Chapter 43

Privacy-Enhancing Technologies
sender a
message 01001000
key with b + 10101010
key with c + 11100011
transmission 00000001

sender b
message 00000000
key with a + 10101010
key with c + 00111010
transmission 10010000

sender c
message 00000000
key with a + 11100011
key with b + 00111010
transmission 11011001

broadcast

01001000

f43-01-9780123943972
The diagram shows a process labeled "mix" with numbered steps and variables. The steps are:

1. Filter duplicates
2. Delay messages
3. Recode messages
4. Reorder messages

The variables are:

- $f(x)$
- $x < y$

The diagram illustrates the flow of data through these steps.
A person sends a message $m$ to $S$. The message $m$ is encrypted twice: first with $e_1$ to get $r_1, A_2, enc_{e_2}(r_2, R, enc_{e_R}(m))$, then with $e_2$ to get $r_2, R, enc_{e_R}(m)$. These encrypted messages are sent to $Mix_{A_1}$ and $Mix_{A_2}$, respectively. The message $m$ is also sent to $R$. The encrypted messages are decrypted and the original message $m$ is retrieved.
1. Merchant's Account
   0.0788880778

2. Blinded Note

3. Customer (User)

4. Merchant's Account
   0.078786776

Bank (Debit User's Account: $1)

Bank (Credit Merchant's Account: $1)

Blind Signature

$1 $
User Alice

Issuer (Identity Provider - IdP)

Verifier (Relying Party)

1. Issues credentials

2. Service request

3. Data request

4. (unlinkable) selective disclosure

Advantages:
- Selective Disclosure
- Unlinkability of Transactions (Idemix)
- No Profiling by IdPs or Relying Parties

f43-06-9780123943972
Send Data?

Your data will be sent and used for the following purposes

<table>
<thead>
<tr>
<th>Data attributes</th>
<th>Administration</th>
<th>Contact</th>
<th>Feedback</th>
<th>Marketing</th>
<th>Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name - Certified By:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driver's License [Swedish] - ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inga Vainstein</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit Card - Certified By:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visa Credit Card [My private...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1234 5678 9012 3456</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exp: 2012-01-12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-Mail:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data will be sent to:
- Example.com (Privacy Policy) (store.example.com, contact@example.com)
- Visa (Privacy Policy) (www.visa.com, customersupport@visa.com)

Privacy policy matching results

My current privacy settings: 
- Medium Privacy Settings

Accept mismatch for this transaction only

Cancel  Send