Blind Signatures and Their Applications

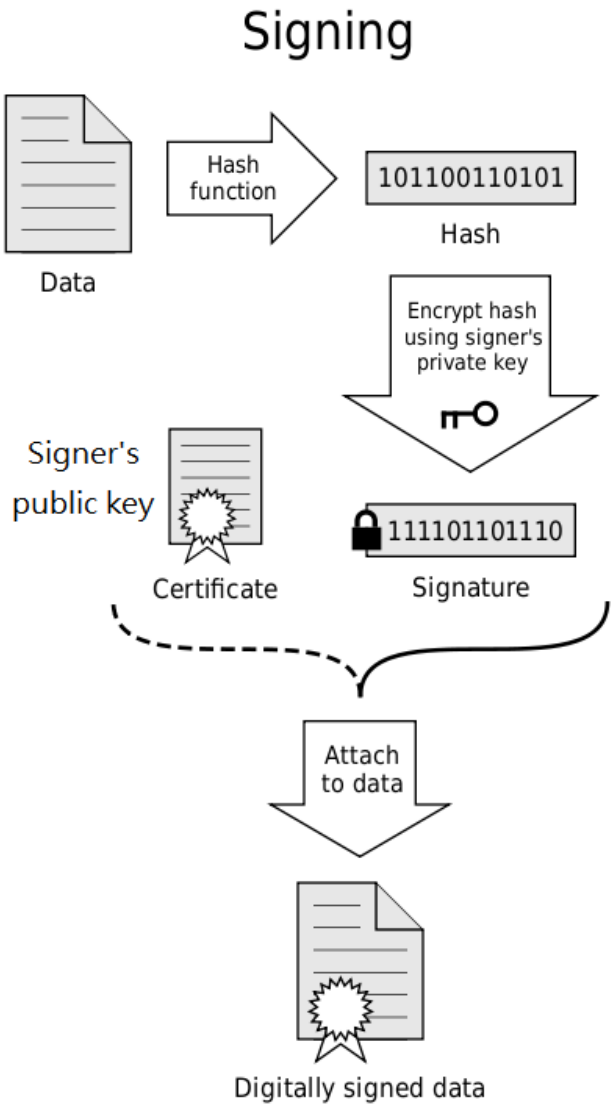
Rong-Jaye Chen

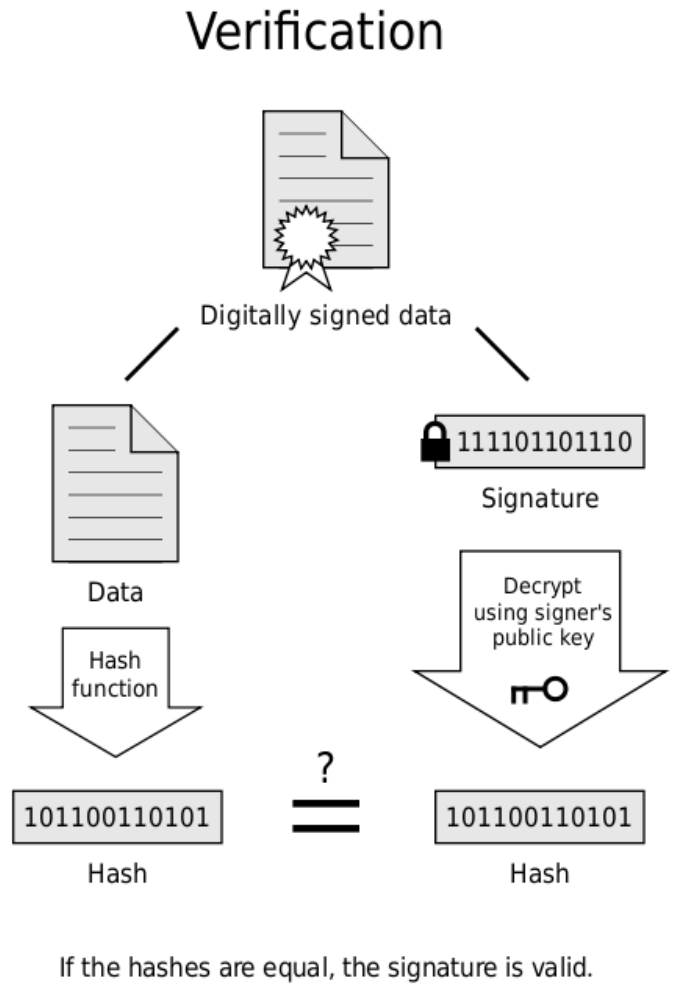
Department of Computer Science, National Chiao Tung University

Crypto 2010

Outline

Digital Signature - (1)





Digital Signature - (2)

- Signing a hash (or message digest) instead of the whole document.

  - **For efficiency:** The signature will be much shorter and thus save time since hashing is generally much faster then signing in practice.
  - **For compatibility:** Messages are typically bit strings, but some signature schemes operate on other domains (such as, in the case of RSA, numbers modulo a composite number N). A hash function can be used to convert an arbitrary input into the proper format.
  - **For integrity:** Without the hash function, the text ”to be signed” may have to be split (separated) in blocks small enough for the signature scheme to act on them directly. However, the receiver of the signed blocks is not able to recognize if all the blocks are present and in the appropriate order.

Digital Signature - (3)

- Uses of digital signatures

  - **Authentication:** Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.
  - **Integrity:** Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. However, if a message is digitally signed, any change in the message after signature will invalidate the signature.
  - **Non-repudiation:** Non-repudiation of origin, is an important aspect of digital signatures. By this property an entity that has signed some information cannot at a later time deny having signed it.

Digital Signature - (4)

- RSA digital signature scheme
  - p and q are primes, and $n = pq$.
  - The public key is e, where $\gcd(e, (p-1)(q-1)) = 1$.
  - The private key is d, where $de \equiv 1 \pmod{(p-1)(q-1)}$.
  - **Signing:** For a message M, the signature of M is $\delta = H(M)^d$.
  - **Verification:** Check if $\delta^e = H(M)$.

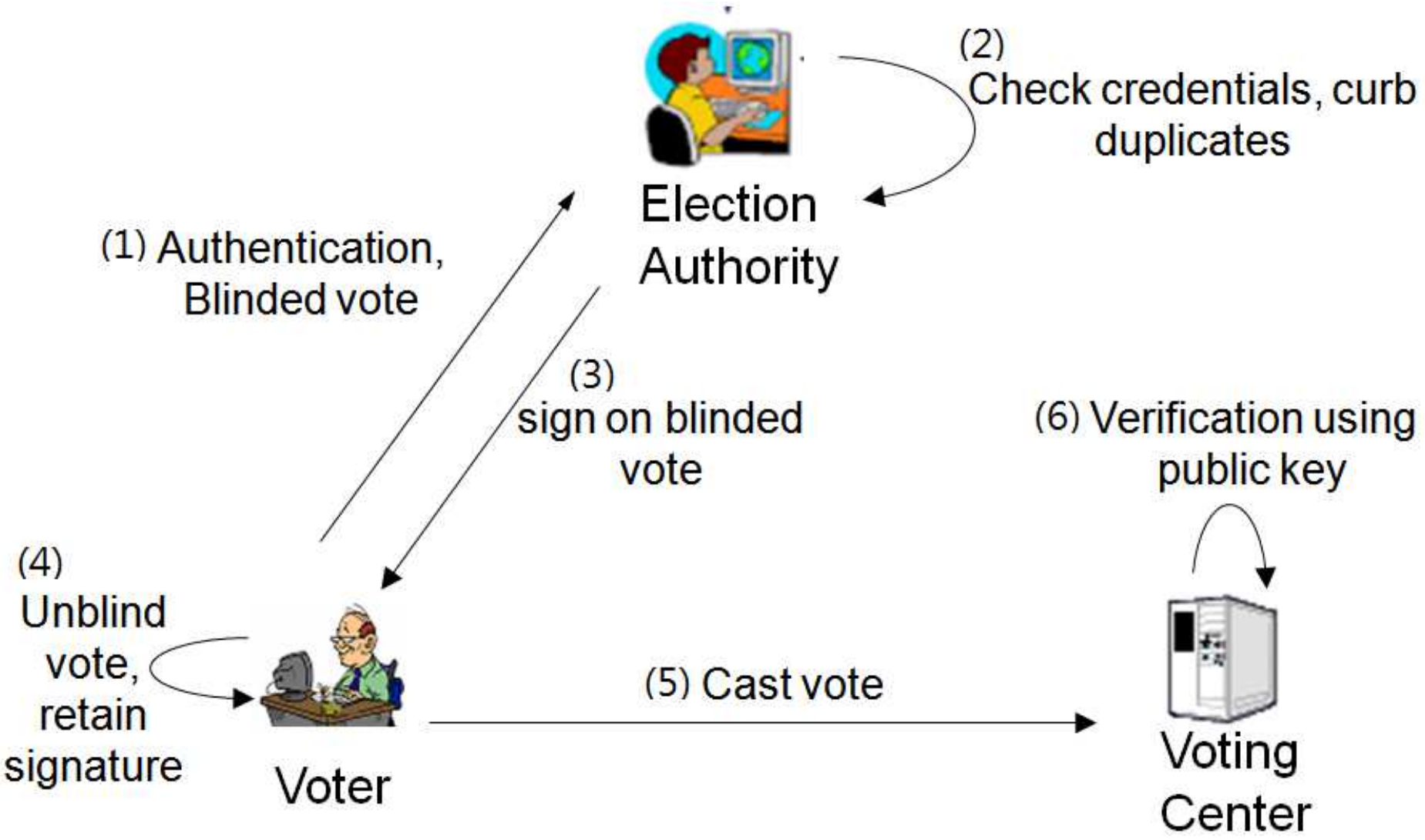
Blind Signature - (1)

- Introduced by David Chaum in 1983.
- Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties.
- Blind signature schemes see a great deal of use in applications where sender privacy is important.
- This can be useful in schemes where anonymity is required.
  - Cryptographic election systems (e-Vote)
  - Digital cash schemes (e-Cash)

Blind Signature - (2)

- **Electronic voting system**
  - The integrity of some electronic voting system may require that each ballot be certified by an election authority before it can be accepted for counting.
  - This allows the authority to check the credentials of the voter to ensure that they are allowed to vote, and that they are not submitting more than one ballot.
  - Simultaneously, it is important that this authority not learn the voter's selections.

Blind Signature - (3)



Blind Signature - (4)

- Voter wants $\langle M, H(M)^{d_{EA}} \rangle$.
- Voter knows the public key (e_{EA}, n_{EA}) of EA(Election Authority).
- The signing procedure
  - **Blinding:** Voter randomly chooses $r \in \mathbb{Z}^*_{n_{EA}}$, and sends EA $H(M) \cdot r^{e_{EA}}$.
  - **Singing:** EA signs $H(M) \cdot r^{e_{EA}}$, and returns $H(M)^{d_{EA}} \cdot r$.
  - **Unblinding:** Voter knows r, so he can calculate $H(M)^{d_{EA}}$.

Blind Signature - (5)

(2)
Check credentials,
Sign(B)=B^d

Election
Authority

(1) B = $H(m).r^e$
authentication, B

(3)
Sign(B) = $(H(m).r^e)^d$
Sign(B) = $H(m)^d.r$

(6) $(Sign(m))^e = H(m)$

(4)
Sign(m) =
Sign(B)/r

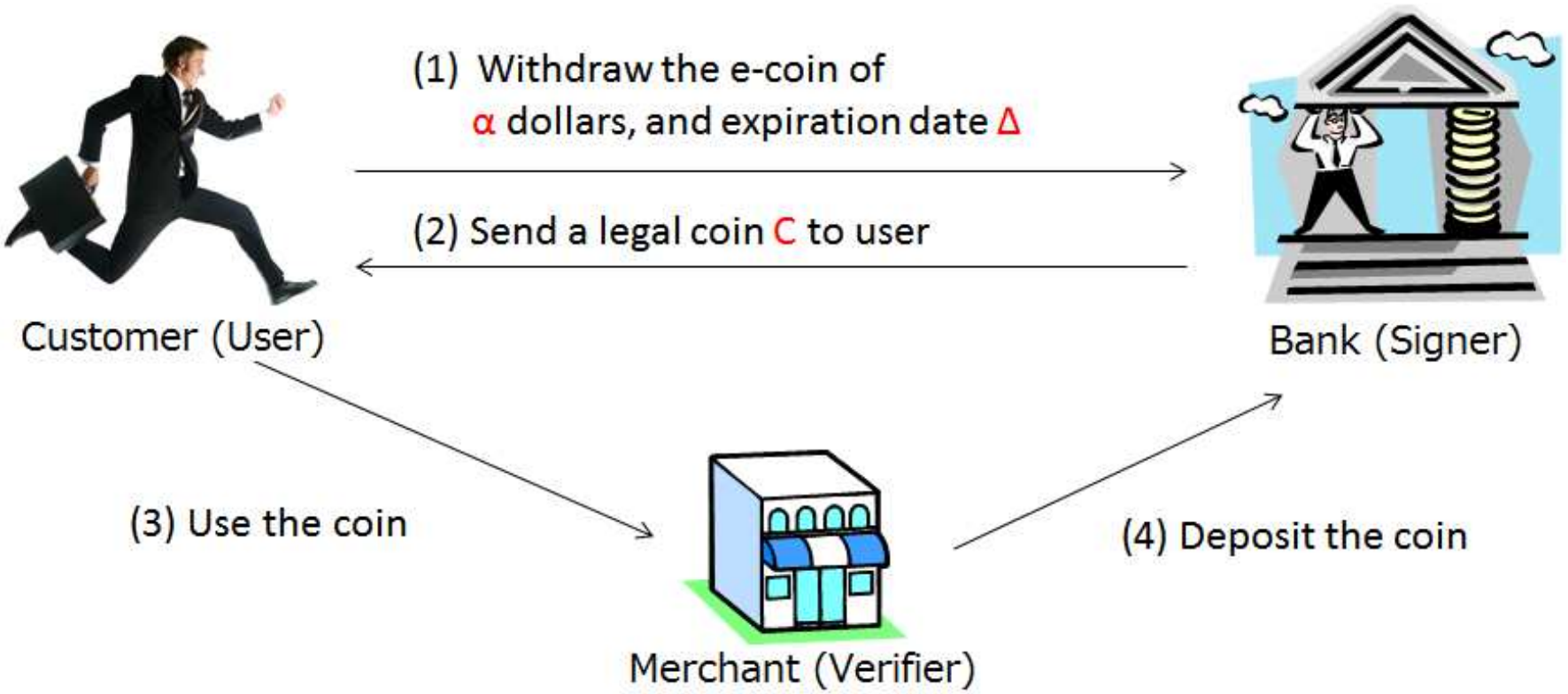
(5) Cast vote <m, Sign(m)>

Voter

Voting
Center

Partially Blind Signature - (1)

- Digital cash scheme



Partially Blind Signature - (2)

- First proposed by M. Abe and E. Fujisaki in ASIACRYPT '96.
- Based on RSA blind signature scheme mentioned above.
- The common information c of length $k-2$ bits, represented by $(c_{k-2}c_{k-1}...c_2c_1)_2$
- $\tau(c) = 2^{k-1} + 2c + 1 = (1c_{k-2}c_{k-1}...c_2c_11)_2$, where $2^{k-1} < \tau(c) < 2^k$.
- Add the following conditions
  - $s \nmid \phi(N)$ for all prime s, $3 \leq s \leq 2^k - 1$.
  - $e \geq 2^k - 1$.

Partially Blind Signature - (3)

- The signing procedure for message (M, c)
  - The user and the signer have a common information c.
  - The user randomly chooses $r \in \mathbb{Z}_n^*$, and send the signer $Z = H(M)r^{e\tau(c)}$.
  - The signer compute the private key $d_c = \frac{1}{e\tau(c)} \pmod{\phi(n)}$ corresponding to c. Then, send the user $\Phi = Z^{d_c} \pmod{n} = H(M)^{d_c} \cdot r$.
  - The user can get the signature $\delta = \frac{\Phi}{r} = H(M)^{d_c}$.
  - The signed message is $\langle (M, c), \delta \rangle$
- The verification procedure
  - The verifier check if $\delta^{e\tau(c)} = H(M)$.

Partially Blind Signature - (4)

- The common information $c = \alpha || \Delta$