PUKYONG NATIONAL UNIVERSITY

Implicit Authentication in Neural Key Exchange Based on the Randomization of the Public Blockchain

Siwan Noh, and Kyung-Hyune Rhee

Pukyong National University(PKNU), S.Korea

Key Exchange Algorithm

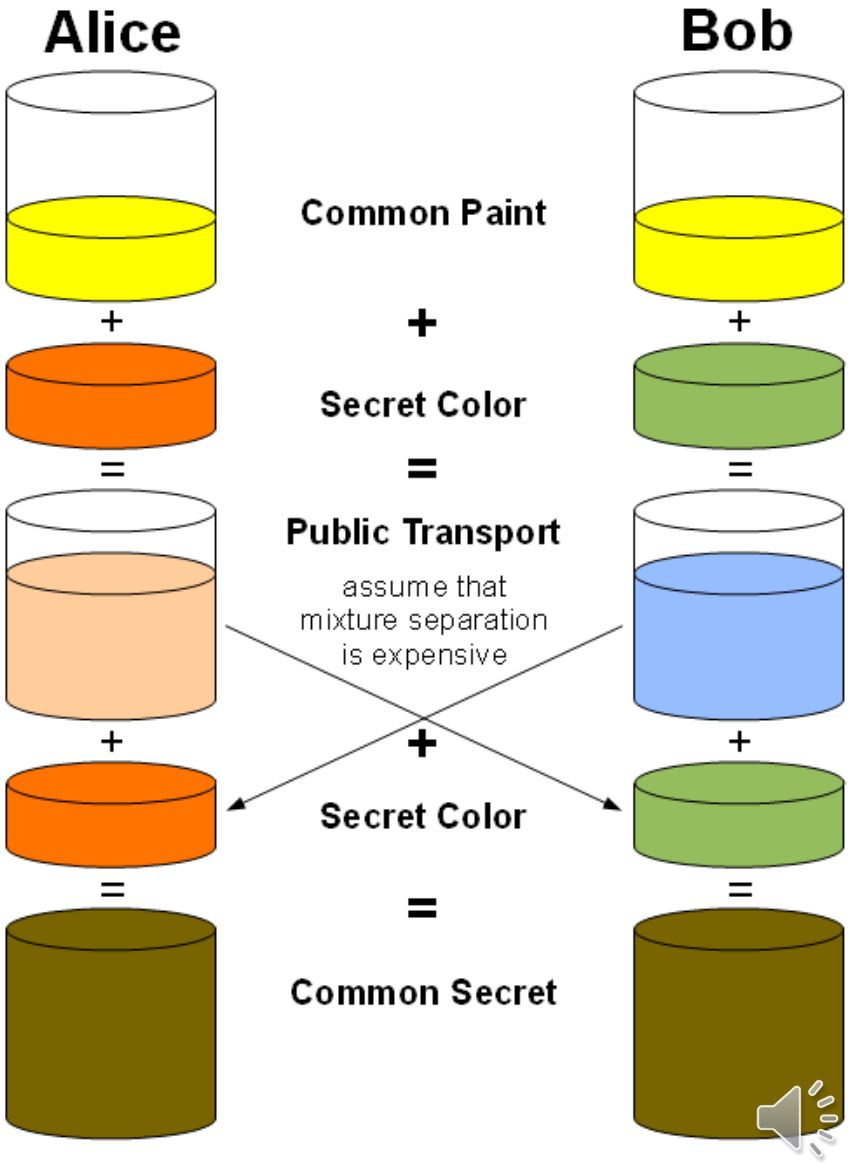
- Key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

How can we exchange keys in an unreliable network?

Diffie-Hellman Key Exchange

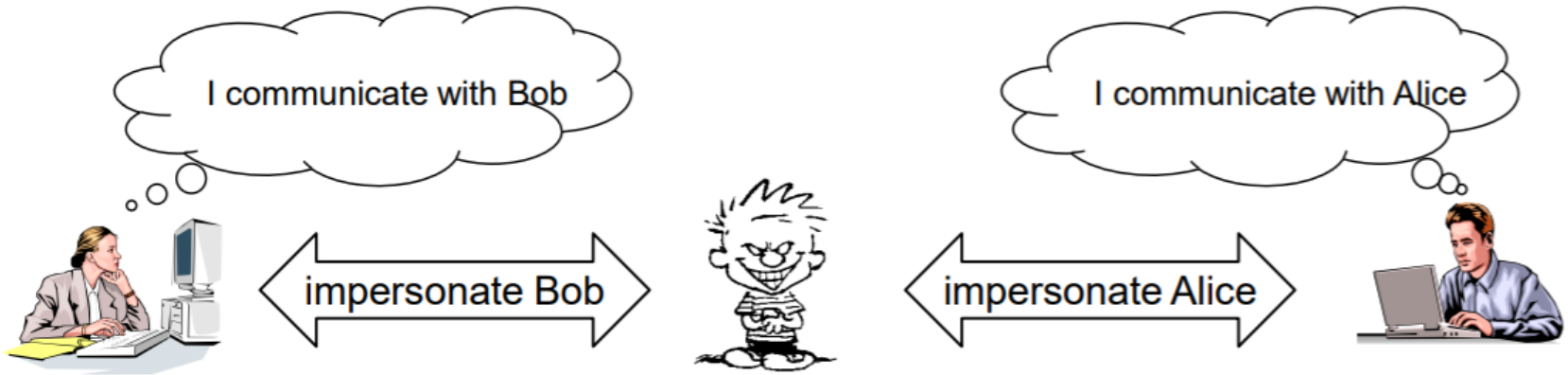
- DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography

- the logarithm $\log_b a$ is a number x such that $b^x = a$
  - no efficient method is known for computing them



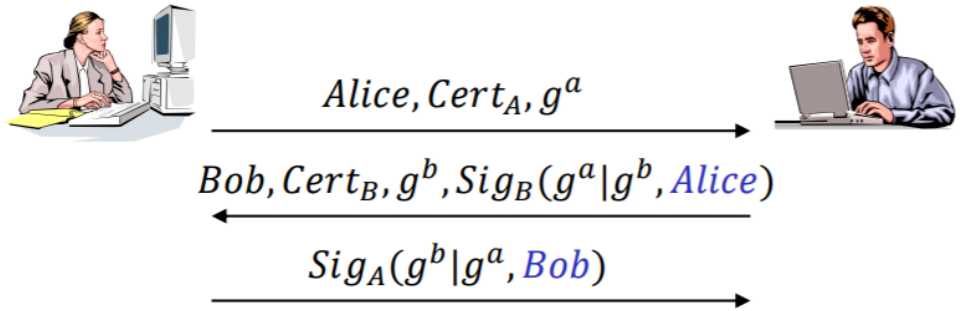
Man-In-The-Middle Attack

- the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other
  - Suppose Alice wishes to communicate with Bob.
  - Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and optionally to deliver a false message to Bob.



Authenticated Key Exchange

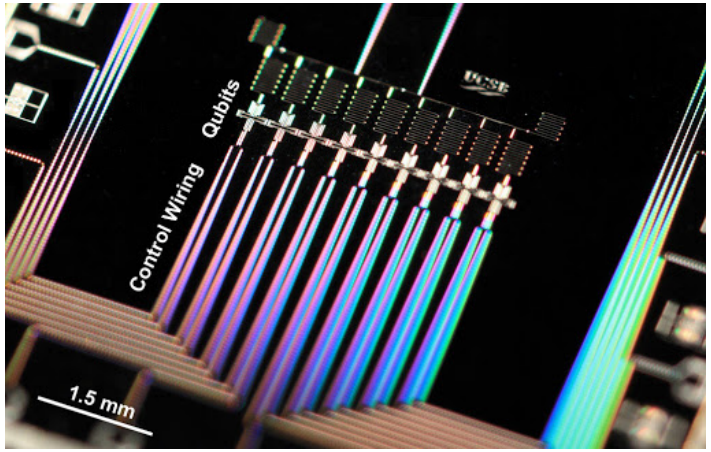
- Authenticated Key Exchange (AKE) is the exchange of session key in a key exchange protocol which also authenticate the identities of parties involved in the key exchange
  - use digital signature and certificate for authentication



- Authenticity problem of public key is often solved by public key certificate
  - bind a public key to owner's identity
  - digitally signed by a trusted authority called CA

Quantum Computing

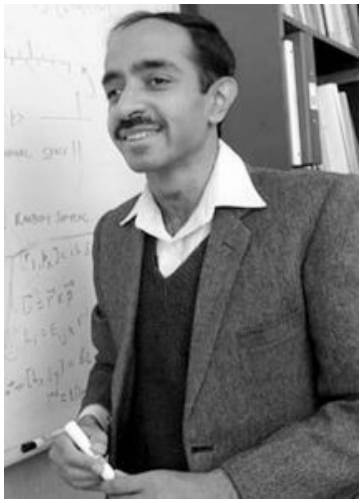
- Quantum computing is the use of quantum phenomena such as superposition and entanglement to perform computation
- Quantum computers are believed to be able to solve certain computational problems
  - Integer factorization, Discrete logarithm



Quantum Algorithm

Algorithm	Function	Security Level	
		Pre-quantum	Post-quantum
AES-128	Encryption	128	64(Grover)
AES-256	Encryption	256	128(Grover)
Salsa20	Encryption	256	128(Grover)
GMAC	MAC	128	128
Poly1305	MAC	128	128
SHA-256	Hash	256	128(Grover)
SHA3-256	Hash	256	128(Grover)
RSA-3072	Encryption	128	Broken(Shor)
RSA-3072	Signature	128	Broken(Shor)
DH-3072	Key Exchange	128	Broken(Shor)
DSA-3072	Signature	128	Broken(Shor)
256bit ECDH	Key Exchange	128	Broken(Shor)
256bit ECDSA	Signature	128	Broken(Shor)

Peter Shor



Lov Grover

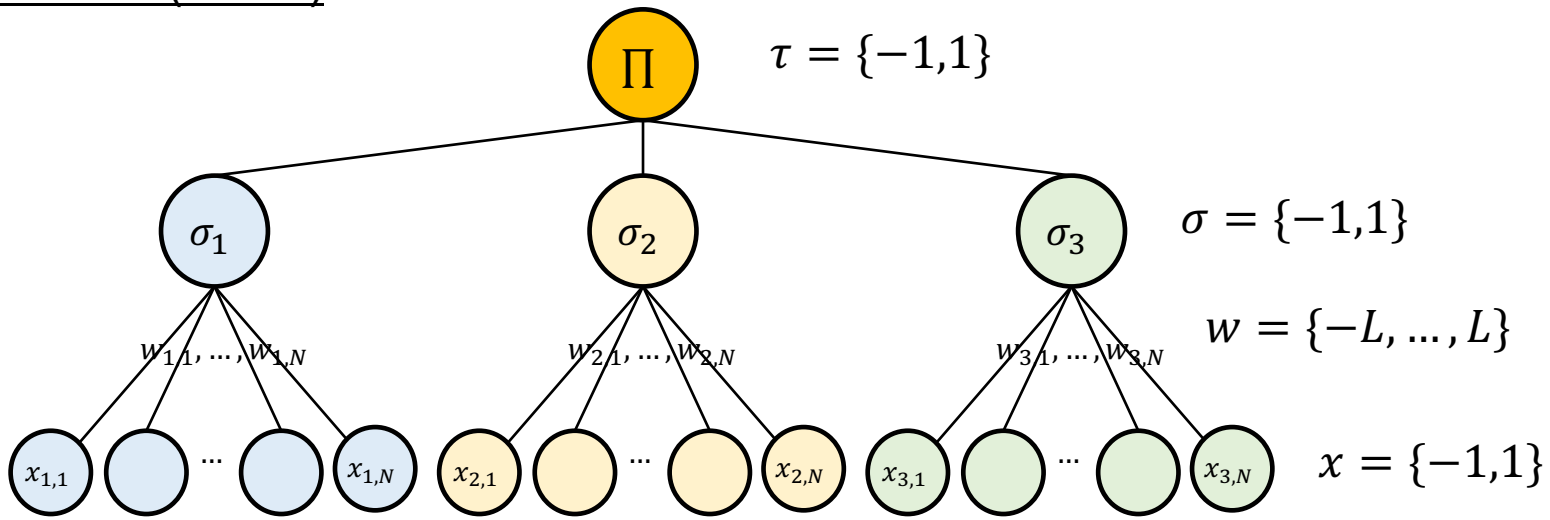
Post Quantum Cryptography

Post-quantum cryptography refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer

✓ Lattice-based, Multivariate, Hash-based, Code-based, Supersingular elliptic curve, etc.

Neural Key Exchange

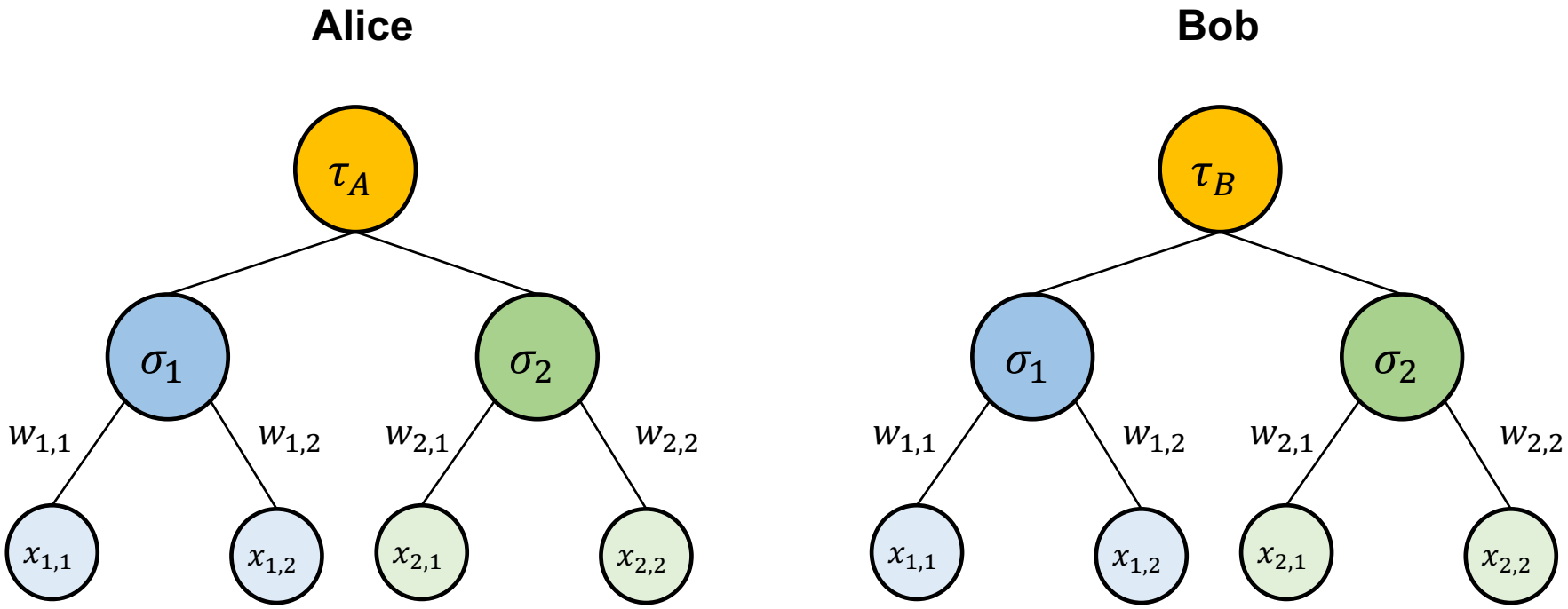
- The mechanism behind neural cryptography is similar to secret key agreement though public discussion
  - Neural key exchange, which is based on the synchronization of two tree parity machines(TPMs)



$$\tau(t) = \prod_{k=1}^{K} sgn\left(\sum_{i=1}^{N} w_{k,i}(t)x_{k,i}(t)\right)$$

$$w_{k,i}^{AB}(t+1) = \begin{cases} w_{k,i}^{AB}(t) + \tau^{A}(t)x_{k,i}(t) & , \tau^{A}(t) = \tau^{B}(t) \\ w_{k,i}^{AB}(t) & , otherwise \end{cases}$$

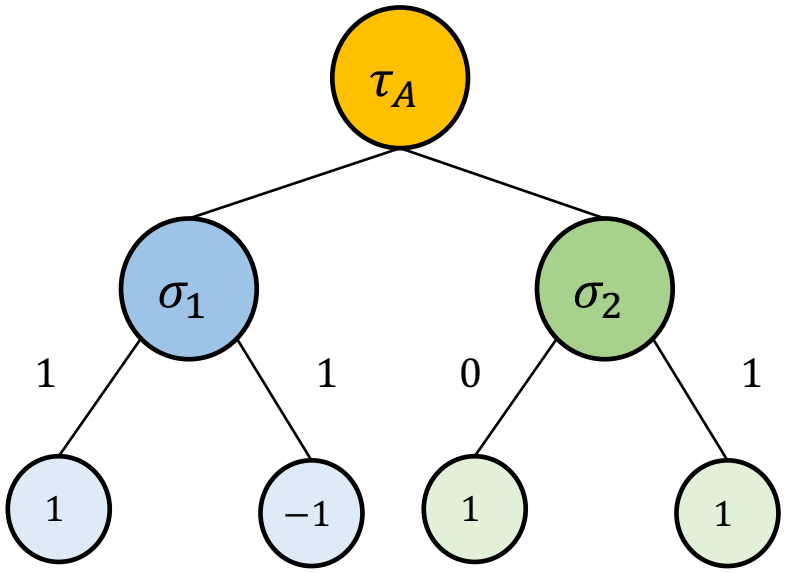
NKE Example



- ✓ number of hidden unit : $K = 2$
- ✓ number of input vector : $N = 2$
- ✓ maximum value for weight : $L = 1$

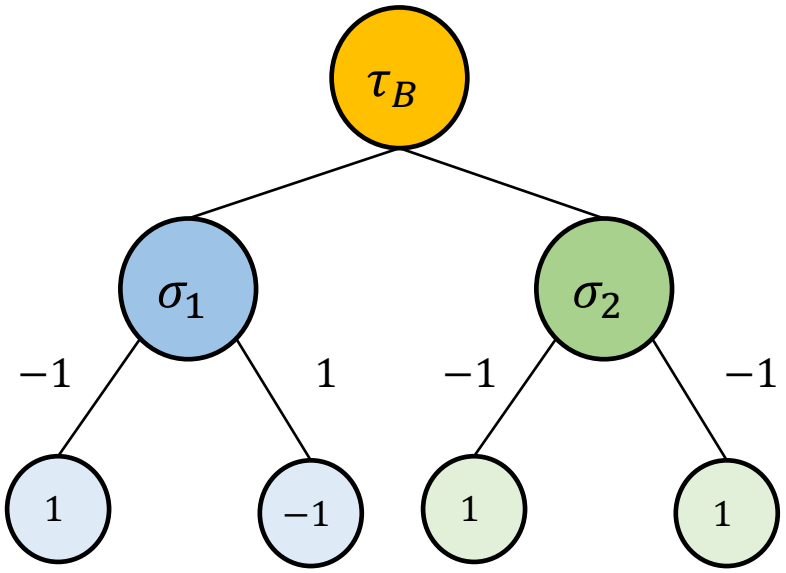
NKE Example : Round 1

Alice



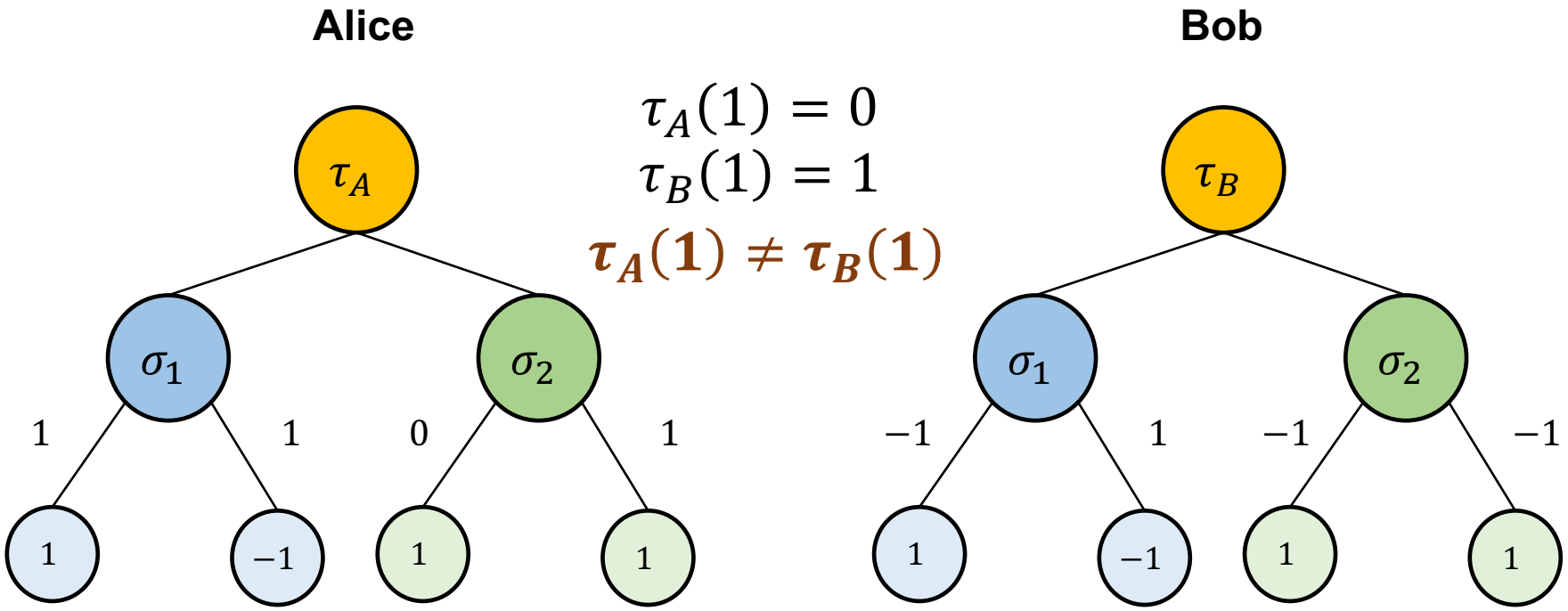
$$\tau_A(1) = \prod_{k=1}^{2} sgn\left(\sum_{i=1}^{2} w_{k,i}(1)x_{k,i}(1)\right) = 0$$

Bob



$$\tau_B(1) = \prod_{k=1}^{2} sgn\left(\sum_{i=1}^{2} w_{k,i}(1)x_{k,i}(1)\right) = 1$$

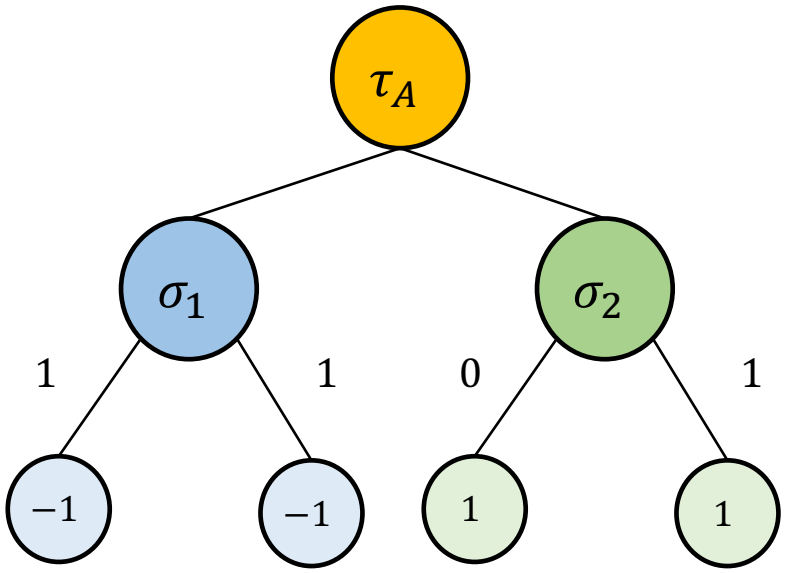
NKE Example : Round 1 – Weight Update



weights W_A and W_B are not changed

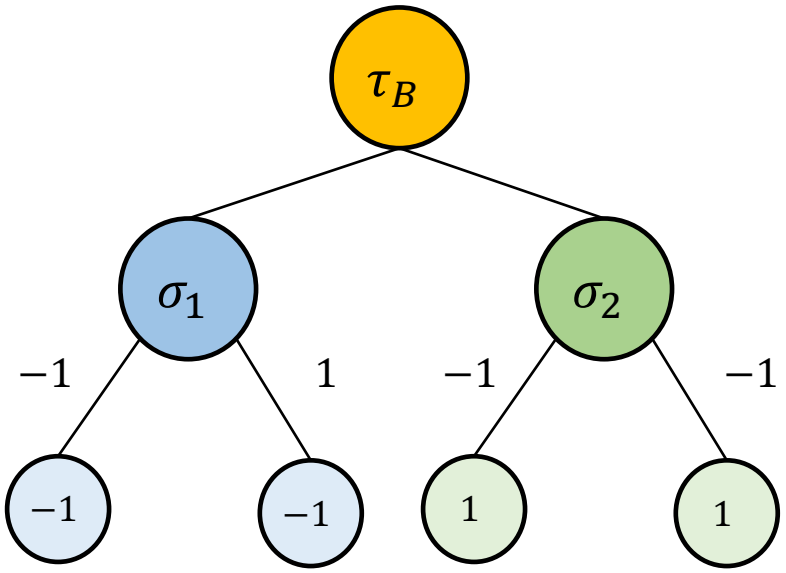
NKE Example : Round 2

Alice



$$\tau_A(2) = \prod_{k=1}^{2} sgn\left(\sum_{i=1}^{2} w_{k,i}(1)x_{k,i}(1)\right) = -1$$

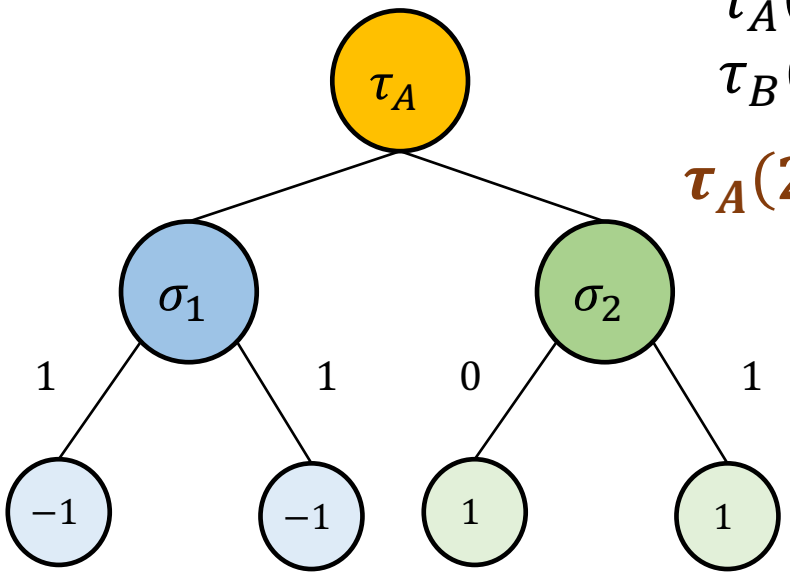
Bob



$$\tau_B(2) = \prod_{k=1}^{2} sgn\left(\sum_{i=1}^{2} w_{k,i}(1)x_{k,i}(1)\right) = -1$$

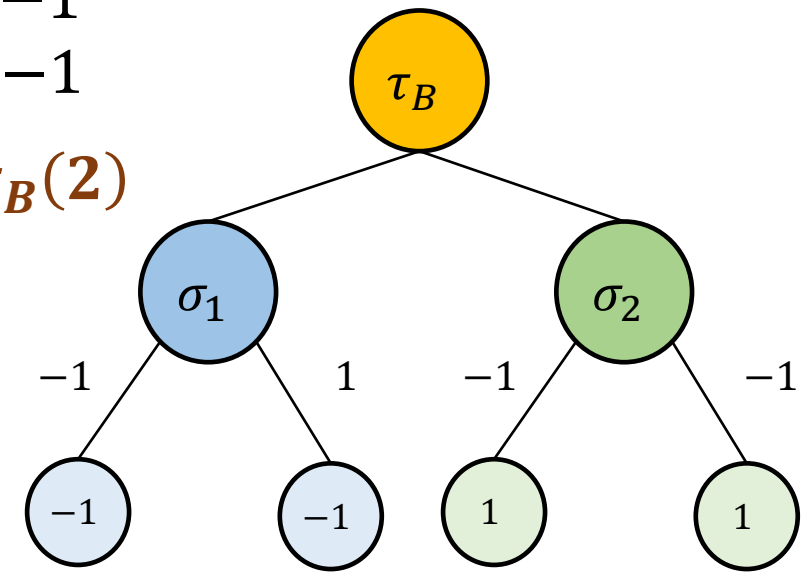
NKE Example : Round 2 – Weight Update

Alice



$$\tau_A(2) = -1$$
$$\tau_B(2) = -1$$
$$\boldsymbol{\tau_A(2) = \tau_B(2)}$$

Bob



- ✓ $w_{A_{1,1}} = 1$
- ✓ $w_{A_{1,2}} = 1$
- ✓ $w_{A_{2,1}} = -1$
- ✓ $w_{A_{2,2}} = 0$

- ✓ $w_{B_{1,1}} = 0$
- ✓ $w_{B_{1,2}} = 1$
- ✓ $w_{B_{2,1}} = -1$
- ✓ $w_{B_{2,2}} = -1$

NKE Example : Round 2 – Weight Update

- Weight Distance
  - Before Updating

✓ $w_{A_{1,1}} = 1$	✓ $w_{B_{1,1}} = -1$	✓ $Distance(w_{A_{1,1}}, w_{B_{1,1}}) = 2$
✓ $w_{A_{1,2}} = 1$	✓ $w_{B_{1,2}} = 1$	✓ $Distance(w_{A_{1,2}}, w_{B_{1,2}}) = 0(\text{Synchronized})$
✓ $w_{A_{2,1}} = 0$	✓ $w_{B_{2,1}} = -1$	✓ $Distance(w_{A_{2,1}}, w_{B_{2,1}}) = 1$
✓ $w_{A_{2,2}} = 1$	✓ $w_{B_{2,2}} = -1$	✓ $Distance(w_{A_{2,2}}, w_{B_{2,2}}) = 2$

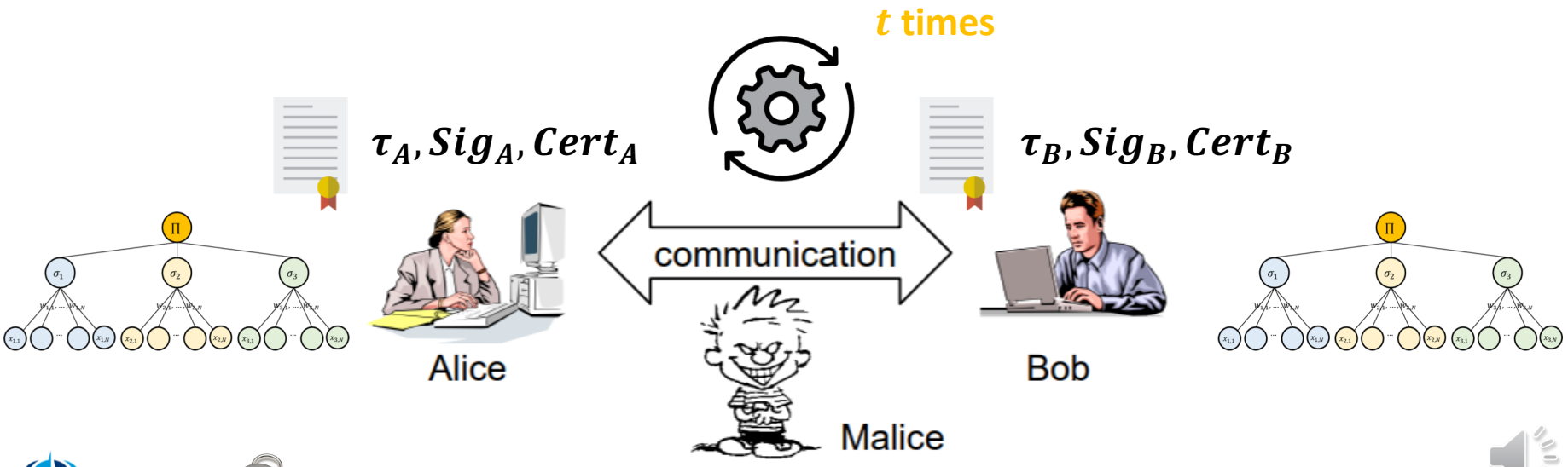
  - After Updating

✓ $w_{A_{1,1}} = 1$	✓ $w_{B_{1,1}} = 0$	✓ $Distance(w_{A_{1,1}}, w_{B_{1,1}}) = 1$
✓ $w_{A_{1,2}} = 1$	✓ $w_{B_{1,2}} = 1$	✓ $Distance(w_{A_{1,2}}, w_{B_{1,2}}) = 0(\text{Synchronized})$
✓ $w_{A_{2,1}} = -1$	✓ $w_{B_{2,1}} = -1$	✓ $Distance(w_{A_{2,1}}, w_{B_{2,1}}) = 0(\text{Synchronized})$
✓ $w_{A_{2,2}} = 0$	✓ $w_{B_{2,2}} = -1$	✓ $Distance(w_{A_{2,2}}, w_{B_{2,2}}) = 1$

Attack of NKE

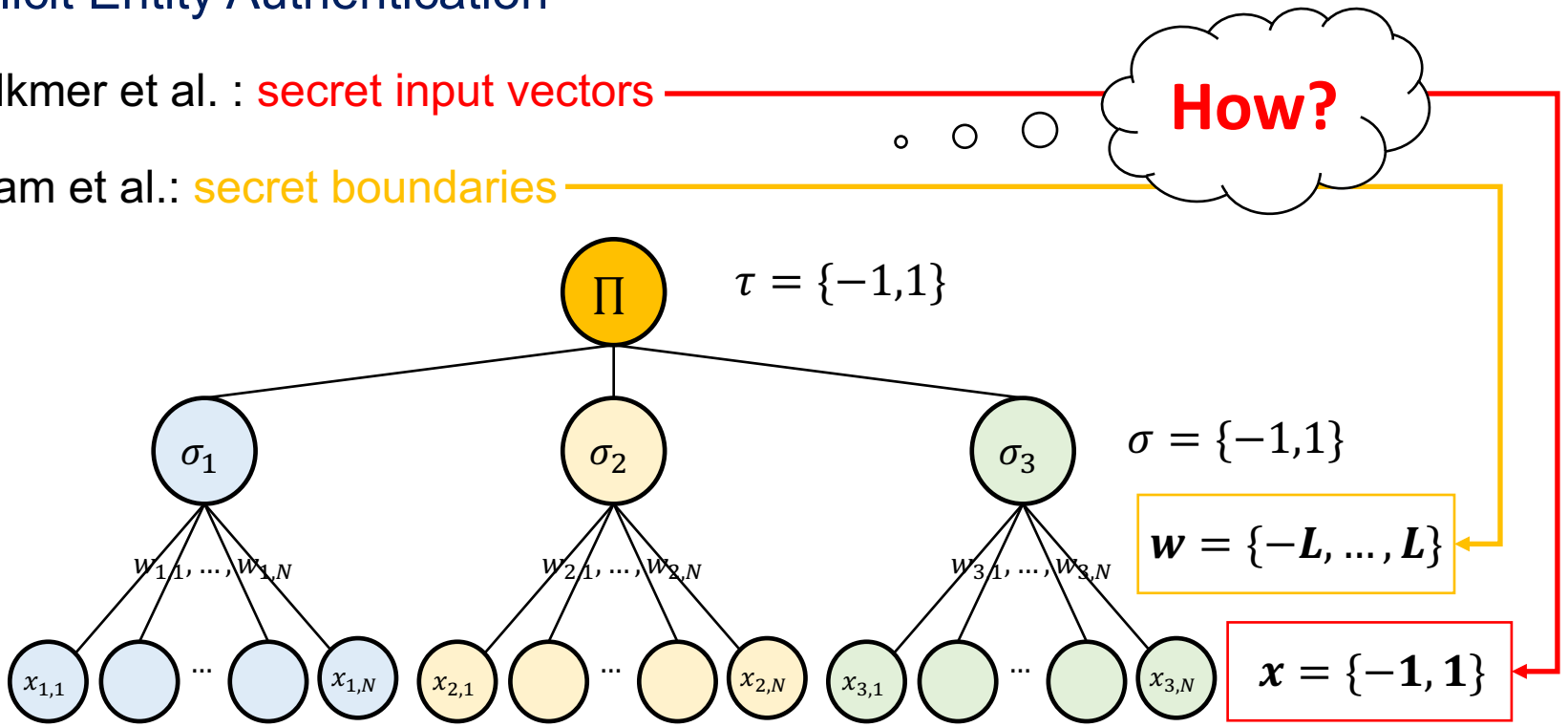
- the attacker E can eavesdrop messages between the parties A and B
  - He can synchronize his tree parity machine with these two parties

- Problem : no authentication between the parties
  - explicit entity authentication : digital signature and certificate



Authenticated Neural Key Exchange

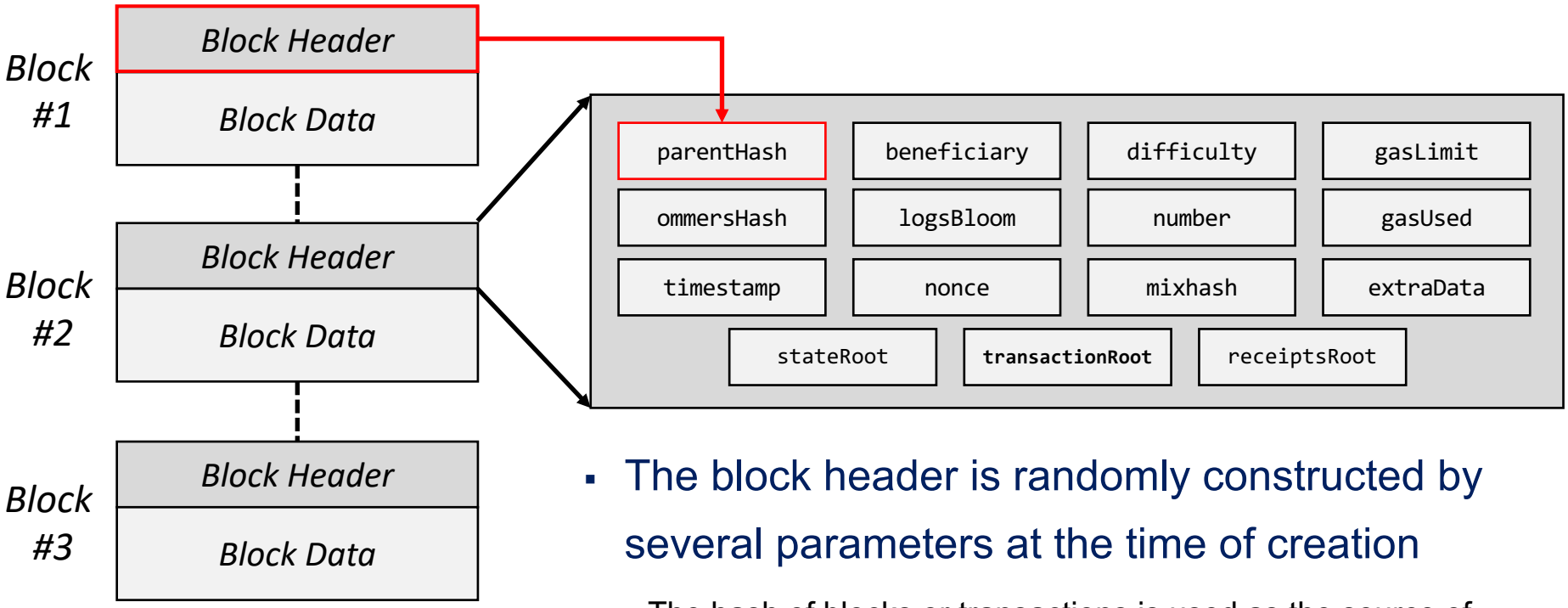
- Implicit Entity Authentication
  - Volkmer et al. : secret input vectors
  - Allam et al.: secret boundaries



- M. Volkmer, "Entity Authentication and Authenticated Key Exchange with Tree Parity Machines." IACR Cryptol. ePrint Arch., vol. 2006, p. 112, 2006.
- A. M. Allam, H. M. Abbas, and M. W. El-Kharashi, "Authenticated key exchange protocol using neural cryptography with secret boundaries," in The 2013 International Joint Conference on Neural Networks (IJCNN). IEEE, 2013, pp. 1–8.

Blockchain

- A blockchain is a growing list of records that are linked using cryptography
  - Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data



- The block header is randomly constructed by several parameters at the time of creation
  - The hash of blocks or transactions is used as the source of randomness

Solution #1 : Simple Transaction

- Use the block header containing the transaction as an authentication secret
  - If we assume that the attacker Eve knows the address of the blockchain of the two users

Transactions

For Block 11110314

Sponsored: - AAX - AAX - 5%+ interest rate on BTC saving. Visit AAX.com now!

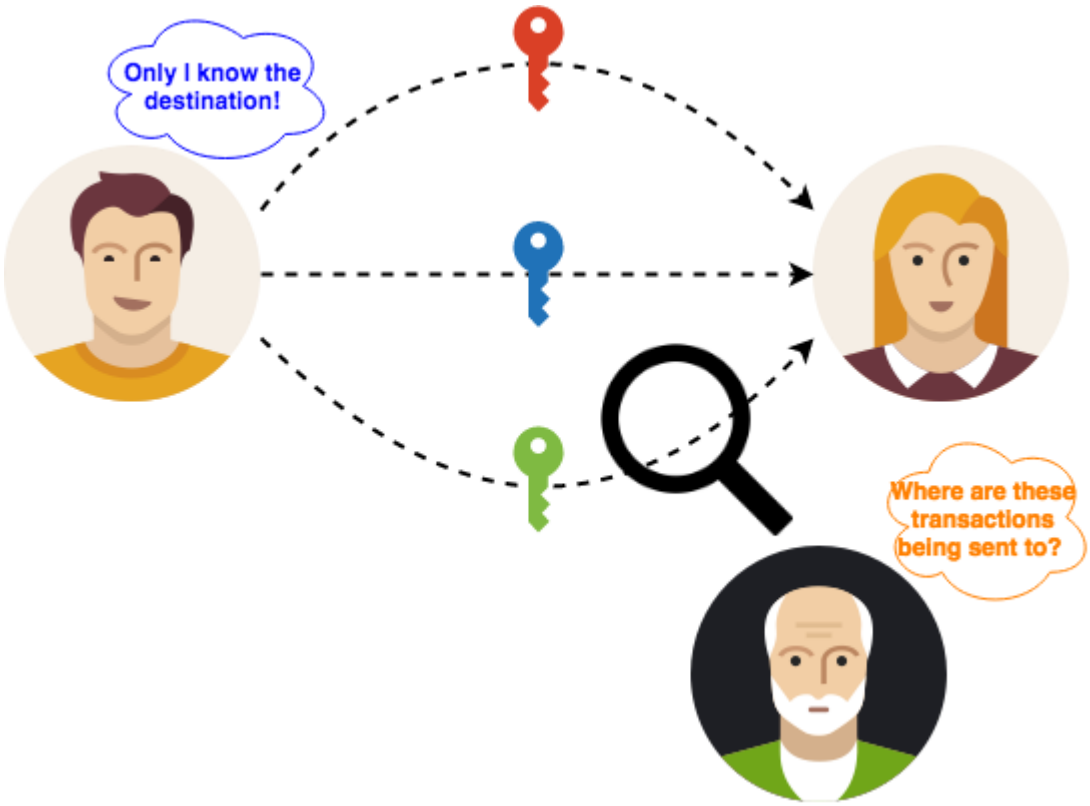
A total of 190 transactions found

First | Page 1 of 4 | Last

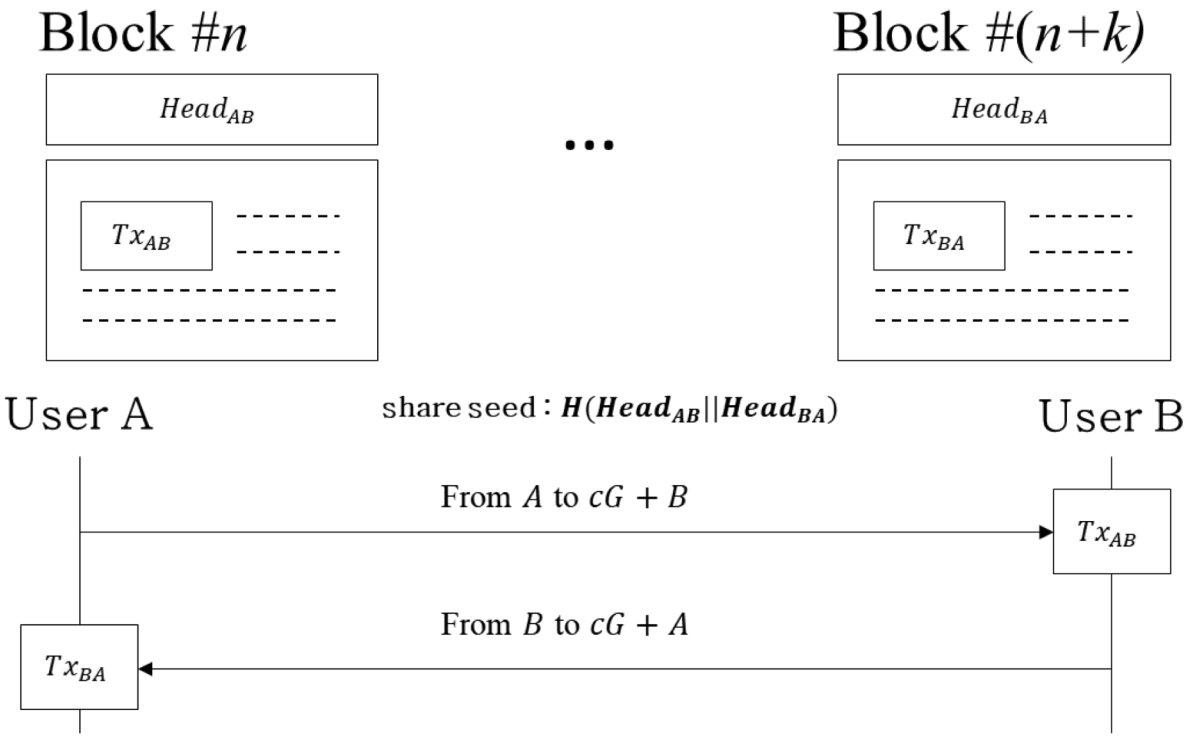
Txn Hash	Block	Age	From	To	Value	[Txn Fee]
0x61c950bbc95ea3b53...	11110314	1 min ago	0x861c2079fc1a7893f3...	0x3e7650b09391e5b52...	0.001822526035404 Ether	0.000525
0xa27714d7880b72c8b...	11110314	1 min ago	0xafa6259364f61c8323...	0xd3167dac1df2b661b...	0.001811476 Ether	0.000525
0xa87d49c3c5302b584...	11110314	1 min ago	0x95d794faad48bacd5...	Tether: USDT Stablecoin	0 Ether	0.00107112
0x7ed65e5dadc07bb39...	11110314	1 min ago	0x9732e2fd9c4557570...	0x7d433ca5b0d4f4edfa...	0 Ether	0.00360288
0xeabe73a7f128d0c61...	11110314	1 min ago	0xadf9f58b9fbf16af15e...	0x227e57c7b302d6610...	0.001370247 Ether	0.00063

Solution #2 : Anonymous Transaction

- Stealth Address
  - a privacy-enhancing technology for protecting the privacy of receivers of cryptocurrencies
    - ✓ the sender creates random, one-time address for every transaction



Security Analysis



Tx_{AB}

From: A's Address

to: B's Stealth Address

Tx_{BA}

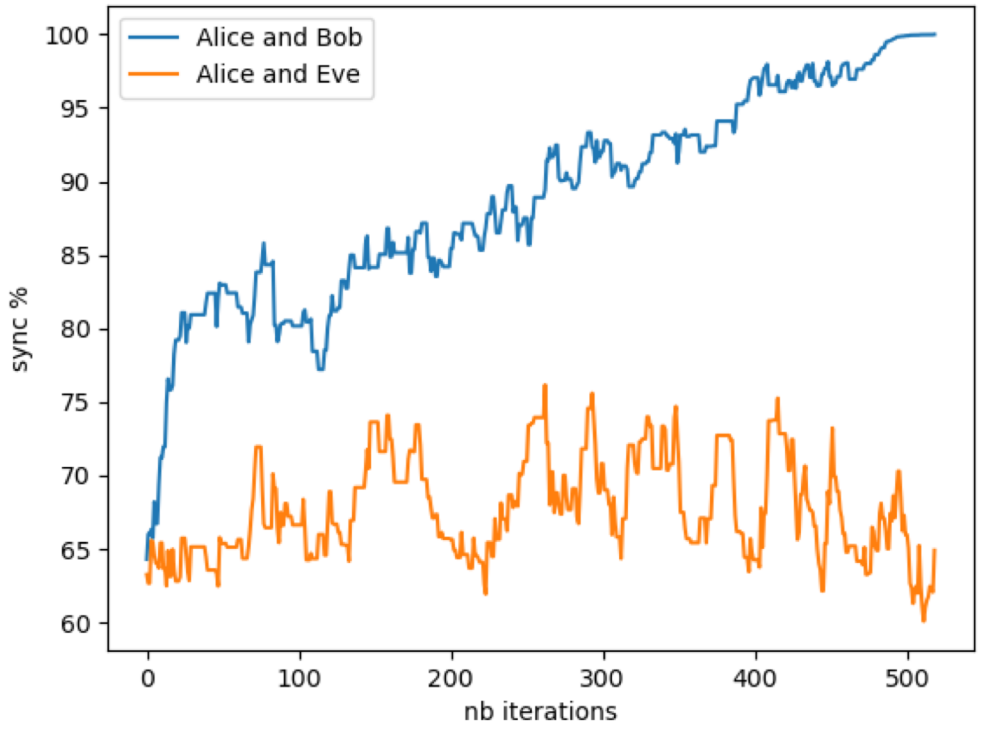
From: B's Address

to: A's Stealth Address

- User A
  - knows B's Address
  - can calculate A's Stealth Address
    B's Stealth Address
- User B
  - knows A's Address
  - can calculate A's Stealth Address
    B's Stealth Address
- Attacker E
  - knows A's Address
    B's Address

PUKYONG NATIONAL UNIVERSITY

Evaluation



- ✓ number of hidden unit : $K = 20$
- ✓ number of input vector : $N = 50$
- ✓ maximum value for weight : $L = 6$

Summary

- Implicit Entity Authentication in NKE
  - We propose the idea of establishing a second secret value using blockchain
    - ✓ implicit entity authentication
  - The strong security of the public blockchain can ensure transparent randomness in the trustless network

Thank You!

Siwan Noh : nosiwan@pukyong.ac.kr