Rabin Crypto System

Murat Kantarcioglu

Rabin's Public Key System

- For Rabins system $G(1^k)$ outputs $n = pq$, p and q
- Define $f_n(m) = m^2 \bmod n$
- Define $f^{-1}(m^2) = x$ s.t. $x^2 = m^2 \bmod n$
- Note that inverse of rabin function has four outputs
  - $x^2 = m^2 \bmod p$ has two solutions
  - $x^2 = m^2 \bmod q$ has two solutions
  - Total four solutions due to CRT
- In practice, some additional information is needed for unique inverse
  - It is easy if Message space M is sparse in Z_n^*

Rabins's Public Key Cryptosystem

- Inverting Rabins function is as hard as factoring
- Note if p, q is known inverting the Rabins function is easy
- Assume you have an adversary A that inverts Rabins function
- Defining adversary B for factorization using A is easy
  - Adversary $B(n)$

```
1   i ←$ Z*_n
2   y ←A(i^2 mod n, n)
3   if y^2 = i^2 mod n and y ≠ ±i then
4    return gcd(i ± y, n)
5   else
6    jump to [1]
```

Rabin's Public Key Cryptosystem

- Note if $y^2 = i^2 \bmod n$ and $y \neq \pm i$ then
  - $y - i \neq 0$ and $y + i \neq 0$
  - $y^2 = i^2 \Rightarrow (y - i)(y + i) = 0 \bmod n$
  - $\Rightarrow$ eitheir $gcd(y + i, n) \neq 0$ or $gcd(y - i, n) \neq 0$
- Also existence of B implies chosen ciphertext attacks