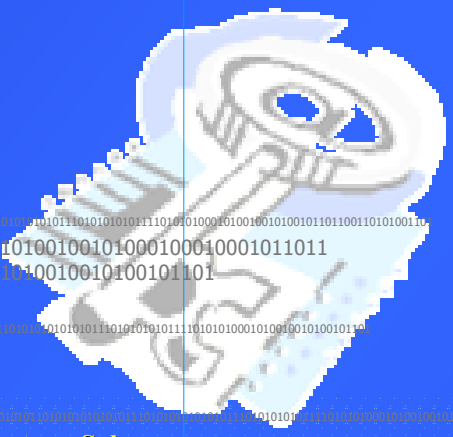
Secure Cryptographic Protocols for E-commerce Transaction on the Internet

Presented by Winson Yeung
Supervised by Prof Xiaotie Deng
Department of Computer Science



Internet is a virtual world for many users to communicate or run their business transactions. When data is translated over the Internet, there would be some intruders who eavesdropping or tampering some useful data such as user's personal password, credit card information or other sensitive secret information. Some intruders may also pretend to be other people to do the illegal activities. So data security is very important when doing E-commerce transaction on the Internet. Our work is to design some secure cryptographic protocols for society activities on the Internet.

Digital signature is one of the major solutions for these kinds of problems. In a digital signature system, all of the users have a pair of public key and private key. Any user can use his private key to sign a digital signature for any message and other people can verify the signature by using the signer's public key.

Undeniable Signature

- Recipient can challenge its signer through confirmation or denial protocols and signer cannot falsely deny a valid signature
- Verification involves the interaction between signer and recipient to ensure the validity of the digital signature

Fair Anonymity

- All the signers are anonymous from the users and it can only check the validity of the signature while it is infeasible to determine original signer except the trusted center
- Necessary for some emergence cases
  E.g. some signers do illegal actions

Application:

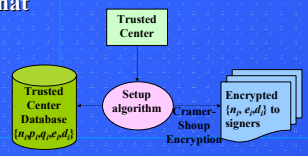
It is especially suitable to those applications that need to provide the commitment of data integrity and signer anonymity while preserving non-repudiation of signers. It can also provide the feature of revoking the original signer when needed.

- Communication in organization like FBI, ICAC
  The trusted center can be the chairman of the organization. Every staff holding their own private key can sign a document while preserving their anonymity and other people can verify the signature. In case of a dispute, the trusted canter can revoke the original signer.
- Open bid auctions
- Stock exchange
- Digital Cash

New Undeniable Signature Scheme

Setup algorithm

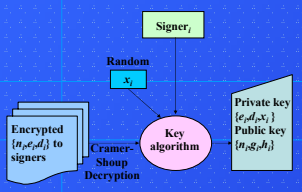
- For $i = 1$ to N
  - Choose prime p_i, q_i where $p_i \equiv q_i \equiv 3 \pmod 4$
  - $n_i = p_i q_i$
  - Choose $e_i, d_i \in Zn_i^*$ randomly such that $e_i d_i \equiv 1 \pmod{\phi(n_i)}$
  - Encrypt and send $\{n_i, e_i, d_i\}$ to signer$_i$
- End Loop



Trusted center's database — $\{(n_i, p_i, q_i, e_i, d_i) | 1 \le i \le N\}$

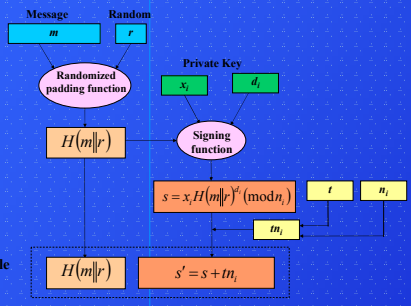
Key algorithm

- For signer$_i$
  - Decrypt $\{n_i, e_i, d_i\}$
  - Choose $x_i \in Zn_i^*$ randomly
  - $g_i = x_i^2 \pmod{n_i}$ and $h_i = g_i^{e_i} \pmod{n_i}$
- Private key – $\{e_i, d_i, x_i\}$
- Public key - $\{n_i, g_i, h_i\}$



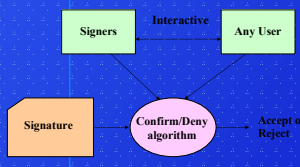
Sign algorithm

- Choose $r \in Zn_i^*$ randomly
- $s = x_i H(m||r)^{d_i} \pmod{n_i}$
- $s' = s + tn_i$ where $|s'| \le k$



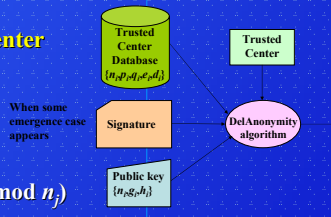
Confirm/Deny algorithm

- Signer$_i$ prove that
  - $h_i \equiv g_i^{e_i} \pmod{n_i}$
  - $(s' \bmod n_i)^{2e_i} \equiv h_i H(m||r)^2 \pmod{n_i}$



DelAnonymity algorithm

- In case of dispute, trusted center "on-line"
  - Search her database $\{(n_i, p_i, q_i, e_i, d_i) | 1 \le i \le N\}$
  - If exist j such that $(s' \bmod n_j)^{2e_j} \equiv h_j H(m||r)^2 \pmod{n_j}$
    $\Rightarrow$ signer$_j$



Department of Computer Science

香港城市大學 City University of Hong Kong