Anonymous Whistleblowing over Authenticated Channels

Thomas Agrikola, Geoffroy Couteau, Sven Maier

November 10, 2022

Motivation

Why Anonymous Whistleblowing?

SPECIAL REPORT

THE SNOWDEN SAGA

A SHADOWLAND OF SECRETS AND LIGHT

Whether hero or traitor, former National Security Agency contractor Edward Snowden is the most important whistle-blower of modern times, one whose disclosures will reverberate for decades to come. With extensive input from Snowden himself, SUZANNA ANDREWS, BRYAN BURROUGH, and SARAH ELLISON have the spy-novel-worthy tale of how a geeky dropout from the Maryland suburbs found himself alone and terrified in a Hong Kong hotel room, spilling America's most carefully guarded secrets to the world

After setting up his personal security systems and piling pillows against the door so no one in the hallway could eavesdrop, he sat on the bed, anxious and alone, in a Hong Kong hotel room. He was 29 years old that night, May 24, 2013, but he looked much younger, thin and pale, like a college kid, in his blue jeans and white T-shirt. Someone who talked to him later described him as "terrified," and it's easy to believe. He was walking away from everything he had ever known, his career, his girlfriend, his entire life, and now it appeared that his plan might fall through.

He had come to Hong Kong four days earlier, his luggage filled with laptop computers and thumb drives containing tens

Reality Winner, Former N.S.A. Translator, Gets More Than 5 Years in Leak of Russian Hacking Report

Give this article

Reality Winner received the longest sentence ever imposed in federal court for an unauthorized release of government information to the media, prosecutors said. Michael Holahan/The Augusta Chronicle, via Associated Press

Images taken from `https://archive.vanityfair.com/article/2014/5/the-snowden-saga` and `https://www.nytimes.com/2018/08/23/us/reality-winner-nsa-sentence.html`.

Motivation

Anonymous Whistleblowing

Remedy: Anonymization networks (*e.g.* TOR (Dingledine, Mathewson, and Syverson 2004), Mix-Nets (Chaum 2003), Riposte (Corrigan-Gibbs, Boneh, and Mazières 2015), Blinder (Abraham, Pinkas, and Yanai 2020), DC-nets (Chaum 1988) . . .)

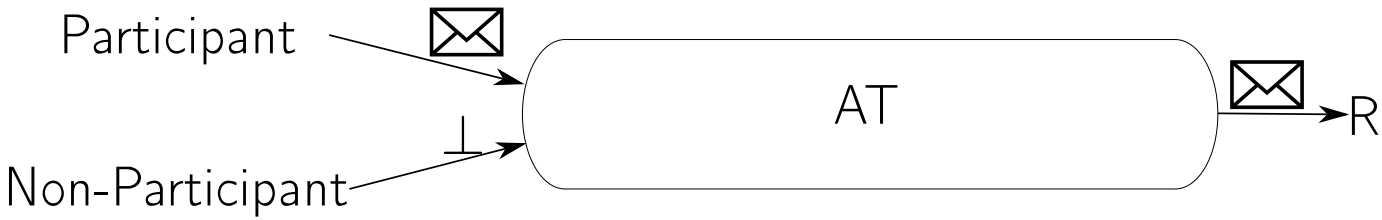
Implicit assumptions:

1. Sufficient amount of entropy
   $\Rightarrow$ this is inherent
2. Some *trusted* or *non-colluding* party is involved at some point.
   $\Rightarrow$ ***is this assumption inherent, too?***

Anonymous Transfer

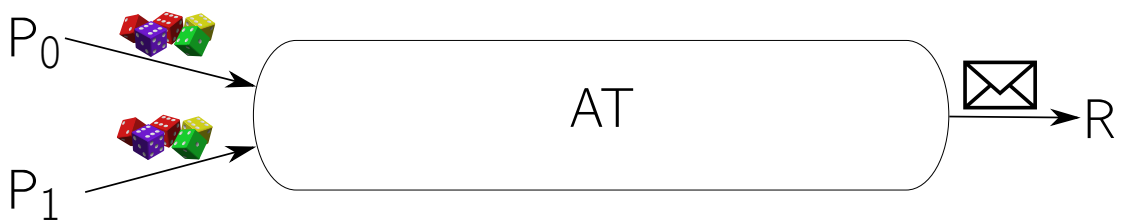
Formalization

Participants viewpoint:



Correctness: Message is delivered correctly with probability $\geq \varepsilon$.

Receivers viewpoint:



Anonymity: Receiver can determine sender with probability $\leq 1 - \frac{\delta}{2}$.

Anonymous Transfer

Impossibility

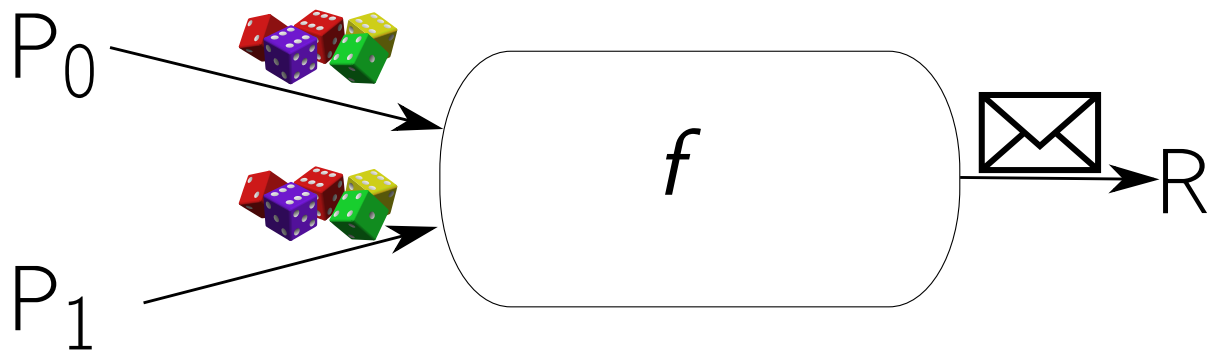
Theorem

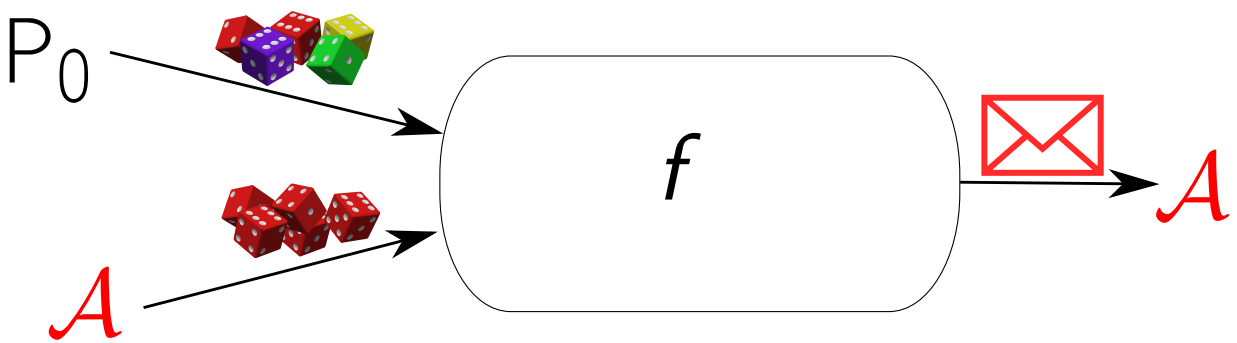
No asymptotically secure AT protocol can have $\varepsilon \in \mathsf{owhl}(\kappa)$ *and* $\delta \in \mathsf{owhl}(\kappa)$.

Anonymous Transfer

Non-Interactive

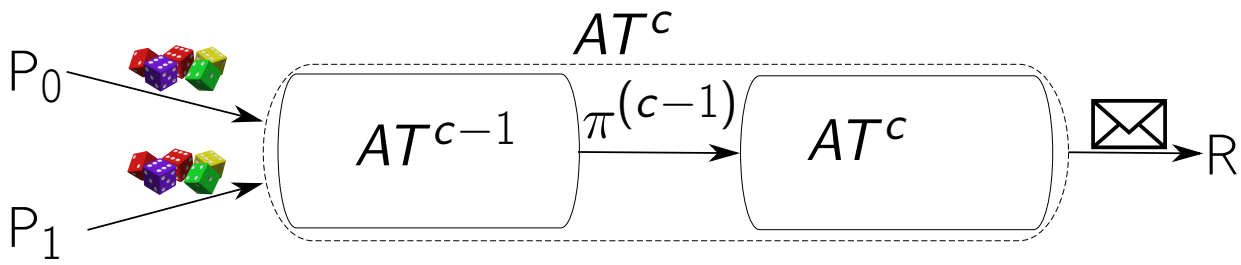
Non-Interactive AT:

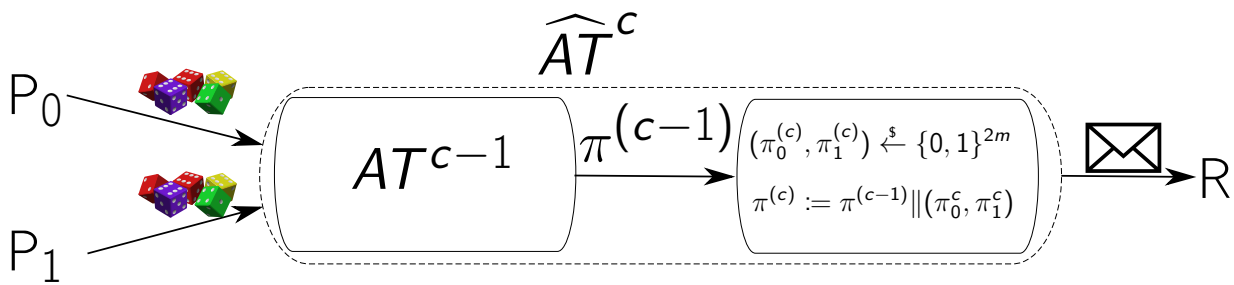




Anonymous Transfer

Interactive





Anonymous Transfer

Interactive

Intuition:

Either final round contributes much to the correctness
$\Longrightarrow$ anonymity can be attacked as before.

Or output is already fixed from previous rounds
$\Longrightarrow$ round-reduced protocol with (approximately) the same correctness.

Eventually inductive round-reductions yield single-round protocol: can use the argument from above.

Anonymous Transfer

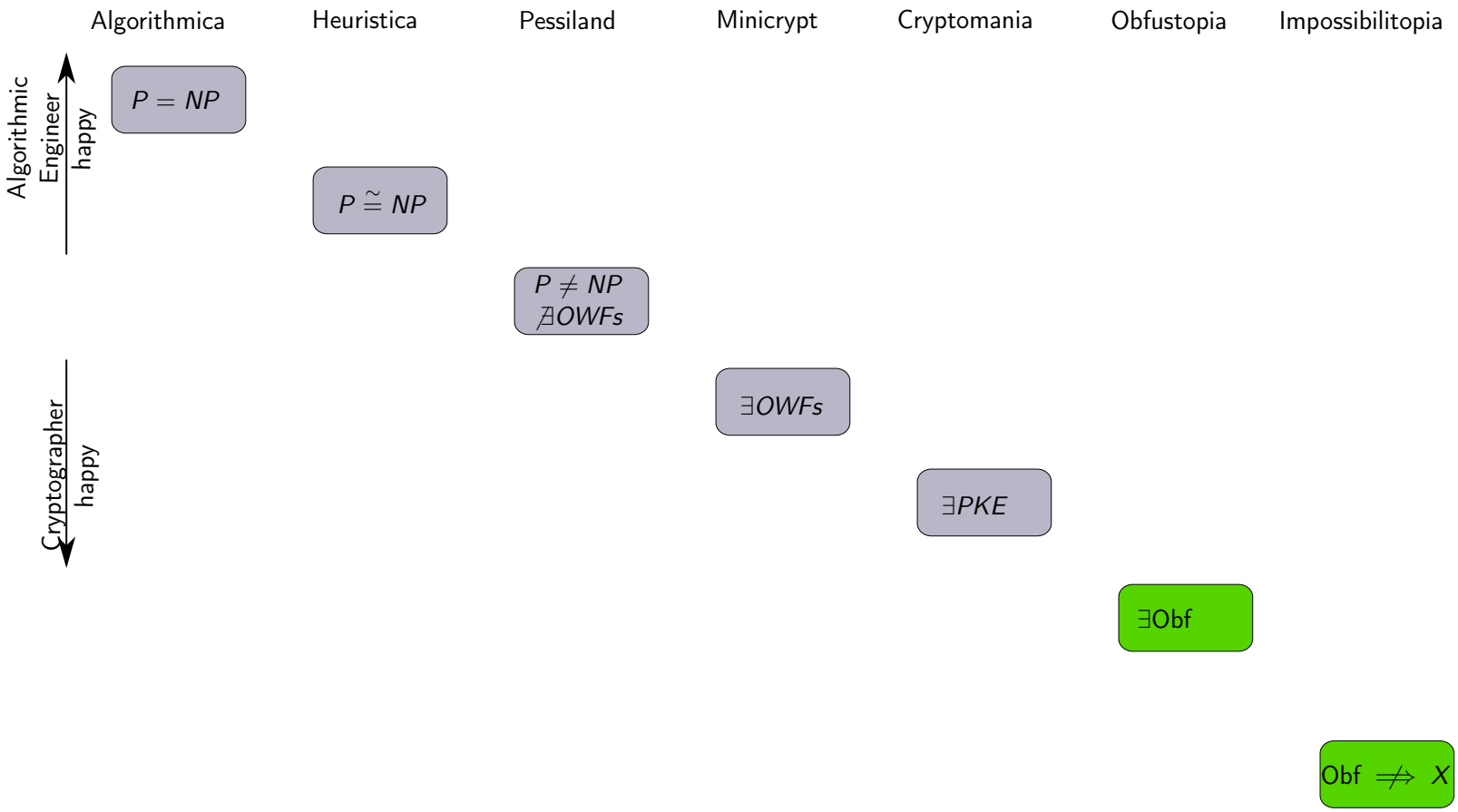
Theorem

There is no asymptotically secure Anonymous Transfer protocol with $\varepsilon \in \mathsf{owhl}(\kappa)$ *and* $\delta \in \mathsf{owhl}(\kappa)$.

Compromises:

- Investigate fixed anonymity δ.
- Investigate in the **fine-grained** setting.
- Use a strong form of obfuscation called *Ideal Obfuscation* (the existence of which does not contradict the impossibility proof).

Seven Worlds



Anonymous Transfer

Philosophical Implications

Separation between Asymptotic and Fine-Grained Worlds:

- Previous work exist.
  – Fine-Grained Public-Key Encryption (FG-*Cryptomania*) from Exponentially Secure One-Way Functions (*Minicrypt*) due to Biham, Goren, and Ishai 2008.
- Anonymous Transfer is in *classical impossibilitopia*.
- Is Anonymous Transfer in *fine-grained obfustopia*?
  $\Longrightarrow$ Open question.
  $\Longrightarrow$ Requires construction with *overwhelming* anonymity.

Conclusion

Anonymous Transfer: Transfer a bit while hiding in a group of potential senders.
Senders are unaware of the transfer and *do not* need to follow any given protocol.

Impossibility: There's no AT with perfect correctness *and* anonymity.

Instantiation: Even fine-grained instantiations are non-trivial.

Open Question: Is there an instantiation in the fine-grained world with overwhelming anonymity *and* correctness?

$\Longrightarrow$ Would imply separation of asymptotic and fine-grained cryptography at the *highest level* of Impagliazzo (1995).