

The DIVORCE: Flipping a coin over the Internet



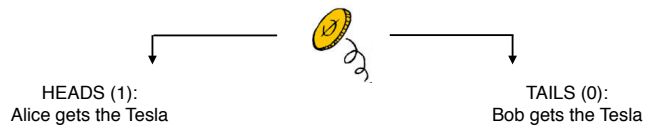
Thinks he's unsupportive. (Sponges are like that.)

Thinks she's unstable. (She keeps changing size.)



Divorce!

But who gets custody of the Tesla Model S?



1

Mihir Bellare, UCSD

It's a question of TRUST



Alice is in Wonderland



Bob is underwater



Internet cable

I don't think so.

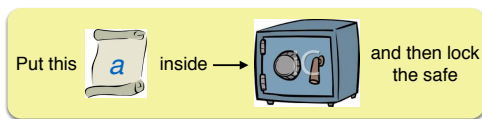
I'll flip a coin and send you the outcome.

Alice has the security mindset!

2

Mihir Bellare, UCSD

Alice gets herself some hardware ...

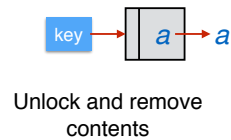
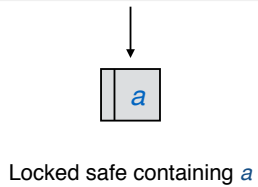


Combination safe



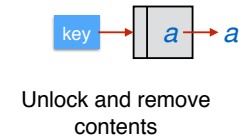
Alice knows the secret combination / key **92093**.

key

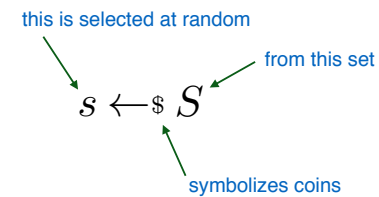


3

Mihir Bellare, UCSD



Alice also gets herself some notation ...



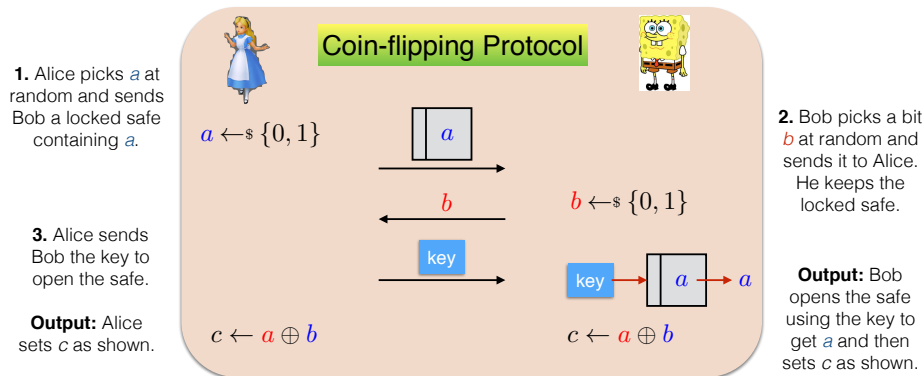
Example

$$a \leftarrow \$ \{0, 1\}$$

$$\Pr[a = 0] = \Pr[a = 1] = \frac{1}{2}$$

4

Mihir Bellare, UCSD



The bit c is the common coin.

Claim: This works, meaning neither party controls the common coin.

Scenario A: Bad Alice, Good Bob

Alice is an adversary trying to make Bob output $c=1$. Bob follows the protocol.

Claim A: Adversary Alice will fail.

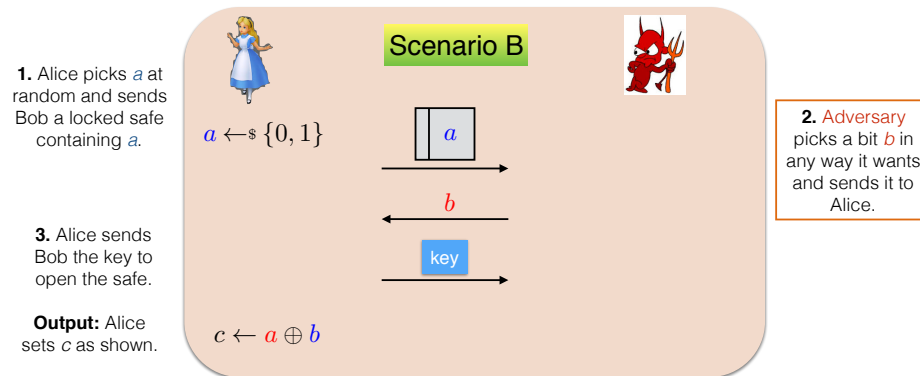
Scenario B: Bad Bob, Good Alice

Bob is an adversary trying to make Alice output $c=0$. Alice follows the protocol.

Claim B: Adversary Bob will fail.

5

Mihir Bellare, UCSD



Adversary wants to make $c = 0$.
 So it must set $b = a$.

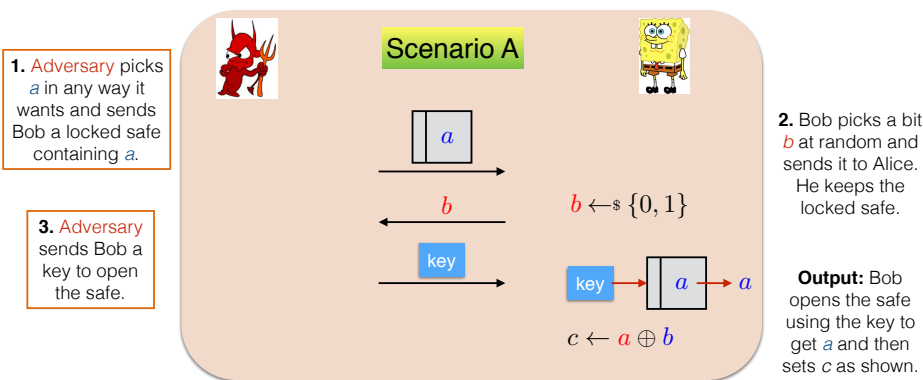
But it can't set $b = a$ because

The safe is **HIDING**: Given a , the adversary has no idea what is a .

It does learn a after getting the key, but this is too late to set $b = a$!

6

Mihir Bellare, UCSD



Adversary wants to make $c = 1$.
 So it must set $a = b \oplus 1$

But it can't set $a = b \oplus 1$ because it doesn't know b at the time it picks a .

But this is not enough to establish **Claim A** because Adversary could pick the safe in a devious way ...

7

Mihir Bellare, UCSD

Sneaky safes? Suppose Adversary Alice could fabricate

a sneaky safe and two different keys key_1 key_0

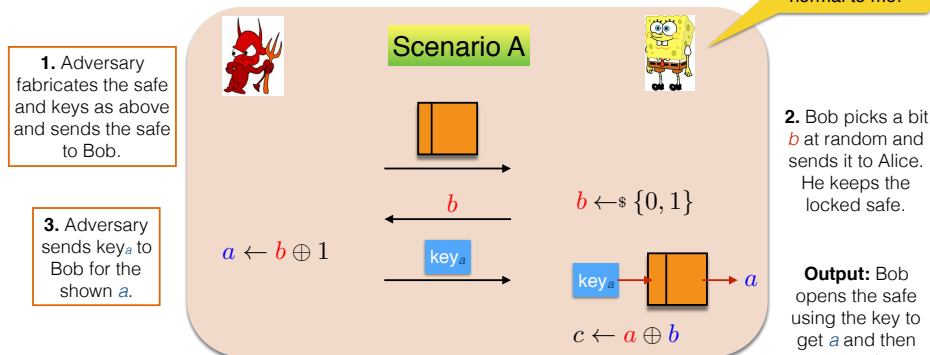
such that

$key_1 \rightarrow 1$ and $key_0 \rightarrow 0$



Alice's lab

The safe looks normal to me!



This results in $c = 1$, so Adversary wins.

8

Mihir Bellare, UCSD

Sneaky safes?

Suppose **Adversary** Alice could fabricate

a sneaky safe  and **two different** keys  

such that

  $\rightarrow 1$ and   $\rightarrow 0$

 Any safe *commits* its creator to one value for its content

Not possible!

Safes are **BINDING**

9

Mihir Bellare, UCSD

Security of the coin-flipping-with-safes protocol relies on the following two facts / assumptions

Safes are **HIDING**: Given  the adversary has no idea what is *a*.

This is the property we know and understand safes as having.

Safes are **BINDING**: One cannot create

such that

  $\rightarrow 1$ and   $\rightarrow 0$

This is a property safes seem to have but we don't usually recognize or enunciate.

It is important to formulate and state the assumptions underlying any claim of security.

10

Mihir Bellare, UCSD

Coin flipping without hardware: From safes to bits

Sending a **safe** from Wonderland to Undersea over the Internet is hard.

Can we get a protocol that we can implement fully in software and that only transmits bits?

YES: Via commitment schemes, which we will later formalize and construct.

11

Mihir Bellare, UCSD

If Bob can drive a Tesla underwater, why do we bother about a little thing like sending safes over the Internet?



Can you think of other problems one can solve with similar methods?
Can you implement a secure Internet Casino?

12

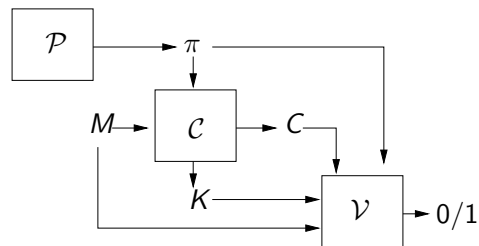
Mihir Bellare, UCSD

APPLICATIONS AND PROTOCOLS

- Internet Casino
 - Commitment
 - Shared coin flips
 - Threshold cryptography
 - Forward security
 - Program obfuscation
 - Zero-knowledge
 - Certified e-mail
 - Electronic voting
 - Auctions
- Identity-based encryption
 - Functional encryption
 - Fully-homomorphic encryption
 - Searchable encryption
 - Oblivious transfer
 - Garbling schemes
 - Secure computation
 - Group signatures
 - Aggregate signatures

Commitment Schemes

A commitment scheme $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ is a triple of algorithms



Parameter generation algorithm $\mathcal{P}$ is run once by a trusted party to produce public parameters π .

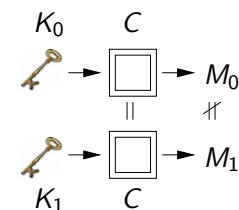
In Divorce protocol, message M is Alice's bit a , committal C is the safe, K is the key to the safe.

Security properties

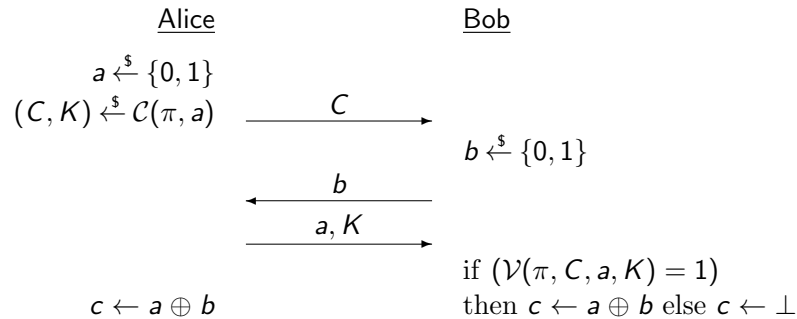
- Hiding: A committal C generated via $(C, K) \leftarrow \mathcal{C}(\pi, M)$ should not reveal information about M .

$$\boxed{\boxed{M}} = C \text{ does not reveal } M.$$

- Binding: It should be hard to find C, M_0, M_1, K_0, K_1 such that $M_0 \neq M_1$ but $\mathcal{V}(\pi, C, M_0, K_0) = \mathcal{V}(\pi, C, M_1, K_1) = 1$.



Divorce Protocol using a commitment scheme



Commitment from hashing

Let H be a hash function and $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ the commitment scheme where $\mathcal{P}$ returns $\pi = \varepsilon$ and

Alg $\mathcal{C}(\pi, M)$ $C \leftarrow H(M); K \leftarrow M$ return (C, K)	Alg $\mathcal{V}(\pi, C, M, K)$ return $(C = H(M) \text{ and } M = K)$
--	--

This is

Commitment from hashing

Let H be a hash function and $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ the commitment scheme where $\mathcal{P}$ returns $\pi = \varepsilon$ and

Alg $\mathcal{C}(\pi, M)$ $C \leftarrow H(M); K \leftarrow M$ return (C, K)	Alg $\mathcal{V}(\pi, C, M, K)$ return $(C = H(M) \text{ and } M = K)$
--	--

This is

- Binding if H is collision-resistant.

Commitment from hashing

Let H be a hash function and $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ the commitment scheme where $\mathcal{P}$ returns $\pi = \varepsilon$ and

Alg $\mathcal{C}(\pi, M)$ $C \leftarrow H(M); K \leftarrow M$ return (C, K)	Alg $\mathcal{V}(\pi, C, M, K)$ return $(C = H(M) \text{ and } M = K)$
--	--

This is

- Binding if H is collision-resistant.
- But not hiding. For example in the Divorce protocol, $M = a \in \{0, 1\}$, so given $C = H(M)$ the casino can recover M via
 - For $i = 0, 1$ do
 - if $H(i) = C$ then return i

Commitment from hashing

Let H be a hash function and $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ the commitment scheme where $\mathcal{P}$ returns $\pi = \varepsilon$ and

Alg $\mathcal{C}(\pi, M)$ $K \xleftarrow{\$} \{0, 1\}^{128}$ $C \leftarrow H(K M)$ return (C, K)	Alg $\mathcal{V}(\pi, C, M, K)$ return $(C = H(K M))$
---	--

This is

- Binding if H is collision-resistant (CR).
- One can give an example of CR H such that it is not hiding.
- But for “real” H such as SHA1 it seems hiding in the sense that no attacks are known.

Commitment schemes usage

Commitment schemes are very broadly and widely used across all kinds of protocol design and in particular to construct zero-knowledge proofs.

Secure summation

Suppose we have n parties $1, \dots, n$

Party i has an integer x_i

The parties want to know the value of

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n$$

Secure summation

Suppose we have n parties $1, \dots, n$

Party i has an integer x_i

The parties want to know the value of

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n$$

Easy: Let

- Party i send x_i to party 1 ($2 \leq i \leq n$)
- Party 1 computes $f(x_1, \dots, x_n) = x_1 + \dots + x_n$ and broadcasts it

Secure summation

Suppose we have n parties $1, \dots, n$

Party i has an integer x_i

The parties want to know the value of

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n$$

Easy: Let

- Party i send x_i to party 1 ($2 \leq i \leq n$)
- Party 1 computes $f(x_1, \dots, x_n) = x_1 + \dots + x_n$ and broadcasts it

What they don't like about this: Party 1 now knows everyone's values

Privacy constraint: Party i does not wish to reveal x_i

Secure summation

Party i has input x_i ($1 \leq i \leq n$). The parties want to know

$f(x_1, \dots, x_n) = x_1 + \dots + x_n$ but do not want to reveal their inputs in the process.

Scenarios:

- x_i = score of student i on midterm exam
- x_i = salary of employee i
- $x_i \in \{0, 1\}$ = vote of voter i on proposition X on ballot

The model and goal

Parties i, j are connected via a secure channel ($1 \leq i, j \leq n$).

Privacy and authenticity of messages sent over channel are guaranteed.

The parties will exchange messages to arrive at $f(x_1, \dots, x_n)$.

If $i \neq j$ then, at the end of the protocol, party i should not know x_j .

For example you, as player i , enter x_i into some app on your cellphone which then communicates with the cellphones of the other parties. At the end, the sum shows up on your screen. Take your phone apart and examine all memory contents and you still will not discover x_j for $j \neq i$.

Setup for secure communication protocol

Let N be such that $x_1, \dots, x_n \in Z_N = \{0, \dots, N-1\}$.

Let $M = nN$.

Let S denote $x_1 + \dots + x_n$.

We will compute $S \bmod M$, which is just S since

$$x_1 + \dots + x_n \leq n(N-1) < M$$

Protocol step 1: secret sharing

For $i = 1, \dots, n$ party i

- Picks $x_{i,1}, \dots, x_{i,n} \in Z_M$ at random subject to $x_{i,1} + \dots + x_{i,n} \equiv x_i \pmod{M}$
- Sends $x_{i,j}$ to party j over secure channel ($1 \leq j \leq n$)

$$\begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\ x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \end{bmatrix} \begin{matrix} \rightarrow x_1 \\ \rightarrow x_2 \\ \rightarrow x_3 \\ \rightarrow x_4 \end{matrix}$$

Observation: $x_{i,j}$ is a random number unrelated to x_i so party j has no information about x_i ($i \neq j$)

Protocol step 2,3: Column sums and conclusion

$$\begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\ x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \end{bmatrix} \begin{matrix} \rightarrow x_1 \\ \rightarrow x_2 \\ \rightarrow x_3 \\ \rightarrow x_4 \end{matrix}$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow \\ C_1 & C_2 & C_3 & C_4 \end{matrix}$$

For $j = 1, \dots, n$ party j

- Computes $C_j = (x_{1,j} + x_{2,j} + \dots + x_{n,j}) \pmod{M}$
- Sends C_j to party i ($1 \leq i \leq n$)

Observation: $S \equiv (C_1 + \dots + C_n) \pmod{M}$.

So each party can compute $S \leftarrow (C_1 + \dots + C_n) \pmod{M}$

Security of the protocol

$$\begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\ x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \end{bmatrix} \begin{matrix} \rightarrow x_1 \\ \rightarrow x_2 \\ \rightarrow x_3 \\ \rightarrow x_4 \end{matrix}$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow \\ C_1 & C_2 & C_3 & C_4 \end{matrix}$$

At end of protocol, party 1 knows (1) x_1 , and the first-row entries of the matrix (2) the sum $S = x_1 + x_2 + x_3 + x_4$ (3) C_1, C_2, C_3, C_4 (4) the first column entries $x_{1,1}, x_{2,1}, x_{3,1}, x_{4,1}$.

Claims:

- Party 1 learn nothing about x_4
- Even if parties 1,2 pool their information, they learn nothing about x_4
- ...

Secure Computation

Parties $1, \dots, n$

Party i has private input x_i

They want to compute $f(x_1, \dots, x_n)$

Fact: For any function f , there is a $n/2$ - private protocol to compute it.

A protocol is t -private if any t parties, getting together, cannot figure out anything about the input of the other parties other than implied by the value of $f(x_1, \dots, x_n)$.

The protocol views f as a circuit (program) and computes it gate (instruction) by gate (instruction).

Enormous body of research.

Secure computation usage: Callisto



WHAT WE DOWHO WE ARECAREERSDONATE

By survivors, for survivors

Callisto is a non-profit that creates technology to detect repeat perpetrators of professional sexual coercion and sexual assault.

Join our team



TEDThe Washington PostTHE WALL STREET JOURNALForbesThe New York Times

The Problem

Sexual assault and professional sexual coercion are far too common and often never reported. The process of reporting can feel isolating—or worse, retraumatizing. Reporting also comes with its own set of personal and professional risks.

Callisto changes the equation. Our technology empowers survivors, providing options and allowing disclosure in a way that feels safe. Our unique matching system securely connects victims of the same perpetrator to identify repeat offenders.

Mihir Bellare

UCSD

21

Secure computation usage: Callisto

Our Solutions

Callisto Campus provides survivors with trauma-informed options for reporting sexual assault and is now in place across 13 partner institutions. Callisto Expansion addresses sexual assault and sexual coercion in professional industries.

ORIGINAL

Callisto Campus

Callisto Campus is designed to detect repeat perpetrators and empower victims to make the reporting decision that feels right for them.

Our flagship online system, Callisto Campus, provides survivors with three options:

WRITE

Save time-stamped written records of a sexual assault.

MATCH

Report only if another victim names the same perpetrator.

REPORT

Report directly to campus administrators, without waiting for a match.

NEW

Callisto Expansion

In 2018 Callisto expanded our reporting platform into professional environments. In this version of Callisto we adapt our signature matching system to empower survivors beyond college campuses:

MATCH

Under the Callisto "Matching Escrow," victims input the identity of their perpetrators under the precondition that, if a match is found, a Callisto Legal Options Counselor will reach out to each victim individually.

LEGAL OPTIONS COUNSELING

A Callisto Legal Options Counselor advises victims on their choices following a match, including reporting —only if this is the right route for them.

Mihir Bellare

UCSD

22

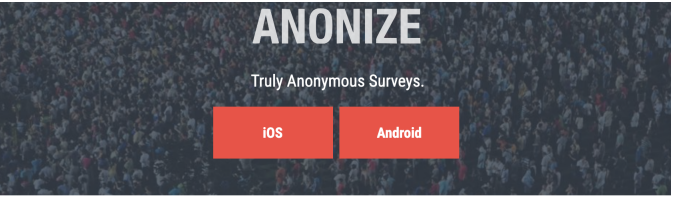
Secure computation usage: Anonize

ANONIZE

Truly Anonymous Surveys.

iOS

Android



Introducing ANONIZE.

Traditional Web Surveys Are Not Anonymous

Traditional survey systems on the web claim that your response is anonymous, but in reality, they keep a database that maintains an explicit link between you and your response. They need this to make sure you only respond ONCE. You must trust them to maintain your anonymity, you must trust that they never get hacked. As demonstrated by recent attacks (e.g., Sony), this is a DANGEROUS principle.

The ANONIZE System Enables True Anonymity

The ANONIZE system is based on a new cryptographic technology that ensures only survey targets can respond, and only once, while unconditionally guaranteeing anonymity: even if our servers are fully compromised, and all data is leaked, a link between users and their responses cannot be found. Anyone can create a survey by specifying a set of target user emails. The survey is posted on a public webpage (like this one) but only targetted users can submit a response.

Mihir Bellare

UCSD

23

Bitcoin



What is money?

Money is a number in a ledger.

A transaction:

"I, Alice, hereby transfer 6 units of money to Chong"

Person	Balance
Alice	18
Bob	13
Chong	14



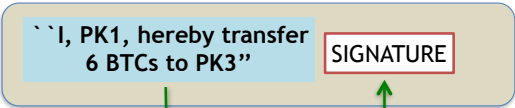
Person	Balance
Alice	12
Bob	13
Chong	20

1

2

Bitcoin transactions

Money is a number in a ledger but names are replaced by public keys.



Use of public keys as opposed to names makes the system anonymous.

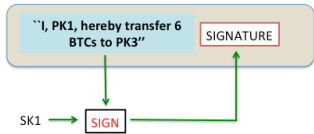
Person	Balance
PK1	18
PK2	13
PK3	14



Person	Balance
PK1	12
PK2	13
PK3	20

3

But ...



Person	Balance
PK1	18
PK2	13
PK3	14



Person	Balance
PK1	12
PK2	13
PK3	20

Question	Answer
Who maintains the ledger?	Everyone
How does PK3 know that PK1 has 6 BTCs to spend?	Transaction linking
How is double-spending prevented?	Block chains, mining

4

Two Problems

Person	Balance
PK1	18
PK2	13
PK3	14

Over-spending

“I, PK1, hereby transfer 20 BTCs to PK3”

SIGNATURE

Double-spending

“I, PK1, hereby transfer 12 BTCs to PK3”

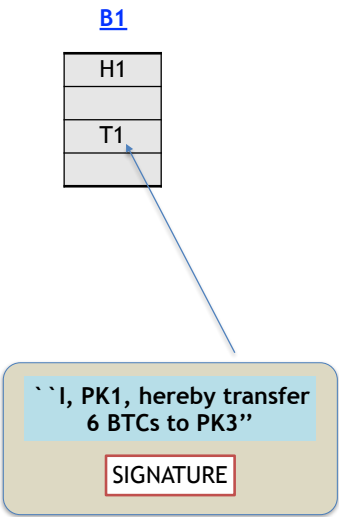
SIGNATURE

“I, PK1, hereby transfer 10 BTCs to PK2”

SIGNATURE

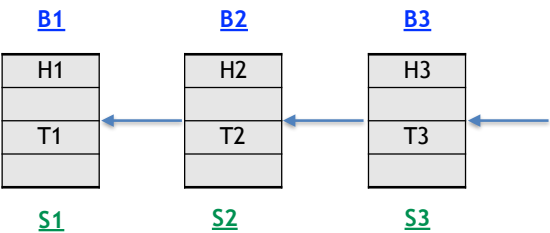
5

Blocks



6

Transaction Linking

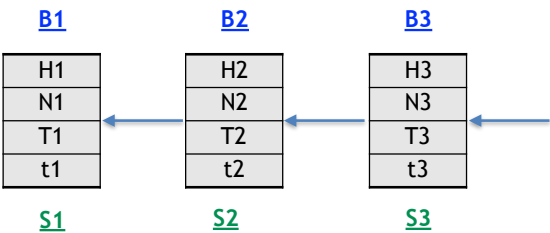


H1 = NULL S1 = SIGN(SK,B1)
H2 = HASH(B1) S2 = SIGN(SK,B2)
H3 = HASH(B2) S3 = SIGN(SK,B3)

Question: Who signs the blocks?
Answer: Anyone, and first person to do it gets a reward

7

Mining



H1 = NULL S1 = SIGN(SK,B1) SHA256(B1)[1..10] = 0¹⁰
H2 = HASH(B1) S2 = SIGN(SK,B2) SHA256(B2)[1..10] = 0¹⁰
H3 = HASH(B2) S3 = SIGN(SK,B3) SHA256(B3)[1..10] = 0¹⁰

To add B3 to blockchain, miner finds N3 such that SHA256(B3)[1..10] = 0¹⁰
This takes computational effort about 2¹⁰
Miner includes in B3 a transaction t3 that pays the miner a reward.
SK is the miner’s signing key.

8

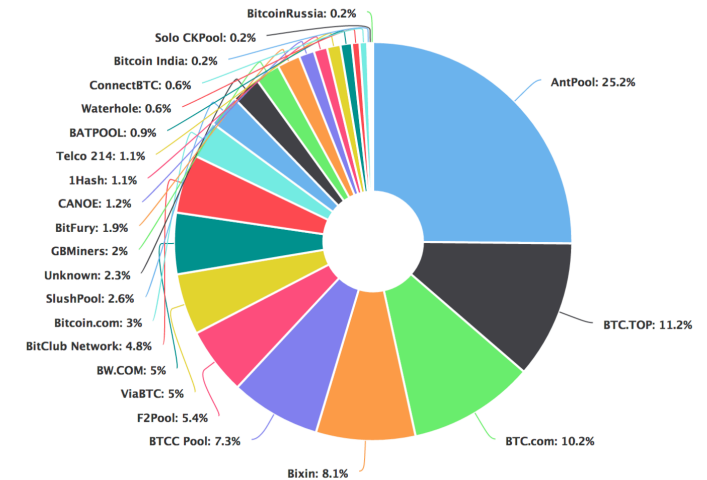
Mining Hardware

AntMiner S7	AntMiner S9	Avalon6
		
Advertised Capacity: 4.73 Th/s	Advertised Capacity: 13.5 Th/s	Advertised Capacity: 3.5 Th/s
Power Efficiency: 0.25 W/Gh	Power Efficiency: 0.098 W/Gh	Power Efficiency: 0.29 W/Gh
Weight: 8.8 pounds	Weight: 8.1 pounds	Weight: 9.5 pounds
Guide: Yes	Guide: Yes	Guide: No
Price: \$479.95	Price: \$1,987.95	Price: \$499.95
		
Appx. BTC Earned Per Month: 0.1645	Appx. BTC Earned Per Month: 0.3603	Appx. BTC Earned Per Month: 0.1232

9

The Biggest Mining Pools

The list below details the biggest Bitcoin mining pools. This is based on info from Blockchain's [pool share](#) chart:



10

The beginning



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1 Introduction

11

The Search for Satoshi



By Leah McGrath Goodman
EST



THE NEW YORKER

SUBSCRIBE MAGAZINE NEWS CULTURE POLITICS BOOKS SCIENCE & TI

ARCHIVE PHOTO BOOTH DAILY SHOUTS DAILY COMMENT CURRENCY AMY DAVIDSON

DEPT. OF TECHNOLOGY
THE CRYPTO-CURRENCY
Bitcoin and its mysterious inventor.
BY JOSHUA DAVIS
OCTOBER 10, 2011

Share PRINT MORE

Subscribers can read the full version of this story by logging into our [digital archive](#). Not a subscriber? Get immediate access to this story, along with a one-month free trial, by [subscribing now](#). Or find out about other ways to [read The New Yorker digitally](#).

DEPT. OF TECHNOLOGY about bitcoin and its mysterious creator. There are lots of ways to make money: You can earn it, find it, counterfeit it, steal it. Or, if you're Satoshi Nakamoto, you can invent it. That's what he did on the evening of January 3, 2009, when he pressed a button on his keyboard and created a new

12

Bitcoin Exchanges

Allow exchange between bitcoins and real currencies such as US\$

Mt. Gox, Bitomat, CoinRnr, BIT, OKPay.com, BitStamp.net, Bitcoinica, CoinCafe, CoinMkt, Coinbase.com, CampBX, BitQuick, First Meta, ...



Exchange Compromises and News

Currencies

Where Did the Bitcoins Go? The Mt. Gox Shutdown, Explained

By Joshua Brustein | February 26, 2014



How did the once-largest Bitcoin exchange lose hundreds of millions

CEO of bitcoin exchange found dead in Singapore

31 | Facebook | Twitter | LinkedIn | Email | Print | More

By Associated Press, Published: March 5

SINGAPORE — The American CEO of a virtual currency exchange was found dead near her home in Singapore.

Exchange	Date
Mt. Gox	June 2011
Bitomat	July 2011
MyBitcoin	August 2011
Bitfloor	September 2012
instawallet	April 2013
Mt. Gox	February 2014

13

14

Silk Road

Online marketplace founded February 2011.

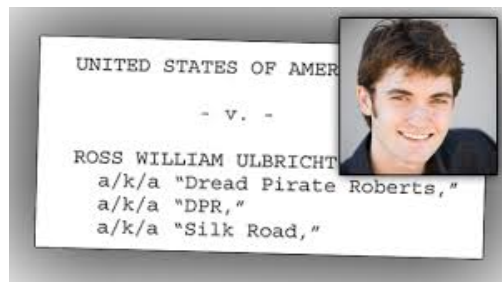
The Amazon.com of illegal drugs.

15 million transactions annually, \$30-\$45 mill

Shutdown by FBI October 2013.

Ross William Ulbricht (aka Dread Pirate Roberts) arrested on suspicion of drug trafficking, soliciting murder, money laundering, ...

FBI seized over 26,000 BTC (\$3.6 million) from accounts on Silk Road



15

XBT to USD Chart

7 Dec 2012 00:00 UTC - 6 Dec 2017 19:07 UTC XBT/USD close:12864.42558 low:13.25005 high:12873.05187

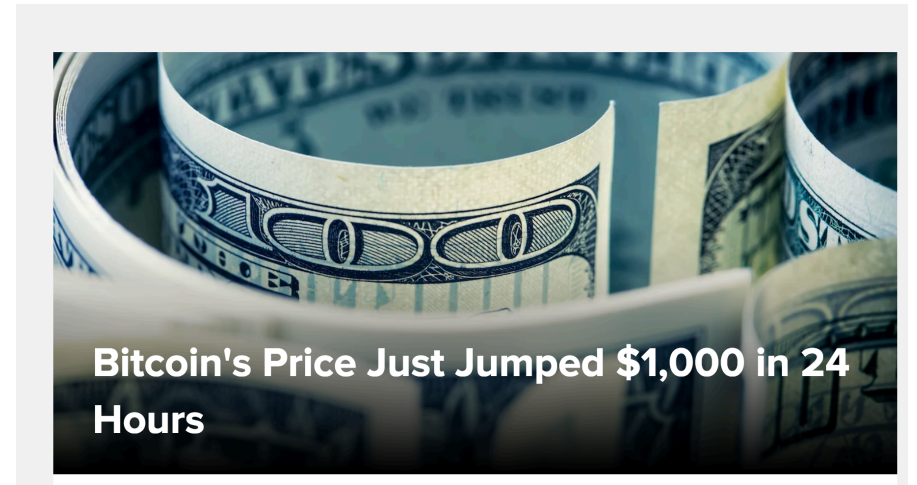


XBT - Bitcoin ↔ USD - US Dollar →

16

XBT to USD Chart

6 Nov 2017 19:00 UTC - 6 Dec 2017 19:07 UTC XBT/USD close: **12864.42558** low: **5694.30868** high: **12873.05187**

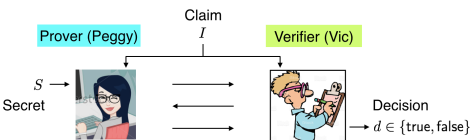


The Bitcoin Movie

By Scott Driscoll
22 minutes

Please turn off all cellphones and pagers
No recording permitted
Interrupt to **PAUSE** or **REWIND** !

Zero-Knowledge Protocols



1

Mihir Bellare, UCSD

The People



The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser
MIT

Silvio Micali
MIT

Charles Rackoff
University of Toronto

on We propose to classify languages according to the amount of additional knowledge that must be released for proving membership in them.

2

Mihir Bellare, UCSD

The Awards



Association for Computing Machinery
Advancing Computing as a Science & Profession

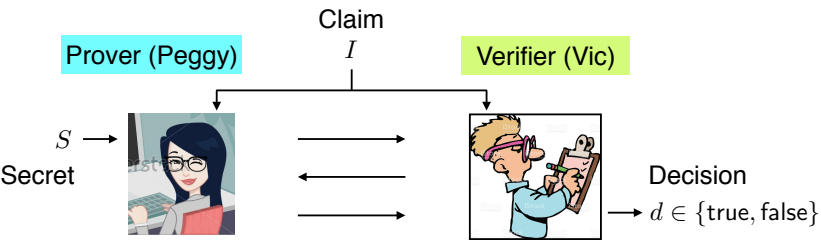
Goldwasser, Micali Receive ACM Turing Award for Advances in Cryptography

MIT Researchers' Innovations Became Gold Standard for Enabling Secure Internet Transactions

acm
The Association for Computing Machinery
Advancing Computing as a Science & Profession

3

Mihir Bellare, UCSD



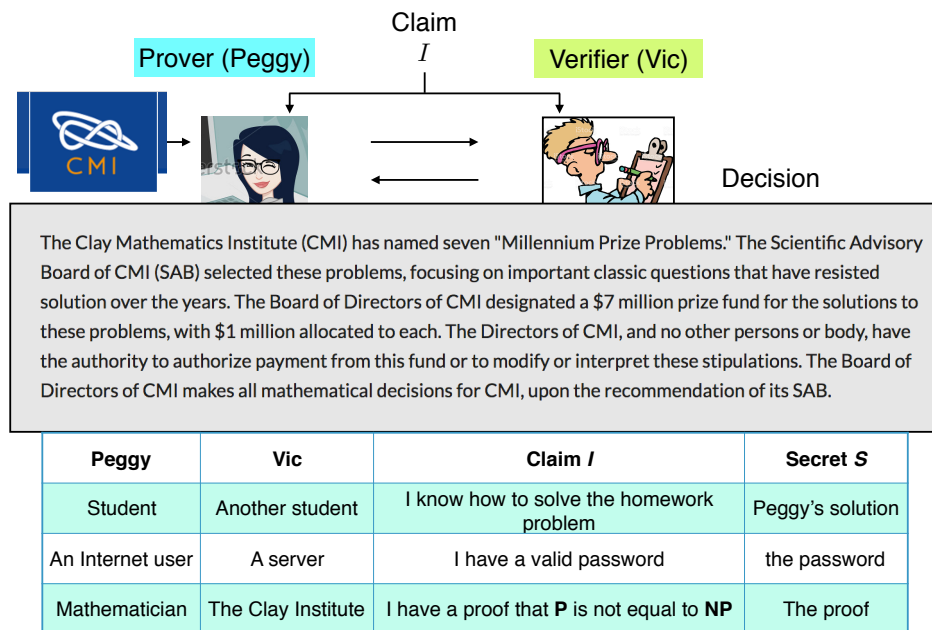
A zero-knowledge protocol allows **Peggy** to

- Convince **Vic** that her claim is true and that she knows **S**
- Without revealing anything beyond that

Peggy	Vic	Claim <i>I</i>	Secret <i>S</i>
Student	Another student	I know how to solve the homework problem	Peggy's solution
An Internet user	A server	I have a valid password	the password
Mathematician	The Clay Institute	I have a proof that P is not equal to NP	The proof

4

Mihir Bellare, UCSD



5

Mihir Bellare, UCSD

Ali-Baba's Zero-Knowledge Protocol

How to Explain Zero-Knowledge Protocols to Your Children

QUISQUATER Jean-Jacques⁽¹⁾, Myriam, Muriel, Michaël
GUILLOU Louis⁽²⁾, Marie Annick, Gaïd, Anna, Gwenolé, Soazig
 in collaboration with Tom *BERSON*⁽³⁾ for the English version

⁽¹⁾ Philips Research Laboratory, Avenue Van Becelaere, 2, B-1170 Brussels, Belgium.

⁽²⁾ CCETT/EPT, BP 59, F-35512 Cesson Sévigné, France.

⁽³⁾ Anagram Laboratories, P.O. Box 791, Palo Alto CA 94301, USA.

The Strange Cave of Ali Baba

◇ Know, oh my children, that very long ago, in the Eastern city of Baghdad, there lived an old man named Ali Baba. Every day Ali Baba would go to the bazaar to buy or sell things. This is a story which is partly about Ali Baba, and partly also about a cave, a

This story is used to explain zero-knowledge in many places.
 Including Wikipedia.
 But it doesn't make a lot of sense.
 We will use Joseph Jaeger's variant.

6

Mihir Bellare, UCSD

$MW[A, B]$ = Magic Words opening the $A \rightarrow B$ portal

$MW[B, A]$ = Magic Words opening the $B \rightarrow A$ portal

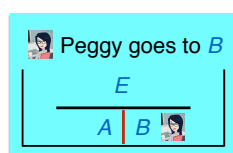
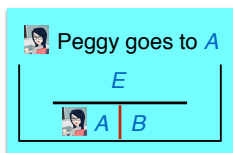
Peggy has secret $S \in \{MW[A, B], MW[B, A]\}$

Peggy does not want Vic to know which of the two magic words she has.

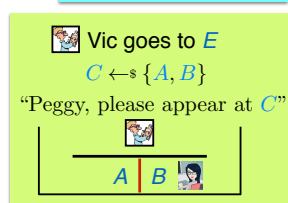
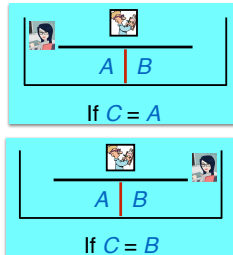
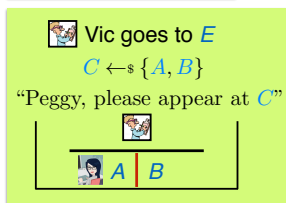
Ali Baba's ZK Protocol

If Peggy knows $MW[A, B]$:

If Peggy knows $MW[B, A]$:



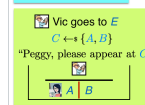
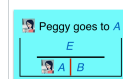
Final step, in either case:



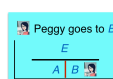
7

Mihir Bellare, UCSD

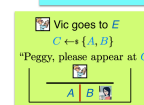
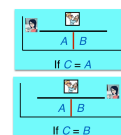
If Peggy knows $MW[A, B]$:



If Peggy knows $MW[B, A]$:



Final step, in either case:

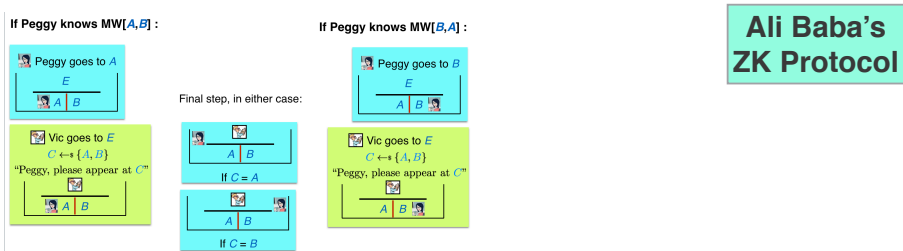


Completeness: If Peggy's claim is true, meaning she knows either $MW[A, B]$ or $MW[B, A]$, and both parties follow the protocol, then Vic will accept.

Why? Peggy can appear at whatever side Vic requests.

8

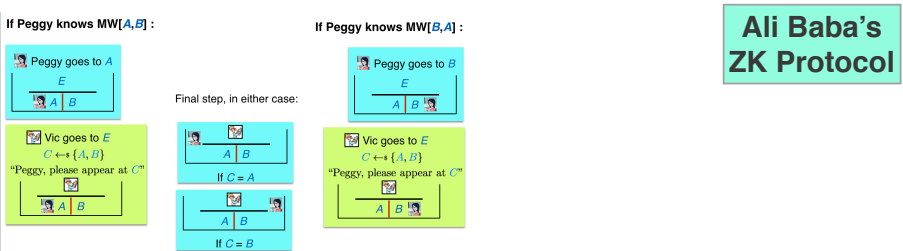
Mihir Bellare, UCSD



Completeness: If Peggy's claim is true, meaning she knows either MW[A,B] or MW[B,A], and both parties follow the protocol, then Vic will accept.

Soundness: If Peggy's claim is false, meaning she knows neither MW[A,B] nor MW[B,A], then Vic will reject with probability at least 1/2, **even if Peggy cheats**, meaning does not follow the prescribed protocol.

Why? Cheating Peggy can start at any $X \in \{A, B\}$ of her choice, but Vic picks C at random and cheating Peggy cannot appear at $C \neq X$.

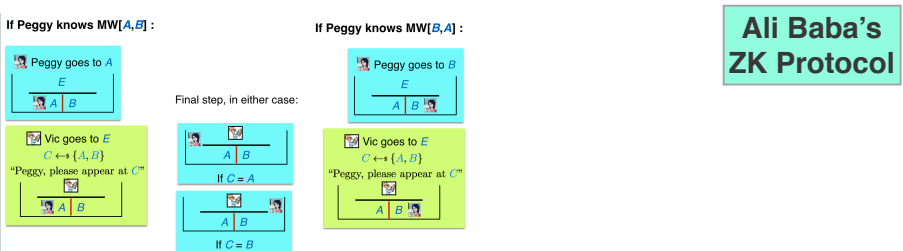
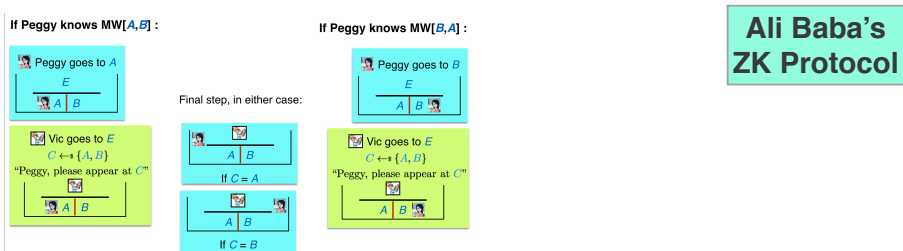


Completeness: If Peggy's claim is true, meaning she knows either MW[A,B] or MW[B,A], and both parties follow the protocol, then Vic will accept.

Soundness: If Peggy's claim is false, meaning she knows neither MW[A,B] nor MW[B,A], then Vic will reject with probability at least 1/2, **even if Peggy cheats**, meaning does not follow the prescribed protocol.

Zero-knowledge: If Peggy's claim is true, and Peggy follows the protocol, then Vic will not learn which of the two secrets MW[A,B], MW[B,A] Peggy knows.

Why? Regardless of the secret, Vic sees Peggy appearing at whatever side he requests.



	Pegg's claim is	Peggy is	Vic will
Completeness	TRUE	honest	always accept
Soundness	FALSE	cheating	accept with probability at most 1/2
Zero-knowledge	TRUE	honest	not learn which of the two secrets Peggy knows

This story may not make complete sense. To make zero-knowledge sensible, we need DEFINITIONS. The definitions are intriguing: how can one mathematically capture the “knowledge” learned by interacting with another party?

	Pegg's claim is	Peggy is	Vic will
Completeness	TRUE	honest	always accept
Soundness	FALSE	cheating	accept with probability at most 1/2
Zero-knowledge	TRUE	honest	not learn which of the two secrets Peggy knows