Public-Key Cryptography

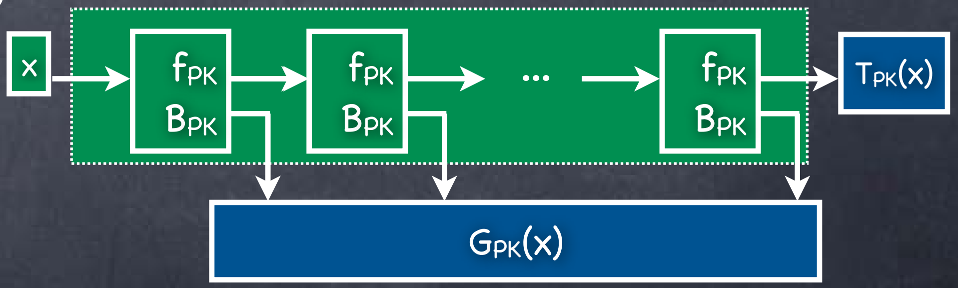
Lecture 11

Some Trapdoor OWP Candidates

RECALL

CPA-secure PKE for Trapdoor OWP

- CPA secure PKE from Trapdoor PRG
  - PRG family with a (PK,SK). PK specifies the family member.
  - Can encapsulate the seed for the PRG such that:
    - PRG output remains pseudorandom even given PK and encapsulated seed
    - Can recover PRG output from encapsulated seed and SK
  - El Gamal: encapsulated seed = g^x, PRG output = Y^x
- Trapdoor PRG from Trapdoor OWP



RECALL

Candidate Trapdoor OWPs

- Two candidates using composite moduli
  - RSA function: $f_{RSA}(x; N,e) = x^e \bmod N$ where N=PQ, P,Q k-bit primes, e s.t. $gcd(e,\varphi(N)) = 1$ (and x uniform from {0...N-1})
    - Fact: $f_{RSA}(.; N,e)$ is a permutation
    - Fact: While picking (N,e), can also pick d s.t. $x^{ed} = x$
  - Rabin OWF: $f_{Rabin}(x; N) = x^2 \bmod N$, where N = PQ, and P, Q are k-bit primes (and x uniform from {0...N-1})
    - Fact: $f_{Rabin}(.; N)$ is a permutation among quadratic residues, when P, Q are $\equiv 3 \pmod 4$
    - Fact: Can invert $f_{Rabin}(.; N)$ given factorization of N

RECALL

Chinese Remainder Theorem

- If P, Q relatively prime then the pair (x mod P, x mod Q) uniquely determines x (mod PQ)
- Called the CRT representation
- Addition, multiplication and exponentiation can be carried out coordinate wise (mod P and mod Q respectively in each coordinate)
- Can efficiently compute the mapping (in both directions) if P, Q known
  - From (a,b) to x: Compute α,β s.t. $\alpha P+\beta Q=1$ (using Extended Euclidean Algorithm). Set $x = b\alpha P+a\beta Q$

Proof of CRT

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$	$\mathbb{Z}_5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where N=PQ, and $\gcd(e,\varphi(N)) = 1$ (i.e., $e \in \mathbb{Z}_{\varphi(N)}^*$)
  - $f_{RSA[N,e]}: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
  - In fact, there exists d s.t. $f_{RSA[N,d]}$ is the inverse of $f_{RSA[N,e]}$
    - d s.t. $ed \equiv 1 \pmod{\varphi(N)} \Rightarrow x^{ed} \equiv x \pmod N$
    - Why? By CRT!
      - Exponentiation works coordinate-wise
      - $ed \equiv 1 \pmod{\varphi(N)} \Rightarrow ed \equiv 1 \pmod{\varphi(P)}$ and $ed \equiv 1 \pmod{\varphi(Q)}$

RSA Function

- $f_{RSA[N,e]}(x) = x^e \bmod N$
  - Where $N=PQ$, and $\gcd(e,\varphi(N)) = 1$ (i.e., $e \in \mathbb{Z}_{\varphi(N)}^*$)
  - $f_{RSA[N,e]}: \mathbb{Z}_N \to \mathbb{Z}_N$
    - Alternately, $f_{RSA[N,e]}: \mathbb{Z}_N^* \to \mathbb{Z}_N^*$
- $f_{RSA[N,e]}$ is a permutation with a trapdoor (namely (N,d))
- RSA Assumption: $f_{RSA[N,e]}$ is a OWF collection, when P, Q random k-bit primes and $e < N$ random number s.t. $\gcd(e,\varphi(N))=1$ (with inputs uniformly from $\mathbb{Z}_N$ or $\mathbb{Z}_N^*$)
  - Alternate version: $e=3$, P, Q restricted so that $\gcd(3,\varphi(N))=1$
- RSA Assumption will be false if one can factorize N
  - Then knows $\varphi(N) = (P-1)(Q-1)$ and can find d s.t. $ed \equiv 1 \pmod{\varphi(N)}$
  - Converse not known to hold
- Trapdoor OWP Candidate

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$ where N=PQ, P,Q primes $\equiv 3 \bmod 4$
  - Is a candidate OWF collection (indexed by N)
    - Equivalent to the assumption that f_{mult} is a OWF (for the appropriate distribution)
      - If can factor N, will see how to find square-roots
        - So (P,Q) a trapdoor to "invert"
      - Fact: If can take square-root mod N, can factor N
  - Coming up: Is a permutation over $\mathbb{QR}_N^*$, with trapdoor (P,Q)

Square-roots in $\mathbb{Z}_P^*$

- What are the square-roots of x^2?
- $\surd 1 = \pm 1$
  - $x^2=1 \pmod P \Leftrightarrow (x+1)(x-1) = 0 \pmod P$

    $\Leftrightarrow (x+1)=0$ or $(x-1)=0 \pmod P$

    $\Leftrightarrow x=1 \pmod P$ or $x=-1 \pmod P$
  - Where $-1 = g^{(P-1)/2}$
- More generally $\surd(x^2) = \pm x$ (because $x^2=y^2 \pmod P \Leftrightarrow x = \pm y$)
  - $-x = -1 \cdot x$,

Square-roots in $\mathbb{Z}_P^*$

- What are the square-roots of x^2?
- $\sqrt{1} = \pm 1$
  - $x^2 = 1 \pmod{P} \Leftrightarrow (x+1)(x-1) = 0 \pmod{P}$

    $\Leftrightarrow (x+1)=0$ or $(x-1)=0 \pmod{P}$

    $\Leftrightarrow x=1 \pmod{P}$ or $x=-1 \pmod{P}$
  - Where $-1 = g^{(P-1)/2}$
- More generally $\sqrt{(x^2)} = \pm x$ (because $x^2=y^2 \pmod{P} \Leftrightarrow x = \pm y$)
  - $-x = -1 \cdot x$,

Square-roots in $\mathbb{QR}_p^*$

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- How many square-roots stay in $\mathbb{QR}_p^*$?
  - Depends on P!
  - e.g. $\mathbb{QR}_{13}^* = \{\pm1, \pm3, \pm4\}$
    - 1,3,-4 have 2 square-roots each. But -1,-3,4 have none within $\mathbb{QR}_{13}^*$
    - Since $-1 \in \mathbb{QR}_{13}^*$, $x \in \mathbb{QR}_{13}^* \Rightarrow -x \in \mathbb{QR}_{13}^*$
    - $-1 \in \mathbb{QR}_p^*$ iff (P-1)/2 even
- If (P-1)/2 odd, exactly one of $\pm x$ in $\mathbb{QR}_p^*$ (for all x)
  - Then, squaring is a permutation in $\mathbb{QR}_p^*$

Square-roots in $\mathbb{QR}_P{}^*$

- In $\mathbb{Z}_P{}^*$ $\surd(x^2) = \pm x$ (i.e., x and $-1 \cdot x$)
- If (P-1)/2 odd, squaring is a permutation in $\mathbb{QR}_P{}^*$
  - (P-1)/2 odd $\Leftrightarrow$ P $\equiv$ 3 (mod 4)
- But easy to compute both ways!
  - In fact $\surd z = z^{(P+1)/4} \in \mathbb{QR}_P{}^*$ (because (P+1)/2 even)
- Rabin function defined in $\mathbb{QR}_N{}^*$ and relies on keeping the factorization of N=PQ hidden

$\mathbb{QR}_N^*$

- What do elements in $\mathbb{QR}_N^*$ look like, for N=PQ?
  - By CRT, can write $a \in \mathbb{Z}_N^*$ as $(x,y) \in \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - CRT representation of a^2 is $(x^2,y^2) \in \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
  - If both $P,Q \equiv 3 \pmod 4$, then squaring is a permutation in $\mathbb{QR}_N^*$
    - $\sqrt{(x^2,y^2)} = (\pm x, \pm y)$ in $\mathbb{Z}_P^* \times \mathbb{Z}_Q^*$ but exactly one in $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
    - Can efficiently do this, if can compute (and invert) the isomorphism from $\mathbb{QR}_N^*$ to $\mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
      - (P,Q) is a trapdoor
    - Without trapdoor, OWF candidate
      - Follows from assuming OWF in $\mathbb{Z}_N^*$, because $\mathbb{QR}_N^*$ forms 1/4th of $\mathbb{Z}_N^*$

Rabin Function

- $f_{Rabin[N]}(x) = x^2 \bmod N$
  - Candidate OWF collection, with N=PQ (P,Q random k-bit primes)
  - If P, Q $\equiv$3 (mod 4), then in $\mathbb{QR}_N^*$
    - A permutation
    - Has a trapdoor for inverting (namely (P,Q))
- Candidate Trapdoor OWP

Summary

- A DLA candidate: $\mathbb{Z}_P^*$
- A DDH candidate: $\mathbb{QR}_P^*$ where P is a safe prime
- Chinese Remainder Theorem
  - $\mathbb{Z}_N \cong \mathbb{Z}_P \times \mathbb{Z}_Q$
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$
  - $\mathbb{QR}_N^* \cong \mathbb{QR}_P^* \times \mathbb{QR}_Q^*$
- Trapdoor OWP candidates:
  - $f_{RSA[N,e]} = x^e \bmod N$ where $N=PQ$ and $\gcd(e,\varphi(N))=1$
    - Trapdoor: $(P,Q) \to \varphi(N) \to d=e^{-1}$ in $\mathbb{Z}_{\varphi(N)}^*$
  - $f_{Rabin[N]} = x^2 \bmod N$ where $N=PQ$, where $P,Q \equiv 3 \pmod 4$
    - Trapdoor: (P,Q)
- Trapdoor OWP can be used to construct Trapdoor PRG
  - Trapdoor PRG can give IND-CPA secure PKE