National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 1090-1091

An effective multi user setting schemes

Seema Kumari Nagar[1], Dr. Amit Sharma[2]
[1] M.Tech. Scholar, Computer Science & Engineering, Vedant College of Engineering & Technology, Bundi, Rajasthan, India
[2] Professor, Computer Science & Engineering, Vedant College of Engineering & Technology, Bundi, Rajasthan, India

Abstract
Digital signatures achieved through public key cryptography work for individual users. They do not have features such that they can be used for multiple documents or multiple users. Signatures with homomorphic property are designed for this purpose. Yet, most of the homomorphic signatures pertain to signature of an algorithm thus providing verifiability that the algorithm has been executed over a set of inputs. There is still need of homomorphic signatures in which only the signatures have homomorphic properties that can be used to concatenate or combine multiple signatures. Such malleability, though desirable, may have vulnerability towards forging or other attacks. So a homomorphic signature has to suffice both conditions: meet the malleability requirements of the application and be secure against attacks.

Keywords: multi user settings (MUS), key generation (KG), signing primitives (SP), signatures scheme primitives (SSP)

1. Introduction
We propose a homomorphic signature scheme that can be used to verify document signed by multiple users. We propose to have two different verification primitives, one for individual signature verification and another for multiple signatures.

2. Homomorphic signature schemes from digital signature
Signature is a cryptographic primitive whose purpose is to provide:-

- Integrity: prevention from non-authorized modifications of the signed message;
- Authenticity: The process of granting or denying access to a network resource is called authorization;
- Non-repudiation: Non-repudiation is the assurance that someone cannot deny something.

2.1 Multi User Setting (MUS)
A single document is signed by all parties involved. But, the verifying authority may need to save effort required for individual verification of signature. So, it is required that verification be done only as a single process that verifies all signatures as if they are a single signature.

- There are n signers.
- There is one single message m.
- A hashing function exists such that $H(m) = h$ and is available to both signer and verifier.
- There is one verifier.
- There are n pairs of private and public keys, one per signer.
- There is also one common public key
- The i[th] signer produces signature s_i.

2.2 Homomorphic Signatures
Homomorphic signature scheme that can be used to verify document signed by multiple users. We propose to have two different verification primitives, one for individual signature verification and another for multiple signatures.

3. Homomorphic signatures schemes for multi user setting
Key generating authority that generates n pairs of private key and public key and a common public key associated with them for the verifier

3.1 Classification of signatures schemes primitives
encryption and decryption as a black box and entire signing process can be either over the cipher or within the cipher. The signature scheme consists of primitives:

1. Key Gen,
2. Sign.,

3.1.1 Key Generation

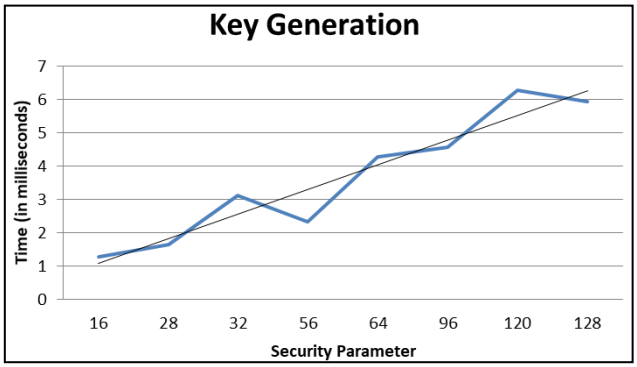

Fig 1: Growth of runtime of key generation with security parameter

3.2.1 Signing

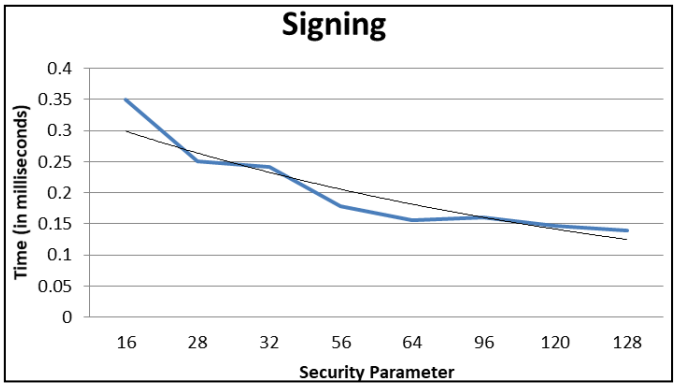

Fig 2: Growth of runtime of signing primitive with security parameter

4. Features and Advantage of multi user settings

- The signatures are homomorphic. They have both multiplicative and additive homomorphic properties. The idea of construction can be used for digital signatures in various settings.
- Only addition is used for combination of signatures, making it very easy operation.
- The proposal is specifically shown for multiple user settings where a single message is signed by more than one user. Yet it can be used for single user setting, that is, a simple single user signature and verification is possible.
- Both signing and verification have low time complexity.
- The primitives have simple integer operations hence no complicated computations involved and are easy to practically use it.
- The proposed scheme is secure with commonly used length of keys.
- A verification protocol is also proposed, to detect which individual signature was corrupted in case the combined signature is rejected by the verifier.

5. Conclusions

Simple integer operations based on modulo arithmetic are easy to implement. Moreover, the time complexity reduces when the size of modulus increases. But if size of modulus is increased, it implies the size of key is increased. This will provide more security to the proposed scheme. Thus, we have proposed a scheme that has very low time complexity that falls if size of keys is increased. This is a very desirable feature of any cryptographic primitive. Also, the combination of signatures is a simple addition process. Hence, our proposal is a practically feasible technique.

6. References

1. Catalano D, Fiore D, Warinschi B. Efficient network coding signatures in the standard model, Public Key Cryptography-PKC, Springer, 2012, 680-696.
2. Waters B. Efficient identity-based encryption without random oracles, Advances in Cryptology Eurocrypt, Springer, 2005, 114-127.
3. Boneh D, Boyen X. Short signatures without random oracles, Advances in Cryptology-Eurocrypt, Springer, 2004, 56-73.
4. Gennaro R, Halevi S, Rabin T. Secure hash-and-sign signatures without the random oracle, Advances in Cryptology-Eurocrypt, Springer, 1999, 123-139.
5. Hohenberger S Waters B. Short and stateless signatures from the rsa assumption, Advances in Cryptology-Crypto, Springer, 2009, 654-670.
6. Attrapadung N, Libert B, Peters T. Efficient completely context-hiding quotable and linearly homomorphic signatures, Public-Key Cryptography-PKC, Springer, 2013, 386-404.