The University of Hong Kong
Standard Chartered Foundation
FINTECH ACADEMY
香港大學 渣打慈善基金 金融科技學院

渣打香港
Standard Chartered Hong Kong
150th 週年慈善基金 Anniversary Community Foundation

Do not put all eggs in one basket:

Securing your wallet with threshold cryptography

Haiyang Xue
Department of Computer Science, Faculty of Engineering, HKU
Sep 2022

Outline

- (wallet) security in cryptocurrency
- What is threshold cryptography
- State-of-the-art of threshold cryptography
- Applications

Cryptocurrency

>$ 381 B

The market capitalization of Bitcion is > $381 B

9000
70 x(>$1 B)

more than 70 had a market cap exceeding $1 billion

Cryptocurrency (wallet) security

>$ 381 B

The market cap of Bitcion is > $381 B

$ 2.66 B

$2.66 Billion has been stolen since 2012

70 x(>$1 B)

more than 70 had a market cap exceeding $1 billion

>46 Hacked

Since 2012, at least 46 cryptocurrencies have been hacked

List of Hacked Cryptocurrencies

Bitcoin's Biggest loss

At the beginning of 2014, Mt Gox was handling 70% of Bitcoi's transactions.

In Feb. 2014, Mt. Gox lost about 740,000 bitcoins (6% of all bitcoin in existence at the time)
due to a "leak" in the wallet.

DATE	EXCHANGE	CAUSE OF HACK	AMOUNT STOLEN (USD)
2022, January 17	Crypto.com	Unknown	$34 million
2021, December 11	AscendEX	Obtained access to hot wallet	$80 million
2021, December 5	BitMart	Obtained access to hot wallet	$150 million
2021, August 19	Liquid	Obtained access to hot wallet	$97 million
2021, April 29	Hotbit	Obtained access to hot wallet	Nil
2020, December 23	Livecoin	Compromised system/servers	Unknown
2020, December 21	EXMO	Obtained access to hot wallet	$4 million
2020, December 1	BTC Markets	Internal staff error/mistake	270,000 user's private details
2020, September 25	KuCoin	Data leak	$275 million
2020, July 11	Cashaa	Malware	$3.1 million
2020, June 29	Balancer	Vulnerability in protocol	$500,000
2020, April 19	Lendf.me	Bugs and Re-entrancy attack	$24.5 million
2020, April 19	Uniswap	Bugs and Re-entrancy	$500,000

https://cryptosec.info/exchange-hacks/
https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/

Loss of key = loss of money ☹

A transaction in bitcoin looks like

Tr_1 :

Alice sends
$100 to Bob

h=hash (Tr_1)

Signature (sk_A, h)

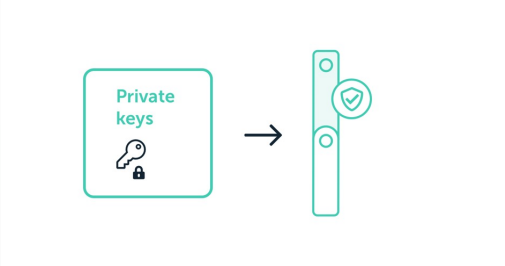
Signature is the standard ECDSA proposed by NIST

The private key sk_A is the only secret that Alice uses to generate this transaction

Lessons Learned

In cryptocurrency, we need to protect the private key

- **Cold Wallet:** a hardware wallet only stores and protects your **private key.**

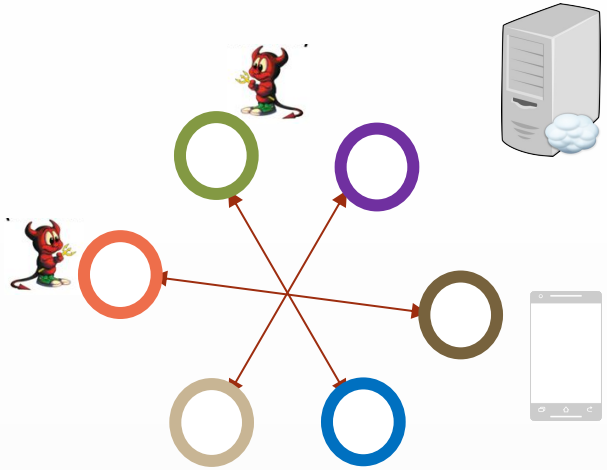


- **Threshold Cryptography:** Distribute the trust

Threshold Cryptography

-Do not put all you eggs in one basket

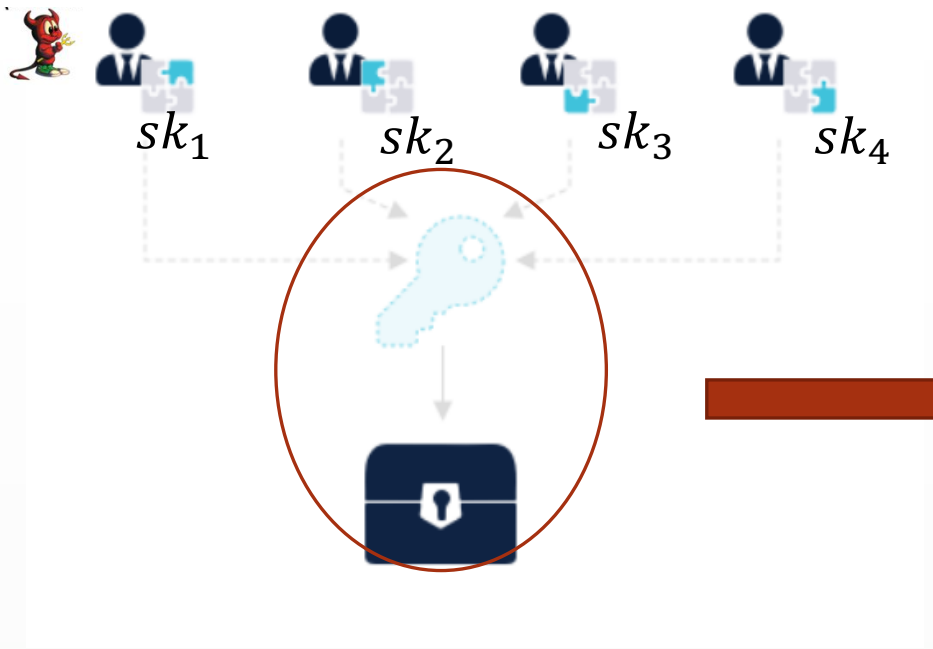
How to address
single-point
of failure ?



The threshold approach

Yvo Desmedt. 1987. Society and group-oriented cryptography: A new concept.

Threshold signature in cryptocurrency



- Ex. At least 2 of the 4 partis could generate the signature
- Need cryptography tools
  - Homomorphic encryption (HE)
  - Oblivious Transfer
  - and so on

Threshold Cryptography Project at NIST

- Upcoming call for standardization of threshold schemes
  - ECDSA(related to cryptocurrency), EdDSA
  - RSA, EC-KE, etc.

https://csrc.nist.gov/projects/threshold-cryptography

A short Summary

- In cryptocurrency, loss of the private key = the loss of money
- We need to protect the private key to reduce the risk
- Threshold signature (e.g. ECDSA) helps to distribute the trust

State-of-the-art of Threshold Cryptography

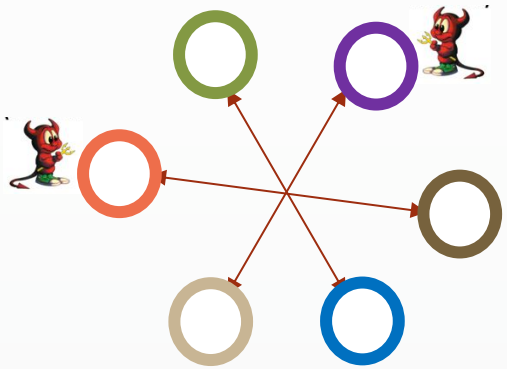
- **R**esearch: Paillier, CL, JL, OT
- **I**ndustry: ZenGo, Unbounded, Coinbase, etc.
- **G**overnment: NIST

We focus on Threshold ECDSA

- ECDSA
  - Digital Signature Standard using Elliptic Curve Cryptography
  - Widely deployed in cryptocurrency, such as Bitcoin etc.

single-points
of failure ?

- Threshold ECDSA
  - Protect the key by sharing it among n parties
  - Such that no fewer t users (here, t is called the threshold) could generate a valid ECDSA signature

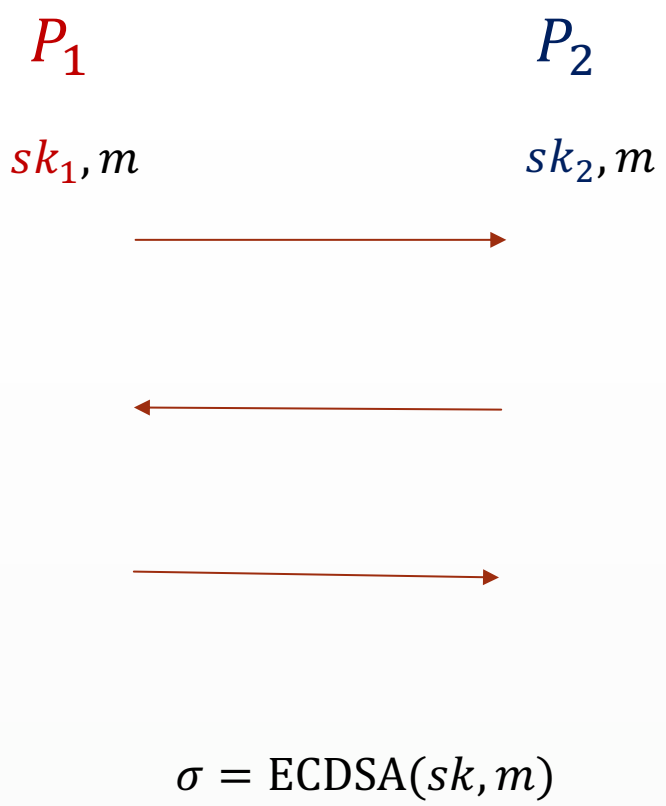


The threshold approach

Threshold Signature (with threshold $t = 2$)

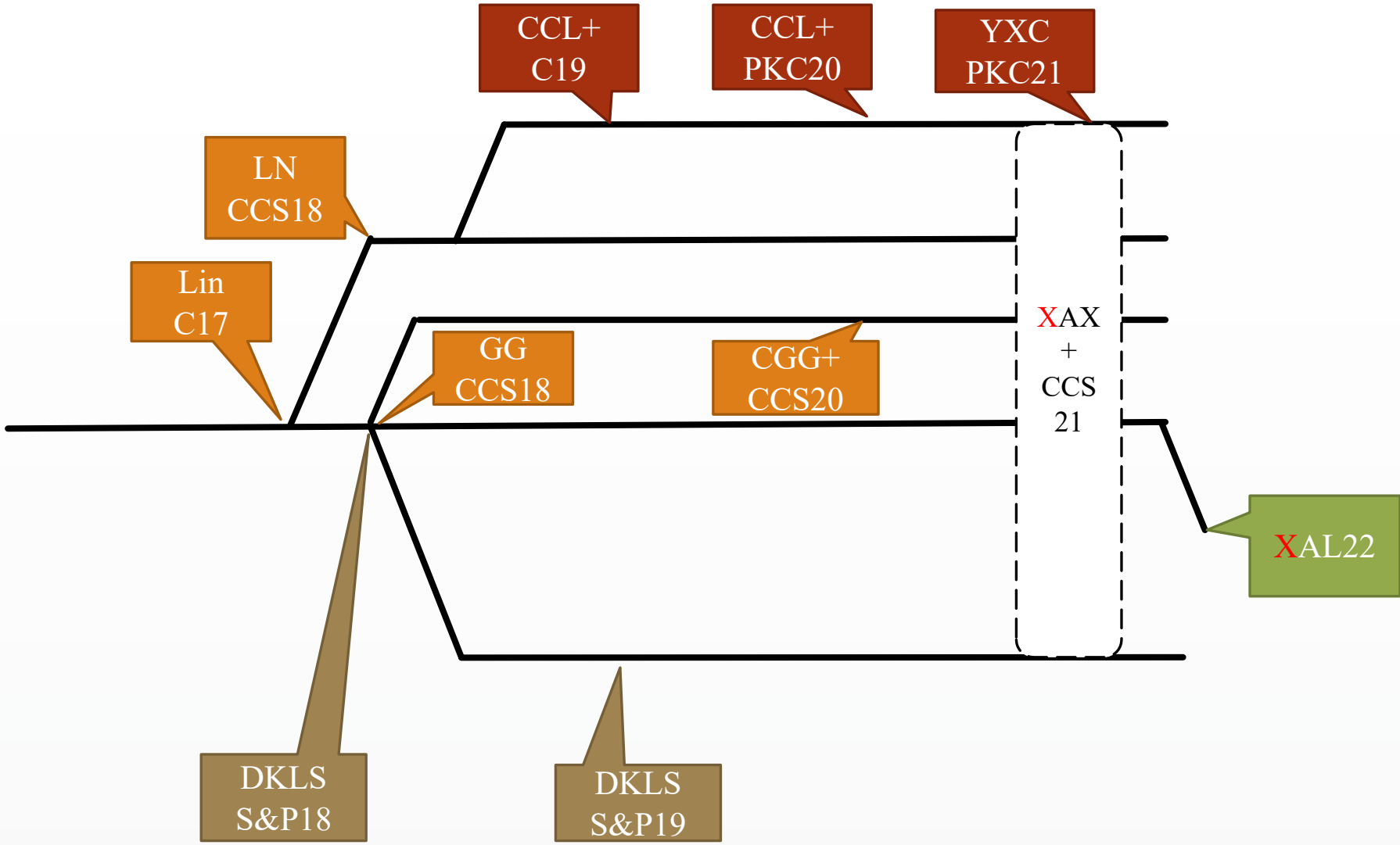
- **KeyGen:** The signing key is secretly shared across n parties
- **Interaction:** The t parties may collaborate to generate the signature.

- **Correctness:** sign a message in a threshold manner
- **Security:**
  - Any P_i can not forge signature alone, or learn anything on sk



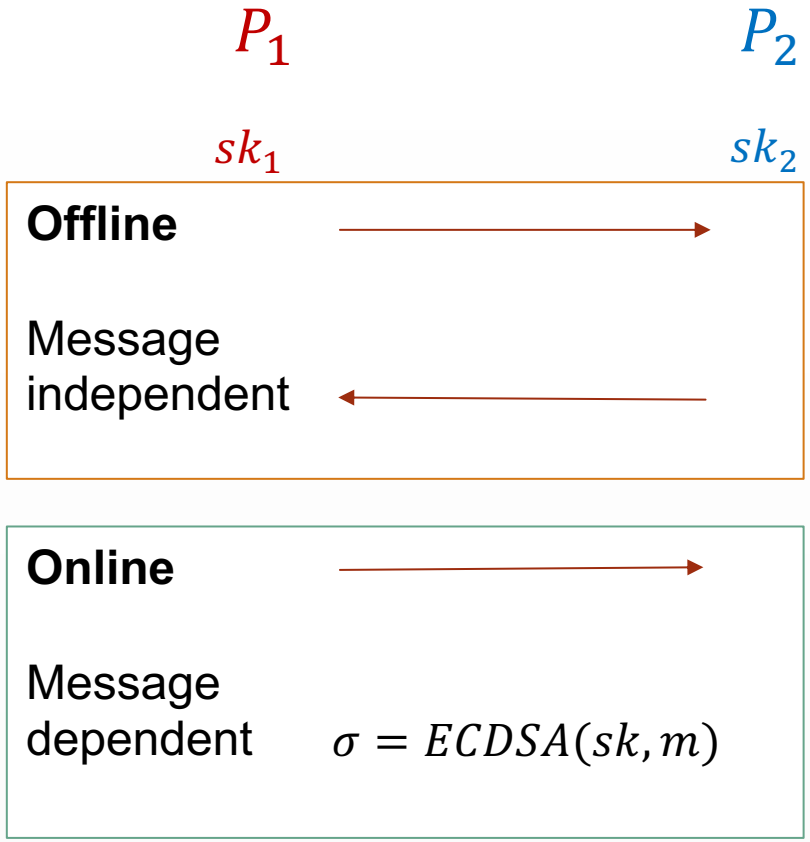
State-of-the-art in **R**esearch

- Homomorphic Enc: CL
- Homomorphic Enc: Paillier
- Homomorphic Enc: JL
- Oblivious Transfer (OT)



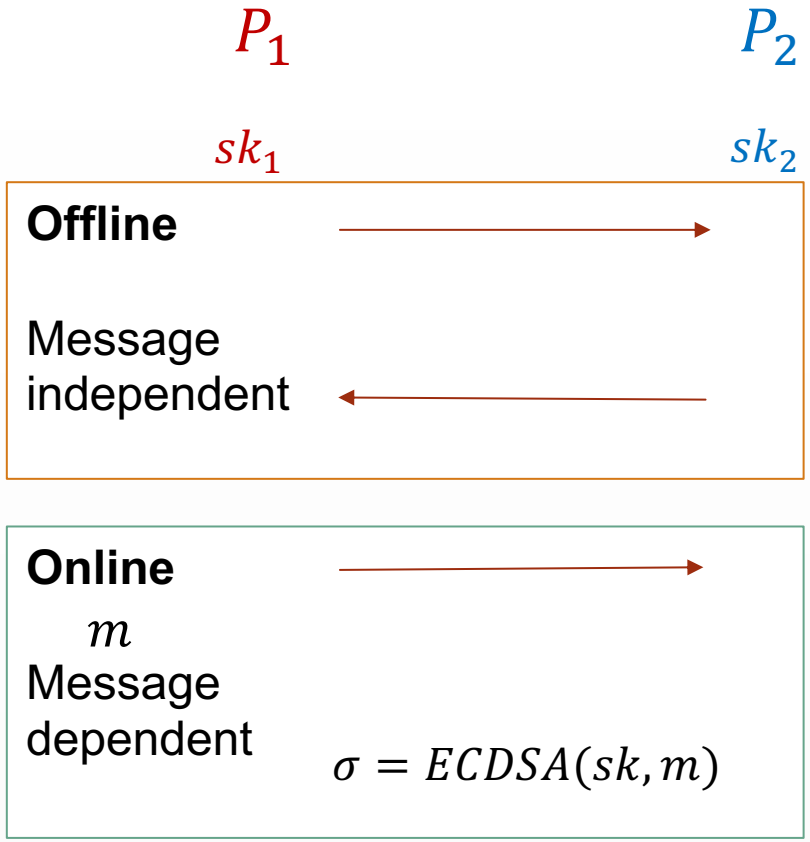
Previous works

- According to the message (that we would like to sign) is needed or not,
- Offline: Message independent
- Online: Message dependent
- Online cost is less, the better



Previous works （ in case t =2 ）

Schemes	Offline	Online
[Lin17, CCL+19]	Enc	Dec
[LN18]	2*MtA	MtA
[GG18, CCL+20,YXC21]	4*MtA	Fast
[DKLS18]	2~3*MtA	Optimal
[CGG+20, DKLS19]	4*MtA	Optimal



Previous works （ in case t =2 ）

Schemes	Offline	Online
[Lin17, CCL+19]	Enc	Dec
[LN18]	2*MtA	MtA
[GG18, CCL+20,YXC21]	4*MtA	Fast
[DKLS18]	2~3*MtA	Optimal
[CGG+20, DKLS19]	4*MtA	Optimal

Costly

Paillier	~10ms	~1KB
CL	~200ms	~200B

Multi-to-Add protocol

Paillier	~240ms	~9KB
CL	~1200ms	~2KB
OT	cheap	~90KB

What we could do, and have done

Schemes	Offline	Online
[Lin17,CCL+19]	Enc	Dec
[LN18]	2*MtA	MtA
[GG18, CCL+20,YCX21]	4*MtA	Fast
[DKLS18]	2~3*MtA	Optimal
[CGG+20, DKLS19]	4*MtA	Optimal
?	1*MtA	Optimal

Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient friendly Two-party ECDSA. ACM CCS 2021

What we could do, and have done

Schemes	Offline	Online
[Lin17,CCL+19]	Enc	Dec
[LN18]	2*MtA	MtA
[GG18, CCL+20,YCX21]	4*MtA	Fast
[DKLS18]	2~3*MtA	Optimal
[CGG+20, DKLS19]	4*MtA	Optimal
Our work: 2ECDSA	1*MtA	Optimal

Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient friendly Two-party ECDSA. ACM CCS 2021

State-of-the-art in Industry

ZenGo X

Multi-party ECDSA

build passing License GPL v3

This project is a Rust implementation of {t,n}-threshold ECDSA (elliptic curve digital signature algorithm).

Threshold ECDSA includes two protocols:

- Key Generation for creating secret shares.
- Signing for using the secret shares to generate a signature.

ECDSA is used extensively for crypto-currencies such as Bitcoin, Ethereum (secp256k1 curve), NEO (NIST P-
curve) and much more. This library can be used to create MultiSig and ThresholdSig crypto wallet. For a full

https://github.com/ZenGo-X/multi-party-ecdsa

State-of-the-art in Industry

Coinbase

The generic protocol interface pkg/core/protocol/protocol.go. T
implementation.

- Cryptographic Accumulators
- Bulletproof
- Oblivious Transfer
  - Verifiable Simplest OT
  - KOS OT Extension
- Threshold ECDSA Signature
  - DKLs18 - DKG and Signing
  - GG20 - DKG
  - GG20 - Signing
- Threshold Schnorr Signature
  - FROST threshold signature - DKG
  - FROST threshold signature - Signing

https://github.com/coinbase/kryptology

Government-NIST

2023 2024? 1st 2025? 2ed

Contribute to NIST's Threshold standardization?

Presentation from NIST at CRYPTO 2022

Applications

- Threshold signature could be used to enhance security whenever a signature is used.

- Direct applications
  - Blockchain-based cryptocurrency
  - NFT (non-fungible token)

- Authentication
  - Certificate authentication (CA)
  - etc.

Take-home points

- In cryptocurrency, we should protect the private key
- Threshold cryptography (especially, ECDSA) can provide a high level of private key protection
- It involves several cryptographic tools (homomorphic enc, oblivious transfer, etc.)
- More efforts should be done to standardize threshold schemes.

Thank you
Q & A

Emails to haiyangxc@gmail.com are welcome.

Reference

- [XAX+21] Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient Online-friendly Two-Party ECDSA Signature. ACM CCS 2021
- [YCX21] Tsz Hon Yuen, Handong Cui, and Xiang Xie. Compact Zero-Knowledge Proofs for Threshold ECDSA with Trustless Setup. PKC 2021
- [CGG+20] Ran Canetti, Rosario Gennaro, Steven Goldfeder, Nikolaos Makriyannis, and Udi Peled. UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts. ACM CCS 2020
- [CCL+20] Guilhem Castagnos, Dario Catalano, Fabien Laguillaumie, Federico Savasta, and Ida Tucker. 2020. Bandwidth-efficient threshold ECDSA. PKC 2020
- [CCL+19] Guilhem Castagnos, Dario Catalano, Fabien Laguillaumie, Federico Savasta, and Ida Tucker. 2019. Two-party ECDSA from hash proof systems and efficient instantiations. CRYPTO 2019
- [DKLS18] Jack Doerner, Yashvanth Kondi, Eysa Lee, and Abhi Shelat. Secure two-party threshold ECDSA from ECDSA assumptions. IEEE S&P 2018
- [DKLS19] Jack Doerner, Yashvanth Kondi, Eysa Lee, and Abhi Shelat.Threshold ECDSA from ECDSA assumptions: the multiparty case. IEEE S&P 2019
- [GG18] Rosario Gennaro and Steven Goldfeder. Fast multiparty threshold ECDSA with fast trustless setup. ACM CCS 2018
- [LN18] Yehuda Lindell and Ariel Nof. Fast secure multiparty ECDSA with practical distributed key generation and applications to cryptocurrency custody. ACM CCS 2018
- [Lin17] Yehuda Lindell. Fast secure two-party ECDSA signing. CRYPTO 2017

Preliminary: Homomorphic Encryption

- Additive Homomorphic Encryption Scheme:

$$\mathrm{Enc}(m_1 + m_2) = \mathrm{Enc}(m_1) \oplus \mathrm{Enc}(m_2)$$

$$\mathrm{Enc}(a \cdot m) = \mathrm{Enc}(m)^a = a \odot \mathrm{Enc}(m)$$

Schemes	over	Message Space
Paillier	Z_{N^2} (N is RSA modulus)	Z_N
CL Encryption	Class group	Z_q ($=\#G$)

Paillier Encryption

- Let $N = pq$ be RSA modulus. Secret key: $\phi(N)$ public key : N

$$\mathrm{Enc}(m) = \mathrm{c} = (1 + \mathrm{N})^m \, r^N \; mod \; N^2$$

$$\mathrm{c}^{\phi(N)} = 1 + m \, \phi(N) N \;\; mod \; N^2$$

Oblivious Transfer (OT)

OT is a fundamental primitive of multiparty computation (MPC).