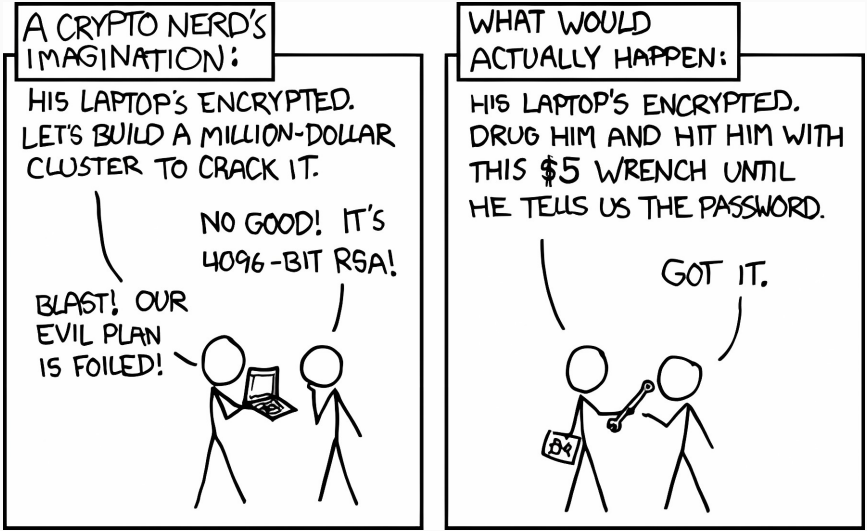
Limits of Proofs: Societal Foundations

Advanced Topics in ~~Cybersecurity~~Cryptography (7CCSMATC)

Martin R. Albrecht

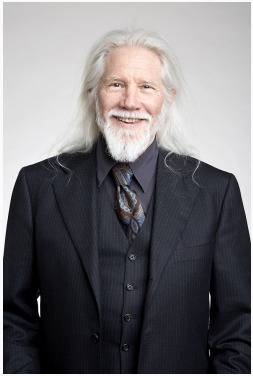
Setting Up the Question

This Lecture: How the Crypto Nerds are Right



https://xkcd.com/538/

Main Reference



Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638

Astronomically Powerful Adversaries w/o a $5 Wrench

The Tension

Randall Munroe (who writes XKCD) observes that cryptography makes two crucial assumptions:

1. The adversary has and is motivated to invest immense resources
   - it invests vast computational resources
   - it can inject messages
   - it controls the network
   - it can corrupt participating parties' devices
   - ...
2. The adversary does not use force

Concrete Security

We say a PRG is secure if no "efficient" $\mathcal{D}$ exists:

$$\forall \mathcal{D} \in t \text{ steps}: \ \mathsf{Adv}^{\mathsf{PRG}}_{G}(\mathcal{D}) = |\Pr[\mathcal{D}^{\mathsf{Game}_1} = 1] - \Pr[\mathcal{D}^{\mathsf{Game}_0} = 1]| < \varepsilon.$$

For example $(t, \varepsilon) = 2^{64}, 2^{-64}$, s.t. $t/\varepsilon = 2^{128}$.

- 2Ghz CPU: $\approx 2^{31} = 2 \cdot 2^{3 \cdot 10}$ ops per second
- $3600 \cdot 24 \cdot 365 \cdot 100 \approx 2^{11} \cdot 2^5 \cdot 2^8 \cdot 2^7 \approx 2^{31}$ seconds in 100 years
- 190 billion $\approx 2^{38}$ ARM chips by 2020.

All ARM cores ever clocked at 2GHz for 100 years gives you only 2^{100} ops.[a]

[a] All Bitcoin miners together perform about 2^{68} hashes per second.

Two Premises

Cryptography assumes (a) fundamental conflicts and (b) the absence of force.

Pre-History: Cryptography as a Military Science

Until the mid 20th century cryptography was almost exclusively confined to statecraft (the military and diplomacy).[1]

- Here parties, i.e. states, comparable in their ability to mete out violence confront each other.
- Spies may have operated behind enemy lines and could intercept messages, but lacked the required means of violence to extract decryption keys through coercion.
- Host countries of embassies could intercept the communications of embassies but refrained from violence to avoid war.

[1] "a nearly total government monopoly" [DH76]

The Modern History of Cryptography begins with Diffie-Hellman

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

— [DH76, our emphasis]

The Modern History of Cryptography begins with Diffie-Hellman

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

— [DH76, our emphasis]

The World in which Business Communications Takes Place

Any channel may be threatened with eavesdropping or injection or both, depending on its use. In telephone communication, the threat of injection is paramount, since the called party cannot determine which phone is calling. Eavesdropping, which requires the use of a wiretap, is technically more difficult and ***legally hazardous****. In radio, by comparison, the situation is reversed. Eavesdropping is passive and involves no legal hazard, while injection exposes the illegitimate transmitter to discovery and* ***prosecution****.*
— [DH76, our emphasis]

- Diffie and Hellman[a] explicitly discussed that the activities of adversaries are subject to laws.
- Cryptography ought to regulate behaviour where the law can/does not.

[a] In contrast to almost all follow-up work.

Baseline for Cryptography: Prohibition of Interpersonal Torture

A Constitutional State rules out torture.

In the UK, the $5 Wrench scenario is covered by the Human Rights Act 1998.

> *No one shall be subjected to torture or to inhuman or degrading treatment or punishment.*
> — *Human Rights Act 1998, Schedule 1*

Are We Done Yet?

Just because the State declares something as prohibited, this does not mean it does not happen.

Public authorities must not inflict this sort of treatment on you and they must also protect you if someone else is treating you in this way.

Rights and Law Depend on the Monopoly of Violence

The combination of the ***monopoly of violence and the concomitant ability to impose abstract legal norms*** *on an abstract population (confined within geographical borders) thus afforded modern positive law: a law explicitly authored by a sovereign that commands obedience from its subjects (internal sovereignty) while protecting them from occupation or interference by other sovereigns (external sovereignty).*[2]

TL;DR

The State's wrenches allows it to dictate rules: positive law prohibiting torture.

[2] Mireille Hildebrandt. Law for Computer Scientists and Other Folk. Oxford University Press, 2020, our emphasis.

Monopoly of Violence

The State amasses a superior capacity for exercising violence (the police, the prison system, the military).

Max Weber[3] even defined a modern state as:

> *Today, however, we have to say that a state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory.* — Max Weber. Politics as a Vocation. 1919

TL;DR

The State is defined by its big wrenches and the people to wield them.

The monopoly on force not only rules out interpersonal torture but any interpersonal force unless sanctioned by the State.

[3] Max Weber was one of the central figures in the development of sociology and the social sciences more generally.

Are We Done Yet?

The mere existence of superior force does not suppress interpersonal violence, this superior force must be brought to bear.

Common Assault

Definition

Common assault is when a person inflicts violence on someone else or makes them think they are going to be attacked. It does not have to involve physical violence. Threatening words or a raised fist is enough for the crime to have been committed provided the victim thinks that they are about to be attacked.

— `https://www.sentencingcouncil.org.uk/outlines/assault/`

Punishment

Common assault and battery shall be summary offences and a person guilty of either of them shall be liable to a fine not exceeding level 5 on the standard scale, to imprisonment for a term not exceeding six months, or to both.

— Criminal Justice Act 1988, Section 39

A Higher-Level Conflict: Between State and Citizen

If a person uses force against another person then the State turns this into a conflict with itself rather than merely a conflict between these two persons.

- In a criminal case, a conflict between two people (say, one with a password and one with a $5 wrench) is turned into a conflict between the State and one of these two (the one with the $5 wrench)
  - In UK law is this expressed as “Regis v That $5 Wrench Guy” where Regis means The Crown
  - In US law this is expressed as “The People v That $5 Wrench Guy”
- The State considers a threat of violence against another person as an act against its rules and itself and punishes it.

TL;DR

The use of a $5 wrench is not only illegal, but the State brings its “wrenches” to bear.

Intermediate Conclusion

Cryptography relies on power

Cryptography assumes fundamental conflicts and the absence of force. Force is ruled out in conditions of fundamental conflict by (threat of) superior force.

Discuss

Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.[4]

[4] Phillip Rogaway. The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162. 2015. URL: https://eprint.iacr.org/2015/1162.

Discuss

Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.[4]

[4] Phillip Rogaway. The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162. 2015. URL: https://eprint.iacr.org/2015/1162.

Discuss

Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.[4]

[4] Phillip Rogaway. The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162. 2015. URL: https://eprint.iacr.org/2015/1162.

A Counter Point

In this analysis, cryptography holds a unique role. If software architecture, hardware design, or protocols induce constraints on cyberspace as side effects of their primary engineering purposes (say, the delays associated with Internet packet switching), cryptography is code created with the sole purpose of regulating behavior.[5]

[5] Jean-François Blanchette. Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents. MIT Press, 2012, p.95.

A Counter Point

In this analysis, cryptography holds a unique role. If software architecture, hardware design, or protocols induce constraints on cyberspace as side effects of their primary engineering purposes (say, the delays associated with Internet packet switching), cryptography is code created with the sole purpose of regulating behavior.[5]

[5] Jean-François Blanchette. Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents. MIT Press, 2012, p.95.

Nation-State Adversaries w/o a $5 Wrench

Transition

So far, we've only covered private adversaries (or foreign adversaries) but not the (home) nation state

- Famously, the US and the UK have vast signal intelligence capabilities
- The cryptographic literature is chiefly concerned with unspecified "nation-state (level) adversaries".

(Constitutional) Nation-State Adversaries

Means

- The State monopolises means of violence in society
- The State has the wealth of society at its disposal
  - Example: UK government spending averaged between 40%-45% of the GDP each year in recent years

Motive

- To police its society, the State relies on investigative powers
- The State starts conflicts with members of its society in criminal law
  - This opens the potential for conflict from some of its subjects

Self-restraining adversary

In many countries encryption is not illegal. It is funded and promoted by governments and taught at universities.

Self-Restricting Nation-State Adversaries

That the State prevents its own the police from beating that password out of you, is a matter of public law, specifically constitutional law.[6]

> *Constitutional law restricts the competences it attributes by requiring specific safe- guards which constitute legal conditions that limit the exercise of the powers that have been allocated. This clearly shows the constitutive and limitative nature of the attribution of powers in a constitutional democracy. These limitations may concern procedural or substantial prerequisites, for example, making sure that privacy is not unnecessarily infringed, unjustified discrimination is prevented, and the freedom of speech is not violated.*[7]

[6] The Human Rights Act 1998 is an example of constitutional law since it also binds the State.

[7] Mireille Hildebrandt. Law for Computer Scientists and Other Folk. Oxford University Press, 2020.

That the State prevents its own the police from beating that password out of you, is a matter of public law, specifically constitutional law.[6]

> *Constitutional law restricts the competences it attributes by requiring specific safe- guards which constitute legal conditions that limit the exercise of the powers that have been allocated. This clearly shows the constitutive and limitative nature of the attribution of powers in a constitutional democracy. These limitations may concern procedural or substantial prerequisites, for example, making sure that privacy is not unnecessarily infringed, unjustified discrimination is prevented, and the freedom of speech is not violated.*[7]

[6] The Human Rights Act 1998 is an example of constitutional law since it also binds the State.
[7] Mireille Hildebrandt. Law for Computer Scientists and Other Folk. Oxford University Press, 2020.

“Crypto Wars”: Limits to Self-Restraint I

> *(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds— (a) that a key to the protected information is in the possession of any person,*
> *[...]*
> *the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.*
> *[...]*
> *(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary— (a) in the interests of national security; (b) for the purpose of preventing or detecting crime; or (c) in the interests of the economic well-being of the United Kingdom.*
> — *Regulation of Investigatory Powers Act 2000 (RIPA), Section 49*

Refusal can result in a maximum sentence of two years imprisonment, or five years in cases involving national security or child indecency.

“Crypto Wars”: Limits to Self-Restraint II

> *(2) A notice under subsection (1) that relates to a regulated user-to-user service is a notice requiring the provider of the service— (a) to do any or all of the following— […]*
> *(iii) use accredited technology to identify CSEA content, whether communicated publicly or privately by means of the service, and to swiftly take down that content;*
> — *Online Safety Act 2023, Section 121*

“content” means anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description;

Intermediate Conclusion

Cryptography has its limits in power

The limits to the self-restraint of nation-state adversaries are the limits of cryptography outside the realm of statecraft.

Discuss: IACR Copenhagen Resolution

The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards. Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.[8]

[8] https://www.iacr.org/misc/statement-May2014.html

Discuss: IACR Copenhagen Resolution

The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards. Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.[8]

[8] https://www.iacr.org/misc/statement-May2014.html

Adversarial Reasons

"Why govern at all?"

The IACR Copenhagen Resolution expresses a classical liberal idea:

As Foucault points out, liberalism historically became identified with the idea that there might be an excess of government, one which opens the way for the state to trample on civil society in general and liberty in particular. But the suspicion that there is always a risk of too much government is always tied to the question: why is it necessary to govern at all?[9]

Too much of government begs the questions:

- What is the right "amount" of government?
- For what reason does government exist?

[9] Mark Neocleous. Critique of Security. Edinburgh University Press, 2008, p.27.

Partial Answer

- Cryptography presumes fundamental conflicts and the absence of force.
- A status of conflict can only be perpetual if force is ruled out by superior force.

Left to answer:

What brings about such a perpetual state of conflict?

Hobbes: Violence is the State of Nature

For **Thomas Hobbes**, humans are so driven by their desire for pride, revenge and natural passions that nothing is secure in the state of nature. A sufficiently strong authority is required for our security:

> *"The only way to erect such a Common Power, as may be able to defend them from the invasion of Forraigners, and the injuries of one another, and thereby to secure them … is to conferre all their power and strength upon one Man, or upon one Assembly of men, that may reduce all their Wills, by plurality of voices, unto one Will." — Thomas Hobbes, Leviathan, 1651*

[DH76]: Adversarial Reasons: Business

Diffie & Hellman give two reasons for adversarial behaviour and why security controls – whether cryptographic in nature or otherwise – are required:

> *For example, submitting a proposal to a competitor may result in his enciphering it for transmission to his headquarters.*

> *For example, a dishonest stockbroker might try to cover up unauthorized buying and selling for personal gain by forging orders from clients, or a client might disclaim an order actually authorized by him but which he later sees will cause a loss.*

Conflicts to Regulate

The problem of authentication is perhaps an even more serious barrier to the universal adoption of telecommunications for business transactions than the problem of key distribution. Authentication is at the heart of any system involving contracts and billing. Without it, business cannot function. Current electronic authentication systems cannot meet the need for a purely digital, unforgeable, message dependent signature. They provide protection against third party forgeries, but do not protect against disputes between transmitter and receiver.
— [DH76, emphasis added]

Business Conflicts are Regulated by Judges

> *It must be easy for anyone to recognize the signature as authentic, but impossible for anyone other than the legitimate signer to produce it.*
> *— [DH76, emphasis added]*

Rivest, Shamir, Adleman solved the authentication problem posed in [DH76] make the conflict resolution between signer (sender) and verifier (receiver) via a judge explicit:

> *If electronic mail systems are to replace the existing paper mail system for business transactions, "signing" an electronic message must be possible. The recipient of a signed message has proof that the message originated from the sender. This quality is stronger than mere authentication [...]; the recipient can convince a "judge" that the signer sent the message. To do so, he must convince the judge that he did not forge the signed message himself!*
> *— [RSA78, emphasis added]*

Good Company: Locke, Smith, Hegel, ...

"The great and chief end therefore, of Mens uniting into Commonwealths, and putting themselves under Government, is the Preservation of their Property." — John Locke. Second Treatise. 1689

"[T]he first and chief design of every system of government is to maintain justice; to prevent the members of a society from incroaching on one anothers property, or seizing what is not their own." — Adam Smith. Lectures on Jurisprudence. 1763

This primary mode of freedom is the one which we are to become acquainted with as ***property****, the sphere of formal and abstract right. To this sphere there also belong property in its mediated form as* ***contract****, and right in its infringement as* ***crime*** *and* ***punishment****. — Georg W. F. Hegel. Outlines of the Philosophy of Right. 1820, emphasis in the original*

For liberalism, the link was clear: liberty is dependent on property and vice versa, but both can flourish only in conditions of security.

[...]

It is this that distinguishes the fear that Hobbes believes drives the atomised individuals in the state of nature into the security of the sovereign from the fear of the loss of liberty-property which Locke believes is the driving force behind the creation of a more secure body politic.
— Mark Neocleous. Critique of Security. Edinburgh University Press, 2008, *p.29/30*

Non-Repudiation

- [DH76] and [RSA78] were both concerned with what is called “non-repudiation” in law.
- They envisioned contracts and the disputes arising from them as a major area of conflict for cryptography to regulate behaviour in.
- Their vision did not pan out:
  - The link between standard notion of security for a signature scheme envisioned by them – EUF-CMA – and “non-repudiation” is a bit more mediated than they perhaps anticipated
  - E-commerce took off without cryptographic digital signatures under contracts being common.
- This disconnect is the topic of the next lecture.

Fin

"The first blind spot stems from the idea that 'natural security concerns' exist as timeless entities, independent of the cryptographer's own social and historical world"

[Bla12]

References I

[Bla12] Jean-François Blanchette. **Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents.** MIT Press, 2012.

[DH76] Whitfield Diffie and Martin E. Hellman. **New Directions in Cryptography.** In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[Hil20] Mireille Hildebrandt. **Law for Computer Scientists and Other Folk.** Oxford University Press, 2020.

[Neo08] Mark Neocleous. **Critique of Security.** Edinburgh University Press, 2008.

[Rog15] Phillip Rogaway. **The Moral Character of Cryptographic Work.** Cryptology ePrint Archive, Report 2015/1162. 2015. URL: https://eprint.iacr.org/2015/1162.

References II

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.** In: *Communications of the Association for Computing Machinery* 21.2 (Feb. 1978), pp. 120–126. DOI: 10.1145/359340.359342.

[Web19] Max Weber. **Politics as a Vocation.** 1919.