Impagliazzo-Rudich OWF/KA separation

15-859I
Spring 2003

Road Map

- Re-Introduce "Key Agreement" (KA)
- 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.

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 Protocol Normal Form

- A KA protocol is in normal form if it has the following syntax:
- 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

- Set $E_{0,m} = \{\}$
- For round r=1 up to n
  - Set $E_{r,0} = E_{r-1,m}$.
  - For i = 1 up to m = $(3n/\delta)\ln(2n/\delta)$ ("segments")
    SIMULATE: uniformly sample an $A_{r,i}$ consistent with conversation up to round r (C_r) and a RRO subject to $E_{r,i-1}$
    UPDATE: Set $E_{r,i} = E_{r,i-1} \cup \{(q,O(q)): A_{r,I} \text{ queries } q\}$
- OUTPUT: uniformly select a $q \in E_{n,m}$.

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 Eve includes all intersection queries.
- So given that Eve queries at all intersection queries and A and B agree, Eve's output agrees with A with probability at least 1/#E = 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 Eve 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, Eve can learn q_{r+1} whp.
- Now Eve knows as much about A as B again. Apply induction.

Notation & Variables

- A_r, B_r – the set of queries the actual A,B make up to round r
- $BPQ_{r,j}$ – The set of queries made by B up to round r which are not in $L_{r,i}$. (B's Private Queries)
- W[k] : The set of possible *Worlds* for security parameter k. (random tapes of A,B,E, and oracle values up to strings of length poly(k))

Formal statement

- IQ Theorem:
  $Pr_{W[k]}[A_n \cap B_n \subseteq E_{n,m}] \geq 1-\delta$
  i.e., E finds all the intersection queries of A and B with probability at least 1-δ.
- Proof: Suppose Eve fails to find all IQs. Then there is a first round *r* prior to which Eve finds all IQs ($A_r \cap BPQ_{r,0} = \{\}$), such that $q_{r+1} \in A_{r+1} \cap B_{r+1}$ and $q_{r+1} \notin E_{r,m}$. WLOG, say Alice speaks in round r. Then $A_{r+1}=A_r$ and $q_{r+1} \in A_r - E_{r,m}$. We will show that this happens with probability at most δ/n. Thus the probability that there exists such an r is at most δ.

IQ Lemma

- IQ Lemma: WLOG, say Alice speaks in round r. Define the events:
  (C1) $A_r \cap BPQ_{r,0} \neq \{\}$ (Eve missed an IQ prior to round r)
  (C2) $q_{r+1} \notin A_r$ (q_{r+1} is not an IQ in round r+1)
  (C3) $q_{r+1} \in E_{r,m}$ (Eve finds q_{r+1})
  Then, conditioned on any choice of C_r, Eve's random choices up to round r, B's random tape, $E_{r,0}$, and $BPQ_{r,0}$,
  $Pr_{W[k]}[(C1) \text{ or } (C2) \text{ or } (C3)] \geq 1 - \delta/n$

IQ Lemma proof

- Let W*[k] be the set of worlds in W[k] which fix the variables given in the lemma statement. Notice that W*[k] all result in a fixed value for q_{r+1}.
  We will partition the set W*[k] into three sets P1, P2, and P3. We will show that:
  (P1 lemma) $Pr_{W^*[k]}[P1] \leq \delta/2n$
  (P2 lemma) $Pr_{P2}[C3] > 1 - \delta/2n$
  (P3 lemma) $Pr_{P3}[C1 \text{ or } C2] = 1$
  Giving: Pr[C1 or C2 or C3] > 1 - δ/n, QED

P1 Lemma

Define the set P1 as:

P1 = {$w \in W^*[k]$: not (C1), not (C2), and $\exists i$.
$Pr_{W^*[k]}[(C1) \text{ or } (C2) : E_{r,i}[w], EveRand_{r,i}[w]] > 1 - \delta/2n$ }

That is, the world situations in which after round r, segment i, *most worlds* would lead to (C1) or (C2) but those in P1 do not.

P1 Lemma: $Pr_{W^*[k]}[P1] < \delta/2n$

P2 Lemma

Define the set P2 as:

P2 = {$w \in W^*[k]$: not (C1), not (C2), and $\forall i$.
$Pr_{W^*[k]}[(C1) \text{ or } (C2) : E_{r,i}[w]] \leq 1 - \delta/2n$ }

That is, the world situations in which neither (C1) nor (C2) ever look likely. (The "rest" of P1)

P2 Lemma: $Pr_{P2}[\text{not C3}] < \delta/2n$

P2 Lemma proof

- In P2 worlds, there is probability at least $\delta/2n$ that A queries q_{r+1} given that Eve has discovered all of the IQs up to round r.
- So, in P2 worlds, when Eve samples an A consistent with C_r, either the sampled A makes some query which intersects $BPQ_{r,i}$ or A queries q_{r+1} with probability at least $\delta/2n$.
- But $BPQ_{r,i}$ can have at most n elements.
- So $\#\{A_{r,i} : A_{r,i} \cap BPQ_{r,i} \neq \{\}\} < n$
- Thus Eve samples at least m-n A's which query q_{r+1} with probability > $\delta/2n$

P2 Lemma proof

- Thus Eve samples at least m-n A's which query q_{r+1} with probability > $\delta/2n$
- So in a P2 world, what is the probability that Eve fails to sample an A which queries q_{r+1}?
- $Pr_{P2}[\text{not (C3)}] < (1-\delta/2n)^{m-n}$
  $= (1-\delta/2n)^{(3n/\delta)\ln(2n/\delta) - n}$
  $< (1-\delta/2n)^{(2n/\delta)\ln(2n/\delta)}$
  $< (1/e)^{\ln(2n/\delta)} < \delta/2n$, QED

P3 Lemma

- Define the set P3 = {$w \in W^*[k]$: (C1) or (C2)}
- P3 Lemma: $Pr_{P3}[(C1) \text{ or } (C2)] = 1$.
- So we have that:
  $Pr_{W^*[k]}[P1] < \delta/2n$
  $Pr_{P2}[(C3)] > 1 - \delta/2n$
  $Pr_{P3}[(C1) \text{ or } (C2) \text{ or } (C3)] = 1$
  and $|P1| + |P2| + |P3| = |W^*[k]|$
  This gives us:
  $Pr_{W^*[k]}[\text{not (C1) and not (C2) and not (C3)}] < \delta/n$.

Strongly Breaking any KANF

- StrongEve: for rounds r=1,…,n-1, the same as WeakEve. Assume secrets are distinguishable from oracle queries.
- For round n, run SIMULATE as in WeakEve. In UPDATE, maintain a list S_i which contains the last query made by $A_{r,j}$ for $j \leq i$.
- OUTPUT: a random query from S_m.
- Theorem: if $Pr[out(A)=out(B)] > 1-\alpha(k)$ then $Pr[StrongEve(C_n) = out(B)] > 1-\alpha(k)-2\delta$

Strongly Breaking KANF

- WLOG, say A queries q_{n-1}, B queries q_n. We assume $Pr[q_n \notin A_{n-1}] < \alpha(k)$
- We know from previous theorems that $Pr[A_{n-1} \cap BPQ_{n-1,i} \neq \{\}] \leq \delta$
  So with probability at least $1-\alpha(k)-\delta$ in the i^{th} segment, Eve learns either a new element of $BPQ_{n-1,i}$ or q_{n+1}. But Eve learns a new element of $BPQ_{n-1,i}$ in at most n segments, so this bad event happens in a randomly chosen segment with probability at most $n/m < \delta$.