

EXHIBIT C

The cr.yp.to blog

2019.04.30: [An introduction to vectorization](#)

2017.11.05: [Reconstructing ROCA](#)

2017.10.17: [Quantum algorithms to find collisions](#)

2017.07.23: [Fast-key-erasure random-number generators](#)

2017.07.19: [Benchmarking post-quantum cryptography](#)

2016.10.30: [Some challenges in post-quantum standardization](#)

2016.06.07: [The death of due process](#) A few notes on technology-fueled normalization of lynch mobs targeting both the accuser and the accused.
#ethics #crime #punishment

2016.05.16: [Security fraud in Europe's "Quantum Manifesto"](#)

2016.03.15: [Thomas Jefferson and Apple versus the FBI](#)

2015.11.20: [Break a dozen secret keys, get a million more for free](#)

2015.03.14: [The death of optimizing compilers](#)

2015.02.18: [Follow-You Printing](#)

2014.06.02: [The Saber cluster](#)

2014.05.17: [Some small suggestions for the Intel instruction set](#)

2014.04.11: [NIST's cryptographic standardization process](#)

2014.03.23: [How to design an elliptic-curve signature system](#)

2014.02.13: [A subfield-logarithm attack against ideal lattices](#)

2014.02.05: [Entropy Attacks!](#)

2016.06.07: The death of due process

Suppose someone is accused of rape, or some other horrifying crime. If the accusation is true then the perpetrator should go to jail. If the accusation is false then the source of this false accusation should pay for this slander. Clearly *someone* has broken the law.

A lynch mob forms to punish the alleged rapist by whatever means possible. A second lynch mob forms to punish the accuser, the alleged slanderer, again by whatever means possible. These mobs are full of angry people who want to be judges and juries and executioners. The members of the first lynch mob dismiss the possibility that the accusation is false. The members of the second lynch mob dismiss the possibility that the accusation is true.

Evidently many of these people are wrong: accidentally or maliciously deceived. At the same time all of these people are convinced that they know who deserves punishment.

Is it really so hard to recognize both of these directions of error? If I prejudge and punish alleged culprits who have not had their day in court, then I will inevitably punish some innocent people: the unfortunate reality is that **many accusations of crimes are false**. If I prejudge and punish *accusers* who have not had their day in court, then I will inevitably punish some innocent people: the unfortunate reality is that **many accusations of crimes are true**.

When I say "day in court", what I really mean is **due process**. Due process is a set of ethical principles that civilization has painstakingly developed over several centuries, recognizing that punishment is corrupted by many sources of error on both sides: communication is poor; memories are faulty; sometimes people don't tell the whole truth; sometimes people tell something other than the truth. I won't try to [summarize all of the principles of due process](#), but here are some of the most fundamental, well-established principles:

- The accused receives adequate notice of the allegations.
- The accused has an adequate opportunity to respond.
- Judgments are made by an unbiased tribunal.

These principles are followed by criminal courts (where, as an extra protection, defendants are presumed innocent unless and until proven guilty); by civil courts (where the winner is whichever side has the strongest overall evidence); by arbitrators; etc.

I'm not saying that judges never make mistakes. I'm saying that the lynch mobs rushing to judgment are *much more likely to make mistakes*, exactly because of the absence of due process.

Have you ever heard one side of a story, thought you understood what was going on, and then, after hearing the other side of the story, realized that you were wrong? Have you ever read news about liars being convincingly exposed in court as their lawyers watched in despair, shoulders slumped? You're seeing examples of the power of due process to correct errors. Again, I'm not saying that these systems are perfect; I'm saying that the alternatives are much worse.

Is any of this new? Is any of it hard to understand? I don't think so. Why, then, do these lynch mobs form like clockwork?

Imagine the least trustworthy person you can think of. Maybe it's a modern-day J. Edgar Hoover, or maybe it's some money-grubbing corporate type, or maybe it's one of the candidates for the 2016 U.S. presidential election. Imagine that this person, for whatever reason, wants to destroy someone's life. Look at how attractive these lynch mobs are as weapons! The first lynch mob is a weapon to destroy the life of the accused. The second lynch mob is a weapon to destroy the life of the accuser. These weapons can be used by anyone with a moderate level of marketing skill, and cost almost nothing in the Internet age.

Is it clear that this is never happening: that these weapons are never being used maliciously against innocent victims? I don't find it at all clear. Sure, the courts can be used as weapons too, but at least the courts have *some* protections against abuse.

Perhaps there's never any malice. The error rate of the lynch mobs is nevertheless terribly high: so high that the existence of these mobs cannot, must not, be tolerated by society.

Now suppose an accuser or accused claims to be the victim of a crime or slander respectively—but, instead of calling for a prosecution or a civil case or at least an arbitration, calls for a lynch mob. The costs are low, the expected damage is high, and the pesky concept of due process is neatly dodged. Is this behavior any less antisocial than the behavior of the angry people who heed the call?

Perhaps you feel, intellectually, that you understand all this, and that you detest the lynch mobs on both sides. But then a new event occurs and suddenly you're faced with angry people trying to browbeat you into joining their lynch mob, screaming either "HOW CAN YOU CONDONE THIS CRIME!" or "HOW CAN YOU CONDONE THIS SLANDER!" depending on which side they're on.

It's really not that hard to stay calm and say something like this: "We weren't there. At this point we can't be sure what happened. Sometimes accusations are true, and sometimes they aren't. It's important for a neutral judge to hear testimony from the accuser and from the accused."

But not everyone stays calm. Angry people continue to join these mobs. They blog and tweet and report their ill-informed speculations in favor of the accuser or the accused, confident in their own righteousness and blithely unaware of the possibility of being wrong. Ultimately the accused and the accuser are both punished, truth be damned.