Applying cryptography to protect privacy

Applications, usability, and uptake of Privacy Enhancing Technologies

Victor Morel
https://victor-morel.net/

Chalmers University of Technology

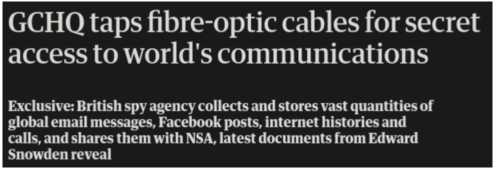
morelv@chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY

9th December 2022

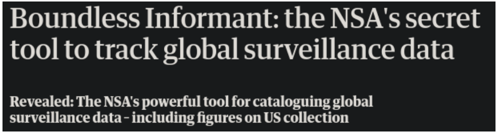
Something happened in 2013

Remember this guy?



GCHQ taps fibre-optic cables for secret access to world's communications

Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA, latest documents from Edward Snowden reveal



Boundless Informant: the NSA's secret tool to track global surveillance data

Revealed: The NSA's powerful tool for cataloguing global surveillance data - including figures on US collection

https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Crypto as a remedy?

What I hope you will learn in this lecture

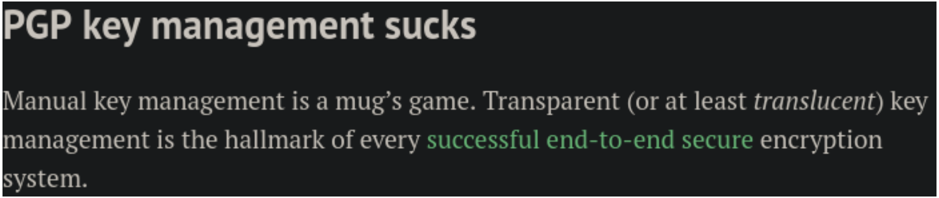
- Unusable crypto systems are (arguably) bad crypto
- Outdated crypto defeats its purpose
- And so does badly implemented crypto
- But crypto can be well done! ... and that's really worth it

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Pretty Good Privacy

PGP ain't that bad, yet ...



PGP key management sucks

Manual key management is a mug's game. Transparent (or at least *translucent*) key management is the hallmark of every successful end-to-end secure encryption system.

Long story short: it involves individuals signing each others' keys

Pitfall

Usability (and therefore uptake)

https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/
https://moxie.org/2015/02/24/gpg-and-me.html

Of the difficulty of having a certificate twenty years ago

HTTPS used to be expensive

As in *financially* expensive! In 2002:

> *GeoTrust sells its certs for $119 a year, compared to VeriSign's between $250 and $350.*

Pitfall

Uptake

https://www.theregister.com/2002/07/24/theres_certs_and_certs_verisign/
https://www.ssldragon.com/blog/evolution-of-ssl-certificates-over-20-years/

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Out of the box E2E messaging

E2E messaging app by default:

- Signal
- [matrix]
- WhatsApp

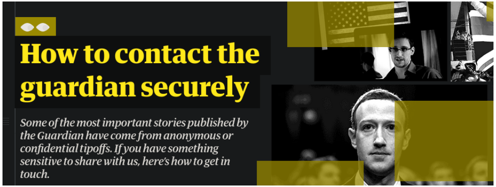
Turnkey encrypted email solutions:

- Proton Mail
- Tutanota®

Uptake

✅ Many communications are secure by default!

Safe communications for whistleblowing

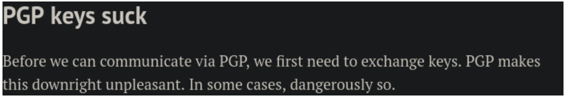


How to contact the guardian securely

Some of the most important stories published by the Guardian have come from anonymous or confidential tipoffs. If you have something sensitive to share with us, here's how to get in touch.

They provide solutions tailored to the *threat level*, as well as pros and cons!

PGP not that bad in combination with Thunderbird, although:



PGP keys suck

Before we can communicate via PGP, we first need to exchange keys. PGP makes this downright unpleasant. In some cases, dangerously so.

Loooong, hard to manage keys

Still, it is fair to conclude that

Usability

✅

https://www.theguardian.com/help/ng-interactive/2017/mar/17/contact-the-guardian-securely

Encrypt the web

Google made HTTPS almost mandatory in 2014 (incentive via SEO)
Let's encrypt and *HTTPS Everywhere* finalized the move to encrypt web traffic

HTTPS Is Actually Everywhere

Uptake

✅ (more than 95% of the global traffic)

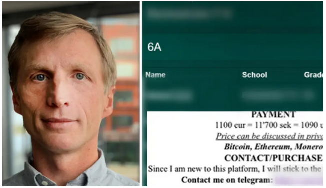
HTTPS everywhere in maintenance mode

https://www.eff.org/deeplinks/2021/09/https-actually-everywhere

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Using outdated schemes when storing passwords

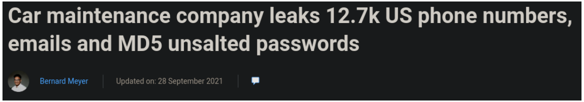


6A

Name School Grade

PAYMENT
1100 eur = 11'700 sek = 1090 u
Price can be discussed in priva
Bitcoin, Ethereum, Monero
CONTACT/PURCHASE
Since I am new to this platform, I will stick to the
Contact me on telegram: [redacted]

Yet another data leak, October 2022



Car maintenance company leaks 12.7k US phone numbers, emails and MD5 unsalted passwords

Bernard Meyer | Updated on: 28 September 2021

And one with notoriously outdated hash algorithm

Pitfall

Outdated

https://www.svt.se/nyheter/lokalt/vast/it-experten-om-vklass-och-lackta-elevuppgifterna-i-goteborg

https://cybernews.com/security/xado-leaks-us-phone-numbers-emails-md5-unsalted-passwords/

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Proper implementation of password storage schemes

Hacked but not compromised

Up-to-date

✅

https://www.theregister.com/2022/12/01/lastpass/

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Your ID please!

SYSTEM
BOLAGET

Alice 🧑 wants to buy 🍷

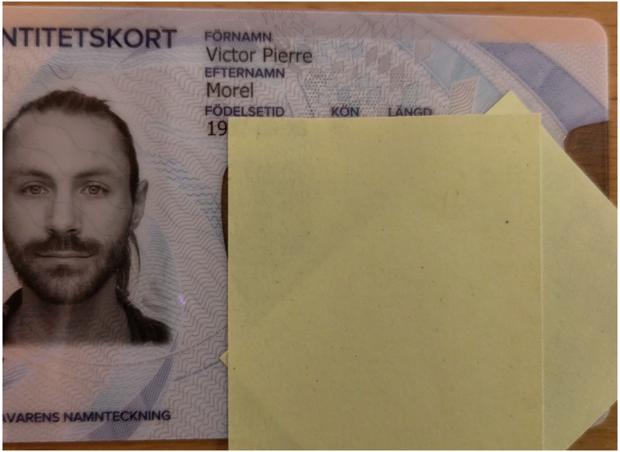
- SB (verifier) asks Alice (prover) their ID
- But an ID includes lots of superfluous information:
  - Exact age
  - Nationality
  - Gender
  - Name
- Not privacy-friendly!

How can Alice proves she's over 21 without revealing her exact age (nor being tracked)?

Old enough?

Grow a beard?
→ Sexist and unreliable

A clever (??) trick



NTITETSKORT

FÖRNAMN
Victor Pierre

EFTERNAMN
Morel

FÖDELSETID
19

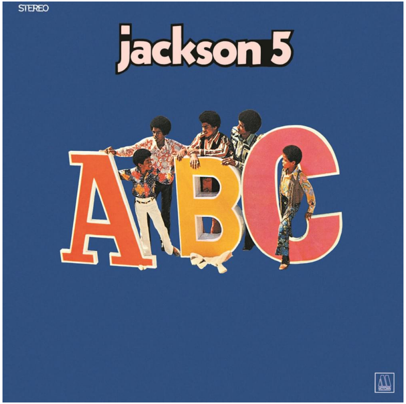
KÖN

LÄNGD

VARENS NAMNTECKNING

Hide the last two digits of your ID card?
→ only works if you're born in the last century ...

ABC



You mean the song by the Jackson Five?

→ More like Attribute Based Credentials!

ABC? Easy as 1, 2, 3

Briefly put

- It's a form of authentication mechanism
- Allows to flexibly and selectively authenticate different attributes about an entity
- Without revealing additional information about the entity (zero-knowledge property).

For instance

Prove to System Bolaget you are over 21 without disclosing your *exact* age.

ABC is a system, it requires:

Blocks and properties

- Basic blocks (some are primitives but not all)
- Main requirements a protocol should meet

http://www.cs.ru.nl/~gergely/thesis.html

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Pedersen commitment

Pedersen Commitment Scheme

Setup(sec.par) → ($\mathbb{G}$, q, g, h)
Commit(m,r) = $g^m h^r$ mod q =: c
Open(m,r,c) = 1 if c = $g^m h^r$ mod q,
and 0 otherwise

Setting: g,h are two distinct generators of a group $\mathbb{G}$ of order q

Binding? yes, *computationally*

Prob[Commit(m , r) = c = Commit(m*, r*) | m≠m*] ≤ negligible

Proof by reduction:

Given the values {c, (m,r) , (m*,r*)} we can extract the discrete logarithm of h with respect to g via

$$dLog_g(h) = \frac{m^* - m}{r - r^*}$$

Hiding? yes, information-theoretically

|Prob[b* = b] - 1/2| ≤ negligible

Proof: for every m_1 there exist an r* s.t. commit(m_1,r*)=commit(m_0,r) [similar to the one time pad]

Credentials signature

- An Attribute-Based Credential can be realised as a (generalised) Pedersen commitment signed by a credential issuer.
- Brands [1] proposes a signature that can be used for Attribute-Based Credentials.
- Camenisch and Lysyanskaya [2] propose another signature scheme to construct Attribute-Based Credential, also based on a Pedersen commitment.

[1] S. A. Brands. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.

[2] Camenisch, Jan, and Anna Lysyanskaya. "A signature scheme with efficient protocols." International Conference on Security in Communication Networks.

Group signatures (basically)

Group Signatures

signers / group members

group manager

Group signatures (less basically)

Group Signatures

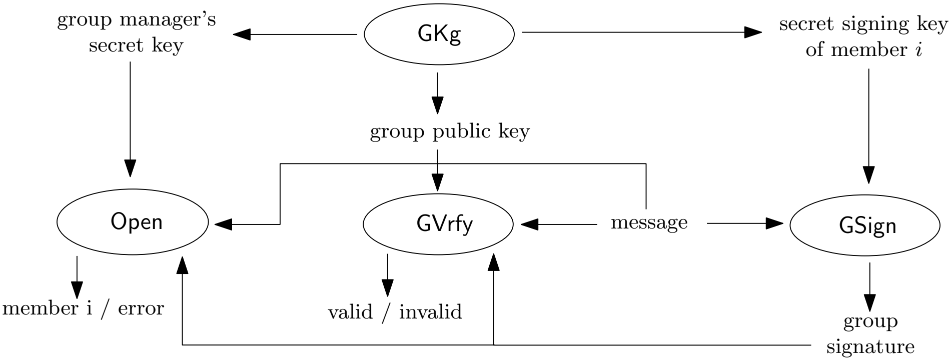


Figure 1.1.: Static Group Signatures

Achieving zero-knowledge proof

- One party (🧑 the prover) can prove to another party (🍷 the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.
- An (honest verifier) zero-knowledge proof of knowledge has to be:

  Complete If the prover knows x, they can convince the verifier

  Sound If the prover doesn't know x, they **can't** convince the verifier

  Zero knowledge The verifier does not learn any other information but that the prover knows x

Blind signatures

Blind signatures

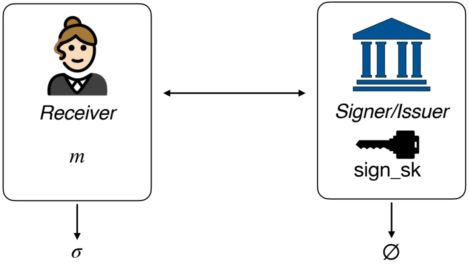
Blind Signatures

Definition: Blind Signature

A blind signature scheme is a signature scheme where the signing algorithm algorithms $Sign$ is replaced by an *interactive protocol* run between a signer/issuer (S) and a receiver (R).

The protocol starts with R who has as input a message m, and S who has as input a secret key sk.

At the end of the interaction R obtains a signature σ on m, and S learns nothing about m or σ.



🧐 *where can this be useful?*

untraceable electronic payment system

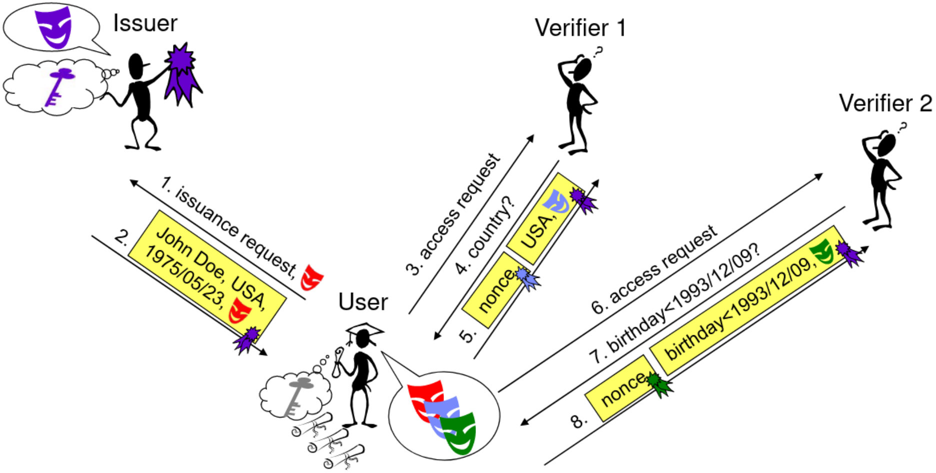
attribute-based credentials *[ABC, lecture 12 by Victor]*

Combining the blocks

Attribute-Based Credentials can be designed as such:

- Construct a suitable signature scheme:
  a) Consider a commitment scheme;
  b) Generalize the commitment scheme to a tuple of values instead of only one value;
  c) Apply a signature on the commitment.
- Develop ABC protocols based on the signature:
  (a) Use a blinded version of the signature for issuing;
  (b) Apply a (zero) proof of knowledge for selective disclosure.

A possible implementation - Idemix



https://csrc.nist.gov/csrc/media/events/meeting-on-privacy-enhancing-cryptography/documents/neven.pdf

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Security features (requirements)

S1 Authenticity: Alice 🧑 has a genuine credential

S2 Unforgeability: (3^{rd} party) Eve 😈 can't forge a credential

S3 Non-repudiation: Credentials issuer can't deny

S4 Non-transferability: Alice 🧑 can't transfer her credential to Bob 👶

Privacy features (requirements)

P1 Offline issuer: The issuer doesn't have to be online when Alice 🧑 buys 🍷

P2 Issuer unlinkability: The issuer can't track Alice 🧑

P3 Multi-show unlinkability: System Bolaget 🍷 can't track Alice 🧑

P4 Selective disclosure: Alice 🧑 can show her age OR her subscription to the 🎭 independently

P5 Minimal information: When Alice 🧑 shows her age, her name doesn't leak

→ Although everyone knows Alice here!

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Demonstration

A demonstration of a minimal ABC system

- Uses group signatures
  → Seen in Lecture 7!
- Signatures are not blind
- Unlinkability is not guaranteed 😭

Demo time! ⌨️

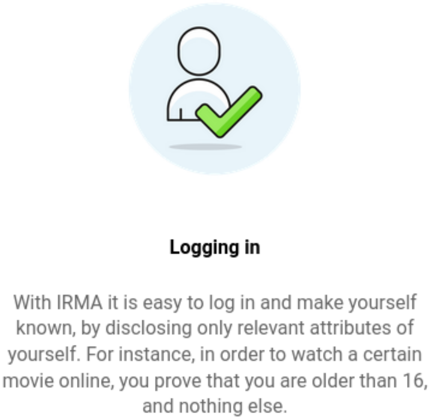
Baseline for Bonus HA3

A full-fledged ABC system - IRMA

Open-source applications actually used in the real-world!

https://irma.app/ & https://privacybydesign.foundation/en/

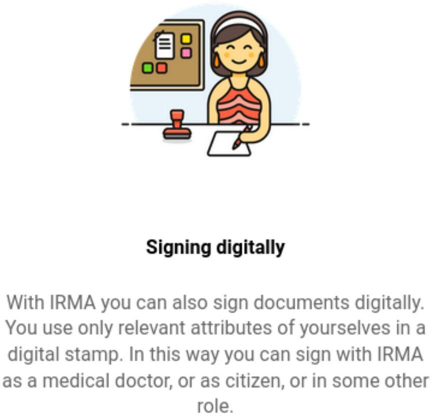
IRMA - dutch BankID (and privacy-friendly)



Logging in

With IRMA it is easy to log in and make yourself known, by disclosing only relevant attributes of yourself. For instance, in order to watch a certain movie online, you prove that you are older than 16, and nothing else.

IRMA - signing



Signing digitally

With IRMA you can also sign documents digitally. You use only relevant attributes of yourselves in a digital stamp. In this way you can sign with IRMA as a medical doctor, or as citizen, or in some other role.

IRMA - usages

In the Netherlands, IRMA is used

- In the health sector
- In municipalities
- Universities
- Insurances
- Signing documents
- Covid stuff
- etc

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Backdoors 101

What's the catch?

Encryption backdoors

- It might mean that something random is not so random
- Hard to tell if intentional (backdoor) or not (vulnerability)
- Also related to *front doors*

→ Back or front, same result: the system is not safe anymore

https://www.thesslstore.com/blog/all-about-encryption-backdoors/

https://www.quora.com/The-NSA-put-a-backdoor-in-Dual_EC_DRBG-Could-there-be-a-backdoor-in-AES-as-well

Surveillance and backdoors

What can go wrong?

Surveillance

- Illegitimate state-surveillance (NSA, GCHQ, etc)
- Some governments are pushing for backdoors 🚪
- ... but it's a very bad idea!
- Weakening cryptography weakens it for **everybody**

Pitfall

Intentionally compromised crypto

https://www.schneier.com/essays/archives/2007/11/did_nsa_put_a_secret.html

https://www.theverge.com/2020/10/12/21513212/backdoor-encryption-access-us-canada-australia-new-zealand-uk-india-japan

http://dspace.mit.edu/handle/1721.1/97690

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Compromised crypto and large-scale surveillance ... so what?

A guy once said:

> *Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.*

I don't have anything to hide

... not necessarily for you!

We don't exactly live in an ideal world

- Some socially dominated groups needs privacy, it's a human right
- Enshrined in Article 8 of the Charter of Fundamental Rights of the European Union

Why privacy matters

According to Daniel J. Solove:

- Limit on Power
- Respect for Individuals
- Reputation Management Systembolaget 👋
- Maintaining Appropriate Social Boundaries
- Trust
- Control Over One's Life
- Freedom of Thought and Speech
- Freedom of Social and Political Activities
- Ability to Change and Have Second Chances
- Not Having to Explain or Justify Oneself

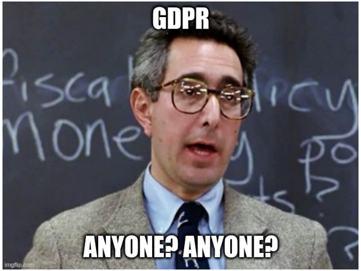
An overlooked link between cryptography and privacy is law.

`https://teachprivacy.com/10-reasons-privacy-matters/`

Encryption in EU law

Encryption enables the application of justice

→ Privacy can be implemented by architecture and by policy
... but the latter cannot function without the former!



Law can foster the use of encryption - General Data Protection Regulation

- GDPR Art 32(1)(a) talks about *the pseudonymisation and encryption of personal data;*
- DPA can impose fines otherwise (€600,000 for EDF recently)
- Recital 83 encourages the application of security through encryption

https://techletters.substack.com/p/techletters-107-probabilistic-user

Using crypto appropriately

Critical mass (there's safety in numbers)

- If everyone use it, those who need it are protected: see Iran for instance
- See also how the widespread use of SSL/TLS prevents eavesdropping and mass surveillance (thanks to the combo *Let's encrypt/HTTPS everywhere*).

Cryptography makes much more sense at the scale of society

- Standards reduce the odds of encryption backdoors!
- Large scale adoption can be driven by law (see GDPR)

https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

Outline

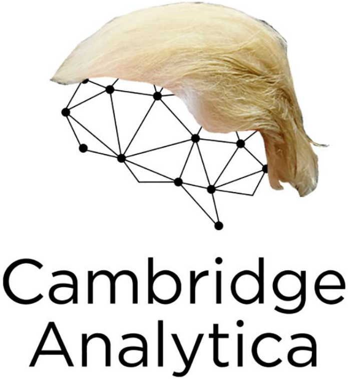
1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

Cannot protect against business surveillance

If you give the keys, the security of the lock doesn't matter

https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

Two sides of the same coin



https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

Outline

1. Securing communications
   - The bad stuff
   - The good stuff
2. Securing data and systems
   - The bad stuff
   - The good stuff
3. A PET in practice: ABC
   - Cryptographic requirements
   - Features for an ABC system
   - Real world use
     - Demonstration
     - IRMA
4. Securing society at large
   - The bad stuff
   - Why the good stuff?
5. Conclusion
   - What crypto cannot do
   - Crypto is a tool

A tool to protect privacy

Crypto is a tool

One needs to know how to handle a tool

Crypto is not the only tool to protect privacy

- Law is a tool as well
- Privacy by architecture and by policy go hand in hand

https://ieeexplore.ieee.org/iel5/32/4771845/04657365.pdf