Final Review Session

Post Quantum Crypto

2. $\mathcal{D}_1$: unif. dist. on $\{0, \ldots, 8\}$

$\mathcal{D}_2 : Z = X + Y$

$X \sim \{0, \ldots 4\}$ unif

$Y \sim \{0, \ldots 4\}$ unif.

How to rejection sample from $\mathcal{D}_2$ given samples from $\mathcal{D}_1$.

1. $x \sim \mathcal{D}_1$
2. Accept with $\dfrac{\mathcal{D}_2(x)}{M \cdot \mathcal{D}_1(x)}$

How to set M?

$\forall x \quad \mathcal{D}_2(x) \leq M \cdot \mathcal{D}_1(x)$

$\mathcal{D}_2(x) \leq \dfrac{M}{9}$

$N(\mu, \sigma)$

$$\operatorname*{argmax}_x Q_2(x) = x^*$$

$$Q_2(x^*) \leq \frac{M}{9}$$

$$x^* = 4$$

X	Y	Pr
0	4	$\frac{1}{25}$
1	3	⋮
2	2	⋮
3	1	⋮
4	0	⋮

$$Q_2(4) = \frac{1}{5}$$

$$\frac{1}{5} \leq \frac{M}{9}$$

$$M \geq \boxed{\frac{9}{5}}$$

Digital Signatures

1. Plain RSA $\sigma = m^d \bmod N$

   FDH-based $\sigma = [H(m)]^d \bmod N$

a. $\underbrace{0x00}_{0\text{byte}} \| m \| 0^{k/10} = enc(m)$

$\sigma = [enc(m)]^d \bmod N$

Is this secure?

Pick a carefully crafted message m

query m to signing oracle

$\sigma = [enc(m)]^d \bmod N$

$\sigma \cdot \sigma = [enc(m)]^d \cdot [enc(m)]^d =$

$[enc(m) \cdot enc(m)]^d$

our goal is to find an m s.t.

$$enc(m) \cdot enc(m) = enc(m')$$

$m = 0 \cdots 01$

$enc(m) = m \cdot 2^{K/10} = 2^{K/10}$ for $m = 1$

$enc(m) \cdot enc(m) = 2^{K/10} \cdot 2^{K/10} \mod N$

for $m = 1$

$= 2^{K/5}$

Find m' s.t. $enc(m') = m' \cdot 2^{K/10} = 2^{K/5}$

$m' = 2^{K/10}$

Forgery: σ^2, $m' = 2^{K/10}$ $m \cdot m = 1$

$= 10^{K/10}$

$(\sigma^2)^e \mod N \stackrel{?}{=} enc(m')$

$2^{K/5}$

$\pm 2^{K/10}$

for $m' = 1$

(b) $enc = 0||m||0||m$ use the fact that $e = 3$.

$m^{1/3} \bmod N$

$m = 8$

$8^d = 2 \bmod N$

$\Rightarrow$

$(8^d)^3 = 2^3$

$8 = 8.$

Attack: $m = 1$

$enc(m) = 0||\underbrace{0\cdots01}_{m}||0||\underbrace{0\cdots01}_{m}$

$0||0\cdots1000||0||0\cdots1000$

$[enc(m)]^d = 6$ from oracle

$[8 \cdot enc(m)]^d$

$e = 3$

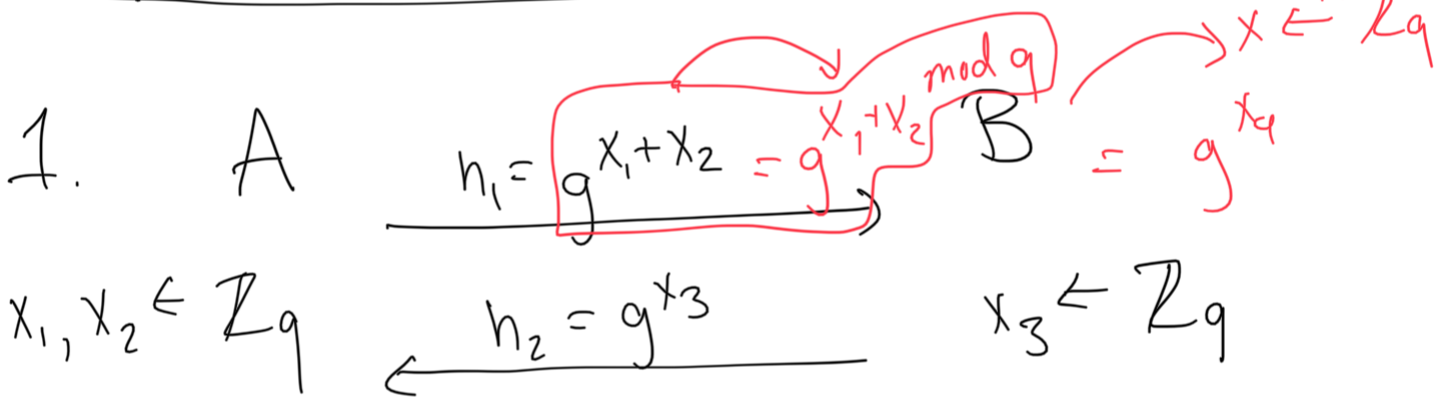
$8 \cdot enc(m) = enc(m') = enc(\sigma)$

Can compute $\left[8 \cdot enc(m)\right]^d = 8^d \cdot \left[enc(m)\right]^d$

$2 \cdot \sigma$

Forgery: $\sigma' = 2 \cdot \sigma$, $m' = 8$

Key Exchange and Public Key Encryption



$(h_2)^{x_1+x_2}$

$(g^{x_3})^{x_1+x_2} =$

$g^{x_3(x_1+x_2)}$

Correctness

$h_1^{x_3}$

$(g^{x_1+x_2})^{x_3}$

$= g^{(x_1+x_2)x_3}$

Security:

Number theory

2. Use CRT and Fermat's little Th

to prove that $N = p \cdot q$

$$x^{\phi(N)} \equiv 1 \bmod N$$

Fermat's little Th

$x \in \mathbb{Z}_p^*$ p prime then $\boxed{x^{p-1} = 1 \bmod p}$

$x \in \mathbb{Z}_N^*$

use C.R.T.

$x \bmod p$

$x \bmod q$

$x^{\phi(N)} \bmod N =$

$$\psi^{-1}\left(x^{\phi(N)} \bmod p,\ x^{\phi(N)} \bmod q\right)$$

$$= \psi^{-1}\Big(\underbrace{x^{(p-1)(q-1)} \bmod p = 1 \bmod p}_{},$$

$$\underbrace{x^{(q-1)(p-1)} \bmod q = 1 \bmod q}_{}\Big) =$$

$$\psi^{-1}(1,1) = \boxed{1} \quad \checkmark$$

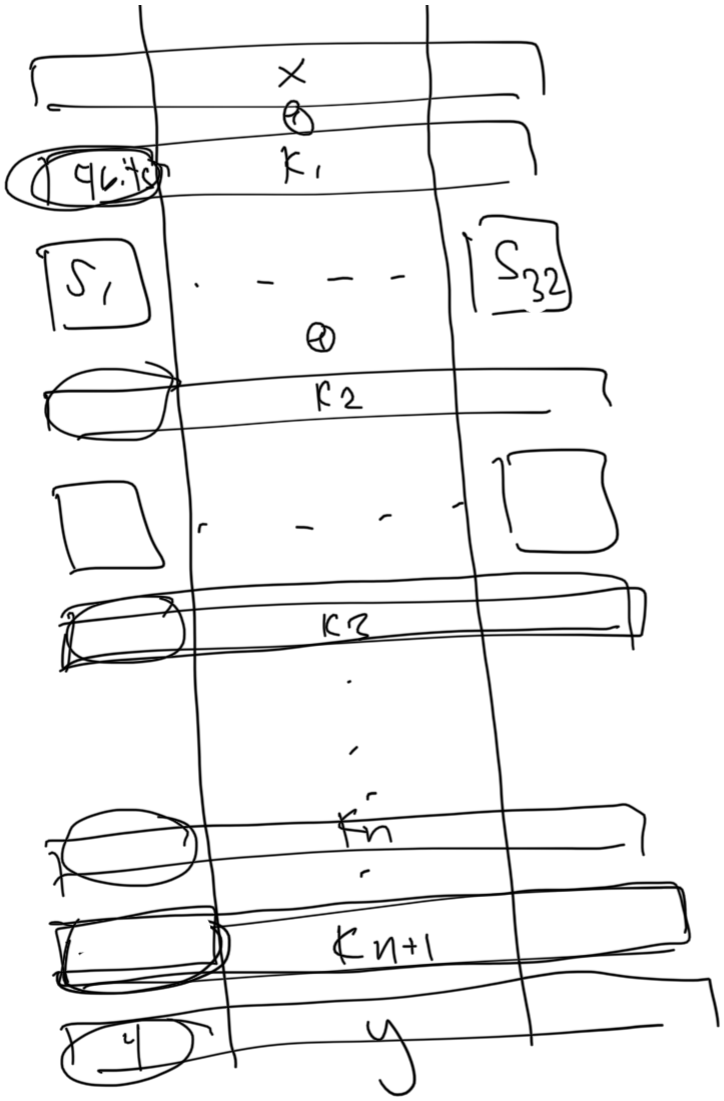
CRT thm exists a isomorphism
bijection

$$\psi: \mathbb{Z}_N \to \mathbb{Z}_p \times \mathbb{Z}_q$$

Symmetric Key

2. n-round SPN no permutation

2^4



$n\,2^{128 \cdot n}$

$n\,2^{4n} \cdot 32 = n\,2^{4n} \cdot 2^5 = 2^{40}$

$n = 8$

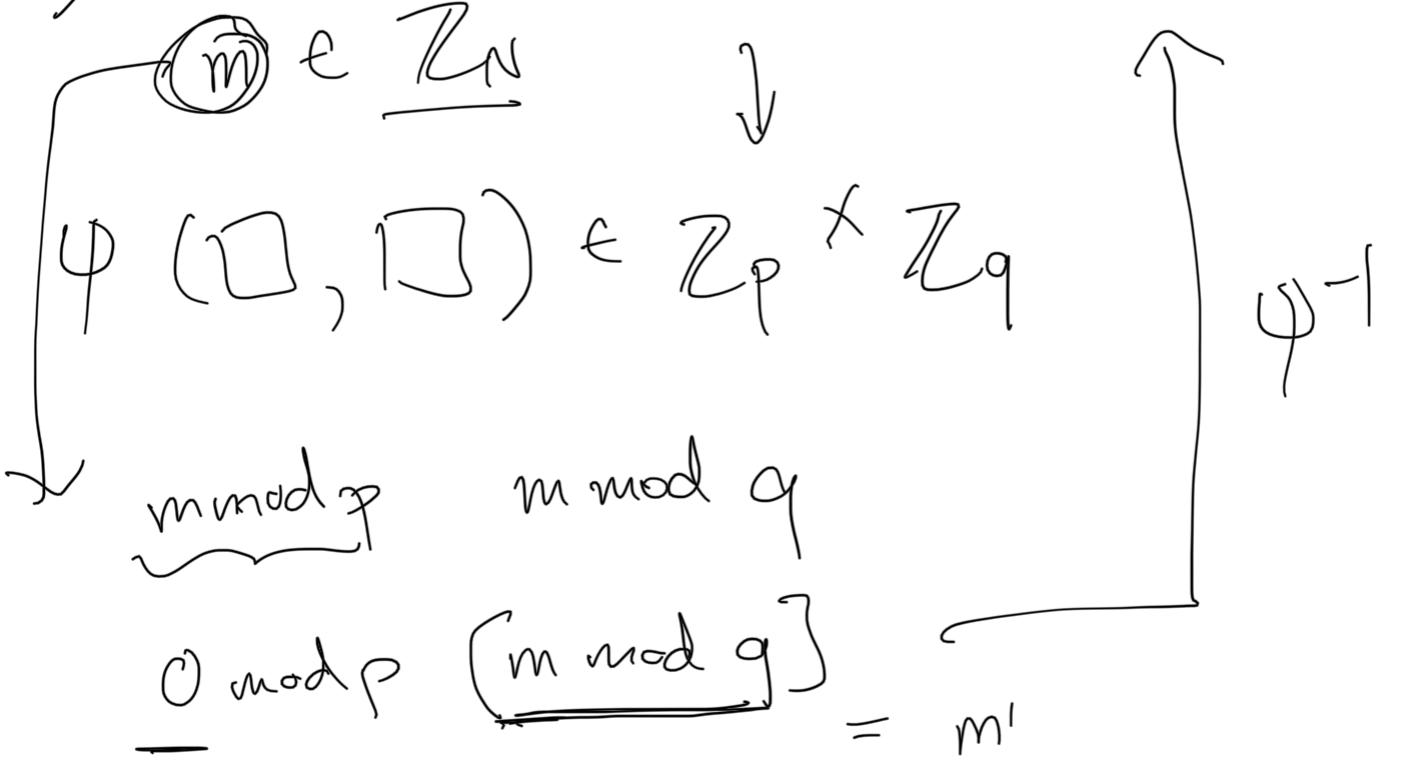
$\left(\frac{1}{2^4}\right)^t$

$2^3 \cdot 2^{32} \cdot 2^5 = 2^{40}$

$2^{4n} \cdot \left(\frac{1}{2^4}\right)^t = 1$

Number Theory

1)



$0^{e \cdot d} \bmod p$ $\quad m'^{e \cdot d} \bmod q$ $\quad m \in \mathbb{Z}_q^*$

$=$

$m'^{e \cdot d \bmod (q-1)} = m' \bmod q$

$\phi(N) \mid (e \cdot d - 1)$

$(p-1)(q-1) \mid (e \cdot d - 1)$

?

$$(q-1) \mid (e \cdot d - 1)$$

$0 \bmod p \qquad m' \bmod q$

$\Downarrow$

$m \bmod N$