Research in Information Security

Dr. Ashok Kumar Das

IEEE Senior Member
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Home Page: http://sites.google.com/site/iitkgpakdas/

Algorithms and Approaches of Proxy Signatures

Proxy Signatures

Digital Signature

- Digital signature is a cryptographic means through which the authenticity, data integrity and signer's non-repudiation can be verified.
- Typically, digital signature of a document is a piece of information encrypted by the signer's private key.
- Numerous researches have shown significant contributions to this field using various cryptographic primitives.
- Nevertheless, there are many practical environments where digital signatures do not possess specific requirements, and thereby digital signatures appear in several other forms, namely proxy signatures, multi signatures, blind signatures, ring signatures etc.

Proxy Signatures

Various signatures

- **Multi-signature:** A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document, and has many potential uses.

Proxy Signatures

Various signatures

- **Multi-signature:** A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document, and has many potential uses.
- **Blind signature:** In many applications involving anonymity, it is desirable to allow a participant to sign a message without knowing what the message is. This is called a blind signature.

Proxy Signatures

Various signatures

- **Multi-signature:** A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document, and has many potential uses.
- **Blind signature:** In many applications involving anonymity, it is desirable to allow a participant to sign a message without knowing what the message is. This is called a blind signature.
- **Ring signature:** Ring signatures, first introduced by Rivest, Shamir, and Tauman, enable a user to sign a message so that a ring of possible signers (of which the user is a member) is identified, without revealing exactly which member of that ring actually generated the signature.

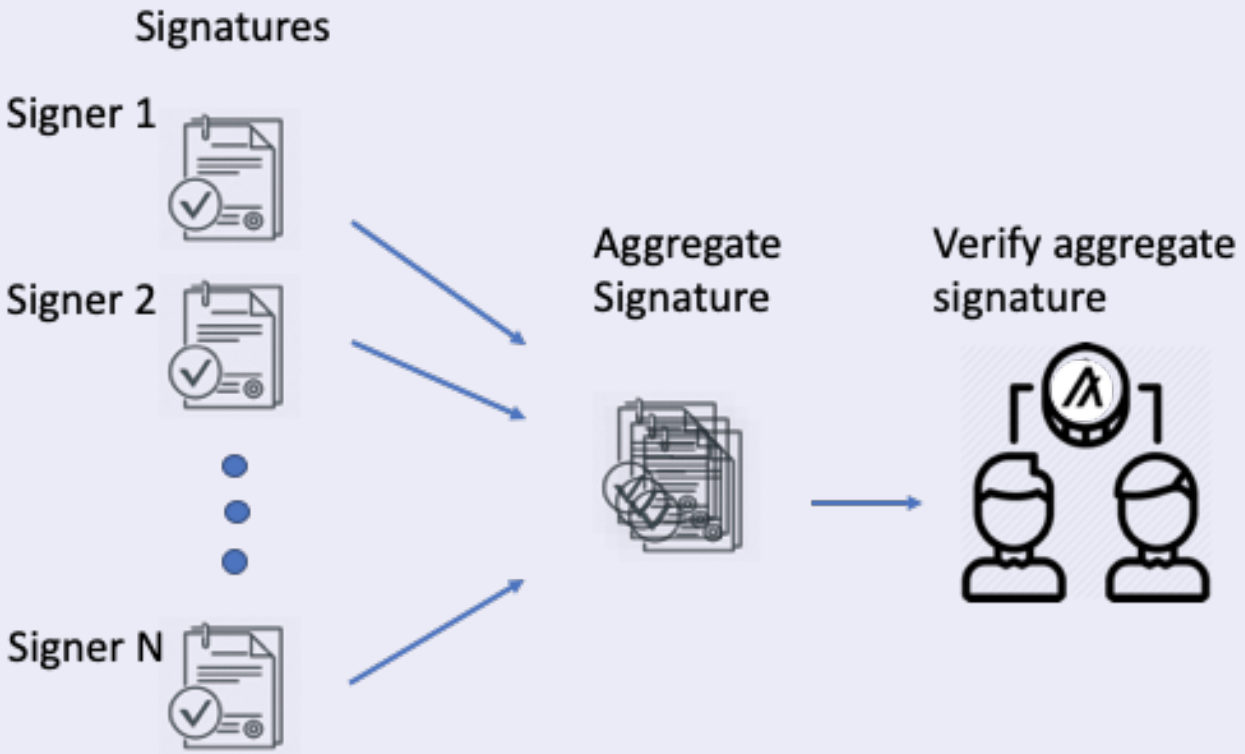
Proxy Signatures

Various signatures

- **Multi-signature:** A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document, and has many potential uses.
- **Blind signature:** In many applications involving anonymity, it is desirable to allow a participant to sign a message without knowing what the message is. This is called a blind signature.
- **Ring signature:** Ring signatures, first introduced by Rivest, Shamir, and Tauman, enable a user to sign a message so that a ring of possible signers (of which the user is a member) is identified, without revealing exactly which member of that ring actually generated the signature.

Aggregate Signature

- In a general aggregate signature scheme, signatures are generated by individual users. They can then be combined into an aggregate signature by some aggregating party.
- An aggregate signature is the same length as an ordinary signature in the underlying scheme.



Proxy Signatures

Proxy signatures

- Proxy signature is a digital signature where an original signer delegates her signing capability to a proxy signer, and then the proxy signer performs message signing on behalf of the original signer.
- **Example:** A manager of a company wants to go for a long trip. She would need a proxy agent, to whom she would delegate her signing capability, and thereafter the proxy agent would sign the documents on behalf of the manager.

Proxy Signatures

Proxy signatures

- The notion of proxy signature has been evolved over a long time (over 25 years now).
- However, the cryptographic treatment on proxy signature was introduced by Mambo *et al.* in 1996.
  M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures: Delegation of the Power to Sign Messages," IEICE Transactions Fundamentals, vol. E79-A, no. 9, pp. 1338-1353, 1996.
- Mambo *et al.* classified the proxy signature on the basis of delegation, namely ***full delegation***, ***partial delegation*** and ***delegation by warrant***.

Proxy Signatures

Full delegation

- In full delegation, an original signer gives her private key to a proxy signer and the proxy signer signs document using original signer's private key.
- The drawback of proxy signature with full delegation is that the absence of a distinguishability between original signer and proxy signer.

Proxy Signatures

Partial delegation

- In partial delegation, the original signer derives a proxy key from her private key and hands it over to the proxy signer as a delegation capability.
- In this case, the proxy signer can misuse the delegation capability, because partial delegation cannot restrict the proxy signer's signing capability.

Proxy Signatures

Delegation by warrant

- The weaknesses of full delegation and partial delegation are eliminated by partial delegation with warrant.
- A warrant explicitly states the signers' identity, delegation period and the qualification of messages on which the proxy signer can sign, etc.

Proxy Signatures

Discrete logarithm problem and its applications

- The discrete logarithm is the inverse of discrete exponentiation in a finite cyclic group.
- **Instance:** A multiplicative group $(G, \cdot)$, an element $g \in G$ having order n and $y = g^x \mod n$.
  Question: Find x.
  This problem is computationally infeasible when n is large.

Formal definition of discrete logarithm problem

Let G be a cyclic group of order n, g a generator of G, and A an algorithm that returns an integer in Z_n, where $Z_n = \{0, 1, \ldots, n-1\}$. Let $a \in_R S$ denote that a is chosen randomly from the set S. Consider the following experiment, $EXP^{DLP}_{G,g}(A)$ in Algorithm 1.

Algorithm 1: $EXP^{DLP}_{G,g}(A)$

1: $x \in_R Z_n$
2: $X \leftarrow g^x \mod n$
3: $x' \leftarrow A(X)$
4: **if** $g^{x'} = X \mod n$ **then**
5: **return** 1 (Success)
6: **else**
7: **return** 0 (Failure)
8: **end if**

Formal definition of discrete logarithm problem

- The DLP-advantage of A is defined by $Adv_{G,g}^{DLP}(A) = Pr[Exp_{G,g}^{DLP}(A) = 1]$, where $Pr[E]$ denotes the probability of an event E.
- The discrete logarithm problem (DLP) is said to be a hard problem in G if the DLP-advantage of any adversary of reasonable resources is small, where resources are measured in terms of the time complexity of the adversary including its code size as usual.
- In other words, DLP is called a hard problem, if $Adv_{G,g}^{DLP}(A) \leq \epsilon$, for any sufficiently small $\epsilon > 0$.
- **Reference: Ashok Kumar Das. A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. Networking Science (Springer), 2(1-2):12-27, 2013.**

The Schnorr signature scheme

The scheme is based on hardness of solving DLP. It consists of the following phases.

- **Setup** ($\mathcal{SP}_{dlp}$)**:** Takes input 1^k and outputs **params-dlp**.
  The **params-dlp** consists of primes q and l such that $2^{k-1} \leq q < 2^k$, an element $g \in Z_q^*$ of order l that divides $q-1$, and a hash function $h : \{0,1\}^* \rightarrow Z_l$.
- **KeyGen** ($\mathcal{KG}_{dlp}$)**:** The users agree on a group G (multiplicative group of integers modulo q) for some prime q with generator g of prime order l in which the DLP is hard problem.
  The user chooses a private key $x \in Z_l$ and then computes the publlic key as $y = g^x \pmod{q}$.
  In other words,
  user public key $\leftarrow \mathcal{KG}_{dlp}$(**params-dlp**, user private key), that is,
  $y \leftarrow \mathcal{KG}_{dlp}$(**params-dlp**, x).

The Schnorr signature scheme (Continued...)

- **Sign** ($\mathcal{S}_{dlp}$)**:** To sign a message, say m, the signer has to choose a random number $t \in Z_l$ and calculate $r = g^t \pmod{q}$.
  Then the signer computes $c = h(m||r)$ and $\sigma = (t - xc) \pmod{l}$.
  The signature on message m is then (σ, c).
  In other words, $\sigma \leftarrow \mathcal{S}_{dlp}($ **params-dlp**, $(t, r), x, m)$.
- **Verify** ($\mathcal{V}_{dlp}$)**:** The verifier calculates $r' = g^{\sigma} y^{c} \pmod{q}$ and $c' = h(m||r')$.
  If the condition $c' = c$ is satisfied, the signature is treated as valid; otherwise, the signature is invalid.
  In other words, **result** $\leftarrow \mathcal{V}_{dlp}($ **params-dlp**, $y, \sigma, m)$,
  where **result** $\in \{valid, invalid\}$.

Remark: The Schnorr signature scheme is proven to be secure under the assumption that the DLP is intractable (NP-hard).

Proxy Signatures

Security properties of proxy signature

- **Strong unforgeability:** A designated proxy signer can create a valid proxy signature on behalf of the original signer. But the original signer and other third parties cannot create a valid proxy signature.
- **Strong identifiability:** Anyone can determine the identity of corresponding proxy signer from the proxy signature.
- **Strong undeniability:** Once a proxy signer creates a valid proxy signature on behalf of the original signer, he cannot deny the signature creation.
- **Verifiability:** The verifier can be convinced of the signers' agreement from the proxy signature.
- **Distinguishability:** Proxy signatures are distinguishable from the normal signatures by everyone.
- **Secrecy:** The original signer's private key cannot be derived from any information, such as the shares of the proxy key, proxy signatures, etc.