Limitations of black-box cryptography

15-859I
Spring 2003

Course review

- OWFs and Pseudorandomness
  - Luby: There is a OTM S such that if f is a weak OWF then S^f is a strong OWF. Proof: There is a OTM M such that if A inverts S^f then M^A inverts f.
  - HILL: There is a OTM G such that if f is a OWF, then G^f is a PRG. Proof: There is a OTM M such that if A distinguishes G^f then M^A inverts f
  - GGM: There is a OTM F such that if g is a PRG, F^g is a PRF… etc.…
  - NR: There is a OTM P such that if F is a PRF family, P^F is a SPRP family… etc…

Course review

- Symmetric Cryptography
  - There are OTMs E,D such that if F is a PRF family, E^F,D^F is a IND-CPA secure encryption scheme.
  - There are OTMs S,V such that if F is a PRF family, S^F,V^F is a SUF-CMA secure MAC…
  - There are OTMS E,D such that if (e,d) is a IND-CPA encryption scheme, and (s,v) a SUF-CMA MAC, then ($E^{e,s}$,$D^{d,v}$) is a IND-CPA+INT-CTXT ⇒ IND-CCA2 – secure encryption scheme.
  - There is an OTM f such that if E is a secure encryption scheme f^E is a OWF.

Course review

- Signatures
  - There are OTMs G,S,V such that if f is a OWF, G^f,S^f,V^f is a EUF-CMA secure signature scheme.
  - There is an OTM F such that if (G,S,V) is a EUF-CMA secure signature scheme, then F^G is a OWF.
- So, all of the following are equivalent: OWFs, Encryption, PRGs, PRFs, Signatures, MACs.
- All can be proved through the following methodology: There are OTMs B,M such that if A breaks M^N, B^A breaks N.

Course review

- Public-Key Cryptography
  - There are OTMs G,E,D such that if P is an UTP family, G^P,E^P,D^P is a IND-CPA secure PKC
  - There are OTMs G,S,P such that if E is an IND-CPA secure PKC, G^E,S^E,P^E is a UTP.
  - There are OTMs G,E,D such that if P is a trapdoor OWP, G^P,E^P,D^P is an IND-CCA2-secure PKC
- Questions: Do OWFs imply any of the above? How are OWPs and UTPs related? What about some other notions?

Plan for the next 3 weeks

- We will see that there are fundamental limitations to the black-box approach in addressing these questions.
- Impagliazzo-Rudich: A black-box proof that OWFs imply any "public-key" notion would contain a proof that P≠NP
- Several Others: In fact, almost no two public-key notions are equivalent to each other.
- If there's time: Generic constructions also have inherent efficiency limits.

Semi-Black Box and Strongly Black-Box Arguments

- A Semi-Black Box reduction has the form:
  If f is one-way, then there is no PPT A such that A^f break protocol P^f with non-negligible probability.
- A *Strongly* Black-Box reduction has the form:
  There exists a protocol P and an inverter A such that if B^f breaks P^f with non-negligible probability then $A^{B,f}$ inverts f with non-negligible probability.
- All Known Crypto Results are Strongly BB

Road Map

- Introduce "Key Agreement" (KA)
- Show P=NP implies KA is impossible
- Show a random function (permutation) oracle is a one-way function (permutation).
- Show that relative to a random oracle, if P=NP then KA is impossible.
- Conclude that giving a Semi-BB construction of KA from OWFs (OWPs) is as hard as proving P≠NP.
- Show that there is a fixed oracle relative to which OWPs exist and KA is impossible.
- Conclude that *there is no strongly Black Box construction of KA from OWFs. (OWPs)*

Key Agreement

- A Key Agreement Protocol is a pair of PPTs A,B with a common communication tape.
- A *run* of the protocol initializes A and B's random tapes and sets input tapes to 1^k.
- A and B alternate running, writing to the common tape. Call the entire history written to tape the *Conversation.*
- Finally, both write a string of length k to output tape.
- A and B *agree* if their output string is the same.
- Let α(k) denote the probability of agreement.

Key Agreement Security

- A PPTM E (weakly) *breaks* the KA protocol if given the conversation, E agrees with B's output with probability at least α(k)/poly(k)
- E *strongly breaks* a KA protocol if
  $Pr[E(k,C)=(B(1^k),A(1^k))] > (1-o(1))\alpha(k)$
- A KA protocol (A,B) is *secure* if no E (weakly) breaks (A,B)

KA and PKC

- The following "public crypto" primitives can be used to construct a KA protocol:
- Semantically Secure PKC.
- Trapdoor OWPs
- Oblivious Transfer
- Interactive PKCs.
- So KA can be seen as a "minimal public-key primitive." If we can't build KA from a OWF we can't build any of the others either.

P vs NP and Key Agreement

- Uniform Generation
  - A Relation is *polynomial time* if $(x,y)\in R$ can be decided in time $poly(|x|+|y|)$ and $|y| < poly(|x|)$.
  - A PPT M *uniformly generates R* if given an x, M either outputs "fail" (with probability at most ½) or outputs a y uniformly chosen from the set
    $$\{ y : (x,y) \in R \}$$
  - [JVV] Give an algorithm to uniformly generate any polytime R with an oracle for Σ_2. Thus if P=NP uniform generation is possible for any polytime R.

P vs NP and Key Agreement

- [BGP] give an algorithm for uniform generation given an NP oracle:
  1) If $\#R(x) = \#\{y : R(x,y)\} < 2|x|^2$ compute a listing of R(x) and choose one uniformly
  2) Otherwise, pick an $h \in H(n,i\text{-}2 \lg n, n)$ such that
     - for all a, $\#h^{-1}(a) \cap R(x) < 2n^2$ and
     - with Pr at least .9, $\exists a$ with $\#h^{-1}(a) \cap R(x) > n^2/2$
  3) Pick an a at random and list the (at most) $2n^2$ elements of $h^{-1}(a) \cap R(x)$ as $y_1,\ldots,y_s$.
  4) Pick a random $j \in \{1,\ldots,2n^2\}$. If $j < s$ output y_j, else output "FAIL"

P vs NP and Key Agreement

- Corollary: If P=NP then for any PPTM M, given an input I and an output O, we can generate a random computation (tableaux) consistent with M(I)=O
- Corollary: If P=NP, given a conversation between two interactive TMs M and N, we can uniformly generate a possible computation of M.

P vs NP and Key Agreement

- Thm: if P=NP then there is an E which breaks any KA protocol in the strongest possible sense: E computes the secret with probability exactly $\alpha(k)$
- Proof: Fix any computation of B and the resulting secret. E can generate a random computation of A consistent with the conversation. By definition, Pr[E outputs the secret] = Pr[A outputs the secret] = $\alpha(k)$.

ROs and OWFs

- We will show that A Random Oracle is a OWF.
- Recall that Random Permutations and Random functions are polynomial-time indistinguishable.
- So if we can break any KA wrt a random oracle, we can break any KA wrt a random permutation oracle.
- So our results about KA and OWFs will also apply to OWPs.

ROs are OWFs

- Claim: Fix any PPTM T. Then there is a polynomial p(n) so that $Pr_f[f(T^f(x))=x] < p(n)/2^n$.
- Proof: T makes at most p(n) queries. For each query y, $Pr[f(y)=x] = 1/2^n$ so Pr[T finds a y with $f(y)=x] < p(n)/2^n$.
- Claim: Fix any PPTM T. Let E be the event $Pr[f(T^f(x))=x] > poly(n)/2^n$. Then $Pr_f[E] < 1/n^2$.
- Proof: Markov Inequality.

ROs are OWFs

- Claim: Fix any PPTM T. Then there is a polynomial p(n) so that $Pr_f[f(T^f(x))=x] < p(n)/2^n$.
- Claim: Fix any PPTM T. Let E be the event $Pr[f(T^f(x))=x] > poly(n)/2^n$. Then $Pr_f[E] < 1/n^2$.
- Claim: For every PPTM T, there exists a polynomial q such that for measure 1 of oracles f, T inverts f on inputs of size n with probability better than $q(n)/2^n$ for only finitely many n.

ROs are OWFs

- RO Theorem: With probability 1 over random oracles f, for every PPTM T, there is a polynomial q such that $Pr[f(T^f(x)) = x] < q(n)/2^n$.
- Proof: For every PPTM T, throw away the finite number of oracles for which T inverts with probability > $q(n)/2^n$. There are countably many TMs, so we throw out a countable number of f. But there are uncountably many f. So the remainder have probability mass 1.

Uniform generation and random oracles

- Theorem implies that uniform generation *relative to a random oracle* is impossible. (why?)
- But: uniform generation consistent with a *random* random oracle is still possible. (how?)
- Given a list L of (x,f(x)) pairs, we can also uniformly generate a history consistent with a random random oracle subject to L.

KA relative to a RO

- Goal: Show that we can modify the uniform generation approach to continue working in the presence of a RO.
- Steps:
  - Give a "normal form" for KA protocols
  - Show how to weakly break any KA protocol in normal form if P=NP
  - Extend result to strongly breaking.

KA Protocol Normal Form

- A KA protocol is in normal form if it has the following form:
- A makes a single oracle query; A computes; A writes to the communication tape
- B makes a single oracle query; B computes; B writes to the communication tape; etc.
- Finally, A and B query the oracle at their respective outputs and write them to output tapes.
- Let n=poly(k) be the number of rounds.

Weakly Breaking a KANF Protocol

- High-level idea: E maintains a list L of oracle queries and answers it knows.
- After round r, repeat poly(k) times:
  - Sample a computation of A consistent with the conversation so far and a RRO subject to L.
  - Query the oracle at each of the (at most r) queries in the sample, and add the query, answer pairs to L.
- After n rounds, pick a query $q \in L$ and output q.

Why it works

- Call a query an *intersection query in round r* if it is asked in round r by one party and previously by the other party.
- Upon agreement, the secret is an intersection query.
- We will show that with high probability, the list of queries made by E includes all intersection queries.
- So given that E queries at all intersection queries and A and B agree, E's output agrees with A with probability at least 1/#L = 1/poly(k).

Why it works

- Consider the first intersection query. (IQ)
- Before it becomes an IQ, A and B's views of the oracle are independent.
- So E knows as much about A as B.
- Suppose up to round r there are no IQs and in round r+1 B's query q_{r+1} is an IQ with non-negligible probability.
- Then some non-negligible fraction of consistent computations of A must have asked q_{r+1} previously. So by sampling enough A's, E can learn q_{r+1} whp.
- Now E knows as much about A as B again. Apply induction.

Result

- We will show on Wednesday how to strengthen this to strongly breaking any KANF protocol.
- So: If P=NP KANF is impossible relative to a RO.
- Thus: proving a KA protocol is secure relative to an oracle for a OWF (Semi-BB) is as hard as proving P≠NP.

Strong BB results

- Recall: A Strong BB reduction from KA to OWFs gives an A,B,R such that:
- If E^f breaks A^f,B^f with non-negligible probability then $R^{E,f}$ inverts f with non-negligible probability.
- This proof technique *relativizes*: it holds relative to any oracle.
- So if we can give an oracle relative to which an OWF exists and no such R exists, no Strong-BB reduction from KA to OWFs exists.

The Oracle

- Previous results mean we just need to combine a random oracle with one relative to which P=NP.
- Let RO be a random oracle and define the oracle O as follows:
- $O(0||x) = x \in QSAT$
- $O(1||x) = RO(x)$
- Since relative to a QSAT oracle P=NP and $O(1||.)$ is a OWF, we get the desired result.
- Standard diagonalization gives a single oracle relative to which there is a OWF and P=NP.

Summary

- Summary:
- All known crypto results are strongly BB.
- All known "Public Crypto" primitives imply KA
- Proving via a semi-BB reduction that OWFs imply KA is as hard as proving P≠NP
- Proving via a strongly BB reduction that OWFs imply KA is *impossible.*
- So existence of PKC appears to be strictly stronger assumption that symmetric crypto; proving otherwise will involve new proof techniques.