Electronic Cash

Merlijn Koek

October 22, 2014
What is Electronic Cash?
Desirable security features:

- **Authenticity, unforgeable:** (Unable for anyone to forge money.)
- **Nonrepudiation:** (Unable to deny having performed the transaction.)
- **No double spending**
Desirable practical features:

- Portable
- Recognizable (Widely accepted as being money, or even legal tender.)
- Easily transferable (Without a trusted third party such as a bank)
- Untraceability (Impossible to ‘follow the money’, or establish a link between transactions)
Today’s goal:
Explain fundamental ideas that allow for offline electronic cash schemes, i.e. cash schemes that do not require interaction with the bank during payment.
The scheme in general

Alice withdraws money from the bank and receives a signed coin which contains a serial number and an encryption of the identity of Alice.

Upon payment Alice proves that the encryption of her identity is written on the coin.

For the deposit, the shop sends the coin together with a proof of inclusion of Alice’s identity to the bank.
Three questions arise:

- How can the bank sign the coin without knowing the serial number that is included in the coin?
- How can Alice give a proof of her encrypted identity being included without revealing her identity?
- How to prevent double spending?
‘Textbook’ Blind RSA signatures

- Alice generates a random ‘blinding factor’ $b$ and sends $M' = M \cdot b^e$
- Bank signs $M'$, returning $(M \cdot b^e)^d = M^d \cdot b^{e \cdot d} = M^d \cdot b$
- Alice recovers $M^d$

Result: the bank signed $M$ without knowing what $M$ is, and without Alice knowing the secret signing key $d$. 
Partially blind signatures

- Alice creates \( d \) coins \( C_k = (\text{Serial}_k, \text{Enc}_{r_k}(\text{id}_{Alice})) \)

These contain a serial number and Alice’s encrypted identity. The encryption key \( r_k \) is a secret random number known to Alice belonging to \( C_k \).

- Alice sends for every \( k \leq d \) a blinded coin \( B_k = C_k \cdot b_k^e \) to the bank.

- Then the bank sends Alice a random number \( i \leq d \).

- Alice sends \( r_k \) and the blinding factor \( b_k^e \) for every \( k \neq i \).

The bank checks all those coins, and if those are honest trusts the coin \( C_i \), signs it and returns it to Alice.
Does this satisfy our needs?

With a probability $\frac{1}{d}$, Alice has a chance to create a valid coin that is not honest.

We can fix this by choosing $d$, the amount of coins to be very large, but this is terribly inefficient.
Two questions remain:

▶ How can Alice give a proof of her encrypted identity being included without revealing her identity?
▶ How to prevent double spending?
Payment
When Alice wants to spend the coin, the payee sends her a random challenge number \( c \).

- Alice responds with a value \( x \) such that \((x, c)\) is on the line \( y = id_{Alice} \cdot x + r_k \).

How can the shop check whether this is a correct answer belonging to the coin?
Coin withdrawal: $Enc_{r_k}(id_{Alice})$

- For every coin $C_k$, Alice generates a random $r_k$. This together with $id_{Alice}$ forms the line $y = id_{Alice} \cdot x + r_k$.
- Note that $y = id_{Alice} \cdot x + r_k \iff g^y = g^{id_{Alice} \cdot x + r_k}$

where $g \in \mathbb{Z}_p^*$. 
- Alice computes $s = g^{r_k}$ and $t = g^{id_{Alice}}$.
- Now, $Enc_{r_k}(id_{Alice}) = (s, t)$. 
Double spending

Remember, $s = g^{rk}$ and $t = g^{id_{Alice}}$

The shop can check Alice’s answer without knowing $rk$ or $id_{Alice}$ by checking $g^y = t^x \cdot s \iff g^y = g^{id_{Alice} \cdot x + rk}$

Given two points on the line $y = id_{Alice} \cdot x + r_k$, it is possible to determine both $r_k$ and $id_{Alice}$.

Double spending reveals Alice’s identity!
The scheme in detail

- Alice generates coins $C_k = (\text{Serial}_k, (g^{r_k}, g^{lA}))$ and stores the secret values $r_k$
- Alice generates blinding factors $b_k$ and sends $B_k = C_k \cdot b_k^e$ to the bank
- The bank randomly selects a coin $C_i$ and Alice then provides $b'_k$ and $r'_k$ for all $k' \neq i$.
- The bank checks all these coins and then signs $C_i$
- Alice pays by giving the coin and answering the challenge $c$ by providing an $x$ such that $g^c = g^{lA \cdot x + r_k}$
- The payee deposits the money by giving $C_k$ and $(x, c)$ and the banks checks this serial number for double spending
Thank you.