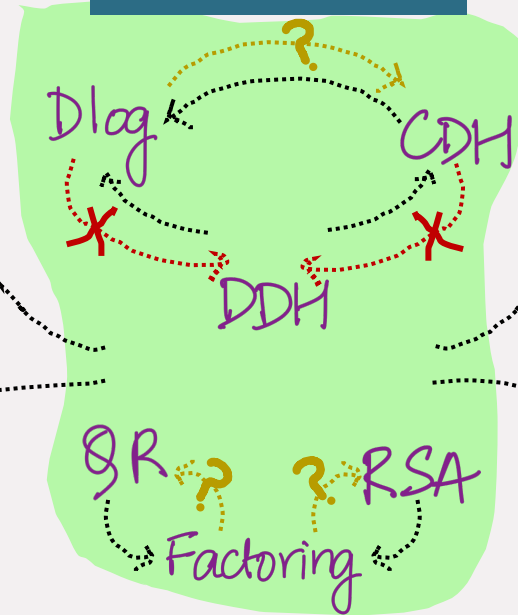


Today

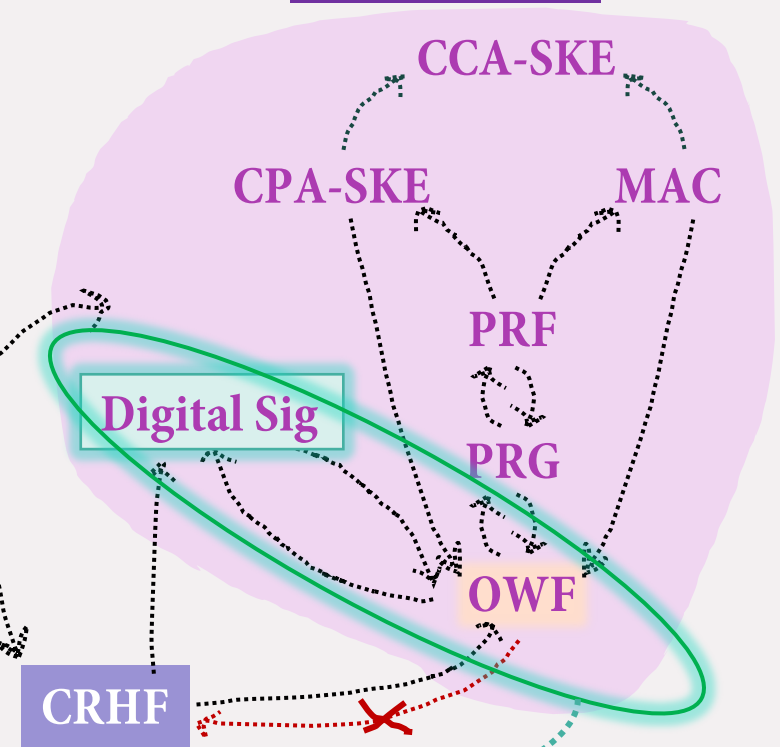
CRYPTOMANIA



HARDNESS ASSUMPTIONS



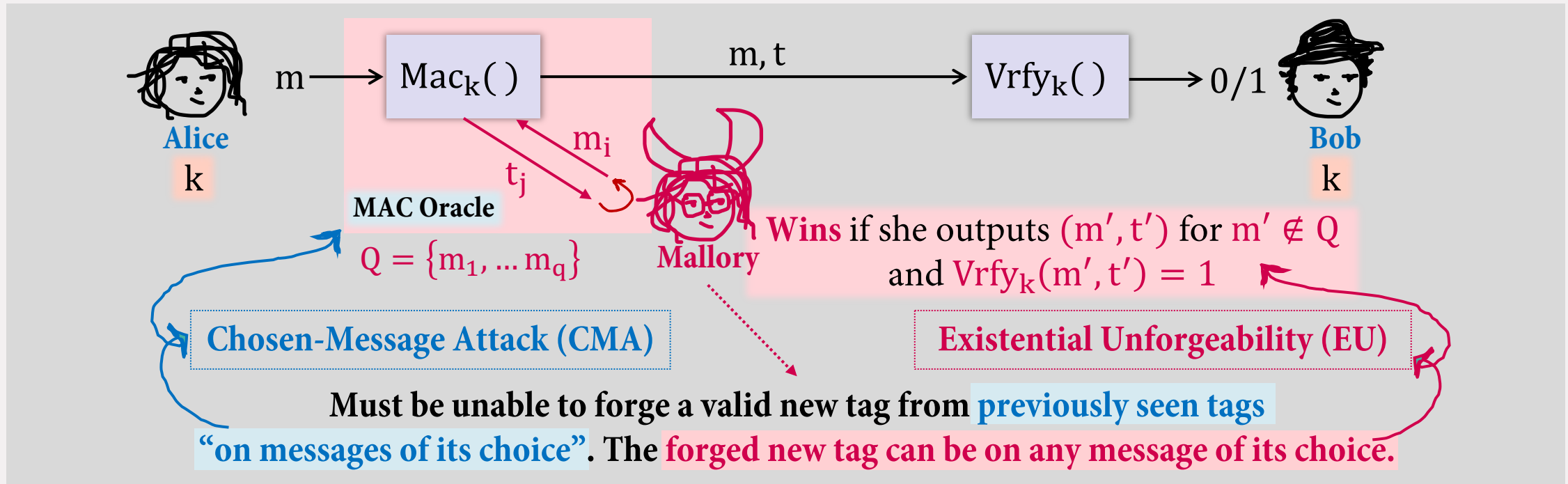
MINICRYPT



- ① Lamport Signature (For fixed-length messages)
- ② For arbitrary-length messages $\left[\textcircled{1} + \text{CRHF} \right]$

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

Recall: Message Authentication Codes

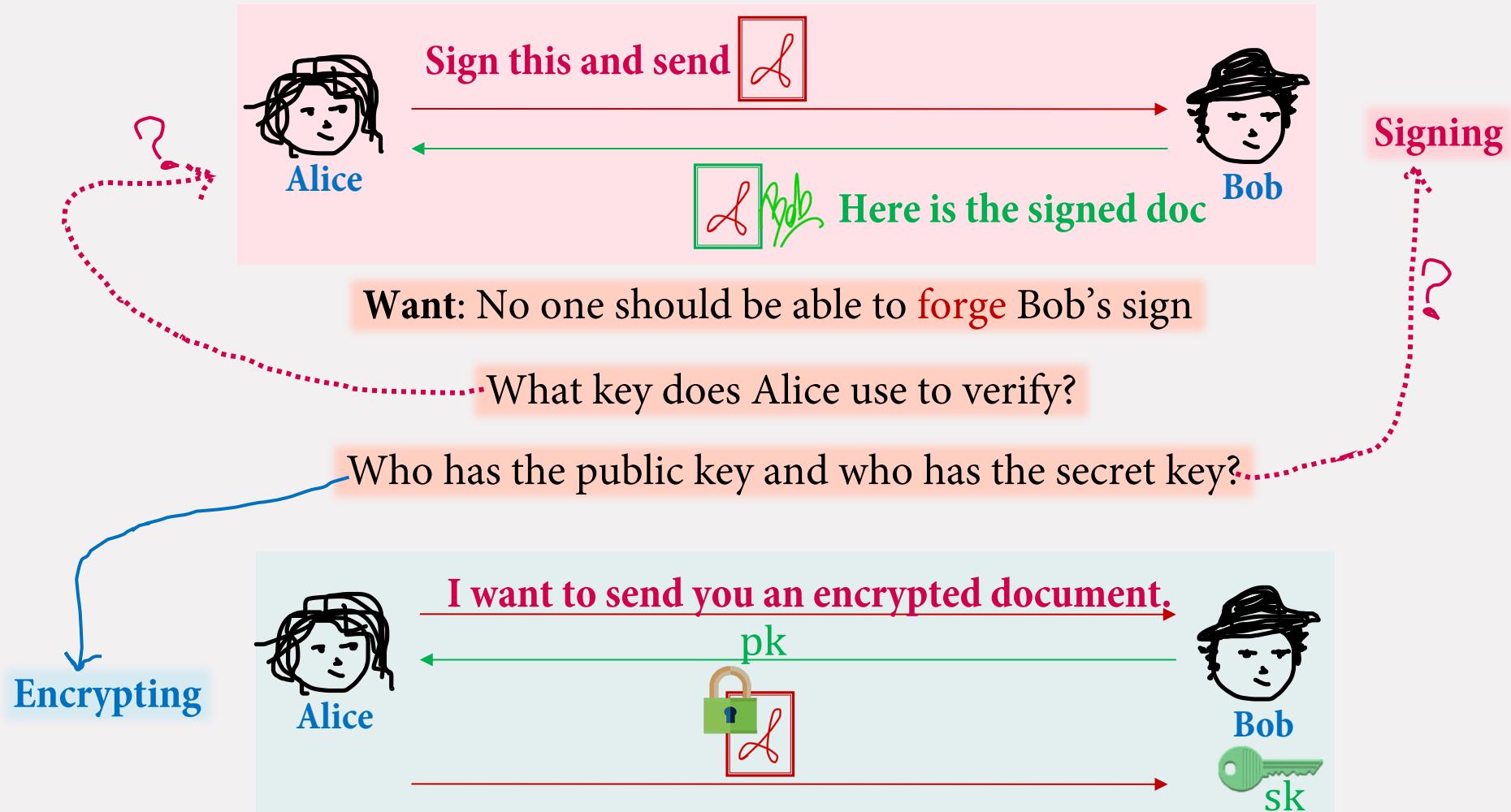


SYMMETRIC WORLD

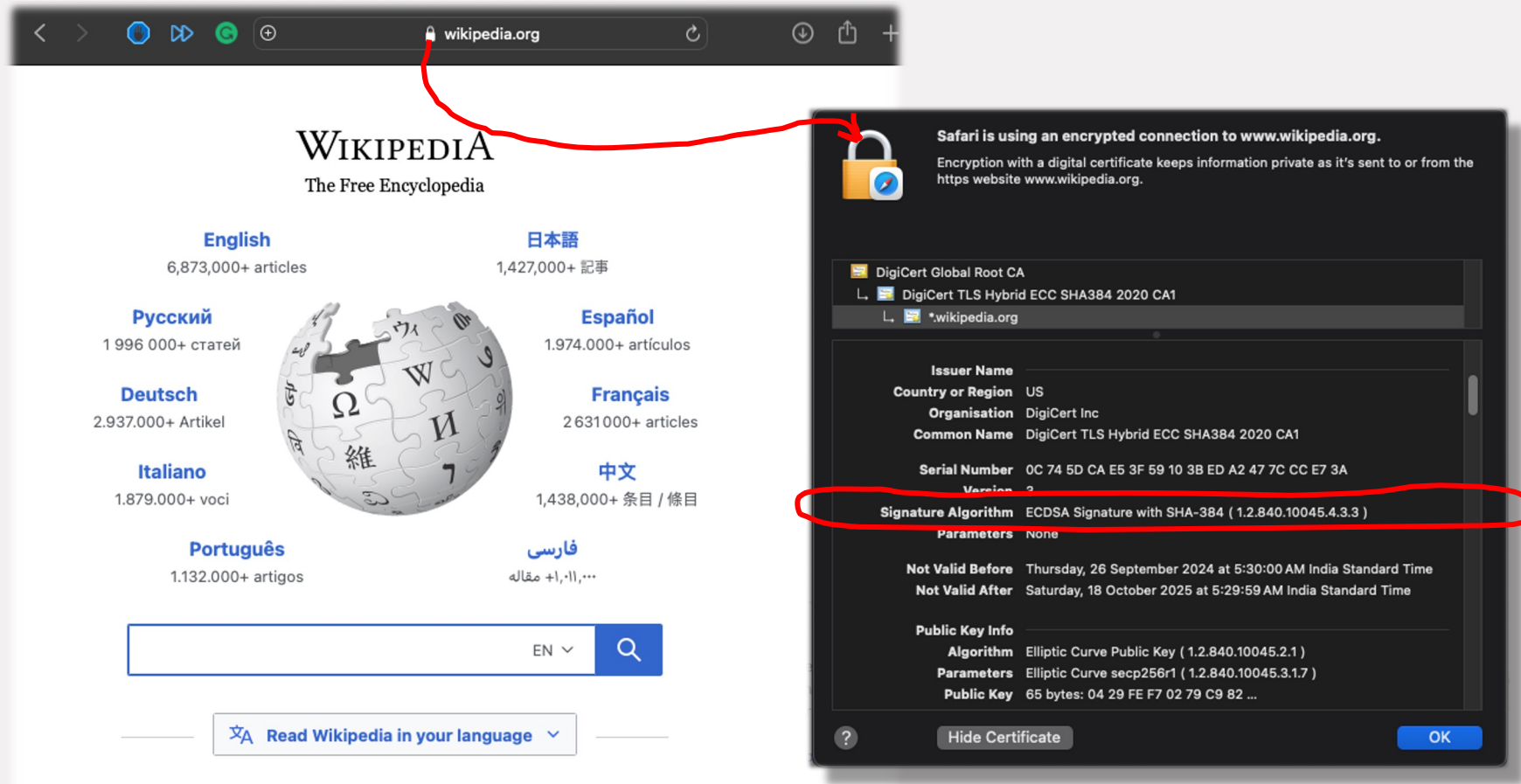
THE PUBLIC-KEY WORLD



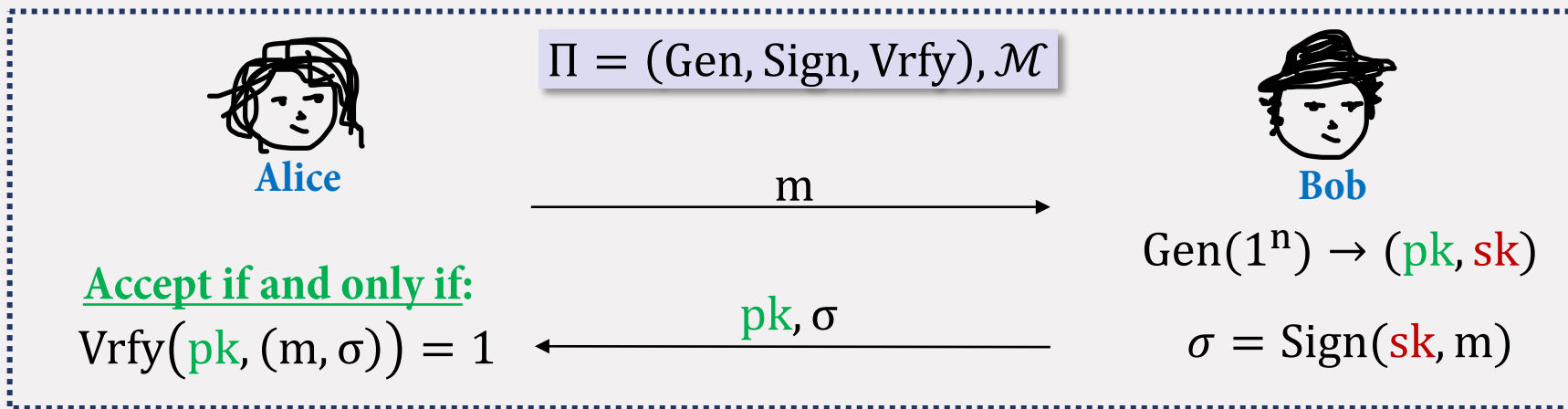
Public-key Analogue of MACs



Digital Signatures in Action



Digital Signatures: Syntax



Digital Signature Scheme (Correctness)

$$\Pr[\text{Vrfy}(\text{pk}, (m, \text{Sign}(\text{sk}, m))) = 1] = 1$$

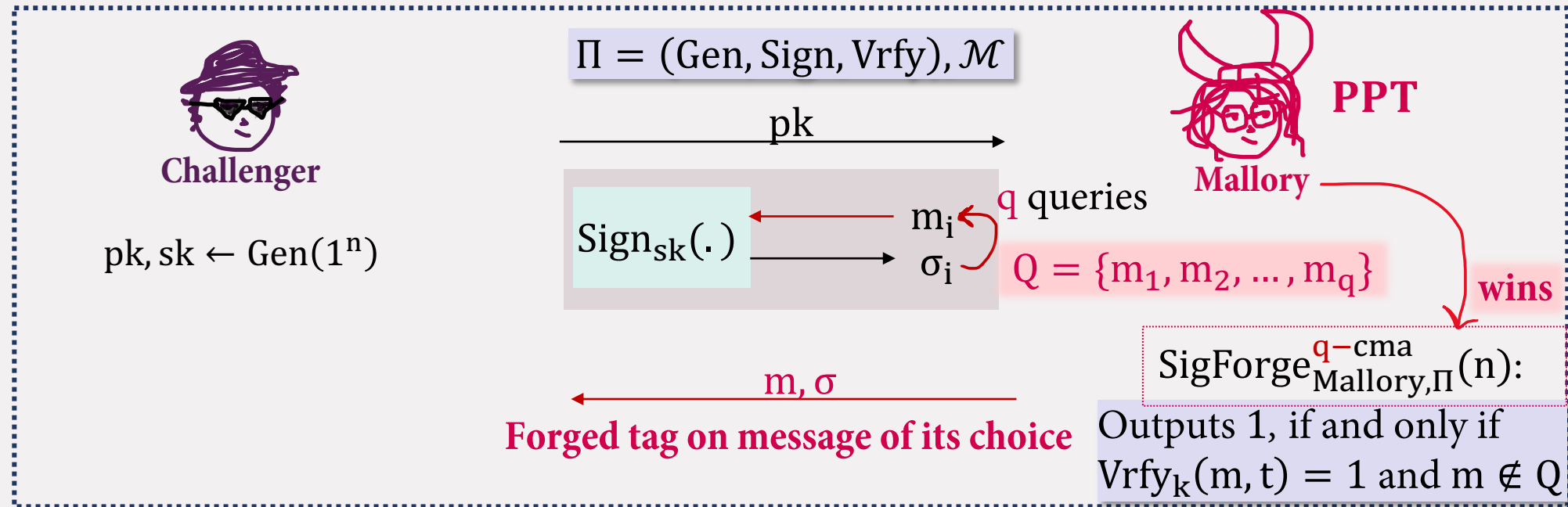
Security? 

Mallory must be unable to forge a valid new tag from previously seen tags “on messages of its choice”. The forged new tag can be on any message of its choice.

Chosen-Message Attack (CMA)

Existential Unforgeability (EU)

EU-CMA Security of Digital Signatures



Definition 1 (EU-CMA Security of Digital Signatures)

A digital signature scheme $\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$ is **existentially unforgeable under a chosen-message attack** if for all PPT **Mallory** (q queries), there exists a negligible negl such that $\forall n$:

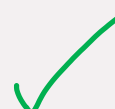
$$\Pr \left[\text{SigForge}_{\text{Mallory}, \Pi}^{q\text{-cma}}(n) = 1 \right] \leq \text{negl}(n)$$

Quiz Time

EU-CMA secure or not? $\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$ be EU-CMA secure

Truncate-then-sign : $\text{Sign}'(\text{sk}, m = m_1 \dots m_{\ell-1} m_{\ell}) := \text{Sign}(\text{sk}, m_1 \dots m_{\ell-1})$ $\text{Vrfy}'(\text{pk}, m, \sigma) := \text{Vrfy}(\text{pk}, m_1 \dots m_{\ell-1}, \sigma)$ 

Sign-then-truncate :

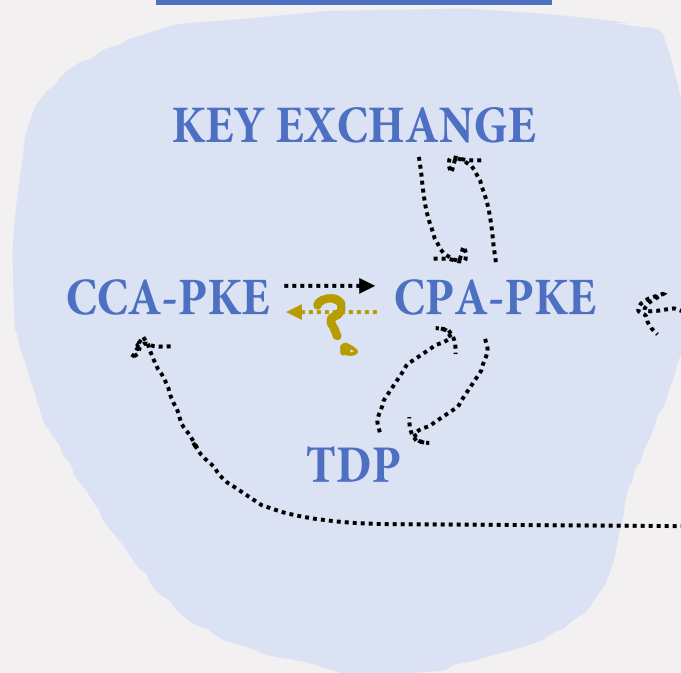
$\text{Sign}'(\text{sk}, m) := \sigma_1 \dots \sigma_{s-1},$ where $\sigma_1 \dots \sigma_{s-1} \sigma_s \leftarrow \text{Sign}(\text{sk}, m)$ 
 $\text{Vrfy}'(\text{pk}, m, \sigma') := \text{accept if } \text{Vrfy}(\text{pk}, m, \sigma'0) = 1 \text{ or } \text{Vrfy}(\text{pk}, m, \sigma'1) = 1$

Sign-then-append : $\text{Sign}'(\text{sk}, m) := \sigma 0,$ where $\sigma \leftarrow \text{Sign}(\text{sk}, m)$ 
 $\text{Vrfy}'(\text{pk}, m, \sigma b) := \text{Vrfy}(\text{pk}, m, \sigma)$

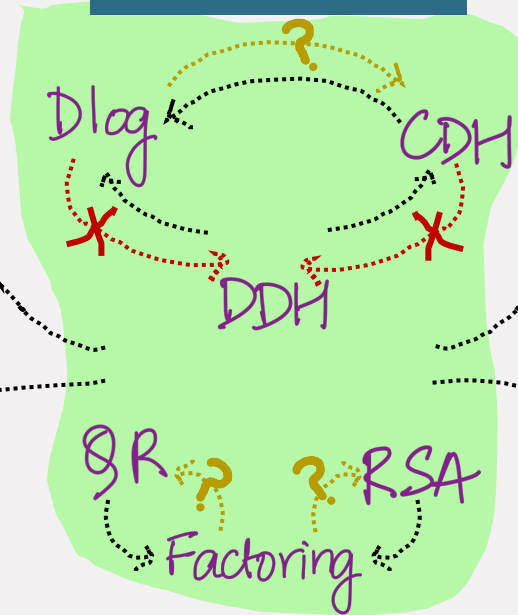
HW 1: Prove by reduction that sign-then truncate and sign-then-append are secure!

Today

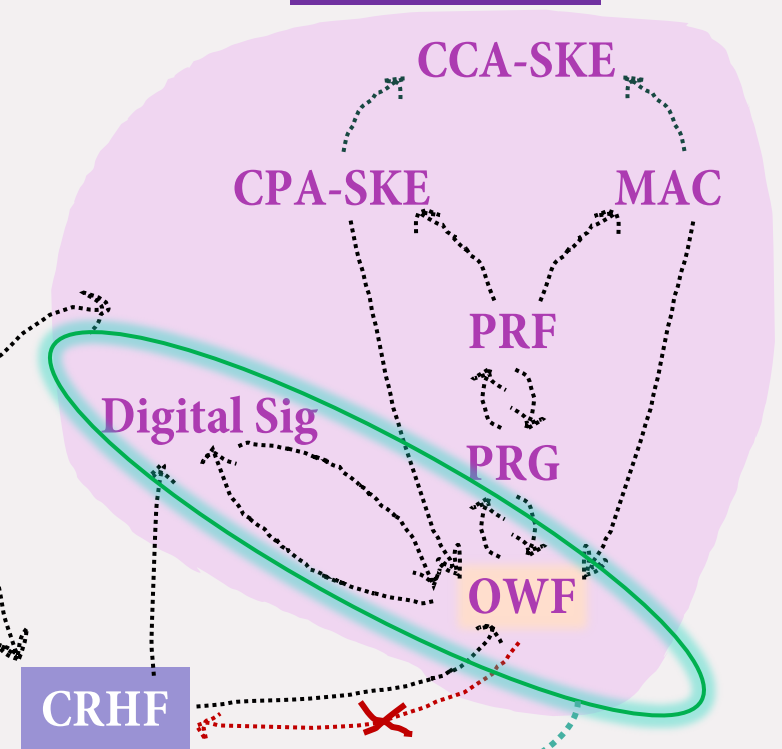
CRYPTOMANIA



HARDNESS ASSUMPTIONS



MINICRYPT



- ① Lamport Signature (For fixed-length messages)
- ② For arbitrary-length messages $\left(\textcircled{1} + \text{CRHF} \right)$

A One-time DS ($q=1$): Lamport's Signature

Theorem 1: OWF $\Rightarrow$ One-time Digital Signatures for fixed-length messages

If OWFs exist, then for any polynomial ℓ , $\exists$ **one-time digital signature scheme** for length- ℓ messages.



$\{f_n: \{0,1\}^n \rightarrow \{0,1\}^n\}_{n \in \mathbb{N}}$: OWF Family

$\mathcal{M} = \{0,1\}^3$
($\ell = 3$)

$\text{Gen}^{\text{OWF}}(1^n) \rightarrow f_n$



$\text{Vrfy}(\text{pk}, 011, \sigma)$:

$\sigma =$

x_{01}		
	x_{12}	x_{13}

$\text{pk}[011]:$

y_{01}		
	y_{12}	y_{13}

Output: 1, if and only if
" $f(\sigma) = \text{pk}[011]$ "

$\text{Gen}(1^n)$:

$\text{sk} =$

x_{01}	x_{02}	x_{03}
x_{11}	x_{12}	x_{13}

$x_{ij} \in_R \{0,1\}^n \forall i,j$

$\text{pk} =$

y_{01}	y_{02}	y_{03}
y_{11}	y_{12}	y_{13}

$y_{ij} = f(x_{ij}) \forall i,j$

$m = 011$

$\text{Sign}(\text{sk}, 011)$:

$\sigma = x_{01}, x_{12}, x_{13}$

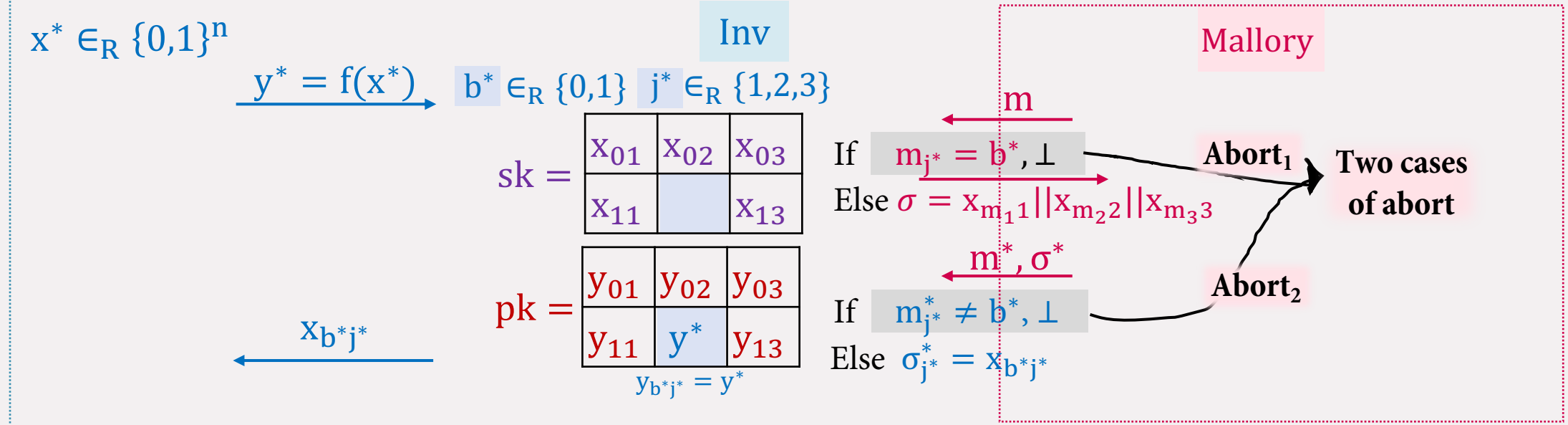
x_{01}		
	x_{12}	x_{13}

A One-time DS ($q=1$): Lamport's Signature

Theorem 1: OWF $\Rightarrow$ One-time Digital Signatures for fixed-length messages

If OWFs exist, then for any polynomial ℓ , $\exists$ **one-time digital signature scheme** for length- ℓ messages.

Proof Sketch: $\exists$ **Mallory** against (Gen, Sign, Vrfy) $\Rightarrow \exists$ **Inv** against the OWF



$$\begin{aligned} \Pr[\text{Inv inverts } f(x^*)] &= \Pr[\overline{Abort_2} | \text{Mallory wins}, \overline{Abort_1}] \cdot \Pr[\text{Mallory wins} | \overline{Abort_1}] \cdot \Pr[\overline{Abort_1}] \\ &\geq \frac{1}{2\ell} \cdot \text{non-negl} \quad (**\text{the above game is only for } \ell = 3, \text{ can be generalized}) \end{aligned}$$

One-time DS to Many-time DS?



Can you find an attack if Mallory is allowed to make two queries to Sign_{sk} ?



How to fix Lamport signature to get EU-CMA secure DS for fixed length messages?

Assuming stateful signing (Sign_{sk} maintains a state) – tree-based signatures

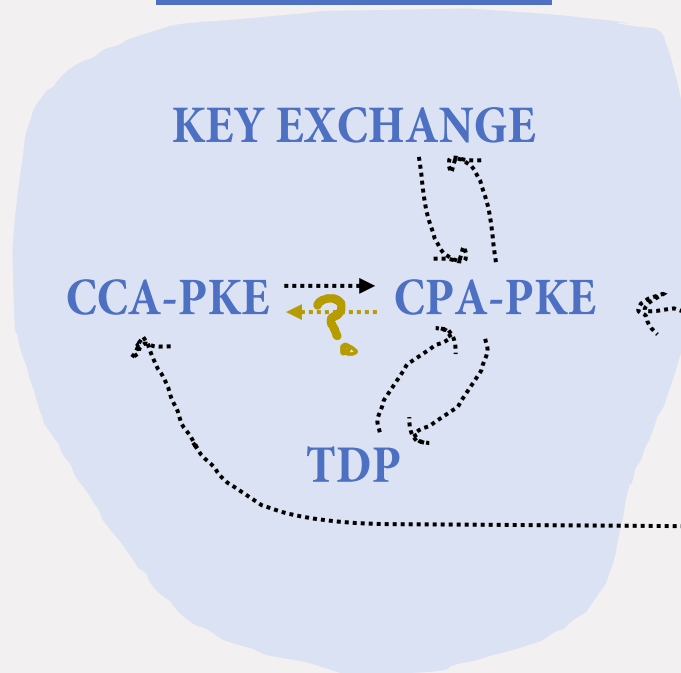
For stateless, assuming that CRHF exists, there exists an EU-CMA DS



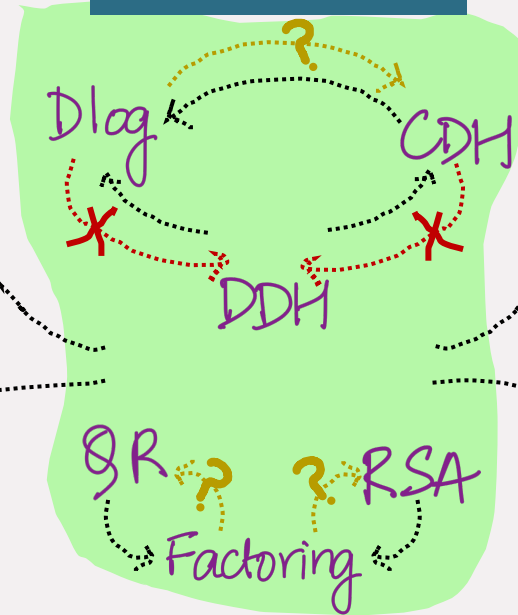
Can skip, if interested see: [Katz and Lindell (Third edition), Ch 14]

Today

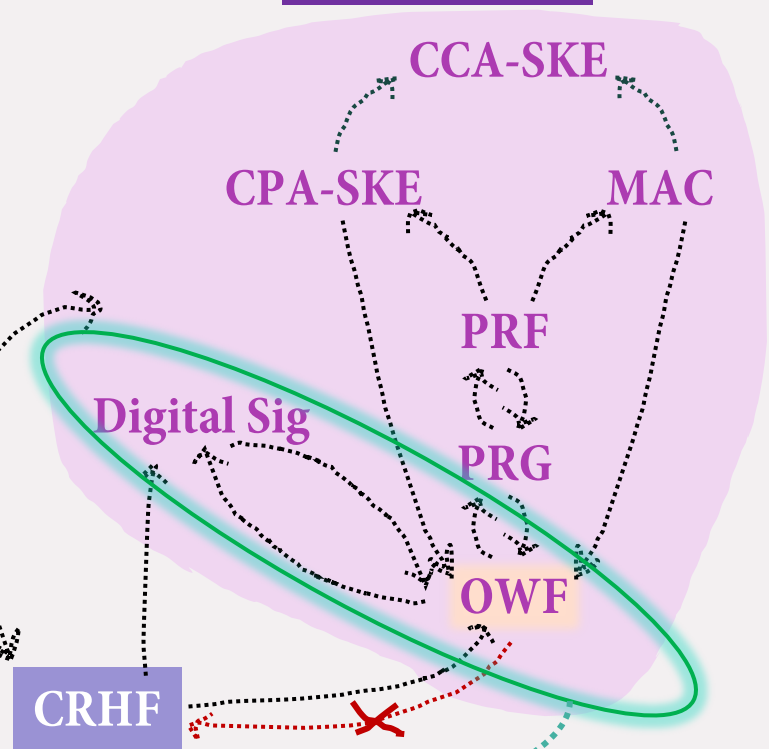
CRYPTOMANIA



HARDNESS ASSUMPTIONS



MINICRYPT



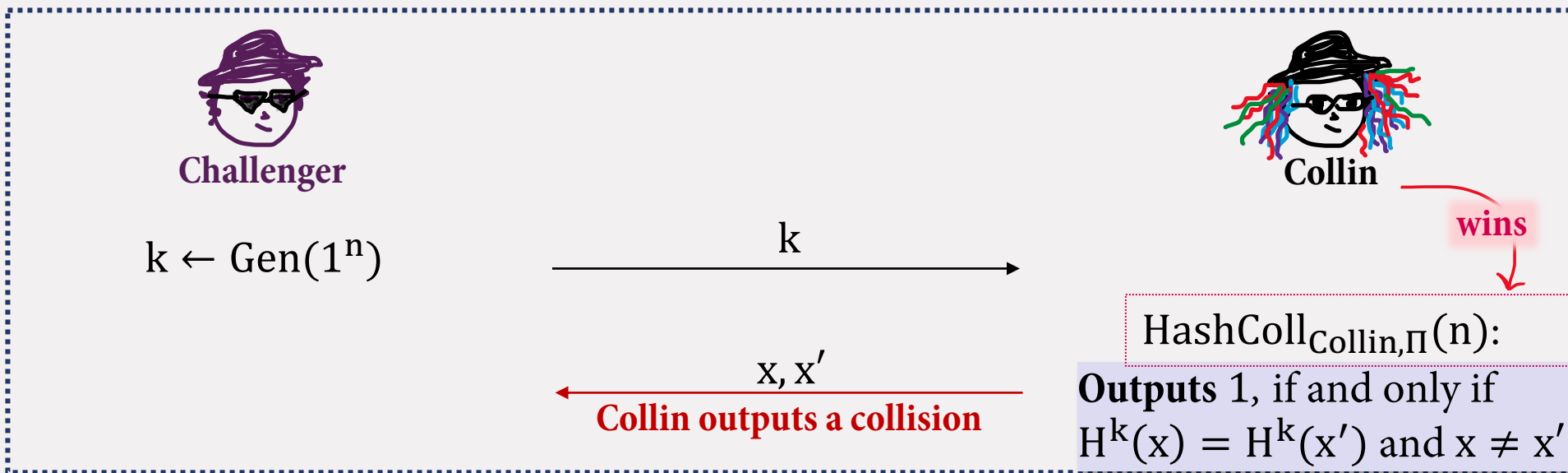
- ① Lamport Signature (For fixed-length messages)
- ② For arbitrary-length messages $\left[\textcircled{1} + \text{CRHF} \right]$

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

Recall: Collision Resistant Hash Functions

$\Pi = (\text{Gen}, H)$: $\text{Gen}(1^n) \rightarrow k$, H^k takes input $x \in \{0,1\}^*$ and outputs $H^k(x) \in \{0,1\}^{\ell(n)}$

If H^k only defined for $\{0,1\}^{\ell'(n)}$ for $\ell'(n) > \ell(n)$ called a **compression function**.



Collision Resistance

A hash function $\Pi = (\text{Gen}, H)$ is **collision resistant** if, for all **PPT** adversary **Collin**, there exists a negligible function **negl** such that

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

The Hash-then-Sign Paradigm

$\Pi_{\text{fl}} = (\text{Gen}_{\text{fl}}, \text{Sign}_{\text{fl}}, \text{Vrfy}_{\text{fl}}), \mathcal{M} = \{0,1\}^\ell$

Fixed-length EU-CMA DS

$(\text{Gen}_H, H): \text{output length } \ell$

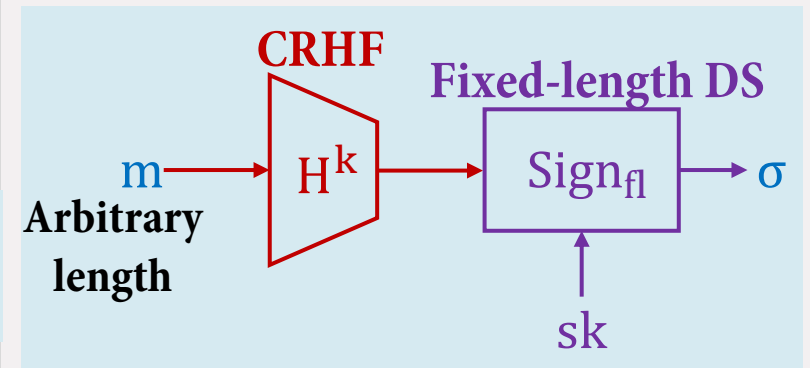
CRHF

$\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy}), \mathcal{M} = \{0,1\}^*$

$\text{Gen}(1^n)$: Compute $(\text{pk}, \text{sk}) \leftarrow \text{Gen}_{\text{fl}}(1^n)$ and $k \leftarrow \text{Gen}_H$
output public key (pk, k) and secret key (sk, k)

$\text{Sign}((\text{sk}, k), m)$: On input $m \in \{0,1\}^*$ compute and
output $\sigma = \text{Sign}_{\text{fl}}(\text{sk}, H^k(m))$

$\text{Vrfy}((\text{pk}, k), m, \sigma)$: Output 1 if and only if $\text{Vrfy}_{\text{fl}}(\text{pk}, H^k(m), \sigma) = 1$



The Hash-then-Sign Paradigm

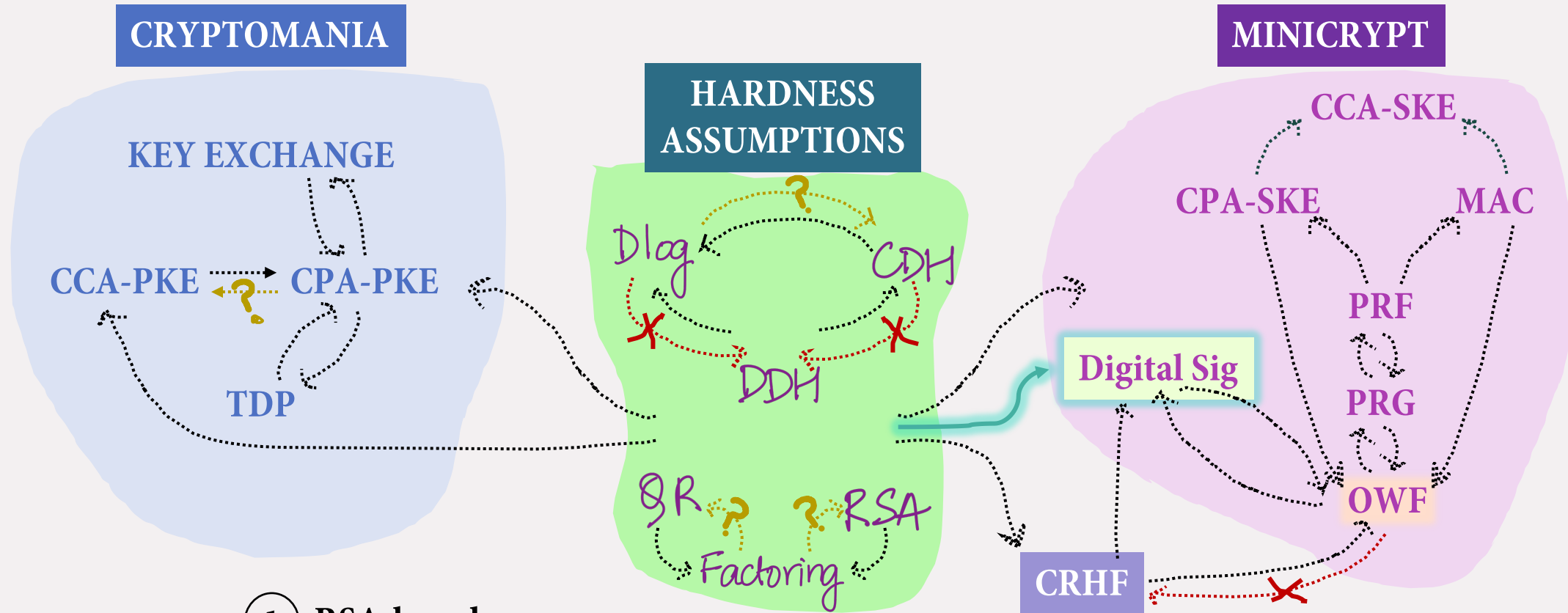
Theorem: CRHF $\Rightarrow$ Digital Signatures for arbitrary length messages

If $\Pi_{fl} = (\text{Gen}_{fl}, \text{Sign}_{fl}, \text{Vrfy}_{fl})$ is EU-CMA secure DS and (Gen^H, H) is a CRHF, then Π is an EU-CMA DS.

Proof

ON THE BOARD BY ONE OF YOU

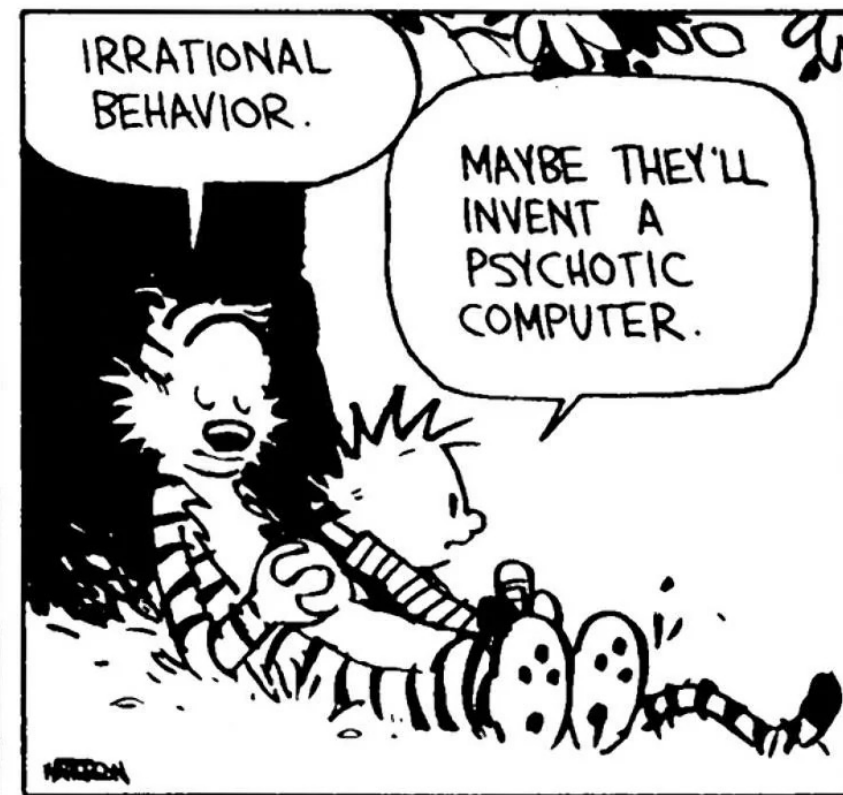
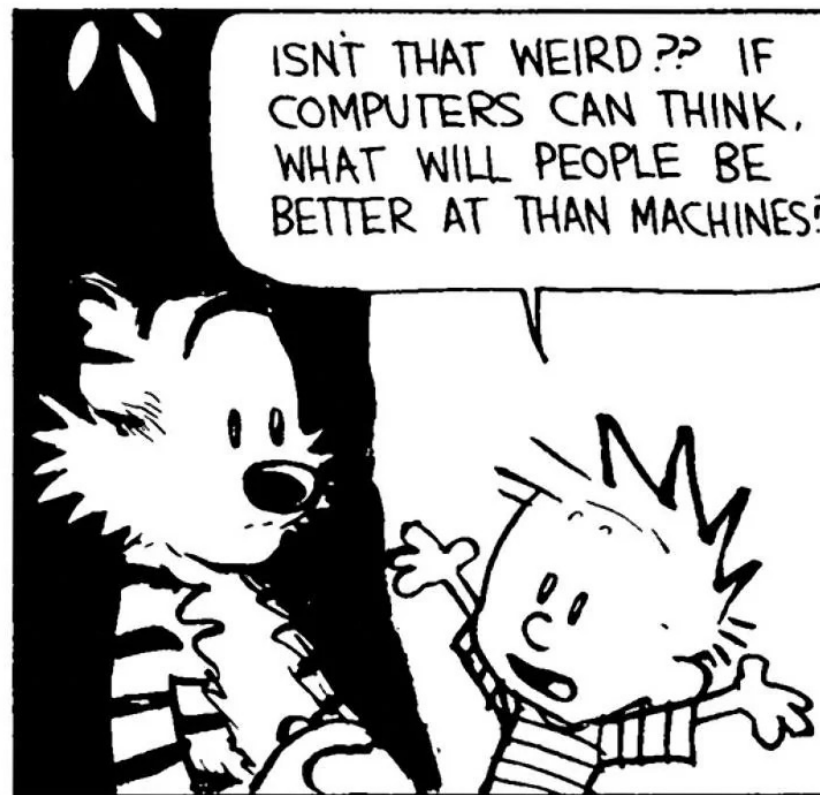
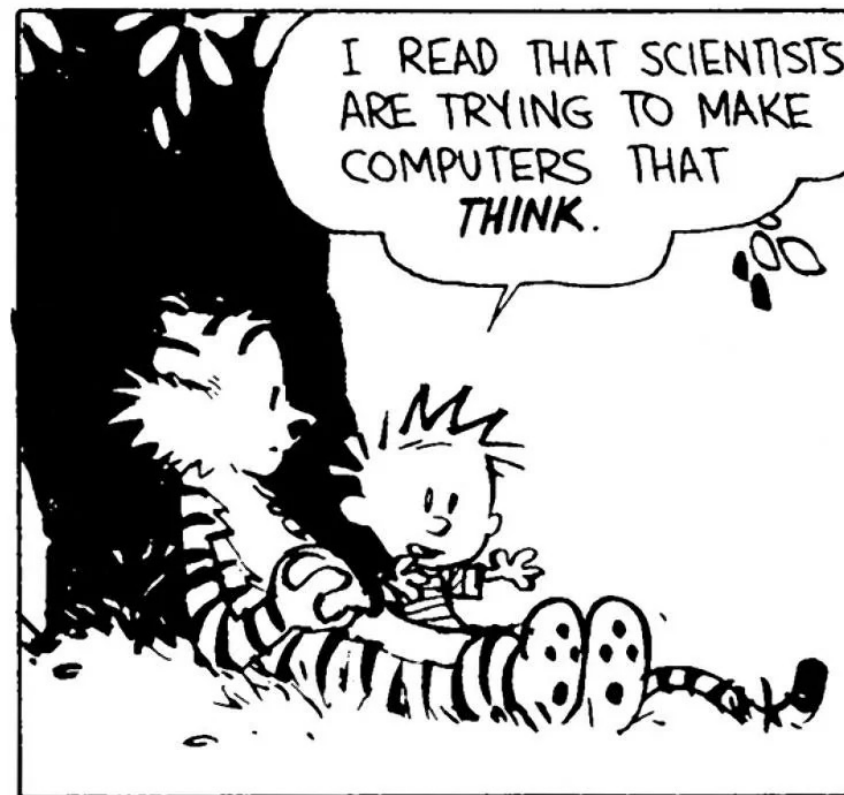
Next class



① RSA-based

② Dlog-based: Identification Scheme + Fiat-Shamir

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



THANK YOU