

# A Bird's Eye View on Multi-Authority Attribute-Based Encryption

Greg Alpár<sup>1,2</sup> Leon Botros<sup>2</sup> Antonio de la Piedra<sup>3</sup> **Marloes Venema<sup>4</sup>**

<sup>1</sup>Open University of the Netherlands, Heerlen, the Netherlands

<sup>2</sup>Radboud University, Nijmegen, the Netherlands

<sup>3</sup>Kudelski Security Research Team, Cheseaux-sur-Lausanne, Switzerland

<sup>4</sup>University of Wuppertal, Wuppertal, Germany

27 September 2023

NIST Workshop on Multi-party Threshold Schemes (MPTS) 2023



BERGISCHE  
UNIVERSITÄT  
WUPPERTAL

# Motivation

- Attribute-based encryption (ABE) is a versatile primitive that has been considered extensively to securely manage access to data
- Various use cases, e.g., cloud-based settings

# Motivation

- Attribute-based encryption (ABE) is a versatile primitive that has been considered extensively to securely manage access to data
- Various use cases, e.g., cloud-based settings
- Most ABE schemes employ a single authority
- Multi-authority variants exist
- These have different levels of security, flexibility and availability

# High-level overview

- 1 Introduction to ABE
- 2 Multi-authority ABE
- 3 Discussion
- 4 Conclusion

# High-level overview

1 Introduction to ABE

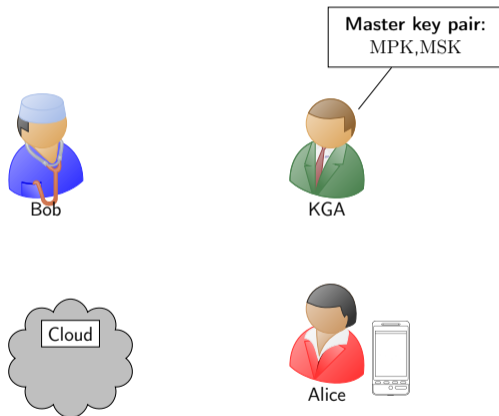
2 Multi-authority ABE

3 Discussion

4 Conclusion

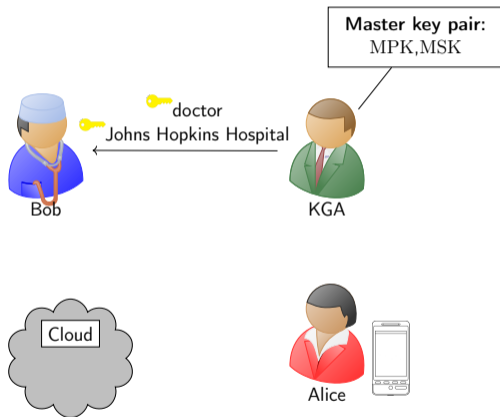
# Ciphertext-policy attribute-based encryption (CP-ABE)

## Setup:



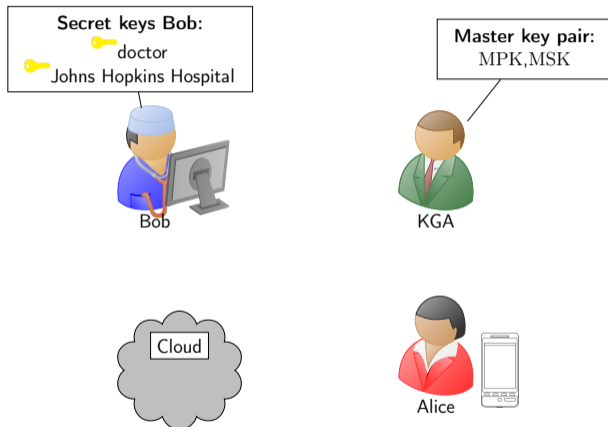
# Ciphertext-policy attribute-based encryption (CP-ABE)

## Key generation:



# Ciphertext-policy attribute-based encryption (CP-ABE)

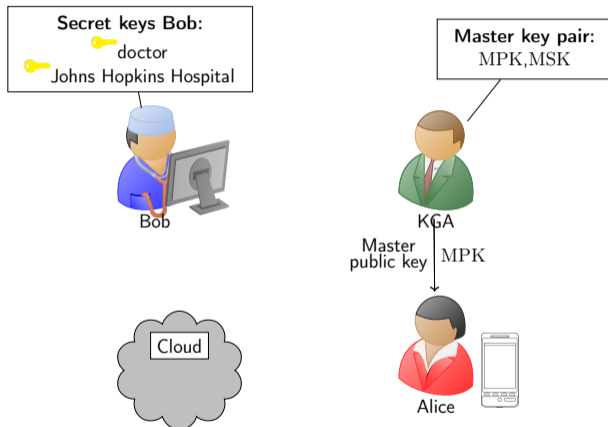
## Key generation:





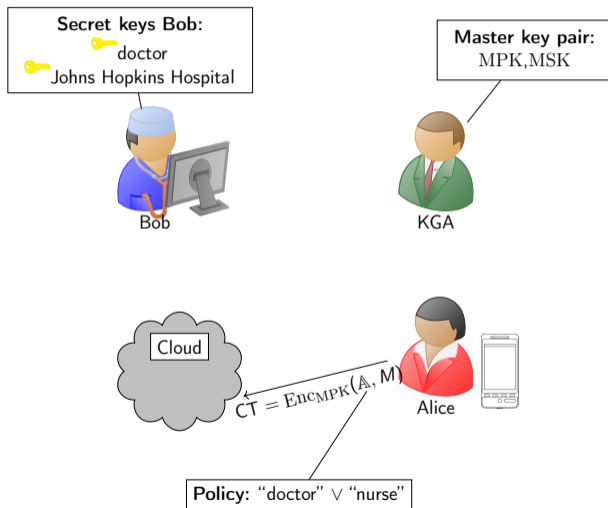
# Ciphertext-policy attribute-based encryption (CP-ABE)

## Encryption:

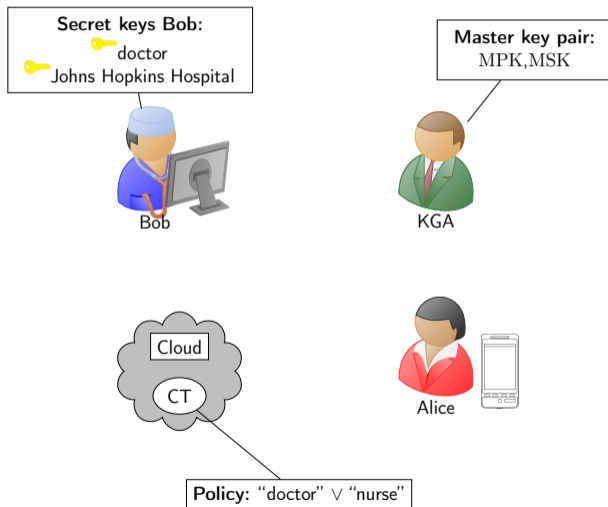


# Ciphertext-policy attribute-based encryption (CP-ABE)

## Encryption:

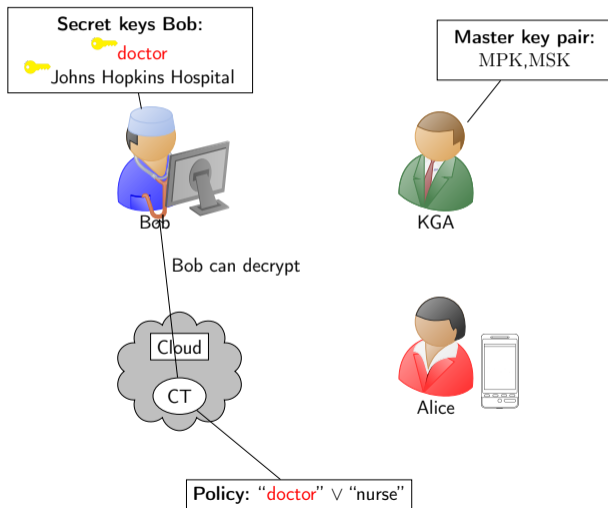


# Ciphertext-policy attribute-based encryption (CP-ABE)



# Ciphertext-policy attribute-based encryption (CP-ABE)



## Decryption:



# Enforcing access control with CP-ABE

- By its functionality, ABE implements access control
- Popular in settings in which data has to be stored on untrusted platforms

# Enforcing access control with CP-ABE

- By its functionality, ABE implements access control
- Popular in settings in which data has to be stored on untrusted platforms
- The European Telecommunications Standards Institute (ETSI) considers several use cases for ABE, e.g., Cloud, IoT 
- More recently, Cloudflare has presented an updated version of their Geo Key Manager: Portunus  [LVV<sup>+</sup>23]

# High-level overview

- 1 Introduction to ABE
- 2 Multi-authority ABE**
- 3 Discussion
- 4 Conclusion

# Multi-authority ABE

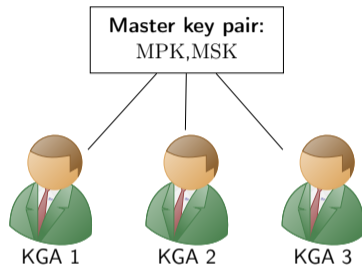
- Most ABE schemes employ a single authority to generate keys
- This authority is a single point of failure in terms of confidentiality and availability



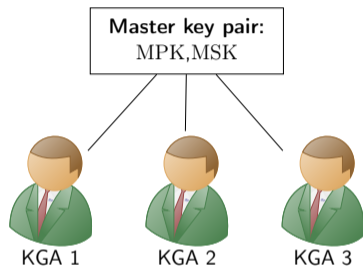
# Multi-authority ABE

- Most ABE schemes employ a single authority to generate keys
- This authority is a single point of failure in terms of confidentiality and availability
- In multi-authority ABE, the role of the authority is shared among multiple authorities
- Depending on the scheme, this may improve ABE in terms of
  - ▶ confidentiality
  - ▶ availability
  - ▶ independence (i.e., different authorities may manage different sets of attributes)

## First attempt: “simply” thresholdizing the master keys



## First attempt: “simply” thresholdizing the master keys



- Assume that the user's attribute set is the same at each authority
- Even with this restriction, achieving security may not be trivial [Cha07, CC09, LW11]
- It is static; not flexible to authorities joining or leaving

## Decentralized ABE

Many efforts around decentralized ABE [LW11, OT13, RW15, DKW21, Ven23, AG23]

## Decentralized ABE

Many efforts around decentralized ABE [LW11, OT13, RW15, DKW21, Ven23, AG23]

- Less dependent: authorities can manage different sets of attributes
- More dynamic and resilient: authorities can join or leave the system
  - ▶ without impacting all ciphertexts
  - ▶ no need to reissue all keys
- More flexible support for various access structures
- Encrypting user can choose which authorities to trust

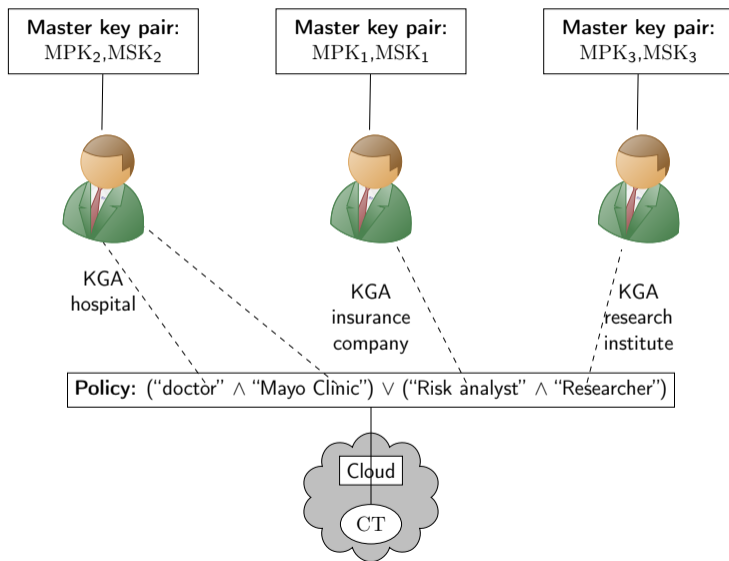
## Decentralized ABE

Many efforts around decentralized ABE [LW11, OT13, RW15, DKW21, Ven23, AG23]

- Less dependent: authorities can manage different sets of attributes
- More dynamic and resilient: authorities can join or leave the system
  - ▶ without impacting all ciphertexts
  - ▶ no need to reissue all keys
- More flexible support for various access structures
- Encrypting user can choose which authorities to trust

Decentralized ABE is very useful for settings with multiple trust domains. For instance, add insurance companies and research institutes to the medical setting.

## Example of decentralized ABE



## Decentralized versus thresholdized ABE

- Decentralized ABE can be considered structurally different from thresholdized ABE
- Thresholdization is applied in the ciphertext by the encrypting user
- e.g., decrypting user may need keys from two out of the five following authorities



## Decentralized versus thresholdized ABE

- Decentralized ABE can be considered structurally different from thresholdized ABE
- Thresholdization is applied in the ciphertext by the encrypting user
- e.g., decrypting user may need keys from two out of the five following authorities
- Yet, decentralized ABE seems to imply thresholdized ABE
  - ▶ fix the thresholdization upon setup
  - ▶ master keys of the authorities are of similar forms
- Question: could thresholdized ABE, which seems strictly weaker, have any advantages?

## Efficiency of multi-authority ABE

- Compared to single-authority ABE, multi-authority ABE is less efficient
- (Disclaimer: the remarks on this slide are mostly applicable to pairing-based and not lattice-based schemes)
- Question: may we be able to devise thresholdized ABE that is more efficient than decentralized ABE?

# Efficiency of multi-authority ABE

- Compared to single-authority ABE, multi-authority ABE is less efficient
- (Disclaimer: the remarks on this slide are mostly applicable to pairing-based and not lattice-based schemes)
- Question: may we be able to devise thresholdized ABE that is more efficient than decentralized ABE?
- Answer: difficult to say
  - ▶ Difficult to compare: few thresholdized schemes exist that are not broken [VA21]
  - ▶ In most cases, thresholdizing seems to incur some non-trivial overhead
  - ▶ For decentralized ABE, mostly the encryption efficiency is impacted
  - ▶ But recent advances are catching up: [AG23]

# High-level overview

- 1 Introduction to ABE
- 2 Multi-authority ABE
- 3 Discussion**
- 4 Conclusion

# Discussion

More research is needed

- to see how far we can take decentralized ABE
- to devise (constructions and security models for) thresholdized ABE
- compare the efficiency of suitable candidates in both categories

The call for MPTS can help to boost interest in these different types of multi-authority ABE.

# High-level overview

- 1 Introduction to ABE
- 2 Multi-authority ABE
- 3 Discussion
- 4 Conclusion**

# Conclusion

- ABE is a useful primitive to enforce access control cryptographically
- Most schemes employ a single authority
- Multi-authority variants exist that share key generation duties among multiple authorities

# Conclusion

- ABE is a useful primitive to enforce access control cryptographically
- Most schemes employ a single authority
- Multi-authority variants exist that share key generation duties among multiple authorities
- In this talk, we considered two flavors: thresholdized and decentralized ABE
- Decentralized ABE seems to outperform thresholdized ABE in flexibility and availability
- Thresholdized ABE may be more efficient
- Much room for more research



# References I

- [AG23] M. Ambrona and R. Gay.  
**Multi-authority ABE for non-monotonic access structures.**  
In A. Boldyreva and V. Kolesnikov, editors, *PKC*, volume 13941 of *LNCS*, pages 306–335. Springer, 2023.
- [CC09] M. Chase and S. S. M. Chow.  
**Improving privacy and security in multi-authority attribute-based encryption.**  
In E. Al-Shaer, S. Jha, and A. D. Keromytis, editors, *CCS*, pages 121–130. ACM, 2009.
- [Cha07] M. Chase.  
**Multi-authority attribute-based encryption.**  
In S. P. Vadhan, editor, *TCC*, volume 4392 of *LNCS*, pages 515–534. Springer, 2007.
- [DKW21] P. Datta, I. Komargodski, and B. Waters.  
**Decentralized multi-authority abe for  $nc^1$  from computational-bdh.**  
Cryptology ePrint Archive, Report 2021/1325, 2021.
- [LVV<sup>+</sup>23] W. Ladd, T. Verma, M. Venema, A. Faz-Hernández, B. McMillion, A. Wildani, and N. Sullivan.  
**Portunus: Re-imagining access control in distributed systems.**  
In *USENIX ATC*, pages 35–52, 2023.
- [LW11] A. Lewko and B. Waters.  
**Decentralizing attribute-based encryption.**  
In *EUROCRYPT*, pages 568–588. Springer, 2011.
- [OT13] T. Okamoto and K. Takashima.  
**Decentralized attribute-based signatures.**  
In K. Kurosawa and G. Hanaoka, editors, *PKC*, volume 7778 of *LNCS*, pages 125–142. Springer, 2013.

# References II

- [RW15] Y. Rouselakis and B. Waters.  
Efficient statically-secure large-universe multi-authority attribute-based encryption.  
In R. Böhme and T. Okamoto, editors, *FC*, volume 8975 of *LNCS*, pages 315–332. Springer, 2015.
- [VA21] M. Venema and G. Alpár.  
A bunch of broken schemes: A simple yet powerful linear approach to analyzing security of attribute-based encryption.  
In K. G. Paterson, editor, *CT-RSA*, volume 12704 of *LNCS*, pages 100–125. Springer, 2021.
- [Ven23] M. Venema.  
A practical compiler for attribute-based encryption: New decentralized constructions and more.  
In M. Rosulek, editor, *CT-RSA*, volume 13871 of *LNCS*, pages 132–159. Springer, 2023.