# Privacy-Preserving Trust Management Mechanisms from Private Matching Schemes

**Oriol Farràs**
Josep Domingo-Ferrer
Alberto Blanco-Justicia

Universitat Rovira i Virgili, Tarragona, Catalonia

Data Privacy Management 2013

# Overview

- Trust Management mechanism.

# Overview

- Trust Management mechanism.
- Trust among parties is established by means of the exchange of credentials.

# Overview

- Trust Management mechanism.
- Trust among parties is established by means of the exchange of credentials.
- Mechanism for choosing the credentials to be exchanged...

# Overview

- Trust Management mechanism.
- Trust among parties is established by means of the exchange of credentials.
- Mechanism for choosing the credentials to be exchanged...
- ... preserving the privacy of the parties.

# Overview

- Trust Management mechanism.
- Trust among parties is established by means of the exchange of credentials.
- Mechanism for choosing the credentials to be exchanged...
- ... preserving the privacy of the parties.
- Based on a cryptographic primitive: a secure two-party computation protocol for the set intersection,

# Program

1. Motivation
2. Trust Management
3. Privacy-Preserving Trust Management
4. Our Solution
5. Conclusions

1. Motivation
2. Trust Management
3. Privacy-Preserving Trust Management
4. Our Solution
5. Conclusions

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions
- Medical information

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions
- Medical information
- ...

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions
- Medical information
- ...

These interactions are easy to carry out face to face in a specific context...

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions
- Medical information
- ...

These interactions are easy to carry out face to face in a specific context... but they are challenging on the Internet, where personal identification is not obvious.

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions
- Medical information
- ...

These interactions are easy to carry out face to face in a specific context... but they are challenging on the Internet, where personal identification is not obvious.

Cryptography provides tools to guarantee secure communication and to avoid malicious agents.

# Information Exchange

There are many situations in which we need to exchange sensitive information:

- Credit card payment
- Asking for directions
- Medical information
- ...

These interactions are easy to carry out face to face in a specific context... but they are challenging on the Internet, where personal identification is not obvious.

Cryptography provides tools to guarantee secure communication and to avoid malicious agents.

But it is not always enough...

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn’t purchase on their phone more often. (GPR’13)

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn't purchase on their phone more often. (GPR'13)
- 33% not at all comfortable sharing personal information in an App. (GPR'13)

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn't purchase on their phone more often. (GPR'13)
- 33% not at all comfortable sharing personal information in an App. (GPR'13)
- 43% claim that have been asked for more personal information than necessary. (Eurobarometer)

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn't purchase on their phone more often. (GPR'13)
- 33% not at all comfortable sharing personal information in an App. (GPR'13)
- 43% claim that have been asked for more personal information than necessary. (Eurobarometer)
- Majority is concerned about the behavior being recorded.

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn't purchase on their phone more often. (GPR'13)
- 33% not at all comfortable sharing personal information in an App. (GPR'13)
- 43% claim that have been asked for more personal information than necessary. (Eurobarometer)
- Majority is concerned about the behavior being recorded.
- ...

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn't purchase on their phone more often. (GPR'13)
- 33% not at all comfortable sharing personal information in an App. (GPR'13)
- 43% claim that have been asked for more personal information than necessary. (Eurobarometer)
- Majority is concerned about the behavior being recorded.
- ...

There is need of designing methods to establish trust among parties.

# Need of Trust

Cryptography is not always enough.
Consumers ask for more than security:

- 35% of consumers cite a lack of trust as the reason why they didn't purchase on their phone more often. (GPR'13)
- 33% not at all comfortable sharing personal information in an App. (GPR'13)
- 43% claim that have been asked for more personal information than necessary. (Eurobarometer)
- Majority is concerned about the behavior being recorded.
- ...

There is need of designing methods to establish trust among parties.

We need new access control systems in which trust is built.
A solution is to exchange credentials that contain attributes of the parties.

1. Motivation
2. Trust Management
3. Privacy-Preserving Trust Management
4. Our Solution
5. Conclusions

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

Automatic Trust Negotiation schemes (Winslett, Winsborough et al.): t.m.s. in which the trust is built by means of credentials. Credentials are disclosed sequentially, according to access control policies determined by the parties.

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

Automatic Trust Negotiation schemes (Winslett, Winsborough et al.): t.m.s. in which the trust is built by means of credentials. Credentials are disclosed sequentially, according to access control policies determined by the parties.

- TrustBuilder (Lee et al.)

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

Automatic Trust Negotiation schemes (Winslett, Winsborough et al.): t.m.s. in which the trust is built by means of credentials. Credentials are disclosed sequentially, according to access control policies determined by the parties.

- TrustBuilder (Lee et al.)
- Trust-*X* (Squicciarini et al.)

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

Automatic Trust Negotiation schemes (Winslett, Winsborough et al.): t.m.s. in which the trust is built by means of credentials. Credentials are disclosed sequentially, according to access control policies determined by the parties.

- TrustBuilder (Lee et al.)
- Trust-*X* (Squicciarini et al.)
- PeerTrust (Nejdl et al.)

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

Automatic Trust Negotiation schemes (Winslett, Winsborough et al.): t.m.s. in which the trust is built by means of credentials. Credentials are disclosed sequentially, according to access control policies determined by the parties.

- TrustBuilder (Lee et al.)
- Trust-*X* (Squicciarini et al.)
- PeerTrust (Nejdl et al.)
- Xena (Haidar et al.)

# Trust Management Schemes

Trust management schemes: seek the trust among strangers.
Early proposals to establish trust:

- To sign a Service Level Agreement
- Transport Layer Security and Secure Sockets Layers

Automatic Trust Negotiation schemes (Winslett, Winsborough et al.): t.m.s. in which the trust is built by means of credentials. Credentials are disclosed sequentially, according to access control policies determined by the parties.

- TrustBuilder (Lee et al.)
- Trust-*X* (Squicciarini et al.)
- PeerTrust (Nejdl et al.)
- Xena (Haidar et al.)
- Traust (Lee et al.)

# Trust Management Schemes

Trust management and trust negotiation schemes are used as building block of commercial frameworks.

# Trust Management Schemes

Trust management and trust negotiation schemes are used as building block of commercial frameworks.

The project Interoperable Trust Assurance Infrastructure (Inter-Trust) has a trust negotiation module.

# Trust Management Schemes

Trust management and trust negotiation schemes are used as building block of commercial frameworks.

The project Interoperable Trust Assurance Infrastructure (Inter-Trust) has a trust negotiation module.

- Framework for trustworthy applications

# Trust Management Schemes

Trust management and trust negotiation schemes are used as building block of commercial frameworks.

The project Interoperable Trust Assurance Infrastructure (Inter-Trust) has a trust negotiation module.

- Framework for trustworthy applications
- heterogeneous networks and devices

# Trust Management Schemes

Trust management and trust negotiation schemes are used as building block of commercial frameworks.

The project Interoperable Trust Assurance Infrastructure (Inter-Trust) has a trust negotiation module.

- Framework for trustworthy applications
- heterogeneous networks and devices
- looks for agreements on the security policies

# Trust Management Schemes

Trust management and trust negotiation schemes are used as building block of commercial frameworks.

The project Interoperable Trust Assurance Infrastructure (Inter-Trust) has a trust negotiation module.

- Framework for trustworthy applications
- heterogeneous networks and devices
- looks for agreements on the security policies

# Inter-Trust

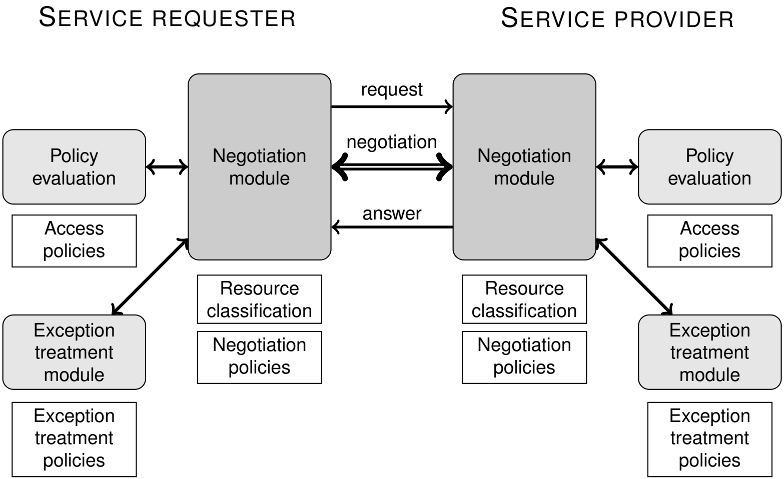

Figure : Negotiation module of Inter-Trust

1. Motivation
2. Trust Management
3. Privacy-Preserving Trust Management
4. Our Solution
5. Conclusions

# The Privacy Problem

- A client C wants to access a service from S.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

The privacy of C and S should not be compromised.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

The privacy of C and S should not be compromised.

The credentials must be appropriate.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

The privacy of C and S should not be compromised.

The credentials must be appropriate.

Moreover:

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

The privacy of C and S should not be compromised.

The credentials must be appropriate.

Moreover:

- C does not want to provide information on his credentials.
  unless those credentials are essential for the transaction.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

The privacy of C and S should not be compromised.

The credentials must be appropriate.

Moreover:

- C does not want to provide information on his credentials.
  unless those credentials are essential for the transaction.
- S is reluctant to show a full description of his access policy.

# The Privacy Problem

- A client C wants to access a service from S.
- C and S exchange credentials.
- If both trust on each other, the service is provided.

The privacy of C and S should not be compromised.

The credentials must be appropriate.

Moreover:

- C does not want to provide information on his credentials.
  unless those credentials are essential for the transaction.
- S is reluctant to show a full description of his access policy.

Each party should learn no information about the access policies or preferences of the other parties beyond what is strictly required for trust establishment.

1. Motivation
2. Trust Management
3. Privacy-Preserving Trust Management
4. Our Solution
5. Conclusions

# Overview

Privacy-preserving mechanism to determine the optimal set of credentials to be disclosed, according to their preferences.
It is an asymmetric solution, for a client-server context.

# Overview

Privacy-preserving mechanism to determine the optimal set of credentials to be disclosed, according to their preferences.
It is an asymmetric solution, for a client-server context.

Based on the private matching scheme of Freedman, Nissim, and Pinkas'04. A secure two-party computation protocols for the set intersection.

# Overview

Privacy-preserving mechanism to determine the optimal set of credentials to be disclosed, according to their preferences.
It is an asymmetric solution, for a client-server context.

Based on the private matching scheme of Freedman, Nissim, and Pinkas'04. A secure two-party computation protocols for the set intersection.

Uses additive homomorphic encryption (Paillier cryptosystem).

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.
- S introduce a list $B \subseteq X \times Y$ of pairs $(b, c)$ showing his access policies:
  if S receives $b \in X$, he would reveal $c \in Y$ and he would provide the service.

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.
- S introduce a list $B \subseteq X \times Y$ of pairs $(b, c)$ showing his access policies:
  if S receives $b \in X$, he would reveal $c \in Y$ and he would provide the service.

Output:

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.
- S introduce a list $B \subseteq X \times Y$ of pairs $(b, c)$ showing his access policies:
  if S receives $b \in X$, he would reveal $c \in Y$ and he would provide the service.

Output:

- C receives the pairs $(b, c)$ with $b \in A$:
  Acceptable credential combinations to obtain the service.

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.
- S introduce a list $B \subseteq X \times Y$ of pairs $(b, c)$ showing his access policies:
  if S receives $b \in X$, he would reveal $c \in Y$ and he would provide the service.

Output:

- C receives the pairs $(b, c)$ with $b \in A$:
  Acceptable credential combinations to obtain the service.

Privacy:

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.
- S introduce a list $B \subseteq X \times Y$ of pairs $(b, c)$ showing his access policies:
  if S receives $b \in X$, he would reveal $c \in Y$ and he would provide the service.

Output:

- C receives the pairs $(b, c)$ with $b \in A$:
  Acceptable credential combinations to obtain the service.

Privacy:

- S does not learn A

# The Mechanism

$X$: domain of combinations of credentials of C,
$X = \{$VISA+ >65 Card, Driving License+Unemployed Card, Student Card+Library Card,... $\}$
$Y$: domain of combinations of credentials credentials of S.
$Y = \{$ISOx, Membership credential+VISA certificate, ... $\}$
Inputs:

- C introduce a list with his combinations of credentials $A \subseteq X$ he could show.
- S introduce a list $B \subseteq X \times Y$ of pairs $(b, c)$ showing his access policies:
  if S receives $b \in X$, he would reveal $c \in Y$ and he would provide the service.

Output:

- C receives the pairs $(b, c)$ with $b \in A$:
  Acceptable credential combinations to obtain the service.

Privacy:

- S does not learn A
- C does not learn the pairs $(b, c) \in B$ with $b \notin A$.

# The Mechanism II

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.
- For every $1 \leq j \leq t$, S picks a random element $r_j \in \mathbb{Z}_n$.

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.
- For every $1 \leq j \leq t$, S picks a random element $r_j \in \mathbb{Z}_n$.
- S computes $Enc(r_j \cdot p(b_j))$ and $Enc(b_j || c_j)$ for $1 \leq j \leq t$.

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.
- For every $1 \leq j \leq t$, S picks a random element $r_j \in \mathbb{Z}_n$.
- S computes $Enc(r_j \cdot p(b_j))$ and $Enc(b_j || c_j)$ for $1 \leq j \leq t$.
- S sends $Enc(r_j \cdot p(b_j) + (b_j || c_j))$ to C.

# The Mechanism II

- Let $A = \{a_1, \dots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \dots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \dots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \dots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.
- For every $1 \leq j \leq t$, S picks a random element $r_j \in \mathbb{Z}_n$.
- S computes $Enc(r_j \cdot p(b_j))$ and $Enc(b_j||c_j)$ for $1 \leq j \leq t$.
- S sends $Enc(r_j \cdot p(b_j) + (b_j||c_j))$ to C.

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.
- For every $1 \leq j \leq t$, S picks a random element $r_j \in \mathbb{Z}_n$.
- S computes $Enc(r_j \cdot p(b_j))$ and $Enc(b_j || c_j)$ for $1 \leq j \leq t$.
- S sends $Enc(r_j \cdot p(b_j) + (b_j || c_j))$ to C.

- C decrypts the received messages.

# The Mechanism II

- Let $A = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_n$ be the list of $C$'s credentials.
- C computes the polynomial $p(x) = \prod_{i=1}^{s}(x - a_i)$
- C encrypts $p_0, \ldots, p_s$, the coefficients of $p$
- C sends $Enc(p_0), \ldots, Enc(p_s)$ to $S$

- Let $B = \{(b_1, c_1), \ldots, (b_t, c_t)\} \subseteq \mathbb{Z}_n^2$ be the list of pairs of accepted credentials.
- For every $1 \leq j \leq t$, S picks a random element $r_j \in \mathbb{Z}_n$.
- S computes $Enc(r_j \cdot p(b_j))$ and $Enc(b_j || c_j)$ for $1 \leq j \leq t$.
- S sends $Enc(r_j \cdot p(b_j) + (b_j || c_j))$ to C.

- C decrypts the received messages.
- C obtains a valid pair $(b, c)$ with $b \in A$ or a random number

# The Mechanism III

The protocol is secure in the honest-but-curious model: parties follow the protocol's instructions.

# The Mechanism III

The protocol is secure in the honest-but-curious model: parties follow the protocol's instructions.

The amount of exponentiations needed is $O(s \cdot t)$, and it can be reduced to $O(s + t \ln \ln s)$, where $s = |A|$, $t = |B|$

# The Mechanism III

The protocol is secure in the honest-but-curious model: parties follow the protocol's instructions.

The amount of exponentiations needed is $O(s \cdot t)$, and it can be reduced to $O(s + t \ln \ln s)$, where $s = |A|$, $t = |B|$

More efficient than other proposals:

# The Mechanism III

The protocol is secure in the honest-but-curious model: parties follow the protocol's instructions.

The amount of exponentiations needed is $O(s \cdot t)$, and it can be reduced to $O(s + t \ln \ln s)$, where $s = |A|$, $t = |B|$

More efficient than other proposals:

- Point-Based Trust (Yao et al.): quantitative approach

# The Mechanism III

The protocol is secure in the honest-but-curious model: parties follow the protocol's instructions.

The amount of exponentiations needed is $O(s \cdot t)$, and it can be reduced to $O(s + t \ln \ln s)$, where $s = |A|$, $t = |B|$

More efficient than other proposals:

- Point-Based Trust (Yao et al.): quantitative approach
- Privacy-Reconciliation Protocols (Meyer et al.): the optimal credentials is hard to compute.

1. Motivation
2. Trust Management
3. Privacy-Preserving Trust Management
4. Our Solution
5. Conclusions

# Conclusions and Open Problems

Conclusions

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.
- Secure two-party computation protocol.

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.
- Secure two-party computation protocol.

Open problems:

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.
- Secure two-party computation protocol.

Open problems:

- Find more suitable private matching schemes.

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.
- Secure two-party computation protocol.

Open problems:

- Find more suitable private matching schemes.
- Extend to other adversary models.

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.
- Secure two-party computation protocol.

Open problems:

- Find more suitable private matching schemes.
- Extend to other adversary models.
- Combine with fair exchange mechanisms.

# Conclusions and Open Problems

Conclusions

- Privacy-preserving mechanism for trust management.
- The parties can control of the information revealed about their credentials.
- Secure two-party computation protocol.

Open problems:

- Find more suitable private matching schemes.
- Extend to other adversary models.
- Combine with fair exchange mechanisms.
- Integration into general frameworks.

# THANK YOU