Digital Signatures and clawfree permutations

15-859I
Spring 2003

Clawfree permutation pairs

- G generates a Claw-Free Permutation family if $[G(1^k)]$ is a set of pairs of permutations $f = (f_0,f_1)$ with common domains. P has the property that for any PPT A:
  $\Pr[f_0(x)=f_1(y)=z : f\leftarrow G(1^k), (x,y,z)\leftarrow A(f,1^k)]$
  is negligible.
- Notice that f_0,f_1 must also be OWPs: otherwise we can draw $(f_0,f_1)\leftarrow G(1^k)$, pick $x\leftarrow Dom(f_0)$, and invert f_1 on $z=f_0(x)$ to find a claw.

Trapdoor Clawfree Permutation Pairs

- Let $G(1^k)$ output a tuple $(f_0,f_0^{-1},f_1,f_1^{-1})$. $[G(1^k)]_k$ is a trapdoor clawfree permutation family if $\{f_b^{-1}\}$ are efficiently evaluable but (f_0,f_1) are clawfree.

Generating infinite clawfree families

- Let $i=i_0i_1\ldots i_d$ be any d-bit string. Let (f_0,f_1) be a claw-free permutation pair. Denote by f_i the function:
  $f_i(x) = f_{i_0}(f_{i_1}(\ldots(f_{i_d}(x))))$
- Let $\langle . \rangle$ be a prefix-free mapping on integers.
- Lemma: Let $i\neq j$ be two binary strings. Then $(f_{\langle i \rangle}, f_{\langle j \rangle})$ is claw-free if (f_0,f_1) is claw-free.
- Proof: let $f_{\langle i \rangle}(x) = f_{\langle j \rangle}(y) = z$. Let c be the longest common prefix of $\langle i \rangle, \langle j \rangle$. Then:
  $(x_1=f_{c0}^{-1}(z), x_2=f_{c1}^{-1}(z), x_3=f_c^{-1}(z))$
  is an f-claw.

Items and Chains

- An f-item is a tuple $(r,t;c_0,c_1)$ such that $f_{\langle c_0 \| c_1 \rangle}(t)=r$.
  - r – the *root*
  - t – the *tag*
  - $c_0.c_1$ – the *children*.
- An f-chain starting at y is a tuple $L_1,L_2,\ldots,L_b$ of f-items such that y is the root of L_1 and for $i>1$, the root of L_{i+1} is a child of L_i.

Signature scheme: Key Generation

- Let G be a clawfree trapdoor permutation generator. Let 2^b be a bound on the number of signatures with this key. To generate a key:
- Choose $(f_0,f_0^{-1},f_1,f_1^{-1})\leftarrow G(1^k)$.
- Choose $(g_0,g_0^{-1},g_1,g_1^{-1})\leftarrow G(1^k)$.
- Choose $r^f_\varepsilon \leftarrow Dom(f)$.
- VK = $(f_0,f_1,g_0,g_1, b, r^f_\varepsilon)$
- SK = $(f_0^{-1},f_1^{-1},g_0^{-1},g_1^{-1})$

Signing,Verification, & Security Proof

(Blackboard Exposition)

Clawfree Trapdoor permutations based on Factoring

- Let p,q be primes such that $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$, and $|p|=|q|=k$
- Fact: mod n=pq, $J(-1)=1$ but $-1 \notin QR_n$.
- Fact: mod n=pq, $J(2)= -1$, so $2 \notin QR_n$.
- Define:

  $f_{0,n}(x) = x^2 \pmod n$ if $x^2 \bmod n < n/2$,
  $-x^2 \pmod n$ ow.

  $f_{1,n}(y) = 4y^2 \pmod n$ if $4y^2 \bmod n < n/2$
  $-4y^2 \pmod n$ ow.

CFTP based on factoring

- Define $D_n = \{ x : J_n(x)=1 \ \& \ x < n/2 \}$
- Lemma: $f_{0,n}(x)$ is a permutation on D_n.
- Proof: suppose we have $x,y \in D_n$ st $f_{0,n}(x)=f_{0,n}(y)$. Then $x^2 \equiv y^2 \pmod n$, (since $-1 \notin QR_n$) so $x = -y$, but then one of x,y not in D_n.
- Same for $f_{1,n}$.
- Lemma: given p,q, $f_{0,n}$ is easy to invert.
- Proof: use p,q to determine whether to negate, take sqrts mod p and q, combine with CRT.

CFTP based on factoring

- Lemma: given a claw (x,y,z) where $f_{0,n}(x)=f_{1,n}(y)=z$, we can factor n.
- Proof: we must have that $x^2 \equiv 4y^2 \bmod n$, since -1 is not a QR mod n.
- Also, must not be that $x=\pm 2y \pmod n$, since $J(x) = 1$, $J(y)=1$, $J(2)= -1$, $J(1)=1$.
- Thus we have $(x-2y)(x+2y) \equiv 0 \pmod n$ and so $\gcd(x \pm 2y, n)$ is a nontrivial factor of n.