Identifikaciona informacija – Primer

Neka je identifikaciona informacija sledeća:

Marko Marković
E-mail: marko.markovic@viser.edu.rs

Binarni zapis identifikacione informacije (pojednostavljen) neka taj niz bude:

P = 1001010

Generiše se n slučajnih nizova iste dužine kao P:

S1 = 1101010
S2 = 0010100
S3 = 1110011

A	B	XOR
0	0	0
1	1	0
1	0	1
0	1	1

Protokolom za deljenje tajne generišu se druge polovine parova:

R1 = S1 XOR P = 0100000
R2 = S2 XOR P = 1011110
R3 = S3 XOR P = 0111001

Parovi:

R1 i S1
R2 i S2
R3 i S3

mogu otkriti poruku P (identifikacionu informaciju) - dok njihove polovine same ne otkrivaju ništa:

R1 XOR S1 = 1001010 = P
R1 XOR S2 = 0110100 <> P

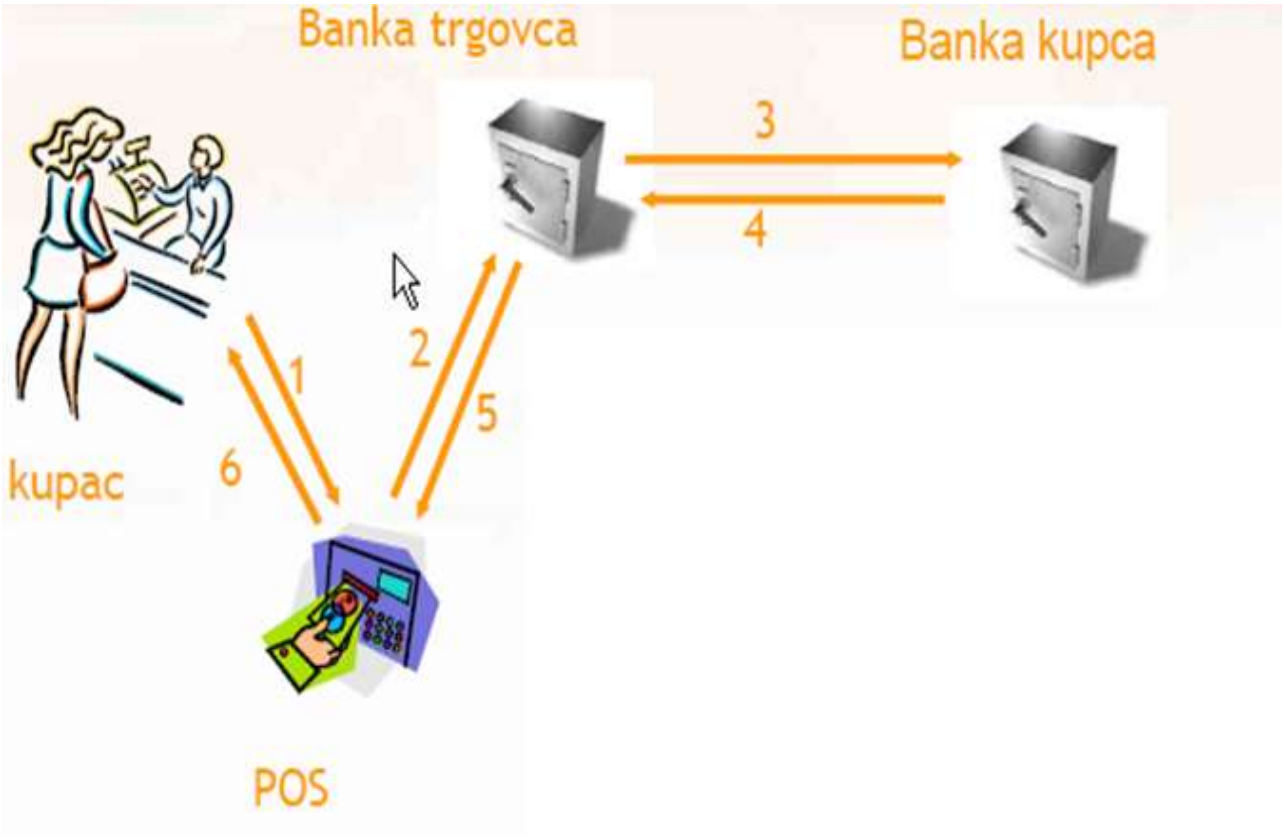
Oblikujemo parove - za hash funkciju uzmimo, radi jednostavnosti, XOR funkciju:

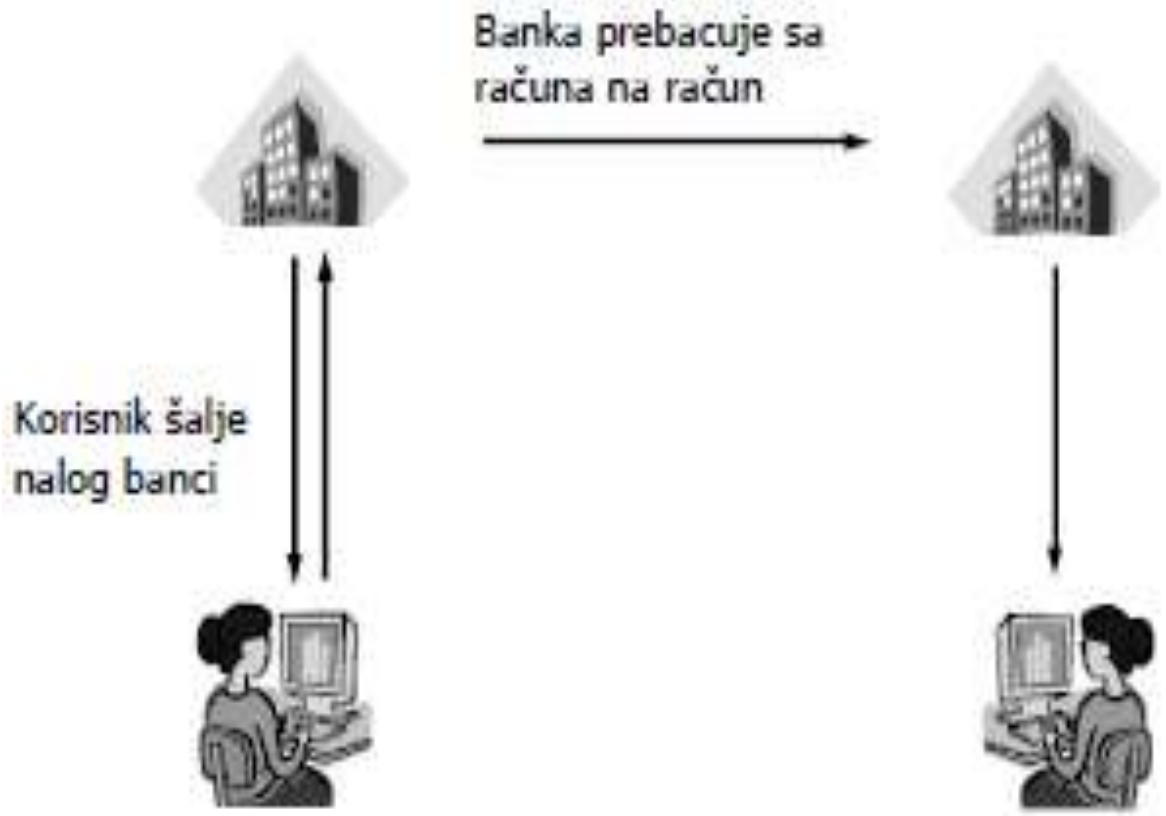
R1 (hash) = XOR (R1) = 0 XOR 1 XOR 0 XOR 0 XOR 0 XOR 0 XOR 0 = 1
S1 (hash) = XOR (S1) = ... = 0
R2 (hash) = XOR (R2) = ... = 1
S2 (hash) = XOR (S2) = ... = 0
R3 (hash) = XOR (R3) = ... = 0
S3 (hash) = XOR (S3) = ... = 1

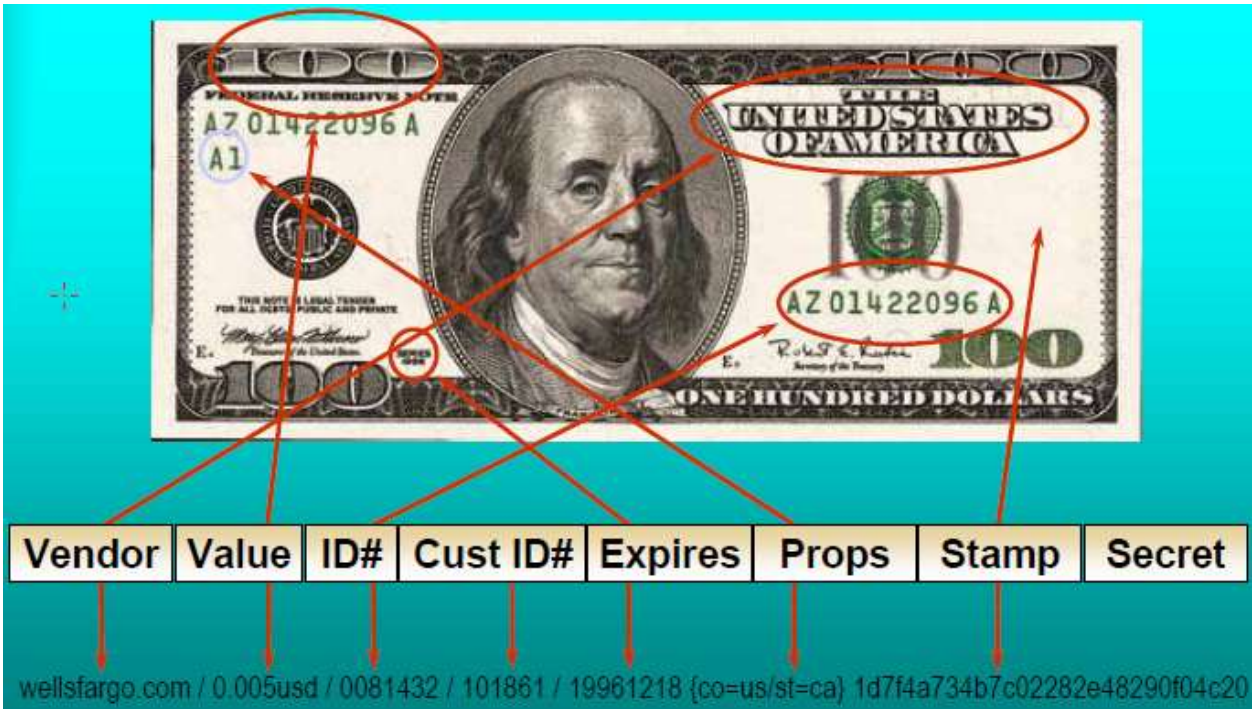
Na novčanicu se zapisuju parovi:

R1 (hash) i S1 (hash)
R2 (hash) i S2 (hash)
R3 (hash) i S3 (hash)


Платите по овом чеку са рачуна бр. 908-20001-18
ДИН.
Словима
Кориснику чека
Који овај чек не може пренети на треће лице
Место и датум издавања чека
Потпис издаваоца чека
Серијски број
Број текућег рачуна
Износ
73308160
200 2603799 35
15Н
Образац бр. 19-ц
По овом пољу не писати и не стављати печате.


Banka trgovca
Banka kupca
3
4
1
2
5
6
kupac
POS


Banka prebacuje sa računa na račun
Korisnik šalje nalog banci


AZ 01422096 A
A1
THE UNITED STATES OF AMERICA
AZ 01422096 A
ONE HUNDRED DOLLARS
Vendor
Value
ID#
Cust ID#
Expires
Props
Stamp
Secret
wellsfargo.com / 0.005usd / 0081432 / 101861 / 19961218 {co=us/st=ca} 1d7f4a734b7c02282e48290f04c20