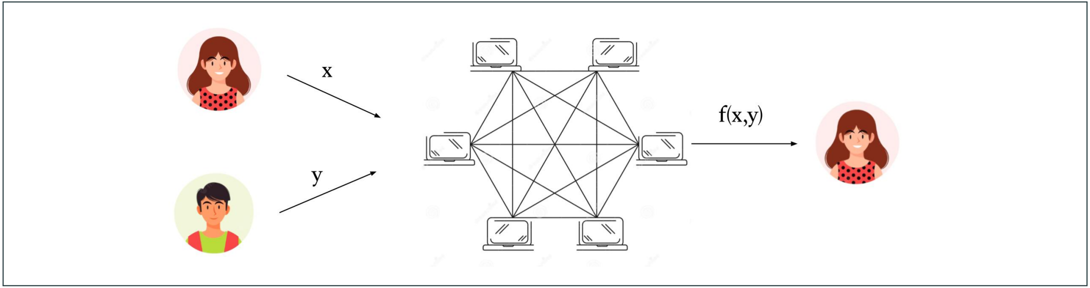
Encryption to the Future

A Paradigm for Sending Secret Messages to Future (Anonymous) Committees

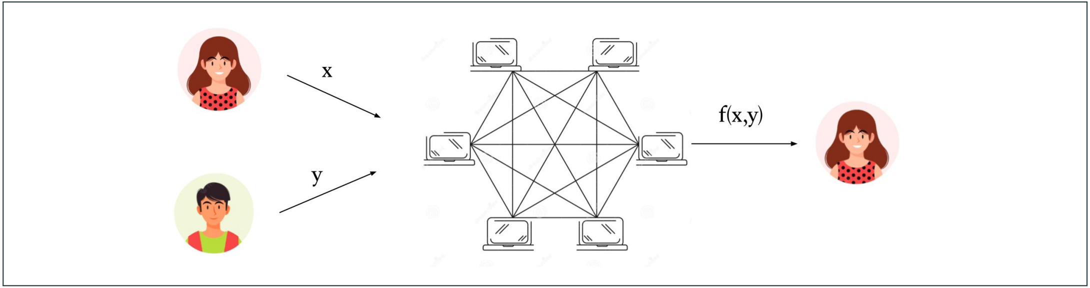
Matteo Campanelli, Bernardo David, Hamidreza Khoshakhlagh,
Anders Konring, Jesper Buus Nielsen

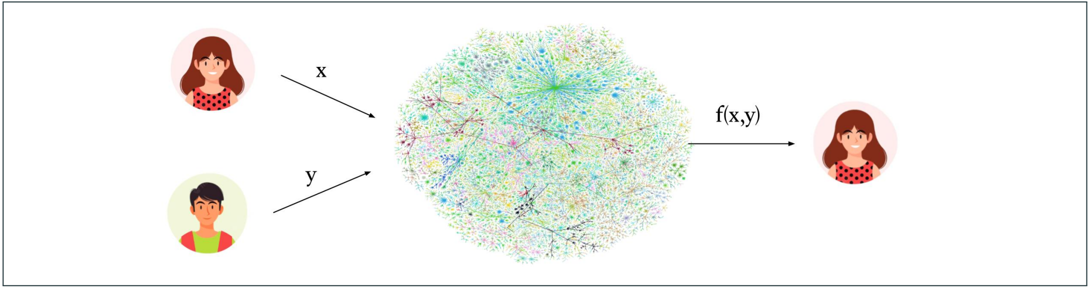
December 8, 2022

Application: Large-Scale MPC on Public Blockchains



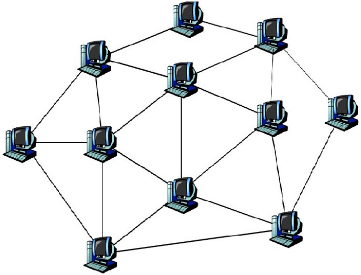
Application: Large-Scale MPC on Public Blockchains





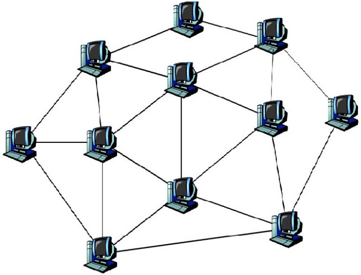
Application: Large-Scale MPC on Public Blockchains

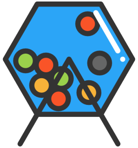
- High-level: (incentivized) coordination platform for miners/stakeholders.
- Blockchains are large public, dynamic P2P networks.
- Built-in consensus layer



Application: Large-Scale MPC on Public Blockchains

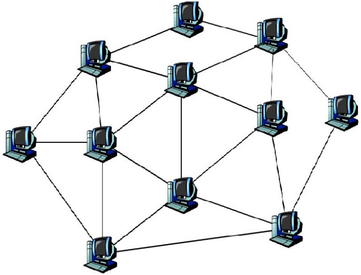
- High-level: (incentivized) coordination platform for miners/stakeholders.
- Blockchains are large public, dynamic P2P networks.
- Built-in consensus layer
    - implements a "lottery" mechanism

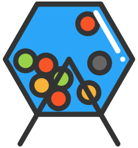




Application: Large-Scale MPC on Public Blockchains

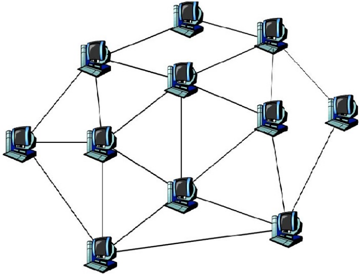
- High-level: (incentivized) coordination platform for miners/stakeholders.
- Blockchains are large public, dynamic P2P networks.
- Built-in consensus layer
  - implements a ”lottery” mechanism
  - implements total-ordered broadcast

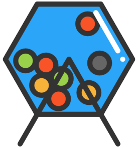




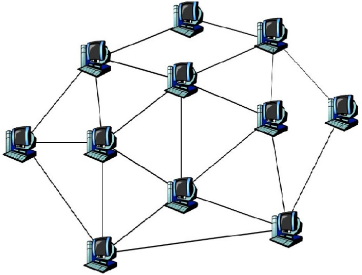
Application: Large-Scale MPC on Public Blockchains

- High-level: (incentivized) coordination platform for miners/stakeholders.
- Blockchains are large public, dynamic P2P networks.
- Built-in consensus layer
    - implements a ”lottery” mechanism
    - implements total-ordered broadcast
- Can we repurpose the blockchain infrastructure to orchestrate MPC?

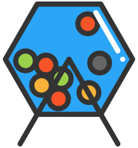




Application: Large-Scale MPC on Public Blockchains



- High-level: (incentivized) coordination platform for miners/stakeholders.
- Blockchains are large public, dynamic P2P networks.
- Built-in consensus layer
  - implements a ”lottery” mechanism
  - implements total-ordered broadcast
- Can we repurpose the blockchain infrastructure to orchestrate MPC?
- YES! [BGG$^+$20, GHK$^+$21, CGG$^+$21]



Application: Large-Scale MPC on Public Blockchains

YOSO MPC [GHK$^+$21]

- Mobile Adversary - imposes requirements on the protocol
  - Limited Interaction Pattern (Only Speak Once)
  - Protocol parties are selected at random and are anonymous until they speak

Application: Large-Scale MPC on Public Blockchains

YOSO MPC [GHK$^+$21]

- Mobile Adversary - imposes requirements on the protocol
  - Limited Interaction Pattern (Only Speak Once)
  - Protocol parties are selected at random and are anonymous until they speak
- Attractive Side-effects
  - Support dynamic network (tolerate node churn)
  - Scalability:
    - Large networks allows for sampling small committees with the right distribution (whp.)
    - Sub-linear size committees can carry out the computation on behalf of the network

Application: Large-Scale MPC on Public Blockchains

YOSO MPC [GHK^{+}21]

- Role Execution
  - Execute the steps according to the protocol specification
  - Send messages to future roles (Only Speak Once)
- Role Assignment
  - Associates a machine in the network with a role in the protocol
  - Establishes a receiver-anonymous channel to the machine
  - Cannot rely on "full" WE or Time-Lock puzzles

Application: Large-Scale MPC on Public Blockchains

YOSO MPC [GHK+21]

- Role Execution
  - Execute the steps according to the protocol specification
  - Send messages to future roles (Only Speak Once)
- Role Assignment
  - Associates a machine in the network with a role in the protocol
  - Establishes a receiver-anonymous channel to the machine
  - Cannot rely on "full" WE or Time-Lock puzzles

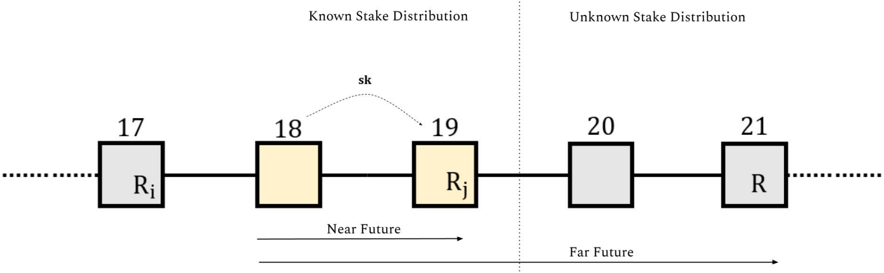
Motivation: Transferring secret state to future committees

- Consider anonymous vs. transparent committee selection.
- Consider secret state to the "near" vs. "far" future.
- Investigate the need for auxiliary committees for carrying state into the future.

Main Contributions

Encryption to the near Future.

1. Instantiate YOSO using EtF with an anonymous lottery.
2. Introduce a relaxed version of WE called "WE over Commitments" (cWE).
3. Construction using cWE based on standard assumptions (OT + GC).



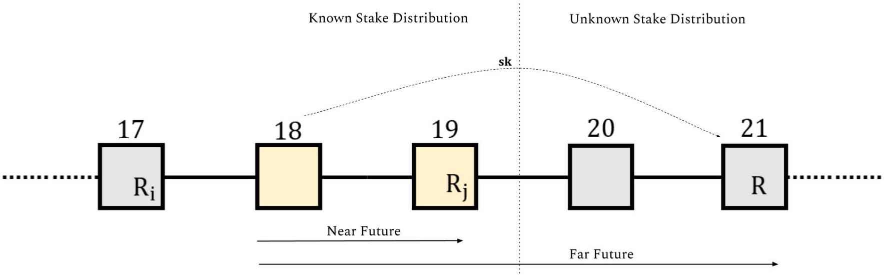
Main Contributions

Encryption to the near Future.

1. Instantiate YOSO using EtF with an anonymous lottery.
2. Introduce a relaxed version of WE called "WE over Commitments" (cWE).
3. Construction using cWE based on standard assumptions (OT + GC).

Encryption to the far Future.

1. No auxiliary committees $\Longrightarrow$ BWE (Blockchain Witness Encryption).



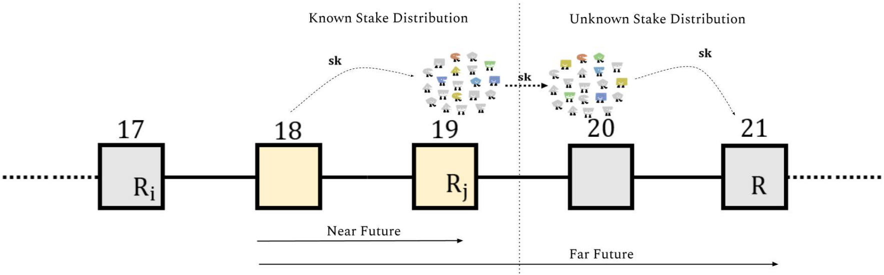
Main Contributions

Encryption to the near Future.

1. Instantiate YOSO using EtF with an anonymous lottery.
2. Introduce a relaxed version of WE called "WE over Commitments" (cWE).
3. Construction using cWE based on standard assumptions (OT + GC).

Encryption to the far Future.

1. No auxiliary committees $\implies$ BWE (Blockchain Witness Encryption).
2. Construction using EtF (near) + TIBE. With minimal use of auxiliary committees (indep. of size/number of messages)



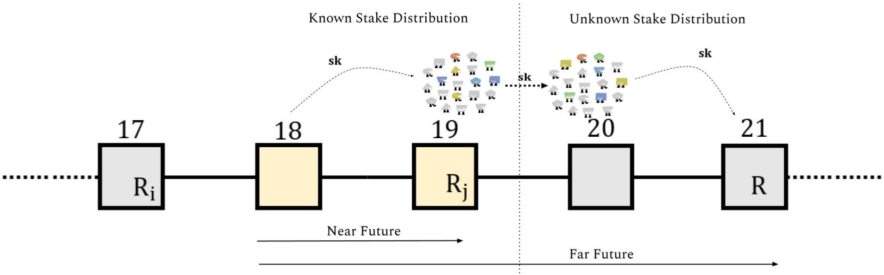
Main Contributions

Encryption to the near Future.

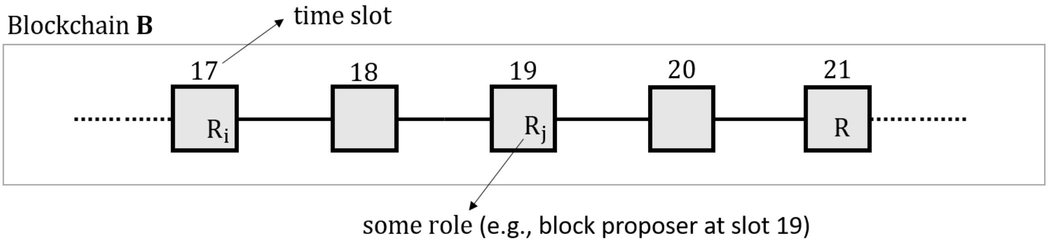
1. Instantiate YOSO using EtF with an anonymous lottery.
2. **Introduce a relaxed version of WE called "WE over Commitments" (cWE).**
3. Construction using cWE based on standard assumptions (OT + GC).

Encryption to the far Future.

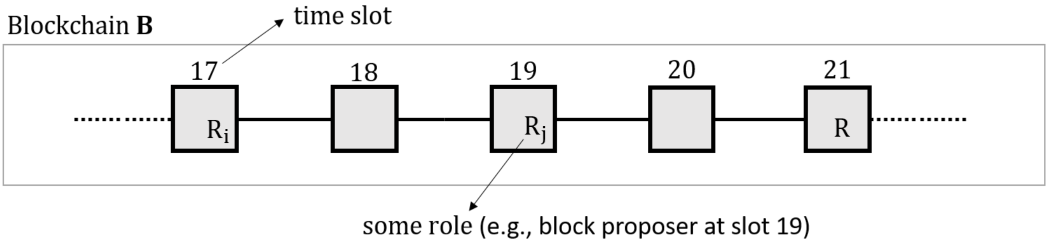
1. No auxiliary committees $\implies$ BWE (Blockchain Witness Encryption).
2. **Construction using EtF (near) + TIBE. With minimal use of auxiliary committees (indep. of size/number of messages)**



Blockchain Lotteries

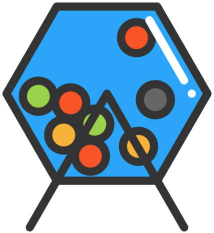


Blockchain Lotteries

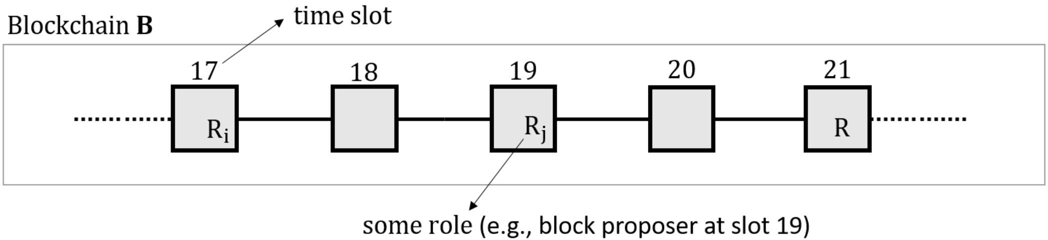


Blockchain Lotteries. A **self-selection** mechanism that gives the winner the right to **play a role** R, e.g.,

- propose a new block for the chain
- introduce new randomness
- become a member of a committee

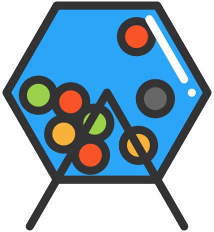


Blockchain Lotteries

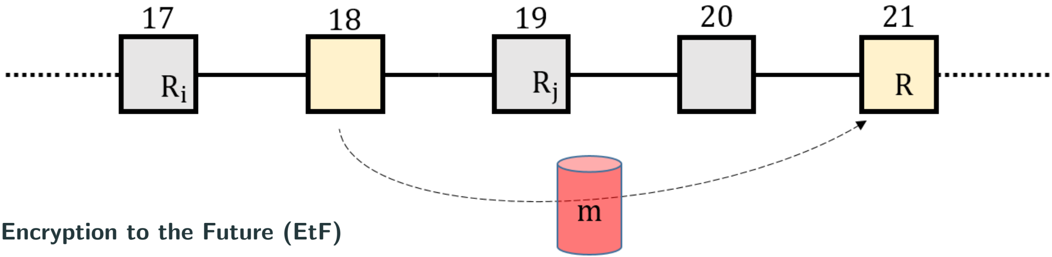


Lottery Predicate. $\text{lottery}(\mathbf{B}, \text{slot}, \text{R}, \text{sk}_i) \in \{0, 1\}$

- Anonymous Lotteries (e.g. Cryptographic Sortition, Nakamoto PoW)
- Transparent Lotteries (e.g. "Follow-the-Satoshi")



Encryption to the Future



Encryption to the Future (EtF)

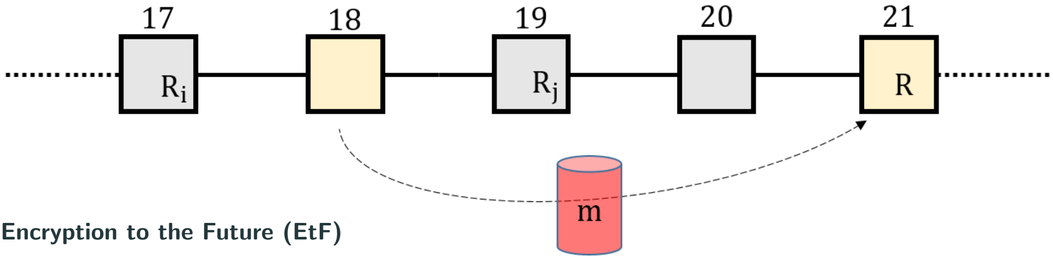
- Encryption w.r.t. $\mathsf{lottery}(\mathbf{B}, \mathsf{slot}, \mathsf{R}, \mathsf{sk})$.

Encryption. $\mathsf{ct} \leftarrow \mathsf{Enc}(\hat{\mathbf{B}}, \mathsf{slot}, \mathsf{R}, m)$

Decryption. $m/\perp \leftarrow \mathsf{Dec}(\tilde{\mathbf{B}}, \mathsf{ct}, \mathsf{sk})$

Outputs m iff $\mathsf{lottery}(\tilde{\mathbf{B}}, \mathsf{slot}, \mathsf{R}, \mathsf{sk}) = 1$

Encryption to the Future



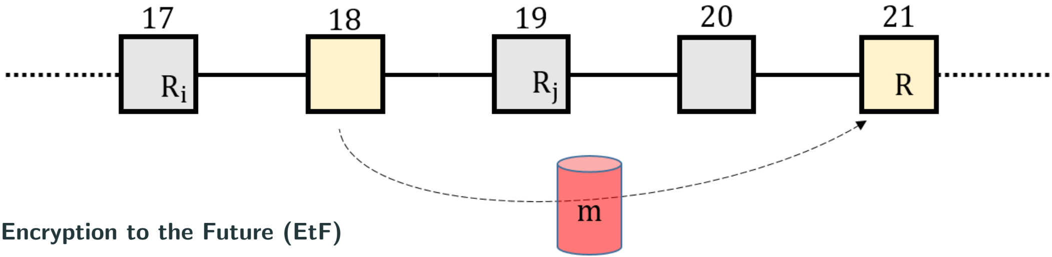
Encryption to the Future (EtF)

- Encryption w.r.t. $\text{lottery}(\mathbf{B}, \text{slot}, \text{R}, \text{sk})$.

  $$\begin{aligned} &\textbf{Encryption.} \quad \text{ct} \leftarrow \text{Enc}(\hat{\mathbf{B}}, \text{slot}, \text{R}, m) \\ &\textbf{Decryption.} \quad m/\perp \leftarrow \text{Dec}(\tilde{\mathbf{B}}, \text{ct}, \text{sk}) \\ &\qquad\qquad\qquad \text{Outputs } m \text{ iff } \text{lottery}(\tilde{\mathbf{B}}, \text{slot}, \text{R}, \text{sk}) = 1 \end{aligned}$$

- $\hat{\mathbf{B}} = \tilde{\mathbf{B}}$ (near future) blockchain state is unchanged. Known stake distribution.

Encryption to the Future



Encryption to the Future (EtF)

- Encryption w.r.t. lottery($\mathbf{B}$, slot, R, sk).

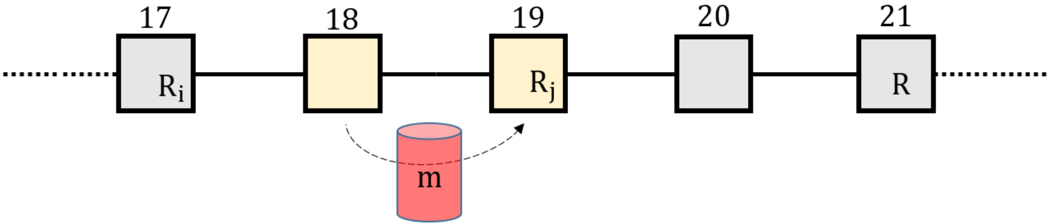
  Encryption. $\mathsf{ct} \leftarrow \mathsf{Enc}(\hat{\mathbf{B}}, \mathsf{slot}, \mathsf{R}, m)$

  Decryption. $m/\perp \leftarrow \mathsf{Dec}(\tilde{\mathbf{B}}, \mathsf{ct}, \mathsf{sk})$
  Outputs m iff $\mathsf{lottery}(\tilde{\mathbf{B}}, \mathsf{slot}, \mathsf{R}, \mathsf{sk}) = 1$

- $\hat{\mathbf{B}} = \tilde{\mathbf{B}}$ (near future) blockchain state is unchanged. Known stake distribution.

- $\hat{\mathbf{B}} \neq \tilde{\mathbf{B}}$ (but $\hat{\mathbf{B}}^{\lceil\kappa} \preceq \tilde{\mathbf{B}}$) (far future) stake distribution is unknown at encryption time. Harder to realize (implies Blockchain WE, similar to [GKM⁺20])

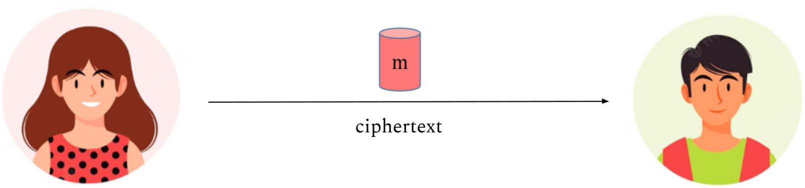
Encryption to the Future



Weaker Notion: Encryption to the Near Future

- Encryption w.r.t. lottery($\tilde{\mathbf{B}}$, slot, R_j, sk)
- The state of blockchain when the lottery winner is decided is known at the time of encryption: $\hat{\mathbf{B}} = \tilde{\mathbf{B}}$
- Can be constructed from "Witness Encryption over Commitments"

Witness Encryption [GGSW13]



m: plaintext

Encryption under NP statement x

Decrypts ciphertext

Using witness w s.t. $(x, w) \in R$

Witness Encryption [GGSW13]

A Witness Encryption scheme for **NP** language $\mathcal{L}$ (and witness relation $\mathbf{R}_{\mathcal{L}}$).

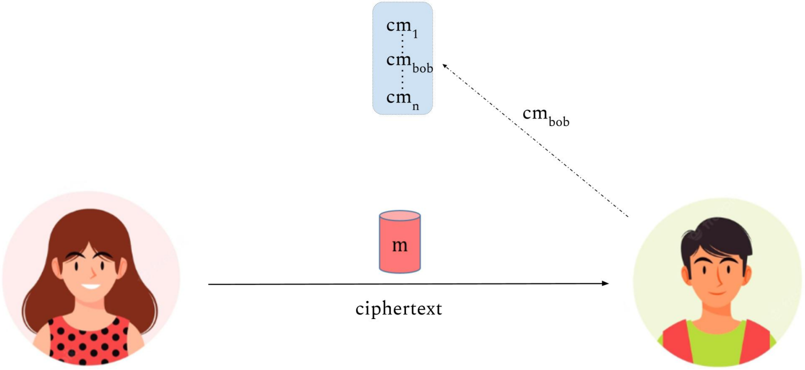
- Encrypt: $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{x}, m)$,
- Decrypt: $m/\perp \leftarrow \mathsf{Dec}(\mathsf{ct}, \mathsf{w})$
- Correctness: For any $\mathsf{x} \in \mathcal{L}$ such that $(\mathsf{x}, \mathsf{w}) \in \mathbf{R}_{\mathcal{L}}$

$$\Pr\left[\mathsf{Dec}(\mathsf{Enc}(x, m), \mathsf{w}) = m\right] = 1$$

- Security: For any PPT A, if $x \notin \mathcal{L}$ then

$$\Pr\left[\mathsf{A}(Enc(x, 0)) = 1\right] - \Pr\left[\mathsf{A}(Enc(x, 1)) = 1\right] \leq \mathsf{negl}(\lambda)$$

Witness Encryption over Commitments (cWE)



m: plaintext

Encryption under statement $x = (\mathrm{cm}_{bob}, C, y)$

Decrypts ciphertext

Using witness $w = (s, \varrho)$ s.t. $\mathrm{C}(s) = y$ AND $\mathrm{cm}_{bob} = \mathrm{Commit}(s, \varrho)$

Witness Encryption over Commitments (cWE)

Setup Phase. Bob publishes a re-usable commitment $\mathsf{cm}_{bob} \leftarrow \mathsf{Commit}(\mathsf{ck}, \mathsf{s}; \rho)$

Encrypt Phase. Define a language of statements $\mathsf{x} = (\mathsf{cm}, C, y)$ and witnesses $\mathsf{w} = (\mathsf{s}, \rho)$.

Let $(\mathsf{x}, \mathsf{w}) \in \mathbf{R}$ iff "cm commits to s using randomness ρ such that $C(\mathsf{s}) = y$"

- Correctness: For any $\mathsf{x} \in \mathcal{L}$ such that $(\mathsf{x}, \mathsf{w}) \in \mathbf{R}$

$$\Pr\left[\mathsf{Dec}(\mathsf{Enc}(x, m), \mathsf{w}) = m\right] = 1$$

- Strong Semantic Security:
  - Adversary receives $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{ck}, (\mathsf{cm}, C, y), m)$ but does not know satisfying witness
  - Adversary sees other $\mathsf{ct}_i \leftarrow \mathsf{Enc}(\mathsf{ck}, (\mathsf{cm}_i, C, y), m)$ but without knowing the opening to cm_i
  - Adversary should still not have an advantage in guessing m.

Encryption to the (near) Future

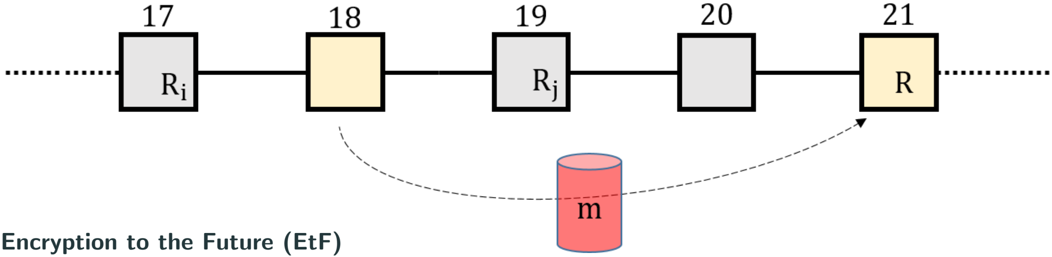
Obtain Encryption to the (near) Future from Witness Encryption over Commitments

- Setup: Let each party publish a commitment $\mathsf{cm}_i \leftarrow \mathsf{Commit}(\mathsf{sk}_i; \rho)$ of the their lottery key
- Encrypt: Let the circuit C encode the predicate $\mathsf{lottery}(\mathbf{B}, \mathsf{slot}, \mathsf{R}, \cdot)$.
  Use the statement $\mathsf{x}_i = (\mathsf{cm}_i, C, 1)$ for encryption.
- Decrypt: The lottery-winning party with sk_i successfully decrypts since $C(\mathsf{sk}_i) = 1$.

Result:

- The first non-interactive (using no auxiliary committees) Role Assignment protocol.
- Downside: The ciphertext size grows linearly with the number of participants in the network (potential lottery winners)
- For additional candidate constructions - read the paper.

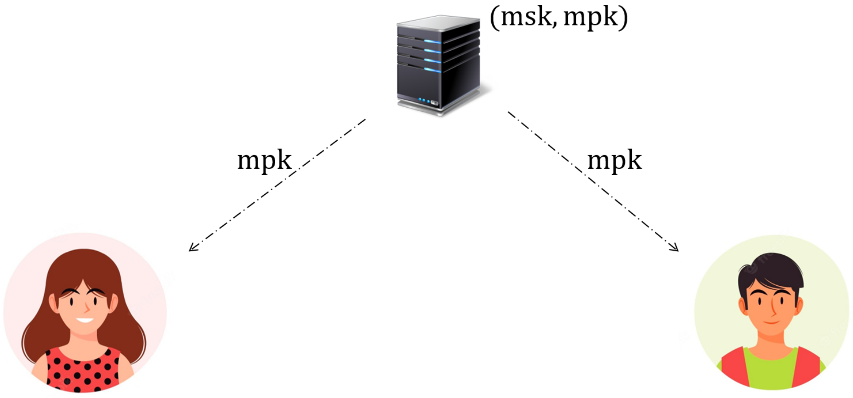
Encryption to the Future



Encryption to the Future (EtF)

- $\hat{\mathbf{B}} = \tilde{\mathbf{B}}$ (near future) blockchain state is unchanged. Known stake distribution.
- $\hat{\mathbf{B}} \neq \tilde{\mathbf{B}}$ (but $\hat{\mathbf{B}}^{\lceil \kappa} \preceq \tilde{\mathbf{B}}$) (far future) stake distribution is unknown at encryption time.
  ~~Hard~~ **Easy** to realize using EtF (near future) + TIBE scheme and **use of auxiliary committees**

Identity Based Encryption (IBE)



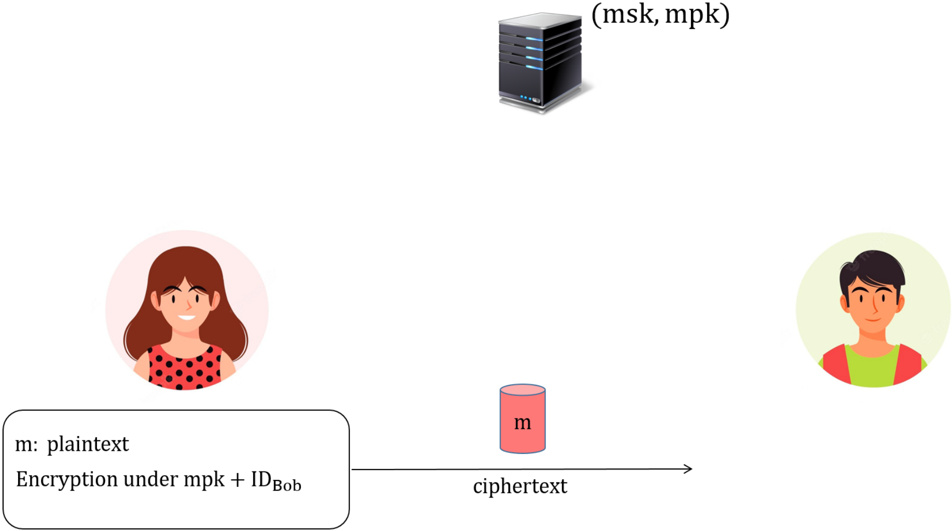
Identity Based Encryption (IBE)

$(\mathrm{msk}, \mathrm{mpk})$

m: plaintext

Encryption under $\mathrm{mpk} + \mathrm{ID}_{\mathrm{Bob}}$

Identity Based Encryption (IBE)

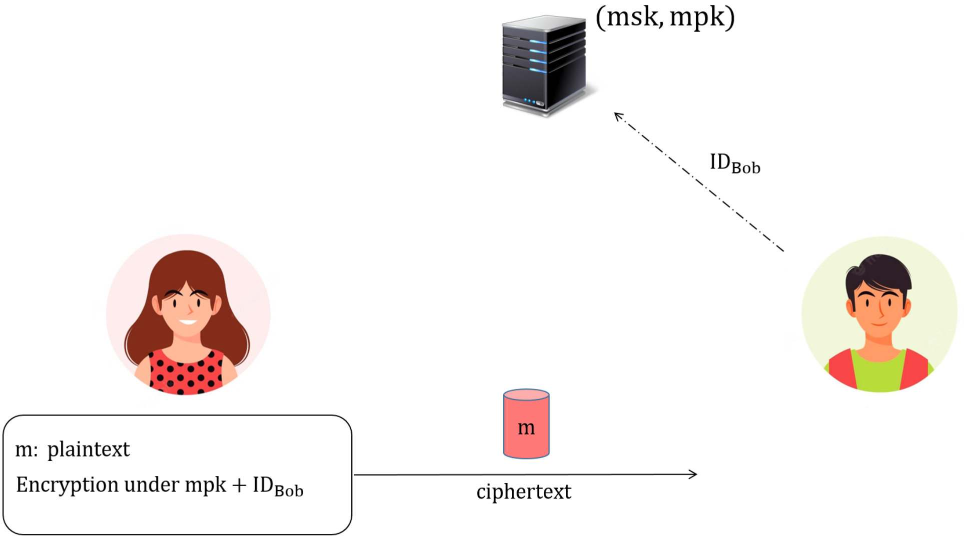


$(\mathrm{msk}, \mathrm{mpk})$

m: plaintext

Encryption under mpk + $\mathrm{ID}_{\mathrm{Bob}}$

Identity Based Encryption (IBE)



$(\mathsf{msk}, \mathsf{mpk})$

$\mathsf{ID}_{\mathsf{Bob}}$

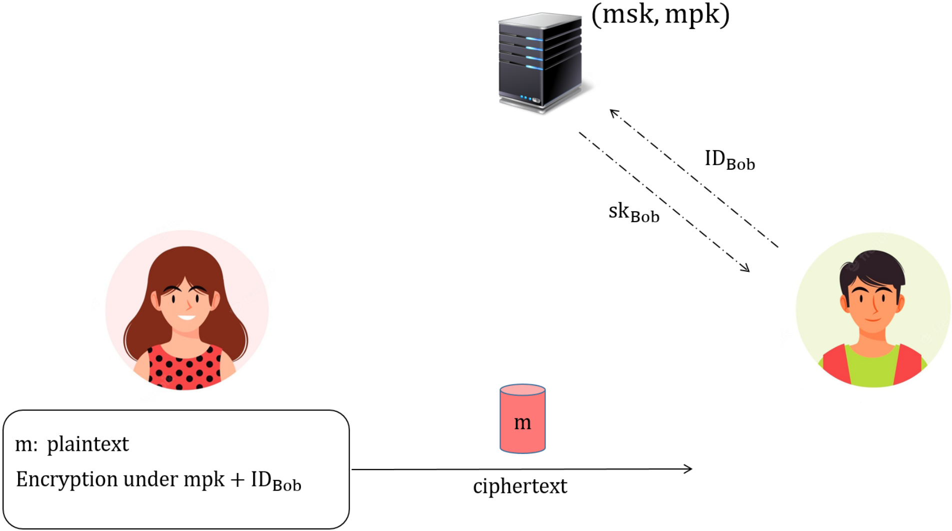
m

m: plaintext

Encryption under $\mathsf{mpk} + \mathsf{ID}_{\mathsf{Bob}}$

ciphertext

Identity Based Encryption (IBE)



$(\mathrm{msk}, \mathrm{mpk})$

$\mathrm{ID}_{\mathrm{Bob}}$

$\mathrm{sk}_{\mathrm{Bob}}$

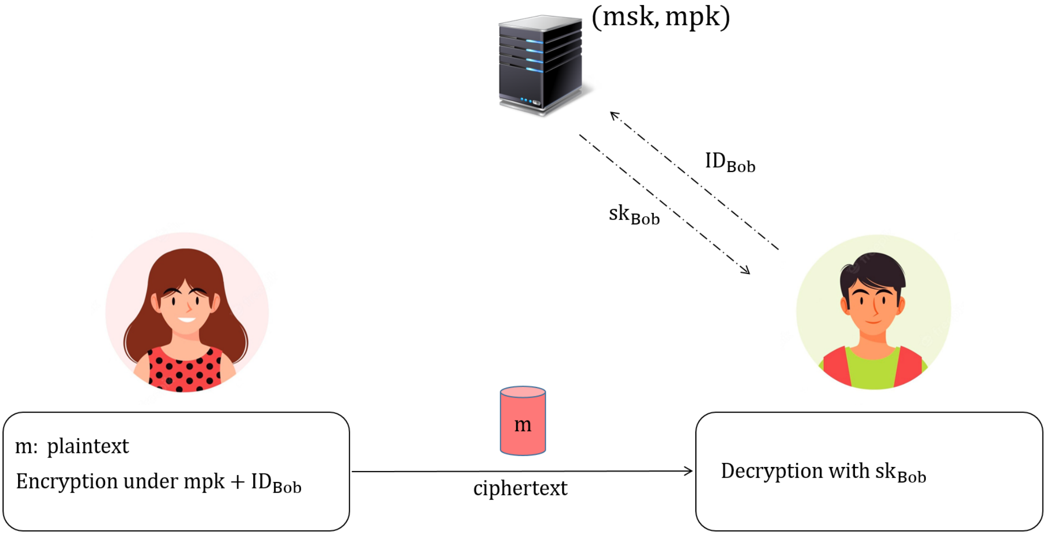
m: plaintext

Encryption under mpk + $\mathrm{ID}_{\mathrm{Bob}}$

m

ciphertext

Identity Based Encryption (IBE)



$(\mathrm{msk}, \mathrm{mpk})$

$\mathrm{ID}_{\mathrm{Bob}}$

$\mathrm{sk}_{\mathrm{Bob}}$

m: plaintext

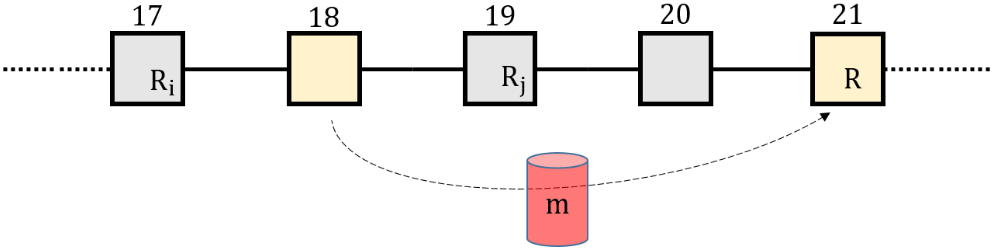
Encryption under mpk + $\mathrm{ID}_{\mathrm{Bob}}$

m

ciphertext

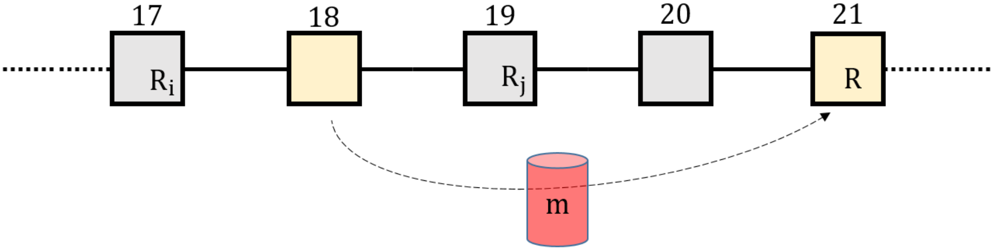
Decryption with $\mathrm{sk}_{\mathrm{Bob}}$

Encryption to the Future with Committee



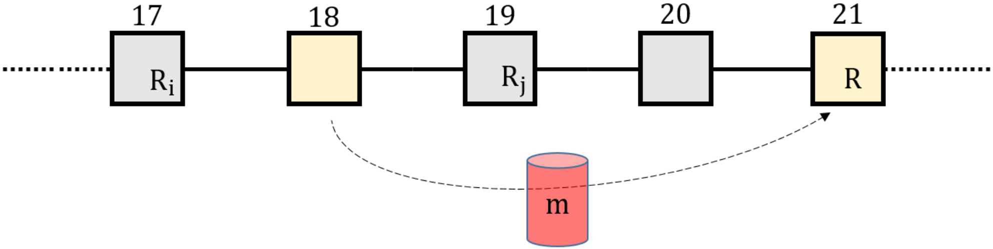
- Setup: (YOSO MPC) constructs the TIBE setup $(\mathsf{mpk}, \vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n))$.

Encryption to the Future with Committee



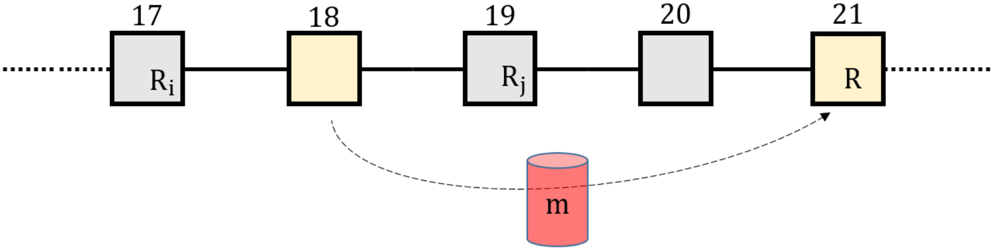
- Setup: (YOSO MPC) constructs the TIBE setup $(\mathsf{mpk}, \vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n))$.
    1. $\vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n)$ is proactively reshared through the slots in blockchain execution.

Encryption to the Future with Committee



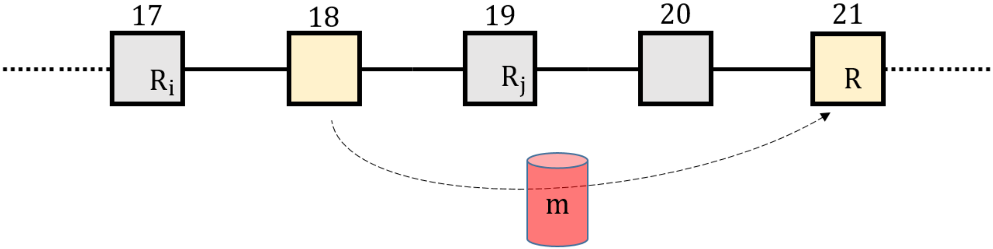
- Setup: (YOSO MPC) constructs the TIBE setup $(\mathsf{mpk}, \vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n))$.
  1. $\vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n)$ is proactively reshared through the slots in blockchain execution.
  2. Check if any EtF ciphertexts have a receiving $(\mathsf{slot}, \mathsf{R})$ that has been decided. If true, then:
     - Sample share of the IBE key for $(\mathsf{slot}, \mathsf{R})$ $\mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})} \leftarrow \Pi_{\mathsf{TIBE}}.\mathsf{IDKeygen}(\mathsf{msk}_i, (\mathsf{slot}, \mathsf{R}))$
     - Send shares of ID-key by EtF (near) $\mathsf{ct}^{\mathsf{sk},i}_{(\mathsf{slot},\mathsf{R})} \leftarrow \Pi_{\mathsf{EtF}}.\mathsf{Enc}(\mathbf{B}, \mathsf{slot}, \mathsf{R}, \mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})})$

Encryption to the Future with Committee



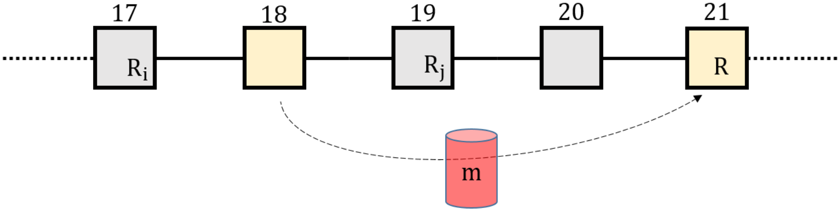
- Setup: (YOSO MPC) constructs the TIBE setup $(\mathsf{mpk}, \vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n))$.
  1. $\vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n)$ is proactively reshared through the slots in blockchain execution.
  2. Check if any EtF ciphertexts have a receiving $(\mathsf{slot}, \mathsf{R})$ that has been decided. If true, then:
     - Sample share of the IBE key for $(\mathsf{slot}, \mathsf{R})$ $\mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})} \leftarrow \Pi_{\mathsf{TIBE}}.\mathsf{IDKeygen}(\mathsf{msk}_i, (\mathsf{slot}, \mathsf{R}))$
     - Send shares of ID-key by EtF (near) $\mathsf{ct}^{\mathsf{sk},i}_{(\mathsf{slot},\mathsf{R})} \leftarrow \Pi_{\mathsf{EtF}}.\mathsf{Enc}(\mathbf{B}, \mathsf{slot}, \mathsf{R}, \mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})})$
- Encrypt: Party publishes $\mathsf{ct} \leftarrow \Pi_{\mathsf{TIBE}}.\mathsf{Enc}(\mathsf{mpk}, \mathsf{ID} = (\mathsf{slot}, \mathsf{R}), m)$.

Encryption to the Future with Committee

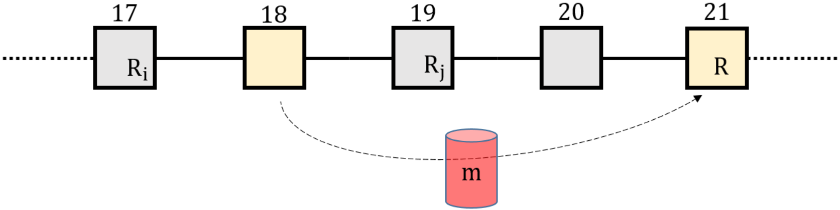


- Setup: (YOSO MPC) constructs the TIBE setup $(\mathsf{mpk}, \vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n))$.
  1. $\vec{\mathsf{msk}} = (\mathsf{msk}_1, \ldots, \mathsf{msk}_n)$ is proactively reshared through the slots in blockchain execution.
  2. Check if any EtF ciphertexts have a receiving $(\mathsf{slot}, \mathsf{R})$ that has been decided. If true, then:
     - Sample share of the IBE key for $(\mathsf{slot}, \mathsf{R})$ $\mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})} \leftarrow \Pi_{\mathsf{TIBE}}.\mathsf{IDKeygen}(\mathsf{msk}_i, (\mathsf{slot}, \mathsf{R}))$
     - Send shares of ID-key by EtF (near) $\mathsf{ct}^{\mathsf{sk},i}_{(\mathsf{slot},\mathsf{R})} \leftarrow \Pi_{\mathsf{EtF}}.\mathsf{Enc}(\mathbf{B}, \mathsf{slot}, \mathsf{R}, \mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})})$
- Encrypt: Party publishes $\mathsf{ct} \leftarrow \Pi_{\mathsf{TIBE}}.\mathsf{Enc}(\mathsf{mpk}, \mathsf{ID} = (\mathsf{slot}, \mathsf{R}), m)$.
- Decrypt: The lottery-winner for $(\mathsf{slot}, \mathsf{R})$ decrypts EtF (near) ciphertexts and combine shares $\{\mathsf{sk}^i_{(\mathsf{slot},\mathsf{R})}\}$ to obtain $\mathsf{sk}_{(\mathsf{slot},\mathsf{R})}$. Finally outputs $m \leftarrow \Pi_{\mathsf{TIBE}}.\mathsf{Dec}(\mathsf{sk}_{(\mathsf{slot},\mathsf{R})}, \mathsf{ct})$.

Encryption to the Future with Committee

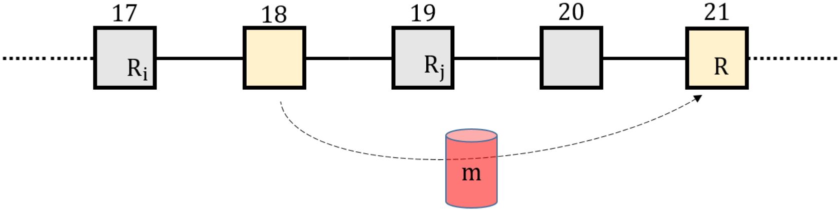


Encryption to the Future with Committee



- 📢 $\mathrm{IBE.\,Enc}_R(m)$

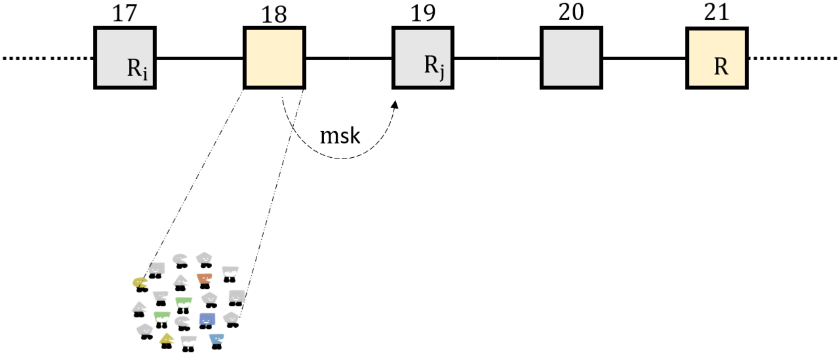
Encryption to the Future with Committee



— 📢 $\text{IBE.}\,\text{Enc}_R(m)$

— Secret share msk to the next comittees

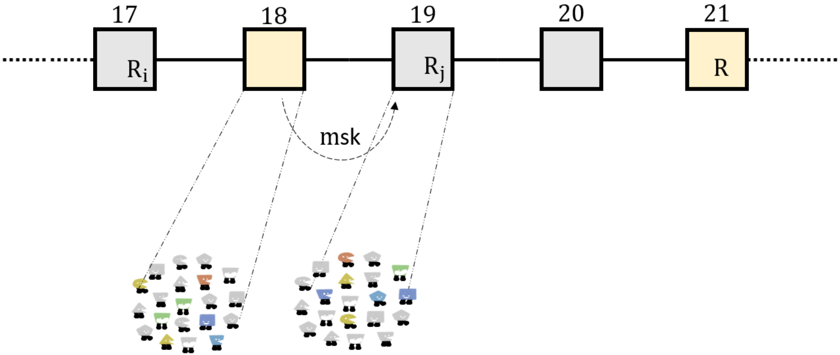
Encryption to the Future with Committee



— 📢 IBE. $\mathrm{Enc}_R(m)$

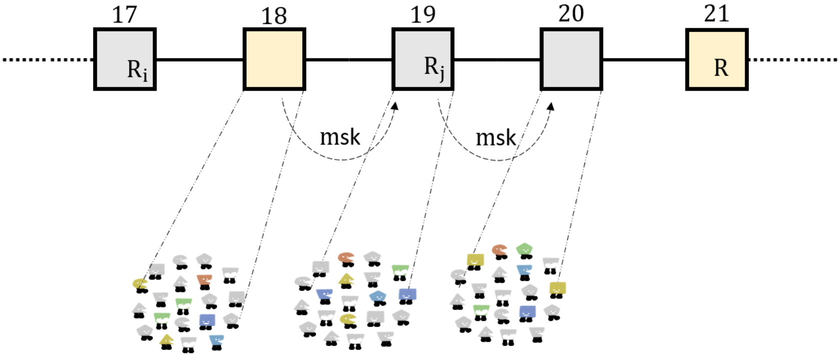
— Secret share msk to the next comittees

Encryption to the Future with Committee



- 📢 $\mathrm{IBE.Enc}_R(m)$
- Secret share msk to the next comittees

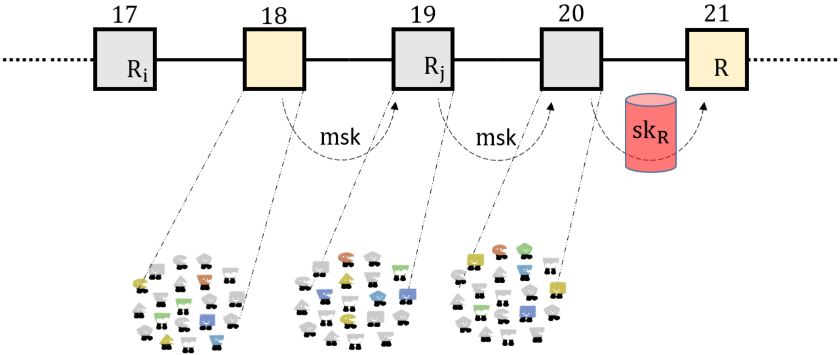
Encryption to the Future with Committee



— 📢 IBE. $\mathrm{Enc}_R(m)$

— Secret share msk to the next comittees

Encryption to the Future with Committee



- 📢 $\mathrm{IBE.Enc}_R(m)$
- Secret share msk to the next comittees
- Committee at slot 20 generates sk_R for R, and encrypt it using encrypion to the near future

Results

Type	Scheme	Communication	Committee?	Interaction?
EtF (near)	CaBKaS [BGG+20]	$O(1)$	yes	yes
	RPIR [GHK+21]	$O(1)$	yes	yes
	cWE(GC+OT) (Sec. 4.2)	$O(N)$	no	no*
EtF (far)	IBE (Sec. 7)	$O(1)$	yes	yes
	WEB [GKM+20]	$O(M)$	yes	yes
	Full-fledged WE	$O(1)$	no	no

- "Committee?" indicates whether a committee is required.
- "Communication" refers to the communication complexity in the number of all parties N, or the number of plaintexts (called deposited secrets in [GKM+20]) M of a given fixed length.
- Asterisk* means non-interactive solutions that require sending a first reusable message

Thank you!

https://eprint.iacr.org/2021/1423

F. Benhamouda, C. Gentry, S. Gorbunov, S. Halevi, H. Krawczyk, C. Lin, T. Rabin, and L. Reyzin.

Can a public blockchain keep a secret?

In TCC 2020, Part I, LNCS 12550, pages 260–290. Springer, Heidelberg, November 2020.

A. R. Choudhuri, A. Goel, M. Green, A. Jain, and G. Kaptchuk.

Fluid MPC: Secure multiparty computation with dynamic participants.

In CRYPTO 2021, Part II, LNCS 12826, pages 94–123, Virtual Event, August 2021. Springer, Heidelberg.

S. Garg, C. Gentry, A. Sahai, and B. Waters.

Witness encryption and its applications.

In Proceedings of the forty-fifth annual ACM symposium on Theory of computing, pages 467–476, 2013.

C. Gentry, S. Halevi, H. Krawczyk, B. Magri, J. B. Nielsen, T. Rabin, and S. Yakoubov.

YOSO: You only speak once - secure MPC with stateless ephemeral roles.

In CRYPTO 2021, Part II, LNCS 12826, pages 64–93, Virtual Event, August 2021. Springer, Heidelberg.

V. Goyal, A. Kothapalli, E. Masserova, B. Parno, and Y. Song.
Storing and retrieving secrets on a blockchain.
Cryptology ePrint Archive, Report 2020/504, 2020.
https://eprint.iacr.org/2020/504.