ANONYMOUS THRESHOLD SIGNATURES

A master's thesis
Submitted to the

Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya

By

Petar Hlad Colic

In partial fulfillment
of the requirements for the master's degree in

Advanced Mathematics and Mathematical Engineering

Advisor: Javier Herranz Sotoca

Barcelona, October 2017

Abstract

Resum

Resum

Resum

Resumen

Resum

ACKNOWLEDGEMENTS

Acknowledgements

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Intro

CHAPTER 2

PRELIMINARIES

Some cryptographic preliminaries and other definitions.

Bilinear pairings

Let G_1 and G_2 be two (multiplicative) cyclic groups of prime order q. Let g_1 be a fixed generator of G_1 and g_2 be a fixed generator of G_2.

Definition 2.1.1. Computation Diffie-Hellman (CDH) Problem: Given a randomly chosen $g \in G_1$, g^a, and g^b (for unknown randomly chosen $a, b \in \mathbb{Z}_q$), compute g^{ab}.

Definition 2.1.2. Decision Diffie-Hellman (CDH) Problem: Given randomly chosen $g \in G_1$, g^a, g^b, and g^c (for unknown randomly chosen $a, b, c \in \mathbb{Z}_q$), decide whether $c = ab$. (If so, (g, g^a, g^b, g^c) is called a valid Diffie-Hellman tuple.)

Definition 2.1.3. Computational co-Diffie-Hellman (co-CDH) Problem on (G_1, G_2): Given $g_2, g_2^a \in G_2$ and $h \in G_1$ as input, compute $h^a \in G_1$.

Definition 2.1.4. Decision co-Diffie-Hellman (co-DDH) on (G_1, G_2): Given $g_2, g_2^a \in G_2$ and $h, h^b \in G_1$ as input, decide whether $a = b$. If so, we say that (g_2, g_2^a, h, h^a) is a co-Diffie-Hellman tuple.

Definition 2.1.5. Bilinear map: Let G_T be an additional group such that $|G_1| = |G_2| = |G_T|$. A bilinear map is a map $e : G_1 \times G_2 \to G_T$ with the following properties:

1. Bilinear: for all $u \in G_1, v \in G_2$ and $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.

2. Non-degenerate: $e(g_1, g_2) \neq 1$.

Homomorphic PKE

Digital Signatures

To ensure integrity of data in communications and authentication, the concept of digital signatures was developed.

A digital signature scheme consists of 3 algorithms:

- **Key generation**: on input of a security parameter k (usually the length), outputs a pair (sk, pk) of secret and public keys.
- **Signature**: given an input message m and the secret key sk, outputs a signature σ.
- **Verification**: given an input message m, a signature σ on the message and a public key pk, ouptuts whether the signature is valid or not.

A signature scheme must satisfy the following properties:

- **Correctness**: A signature generated with the signing algorithm must always be accepted by the verifier.
- **Unforgeability**: Only a user can sign messages on behalf of himself.
- **Non-repudiation**:

Examples

ElGamal

Let H be a collision-resistant hash function. Let p be a large prime such that the *discrete logarithm problem* is difficult over $\mathbb{Z}_p$. Let g be a randomly chosen generator of $\mathbb{Z}_p^*$

2.3.1.1.1 Key Generation Randomly choose a secret key $x \in \mathbb{Z}_p^*$, and compute the public key $y = g^x$.

2.3.1.1.2 Signature To sign a message m, the signer chooses a random $k \in \mathbb{Z}_p^*$. Compute $r = g^k$. To compute s, the following equation must be satisfied: $g^{H(m)} = g^{xr} g^{ks}$. So $s = (H(m) - xr)\, k^{-1} \pmod{p-1}$

If $s = 0$, it starts over again with a different k.

The pair (r, s) is the digital signature for m.

2.3.1.1.3 Verification Check $g^{H(m)} = y^r r^s$

The use of $H(\cdot)$ prevents an existential forgery attack.

Boneh-Lynn-Shacham (BLS)

Let G, G_T be groups of prime order p. Let g be a generator of G. Let $e : G \times G \to G_T$ be a non-degenerate bilinear pairing.

2.3.1.2.1 Key Generation Randomly choose a secret key $x \in \mathbb{Z}_p$. The public key will be $y = g^x$.

2.3.1.2.2 Signature The signature on m is $\sigma = H(m)^x$.

2.3.1.2.3 Verification Given a signature σ and a public key g^x, it verifies that $e(\sigma, g) = e\left(H(m), g^x\right)$.

Signature Aggregation

Explain how different signature schemes allow aggregation of n signatures on n messages from n signers.

Group Signatures

Use of aggregation: group signatures. They are used to sign on behalf of the group, prove group membership.

The easyest way is to give everyone the secret key, so they can sign. But this would let any colluded user to share the secret key to other parties, which is not admissible.

Some group signatures need what is called a Dealer, which will deal with the keys.

Examples of Group signatures:

Shamir secret Sharing

Shamir secret sharing described in [1].

The scheme is based on polynomial interpolation.

Let p be a large prime number. All operations are done in $\mathbb{Z}_p$

We want to share a secret s into n shares so that the secret can be recovered with any k distinct shares.

Let $q(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ be a random polynomial of degree $k-1$ in which $a_0 = s$.

Each participant i in $\mathcal{P} = \{1, ..., n\}$ is given a different random number $x_i \in \mathbb{Z}_p$ which identifies the participant. Then, each participant i is given the share $y_i = q(x_i)$.

To recover the secret, we only need k different shares. Let $P \subset \mathcal{P}$ be any subset of k participants. Then

$$q(x) = \sum_{i \in P} y_i \prod_{\substack{j \in P \\ i \neq j}} \frac{x - x_j}{x_i - x_j}$$

Then, $s = q(0)$.

Threshold signature scheme using Shamir

sdcasdcasd

Anonymity

The concept of anonimity is used in so many ways

You could use ring signatures which proofs the knowledge of a 1-out-of-N secret key. This could be useful for a small amount of signatures. But it is not useful to provide general anonymity.

A signature scheme provides anonymity if:

- Unlinkability: cannot decide whether two different signatures were signed by the same user.
-

CHAPTER 3

SINGLE USE: ANONYMITY

Single use

CHAPTER 4

MULTIPLE USE: ANONYMITY AND NON-TRACEABILITY

Multiple use

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

Conclusions and future work

BIBLIOGRAPHY

[1] A. Shamir. “How to Share a Secret”. In: *Communications of the ACM* 22.11 (1979), pp. 612–613.