Miller-Rabin Primality testing.

Let N be a positive integer.

$N-1 = 2^r u$, where u is an odd integer and $r > 0$

we checked for whether $a^{N-1} \equiv 1 \bmod N$

$a^{2^r u} \equiv 1 \bmod N$.

Instead of checking $a^{2^r u} \equiv 1 \bmod N$,
we will consider the following seq:

$$\left(a^u, a^{2u}, \ldots, a^{2^{r-1}u}, a^{2^r u}\right).$$

$$\left(a^u \bmod N, a^{2u} \bmod N, \ldots, a^{2^r u} \bmod N\right).$$

Note that if $a^{2^i u} \equiv \pm 1 \bmod N$, then
for all $i < j \leq r$. $a^{2^j u} \equiv 1 \bmod N$.

Defn Let $a \in \mathbb{Z}_N^*$. We call 'a' to be strong witness. that N is composite, if the following holds

(a) $a^u \neq \pm 1 \bmod N$ and.

(b) for all $1 \leq i \leq r-1$ $a^{2^i u} \neq -1 \bmod N$.

a is not a strong witness $\Rightarrow$ either $a^u \equiv \pm 1 \bmod N$.
or. $\exists\ 1 \leq i \leq r-1 : a^{2^i u} \equiv -1 \bmod N$

a is not a strong witness $\Rightarrow$ $a^{N-1} \equiv 1 \bmod N$.

Prop: If a is a witness then a is also a strong witness.

['$a \in \mathbb{Z}_N^*$ is called witness if $a^{N-1} \not\equiv 1 \bmod N$']

The number of strong witness that N is composite is at least the number of witness that N is composite.

observation:

If a is not a strong witness, then the seq.

$(a^u \bmod N, a^{2u} \bmod N, \ldots, a^{2^r u} \bmod N)$

takes one of the following forms:

- $(\pm 1, 1, 1, \ldots 1)$
- $(*, *, \ldots, -1, +1, \ldots +1)$

Lemma: If N is a prime number, then the only square root of $1 \bmod N$ is $\pm 1 \bmod N$.

Lemma: If N is a prime number, then there are no strong witnesses.

Pf: as N is prime $\Rightarrow a^{2^r u} \equiv 1 \bmod N$.

$\Rightarrow \exists\, i \leq r$ such that i is the min index at which $a^{2^i u} \equiv 1 \bmod N$.

- If $i = 0 \Rightarrow a^u \bmod N \equiv 1 \bmod N$
- $(a^{2^{i-1} u})^2 \equiv 1 \bmod N$

$\Rightarrow a^{2^{i-1} u} \equiv \pm 1 \bmod N \Rightarrow a^{2^{i-1} u} \equiv -1 \bmod N.$

Thm:
Let N be an odd composite integer that is not a prime power. Then at least half of the elements of $\mathbb{Z}_N^*$ are strong witnesses that N is composite.

Pf: $Bad = \{a \in \mathbb{Z}_N^* : a \text{ is not a strong witness}\}$.

$(-1) \overset{?}{\in} Bad$.

$(-1)^u \equiv -1 \bmod N$ as u is odd.

Thm:
Let N be an odd composite integer that is not a prime power. Then at least half of the elements of $\mathbb{Z}_N^*$ are strong witnesses that N is composite.

Pf: $Bad = \{a \in \mathbb{Z}_N^* : a \text{ is not a strong witness}\}$.

$(-1) \overset{?}{\in} Bad$.

$(-1)^u \equiv -1 \bmod N$ as u is odd.

$$B = \{ a \in \mathbb{Z}_N^* : a^{2^i u} \equiv \pm 1 \bmod N \}$$

Consider an $i \in \{0, \ldots, r-1\}$ be the largest integer for which there exists an element $a \in Bad$ with $a^{2^i u} \equiv -1 \bmod N$.

Is 'i' well-defined ?

Let $(-1) \in Bad$. $(-1)^{2^0 \cdot u} \equiv -1 \bmod N$.

Claims:

1) $Bad \subseteq B$.

Claim 2:

B is a subgroup of $\mathbb{Z}_N^*$

$(-1) \in B$.

$a, b \in B \Rightarrow a^{2^i u} \equiv \pm 1 \bmod N$

$b^{2^i u} \equiv \pm 1 \bmod N$

$\Rightarrow ab \in B$.

Claim 3.

B is a strict subgroup of $\mathbb{Z}_N^*$.

From claim 1, claim 2 and claim 3.

- $Bad \subseteq B$.
- B is a strict subgroup of $\mathbb{Z}_N^*$
- $|B| \leq |\mathbb{Z}_N^*|/2$

$\Rightarrow |Bad| \leq |\mathbb{Z}_N^*|/2$

$\Rightarrow$ The number of strong witnesses that N is composite is at least $|\mathbb{Z}_N^*|/2$.

Proof of claim 3:

Suppose $a \in B \Rightarrow a \in \mathbb{Z}_N^*$.

We can decompose N as:

$$N = N_1 * N_2 \quad \text{s.t. } \gcd(N_1, N_2) = 1$$

From CRT:

$$a \in \mathbb{Z}_N^* \longleftrightarrow \Big(\overbrace{[a \bmod N_1]}^{a_1}, \overbrace{[a \bmod N_2]}^{a_2}\Big)$$

We consider an element $a \in B$ such that

$$a^{2^i u} \equiv -1 \bmod N.$$

$$a^{2^i u} \bmod N = \Big(a_1^{2^i u} \bmod N,\ a_2^{2^i u} \bmod N\Big)$$

Therefore,

$$[a_1^{2^i u} \bmod N_1,\ a_2^{2^i u} \bmod N_2]$$

$$= -1 \bmod N = (-1, -1)$$

$$a_1^{2^i u} \equiv -1 \bmod N_1$$

$$a_2^{2^i u} \equiv -1 \bmod N_2$$

Now we consider an element $b \in \mathbb{Z}_N^*$ such that $b \leftrightarrow (a_1, 1)$

$$b^{2^i u} \equiv (a_1^{2^i u} \bmod N, 1) = (-1, +1) \not\equiv \pm 1 \bmod N$$

$$b \notin B.$$

Algorithm:

Input: Integer N and param-t

output: A decision whether N is prime or not.

- If N is even, return composite
- If N is a perfect power, return composite

else

compute r and u s.t. $N-1 = 2^r u$

for $j = 1$ to t

$a \leftarrow \$\{1, \ldots N-1\}$

- if $\gcd(a, N) \neq 1$, return composite
- if a is strong witness, return composite.

@ $\dfrac{(N-1-|\mathcal{A}_N^*|)+|\mathcal{A}_N^*|/2}{N-1}$

$= (N-1) - \dfrac{|\mathcal{A}_N^*|/2}{N-1}$ failure at i^{th} iteration $< \frac{1}{2}$

$= 1 - \dfrac{|\mathcal{A}_N^*|}{2(N-1)} \geq \frac{1}{2}$

Defn of public key encryption:

A public key encryption system consists of three prob. algorithms. (KGEN, Enc, Dec) where

- KGEN(1^n) → returns a pair of keys (pk, sk) such that each of pk, sk are of n bits in length.
- Enc(pk, m) → takes a public key pk, and a message $m \in \mathcal{M}$ and returns a ciphertext $c \in \mathcal{C}$.
- Dec(sk, c) → takes a secret key sk and a message $c \in \mathcal{C}$. and returns either $\perp$ or an element $m \in \mathcal{M}$.

Correctness Condn.

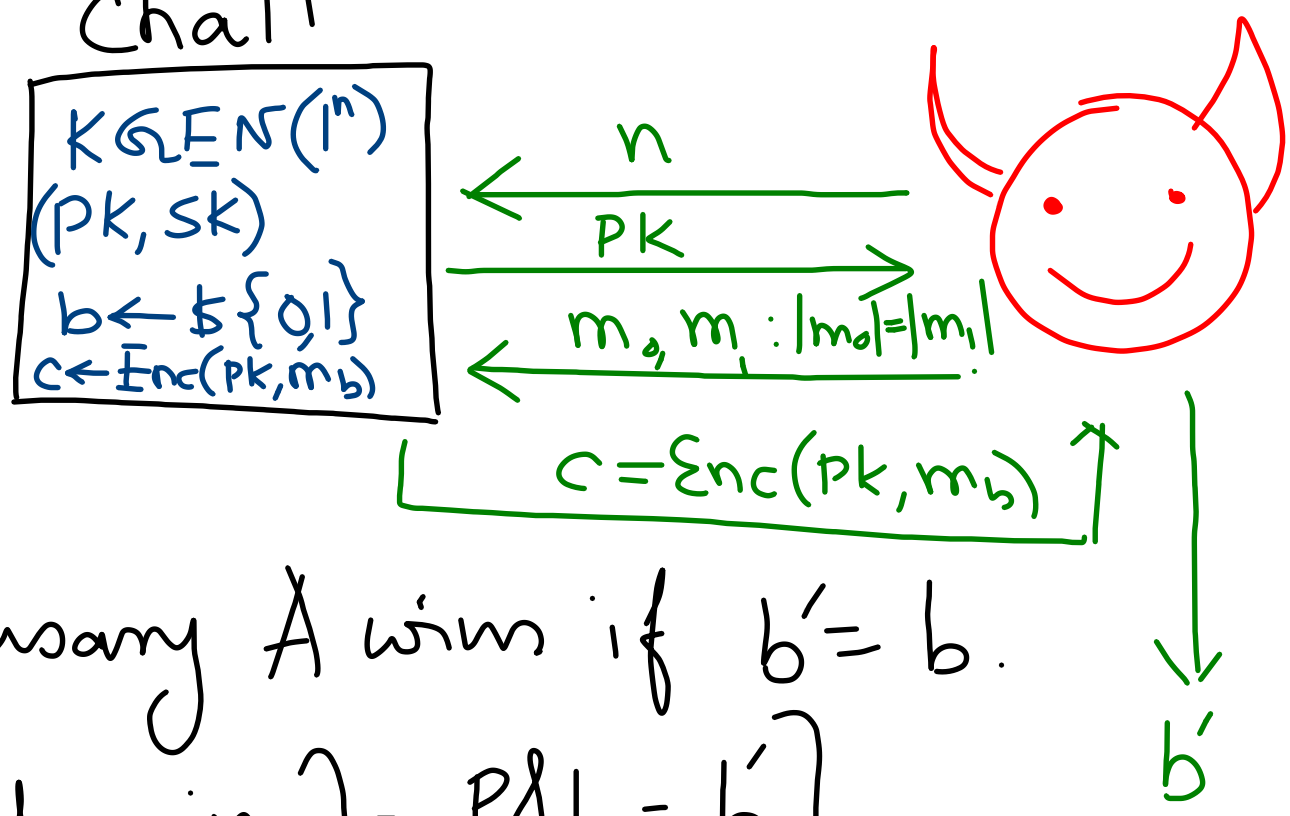
$$Dec(Enc(m, pk), sk) = m, \forall (pk, sk) \leftarrow KGEN(1^n) \; \& \; \forall m \in \mathcal{M}. \; \forall n \in \mathbb{N}.$$

$g(f(x)) = x$

Dec_{sk} is the inverse of Enc_{pk}

Security of a PKE in terms of an eavesdropper.

Let $\Pi = (KGEN, Enc, Dec)$ be a public key encryption system.



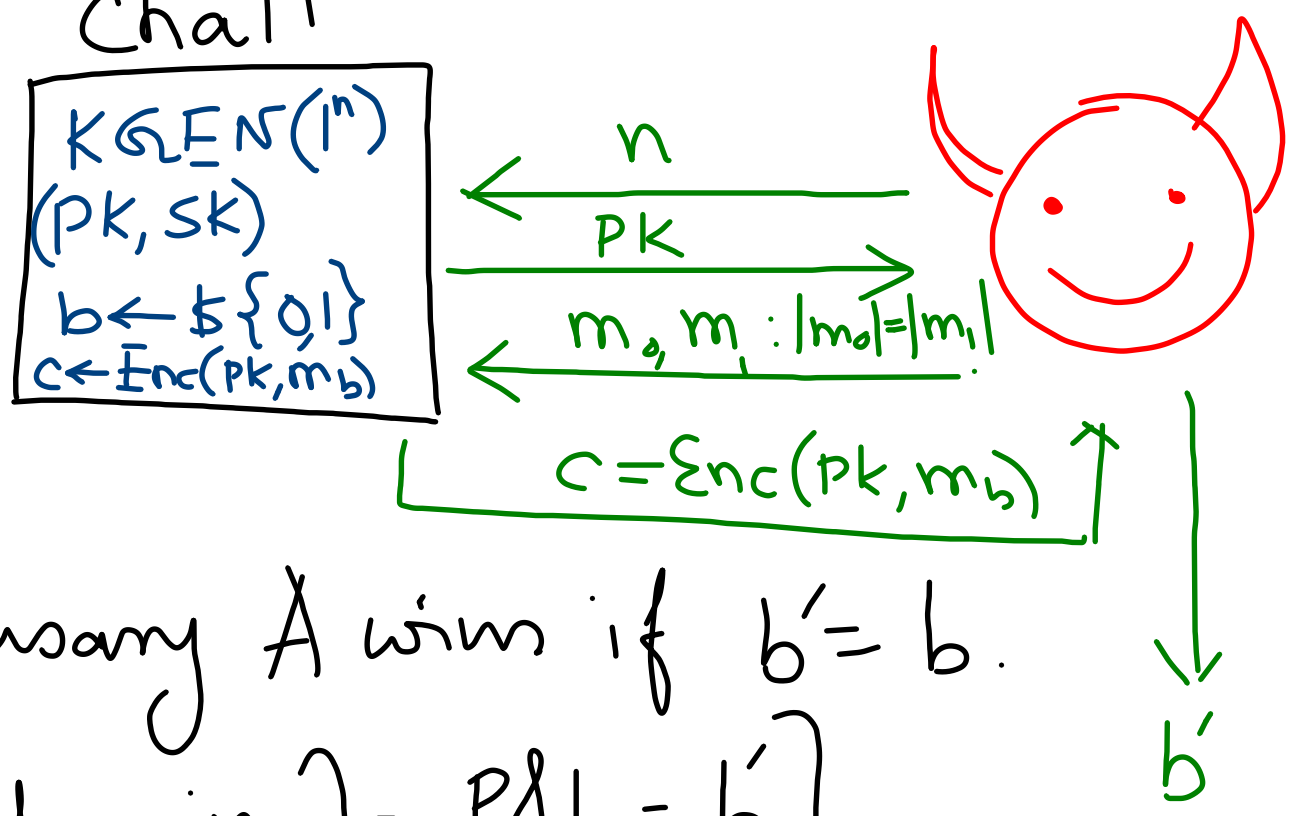
Adversary A wins if $b' = b$.

$Pr[\text{Adv wins}] = Pr[b = b']$.

Π is a secure PKE if $Adv^{eav}_{\Pi}(A) := Pr[A \text{ wins}] \leq \frac{1}{2} + negl(n)$

Security of a PKE in terms of an eavesdropper.

Let $\Pi = (KGEN, Enc, Dec)$ be a public key encryption system.



Adversary A wins if $b' = b$.

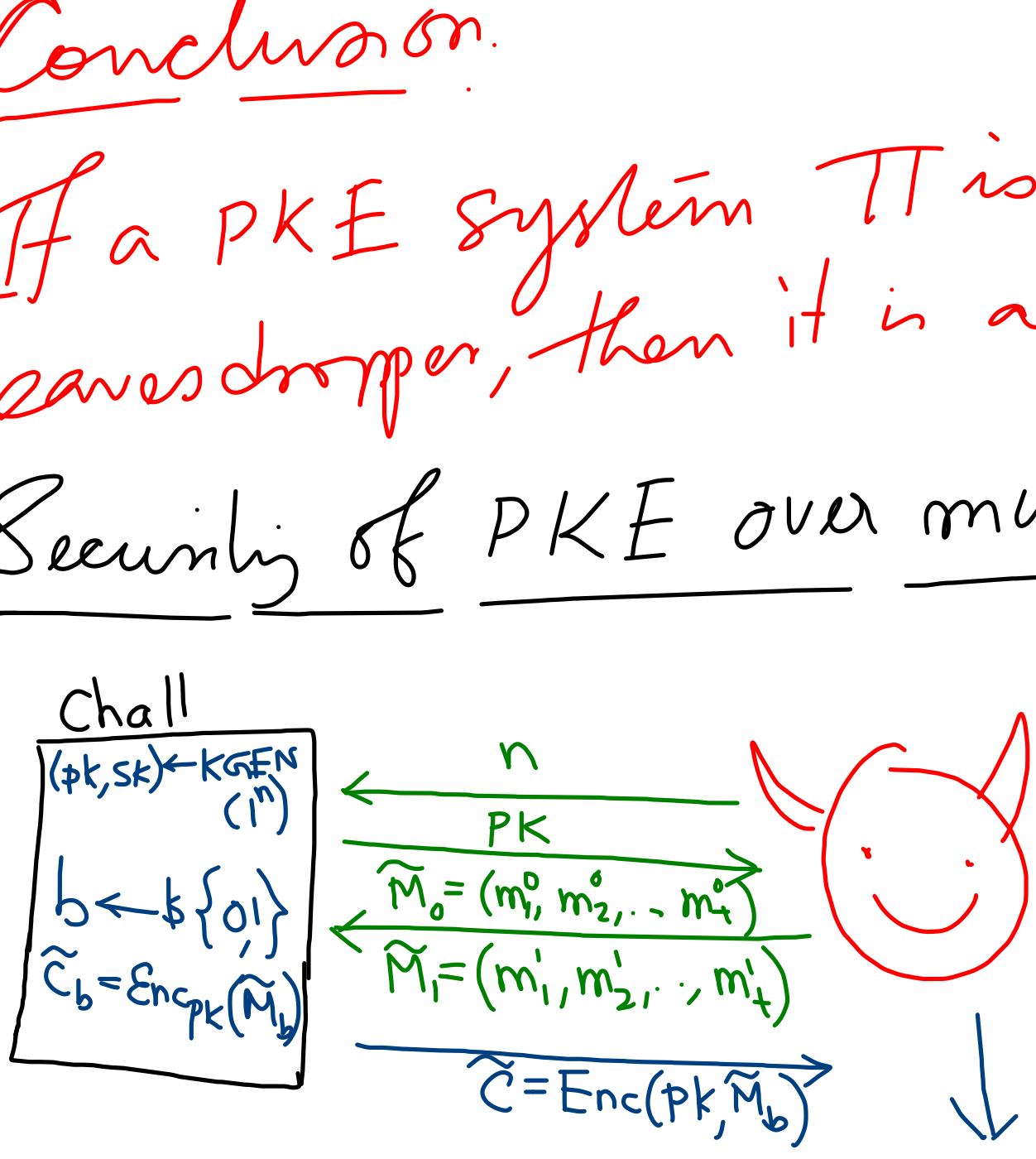
$Pr[\text{Adv wins}] = Pr[b = b']$.

Π is a secure PKE if $Adv^{eav}_{\Pi}(A) := Pr[A \text{ wins}] \leq \frac{1}{2} + negl(n)$

Conclusion:

If a PKE system Π is secure under eavesdropper, then it is also CPA-secure.

Security of PKE over multiple encryptions: in eavesdropper setting



$$P_b[\text{Adversary } A \text{ wins}] = Pr[b = b']$$

We call Π is secure PKE w.r.t multiple enc. in eavesdropper setting if $Adv_{\Pi}^{mcav}(A) := Pr[A \text{ wins}] \leq \frac{1}{2} + negl(n)$.

Thm: If Π is secure PKE in eavesdropper setting, then Π is secure PKE over multiple encryptions in eavesdropper setting.

i.e. $Adv_{\Pi}^{eav}(A) \leq \frac{1}{2} + negl(n) \Rightarrow$

$Adv_{\Pi}^{meav}(A) \leq \frac{1}{2} + negl(n)$.