# It’s Not The Assumption, It’s The Reduction

GMfest13c Assumptions Panel Presentation

Ran Canetti

# Let’s assume P=NP

# Let’s assume P=NP

- But proof is non-constructive…

  … and we still have no idea how to factor…

# Let’s assume P=NP

- But proof is non-constructive…

  … and we still have no idea how to factor…
- Is cryptography as we know it dead?

# Let’s assume P=NP

- But proof is non-constructive…

  … and we still have no idea how to factor…
- Is cryptography as we know it dead?
- Do we need to resort to heuristics?

# Let’s assume P=NP

- But proof is non-constructive…

  … and we still have no idea how to factor…

- Is cryptography as we know it dead?
- Do we need to resort to heuristics?

  NO!

# Let’s assume P=NP

- But proof is non-constructive…

  … and we still have no idea how to factor…
- Is cryptography as we know it dead?
- Do we need to resort to heuristics?

  NO!

The “security by reduction” paradigm still works!

# Need to change mindset

Can no longer assume

“There is no PT algorithm for factoring”.

- But it doesn’t matter:

  The universal quantifier is a nice mathematical abstraction, but doesn’t really capture what we want…

- A “good” reduction to factoring is still as valid as before!

# The case of Collision Resistant Functions [Rogaway 07]

- A single compressing function f:{0,1}*→{0,1}* cannot be CR in the standard sense:

  ∀n ∃polysize $A_n$ that finds n-bit collisions.

# The case of Collision Resistant Functions [Rogaway 07]

- A single compressing function $f:\{0,1\}^* \rightarrow \{0,1\}^*$ cannot be CR in the standard sense:

  $\forall n\ \exists$polysize $A_n$ that finds n-bit collisions.

- "Textbook" Solutions:
  - Move to asymptotic security and require A to be uniform: Way Too Weak
  - Move to a family of functions f_k : Unnatural, Unrealistic

# The case of Collision Resistant Functions [Rogaway 07]

- A single compressing function $f:\{0,1\}^*\rightarrow\{0,1\}^*$ cannot be CR in the standard sense:

  $\forall n\ \exists$polysize $A_n$ that finds n-bit collisions.

- “Textbook” Solutions:
  - Move to asymptotic security and require A to be uniform: Way Too Weak
  - Move to a family of functions f_k : Unnatural, Unrealistic
- “Real” solution:

  Forget the assumption, reduce to Human ignorance…

So, sometimes the gist is in the reduction, not the assumption…

# Classification of reductions

# Classification of reductions

- By  assumption  and complexity:  time, space, #queries,…

# Classification of reductions

- By assumption and complexity: time, space, #queries,…
- By access to the underlying adversary:
  - One pass Black Box
  - “Quantum” (uncontrollable randomness)
  - Resettable Black Box
  - General (“Non BB”)

# Classification of reductions

- By assumption and complexity: time, space, #queries,…
- By access to the underlying adversary:
  - One pass Black Box
  - “Quantum” (uncontrollable randomness)
  - Resettable Black Box
  - General (“Non BB”)
- By advice:
  - No advice: completely algorithmic **(this is what we want!)**

# Classification of reductions

- By assumption and complexity: time, space, #queries,…
- By access to the underlying adversary:
  - One pass Black Box
  - “Quantum” (uncontrollable randomness)
  - Resettable Black Box
  - General (“Non BB”)
- By advice:
  - No advice: completely algorithmic **(this is what we want!)**
  - Advice depending on security parameter + primitive

    (eg: Collision in a hash function)

# Classification of reductions

- By assumption and complexity: time, space, #queries,…
- By access to the underlying adversary:
  - One pass Black Box
  - "Quantum" (uncontrollable randomness)
  - Resettable Black Box
  - General ("Non BB")
- By advice:
  - No advice: completely algorithmic **(this is what we want!)**
  - Advice depending on security parameter + primitive

    (eg: Collision in a hash function)
  - … + adversary program ("non-uniform")

    (eg: inverse of adv's challenge, Points queried in point obfuscation)

# Classification of reductions

- By  assumption  and complexity:  time, space, #queries,…
- By access to the underlying adversary:
  - One pass Black Box
  - “Quantum” (uncontrollable randomness)
  - Resettable Black Box
  - General (“Non BB”)
- By advice:
  - No advice: completely algorithmic  **(this is what we want!)**
  - Advice depending on security parameter + primitive

    (eg: Collision in a hash function)
  - … +  adversary program  (“non-uniform”)

    (eg:  inverse of adv’s challenge, Points queried in point obfuscation)
  - … +  public randomness/  secrets

  (eg: extractable functions,knowledge of exponent/  UCE, DI-IO,…)

# Classification of reductions

- By assumption and complexity: time, space, #queries,…
- By access to the underlying adversary:
  - One pass Black Box
  - “Quantum” (uncontrollable randomness)
  - Resettable Black Box
  - General (“Non BB”)
- By advice:
  - No advice: completely algorithmic **(this is what we want!)**
  - Advice depending on security parameter + primitive

    (eg: Collision in a hash function)
  - … + adversary program (“non-uniform”)

    (eg: inverse of adv’s challenge, Points queried in point obfuscation)
  - … + public randomness/ secrets

    (eg: extractable functions,knowledge of exponent/ UCE, DI-IO,…)

**→ Viewed this way, KOE & friends are not “assumptions”; they are “holes” in a reduction that we fill via external advice.**

# The new mindset*

(This slide is a later addition… was indeed missing in the presentation)

- The goal when analyzing security of a scheme is to come up with a reduction to another problem.

# The new mindset*

(This slide is a later addition… was indeed missing in the presentation)

- The goal when analyzing security of a scheme is to come up with a reduction to another problem.

- The result statement  is now unconditional:

  *“We show how to transform an adversary that breaks X into an adversary that breaks Y.”*

  - If the transformation is not completely specified then need to be explicit about it

# The new mindset*

(This slide is a later addition… was indeed missing in the presentation)

- The goal when analyzing security of a scheme is to come up with a reduction to another problem.

- The result statement  is now unconditional:

  *“We show how to transform an adversary that breaks X into an adversary that breaks Y.”*

  – If the transformation is not completely specified then need to be explicit about it

- This has multiple corollaries:
  – In of itself:  A reduction to “Human Ignorance”
  – Non-u security of Y  implies non-u security of X
  – Uniform security of  Y implies uniform security of X
  – …

# The new mindset*

(This slide is a later addition… was indeed missing in the presentation)

- The goal when analyzing security of a scheme is to come up with a reduction to another problem.

- The result statement is now unconditional:

  *"We show how to transform an adversary that breaks X into an adversary that breaks Y."*

  - If the transformation is not completely specified then need to be explicit about it

- This has multiple corollaries:
  - In of itself: A reduction to "Human Ignorance"
  - Non-u security of Y implies non-u security of X
  - Uniform security of Y implies uniform security of X
  - …

- **(In fact, the mindset is pretty old… was around in the 80's )**