DIDs-assisted Secure Cross-metaverse Authentication Scheme for MEC-enabled Metaverse

Authors: Yingying Yao, Xiaolin Chang, Lin Li, Jiqiang Liu, Jelena Mišić, Vojislav B. Mišić

CONTENTS

01 Introduction

02 The proposed Scheme

03 Security and Performance Analysis

04 Conclusion

Introduction

Introduction

The metaverse is still far from being realized.

- The **stringent requirements of sensing, communication and computing** hinder the implementation of ubiquitous, real-time and scalable metaverse.

- The realized "lite" versions of the metaverse like Fortnite and Roblox are independent platforms that **cannot interoperate**.

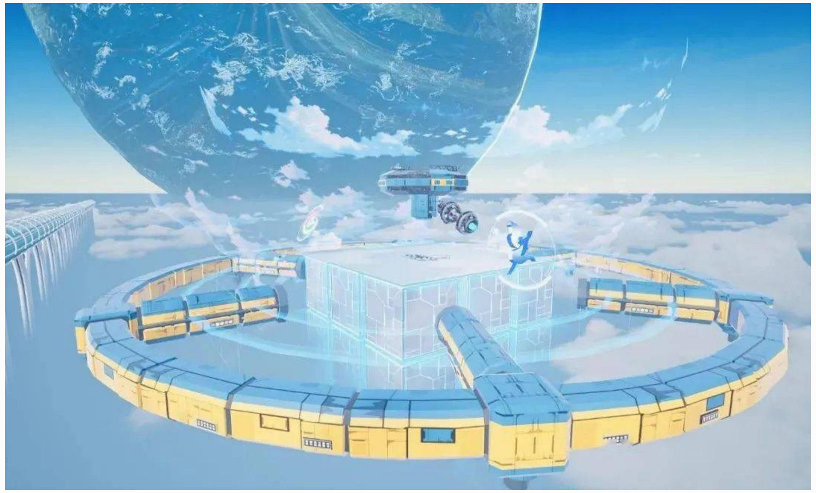
- Distinct sub-metaverses **deploying their services on heterogeneous blockchains**.

Introduction

Challenges:

- Distinct sub-metaverses deploying services on heterogeneous blockchains will **result in major problems for interoperability, preventing the implementation of seamless integrated metaverse**.

- The existing cross-chain schemes realize the interoperability between heterogeneous blockchains through notary, hash-locking, relay chain and sidechain. They mainly **concentrate on digital asset transfer, cross-chain communication, and data exchange**. None of them consider the **cross-chain authentication and real-time cross-chain governance**.



Introduction

Aim:

- Explore efficient cross-metaverse authentication and governance to make sure the security and legitimacy of activities across distinct sub-metaverses built on heterogeneous blockchains.

Contribution:

- Design a novel infrastructure for metaverse based on MEC and consortium blockchain.
- Based on the designed infrastructure, we put forward a DIDs-assisted secure cross-metaverse authentication scheme to simplify the registration process and realize the seamless cross-metaverse authentication. In addition, the adoption of DIDs also increase the decentralization of the metaverse, which means that the users manage their private keys.
- Adopting ID-based aggregate signature to reduce the overhead of computation, communication and storage.
- Providing the security and performance analysis to illustrate security features and the computing, communication and storage efficiency of our proposed scheme.

CONTENTS

01 Introduction

02 The Proposed Scheme

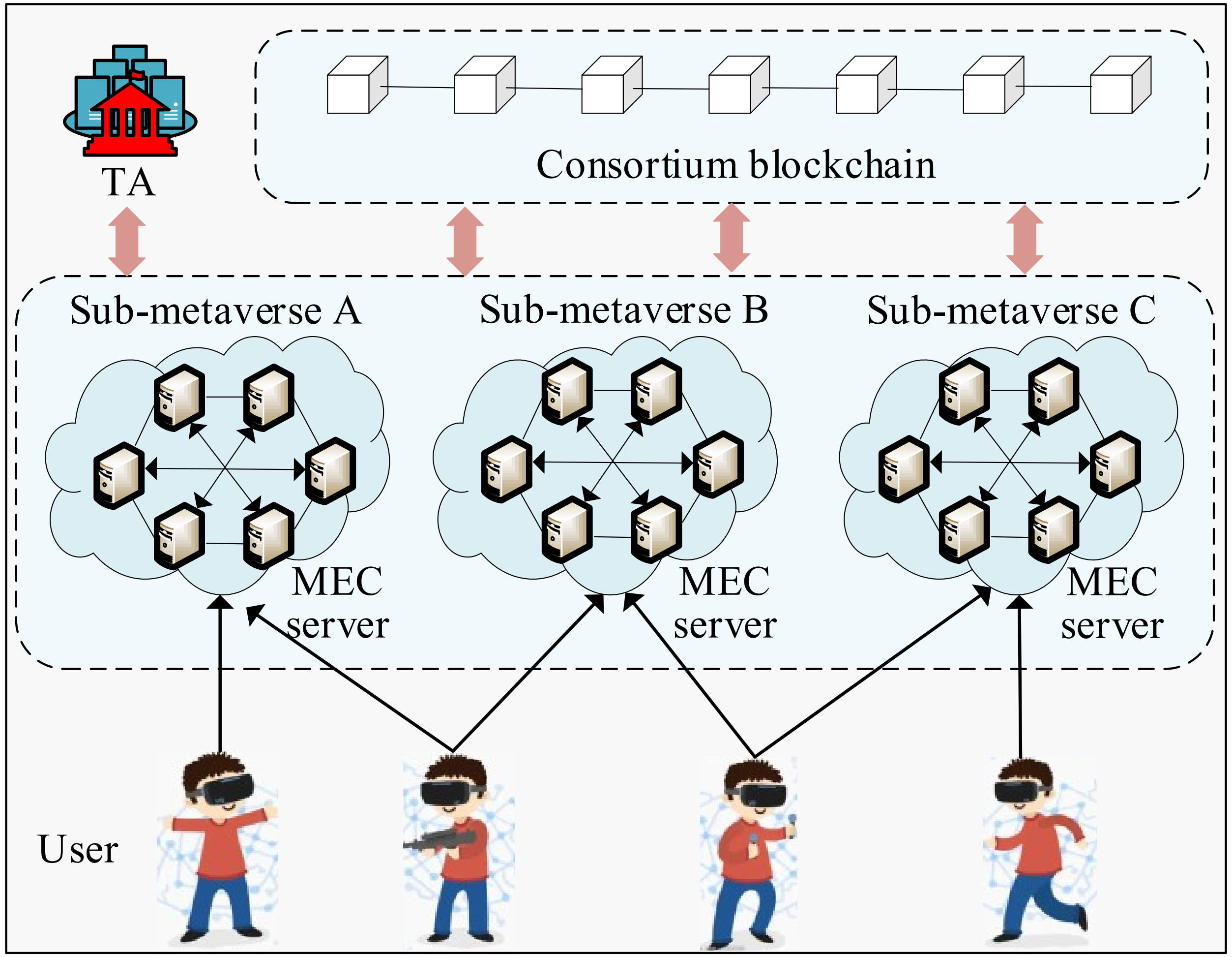
03 Security and Performance Analysis

04 Conclusion

The Proposed Scheme

System Model

- Trusted Authority (TA)
- MEC server
- User
- Consortium blockchain

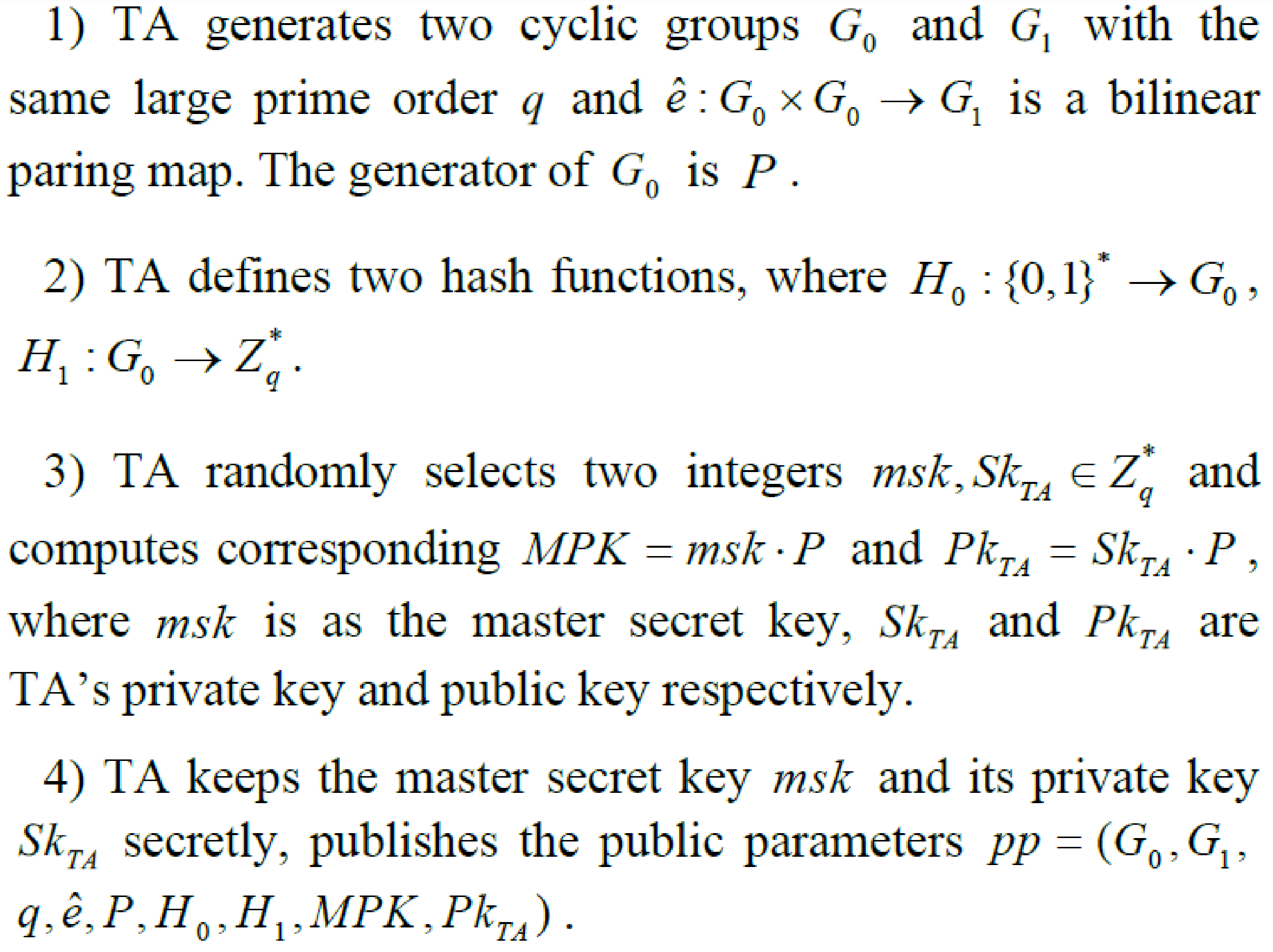


The Proposed Scheme

- Initialization Phase
- Registration Phase
- Authentication phase
- Cross-metaverse phase
- Revocation phase

The Proposed Scheme

Initialization Phase:



1) TA generates two cyclic groups G_0 and G_1 with the same large prime order q and $\hat{e}: G_0 \times G_0 \to G_1$ is a bilinear paring map. The generator of G_0 is P.

2) TA defines two hash functions, where $H_0 : \{0,1\}^* \to G_0$, $H_1 : G_0 \to Z_q^*$.

3) TA randomly selects two integers $msk, Sk_{TA} \in Z_q^*$ and computes corresponding $MPK = msk \cdot P$ and $Pk_{TA} = Sk_{TA} \cdot P$, where msk is as the master secret key, Sk_{TA} and Pk_{TA} are TA's private key and public key respectively.

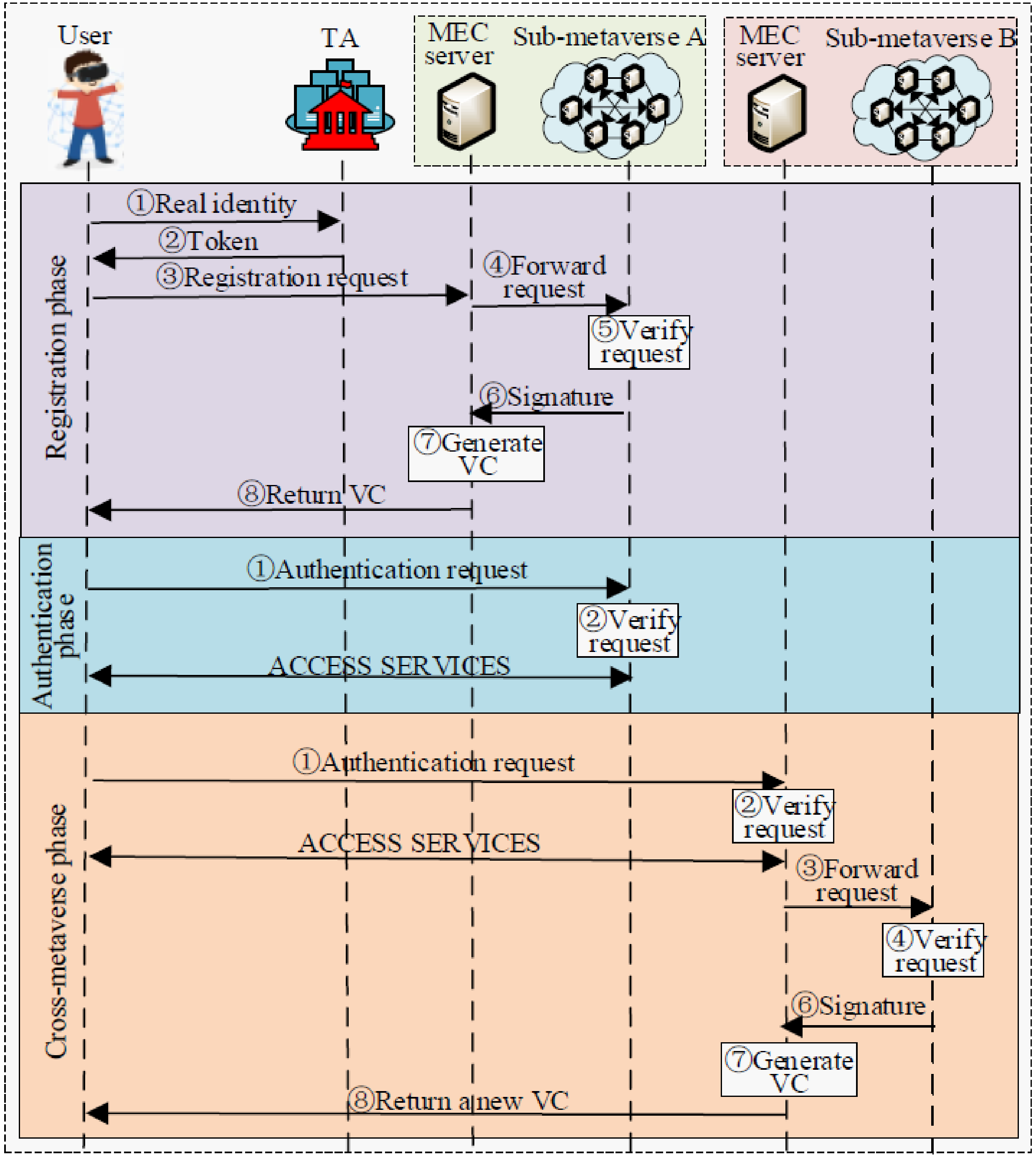
4) TA keeps the master secret key msk and its private key Sk_{TA} secretly, publishes the public parameters $pp = (G_0, G_1, q, \hat{e}, P, H_0, H_1, MPK, Pk_{TA})$.

The Proposed Scheme

Registration Phase

Authentication Phase

Cross-metaverse Phase



The Proposed Scheme

Revocation Phase:

- If a user would like to revoke its own DIDs, it can add the signed DID on the revocation list and store it on the blockchain via consensus algorithm.
- If a user is detected to have illegal behavior, its token and DIDs will be added on the revocation list by MEC servers. And the signed proof and signed revocation list will be stored on the blockchain via consensus algorithm.

CONTENTS

01 Introduction

02 Metaverse-AKA Scheme

03 Security and Performance Analysis

04 Conclusion

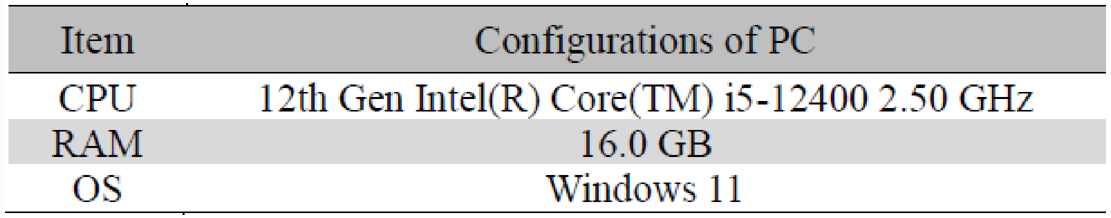
Security and Performance Analysis

Security Analysis

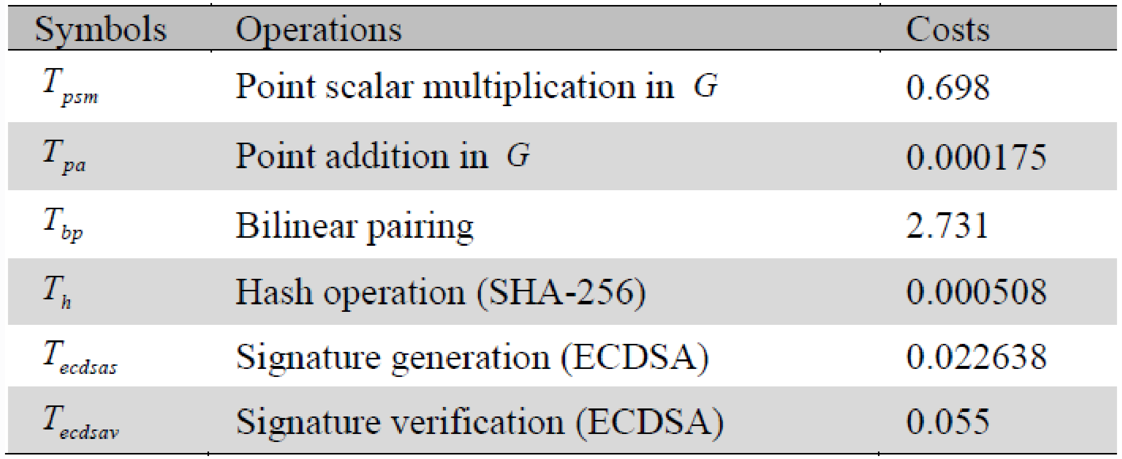
- Confidentiality and integrity
- Signature unforgeability
- Cross-metaverse authentication
- Privacy preserving
- Accountability and non-repudiation

Security and Performance Analysis

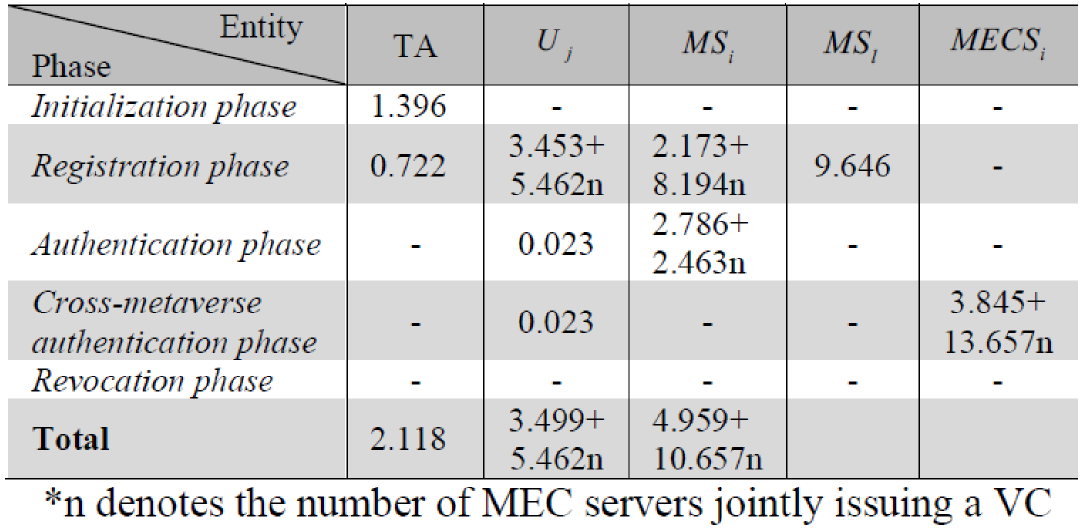
Performance Analysis



Item	Configurations of PC
CPU	12th Gen Intel(R) Core(TM) i5-12400 2.50 GHz
RAM	16.0 GB
OS	Windows 11



Symbols	Operations	Costs
T_{psm}	Point scalar multiplication in G	0.698
T_{pa}	Point addition in G	0.000175
T_{bp}	Bilinear pairing	2.731
T_h	Hash operation (SHA-256)	0.000508
T_{ecdsas}	Signature generation (ECDSA)	0.022638
T_{ecdsav}	Signature verification (ECDSA)	0.055



Entity Phase	TA	U_j	MS_i	MS_l	$MECS_i$
Initialization phase	1.396	-	-	-	-
Registration phase	0.722	3.453+ 5.462n	2.173+ 8.194n	9.646	-
Authentication phase	-	0.023	2.786+ 2.463n	-	-
Cross-metaverse authentication phase	-	0.023	-	-	3.845+ 13.657n
Revocation phase	-	-	-	-	-
Total	2.118	3.499+ 5.462n	4.959+ 10.657n		

*n denotes the number of MEC servers jointly issuing a VC

CONTENTS

01 Introduction

02 Metaverse-AKA Scheme

03 Security and Performance Analysis

04 Conclusion

Conclusion

- This paper designs a decentralized identifiers (DIDs) assisted secure cross-metaverse authentication scheme for MEC-enabled metaverse.
- The proposed scheme simplifies the registration process and realizes the seamless cross-metaverse authentication.
- The adoption of DIDs increases the decentralization of the metaverse.
- ID-based aggregate signature is adopted to reduce the overhead of computation, communication and storage.
- Security and performance analysis is provided to illustrate the security features and efficiency of our proposed scheme.

THANKS