One-Way Function Technique

Satyaki Mahalanabis Xin Li

November 16, 2006

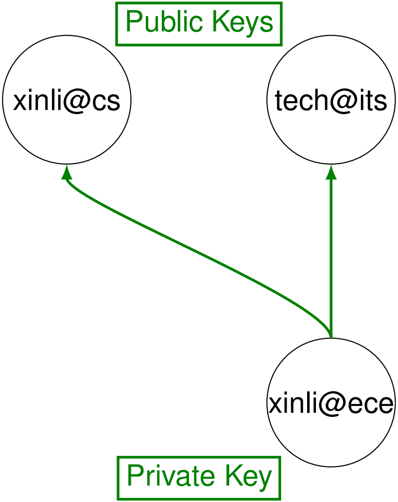
Lecture 1:
Characterizing the Existence of One-Way Functions

Outline

What are one-way functions? – informal notion of one-way

- A function $f\colon\Sigma^* \to \Sigma^*$
- f should be easily computable $f(a) = b$
- It should not be computed easily the other way round $g(b) = a$

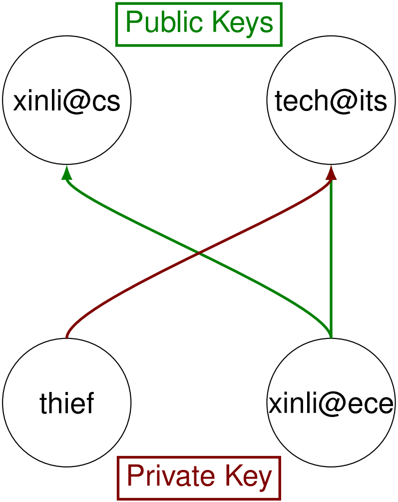
A Cryptography Application



ssh keys

- Private key in my own directory on my desktop
- Public key on the other machines (potentially in a public directory)

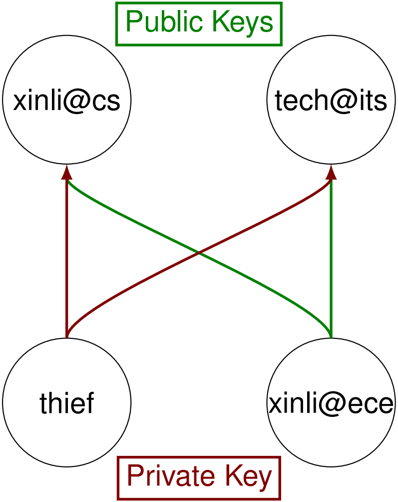
A Cryptography Application



ssh keys

- Private key in my own directory on my desktop
- Public key on the other machines (potentially in a public directory)

A Cryptography Application



ssh keys

- Private key in my own directory on my desktop
- Public key on the other machines (potentially in a public directory)

Existence of One-way Functions vs. P=NP

Question

Do One-way functions exist?

- In worst-case cryptology, one-way functions exist $\leftrightarrow P \neq NP$

Definition: One-way function

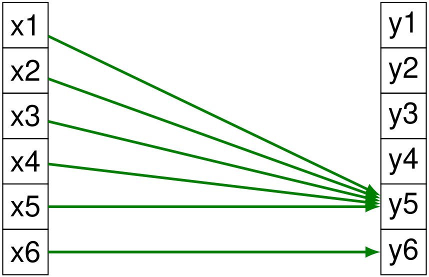
A function f (possibly nontotal) is one-way if

- f is polynomial-time computable
- f is not polynomial-time invertible
- f is honest

Definition: Polynomial-time Invertible

f Polynomial-time Invertible

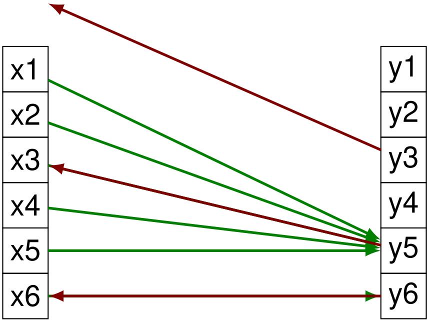
there's polynomial-time computable g (possibly nontotal)
$(\forall y \in range(f))$
$[y \in domain(g) \wedge g(y) \in domain(f) \wedge f(g(y)) = y]$



Definition: Polynomial-time Invertible

f Polynomial-time Invertible

there's polynomial-time computable g (possibly nontotal)
$(\forall y \in range(f))$
$[y \in domain(g) \wedge g(y) \in domain(f) \wedge f(g(y)) = y]$



One-way Definition Revisited

f is one-way if

- f is polynomial-time computable
- f is not polynomial-time invertible
- f is honest

Definition: Honest

f is honest

$(\exists \text{polynomial} q)(\forall y \in range(f))(\exists x)[|x| \leq q(|y|) \wedge f(x) = y]$.

- $|f(x)| = log_2(|x| + 1))$
- $|g(y)| = 2^{|y|} - 1$

Theorem 1

Theorem

One-way functions exist if and only if $P \neq NP$

Theorem 1: Proof – if part

If Part

If P $\neq$ NP then one-way functions exist

- L in NP but not P
- An NPTM N accepts L
- Construct a function f
  - $f(\langle x, w\rangle) = 0x$ if w is an accepting path
  - $f(\langle x, w\rangle) = 1x$ if w is not an accepting path
- We claim f is one-way

Theorem 1: Proof – if part

If Part

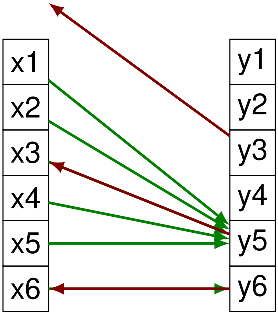
If P $\neq$ NP then one-way functions exist

- Polynomial-time computable: Clearly! Assume the pairing function is polynomial-time computable & invertable.
- Honest: A bit tricky!

Theorem 1: Proof – if part (cont')

If Part

If P $\neq$ NP then one-way functions exist



- Not polynomial-time invertable: suppose the opposite, hope for contradiction
  - Consider the definition again
  - Use g to pull L down to P
  - Given x, $g(0x)$ = ?
    - Not in domain of definition
    - $g(0x) = \langle z, w \rangle$, verify that $z = x$ and w is an accepting path of $N(x)$ (to protect against the cases where g is defined for $0x$, but no preimage is mapped to it by f)

Theorem 1: Proof – only if part

Only if part

If one-way functions exist then P $\neq$ NP

- f is a one-way function
- Construct L = $\{\langle z, pre\rangle | (\exists y)[|y| + |pre| \leq p(|z|) \wedge f(pre \cdot y) = z]\}$
- p is the honesty polynomial of f
- Claim $L \in$ NP - P

Theorem 1: Proof – only if part

Only if part

If one-way functions exist then P $\neq$ NP

- $L \in$ NP: Clearly! Take a wild guess of y
- $L \notin$ P: Suppose the opposite, hope for contradiction
- Construct g to invert f
    - g search the prefixes
        - $f(\epsilon...) = z$
        - $f(1...) = z$
        - $f(0...) = z$
        - decide each bit by asking two questions
    - g does the reverse direction of f in polynomial-time

Theorem 2

Theorem

One-to-one one-way functions exist if and only if $P \neq UP$

Definition: UP

L is in UP if

- L is accepted by an NPTM N
- For each input, N has at most one accepting path

Definition: one-to-one function

$f : \Sigma^* \to \Sigma^*$ is one-to-one if
$(\forall y \in \Sigma^*)[||\{x|f(x) = y\}|| \leq 1]$

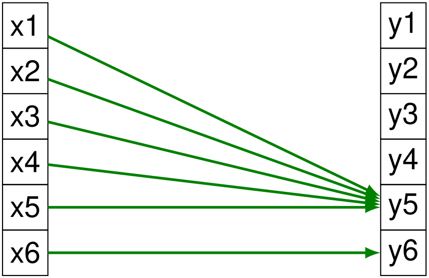
Theorem 2: Proof – if part

If part

If P $\neq$ UP, then one-to-one one-way functions exist.

- Assume $L \in$ UP - P
- Construct a function f that is
  - one-way
  - one-to-one

Construction of f in the previous thereom



Ideal construction of *f* for the current thereom

Theorem 2: Proof – if part

If part

If P $\neq$ UP, then one-to-one one-way functions exist.

- Slightly modify the proof of Theorem 1
- $f(\langle x, w\rangle) = 0x$ if w is an accepting path
- $f(\langle x, w\rangle) = 1\langle x, w\rangle$ if w is not
- Polynomial-time computable, not polynomial-time invertible and honest
- Suppose g inverts f, bring L to P by
  - Inserting 0
  - Computing g
  - Verifying $g(0x)$

Theorem 2: Proof – only if part

Only if part

If one-to-one one-way functions exist, then P $\neq$ UP.

- f is one-to-one
- Construct $L =$ $\{\langle z, pre\rangle | (\exists y)[|y| + |pre| \leq p(|z|) \wedge f(pre \cdot y) = z]\}$
- Note $L \in$ UP now
- Suppose P = UP, which implies $L \in P$.
- We can invert f by
    - Searching the prefix tree
    - $f(1...)$ and $f(0...)$ will not both be z

Lecture 2:
Do One-To-One or 2-Ary One-Way Functions Exist?

Outline

PART I : EXISTENCE OF ONE-TO-ONE ONE-WAY FUNCTIONS

Known Facts

The following were proved in the last lecture:

- One-way functions exist if and only if $P \neq NP$
- One-to-one (unambiguous) one-way functions exist if and only if $P \neq UP$

Existence Of Weaker Condition

Questions

- Can we *weaken* the sufficient condition for existence of one-to-one one-way functions?
- How about: one-to-one one-way functions exist if one-way functions exist?
- Put differently, can we prove that one-to-one one-way functions exist if $P \neq NP$?

Nice Try But . . .

Here's an attempt at a proof:

- Prove that $P \neq NP \Rightarrow P \neq UP$.
- Hence conclude that $P \neq UP$
- Existence of one-to-one one-way functions follows. QED!

Unfortunately it is not known whether $P \neq NP \Rightarrow P \neq UP$, though the converse is easily seen to be true.
Conclusion: This proof strategy does not work.

However, as it turns out, we can *actually* prove a different weaker sufficient condition. But before we proceed to do so, we need some definitions . . .

k-To-One

Definition

For each $k \geq 1$, a (possibly nontotal) function f is k-to-one if $\forall y \in range(f)[|\{x|f(x) = y\}| \leq k]$

Bounded Ambiguity

Definition

A (possibly nontotal) function f is bounded-ambiguity if there is a $k \geq 1$ such that f is k-to-one.

One-to-one functions correspond to $k = 1$ and are also known as unambiguous functions.

$UP_{\leq k}$

Definition

A language $L \in UP_{\leq k}$, $k \geq 1$, if there is a NPTM N such that

- $\forall x \in L$ $N(x)$ has at least 1 and at most k accepting paths
- $\forall x \notin L$ $N(x)$ has no accepting paths

Sufficient Condition

Finally, we state a theorem which contains the promised weaker sufficient condition:

Theorem

One-to-one one-way functions exist if and only if bounded-ambiguity one-way functions exist.

Proof

Proof:

- The "only if" direction is trivial
- How to prove the "if" (sufficiency) direction?

Proof Continued . . .

The proof consists in showing the following:

Fact 1

For each $k \geq 2$ k-to-one one-way functions exist if and only if $P \neq UP_{\leq k}$.

Fact 2

$\forall k \geq 1 \quad P = UP \Rightarrow P = UP_{\leq k}$

Proof Of Fact 1

Proof Of Fact 1:

1. "if":
   - Let $L \in UP_{\leq k} - P$ be accepted by NPTM N as in defn. of $UP_{\leq k}$.
   - Define f as
     $f(\langle x, w \rangle) = 0x$ if N(x) accepts along path w
     $f(\langle x, w \rangle) = 1\langle x, w \rangle$ otherwise
   - f is k-to-one and one-way
2. "only if":
   - Let f be k-to-one and one-way, with honesty poylnomial p
   - Define
     $L = \{\langle z, pre \rangle | \quad \exists y \quad (|y| + |pre| \leq p(|z|)) \wedge (f(pre.y) = z)\}$
   - $L \in UP_{\leq k}$ and $L \in P \Rightarrow f$ is invertible.

Proof Of Fact 2 . . .

Use induction to prove Fact 2 -

- Base Case ($k = 1$): trivial
- Induction ($k > 1$): Assume we have proved $P = UP \Rightarrow P = UP_{\leq k'}$ where $k' = k - 1 > 0$. To prove $P = UP \Rightarrow P = UP_{\leq k}$

Induction Continued . . .

Given a $L \in UP_{\leq k}$ and a NPTM N, $L = L(N)$, such that N has at most k accepting paths for each input, define
$B = \{x | N(x)$ has exactly $k = k' + 1$ accepting paths $\}$

Induction Continued . . .

Claim

Claim: $B \in UP$

Proof: Guess k distinct (lexicographically ordered) computation paths of N and accept iff each path is an accepting path

Since we assumed $P = UP$ and proved that $B \in UP$, $B \in P$

Induction Continued . . .

Claim

Claim: $D = L - B$ is in $UP_{\leq k'}$
Proof: Since $B \in P$, $x \in D$ if and only if the deterministic poly-time algorithm for B rejects x and $N(x)$ accepts.
Note: $x \notin B \Rightarrow N(x)$ has $\leq k - 1 = k'$ accepting paths

Since we assumed $P = UP$ and $P = UP \Rightarrow P = UP_{\leq k'}$, it follows that $D \in P$

Proof Complete

So we have:

- $B \in P$
- $D \in P$
- $L = D \cup B$

Since P is closed under union, $L \in P$.
Thus we have proved that $UP_{\leq k} = P$

PART II : EXISTENCE OF 2-ARY ONE-WAY FUNCTIONS

2-Ary One-Way Function

Definition: honest

A (possibly nontotal) 2-ary function $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ is *honest* if

$$\exists poly \quad q \quad \forall y \in range(f) \quad \exists x, x' \quad (|x|+|x'| \le q(|y|)) \wedge (f(x,x') = y)$$

Definition: poly-time invertible

A 2-ary function $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ is polynomial time invertible if there is a polynomial time computable function $g : \Sigma^* \to \Sigma^* \times \Sigma^*$ such that for each $y \in range(f)$

$$(y \in domain(g)) \wedge (g(y) \in domain(f)) \wedge (f(g(y)) = y)$$

Definition: 2-ary one-way function

A 2-ary polynomial-time computable function f is one-way if it is honest but not polynomial-time invertible.

S-Honest Functions

Defintion

A (possibly nontotal) 2-ary function $f : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ is *s-honest* if

- $\exists$ polynomial $q \; \forall y, u$
  $(\exists v \quad f(u, v) = y) \Rightarrow (\exists w \quad |w| \leq q(|y| + |u|) \wedge f(u, w) = y)$
- $\exists$ polynomial $q \; \forall y, u$
  $(\exists v \quad f(v, u) = y) \Rightarrow (\exists w \quad |w| \leq q(|y| + |u|) \wedge f(w, u) = y)$

Strongly Noninvertible Functions

Defintion

A (possibly nontotal) 2-ary function $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ is *strongly noninvertible* if

- f is s-honest
- There is no (total or nontotal) polynomial-time computable function $g : \Sigma^* \times \Sigma^* \to \Sigma^*$ such that $\forall y \in range(f) \quad \forall u, v \quad ((u, v) \in domain(f) \wedge f(u, v) = y) \Rightarrow ((y, u) \in domain(g) \wedge f(u, g(y, u)) = y)$
- There is no (total or nontotal) polynomial-time computable function $g : \Sigma^* \times \Sigma^* \to \Sigma^*$ such that $\forall y \in range(f) \quad \forall u, v \quad , ((u, v) \in domain(f) \wedge f(u, v) = y) \Rightarrow ((y, v) \in domain(g) \wedge f(g(y, v), v) = y)$

Existence of 2-Ary One-Way Functions

Definition

- A total 2-ary function $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ is *associative* if $\forall x, y, z \quad f(f(x, y), z) = f(x, f(y, z))$
- A total 2-ary function $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ is *commutative* if $\forall x, y \quad f(x, y) = f(y, x)$

Finally we have the following theorem:

Theorem

One-Way functions exist if and only if strongly noninvertible total commutative associative 2-ary one-way functions exist.