Two- and Multi-Party Protocols

JASS 2005

Julian Traut

March, 30. - April 9. 2005

Why cryptographic protocols?

Why cryptographic protocols?

- cryptography is concerned with secure communication
- various other tasks
- enable to solve many real-world problems electronically
- theoretical any given functionality can be performed with protocols

Story - Part I

Story - Part I

Suppose Joe has found a way to prove that not $P = NP$. He wants to show this paper to Ernesto, his mentor. But Ernesto is in St. Petersburg doing some fancy stuff on cryptography. So Joe has to wait until Ernesto returns.

Story - Part I

Suppose Joe has found a way to prove that not $P = NP$. He wants to show this paper to Ernesto, his mentor. But Ernesto is in St. Petersburg doing some fancy stuff on cryptography. So Joe has to wait until Ernesto returns.

Joe suspects that Jack might prove $P \neq NP$, too. Since Joe is eager to be promoted he has to prove, that he is first to produce a copy of this important work.

Story - Part I

Suppose Joe has found a way to prove that not $P = NP$. He wants to show this paper to Ernesto, his mentor. But Ernesto is in St. Petersburg doing some fancy stuff on cryptography. So Joe has to wait until Ernesto returns.

Joe suspects that Jack might prove $P \neq NP$, too. Since Joe is eager to be promoted he has to prove, that he is first to produce a copy of this important work.

Joe plans to print the whole paper and go to a notary and let him sign his copy.

Story - Part I

Suppose Joe has found a way to prove that not $P = NP$. He wants to show this paper to Ernesto, his mentor. But Ernesto is in St. Petersburg doing some fancy stuff on cryptography. So Joe has to wait until Ernesto returns.

Joe suspects that Jack might prove $P \neq NP$, too. Since Joe is eager to be promoted he has to prove, that he is first to produce a copy of this important work.

Joe plans to print the whole paper and go to a notary and let him sign his copy.

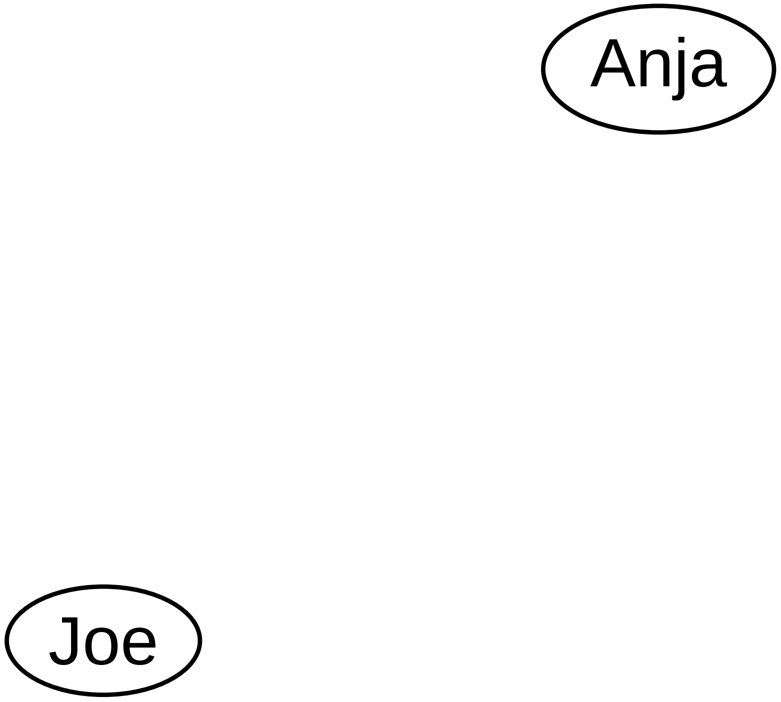
But what's that! All printers in the department seem to malfunction. So Joe needs a way to electronically timestamp his work.

Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.

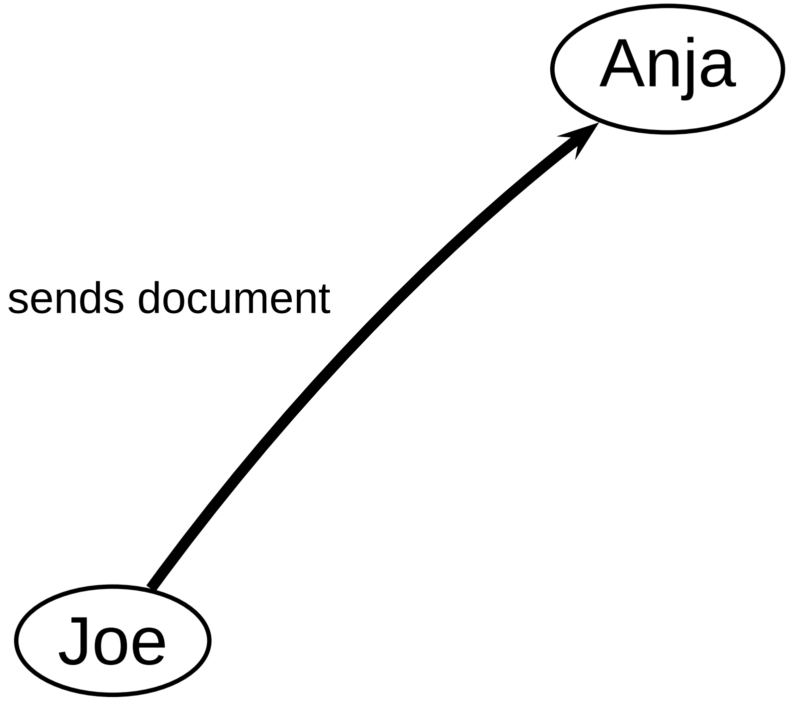
Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.



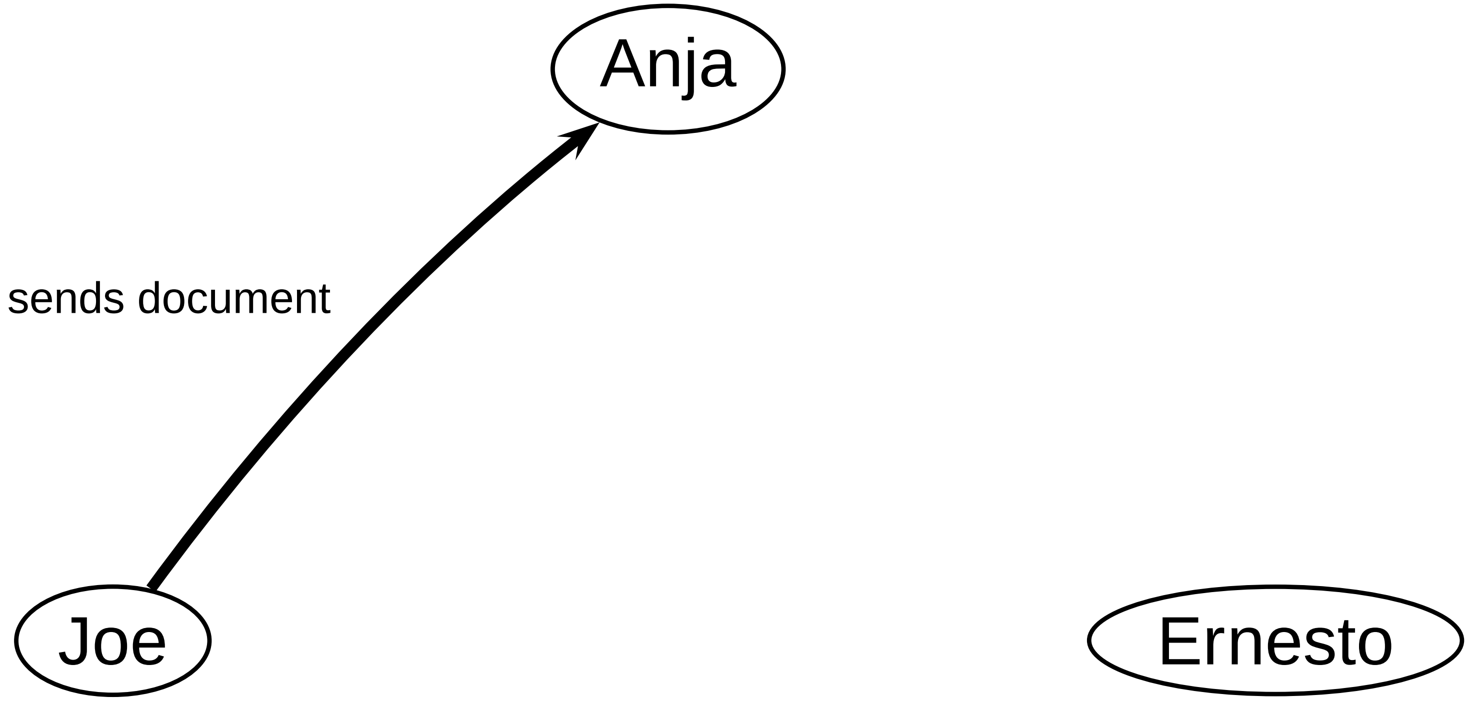
Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.



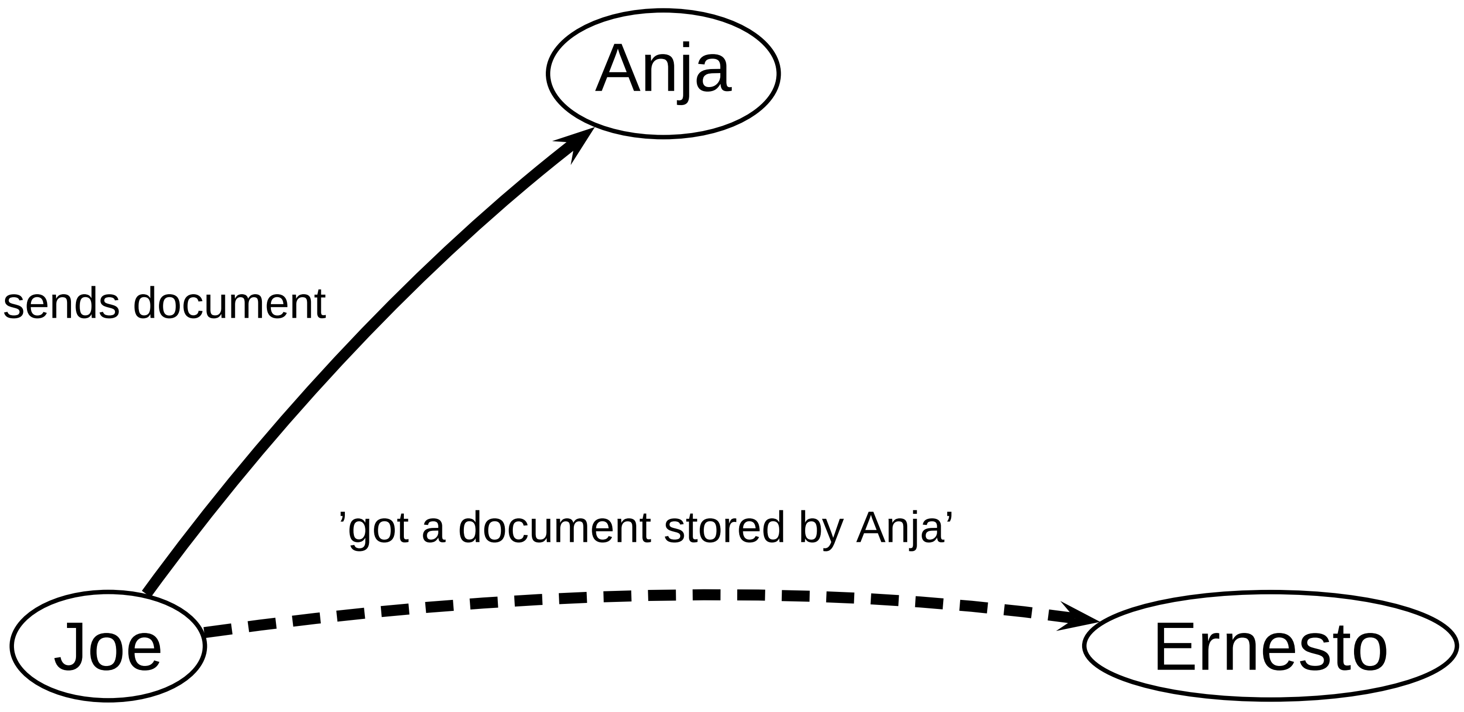
Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.



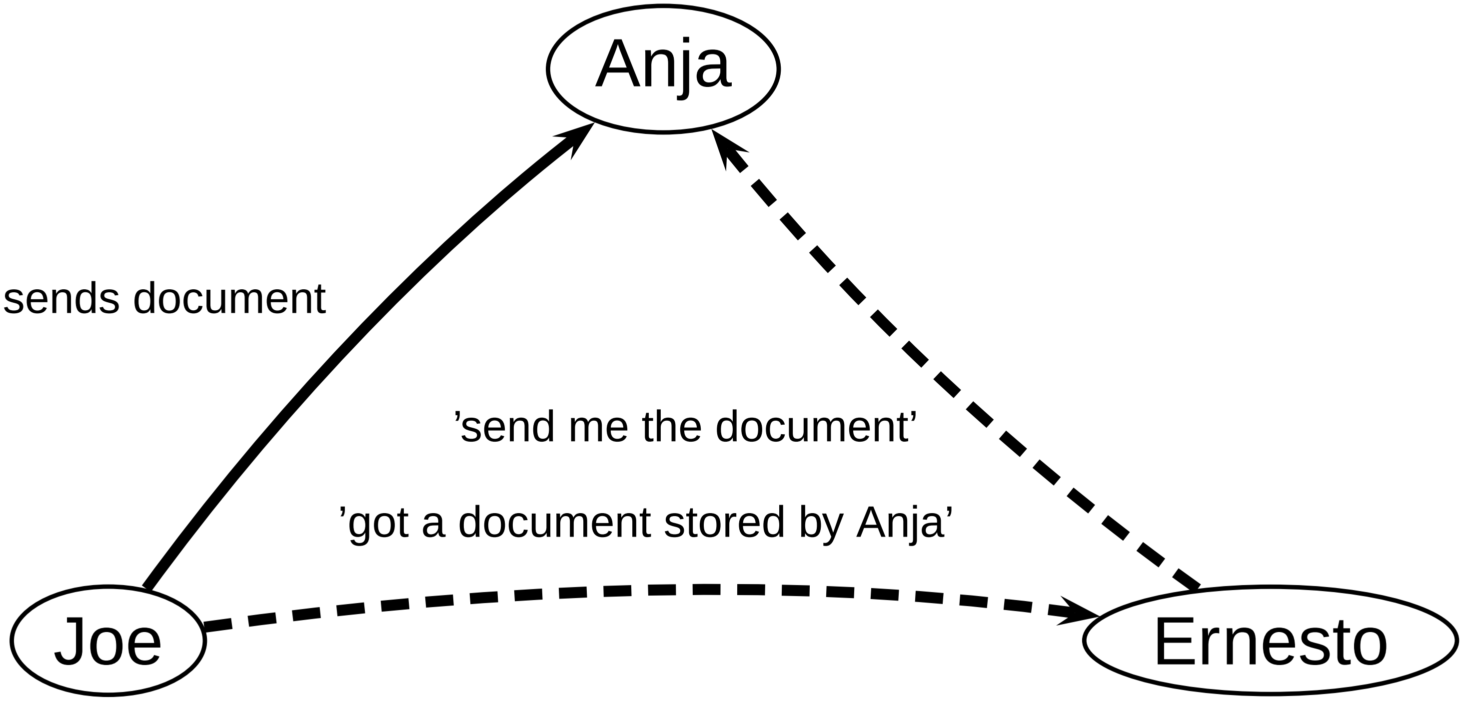
Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.



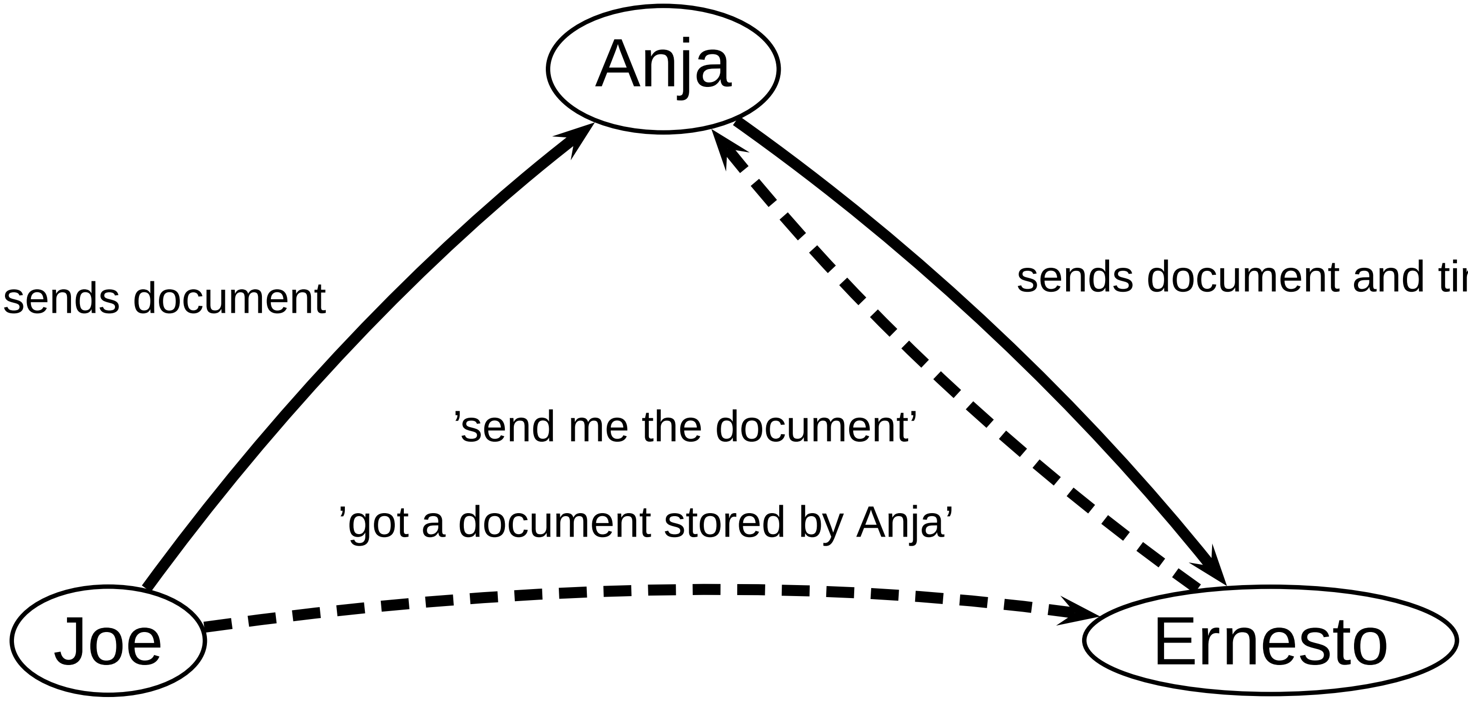
Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.



Timestamping - First Idea (I)

Why not use Anja as a substitute for the notary.



Timestamping - First Idea (II)

There are several problems with this protocol.

Timestamping - First Idea (II)

There are several problems with this protocol.

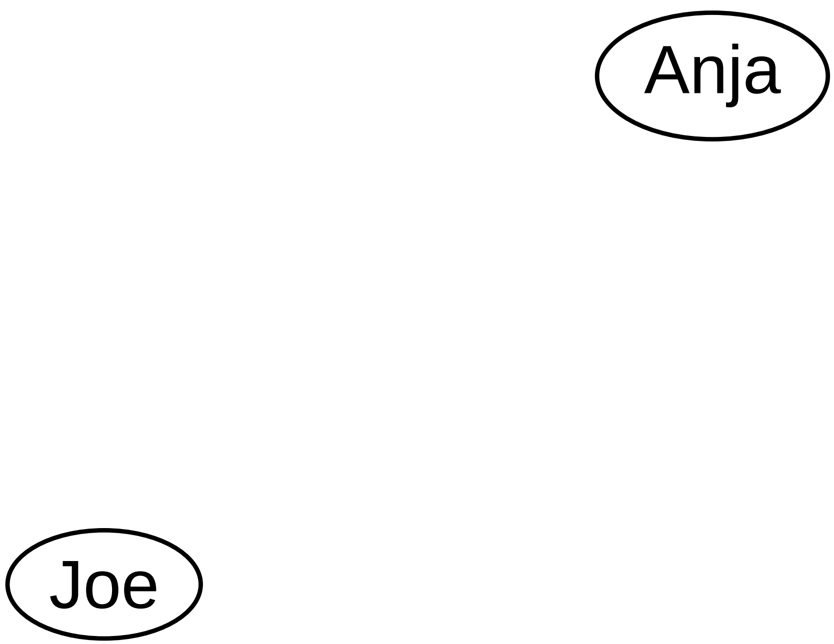
- no privacy (transmission, database)
- no efficiency (huge database)
- errors may occure (transmission, database)
- third party may not be honest

Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.

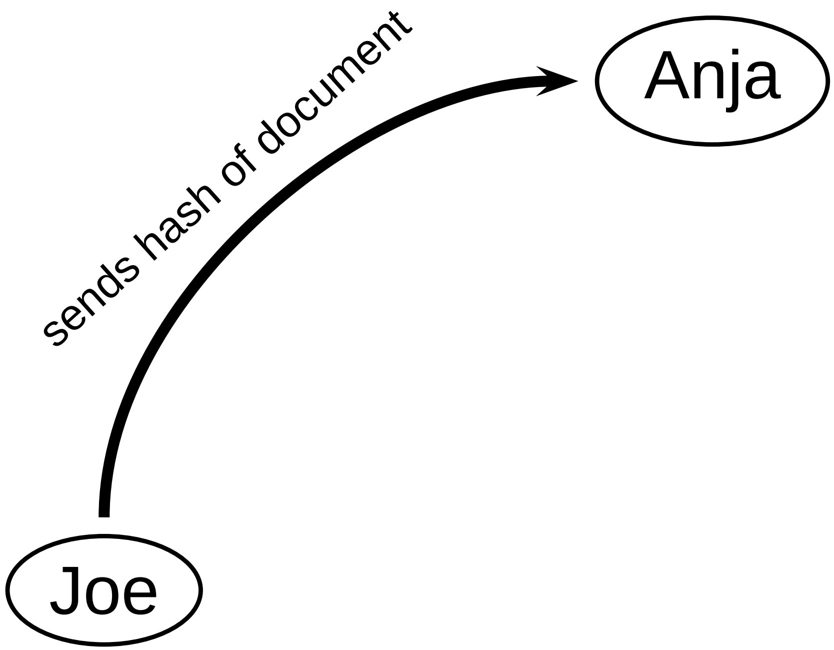
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



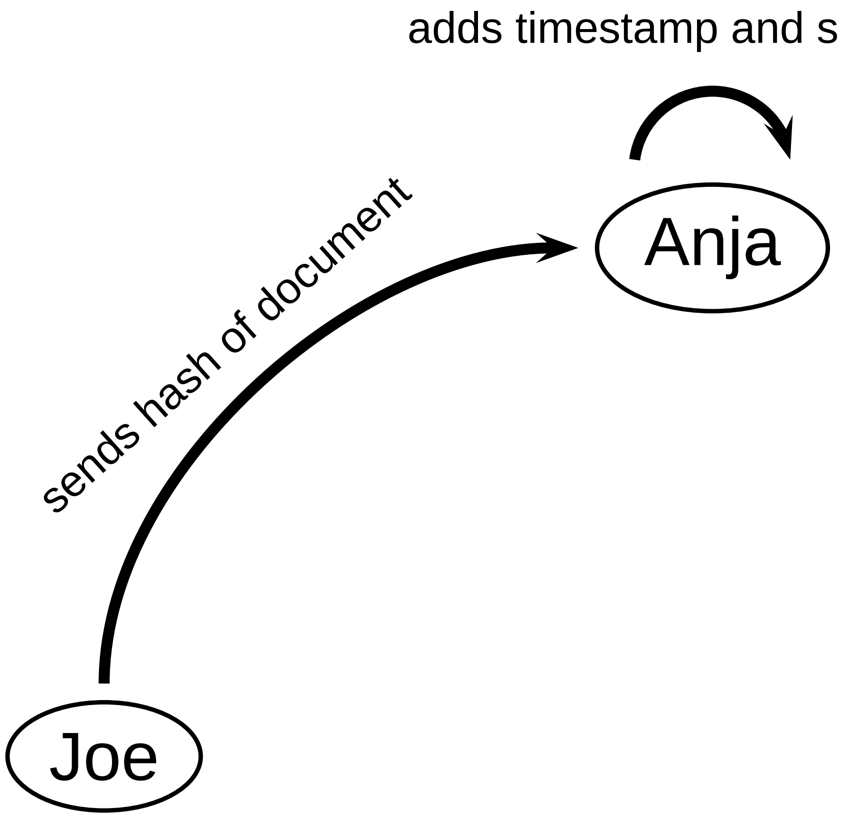
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



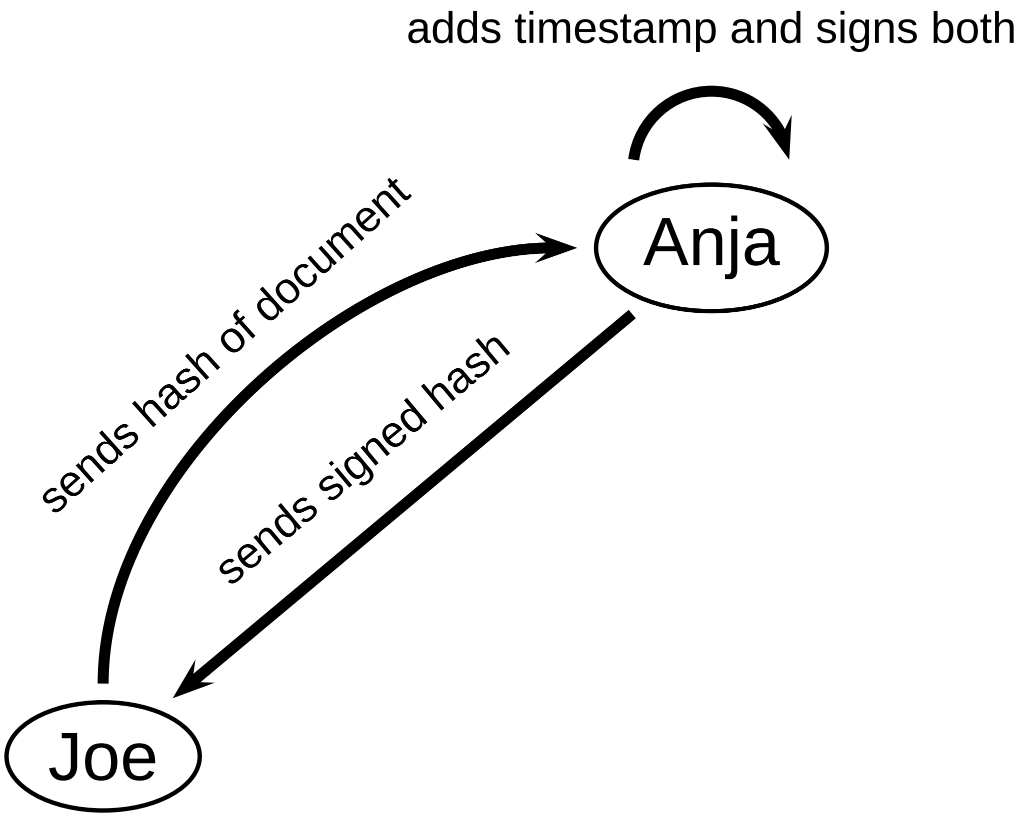
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



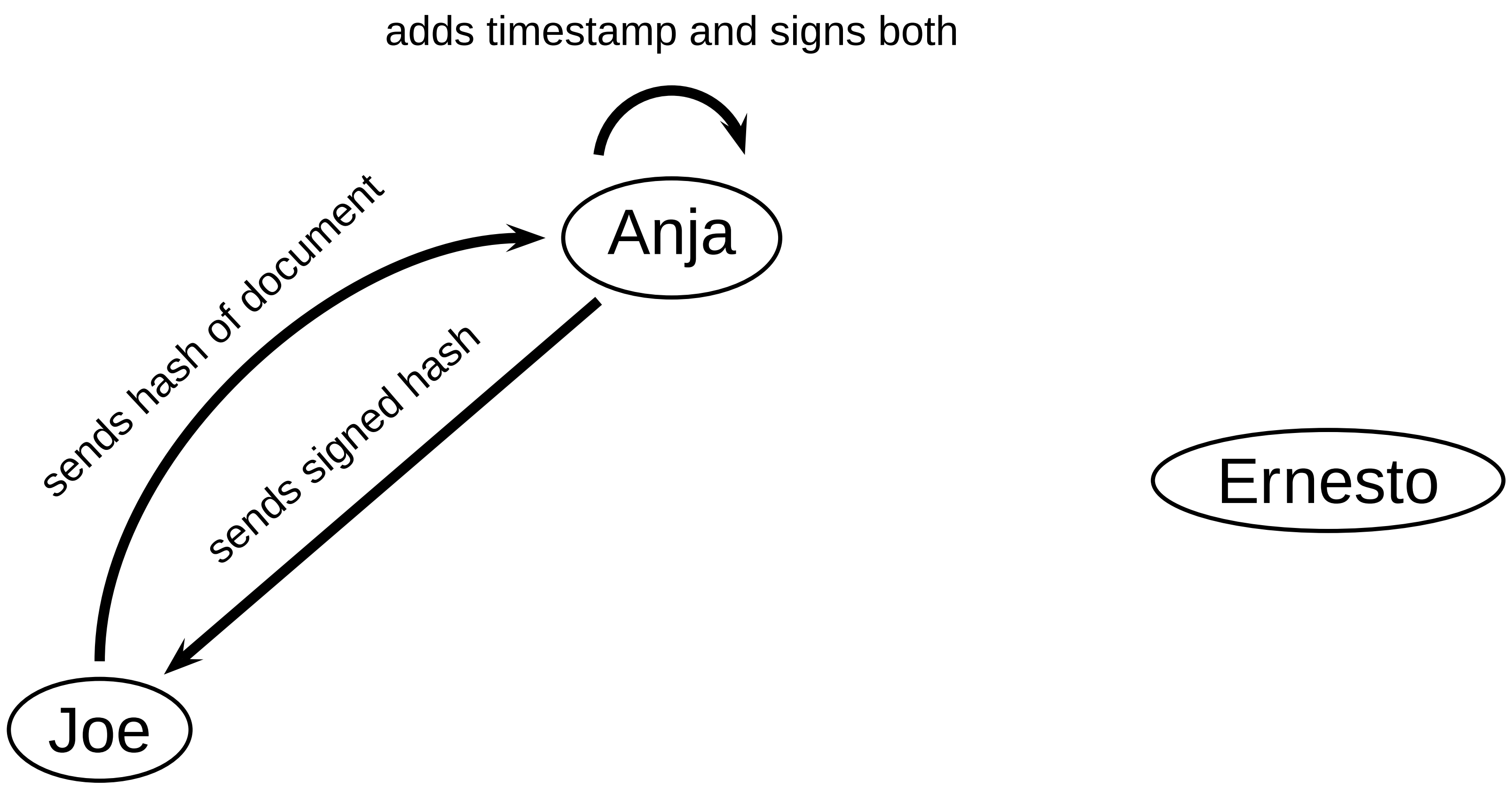
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



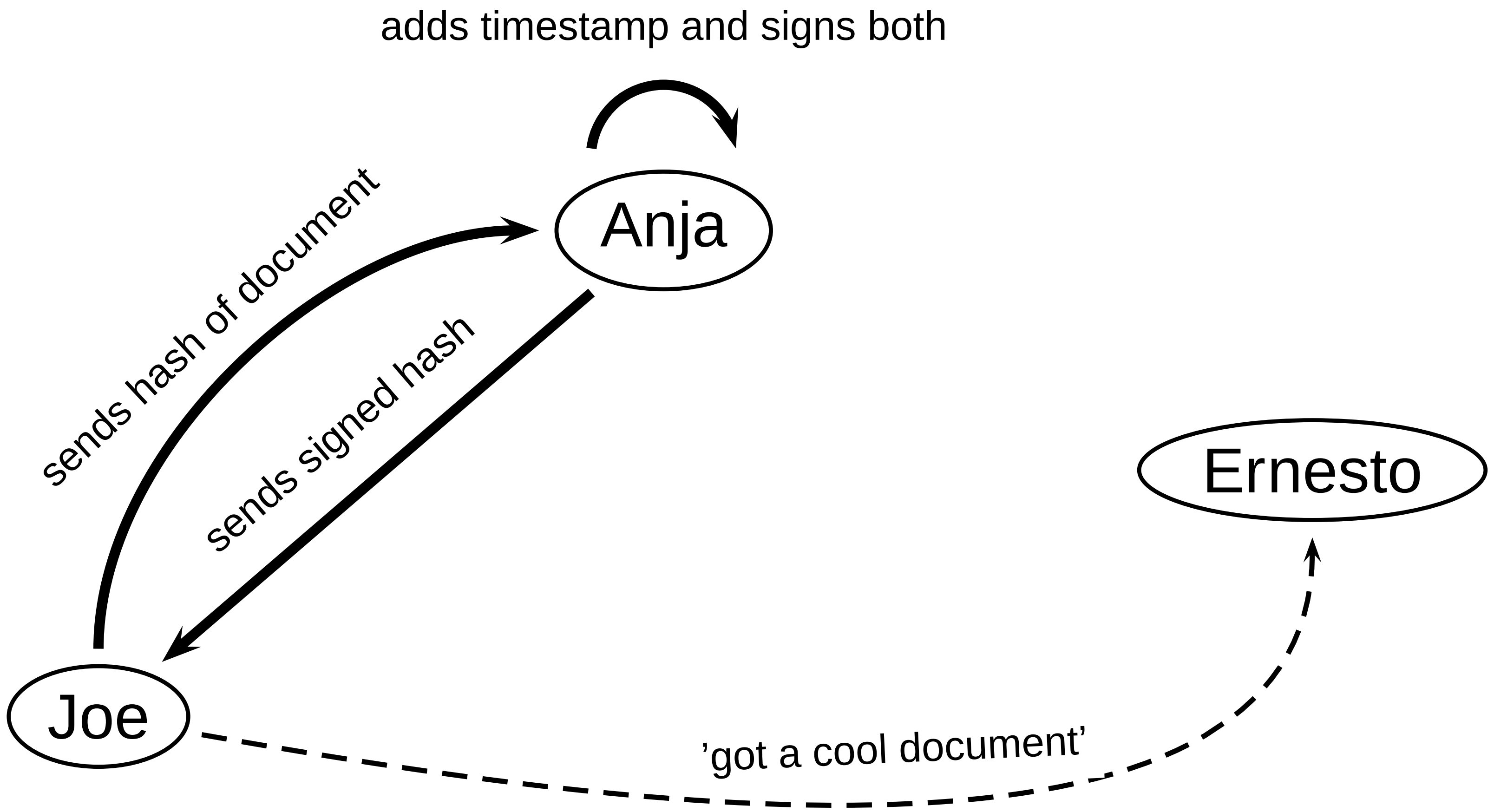
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



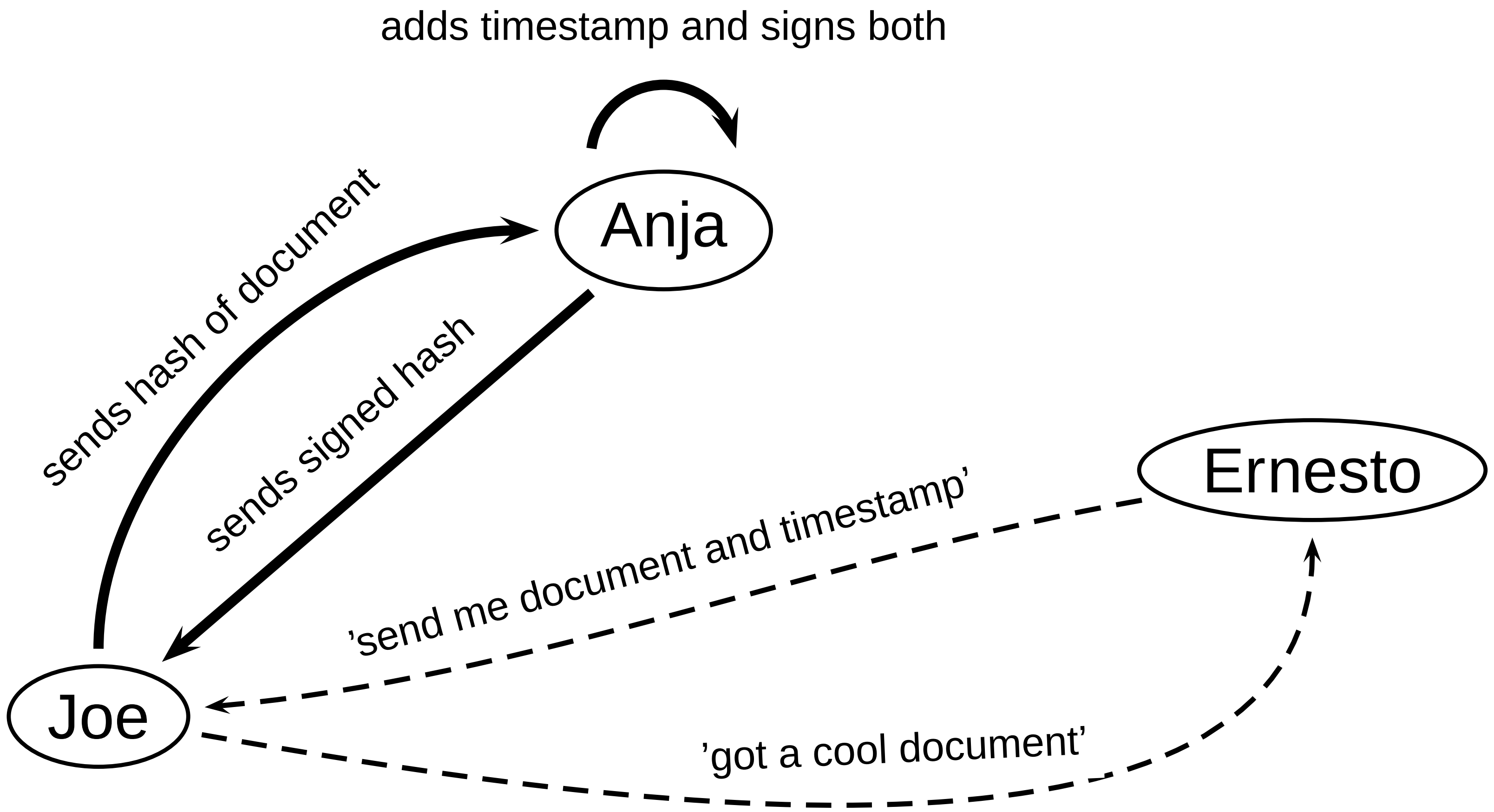
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



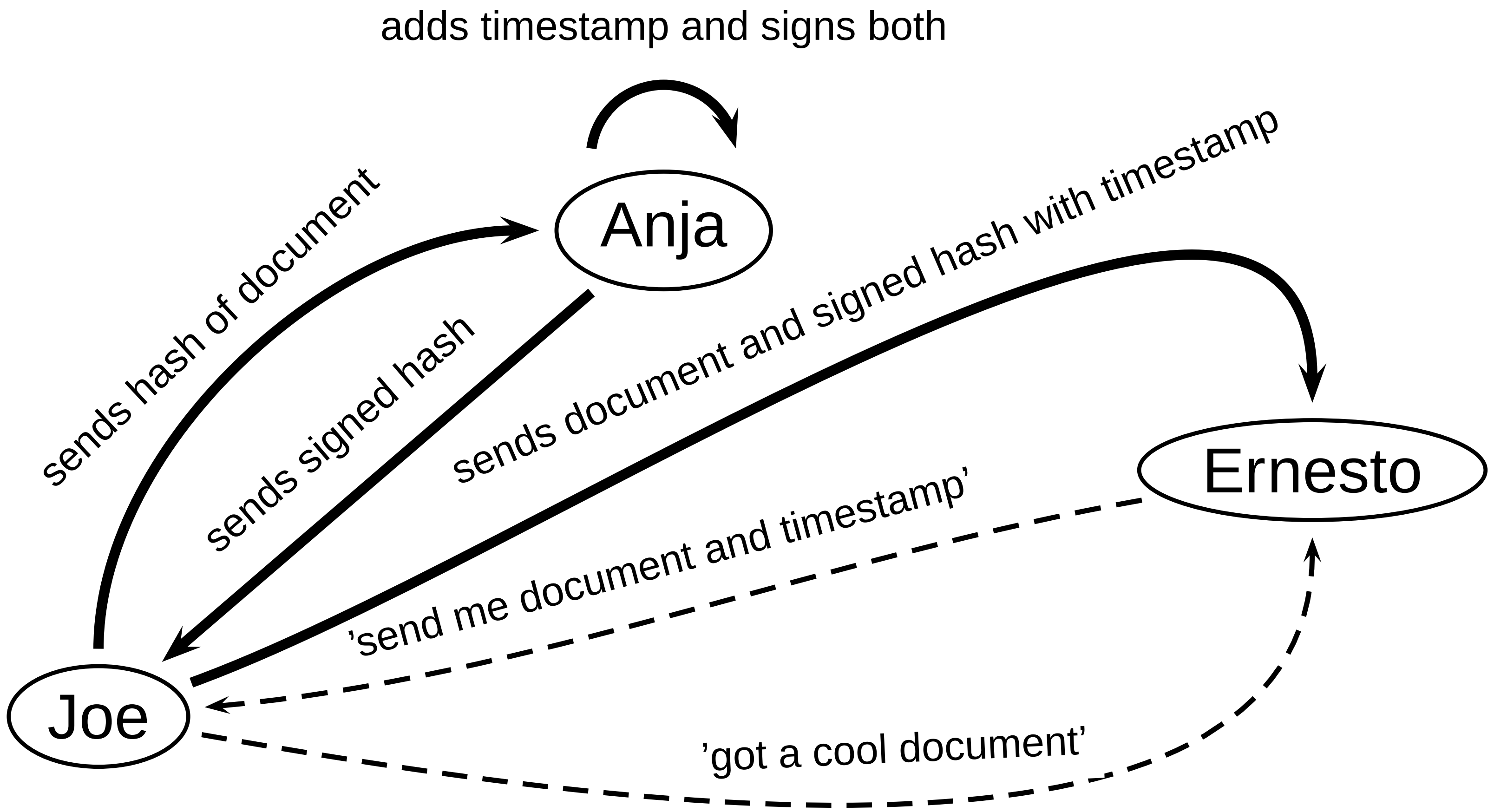
Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



Timestamping - Second Try (I)

We use one-way hashfunctions and digital signatures to enhance the protocol.



Timestamping - Second Try (II)

This protocol solves nearly all problems.

Timestamping - Second Try (II)

This protocol solves nearly all problems.

- privacy (only hash is revealed)
- efficiency (no database is needed)
- no errors (examine signed hash immediately)
- remaining Problem: Joe and Anja might work together

Timestamping - Final Try (I)

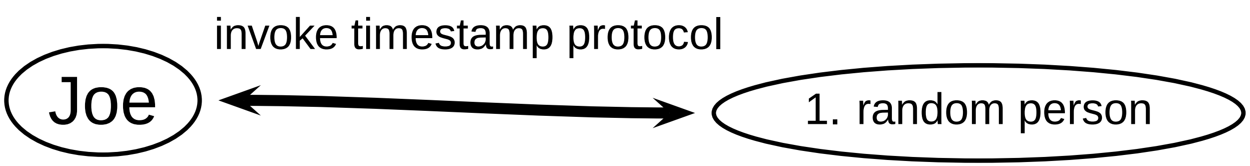
We do away with Anja altogether.

Timestamping - Final Try (I)

We do away with Anja altogether.

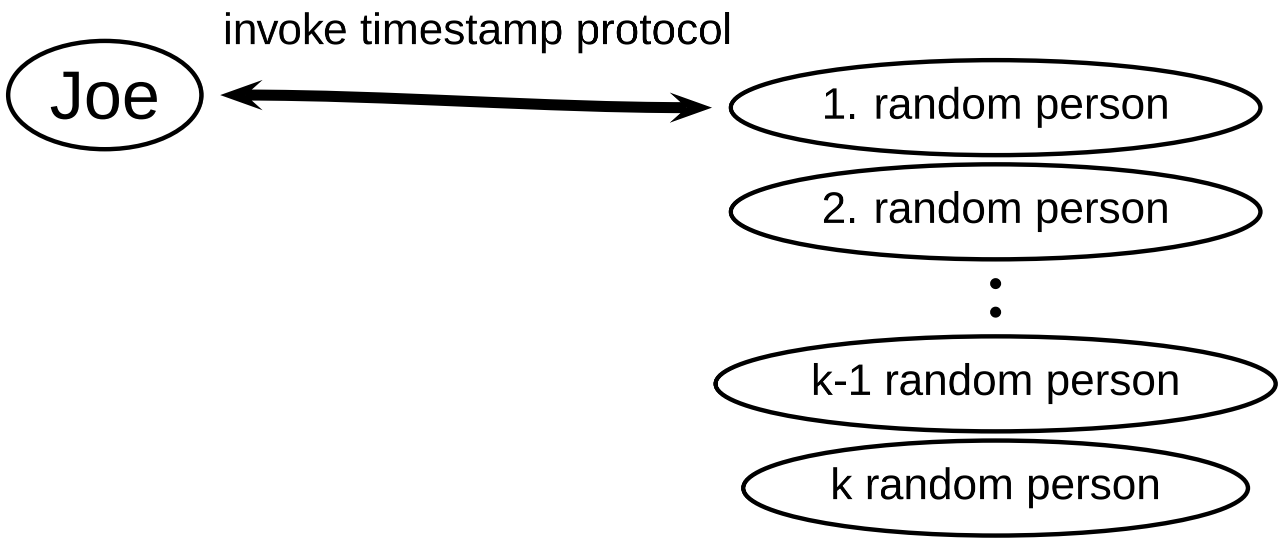
Timestamping - Final Try (I)

We do away with Anja altogether.



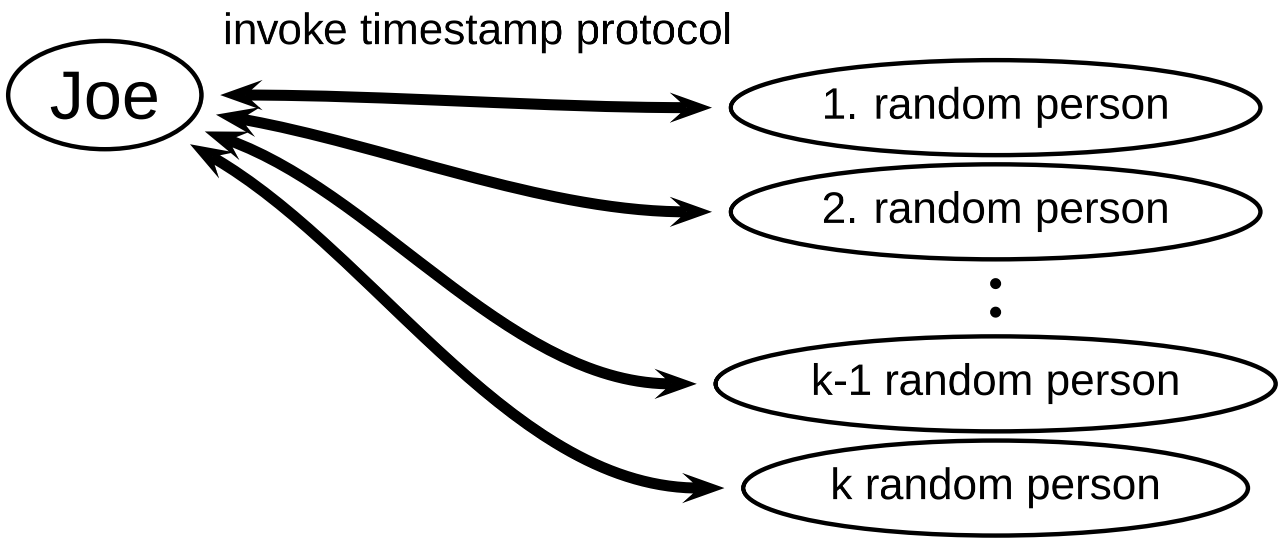
Timestamping - Final Try (I)

We do away with Anja altogether.



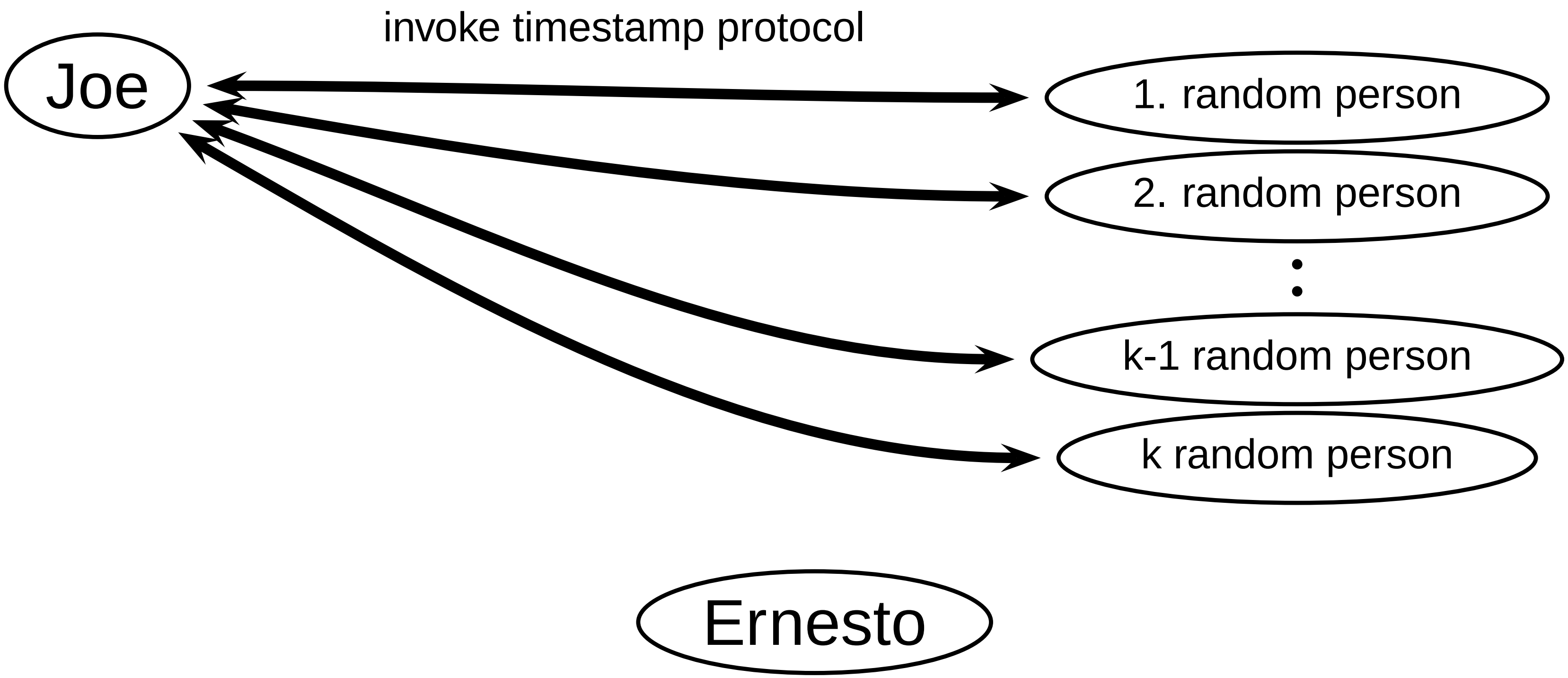
Timestamping - Final Try (I)

We do away with Anja altogether.



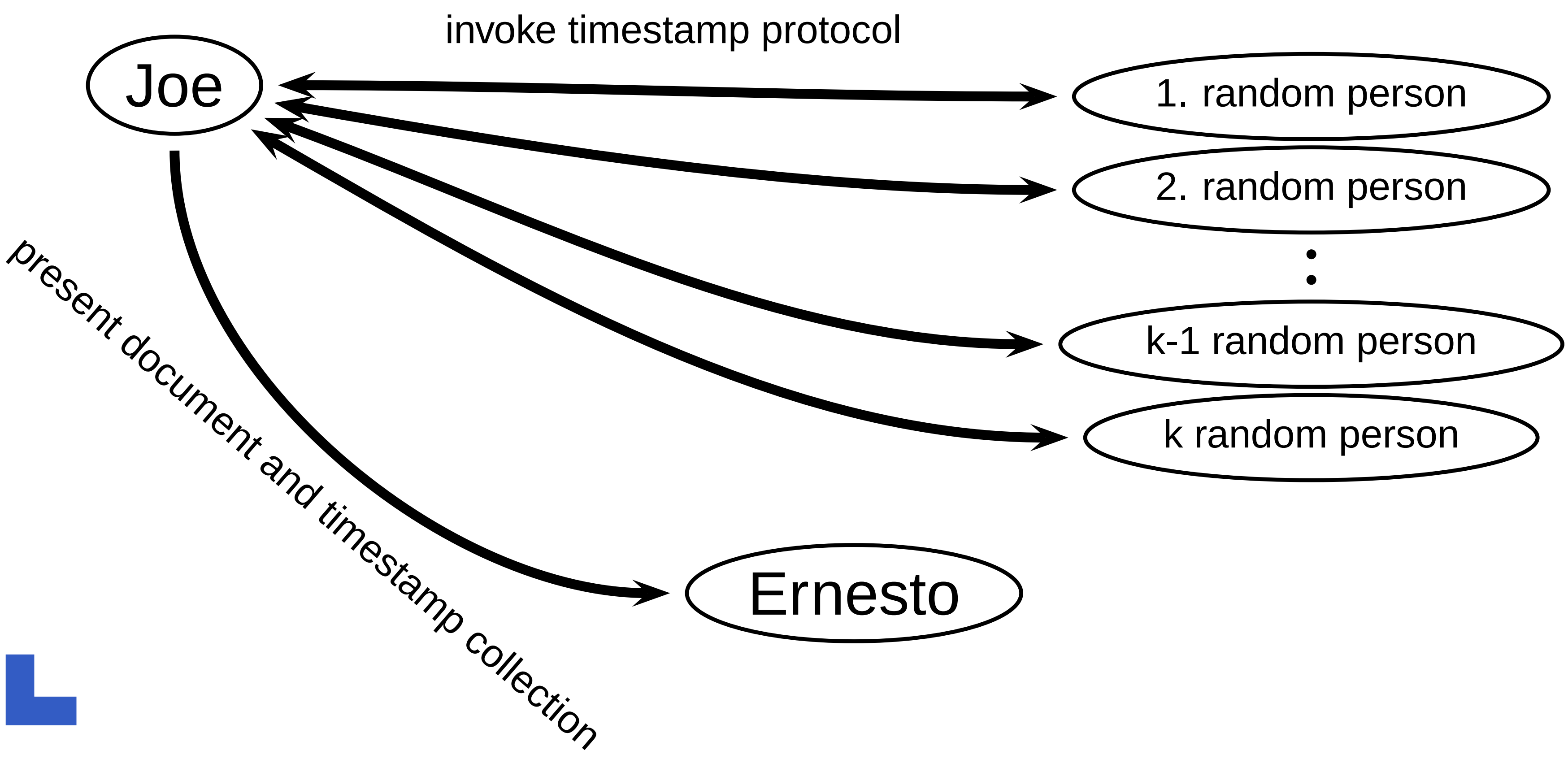
Timestamping - Final Try (I)

We do away with Anja altogether.



Timestamping - Final Try (I)

We do away with Anja altogether.



Timestamping - Final Try (II)

This protocols makes it very hard for Joe to cheat.

Timestamping - Final Try (II)

This protocols makes it very hard for Joe to cheat.

- for selection: random-number-generator with hash of document as input
- choose k sufficiently high
- only a subset of k persons should suffice for a valid timestamp

Story - Part II

Story - Part II

When Ernesto came home he got the promising paper from Joe and gave him a huge advance on salary. Joe does not know what to do with all the money and suggests a cool poker game with his friends.

Story - Part II

When Ernesto came home he got the promising paper from Joe and gave him a huge advance on salary. Joe does not know what to do with all the money and suggests a cool poker game with his friends. But all his poker playing friends got no money to play high stake poker, since they did not prove anything in the last few month.

Story - Part II

When Ernesto came home he got the promising paper from Joe and gave him a huge advance on salary. Joe does not know what to do with all the money and suggests a cool poker game with his friends. But all his poker playing friends got no money to play high stake poker, since they did not prove anything in the last few month.
So he calls up Steve in New York and Lee in Tokyo, who made a lot of money creating approximation algorithms for NP-complete problems, and asks whether they would join some poker game.

Story - Part II

When Ernesto came home he got the promising paper from Joe and gave him a huge advance on salary. Joe does not know what to do with all the money and suggests a cool poker game with his friends.
But all his poker playing friends got no money to play high stake poker, since they did not prove anything in the last few month.
So he calls up Steve in New York and Lee in Tokyo, who made a lot of money creating approximation algorithms for NP-complete problems, and asks whether they would join some poker game.
Since Steve and Lee wont come to Munich just for an evening of poker they agree on playing poker via modem. All they need now is a protocol to do this in a fair way.

Mental Poker - Requirements

We need some things done before the protocol can start.

Mental Poker - Requirements

We need some things done before the protocol can start.

- a public-key/private-key key pair each
- Joe generates 52 messages $M_1, M_2, \ldots, M_{52}$
- unique random string

Mental Poker - Requirements

We need some things done before the protocol can start.

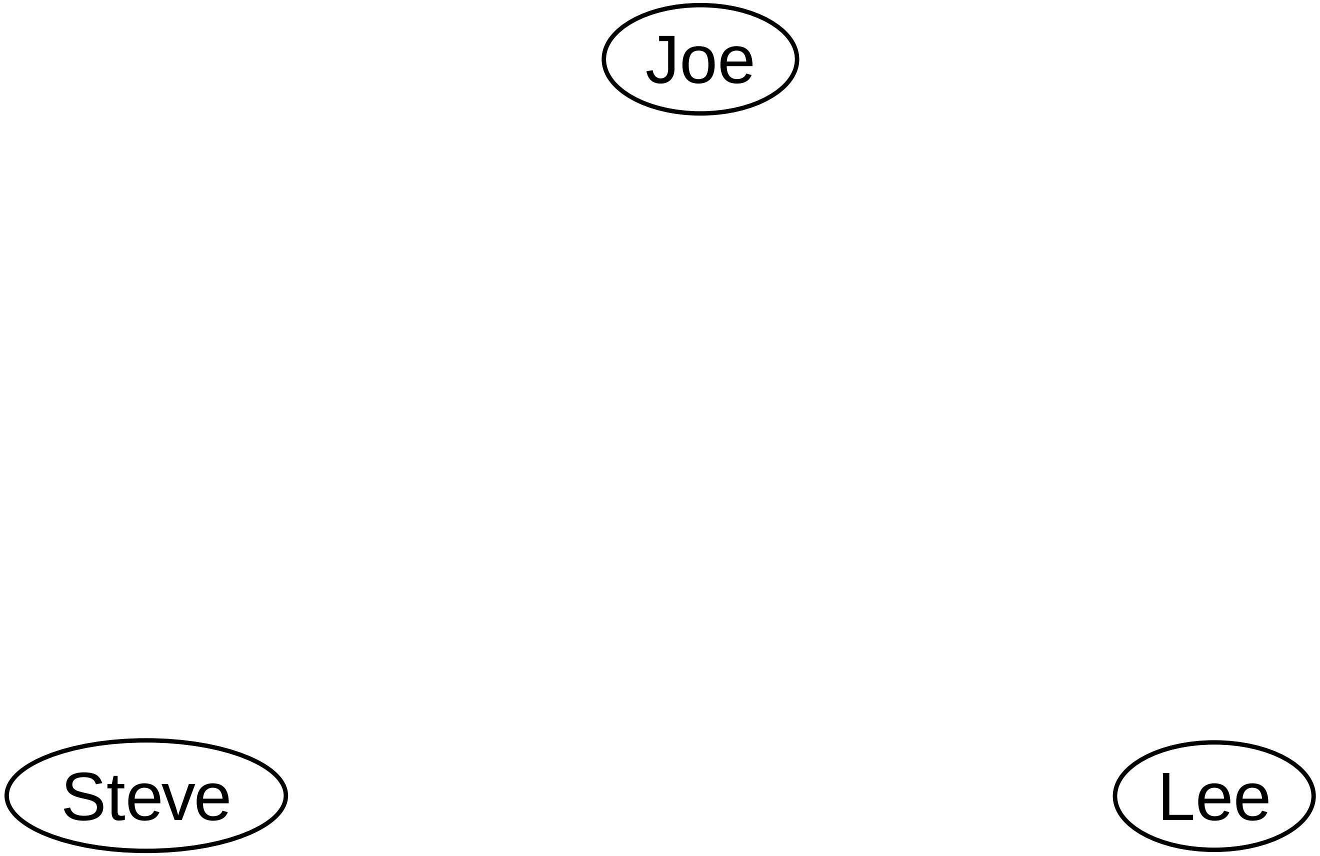
- a public-key/private-key key pair each
- Joe generates 52 messages $M_1, M_2, \ldots, M_{52}$
- unique random string
- $E_J(M_i) :=$ 'M_i encrypted with Joes public-key'
- $D_S(X) :=$ 'X decrypted with Steves private-key'
- cryptographic algorithm commutative, i.e. $D_S(E_L(E_S(X))) = E_L(X)$

Mental Poker - Protocol

Dealing the cards will be the problem here.

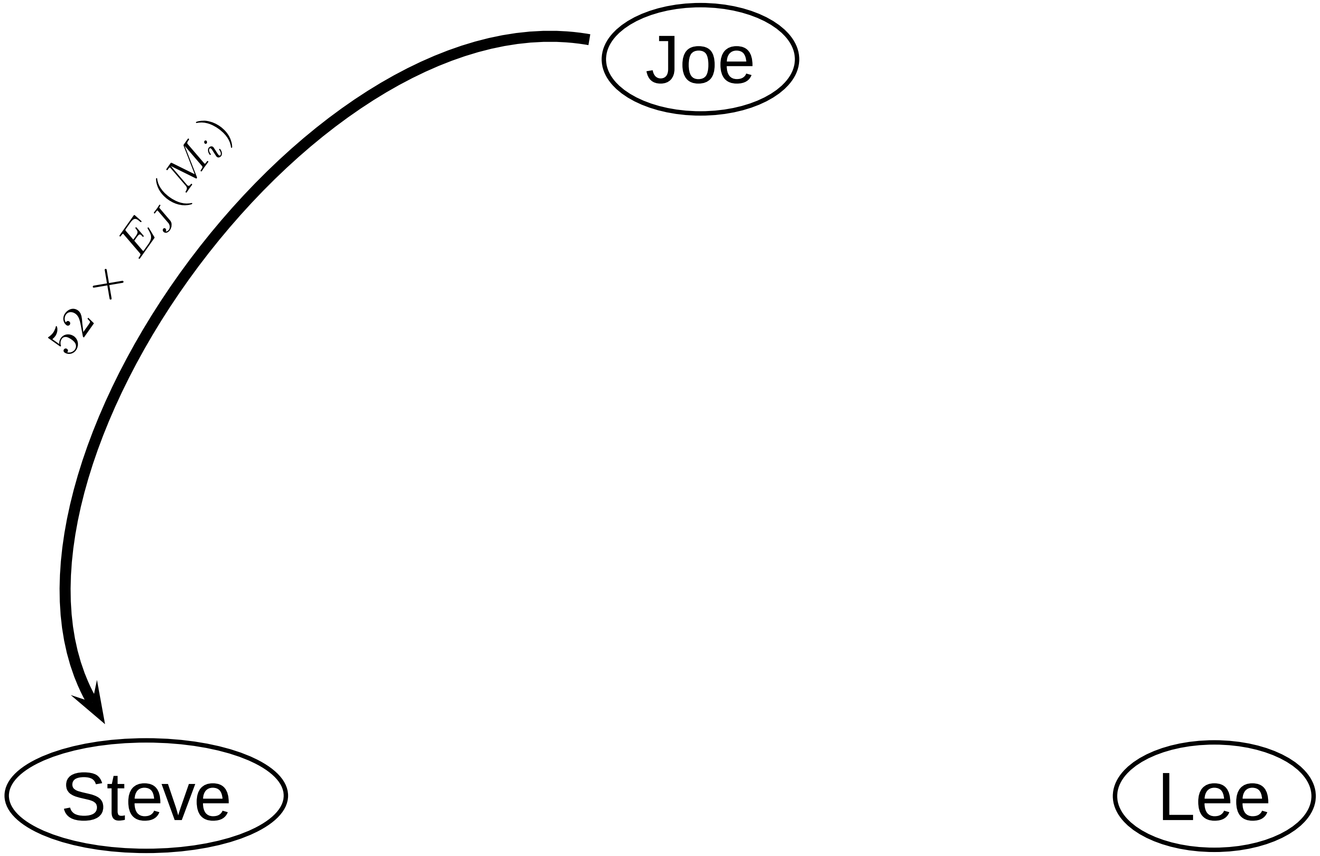
Mental Poker - Protocol

Dealing the cards will be the problem here.



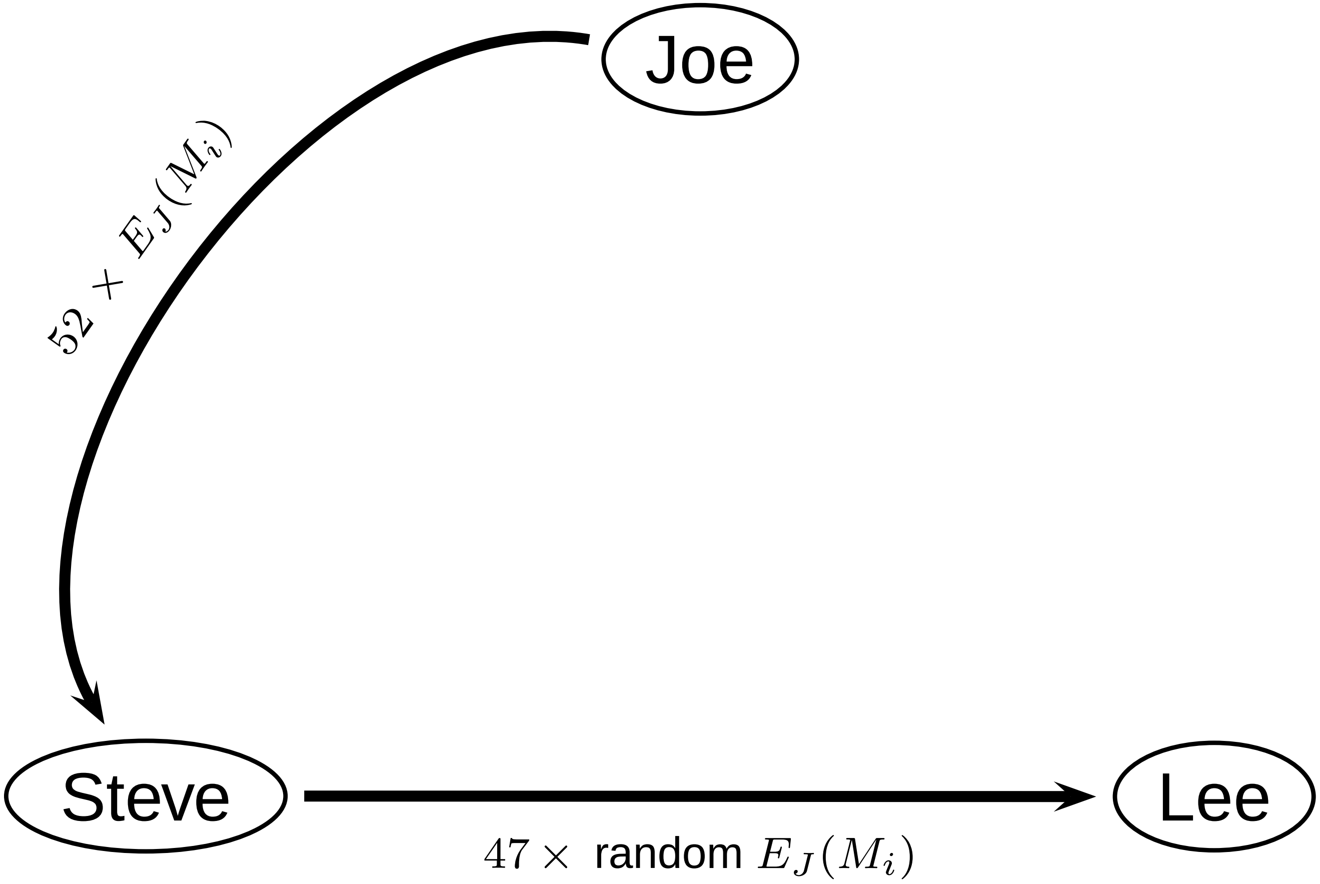
Mental Poker - Protocol

Dealing the cards will be the problem here.



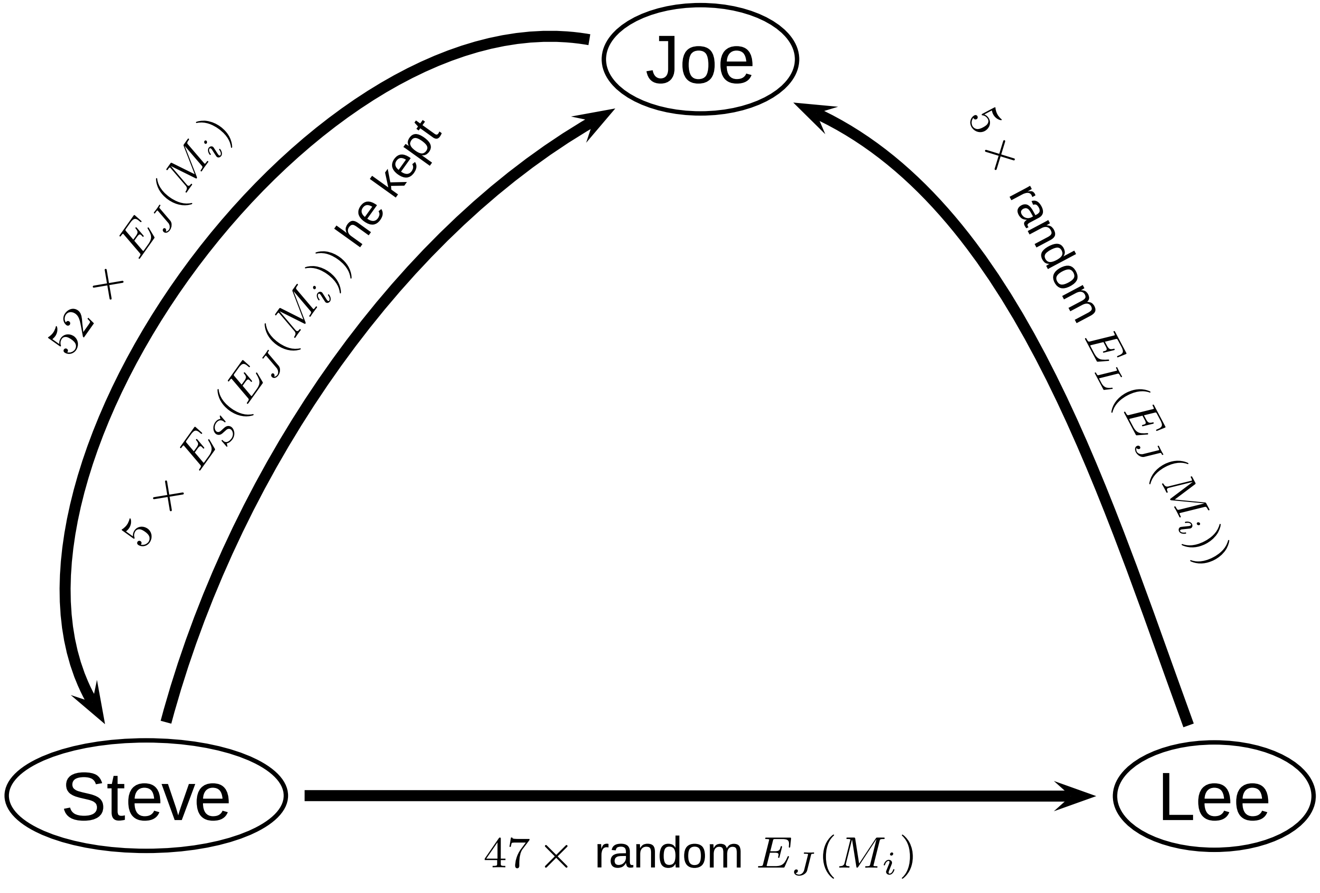
Mental Poker - Protocol

Dealing the cards will be the problem here.



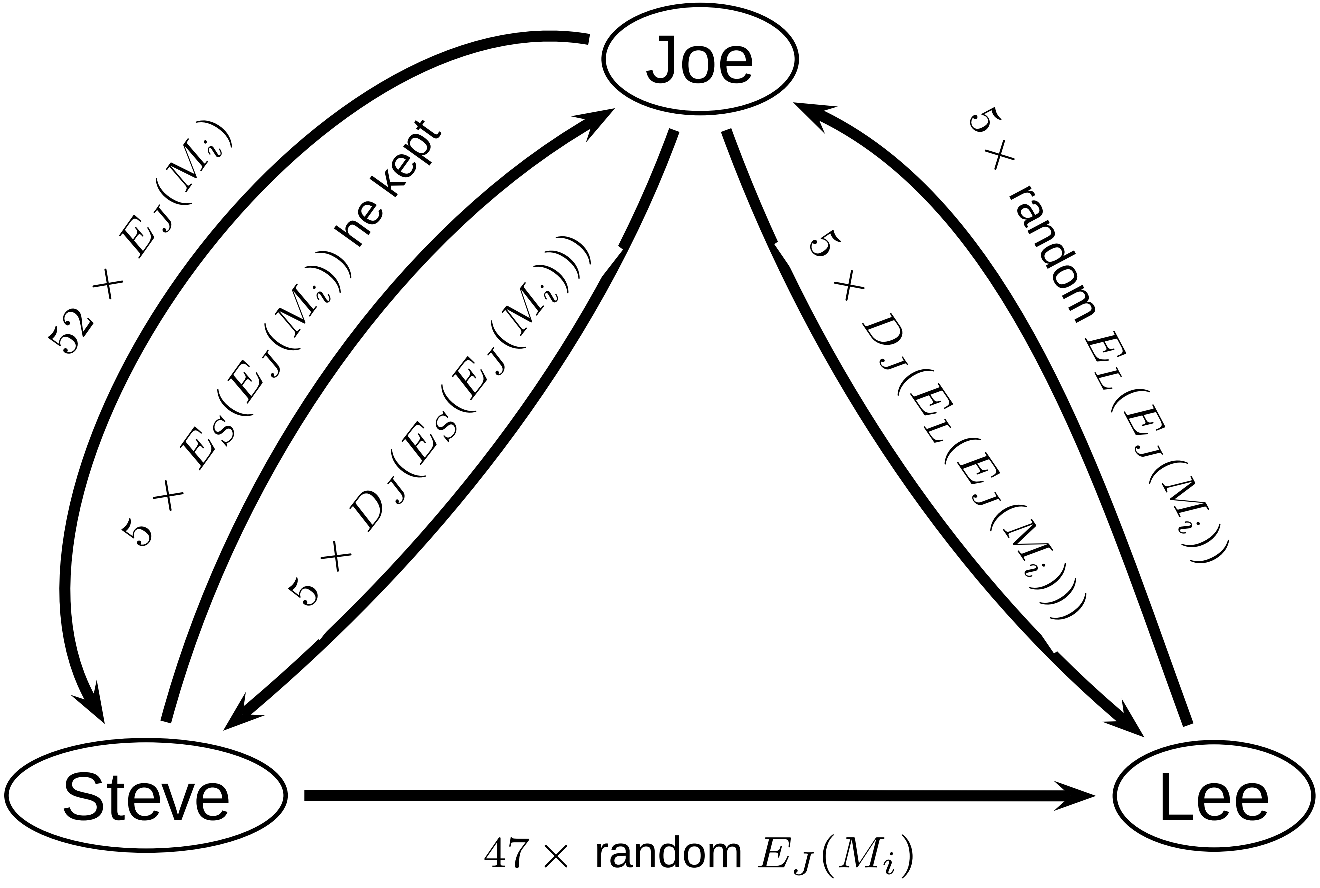
Mental Poker - Protocol

Dealing the cards will be the problem here.



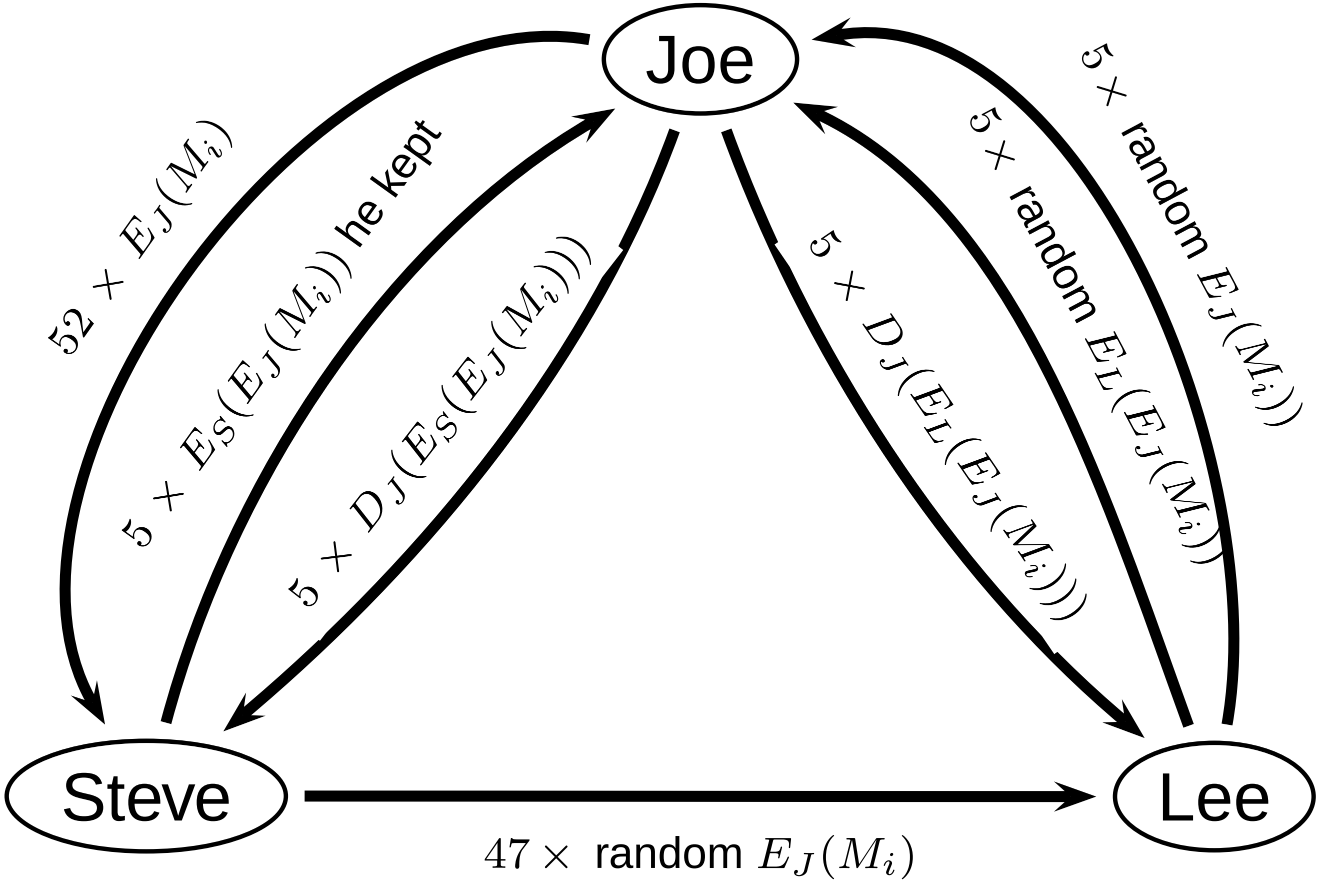
Mental Poker - Protocol

Dealing the cards will be the problem here.



Mental Poker - Protocol

Dealing the cards will be the problem here.



Mental Poker - Discussion

Mental Poker - Discussion

- additional cards
- everyone reveals his hand and keys after the game
- desired: only winner reveals his hand, but this is not secure
- implementation is not effective

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.
Since proving $P \neq NP$ sounds like magic Joe is convinced that he can do other tricks too. So he summons his friend David and claims: 'I can guess what dish you will choose in cafeteria, before you choose it!'.

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.
Since proving $P \neq NP$ sounds like magic Joe is convinced that he can do other tricks too. So he summons his friend David and claims: 'I can guess what dish you will choose in cafeteria, before you choose it!'.
Joe writes down his prediction and puts it in an envelope and seals it shut.

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.
Since proving $P \neq NP$ sounds like magic Joe is convinced that he can do other tricks too. So he summons his friend David and claims: 'I can guess what dish you will choose in cafeteria, before you choose it!'.
Joe writes down his prediction and puts it in an envelope and seals it shut.
They go to the cafeteria and David chooses 'Pasta with mushroom sauce'. Although this seems to be a very unlikely choice, look what happens, when they both open the envelope: The prediction says...

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.
Since proving $P \neq NP$ sounds like magic Joe is convinced that he can do other tricks too. So he summons his friend David and claims: 'I can guess what dish you will choose in cafeteria, before you choose it!'.
Joe writes down his prediction and puts it in an envelope and seals it shut.
They go to the cafeteria and David chooses 'Pasta with mushroom sauce'. Although this seems to be a very unlikely choice, look what happens, when they both open the envelope: The prediction says...

'Rice with vegetables'

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.
Since proving $P \neq NP$ sounds like magic Joe is convinced that he can do other tricks too. So he summons his friend David and claims: 'I can guess what dish you will choose in cafeteria, before you choose it!'.
Joe writes down his prediction and puts it in an envelope and seals it shut.
They go to the cafeteria and David chooses 'Pasta with mushroom sauce'. Although this seems to be a very unlikely choice, look what happens, when they both open the envelope: The prediction says...

'Rice with vegetables'

What's that? Ok, maybe proving $P \neq NP$ *and* doing fancy magic is to much for one week.

Story - Part III

Poker has become boring after a while and so Joe seeks a new distraction.
Since proving $P \neq NP$ sounds like magic Joe is convinced that he can do other tricks too. So he summons his friend David and claims: ’I can guess what dish you will choose in cafeteria, before you choose it!’.
Joe writes down his prediction and puts it in an envelope and seals it shut.
They go to the cafeteria and David chooses ’Pasta with mushroom sauce’. Although this seems to be a very unlikely choice, look what happens, when they both open the envelope: The prediction says...

’Rice with vegetables’

What’s that? Ok, maybe proving $P \neq NP$ *and* doing fancy magic is to much for one week.

’Maybe next week I should try this with Lee from Tokyo?’

Bit Commitment - Protocol

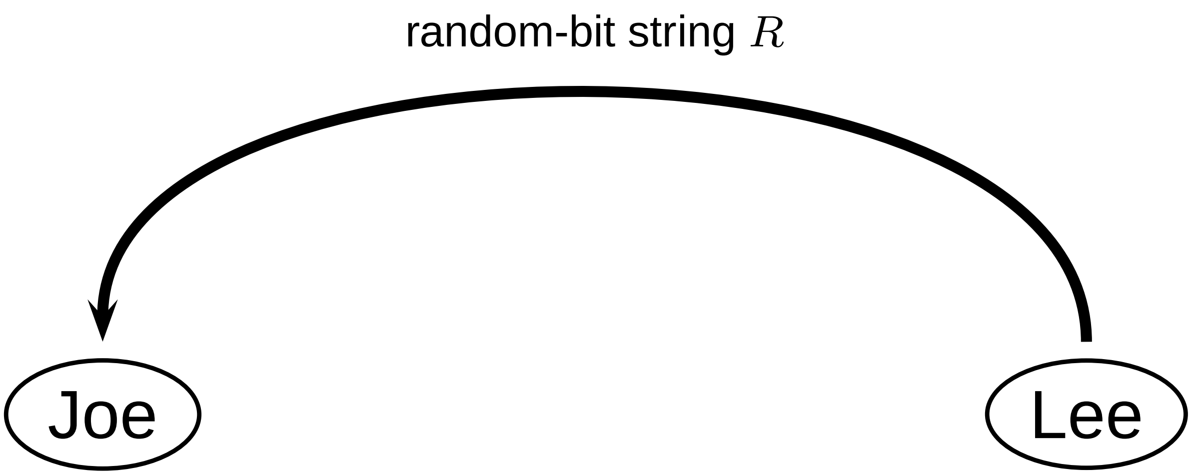
Joe wants to commit to a prediction b (i.e. a bit) but does not want to reveal is until sometime later. Joe holds some random key K.

Bit Commitment - Protocol

Joe wants to commit to a prediction b (i.e. a bit) but does not want to reveal is until sometime later. Joe holds some random key K.

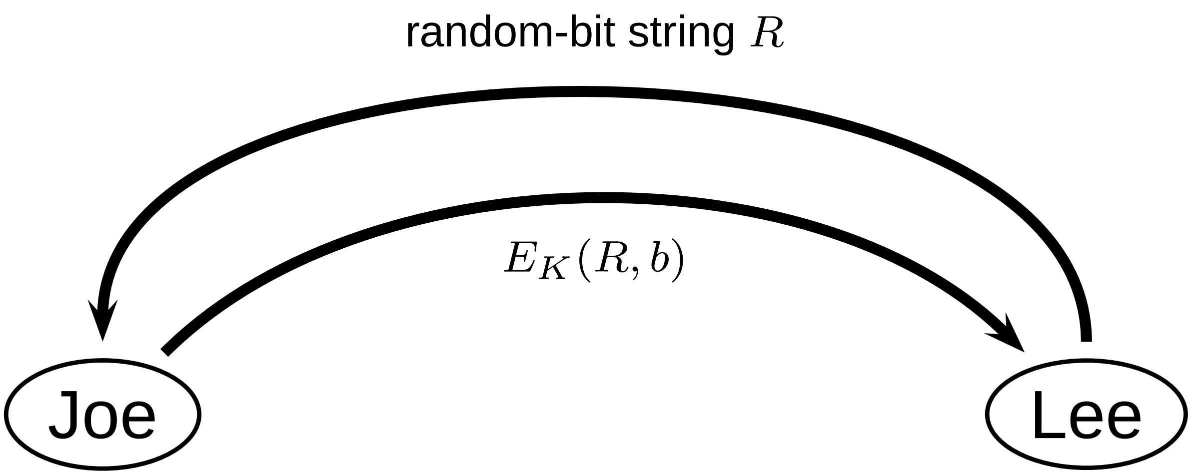
Bit Commitment - Protocol

Joe wants to commit to a prediction b (i.e. a bit) but does not want to reveal is until sometime later. Joe holds some random key K.



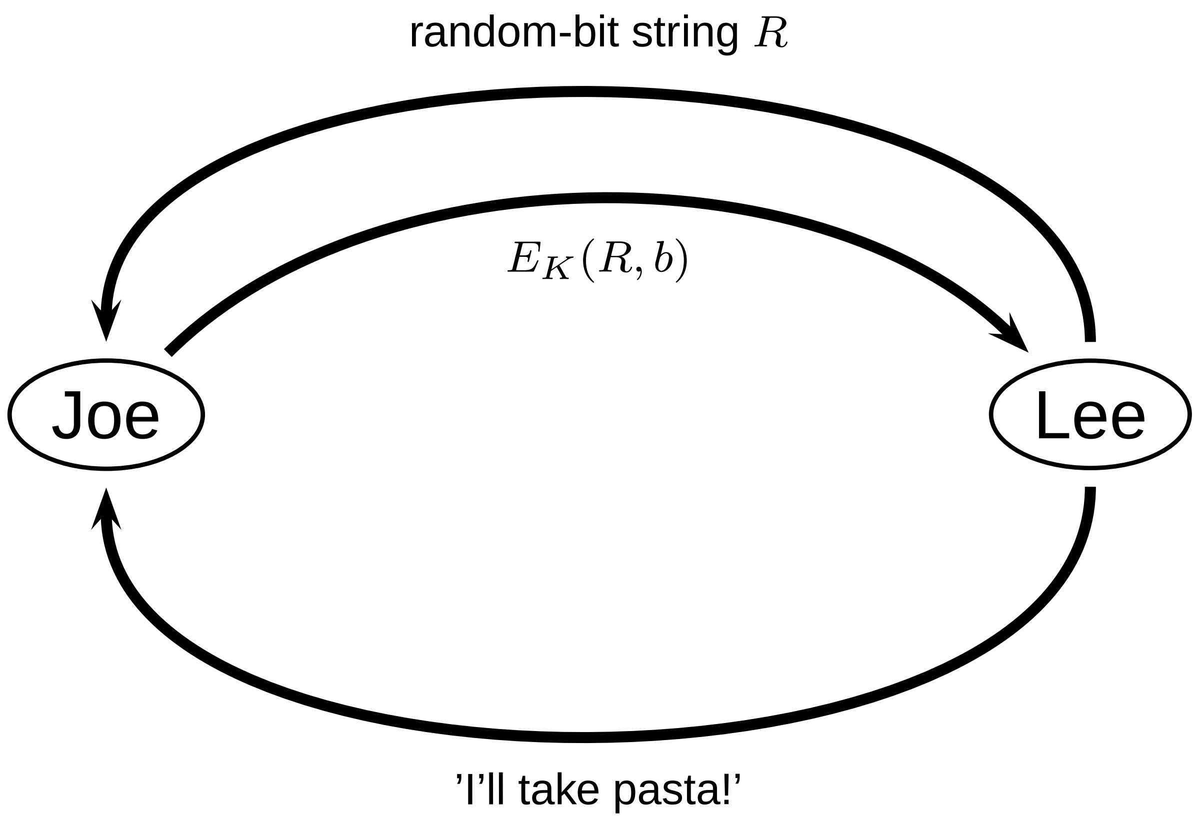
Bit Commitment - Protocol

Joe wants to commit to a prediction b (i.e. a bit) but does not want to reveal is until sometime later. Joe holds some random key K.



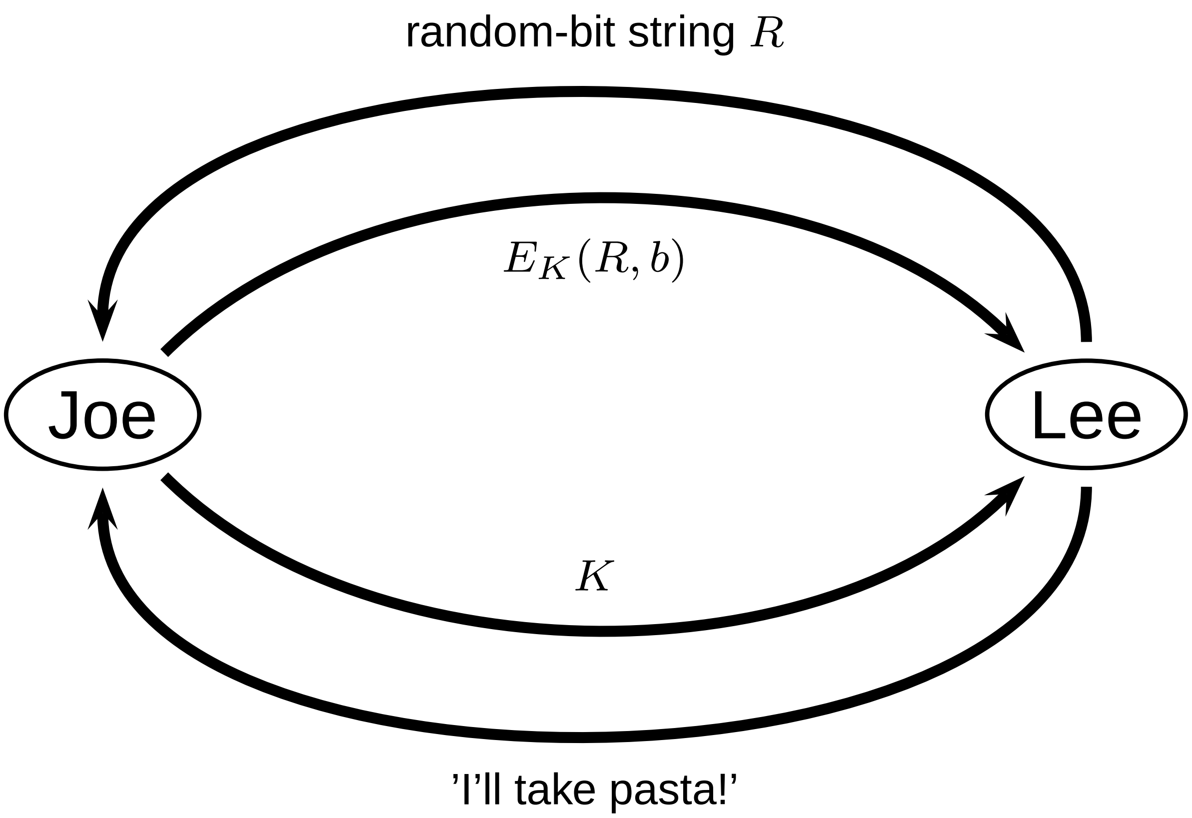
Bit Commitment - Protocol

Joe wants to commit to a prediction b (i.e. a bit) but does not want to reveal is until sometime later. Joe holds some random key K.



Bit Commitment - Protocol

Joe wants to commit to a prediction b (i.e. a bit) but does not want to reveal is until sometime later. Joe holds some random key K.



Bit Commitment - Discussion

Bit Commitment - Discussion

- random-bit string is important
- impossible to cheat
- several other protocols for this task
- e.g. involving one-way functions or pseudo-random-sequence generators

Story - Part IV

Lee has to do some work on approximation algorithms, so he suggests that Joe should call Steve and ask him about his new game.

Story - Part IV

Lee has to do some work on approximation algorithms, so he suggests that Joe should call Steve and ask him about his new game.

Joe does exactly this and Steve proposes following game.

Story - Part IV

Lee has to do some work on approximation algorithms, so he suggests that Joe should call Steve and ask him about his new game.

Joe does exactly this and Steve proposes following game.

Steve:'Let's flip coins. If the result is heads you loose. If its tails I win.'

Story - Part IV

Lee has to do some work on approximation algorithms, so he suggests that Joe should call Steve and ask him about his new game.
Joe does exactly this and Steve proposes following game.
Steve:'Let's flip coins. If the result is heads you loose. If its tails I win.'
Joe:'Hmm something is amiss here. Why do we not flip coins just for the fun of it?'

Story - Part IV

Lee has to do some work on approximation algorithms, so he suggests that Joe should call Steve and ask him about his new game.

Joe does exactly this and Steve proposes following game.

Steve:'Let's flip coins. If the result is heads you loose. If its tails I win.'

Joe:'Hmm something is amiss here. Why do we not flip coins just for the fun of it?'

Steve:'Ok, I will show you how.'

Coin Flipping - Protocol

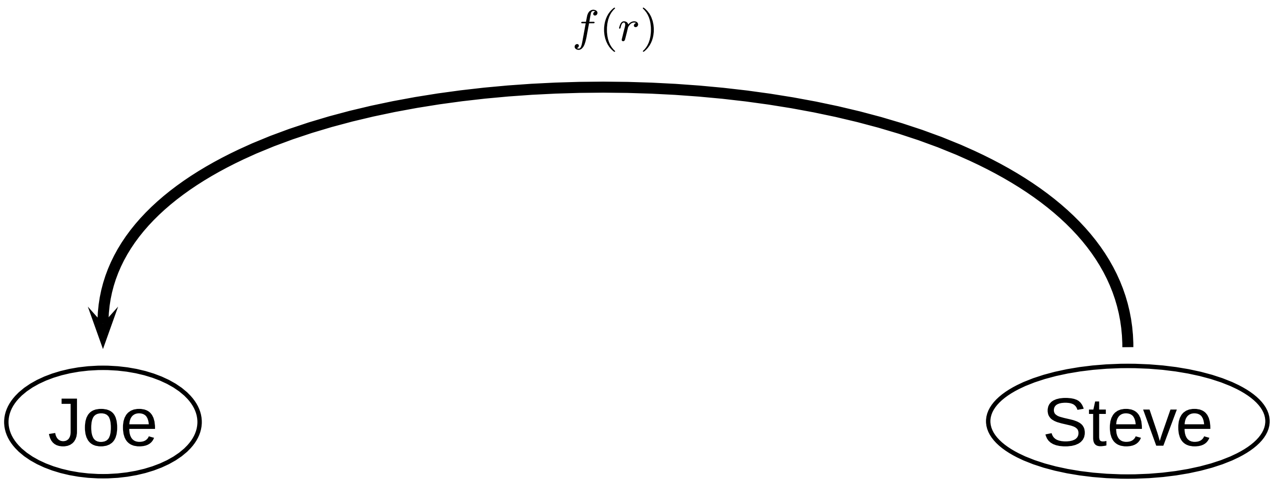
Steve explains following protocol, which uses a one-way function f. Steve chooses a random number r

Coin Flipping - Protocol

Steve explains following protocol, which uses a one-way function f. Steve chooses a random number r

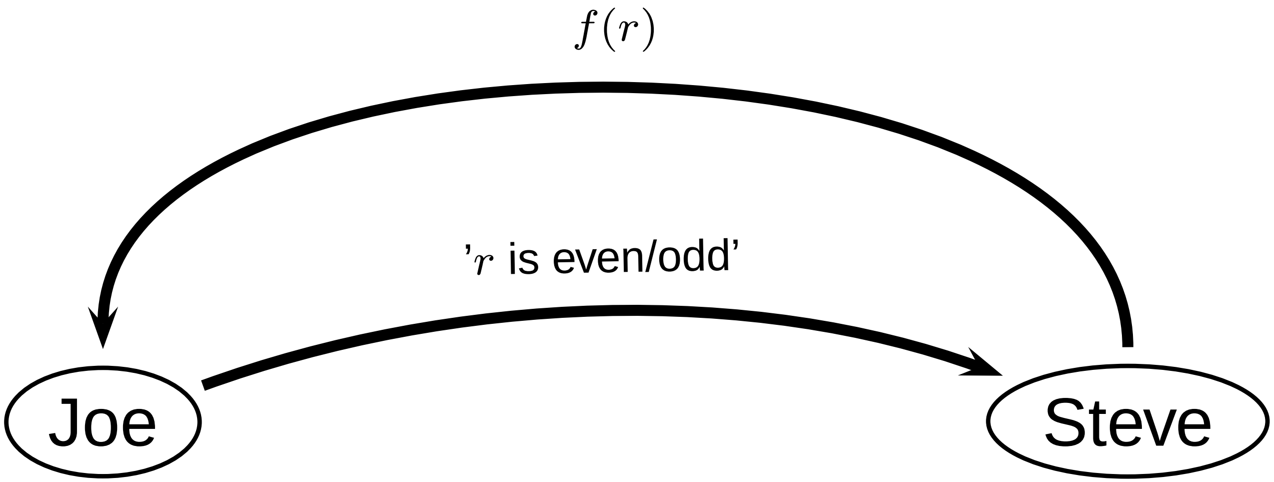
Coin Flipping - Protocol

Steve explains following protocol, which uses a one-way function f. Steve chooses a random number r



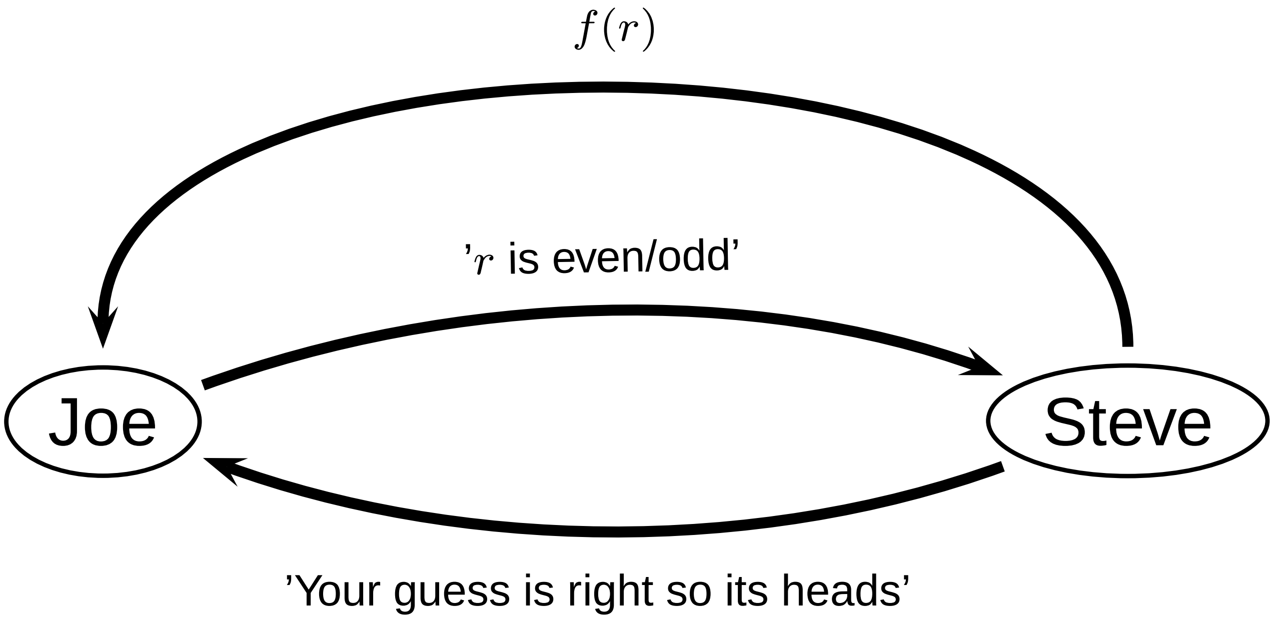
Coin Flipping - Protocol

Steve explains following protocol, which uses a one-way function f. Steve chooses a random number r



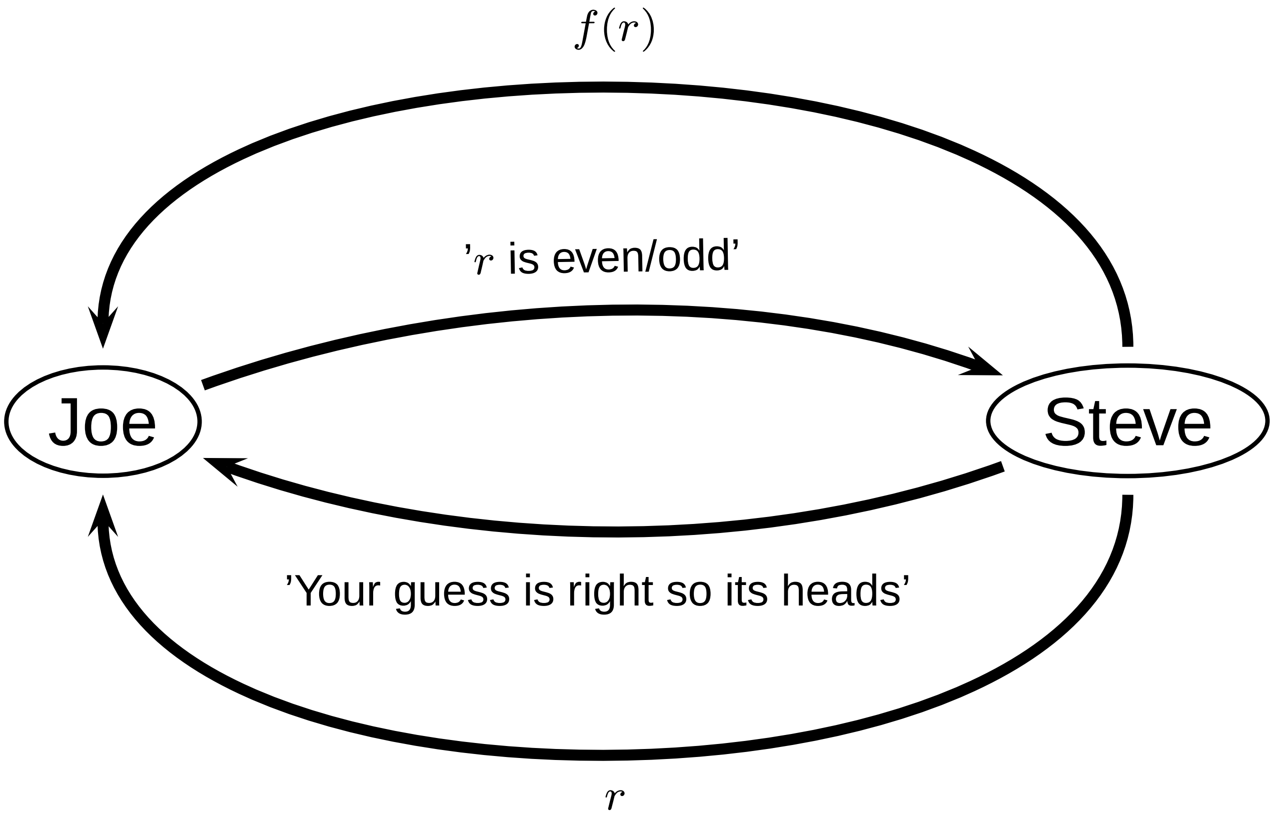
Coin Flipping - Protocol

Steve explains following protocol, which uses a one-way function f. Steve chooses a random number r



Coin Flipping - Protocol

Steve explains following protocol, which uses a one-way function f. Steve chooses a random number r



Coin Flipping - Discussion

Coin Flipping - Discussion

- security rests in one-way function
- least significant bit of $f(x)$ and x must be uncorrelated
- use some other bit
- several other protocols exist

Story - Part V

While doing some coin flips with Steve Joe receives an e-mail from Anja.

Story - Part V

While doing some coin flips with Steve Joe receives an e-mail from Anja.

Hi Joe!
I heard you wrote a paper on $P \neq NP$. I'd love to write something about it in the 'Computer Science Weekly'.
I'd pay you if you would give me a copy before you publish it.
Call me a.s.a.p.
Bye, Anja

Story - Part V

While doing some coin flips with Steve Joe receives an e-mail from Anja.

Hi Joe!
I heard you wrote a paper on $P \neq NP$. I'd love to write something about it in the 'Computer Science Weekly'.
I'd pay you if you would give me a copy before you publish it.
Call me a.s.a.p.
Bye, Anja

When Joe calls Anja, he discovers that she can only pay half of what he wants. So he suggests:

Story - Part V

While doing some coin flips with Steve Joe receives an e-mail from Anja.

Hi Joe!
I heard you wrote a paper on $P \neq NP$. I'd love to write something about it in the 'Computer Science Weekly'.
I'd pay you if you would give me a copy before you publish it.
Call me a.s.a.p.
Bye, Anja

When Joe calls Anja, he discovers that she can only pay half of what he wants. So he suggests:
'I'll give you half the pages for half the price. You will get a good impression of my work and I get the money it is worth.

Story - Part V

While doing some coin flips with Steve Joe receives an e-mail from Anja.

Hi Joe!
I heard you wrote a paper on $P \neq NP$. I'd love to write something about it in the 'Computer Science Weekly'.
I'd pay you if you would give me a copy before you publish it.
Call me a.s.a.p.
Bye, Anja

When Joe calls Anja, he discovers that she can only pay half of what he wants. So he suggests:
'I'll give you half the pages for half the price. You will get a good impression of my work and I get the money it is worth.

Anja:'Ok, but I want to choose the pages, so you don't send me the boring ones.'

Oblivious Transfer - Requirements

Oblivious Transfer - Requirements

- Anja will receive only half of the pages
- Joe will not know which pages Anja receives
- Here: Joe sends Anja one of two messages M_1, M_2
- Joe generates two public-key/private-key pairs K_1, K_2
- Anja chooses a key K_A in a symmetric algorithm (e.g. DES)

Oblivious Transfer - Protocol

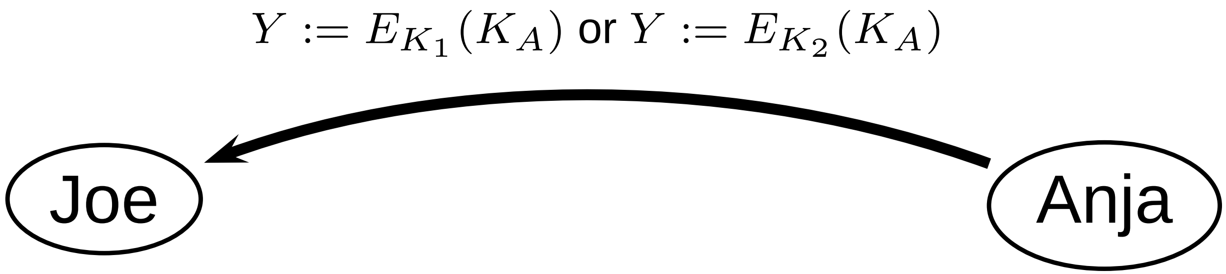
Joe's public keys are known to Anja.

Oblivious Transfer - Protocol

Joe's public keys are known to Anja.

Oblivious Transfer - Protocol

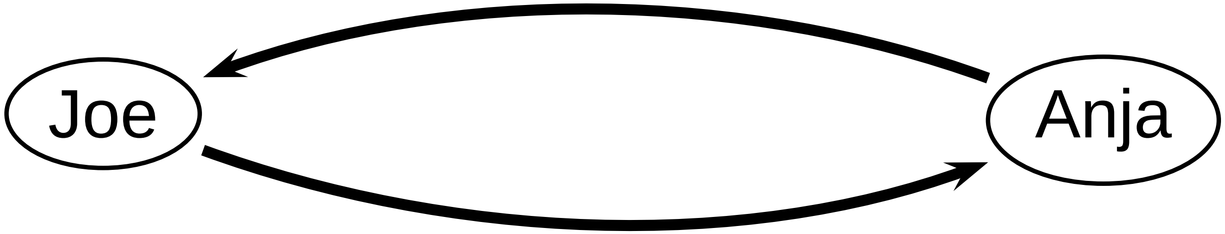
Joe's public keys are known to Anja.



Oblivious Transfer - Protocol

Joe's public keys are known to Anja.

$Y := E_{K_1}(K_A)$ or $Y := E_{K_2}(K_A)$



$E_{D_{K_1}(Y)}(M_1)$ and $E_{D_{K_2}(Y)}(M_2)$

Oblivious Transfer - Discussion

Oblivious Transfer - Discussion

- one message is gibberish
- other is plain
- Joe may encrypt two identical messages
- reveal Joes private-key later
- protocol is strange but useful

Story - Part VI

From selling half of his paper Joe gained even more money than he already has from poker games and advance pay.

Story - Part VI

From selling half of his paper Joe gained even more money than he already has from poker games and advance pay.
He is not fond of carrying so much money around in cash, so he decides to deposit it at a bank of his confidence.

Story - Part VI

From selling half of his paper Joe gained even more money than he already has from poker games and advance pay.
He is not fond of carrying so much money around in cash, so he decides to deposit it at a bank of his confidence.
Since he is a computer crack he immediately accepts, when the clerk asks him to take part in an experiment with digital cash.

Story - Part VI

From selling half of his paper Joe gained even more money than he already has from poker games and advance pay.
He is not fond of carrying so much money around in cash, so he decides to deposit it at a bank of his confidence.
Since he is a computer crack he immediately accepts, when the clerk asks him to take part in an experiment with digital cash.
Reto the bank clerk first explains to Joe, what a blind signature is.

Blind Signatures - Requirements

Blind Signatures - Requirements

- Reto shall sign a document without knowing the content
- in real-life: envelope and carbon paper
- signature function S commutes with an encryption E i.e. $D(S(E(m))) = S(m)$
- RSA and one-time pads

Blind Signature - Protocol

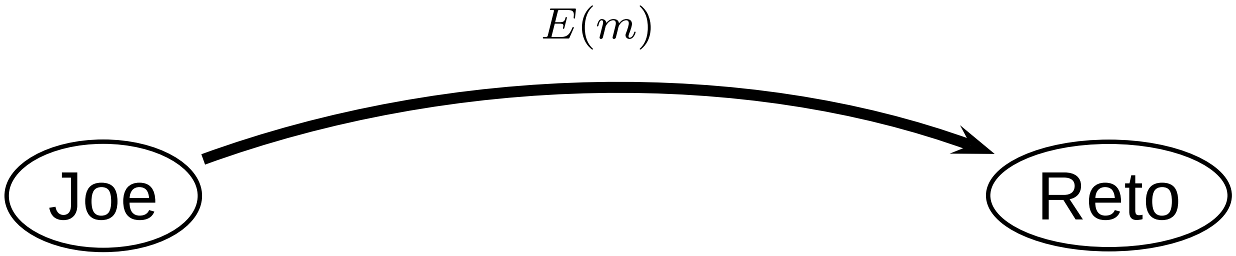
With the signature commuting with the encryption the protocol is quite easy.

Blind Signature - Protocol

With the signature commuting with the encryption the protocol is quite easy.

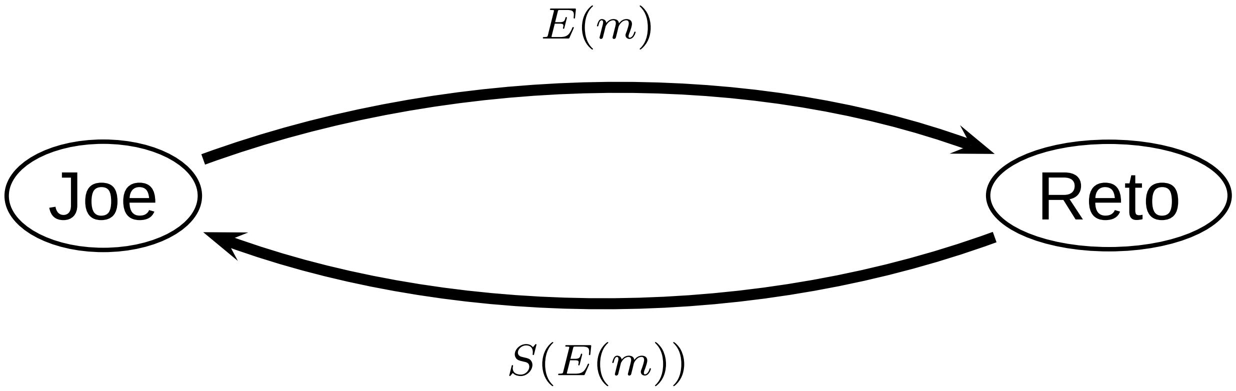
Blind Signature - Protocol

With the signature commuting with the encryption the protocol is quite easy.



Blind Signature - Protocol

With the signature commuting with the encryption the protocol is quite easy.



Blind Signature - Discussion

Blind Signature - Discussion

- when Joe decrypts he gets the signed message
- Reto can not know which document he signed
- Reto can even get the signed document
- Reto signs many documents
- 'Reto owes Joe $ 1.000.000'

Story - Part VII

Joe immediately senses a new possibility of making money.

Story - Part VII

Joe immediately senses a new possibility of making money.
He urges Reto to go on quickly, but Reto refuses. He wants Joe to understand the problems involved with digital money.

Story - Part VII

Joe immediately senses a new possibility of making money.
He urges Reto to go on quickly, but Reto refuses. He wants Joe to understand the problems involved with digital money.
'I will first tell you what is important about digital money.'

Digital Cash - Requirements

Digital Cash - Requirements

- forgery has to be prevented or detected
- duplication has to be prevented or detected
- customers’ anonymity has to be preserved
- no audit trails
- efficiency

Blind Signature enhanced

We want to prevent Joe from cheating.

Blind Signature enhanced

We want to prevent Joe from cheating.

- present 100 documents to Reto
- Reto opens 99 documents at random
- all 99 documents should have the same content

Digital Cash Protocol # 1

Digital Cash Protocol # 1

- Withdrawal: enhanced Blind Signature protocol (eBSP) with a message similar to this ’Confidence Bank owes the bearer $ 1000’

Digital Cash Protocol # 1

- Withdrawal: enhanced Blind Signature protocol (eBSP) with a message similar to this 'Confidence Bank owes the bearer $ 1000'
- Reto will then deduct $ 1000 from Joes account

Digital Cash Protocol # 1

- Withdrawal: enhanced Blind Signature protocol (eBSP) with a message similar to this ’Confidence Bank owes the bearer $ 1000’
- Reto will then deduct $ 1000 from Joes account
- Payment: verify signature

Digital Cash Protocol # 1

- Withdrawal: enhanced Blind Signature protocol (eBSP) with a message similar to this 'Confidence Bank owes the bearer $ 1000'
- Reto will then deduct $ 1000 from Joes account
- Payment: verify signature
- Deposit: verify signature and then credit $ 1000

DC Protocol # 1 - Discussion

DC Protocol # 1 - Discussion

- anonymity
- no cheating
- ’double spending problem’

Digital Cash Protocol # 2

To solve the double spending problem we alter the protocol as follows.

Digital Cash Protocol # 2

To solve the double spending problem we alter the protocol as follows.

- random uniqueness string for each money order

Digital Cash Protocol # 2

To solve the double spending problem we alter the protocol as follows.

- random uniqueness string for each money order
- during the eBSP verify that all uniqeness strings are different

Digital Cash Protocol # 2

To solve the double spending problem we alter the protocol as follows.

- random uniqueness string for each money order
- during the eBSP verify that all uniqeness strings are different
- string should be long enough

Digital Cash Protocol # 2

To solve the double spending problem we alter the protocol as follows.

- random uniqueness string for each money order
- during the eBSP verify that all uniqeness strings are different
- string should be long enough
- Deposit: verify uniqueness string has not been used already

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

- Withdrawal: same as before

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

- Withdrawal: same as before
- Payment: additional random identity string

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

- Withdrawal: same as before
- Payment: additional random identity string
- Deposit: verify uniqueness string and identity string

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

- Withdrawal: same as before
- Payment: additional random identity string
- Deposit: verify uniqueness string and identity string
  - if both have not been used before everything is ok

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

- Withdrawal: same as before
- Payment: additional random identity string
- Deposit: verify uniqueness string and identity string
  - if both have not been used before everything is ok
  - uniqueness string in the database but different identity string then Joe cheated

Digital Cash Protocol # 3

Protocol # 2 does prevent cheating but does not identify the cheater. So we will alter the protocol some more.

- Withdrawal: same as before
- Payment: additional random identity string
- Deposit: verify uniqueness string and identity string
  - if both have not been used before everything is ok
  - uniqueness string in the database but different identity string then Joe cheated
  - uniqueness and identity string in the database then the merchant cheated

Money Order

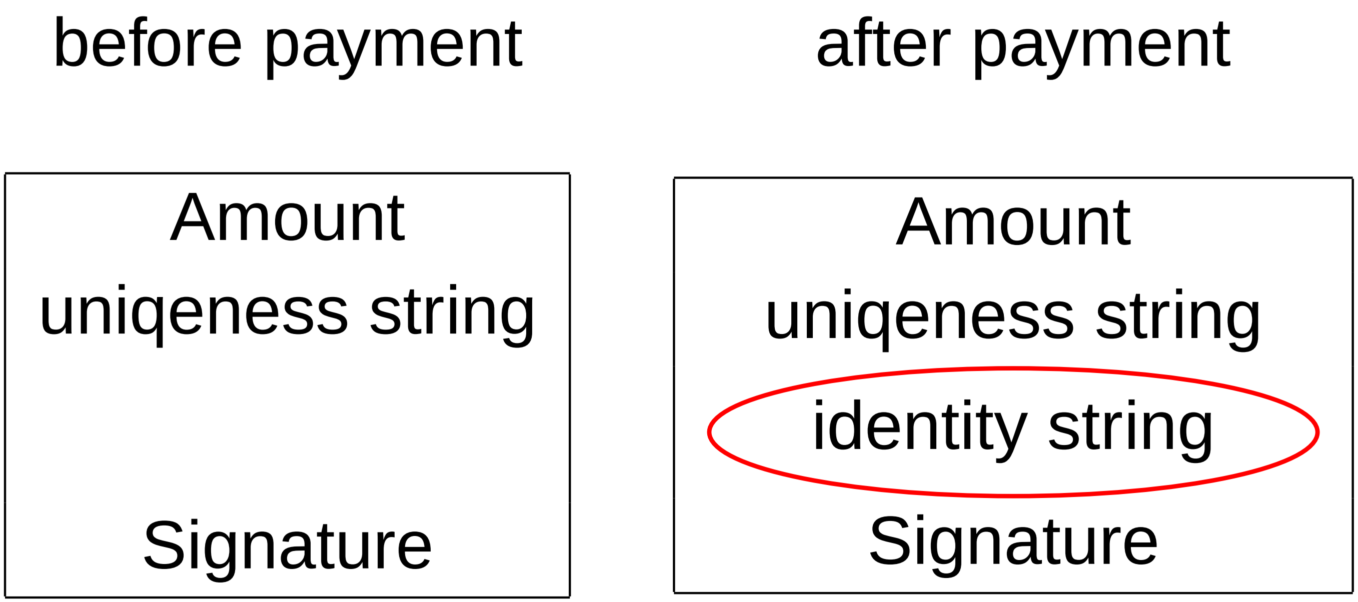
Money Order

before payment

Amount
uniqeness string

Signature

Money Order



before payment
Amount
uniqeness string
Signature
after payment
Amount
uniqeness string
identity string
Signature

DCP # 4 Money Order Creation

We now want to discover who cheated, when the merchant is honest.

DCP # 4 Money Order Creation

We now want to discover who cheated, when the merchant is honest.

- n pairs of identity bit strings generated as follows
- an identity string stating Joes name, address, etc.
- split this into two pieces using a 'secret splitting protocol'
- commit to each piece (bit-commitment)
- any pair reveals Joes identity when opened (e.g. I_{23_L} and I_{23_R} but not I_{23_L} and I_{42_R})

Money Order - After Withdrawal

Money Order - After Withdrawal

after withdrawal

Amount
uniqeness string
I_{1_L} I_{1_R}
I_{2_L} I_{2_R}
I_{3_L} I_{3_R}
$\vdots$ $\vdots$
I_{n_L} I_{n_R}
Signature

DCP # 4 Withdrawal and Payment

DCP # 4 Withdrawal and Payment

- Withdrawal: Reto verifies that all 99 messages are well formed
  - amount
  - uniqueness string
  - all identity strings

DCP # 4 Withdrawal and Payment

- Withdrawal: Reto verifies that all 99 messages are well formed
  - amount
  - uniqueness string
  - all identity strings
- Payment: merchant will give Joe a random n-bit selector string b
- Joe will open either the left or right half, depending on b
- the random identity string is not used anymore

Money Order - identity strings

Money Order - identity strings

before payment

Amount
uniqeness string
I_{1_L} $\quad$ I_{1_R}
I_{2_L} $\quad$ I_{2_R}
I_{3_L} $\quad$ I_{3_R}
$\vdots$ $\quad$ $\vdots$
I_{n_L} $\quad$ I_{n_R}
Signature

Money Order - identity strings

before payment	after payment
Amount	Amount
uniqeness string	uniqeness string
I_{1_L} I_{1_R}	I_{1_L} I_{1_R}
I_{2_L} I_{2_R}	I_{2_L} I_{2_R}
I_{3_L} I_{3_R}	I_{3_L} I_{3_R}
$\vdots$ $\vdots$	$\vdots$ $\vdots$
I_{n_L} I_{n_R}	I_{n_L} I_{n_R}
Signature	Signature

DCP # 4 - Deposit

DCP # 4 - Deposit

- Deposit: Reto will check signature and uniqueness string
  - if uniqueness string is not used yet, record it and all the identity information
  - if the money is double spent, compare identity information
  - if they are identically the merchant has cheated
  - if not identity information is revealed

Digital Cash - Summary

Digital Cash - Summary

- forgery is prevented by eBSP
- duplication is detected with uniqueness string
- customers' anonymity is preserved, as long as he does not cheat
- no audit trails exist, as long as the customer does not cheat
- efficiency

Story - Part VIII

Since Joe has now fully understand digital cash and the protocol, he will probably withdraw his first $ 1000 bill tomorrow.

Story - Part VIII

Since Joe has now fully understand digital cash and the protocol, he will probably withdraw his first $ 1000 bill tomorrow.
Maybe he will get it timestamped to prove that he was the first to enjoy this cool innovation.

Story - Part VIII

Since Joe has now fully understand digital cash and the protocol, he will probably withdraw his first $ 1000 bill tomorrow.
Maybe he will get it timestamped to prove that he was the first to enjoy this cool innovation.
More likely he will spend it in some poker game or loose it trying to forecast the outcome of his next coin flip with Steve.

Story - Part VIII

Since Joe has now fully understand digital cash and the protocol, he will probably withdraw his first $ 1000 bill tomorrow.

Maybe he will get it timestamped to prove that he was the first to enjoy this cool innovation.

More likely he will spend it in some poker game or loose it trying to forecast the outcome of his next coin flip with Steve.

Maybe he will instead give half of the money to Anja or ask Lee to sign some dubious document.

Story - Part VIII

Since Joe has now fully understand digital cash and the protocol, he will probably withdraw his first \$ 1000 bill tomorrow.
Maybe he will get it timestamped to prove that he was the first to enjoy this cool innovation.
More likely he will spend it in some poker game or loose it trying to forecast the outcome of his next coin flip with Steve.
Maybe he will instead give half of the money to Anja or ask Lee to sign some dubious document.
If Joes proof of $P \neq NP$ really holds you may read in the next volume of 'Computer Science Weekly'

The End

That's it.

(Just kidding)

The End

Thank you for your attention.