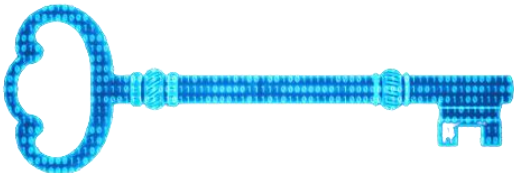




Cryptography: Applications

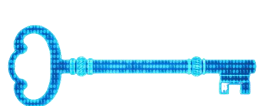
Dr. Balázs Pejő

www.crysys.hu



Agenda

- Dark Patterns
- Tracking
- GDPR
- Machine Learning
- Deidentification
- Anonymization
- Cryptography
- Secure Messaging
 - Signal
- Steganography
- Anonymous Communication
 - Mix Nets
 - Tor
 - Dark Web
- Cryptocurrencies
 - Private Coin
- E-Voting
- Other PETS



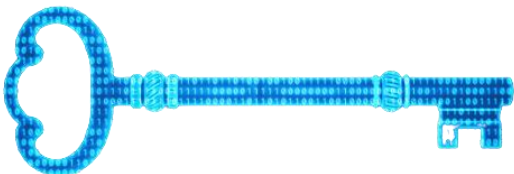
Recap

- The attacker is assumed to know your system (except your private message and secure key).
- Confidentiality and Integrity are key objectives of cryptography.
 - Encryption could tackle the former, MAC and Digital Signatures could tackle the latter.
- Cryptographic hash functions are suitable building blocks of MACs and Commitment schemes.
- While HE enables operations on the ciphertext, SMPC enables joint operations amongst several participants (such as PSI).
- PIR aims to hide the accessed information, while ZKP aims to prove knowledge without revealing that.





Secure Messaging



Snowden Revelations

BBC NEWS

Edward Snowden: Leaks that exposed US spy programme

© 17 January 2014

Edward Snowden, a former contractor for the CIA, left the US in late May after leaking to the media details of extensive internet and phone surveillance by American intelligence. Mr Snowden, who has been granted temporary asylum in Russia, faces espionage charges over his actions.

- Snowden's disclosures revealed numerous global surveillance programs run by the NSA and prompted a cultural discussion about national security and individual privacy.
 - <https://www.lawfareblog.com/snowden-revelations>

The Guardian

Reuters

Thu 3 Sep 2020 14:54 BST

NSA surveillance exposed by Snowden was illegal, court rules seven years on

- Whistleblower revealed collection of phone records to Guardian
- Court says officials who defended dragnet were not telling truth

NEWS

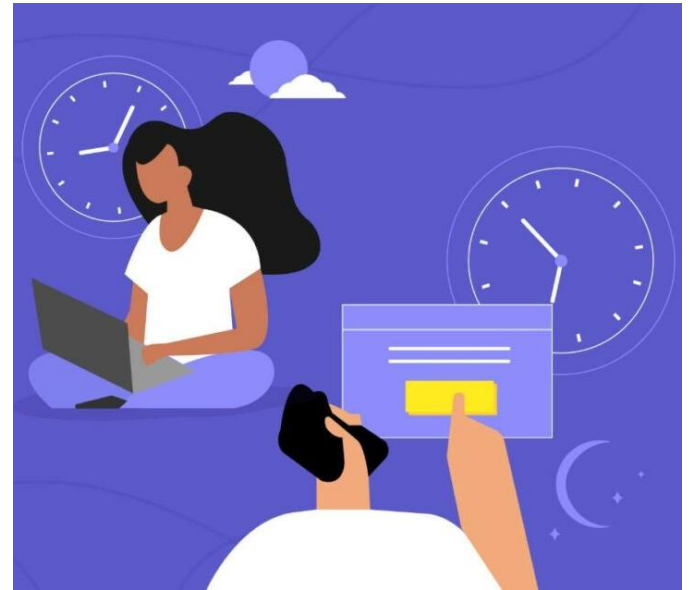
Snowden Leaks Could Cost Military Billions: Pentagon

It might take two years to determine the extent of the damage, Joint Chiefs chairman Gen. Martin Dempsey told Congress.

March 6, 2014, 11:27 PM CET / Updated March 6, 2014, 11:27 PM CET

Secure Messaging

- Secure transmission of instant messages among two or more communicating parties.
- Messages transmitted in real time over the internet.
 - No unauthorized third party can access the content of the communications.
 - Content: text, audio, video, files, etc.
- Synchronous communication requires users to be always on-line.
- Asynchronous communication is a must in the era of smart-phones.
 - Users cannot always be available, messages sent to them need to be temporarily stored at 3rd party servers.



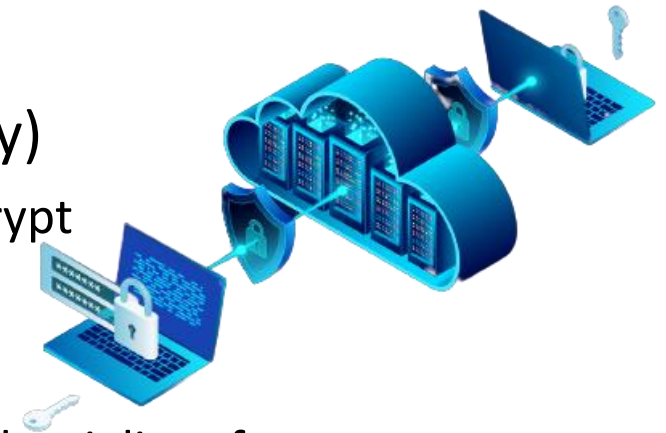
Adversary Model

- Active adversaries
 - Adversaries who may modify messages, mount Man-in-the-Middle attacks, etc.
- Passive adversaries (or honest-but-curious)
 - Adversaries sniffing the traffic and infer from the logged traffic as much as possible
- Service providers
 - Servers buffering the messages can also be malicious.
- Clients (and their device) are supposed to be honest.



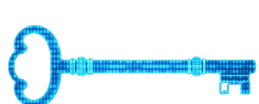
Security Properties

- (Message integrity)
- End-to-end encryption (confidentiality)
 - Only the communicating parties can decrypt the messages (i.e., the server cannot).
- Perfect forward secrecy
 - Key compromise will not affect the confidentiality of past messages.
- Future secrecy
 - Key compromise will not affect the confidentiality of future messages.
- Sender and receiver authentication
- Sender and receiver anonymity
 - No party involved in the communication can be identified.
- Preserving causality of messages
 - Older messages should not appear after more recent messages.



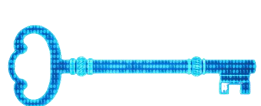
Off-The-Record Protocol

- Predecessor of most modern secure messaging protocols
 - Motivation: it is illegal to tap phone lines but not illegal to eavesdrop communication on the web.
- Sets up an encryption key using Diffie-Hellman key exchange.
- Each message is encrypted with Advanced Encryption Standard (AES) encryption.
- HMAC is used to ensure message integrity/authentication.
- Each message is encrypted with different keys and old keys are deleted immediately.
 - Achieves perfect forward secrecy
- Supports only synchronous communication.
 - No need for 3rd party servers for message buffering and key storage.



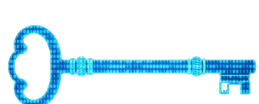
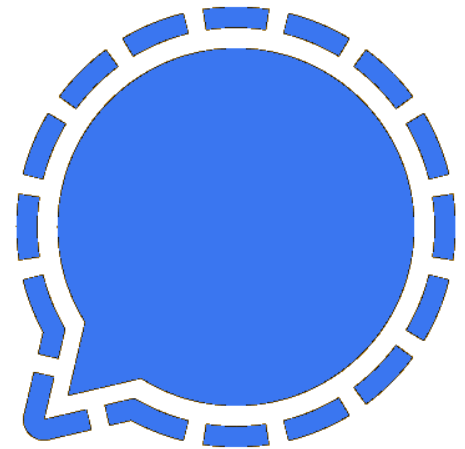
Signal

- Open source (GPLv3) available on GitHub.
 - Core protocol has been implemented into WhatsApp, FB-Messenger, etc.
- Supports asynchronous communication.
 - End-to-end encryption
 - Perfect forward secrecy
 - Future secrecy
- Keys are stored by end points (not by servers).
- For authentication, users can compare QR codes out-of-band.
 - No certificate infrastructure behind.
- Does not provide anonymity preservation and requires servers for the relaying of messages and storing of public key material.

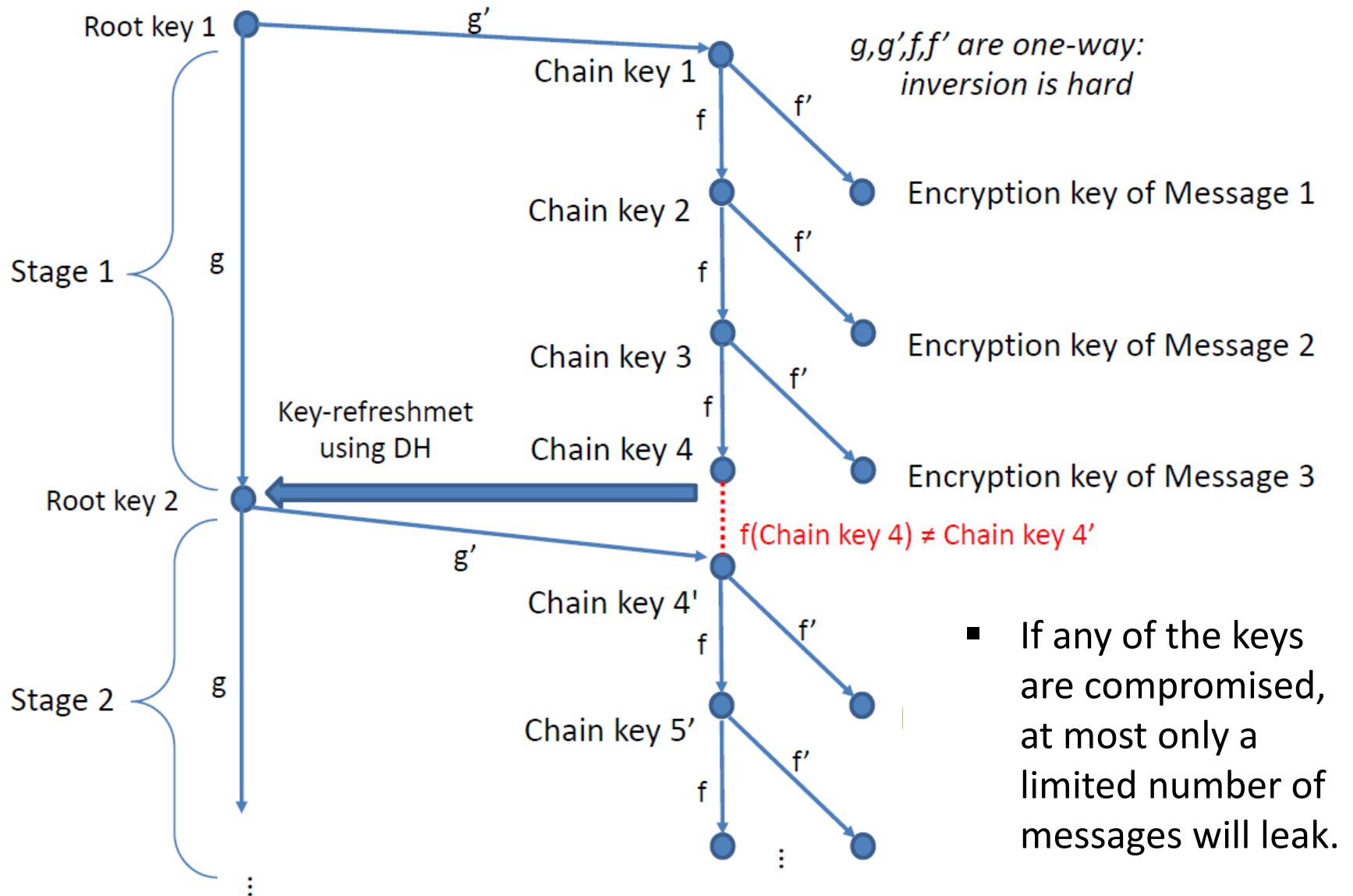


Overview

- Alice (initiator) wants to communicate with Bob (recipient).
- Initialization: Registration at server S
 - All users register at S and send their Diffie-Hellman public keys to S.
- Phase 1: Session setup
 - Alice downloads Bob's public keys from S and use them (along with her own private keys) to derive a long-lived master secret.
- Phase 2: Symmetric-ratchet communication
 - Sender key: Alice derives symmetric keys from the master secret and encrypts her messages sent to Bob.
 - Receiver key: Bob derives his own symmetric keys to send messages to Alice.
- Phase 3: Asymmetric ratchet updates
 - Alice and Bob periodically refresh their symmetric keys using Diffie-Hellman key exchange.
 - Past and future communication cannot be compromised even if session key is compromised!



Signal Protocol



Telegram Case



- Due to asynchronous communication, a server is involved.
- Russia's Federal Security Service required Telegram to share users' encrypted messages to deter "terrorism-related activities" in 2017.
 - Telegram refused to comply, so it was fined and blocked in Russia.
- France followed ...
 - ... but allowed him to leave
- Study found that mass surveillance does not appear to have contributed to the prevention of terrorist attacks.

Crypto 4 Story

ars TECHNICA

CLOSING THE BACKDOOR —

Backdoors that let cops decrypt messages violate human rights, EU court says

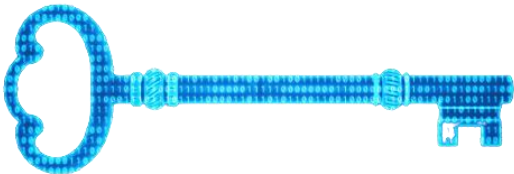
LAW AND JUSTICE | FRANCE

Telegram founder Pavel Durov arrested in France





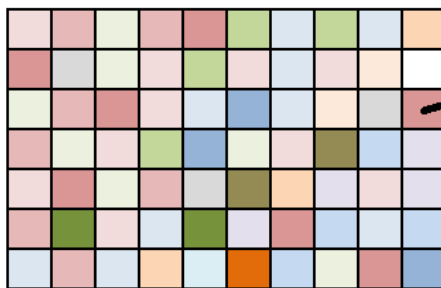
Steganography



Hide the Existence



- The existence of an encrypted message could be suspicious and raise red flags.
- Use seemingly innocent messages as cover traffic.
- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection.
 - Can be combined with encryption.
 - Protection extends to the metadata (to some extent).
- Least Significant Bit (LSB) method



RGB (218,150,149)

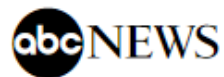
R	=	1	1	0	1	1	0	1	X
G	=	1	0	0	1	0	1	1	X
B	=	1	0	0	1	0	1	0	X

LSB



Meta Data

- With encryption the exact data is hidden, but meta-data is still leaked, such as
 - Who communicates with whom.
 - Time of the communication.
 - Duration of the communication.
 - Number of exchanged messages.
 - Etc.
- Is it a problem?
- it is cheaper to survival everybody than figuring out who to surveil.



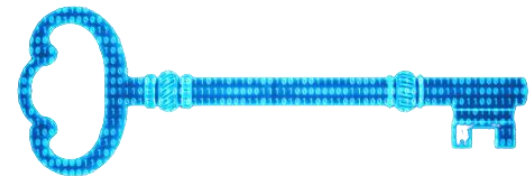
Ex-NSA Chief: 'We Kill People Based on Metadata'

By Lee Ferran May 12, 2014

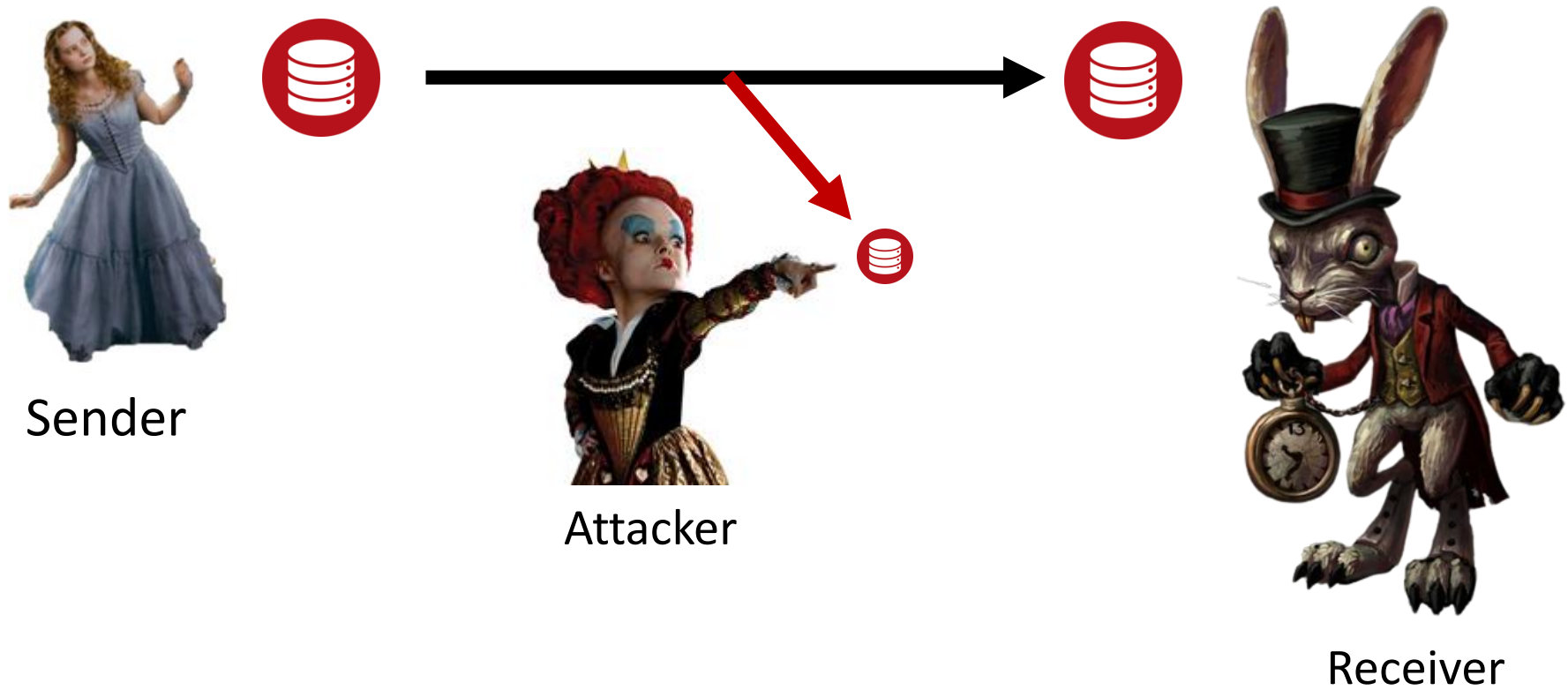




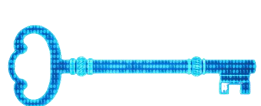
Anonymous Communication



Anonymous Communication



- Traditional crypto problem
 - Communication with a trusted entity on an unsecure channel.
- How to communicate with an untrusted entity in a secure manner?



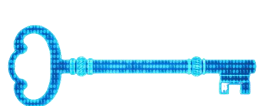
Motivation

- Privacy-protect in online communications enables / disables certain features:
 - View sensitive content
 - Avoid impersonation
 - Avoid profiling and tracking
 - » By companies: price discrimination
 - » By government: manipulation
- What is protected?
 - Sender, Receiver, Message
- Against what adversary?
 - External attackers: local and global eavesdropper.
 - Internal attackers: compromised elements of the system.
 - Communication partner.
- At what cost?
 - Latency
 - Bandwidth
 - Functionality



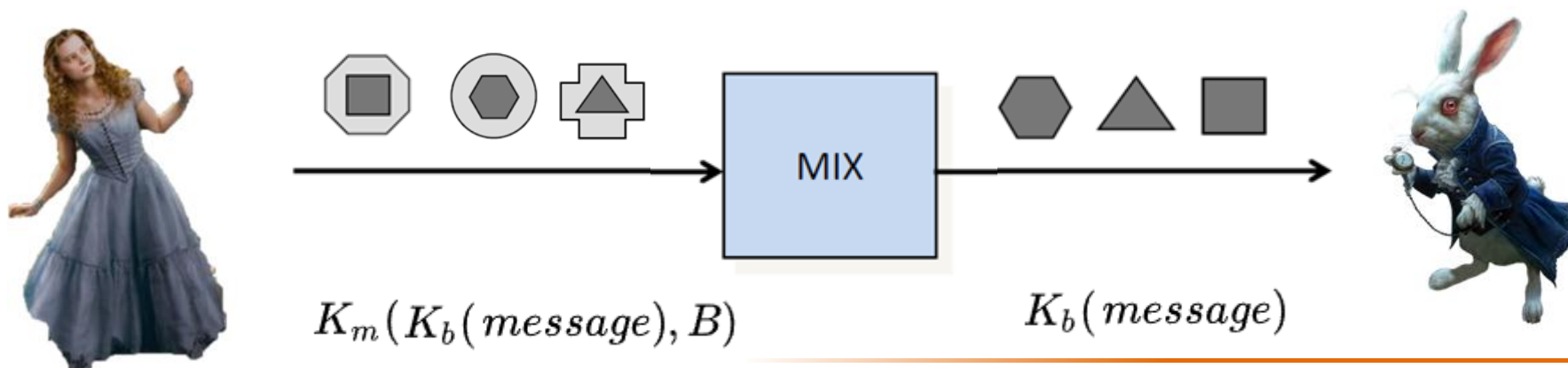
Anonymity Concepts

- Anonymity: The subject is not identifiable within a set of subjects, called the anonymity set.
- Unlinkability: Two or more items are unlinkable if the attacker cannot sufficiently distinguish whether they are related or not.
 - Sender-Receiver Unlinkability (Relationship Anonymity):
We do not learn who communicates with whom.
 - Sender-Message Unlinkability (Sender Anonymity):
We do not learn who sends which message.
 - Receiver-Message Unlinkability (Receiver anonymity):
We do not learn who receives which message.
- Undetectability: The attacker cannot sufficiently distinguish whether something exists or not.



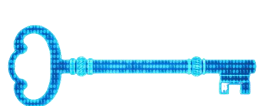
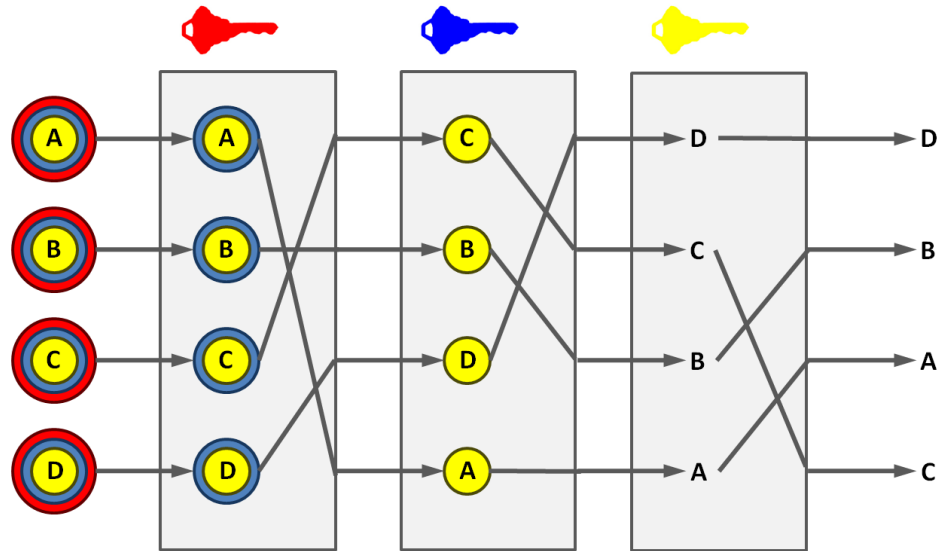
Mix

- A proxy that relays messages between communicating partners such that it
 - Changes encoding of messages.
 - Batches incoming messages and changes order when outputting them.
- Properties:
 - Sender anonymity w.r.t. communication partner.
 - Unlinkability w.r.t. global eavesdroppers.
- The Mix still needs to be trusted.



Mix Net

- Each Mix has an asymmetric key pair.
- Sender of a message selects a path through the Mix Net and encodes the message iteratively for each Mix on the path.
- Each Mix decodes the message with its private key and forwards it to the next Mix indicated in the decoded message.
- Slow due to public key operations.



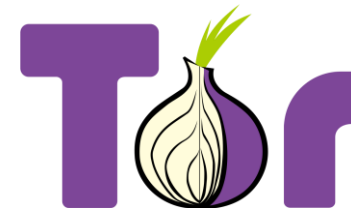
Sending & Receiving

- The sender selects a path $M_n \rightarrow M_{(n-1)} \rightarrow \dots \rightarrow M_1$ through the MIX network and encodes the message iteratively.
- Sender $\rightarrow E_R(m, r_0) \rightarrow$ Receiver
- Sender $\rightarrow E_{M_1}(E_R(m, k, r_0), r_1 \mid R) \rightarrow M_1$
 - $M_1 \rightarrow E_R(m, k, r_0) \rightarrow$ Receiver
- Sender $\rightarrow E_{M_2}(E_{M_1}(E_R(m, k, r_0), r_1 \mid R), r_2 \mid M_1) \rightarrow M_2$
 - $M_2 \rightarrow E_{M_1}(E_R(m, k, r_0), r_1 \mid R) \rightarrow M_1$
 - $M_1 \rightarrow E_R(m, k, r_0) \rightarrow$ Receiver
- Sender $\rightarrow E_{M_n}(E_{M_{(n-1)}}(\dots \dots \dots), r_{n-1} \mid M_{(n-2)}), r_n \mid M_{(n-1)}) \rightarrow M_n$
- r : random, so the same plaintext have different cyphertext.
- k : symmetric key used to encrypt the reply by the destination to the source (as the source cannot share its public key).



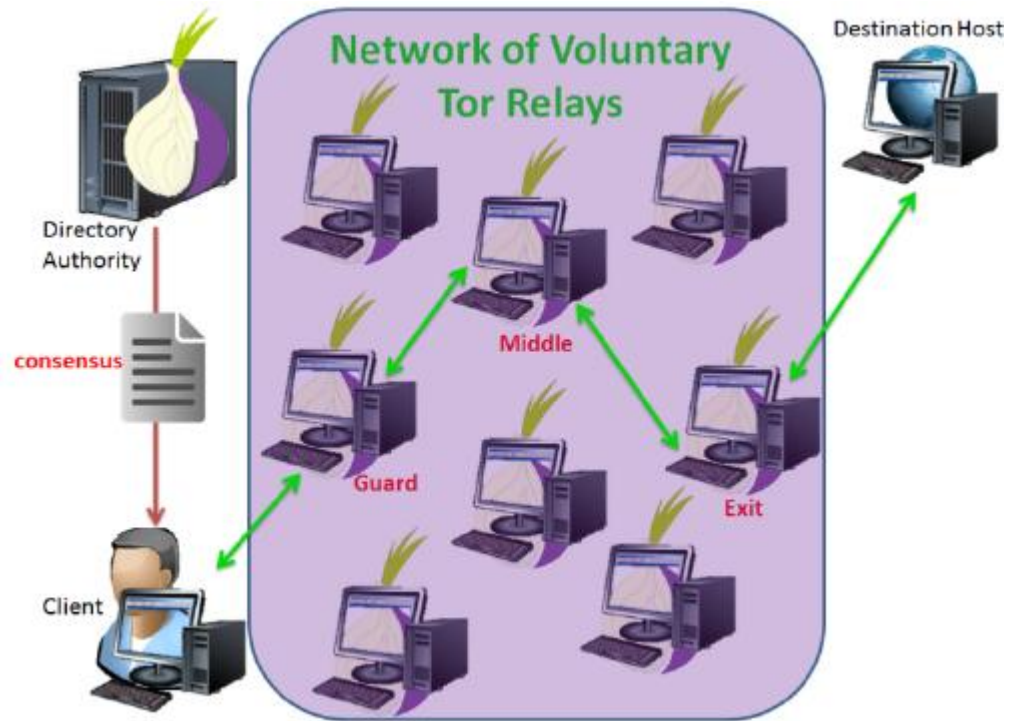
The Onion Router

- Tor is a real-time mix-based anonymous communication service which makes compromise between anonymity and speed.
- Applies minimal traffic shaping and symmetric key encryption to ensure low-latency: no mixing, just packet forwarding.
 - Relay cells consist exactly 512 bytes to prevent traffic analysis.
- Assumes local adversary which can only observe some subset of the connections and can control only a subset of Tor nodes.
- Goals are to make it difficult (but not impossible)
 - for the destination to reveal the IP address of the source.
 - to link multiple communications to or from the source.
 - for any local adversary to reveal the IP address of the destination.
 - to link the source IP address and the destination IP address.



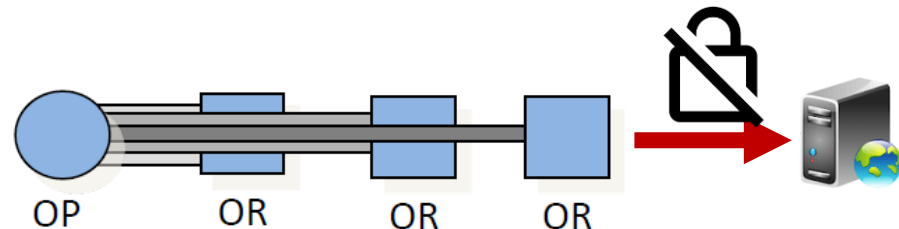
The Tor Network

- It is an overlay network consisting of onion routers (OR).
 - ORs are operated by volunteers on the Internet.
 - A few special directory servers keep track of the ORs in the network.
 - Each OR has a descriptor (keys, address, bandwidth, exit policy, etc.)
 - Each OR maintains a TLS connection to all other ORs.
- The onion proxy (OP) obtains the keys of ORs from a directory.
- OP establishes virtual circuits across the Tor network.
 - OPs rotate to a new circuit once a minute.



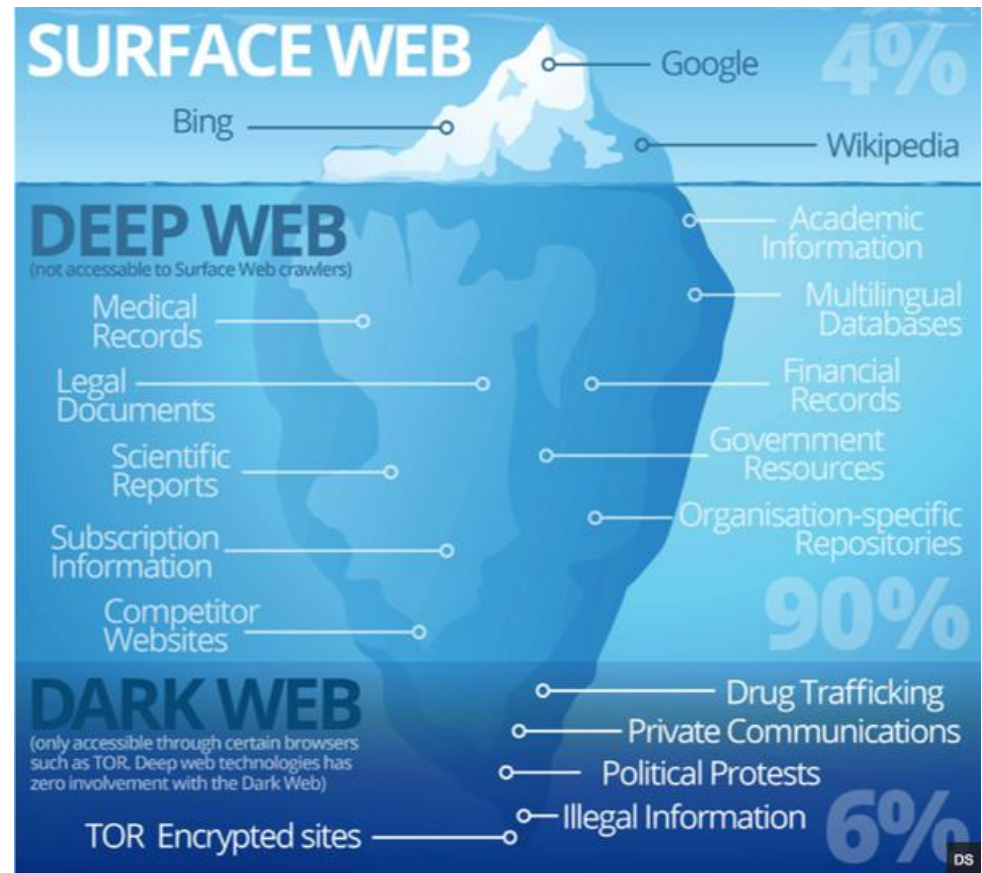
Communicating on Tor

- The OP encrypts the cell iteratively with all the symmetric keys that are shared with the ORs on the path.
- Each OR peels off one layer of encryption, the last OR sends cleartext data to the destination.
 - Hackers can launch their attacks via the Tor network where exit nodes would take the blame, leading to less participants and lower level of anonymity.
- Exit policies:
 - Open exit: connects anywhere.
 - Middleman: only relay traffic to other Tor nodes.
 - Private exit: connect only to the local host or network.
 - Restricted exit: prevent access to certain addresses and services.
- On the way back, each OR encrypts the cell (adds one layer) and the OP removes all encryptions.



Dark Web

- Tor allows someone to offer a TCP-based service anonymously (without revealing his IP address to the world).
- Illegal contents
 - C&C servers for botnets
 - Darknet markets (to sell drugs, guns, software exploits, etc.)
 - Sell hacking services
 - Sell fraud services
 - Illegal pornography
- Search engines
 - Torch
 - DuckDuckGo
 - The Hidden Wiki



Silk Road

- The first online black market.
 - Customers could pay in bitcoins.
 - Alleged creator was sentenced to life in prison.
 - Trump pardoned him recently ...
- Tor does not provide 100% privacy guarantee.
 - As a consequence of the efficiency privacy trade-off, attacks are possible: Congestion attack, Application layer attack, etc.
- Is buying drugs in a dark alley better?



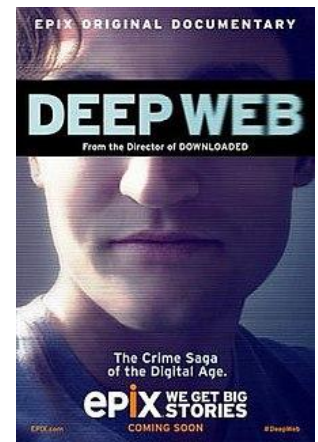
Crypto 5
Story

TECHNOLOGY

Did Shutting Down Silk Road Make the World a More Dangerous Place?

So long as narcotics are illegal, they will be sold on the black market. Better that it happens on the Web than on the street.

By Conor Friedersdorf



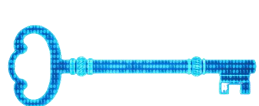
Disclaimer

- Be careful about the websites you visit in the dark web.
 - Webcam can be hijacked by websites.
 - You could infect your device with malware.
 - You can be prosecuted for things you do.
- Law enforcement officials operate on the dark web to catch people engaged in criminal activity.
 - They operate decay hidden services.



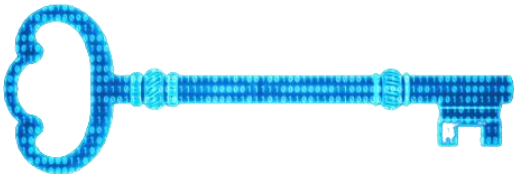
NYM (vs TOR)

- Privately communicating with the blockchain.
- *The way the internet operates today the consequences of surveillance threaten all of us: from stolen funds and identities to profiling and human rights violations.*
- *Nym provides a network level protection, i.e., it protects even against the most powerful, passive adversaries that can observe every packet going in and out of your internet connection.*
- <https://nymtech.net/>



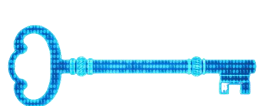
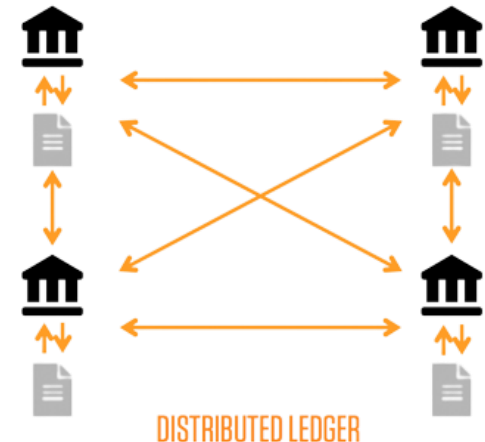
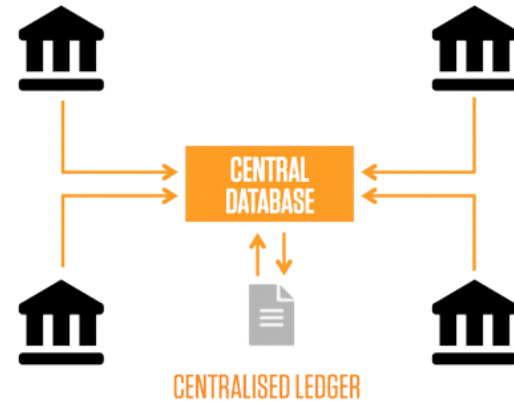


Cryptocurrencies



Traditional & Blockchain Database

- Traditional databases use client-server network architecture.
 - The data is controlled by the server.
 - A client can modify data after the server authenticates a client's credentials before providing access.
- If the security of the server is compromised, the data can be tampered with (single point of failure).
- Blockchain databases consist of several decentralized nodes.
 - Each node participates in administration: all nodes verify new additions to the blockchain.
 - Each node can enter new data to the blockchain, if the majority of nodes reach consensus.
 - This consensus mechanism guarantees the security of the network, making it difficult to tamper with.





Blockchain Workflow (e.g., Bitcoin)

- Transaction is requested (i.e., broadcasted to the network).
- Validity is authenticated (using previous block of the blockchain) by miners.
- Miners create a block with the transaction in it and broadcast to other nodes.
- The block is validated by the nodes and the miner gets a reward.
- The new block is appended to the chain and the transaction is accepted.

From

1 [bc1qnwcy2q4t2jkw35uuggtpa9qjpgsqn35jxa...](#)  
17.27661141 BTC • \$408,995

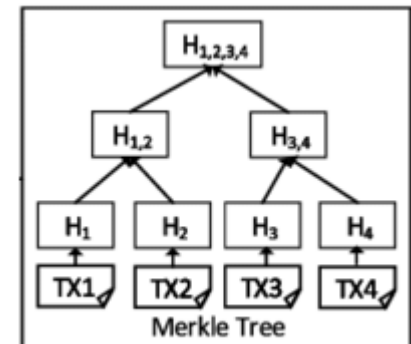
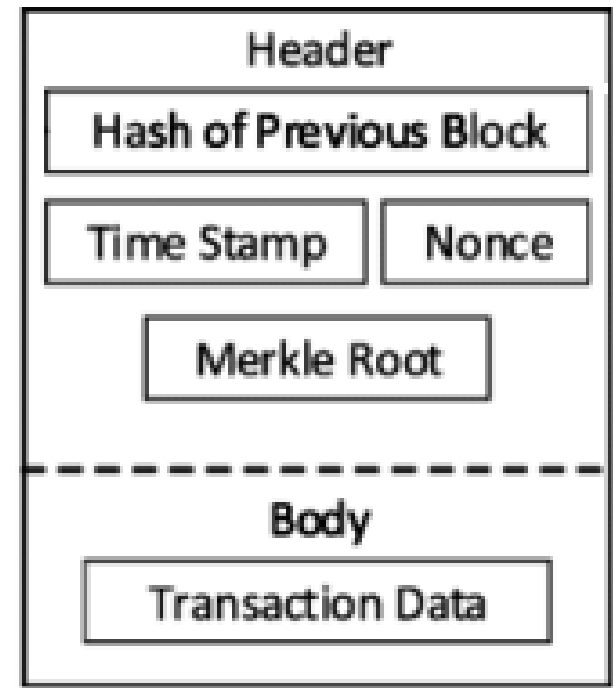
To

1 [bc1qw7ejjnxgqfnjt8nzn27hpe9zz3kykdv0799m...](#)  
17.27628141 BTC • \$408,987



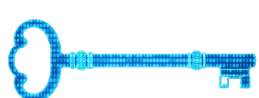
Security & Proof-of-Work (Bitcoin)

- (Cryptographic) hash of previous block: to tamper with a single block, all block after must be tampered with.
- Merkle root: A commitment of all the transactions.
- Nonce: random bits.
- Proof-of-work: find a nonce such that the hash of the block head ends with X zeroes.
 - X is the difficulty, adjusted algorithmically such that the expected time to find a valid block is 10 minutes.
- Reward: miners include a reward transaction in the block.



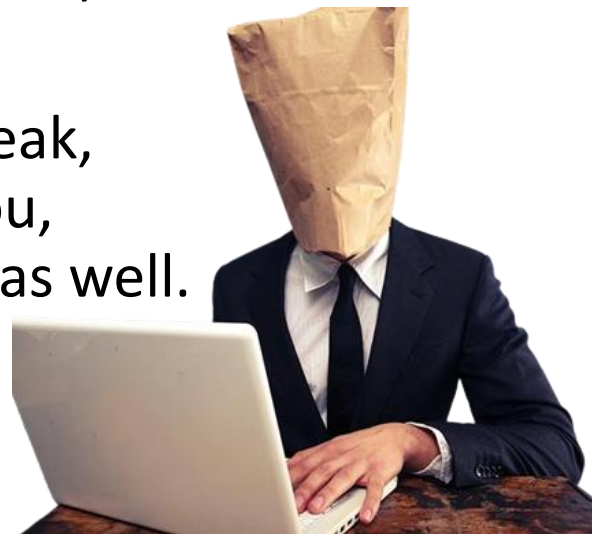
Properties of Blockchain Databases

- Publicly verifiability
 - Integrity: every user can be sure that the data they are retrieving is uncorrupted and unaltered since the moment it was recorded.
 - Transparency: every user can verify how the blockchain has been appended over time.
- How about Privacy?
 - Bitcoin payments are publicly visible → Transaction data can be used to link addresses to a single owner and to a physical entity via chainalysis.
 - Traditional payments are more private as those are only visible to limited audience (e.g., banks, fraud detection agencies, etc.).



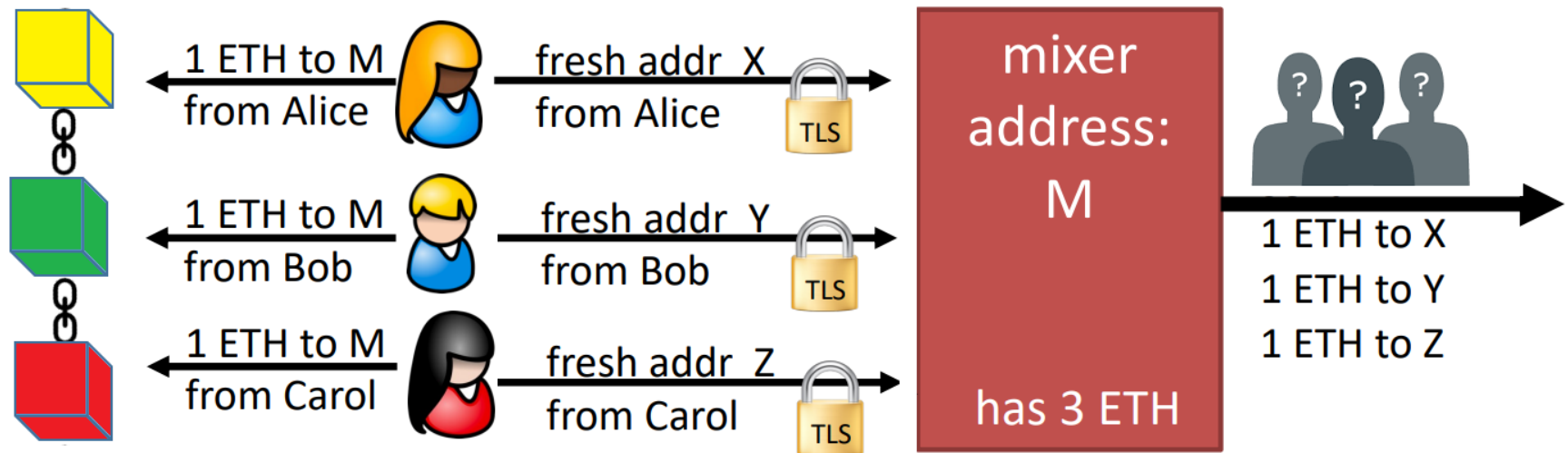
Financial Privacy

- Supply chain privacy
 - E.g., a car company does not want to reveal how much it pays its supplier for tires, etc.
- Payment privacy
 - E.g., a company wants to keep list of employees and their salaries private.
 - E.g., an individual wants to donate anonymously.
- Pseudonymity (e.g., a BTC address) is weak, as once a transaction is connected to you, all previous transactions are connected as well.
- In full anonymity, the system cannot tell if two transactions are from the same person.
 - Anonymity set: the number of indistinguishable participants.



Mixers

- Observer knows Y belongs to one of {Alice, Bob, Carol}, but does not know which one.
 - The size of the anonymity set is 3.
- Problems
 - Mixer knows shuffle.
 - Mixer can abscond with 3 ETH.
- Can we do it without a trusted party?



Private Coins

- Using ZKP-based mixers on non-private blockchains
 - For Bitcoin: CoinJoin
 - For Ethereum: TornadoCash
- Using private blockchain
 - Zcash (using ZKP, anonymity set: all users)
 - Monero (using ring signatures; anonymity set: ring size)
 - Etc.
- How to support positive applications of private payments, but prevent the negative ones?
- Can we ensure legal compliance while preserving privacy?

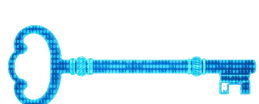


TornadoCash Lawsuit

- A ~~money-laundering service~~ privacy enhancing technology, run as a smart contract on Ethereum.
 - Deposit coins from an address.
 - Using ZKP you prove you have deposited funds, so you can withdraw coin without revealing the original address.
- In the US citizens are not allowed to be affiliated in any financial way with people on the OFAC Sanctions List.
 - E.g., with known terrorists, etc.
- US lawmakers included ETH addresses used TornadoCash, making it illegal to use for US citizens.
 - Controversy: how to outlaw open-source code (i.e., the smart contract)?

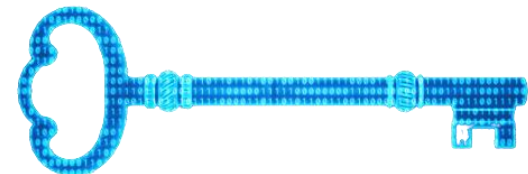


Crypto 6
Story





E-Voting



The Basis of Democracy: Elections

- We have witnessed several spectacular failures of democracy recently.
- Essential that the losers be convinced they lost, and that the correctness of the outcome can be demonstrated to all.



WIKIPEDIA
The Free Encyclopedia



Search Wikipedia

Russian interference in the 2016 United States elections



Trump refuses to accept election results, says it's 'far from over'

PUBLISHED SAT, NOV 7 2020•11:51 AM EST | UPDATED SAT, NOV 7 2020•1:05 PM EST



January 6 U.S. Capitol attack riot, Washington, D.C., U.S. [2021]



Print



Cite



Share



Feedback

Alternate titles: *January 6th storming of the United States Capitol, United States Capitol attack of 2021*

Written by [Brian Duignan](#)

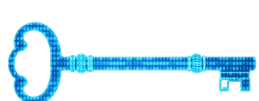
Fact-checked by [The Editors of Encyclopaedia Britannica](#)

Last Updated: Feb 15, 2023 • [Article History](#)



Elections

- The outcome of an election should not only be correct but also universally demonstrable, while ensuring ballots remain private.
- We need to resolve the tension between transparency/accountability and ballot secrecy.
 - As far as possible, without trusted parties.
- In person vs Remote
 - All the insecurities of the internet and client devices.
 - Radically different contexts and threat models.



Internet-based Voting in the Real Word

- Estonia
 - First country to employ internet-based voting in nation-wide political election.

2005

- Switzerland
 - Used since 2016 for Canton-wide elections.

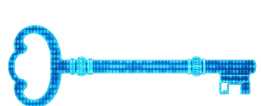
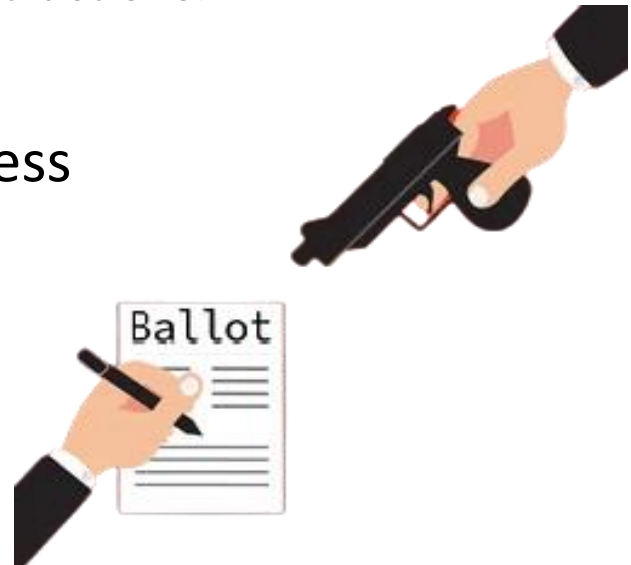


- Human Rights Standards on Elections of the United Nations (UN)
 - Require the elections to be independently verifiable.
 - Require voters' ballot to be secret.
 - Require voters to be protected from coercion or compulsory disclosure of their choice.



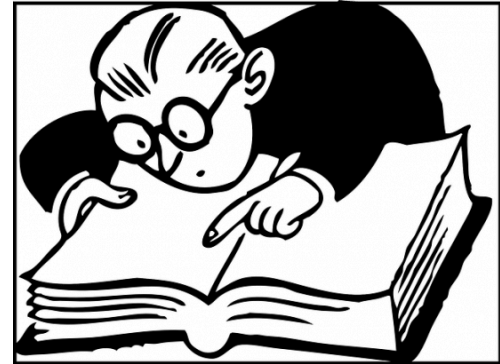
Privacy Requirements

- Ballot secrecy
 - The casted vote should be known only to the voter.
- Receipt-freeness
 - There must be no way for a voter to construct a proof of how she voted.
- Coercion resistance
 - A voter can always vote according to her intent while appearing to comply with a coercer's instructions.
- Coercion resistance \rightarrow Receipt-freeness
- Receipt-freeness \rightarrow Ballot secrecy
- Usability/Understandability



Integrity Requirements

- The count accurately reflects the (legitimately) casted votes.
- Ensured through verifiability
 - Individual Verifiability
Every voter can confirm that her vote is accurately recorded.
 - Universal Verifiability
Anyone can verify that the recorded ballots are accurately tabulated.
 - Eligibility Verifiability
Anyone can verify than only valid votes are cast, and no voter casts more than one vote.
- Someone who cannot trust the system will not use it.
 - If the system works, why should we verify?
 - The counter intuitive aspects of the cryptography in e-voting.

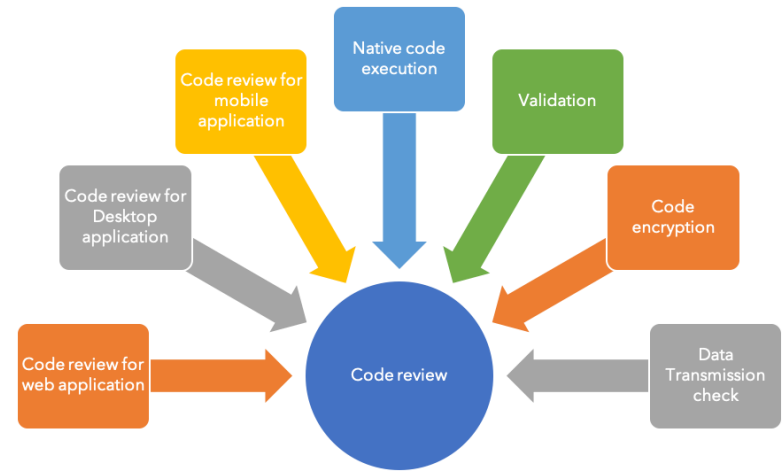


TRUST NO ONE



Verify the Election not the System

- In principle you could verify the code in voting machines, in the tabulation algorithms, etc.
 - In practice such proofs are horrendously expensive, time-consuming and error-prone.



- Design the system such that it generates enough evidence during the election to enable verification of the result (without violating privacy).
- There have been moves to digitize democracy.
 - Can make life easier for voters and election officials, but also much easier for hackers.



E2E Verifiability

- Enables voters and observers to confirm that votes are accurately counted.
- At the time of casting, voters get an encrypted representation of their vote (protected receipt).
- Encrypted votes are posted to a secure web bulletin board (e.g., on a blockchain).
 - Voters can verify that their receipts are correctly posted.
- A (universally) verifiable, anonymizing tabulation is performed on the posted receipts.
 - E.g., by using Homomorphic Encryption or Secure Multi Party Computation.

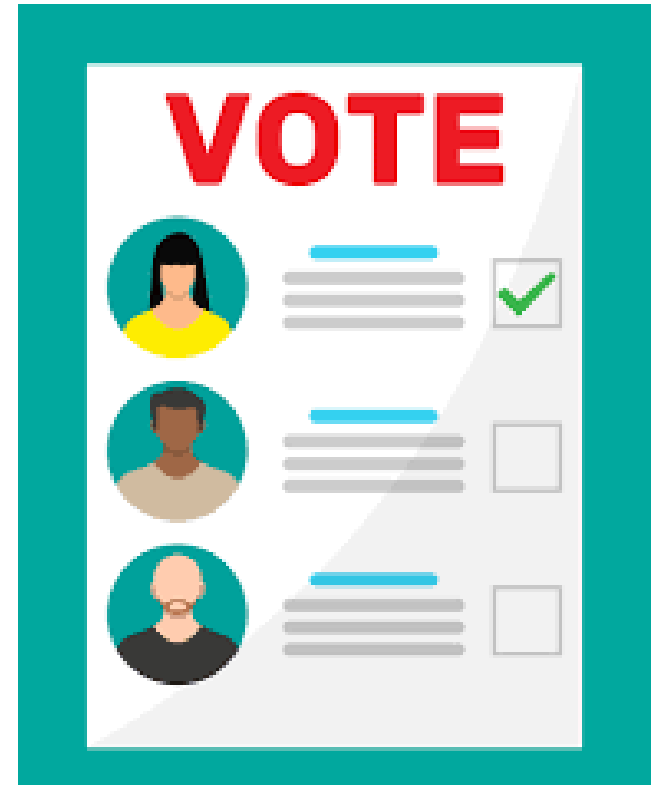


- But people are uncomfortable with having to handle encryptions.
- Voter verification steps can be burdensome and non-intuitive.



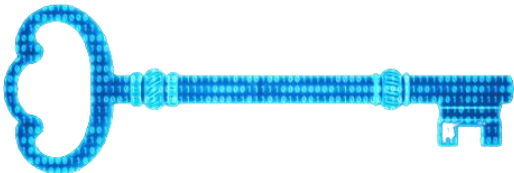
The assurance argument

- A framework that encompasses various aspects of system assurance, including E2E verifiability.
 - Cast as intended: Each voter should be confident that his/her vote is correctly encrypted.
 - Recorded as casted: All legitimately cast (encrypted) votes, and only those are input to the tally.
 - Tallied as recorded: The set of encrypted votes is correctly anonymized and decrypted.
- The tricky bit is the first: how to convince the voter that the correct vote is inside the encryption without creating a transferable proof.



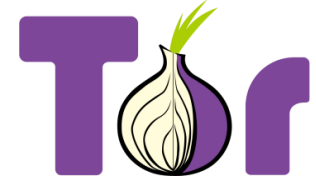


Other PETs



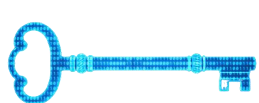
PETs

- Anonymous Communications
- Secure Messaging
- Anti-tracking tools
- Encrypted Cloud Storage
- Virtual Private Network
- Password Managers
- De-centralized Social Networks
- Trusted Execution Environment
 - <https://www.privacytools.io/>
 - enisa.europa.eu/publications/privacy-tools-for-the-general-public



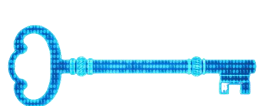
Trusted Execution Environment

- Code and data loaded in the processor are accessible via third party applications, so any information flowing through the processor is not protected from malicious third-party applications.
- TEE is an area on the main processor of a device that is separated from the system's main operating system.
- It ensures data is stored, processed and protected in a secure environment.
 - Secure peripheral access
 - Secure communication with remote entities
 - Trusted device identity and authentication



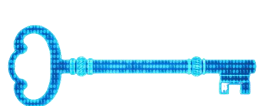
Take Away

- Secure messaging is challenging, and a third party is needed for asynchronous communications.
 - E2E encryption is a right step towards privacy, but far from a stand-alone solution.
- ‘Bitcoin is private’ is a common misconception, as pseudonymity only provides weak guarantees.
- Metadata is a rich source of information but Mix Nets could provide anonymity.
 - Due to efficiency reasons Tor compromises this for usability.
- E-voting means not only ‘voting over the internet’.
 - Cryptography offers solutions (HE, Commitments, ZKP), the challenge is to make it user friendly.



Control Questions

- What are the privacy and integrity requirements for E-voting?
- What is TOR, how does it work, and what protection does it guarantee?
- Give a high-level description of the Signal protocol!
What properties does it guarantee, and how?



References

- [Anonymous Communication](#)
 - [Signal](#)
 - [Mix](#)
 - [TOR](#)
- [Dark Web](#)
- [Steganography](#)
- [Blockchain](#)
 - [Cryptocurrency](#)
- [E-Voting](#)
- [TEE](#)

