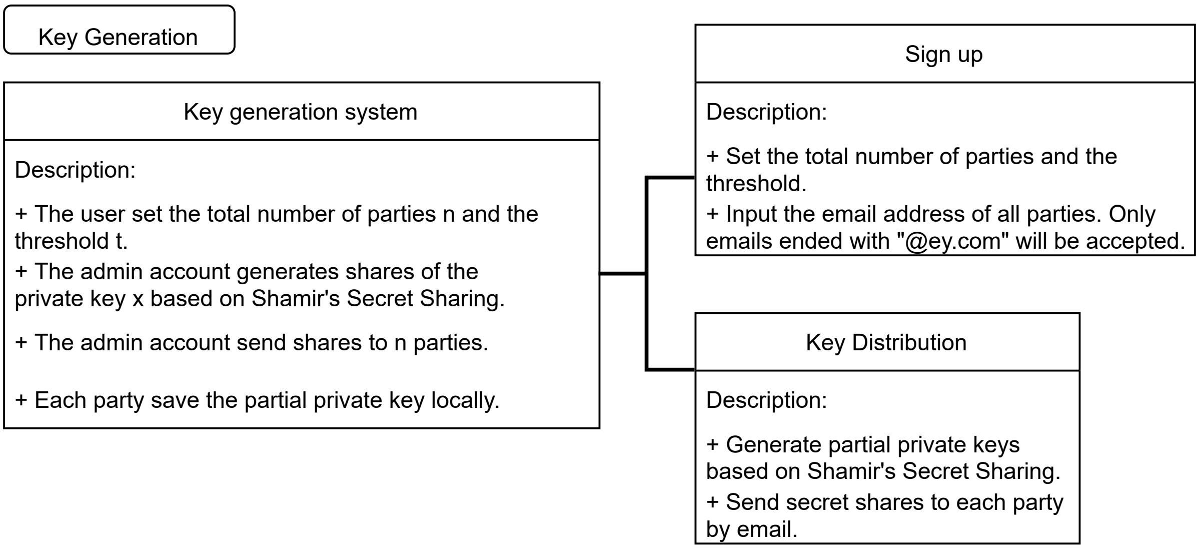
Key Generation



Key generation system

Description:

+ The user set the total number of parties n and the threshold t.

+ The admin account generates shares of the private key x based on Shamir's Secret Sharing.

+ The admin account send shares to n parties.

+ Each party save the partial private key locally.

Sign up

Description:

+ Set the total number of parties and the threshold.

+ Input the email address of all parties. Only emails ended with "@ey.com" will be accepted.

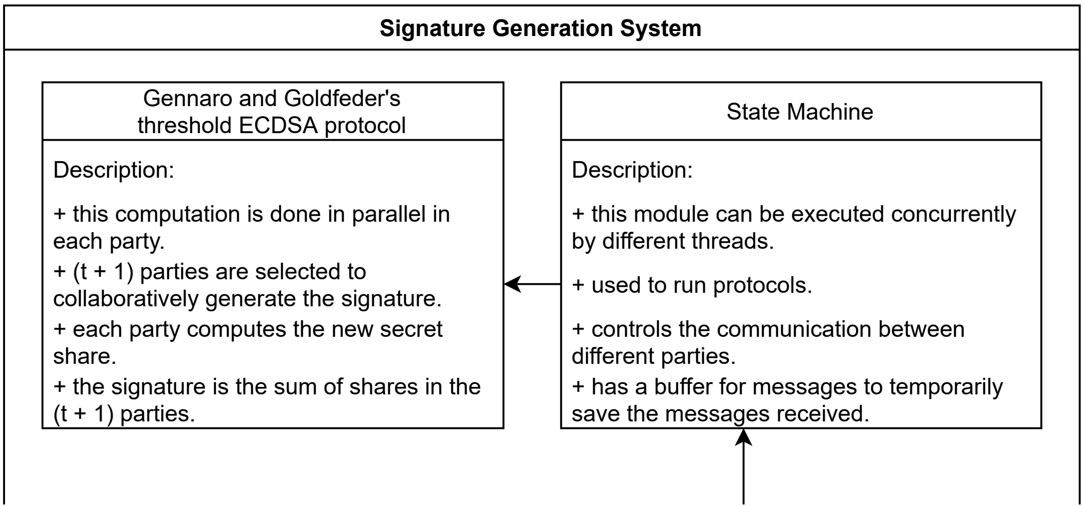
Key Distribution

Description:

+ Generate partial private keys based on Shamir's Secret Sharing.

+ Send secret shares to each party by email.

Signature Generation



Signature Generation System

Gennaro and Goldfeder's threshold ECDSA protocol

Description:

+ this computation is done in parallel in each party.

+ (t + 1) parties are selected to collaboratively generate the signature.

+ each party computes the new secret share.

+ the signature is the sum of shares in the (t + 1) parties.

State Machine

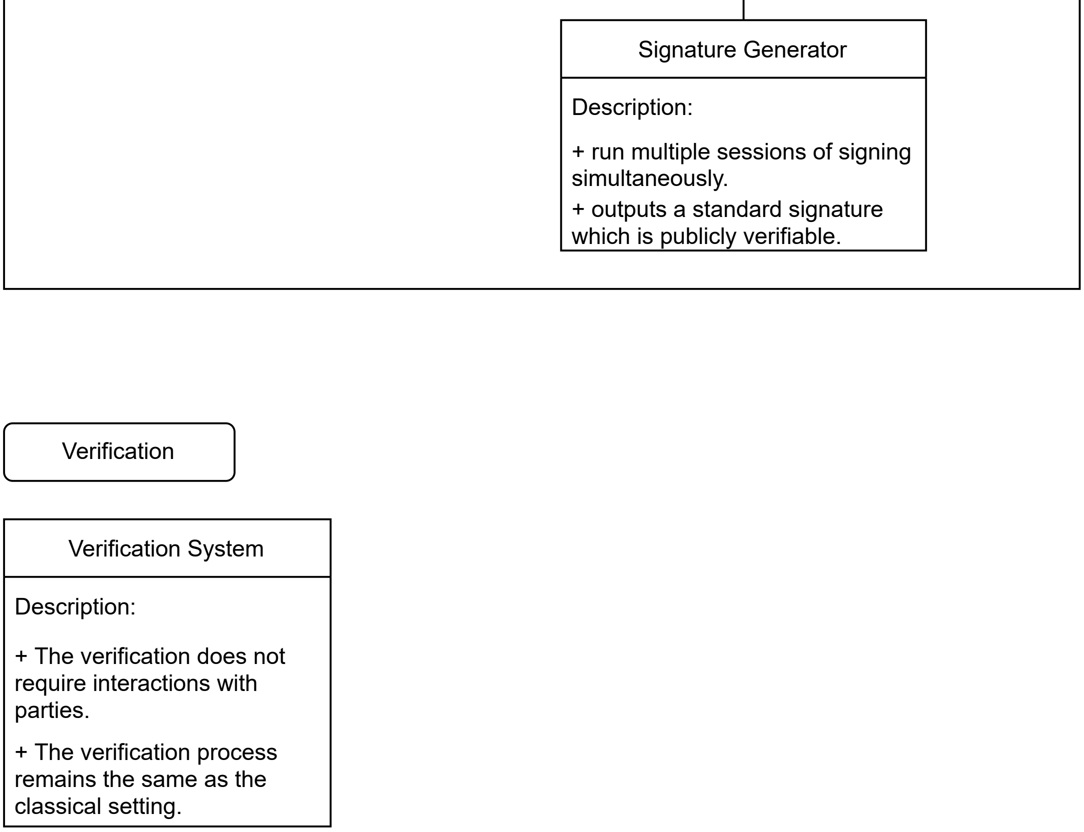
Description:

+ this module can be executed concurrently by different threads.

+ used to run protocols.

+ controls the communication between different parties.

+ has a buffer for messages to temporarily save the messages received.



Signature Generator

Description:

+ run multiple sessions of signing simultaneously.

+ outputs a standard signature which is publicly verifiable.

Verification

Verification System

Description:

+ The verification does not require interactions with parties.

+ The verification process remains the same as the classical setting.