Presentation at FutureDB - Distance-bounding: past, present, future

PUBLIC-KEY DISTANCE BOUNDING AND ITS APPLICATION ON CONTACTLESS ACCESS CONTROL

Handan Kılınç
handan.kilinc@epfl.ch

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

*Handan Kılınç and Serge Vaudenay. Efficient public-key distance bounding protocol. In ASIACRYPT, 2016

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

OUTLINE

- ✓ EFFICIENT PUBLIC-KEY DB PROTOCOL
  - Introduction
  - Weak-authenticated Key Agreement
  - Eff-pkDB and its private variant
  - Comparison
- ✓ ACCESS CONTROL WITH DB
  - Introduction
  - Security and Privacy model for AC
  - Our Framework
  - Conclusion

OUTLINE

- ✓ **EFFICIENT PUBLIC-KEY DB PROTOCOL**
  - **Introduction**
  - Weak-authenticated Key Agreement
  - Eff-pkDB and its private variant
  - Comparison
- ✓ ACCESS CONTROL WITH DB
  - Introduction
  - Security and Privacy model for AC
  - Our Framework
  - Conclusion

INTRODUCTION

DISTANCE BOUNDING

<u>Verifier</u>

<u>Prover</u>

INTRODUCTION

DISTANCE BOUNDING

<u>Verifier</u>

<u>Prover</u>

The prover authenticates and proves its proximity

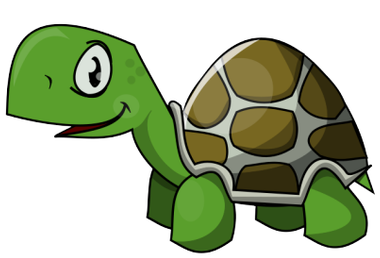
INTRODUCTION

- Symmetric Distance Bounding: The prover and the verifier share a secret

- Public-key Distance Bounding: The prover has its own secret/ public key and the public-key of the verifier

INTRODUCTION
PROBLEMS IN PUBLIC KEY DB

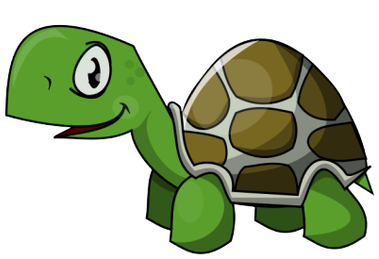
Slower than symmetric key operations



Limited computational resources on the devices

INTRODUCTION
PROBLEMS IN PUBLIC KEY DB

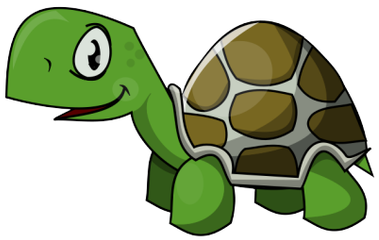
Slower than symmetric key operations



Limited computational resources on the devices

INTRODUCTION
PROBLEMS IN PUBLIC KEY DB

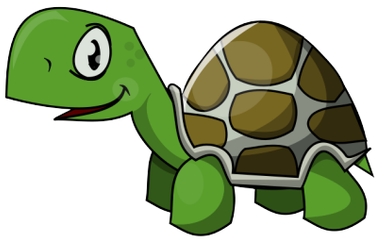
Slower than symmetric key operations



Limited computational resources on the devices

INTRODUCTION
PROBLEMS IN PUBLIC KEY DB

Slower than symmetric key operations



Limited computational resources on the devices

Construct an **efficient** and **secure** public-key distance bounding

STRONG PRIVACY IN DB

HPVP*

- We have provers P1, P2, P3,…, Pn and the adversary $\mathcal{A}$
- $\mathcal{A}$ can corrupt the provers: learns the secret keys of the provers.
- As a challenge, $\mathcal{A}$ picks two provers Pi, Pj
- Challenger picks one of them as a virtual tag and gives the virtual prover to $\mathcal{A}$.
- $\mathcal{A}$ can send messages to the virtual tag.
- $\mathcal{A}$ can send messages to the verifier.
- If $\mathcal{A}$ can recognize the virtual tag, then he wins the game.

* J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel. A new RFID privacy model. In ESORICS, 2011

STRONG PRIVACY IN DB

HPVP*

- We have provers P1, P2, P3,…, Pn and the adversary $\mathcal{A}$
- $\mathcal{A}$ can corrupt the provers: learns the secret keys of the provers.
- As a challenge, $\mathcal{A}$ picks two provers Pi, Pj
- Challenger picks one of them as a virtual tag and gives the virtual prover to $\mathcal{A}$.
- $\mathcal{A}$ can send messages to the virtual tag.
- $\mathcal{A}$ can send messages to the verifier.
- If $\mathcal{A}$ can recognize the virtual tag, then he wins the game.

A DB protocol is **strong private** if $\mathcal{A}$ wins the above game with negligible advantage.

* J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel. A new RFID privacy model. In ESORICS, 2011

AN OVERVIEW OF OUR PROTOCOL

Agree on a key s with using a key agreement (KA) protocol

Run a symmetric DB with s

AN OVERVIEW OF OUR PROTOCOL

Agree on a key s with using a key agreement (KA) protocol

Run a symmetric DB with s

What kind of security properties do we need for the key agreement protocol to have MiM, DF and DH secure and strong private DB protocol?

AN OVERVIEW OF OUR PROTOCOL

Agree on a key s with using a key agreement (KA) protocol

Run a symmetric DB with s

KA	Efficiency	Security
MQV	2.5	No proof
HMQV	2.5	CK
KEA+	3	CK
NAXOS	4	eCK
CMQV	3	eCK

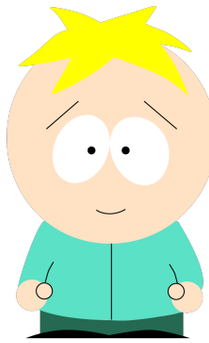
What kind of security properties do we need for the key agreement protocol to have MiM, DF and DH secure and strong private DB protocol?

OUTLINE

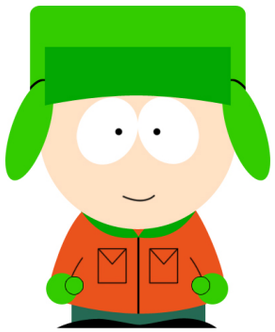
- ✓ **EFFICIENT PUBLIC-KEY DB PROTOCOL**
  - Introduction
  - **Weak-authenticated Key Agreement**
  - Eff-pkDB and its private variant
  - Comparison
- ✓ ACCESS CONTROL WITH DB
  - Introduction
  - Security and Privacy model for AC
  - Our Framework
  - Conclusion

AUTHENTICATED KEY AGREEMENT
ONE PASS

sk_A, pk_A, pk_B



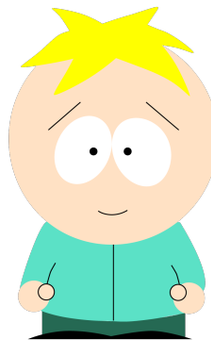
sk_B, pk_B, pk_A



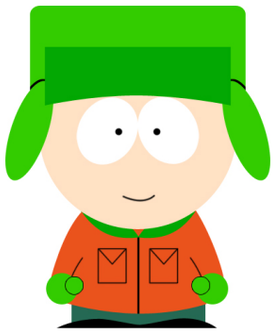
*Handan Kılınç and Serge Vaudenay. Efficient public-key distance bounding protocol. In ASIACRYPT, 2016

AUTHENTICATED KEY AGREEMENT
ONE PASS

sk_A, pk_A, pk_B



sk_B, pk_B, pk_A



$N \leftarrow D(1^n)$

$B(sk_B, pk_B, pk_A, N)$

*Handan Kılınç and Serge Vaudenay. Efficient public-key distance bounding protocol. In ASIACRYPT, 2016

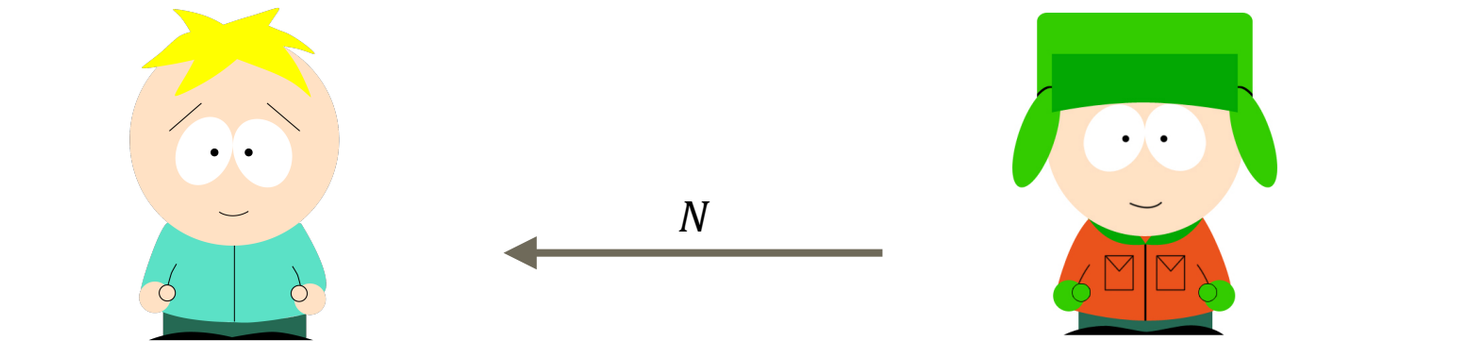
AUTHENTICATED KEY AGREEMENT

ONE PASS

*Handan Kılınç and Serge Vaudenay. Efficient public-key distance bounding protocol. In ASIACRYPT, 2016

AUTHENTICATED KEY AGREEMENT

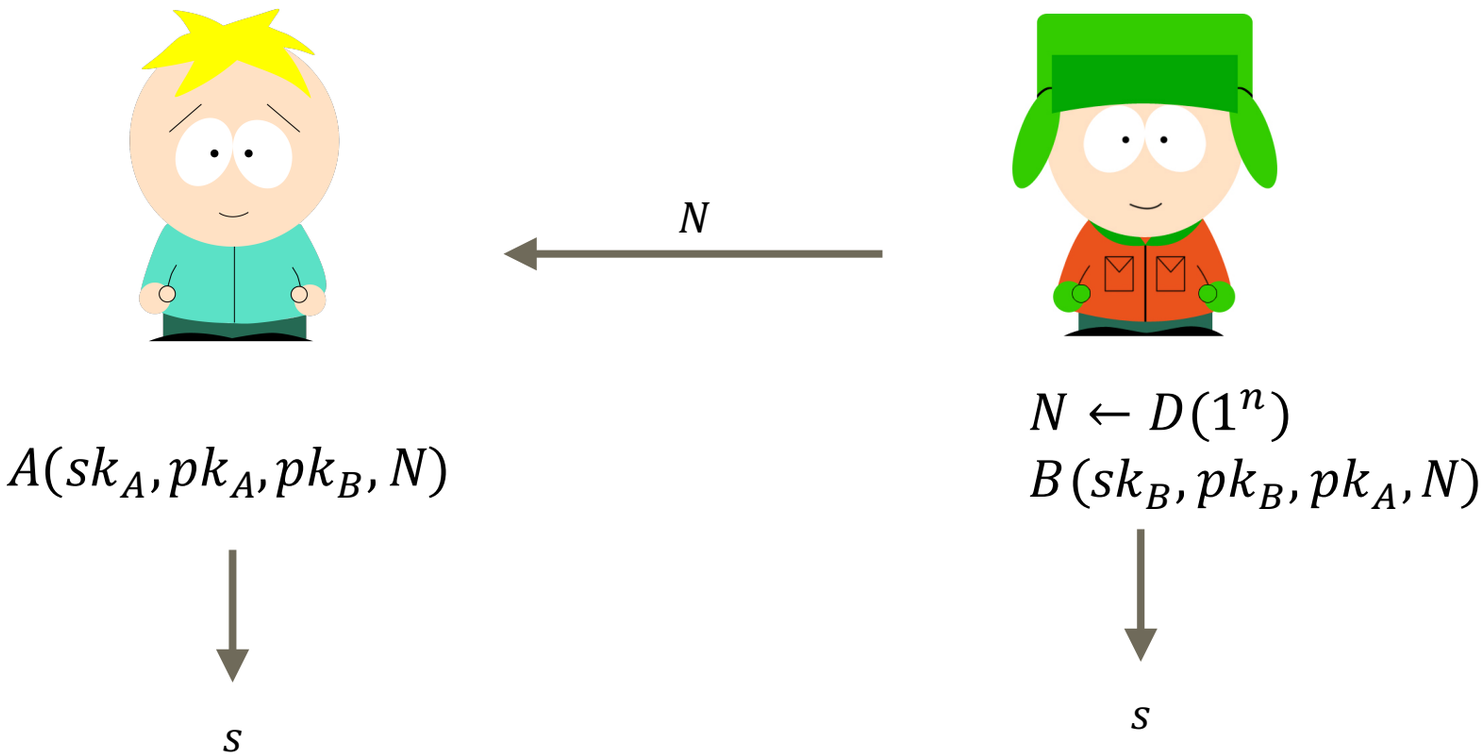
ONE PASS



*Handan Kılınç and Serge Vaudenay. Efficient public-key distance bounding protocol. In ASIACRYPT, 2016

AUTHENTICATED KEY AGREEMENT

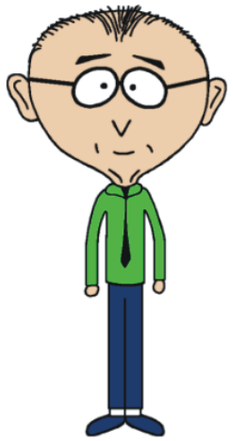
ONE PASS



*Handan Kılınç and Serge Vaudenay. Efficient public-key distance bounding protocol. In ASIACRYPT, 2016

Decisional-Authenticated Key Agreement
(D-AKA)

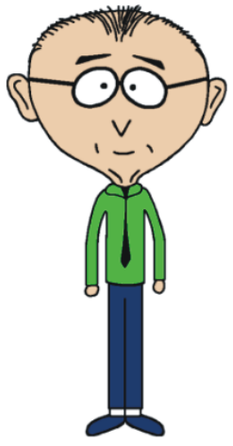
Challenger



Adversary

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger

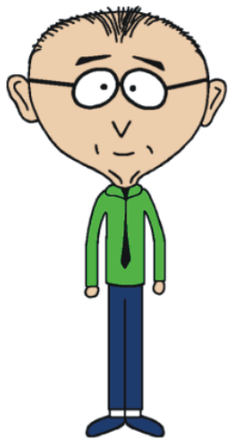


Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

Adversary

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

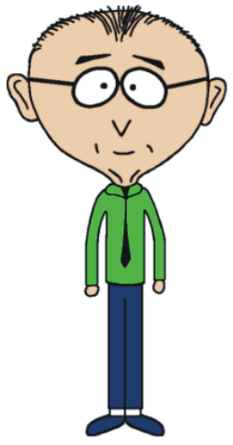
Adversary

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

Adversary

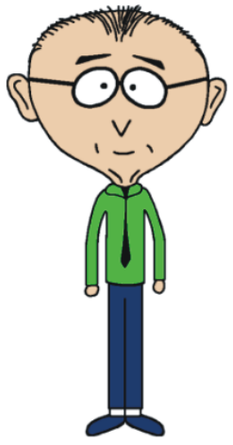
pk_A

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

Adversary

pk_A →

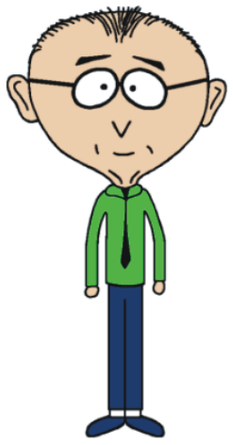
← N, s_0

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

s_b, N, pk_B, pk_A →

Adversary

pk_A →

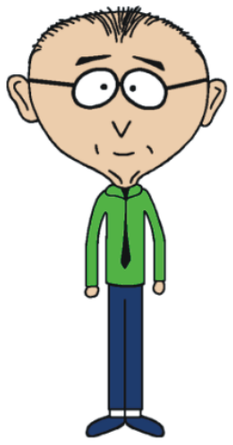
← N, s_0

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

s_b, N, pk_B, pk_A →

pk_A →

← N, s_0

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

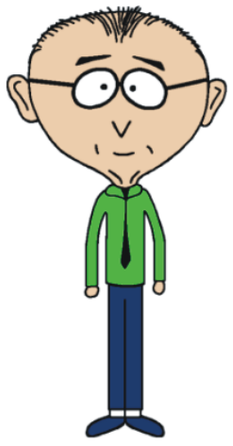
$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

Adversary

It can access the oracles except
~~(pk_B, N)~~

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

s_b, N, pk_B, pk_A →

pk_A →

← N, s_0

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

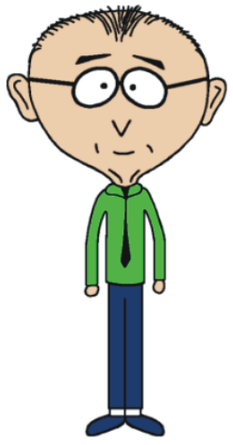
Adversary

It can access the oracles except ~~(pk_B, N)~~

b' ↓

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

s_b, N, pk_B, pk_A →

pk_A →

← N, s_0

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

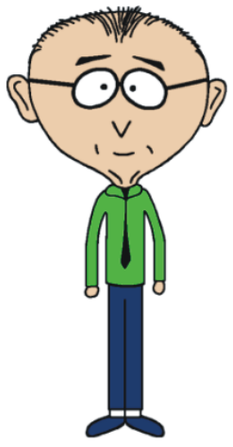
Adversary

It can access the oracles except ~~(pk_B, N)~~

b' If $b' = b$
It wins

Decisional-Authenticated Key Agreement
(D-AKA)

Challenger



Generate $(sk_A,\ pk_A), (sk_B, pk_B)$
Pick s_1
Pick $b \in \{0,1\}$

s_b, N, pk_B, pk_A →

Adversary

It can access the oracles except ~~(pk_B, N)~~

← pk_A

N, s_0 →

$Oracle_B(.)$
$N \leftarrow D(1^n)$
run $B(sk_B, pk_B, ., N)$

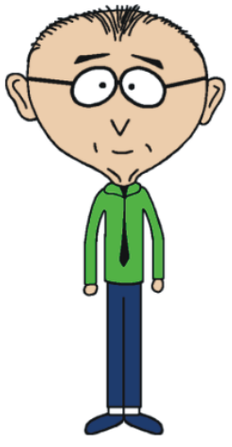
$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

b' If $b' = b$ It wins

A one-pass AKA is **D-AKA secure** if the adversary's advantage winning this game is negligible.

D-AKA PRIVACY GAME

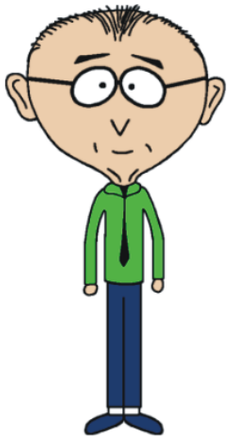
Challenger



Adversary

D-AKA PRIVACY GAME

Challenger

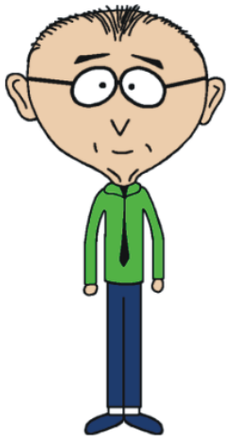


Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Adversary

D-AKA PRIVACY GAME

Challenger



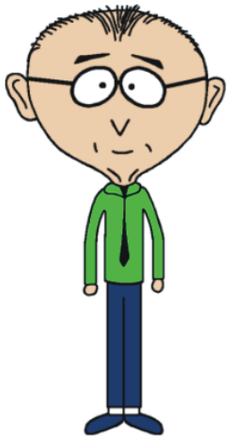
Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Adversary

$Oracle_A(.,.)$
$A(sk_A,pk_A,.,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

pk_A, sk_{B_1}, pk_{B_1}

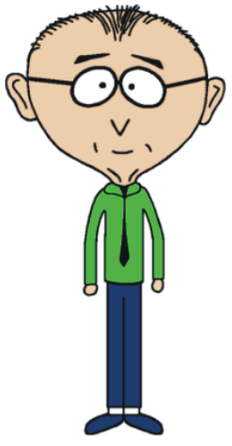
Adversary

$Oracle_A(.,.)$

$A(sk_A,pk_A,.,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

pk_A, sk_{B_1}, pk_{B_1}

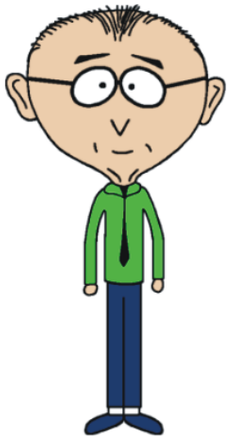
Adversary

Pick sk_{B_0},pk_{B_0}

$Oracle_A(.,.)$
$A(sk_A,pk_A,.,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

pk_A, sk_{B_1}, pk_{B_1}

sk_{B_0}, pk_{B_0}

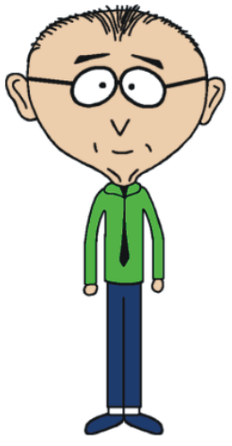
Adversary

Pick sk_{B_0}, pk_{B_0}

$Oracle_A(.,.)$
$A(sk_A, pk_A, ., .)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Pick $b \in \{0,1\}$
$N \leftarrow D(1^n)$,
$s = B(sk_{B_b},pk_{B_b},pk_A,N)$

pk_A,sk_{B_1},pk_{B_1}

sk_{B_0},pk_{B_0}

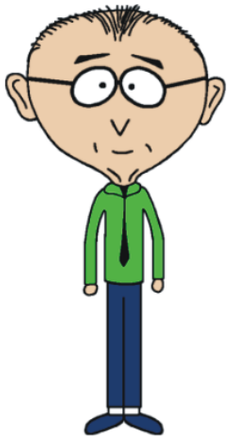
Adversary

Pick sk_{B_0},pk_{B_0}

$Oracle_A(.,.)$
$A(sk_A,pk_A,.,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Pick $b \in \{0,1\}$
$N \leftarrow D(1^n)$,
$s = B(sk_{B_b}, pk_{B_b}, pk_A, N)$

pk_A, sk_{B_1}, pk_{B_1} →

← sk_{B_0}, pk_{B_0}

s →

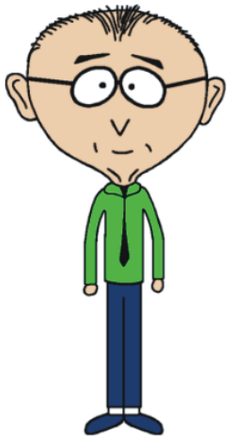
Adversary

Pick sk_{B_0}, pk_{B_0}

$Oracle_A(.,.)$
$A(sk_A, pk_A, .,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Pick $b \in \{0,1\}$

$N \leftarrow D(1^n)$,

$s = B(sk_{B_b}, pk_{B_b}, pk_A, N)$

pk_A, sk_{B_1}, pk_{B_1} →

← sk_{B_0}, pk_{B_0}

s →

Adversary

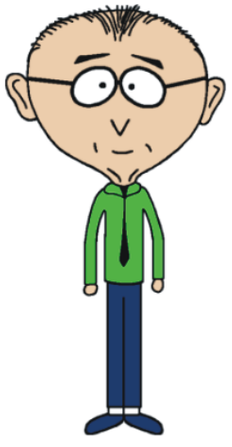
Pick sk_{B_0}, pk_{B_0}

$Oracle_A(.,.)$

$A(sk_A, pk_A, ., .)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Pick $b \in \{0,1\}$

$N \leftarrow D(1^n)$,

$s = B(sk_{B_b}, pk_{B_b}, pk_A, N)$

pk_A, sk_{B_1}, pk_{B_1}

sk_{B_0}, pk_{B_0}

s

Adversary

Pick sk_{B_0}, pk_{B_0}

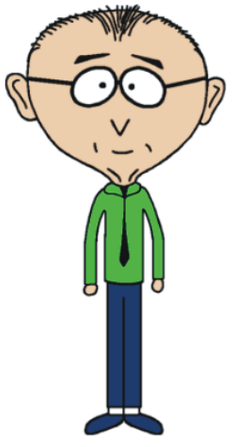
b'

$Oracle_A(.,.)$

$A(sk_A, pk_A, .,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Pick $b \in \{0,1\}$

$N \leftarrow D(1^n)$,

$s = B(sk_{B_b}, pk_{B_b}, pk_A, N)$

pk_A, sk_{B_1}, pk_{B_1}

sk_{B_0}, pk_{B_0}

s

Adversary

Pick sk_{B_0}, pk_{B_0}

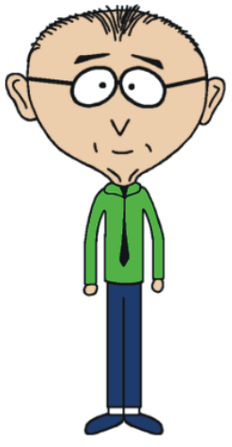
b' If $b' = b$ It wins

$Oracle_A(.,.)$

$A(sk_A, pk_A, .,.)$

D-AKA PRIVACY GAME

Challenger



Generate $(sk_A,\ pk_A),(sk_{B_1},pk_{B_1})$

Pick $b \in \{0,1\}$
$N \leftarrow D(1^n)$,
$s = B(sk_{B_b}, pk_{B_b}, pk_A, N)$

pk_A, sk_{B_1}, pk_{B_1}

sk_{B_0}, pk_{B_0}

s

Adversary

Pick sk_{B_0}, pk_{B_0}

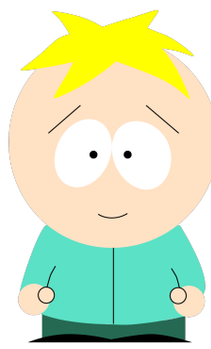
b' If $b' = b$ It wins

$Oracle_A(.,.)$
$A(sk_A, pk_A, .,.)$

A one-pass AKA is **D-AKA private** if the adversary's advantage winning this game is negligible.

NONCE-DH

D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL



NONCE-DH

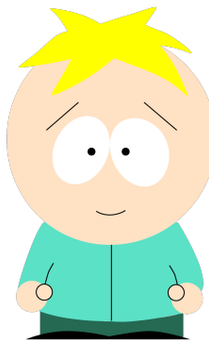
D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL

$sk_A \in \mathbb{Z}_q$
$pk_A = g^{sk_A}$

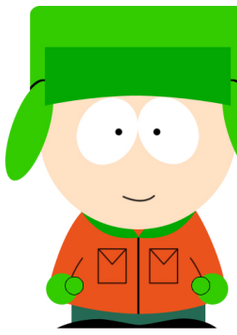
Public parameter G order of q and $g \in G$

$sk_B \in \mathbb{Z}_q$
$pk_B = g^{sk_B}$

sk_A, pk_A, pk_B



sk_B, pk_B, pk_A



NONCE-DH

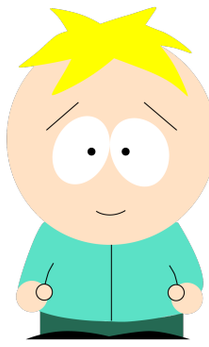
D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL

$sk_A \in \mathbb{Z}_q$
$pk_A = g^{sk_A}$

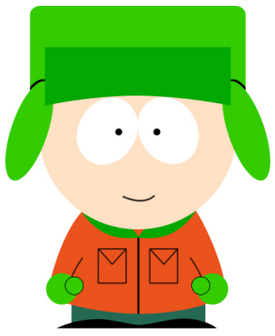
Public parameter G order of q and $g \in G$

$sk_B \in \mathbb{Z}_q$
$pk_B = g^{sk_B}$

sk_A, pk_A, pk_B



sk_B, pk_B, pk_A



Pick $N \in \{0,1\}^{\ell}$
$s = H(g, pk_B, pk_A, pk_A^{sk_B}, N)$

NONCE-DH

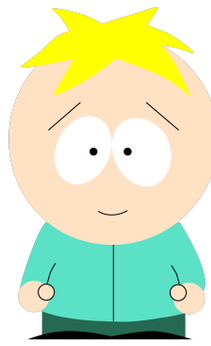
D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL

$sk_A \in \mathbb{Z}_q$
$pk_A = g^{sk_A}$

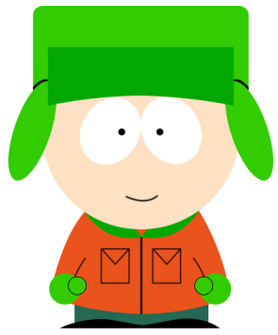
Public parameter G order of q and $g \in G$

$sk_B \in \mathbb{Z}_q$
$pk_B = g^{sk_B}$

sk_A, pk_A, pk_B



N



sk_B, pk_B, pk_A

Pick $N \in \{0,1\}^{\ell}$

$s = H(g, pk_B, pk_A, pk_A^{sk_B}, N)$

NONCE-DH

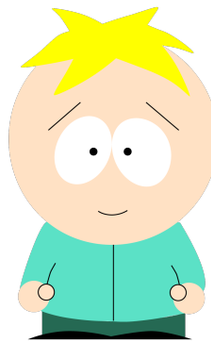
D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL

$sk_A \in \mathbb{Z}_q$
$pk_A = g^{sk_A}$

Public parameter G order of q and $g \in G$

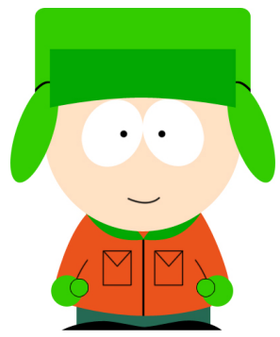
$sk_B \in \mathbb{Z}_q$
$pk_B = g^{sk_B}$

sk_A, pk_A, pk_B



N

sk_B, pk_B, pk_A



$s = H(g, pk_B, pk_A, pk_B^{sk_A}, N)$

Pick $N \in \{0,1\}^{\ell}$
$s = H(g, pk_B, pk_A, pk_A^{sk_B}, N)$

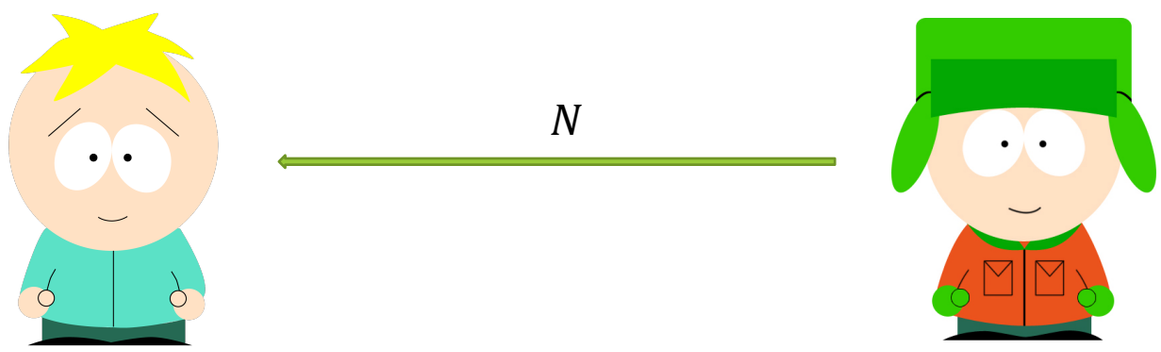
NONCE-DH

D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL

$sk_A \in \mathbb{Z}_q$
$pk_A = g^{sk_A}$

Public parameter G order of q and $g \in G$

$sk_B \in \mathbb{Z}_q$
$pk_B = g^{sk_B}$



$s = H(g, pk_B, pk_A, pk_B^{sk_A}, N)$

Pick $N \in \{0,1\}^{\ell}$
$s = H(g, pk_B, pk_A, pk_A^{sk_B}, N)$

Nonce-DH is D-AKA secure and private in the **random oracle** model assuming that **Gap Diffie-Hellman** problem is hard.

NONCE-DH

D-AKA SECURE AND PRIVATE KEY AGREEMENT PROTOCOL

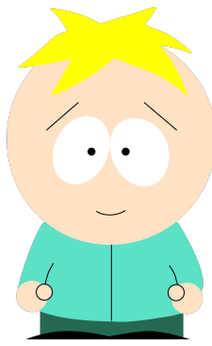
KA	Efficiency	Security
MQV	2.5	No proof
HMQV	2.5	CK
KEA+	3	CK
NAXOS	4	eCK
CMQV	3	eCK
Nonce-DH	**1**	**D-AKA**

$sk_A \in \mathbb{Z}_q$
$pk_A = g^{sk_A}$

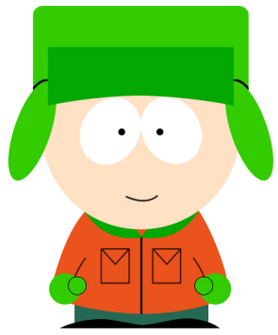
Public parameter G order of q and $g \in G$

$sk_B \in \mathbb{Z}_q$
$pk_B = g^{sk_B}$

sk_A, pk_A, pk_B



N



sk_B, pk_B, pk_A

$s = H(g, pk_B, pk_A, pk_B^{sk_A}, N)$

Pick $N \in \{0,1\}^{\ell}$
$s = H(g, pk_B, pk_A, pk_A^{sk_B}, N)$

Nonce-DH is D-AKA secure and private in the **random oracle** model assuming that **Gap Diffie-Hellman** problem is hard.

OUTLINE

✓EFFICIENT PUBLIC-KEY DB PROTOCOL

- Introduction
- Weak-authenticated Key Agreement
- **Eff-pkDB and its private variant**
- Comparison

✓ ACCESS CONTROL WITH DB

- Introduction
- Security and Privacy model for AC
- Our Framework
- Conclusion

EFF-PKDB

Verifier

sk_V, pk_V

Prover

sk_P, pk_P, pk_V

N, pk_P

$N \leftarrow D(1^n)$

$s = A(sk_A, pk_A, pk_B, N)$

$s = B(sk_P, pk_P, pk_V, N)$

symDB(s)

Out

SECURITY OF EFF-PKDB

MiM Security: If symDB is multi-verifier OT-MiM secure and the key agreement protocol is D-AKA secure, the Eff-pkDB is MiM-secure.

DF Security: If symDB is DF-secure, then Eff-pkDB is DF-secure.

DH security: If symDB is OT-MiM-secure, OT-DH-secure and if the key agreement protocol is D-AKA secure then Eff-pkDB is DH-secure.

STRONG PRIVATE VARIANT OF EFF-PKDB

Verifier

$N, pk_P = Dec_{sk_{V_1}}(e)$

$s = A(sk_A, pk_A, pk_B, N)$

pk_P is private output

e

symDB(s)

Out

Prover

$sk_P, pk_P, pk_V = (pk_{V_1}, pk_{V_2})$

$N \leftarrow D(1^n)$

$e = Enc_{pk_{V_1}}(N, pk_P)$

$s = B(sk_P, pk_P, pk_V, N)$

Assuming the key agreement protocol is D-AKA-private and the cryptosystem is IND-CCA secure, then the variant of Eff-pkDB is strong private in HPVP model.

AN INSTANCE OF EFF-PKDB

NONCE-DH+OTDB*

$sk_V \in \mathbb{Z}_q$
$pk_V = g^{sk_V}$

sk_V, pk_V, pk_P

Public parameter G order of q and $g \in G$

N, pk_P

sk_P, pk_P, pk_V $sk_P \in \mathbb{Z}_q$
$pk_P = g^{sk_P}$

$s = H(g, pk_P, pk_V, pk_P^{sk_V}, N)$

Pick $N \in \{0,1\}^\ell$
$s = H(g, pk_P, pk_V, pk_V^{sk_P}, N)$
$a = N_V \oplus s$

pick $N_V \in \{0,1\}^{2n}$
$a = N_V \oplus s$

N_V

for $i = 0$ to n

c_i

start timer

r_i

end timer

$r_i = a_{2i+c_i}$

check if $\forall i\ rtt_i < 2B$ and r_i is correct

Out

* S. Vaudenay, Private and Secure Distance Bounding: Application to NFC Payment, FC 2015

OUTLINE

✓**EFFICIENT PUBLIC-KEY DB PROTOCOL**

- Introduction
- Weak-authenticated Key Agreement
- Eff-pkDB and its private variant
- **Comparison**

✓ ACCESS CONTROL WITH DB

- Introduction
- Security and Privacy model for AC
- Our Framework
- Conclusion

COMPARISON

Protocol	Security	Privacy	PK Operation	Number of Computations
Brands-Chaum	MiM, DF	No privacy	1 commitment, 1 signature	1 EC multiplication, 2 hashing, 1 modular inversion, 1 random string selection
HPO (Hermans et al.)	MiM, DF	Weak		4 EC multiplication, 2 random string selections, 2 mappings
PrivDB (Vaudenay)	MiM, DF, DH	Strong	1 signature, 1 IND-CCA encryption	3 EC multiplication, 2 hashing, 2 random string selections, 1 symmetric key encryption, 1 modular inversion, 1mapping, 1 MAC
ProProx (Vaudenay)	MiM, DF, DH, TF	No Privacy	n+1 commitment, n ZK proofs	
eProProx (Vaudenay)	MiM, DF, DH, TF	Strong	1 encryption, n+1 commitments, n ZK proofs	
TREAD (Avoine et al.)	MiM, DF, DH, TF*	Strong	1 signature, 1 IND-CCA encryption	3 EC multiplication, 2 hashing, 2 random string selections, 1 symmetric key encryption, 1 modular inversion, 1mapping, 1 MAC
Eff-pkDB	MiM, DF, DH, (TF*)	No Privacy	1 D-AKA secure KA protocol	1 EC multiplication, 2 hashing, 1 random string selection,
Private Variant of Eff-pkDB	MiM, DF, DH, (TF*)	Strong	1 IND-CCA encryption, 1 D-AKA secure KA protocol	3 EC multiplication, 2 hashing, 2 random string selections, 1 symmetric key encryption, 1 MAC

* ECDSA for the signature scheme and ECIES for the IND-CCA secure encryption scheme

OUTLINE

✓ EFFICIENT PUBLIC-KEY DB PROTOCOL

- Introduction
- Weak-authenticated Key Agreement
- Eff-pkDB and its private variant
- Comparison

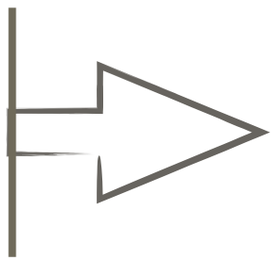
✓ **ACCESS CONTROL WITH DB**

- **Introduction**
- Security and Privacy model for AC
- Our Framework
- Conclusion

INTRODUCTION
PREVIOUS WORKS

- Smart Card Alliance: Defines the components (controller, database, reader and tag) and defines security in a informal way

- PLAID*
- OPACITY**



Based on establishing secret key and mutual authentication

- Privacy is an important issue in access control.

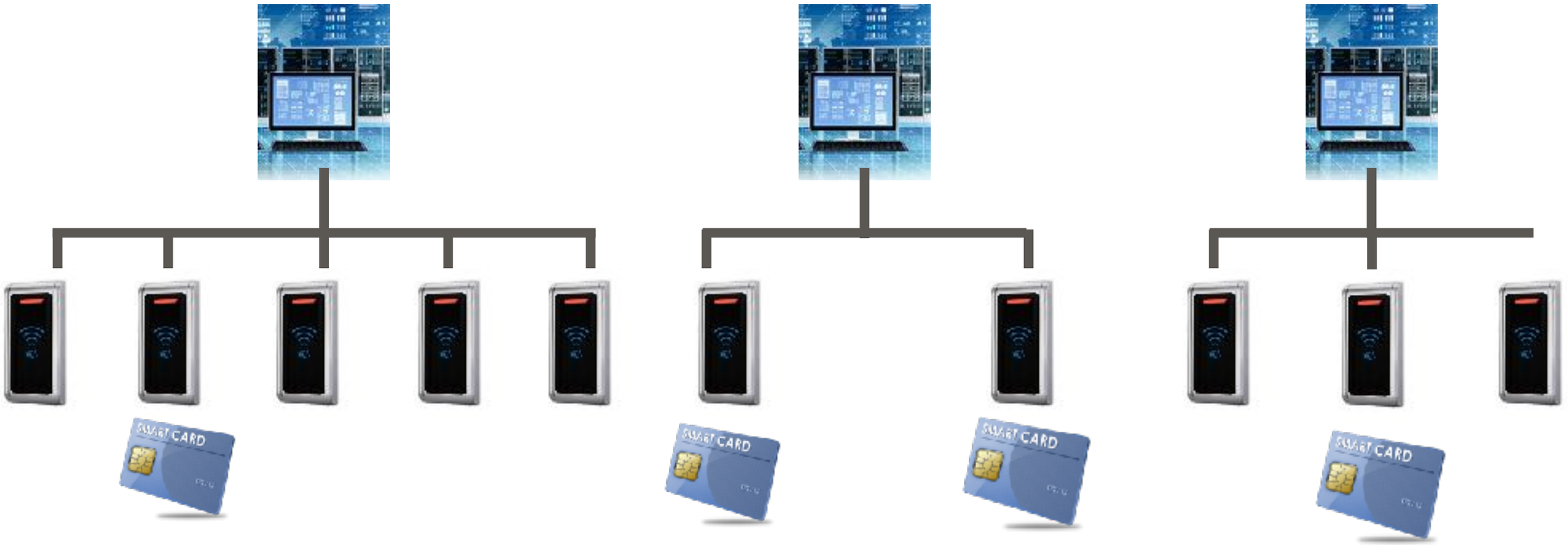
* C. A. governments Department of Human Services (DHS). Protocol for lightweight authentication of identity (PLAID), 2010.
* * S. C. Alliance. Industry technical contributions: Opacity, 2013

INTRODUCTION

THE STRUCTURE (CONTROLLERS, READERS, TAGS)

INTRODUCTION

THE STRUCTURE (CONTROLLERS, READERS, TAGS)



INTRODUCTION
COMPOSITION WITH DB

Controller	Reader	Tag
		

INTRODUCTION
COMPOSITION WITH DB

Controller | Reader | Tag

An AC Protocol

INTRODUCTION
COMPOSITION WITH DB

Controller | Reader | Tag

An AC Protocol



A DB protocol


INTRODUCTION
COMPOSITION WITH DB

Controller | Reader | Tag

An AC Protocol



A DB protocol


OUTLINE

- ✓ EFFICIENT PUBLIC-KEY DB PROTOCOL
  - Introduction
  - Weak-authenticated Key Agreement
  - Eff-pkDB and its private variant
  - Comparison
- ✓ **ACCESS CONTROL WITH DB**
  - Introduction
  - **Security and Privacy model for AC**
  - Our Framework
  - Conclusion

ACCESS CONTROL

CONTACTLESS AC PROTOCOL

Controller and Database

Reader

Tag

ACCESS CONTROL
CONTACTLESS AC PROTOCOL

$\mathsf{Gen}_C \rightarrow (\mathsf{sk}_C, \mathsf{pk}_C)$

$\mathsf{Gen}_T \rightarrow (\mathsf{sk}_{T_1}, \mathsf{pk}_{T_1})$
$(\mathsf{sk}_{T_2}, \mathsf{pk}_{T_2})$
$\ldots$
$(\mathsf{sk}_{T_k}, \mathsf{pk}_{T_k})$

Controller and Database

Reader

Tag

ACCESS CONTROL
CONTACTLESS AC PROTOCOL

$\mathsf{Gen}_C \rightarrow (\mathsf{sk}_C, \mathsf{pk}_C)$

$\mathsf{Gen}_T \rightarrow (\mathsf{sk}_{T_1}, \mathsf{pk}_{T_1})$
$(\mathsf{sk}_{T_2}, \mathsf{pk}_{T_2})$
$\ldots$
$(\mathsf{sk}_{T_k}, \mathsf{pk}_{T_k})$

Controller and Database

$\mathcal{C}(\mathsf{sk}_C, \mathsf{pk}_C, DataB, B)$

Reader

$\mathcal{R}(loc_R)$

Tag

$\mathcal{T}(\mathsf{sk}_T, \mathsf{pk}_T, \mathsf{pk}_C, req)$

ACCESS CONTROL
CONTACTLESS AC PROTOCOL

$\mathsf{Gen}_C \rightarrow (\mathsf{sk}_C, \mathsf{pk}_C)$

$\mathsf{Gen}_T \rightarrow (\mathsf{sk}_{T_1}, \mathsf{pk}_{T_1})$
$(\mathsf{sk}_{T_2}, \mathsf{pk}_{T_2})$
...
$(\mathsf{sk}_{T_k}, \mathsf{pk}_{T_k})$

Controller and Database

$\mathcal{C}(\mathsf{sk}_C, \mathsf{pk}_C, DataB, B)$

Out_C
$\mathsf{POut}_C = (\mathsf{pk}_T, loc_R, req)$

Reader

$\mathcal{R}(loc_R)$

Out_R

Tag

$\mathcal{T}(\mathsf{sk}_T, \mathsf{pk}_T, \mathsf{pk}_C, req)$

ACCESS CONTROL
CONTACTLESS AC PROTOCOL

$\mathsf{Gen}_C \rightarrow (\mathsf{sk}_C, \mathsf{pk}_C)$

$\mathsf{Gen}_T \rightarrow (\mathsf{sk}_{T_1}, \mathsf{pk}_{T_1})$
$(\mathsf{sk}_{T_2}, \mathsf{pk}_{T_2})$
...
$(\mathsf{sk}_{T_k}, \mathsf{pk}_{T_k})$

Controller and Database

$\mathcal{C}(\mathsf{sk}_C, \mathsf{pk}_C, DataB, B)$

Out_C
$\mathsf{POut}_C = (\mathsf{pk}_T, loc_R, req)$

Reader

$\mathcal{R}(loc_R)$

Out_R

Tag

$\mathcal{T}(\mathsf{sk}_T, \mathsf{pk}_T, \mathsf{pk}_C, req)$

$\mathbf{DataB} = \{(\mathsf{pk}_1, loc_{R_i}, req_x), (\mathsf{pk}_2, loc_{R_j}, req_y), ..., (\mathsf{pk}_k, loc_{R_i}, req_x)\}$

ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

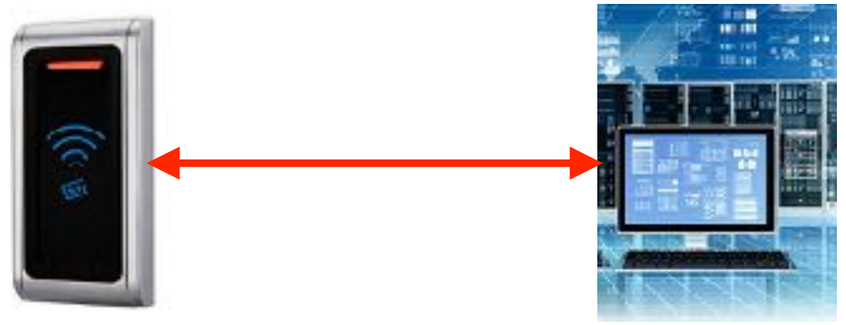
ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

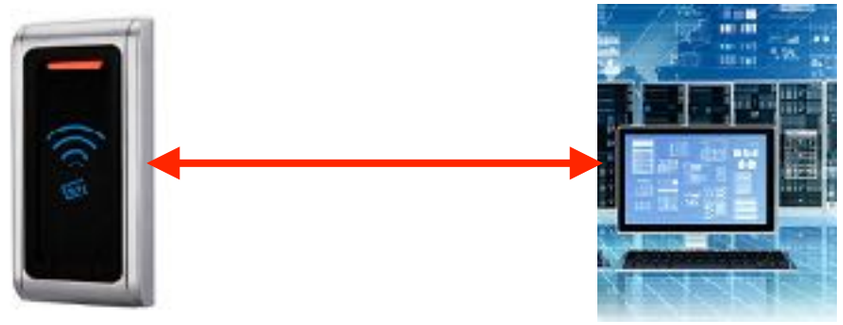
Secure and authenticated



ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

Secure and authenticated



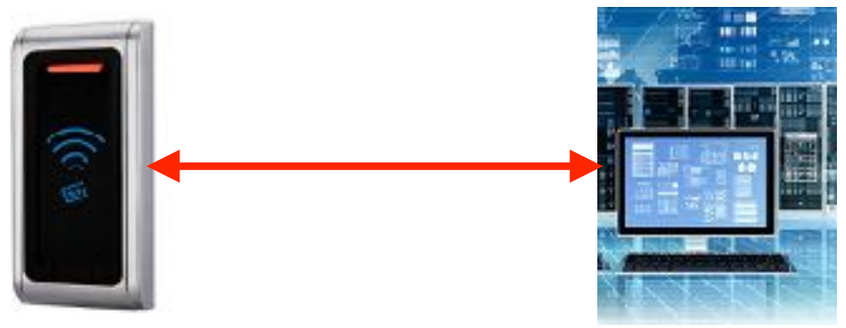
Create Database
Create fake tags

ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

Activate(req)

Secure and authenticated



Create Database
Create fake tags

ACCESS CONTROL

ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

req

Activate(req)

Secure and authenticated

Create Database
Create fake tags

ACCESS CONTROL

ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

req

Activate(req)

Move(loc')

Secure and authenticated

Create Database
Create fake tags

ACCESS CONTROL

ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

req

Activate(req)

Move(loc')

Secure and authenticated

Create Database
Create fake tags

ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

req

Activate(req)

Terminate

Move(loc')

Secure and authenticated

Create Database
Create fake tags

ACCESS CONTROL
ADVERSARIAL AND COMMUNICATION MODEL

Tags are honest

req

Activate(req)

Terminate

Move(loc')

Secure and authenticated

Create Database
Create fake tags

- It can intercept, observe, replace the messages between readers and tags
- It can create may instances of each party

ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$\{\mathsf{pk}_{T_i}\}, \mathsf{pk}_C$

ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$\{\mathsf{pk}_{T_i}\}, \mathsf{pk}_C$

Create fake tags $\{\tilde{\mathsf{sk}}_T, \tilde{\mathsf{pk}}_T\}$

Create $DataB$

ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$\{\mathsf{pk}_{T_i}\}, \mathsf{pk}_C$ →

← $DataB$

Create fake tags $\{\tilde{\mathsf{sk}}_T, \tilde{\mathsf{pk}}_T\}$

Create $DataB$

ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$

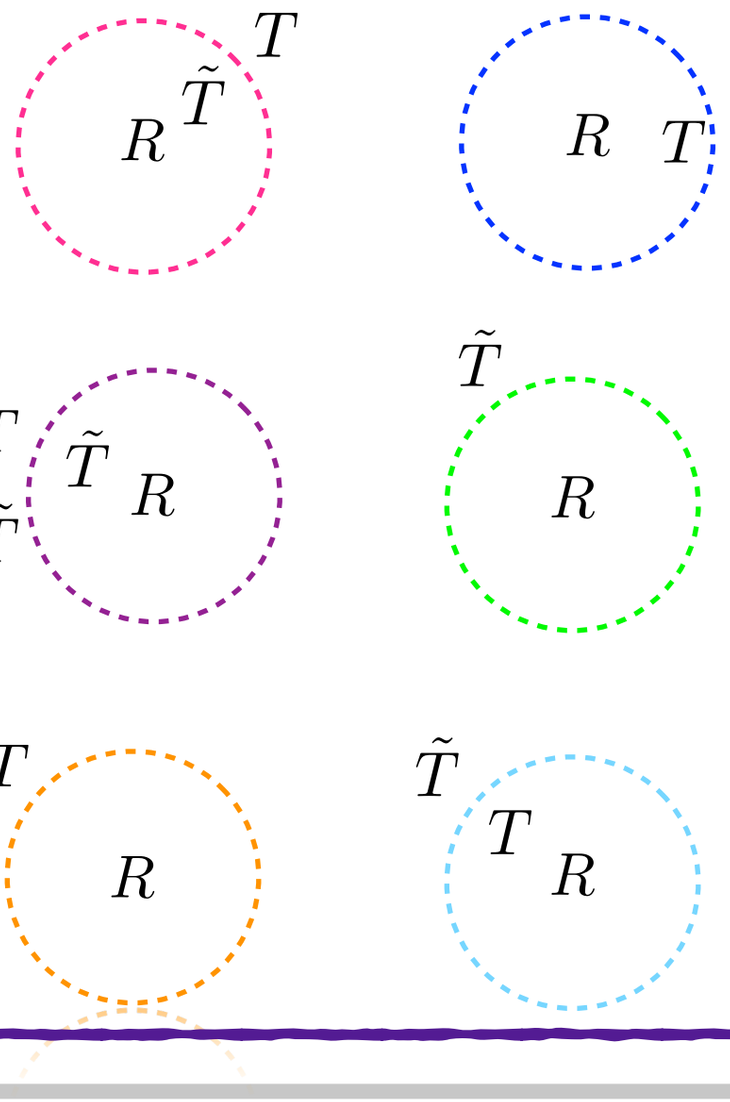
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



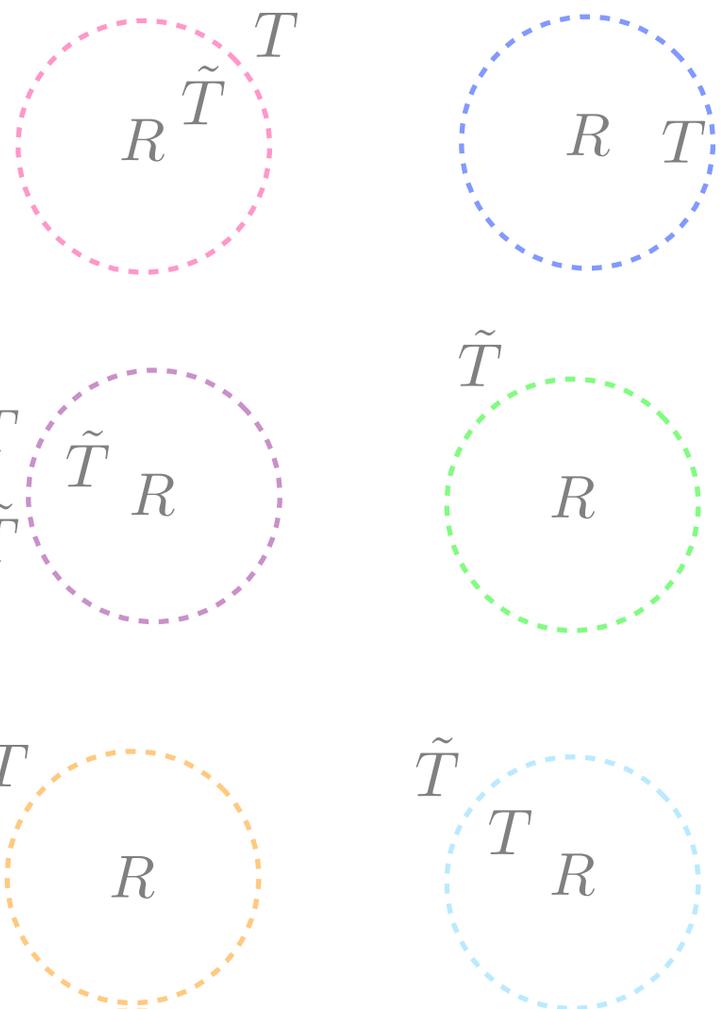
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

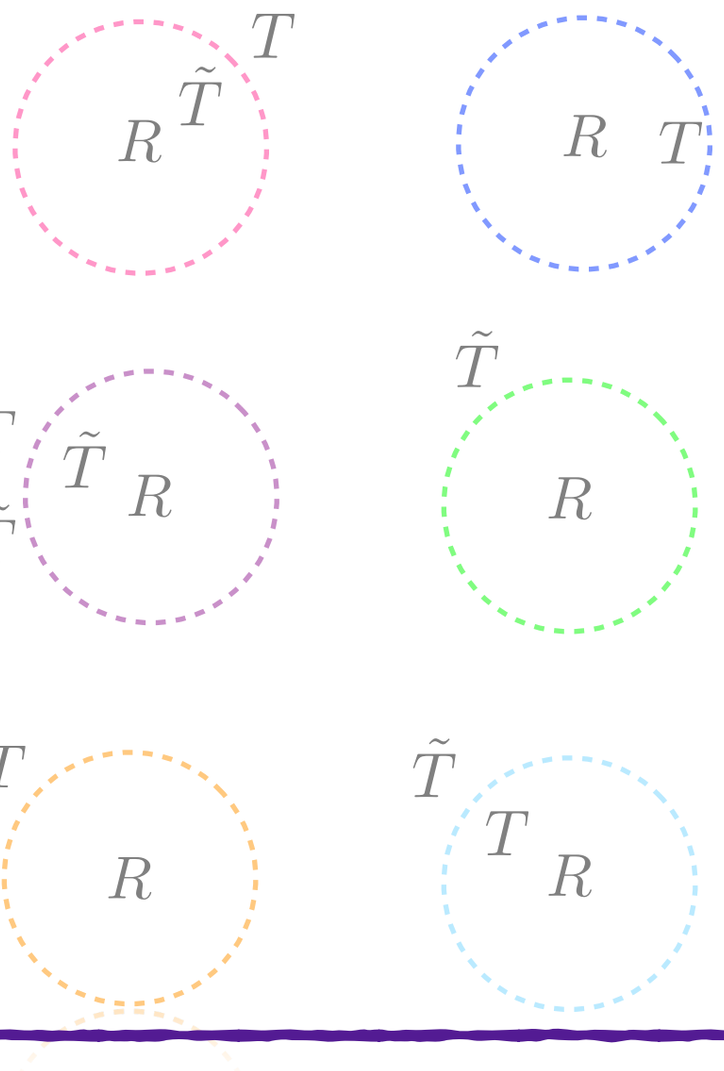
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

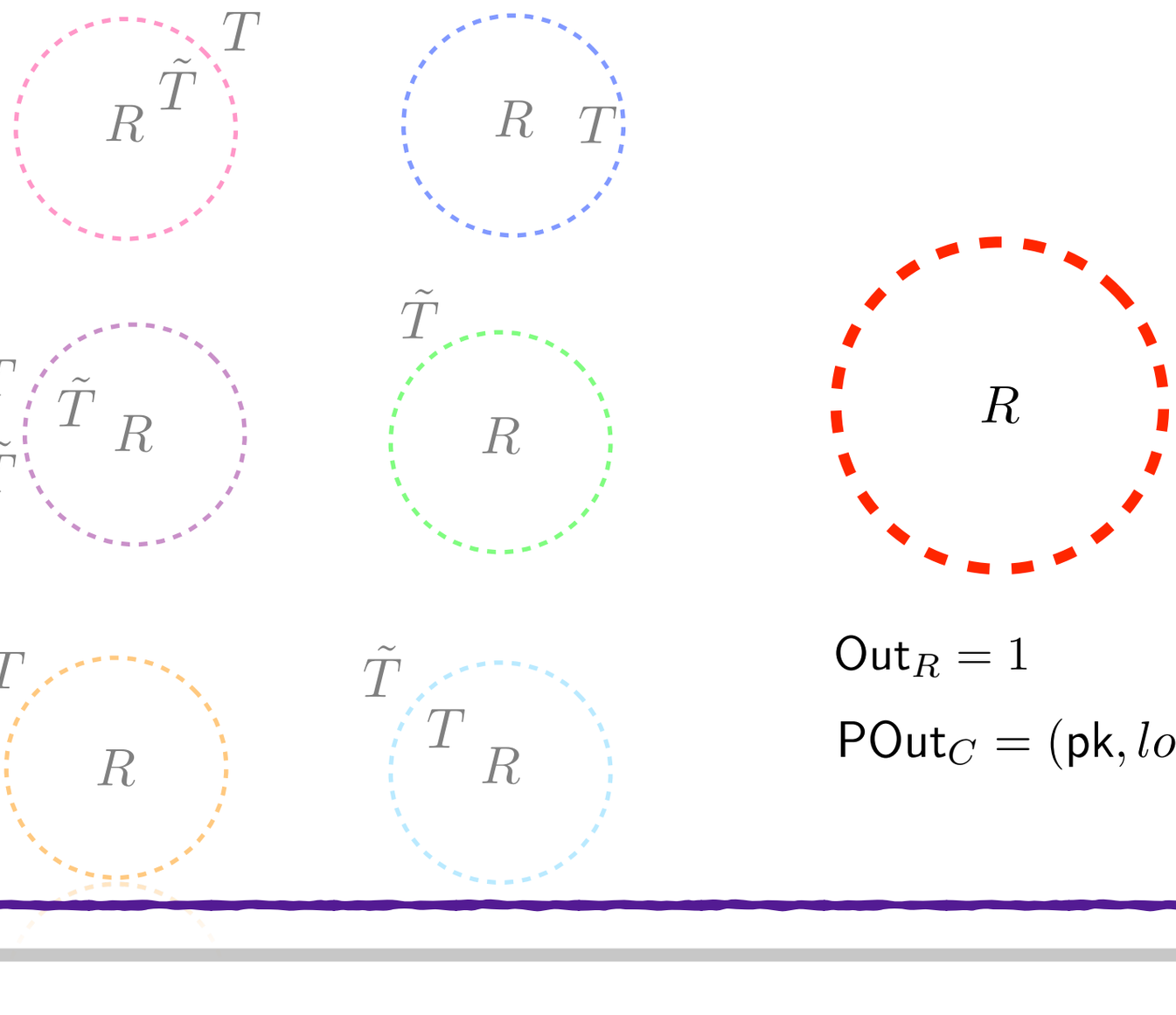
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$

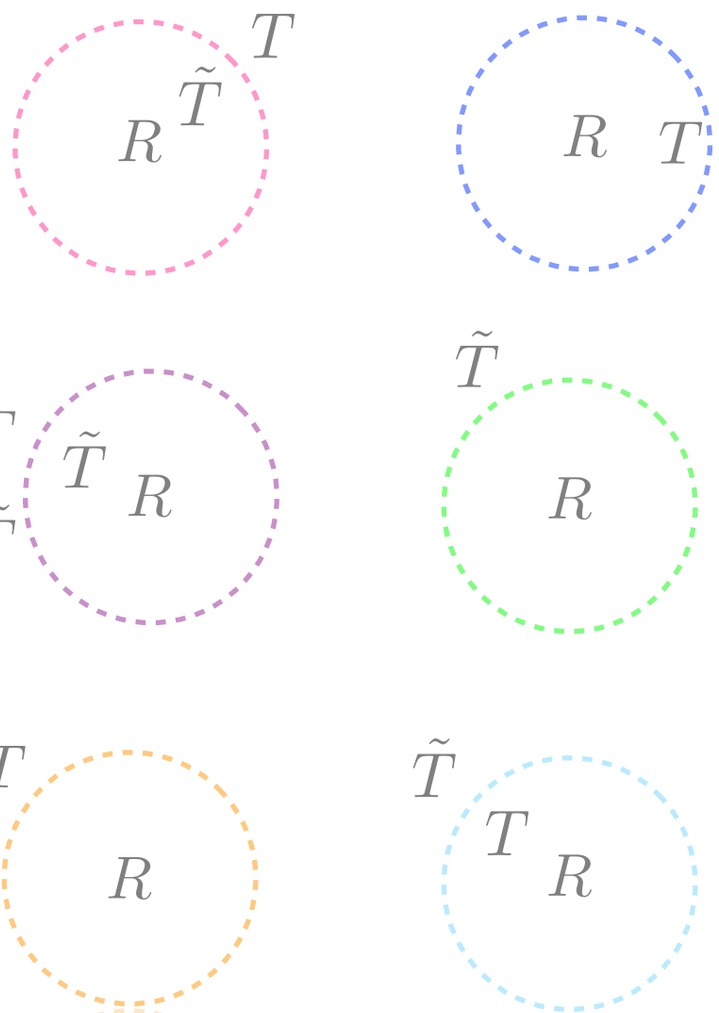
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$
- pk is honest tag's key and no close honest tag (MiM)

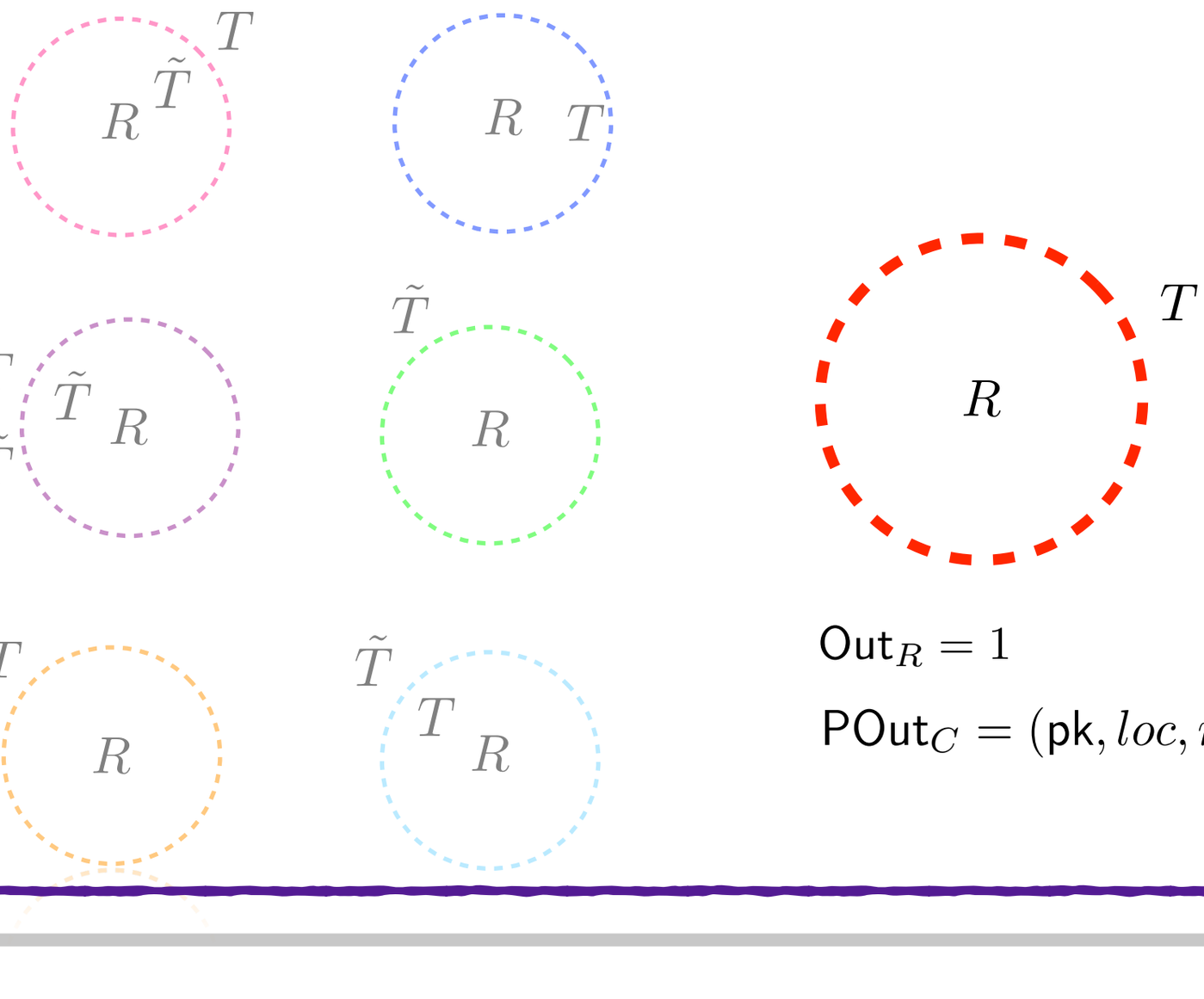
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$
- pk is honest tag's key and no close honest tag (MiM)

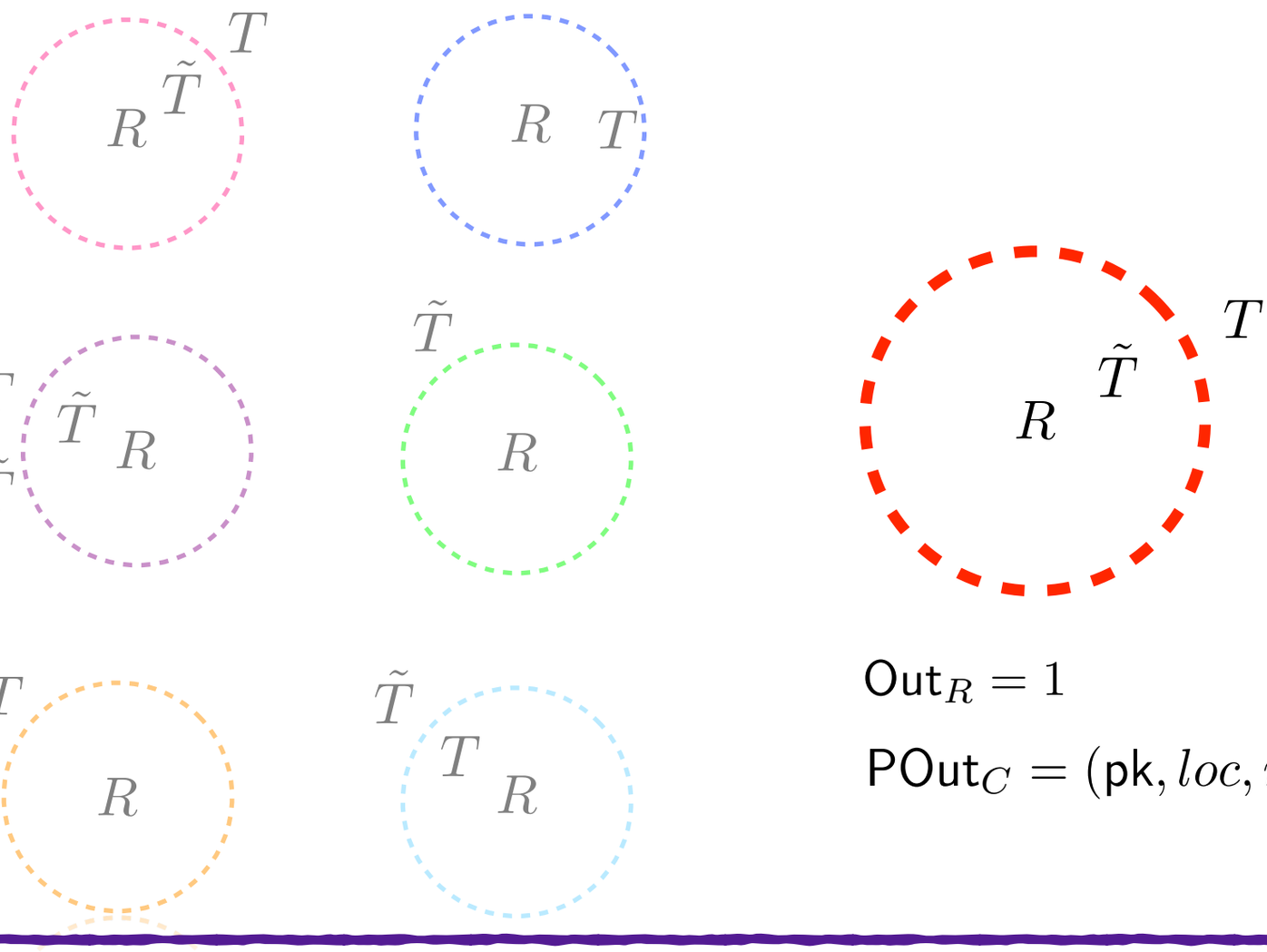
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$
- pk is honest tag's key and no close honest tag (MiM)

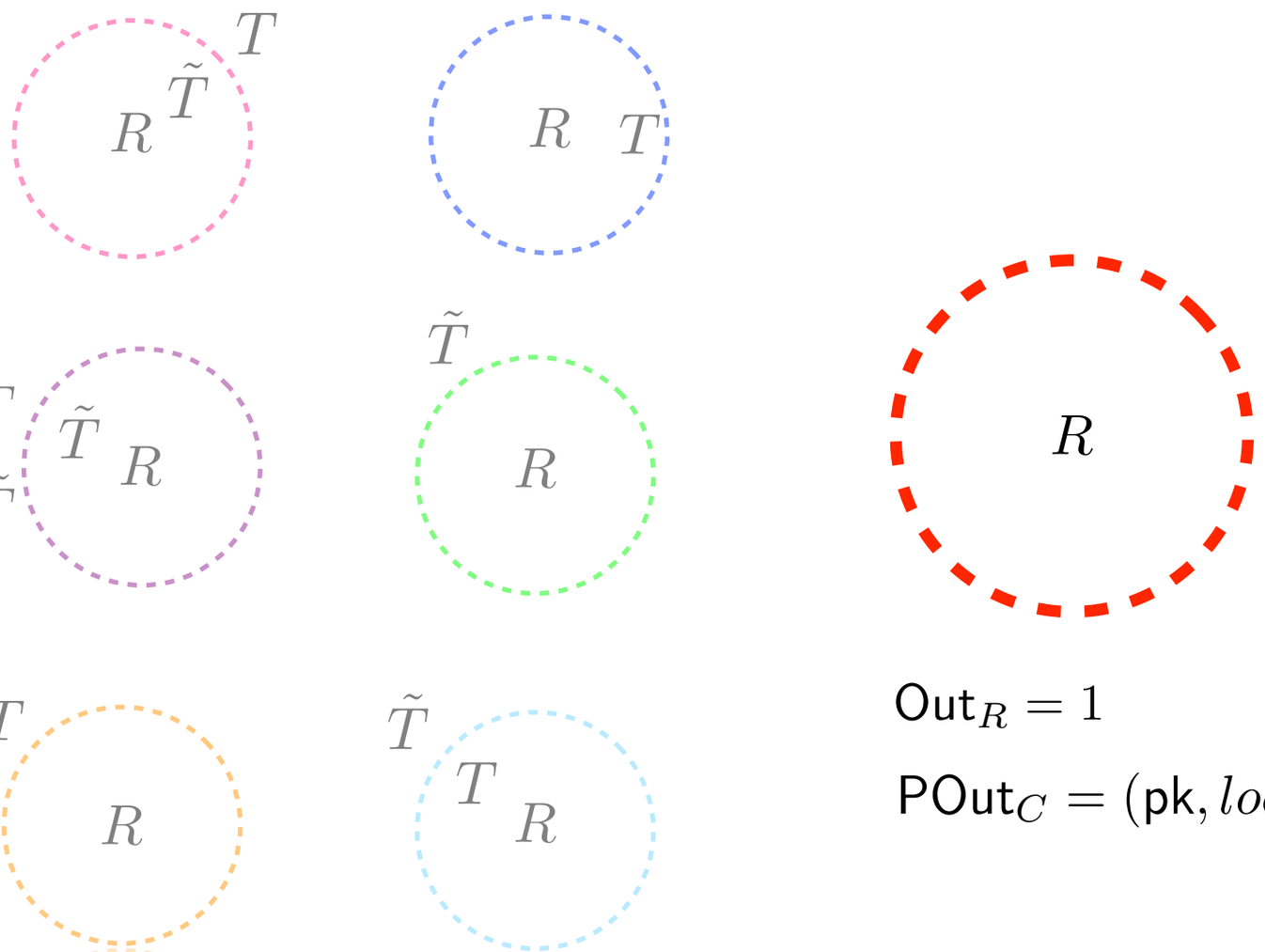
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$
- pk is honest tag's key and no close honest tag (MiM)
- pk is fake tag's key and no close fake tag (DH)

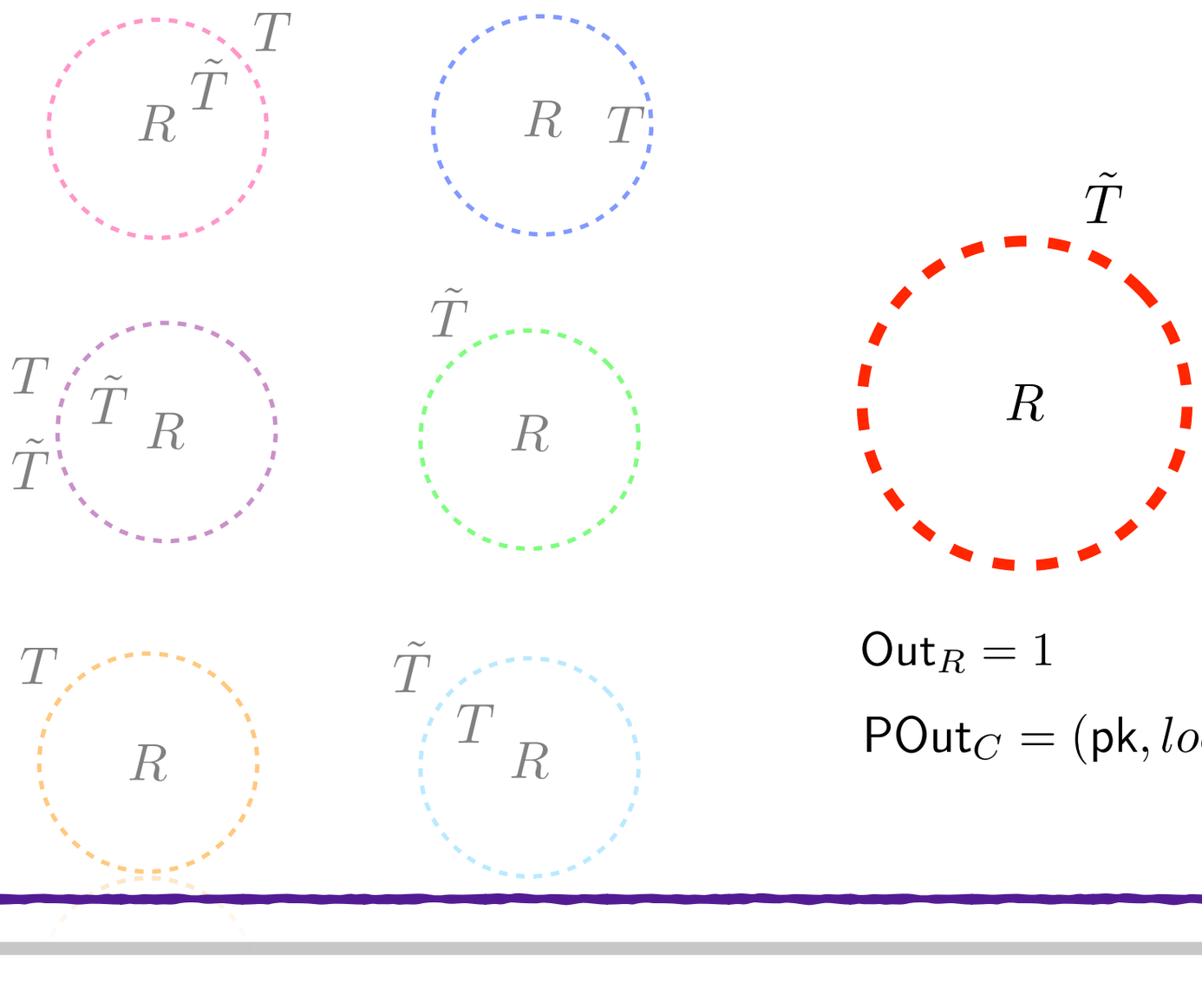
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

$DataB$



$\mathsf{Out}_R = 1$

$\mathsf{POut}_C = (\mathsf{pk}, loc, req)$

Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$
- pk is honest tag's key and no close honest tag (MiM)
- pk is fake tag's key and no close fake tag (DH)

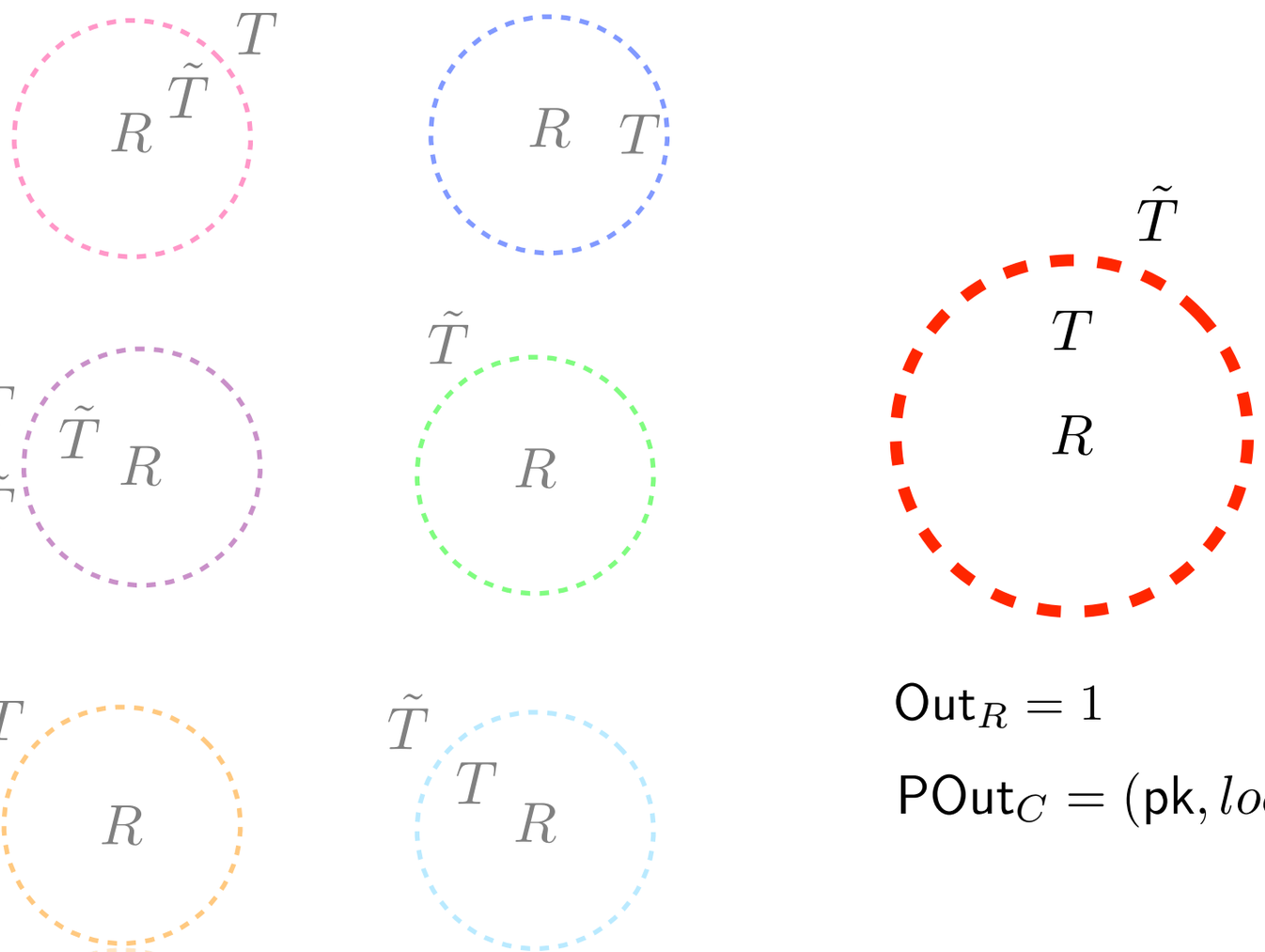
ACCESS CONTROL

AC-GAME

$\mathsf{Gen}_C \rightarrow \mathsf{pk}_C, \mathsf{sk}_C$

$\mathsf{Gen}_T \rightarrow \{\mathsf{pk}_{T_i}, \mathsf{sk}_{T_i}\}$

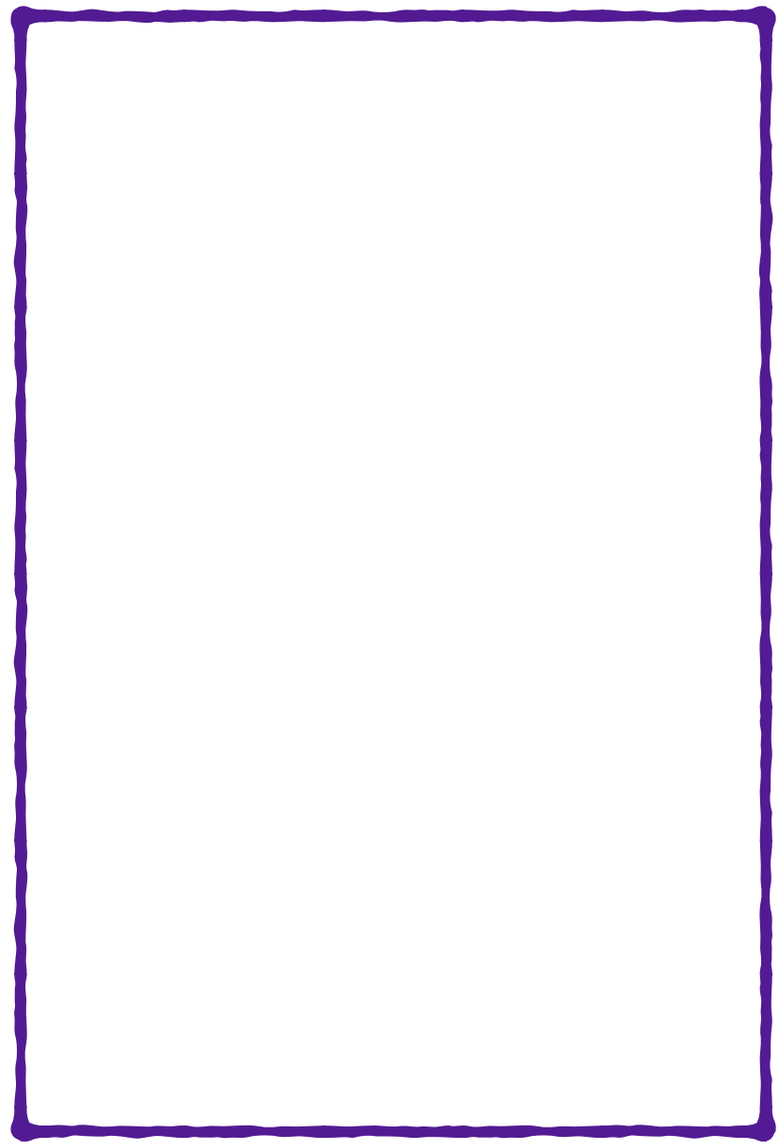
$DataB$



Adversary wins if one of the conditions are satisfied:

- $\mathsf{POut}_C = (\mathsf{pk}, loc, req) \notin DataB$
- pk is honest tag's key and no close honest tag (MiM)
- pk is fake tag's key and no close fake tag (DH)

ACCESS CONTROL
PRIVACY



ACCESS CONTROL
PRIVACY

pick $b \in \{\ell, r\}$

ACCESS CONTROL
PRIVACY

Adversary can pair tags

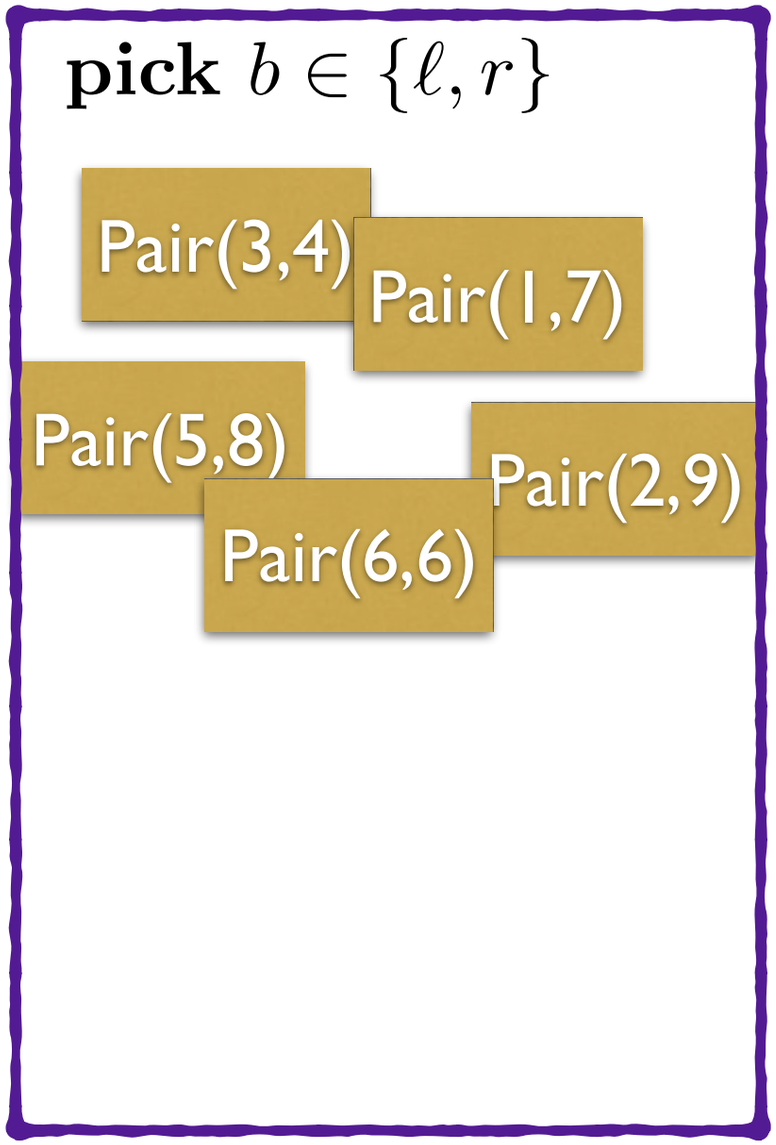
Draw(T_i, T_j)

pick $b \in \{\ell, r\}$

ACCESS CONTROL
PRIVACY

Adversary can pair tags

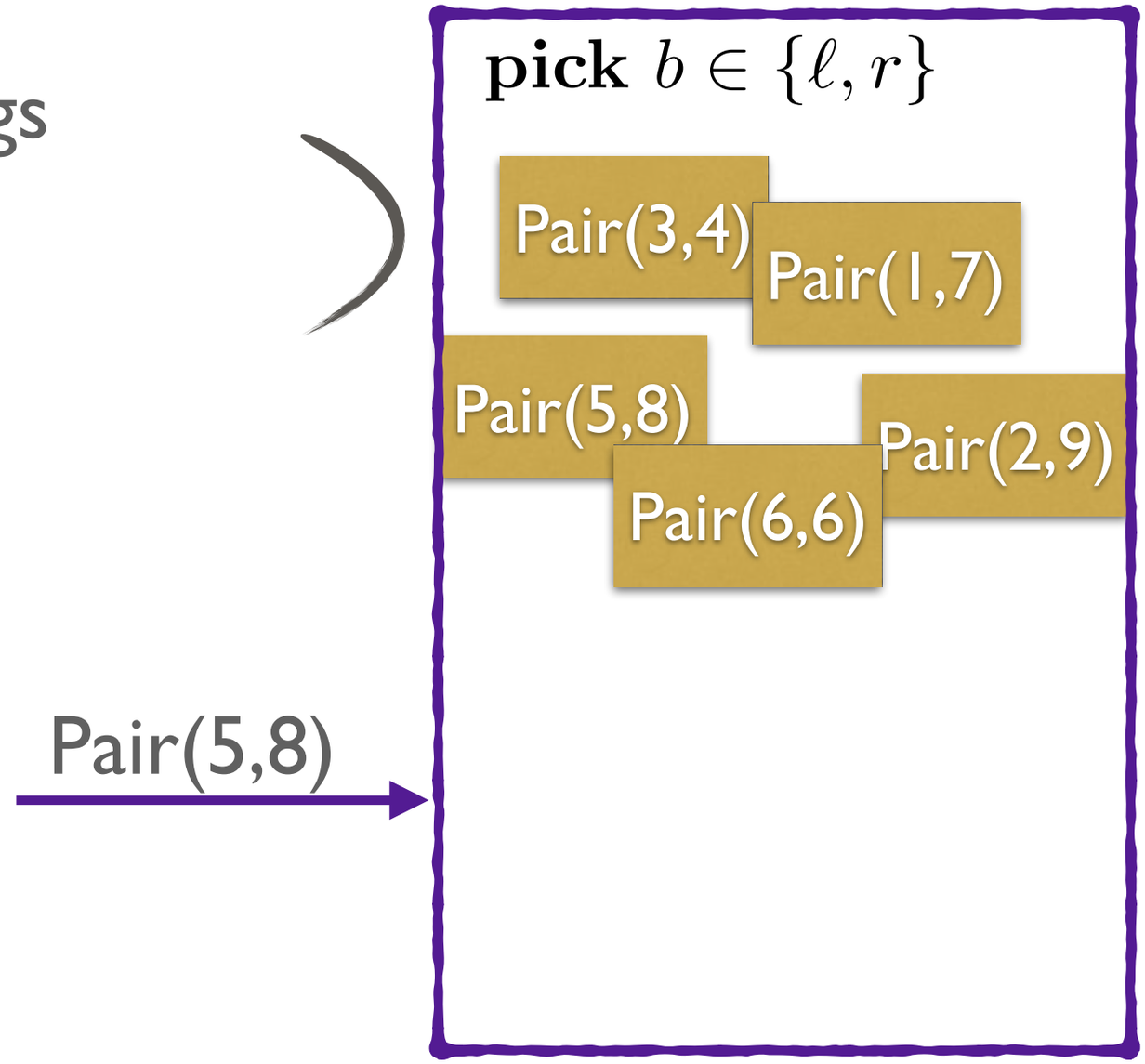
Draw(T_i, T_j)



ACCESS CONTROL
PRIVACY

Adversary can pair tags

Draw(T_i, T_j)



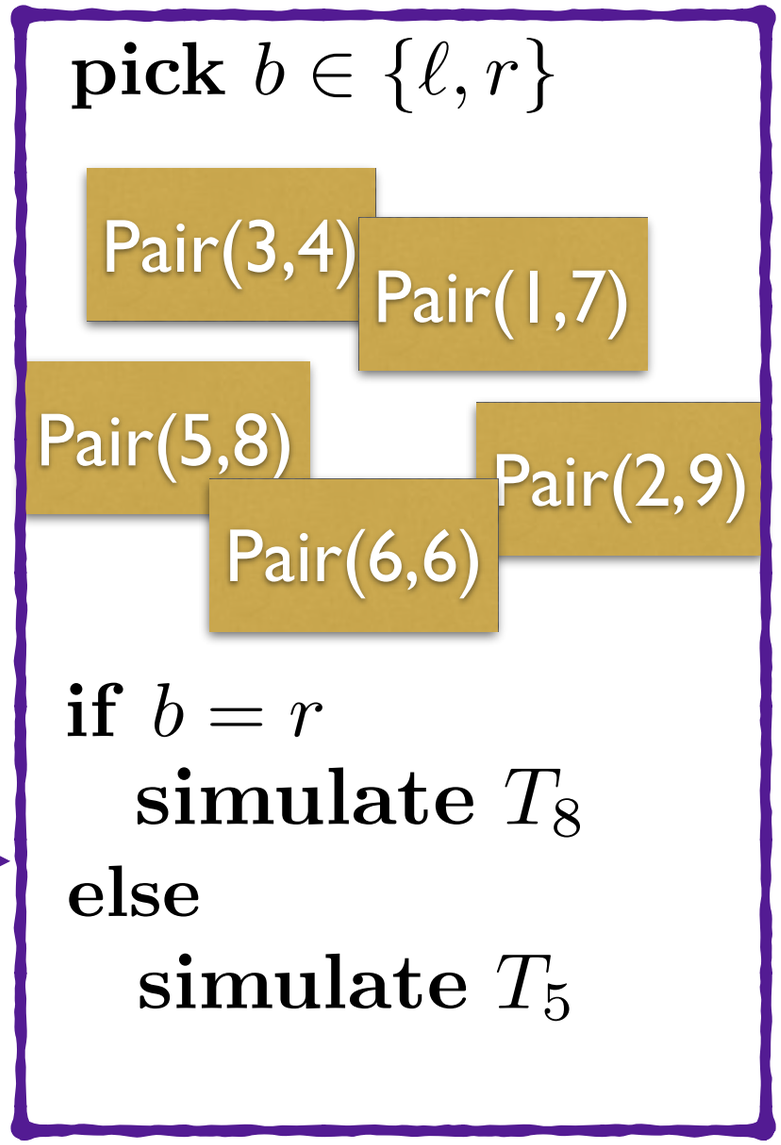
Pair(5,8)

ACCESS CONTROL
PRIVACY

Adversary can pair tags

Draw(T_i, T_j)

Pair(5,8)



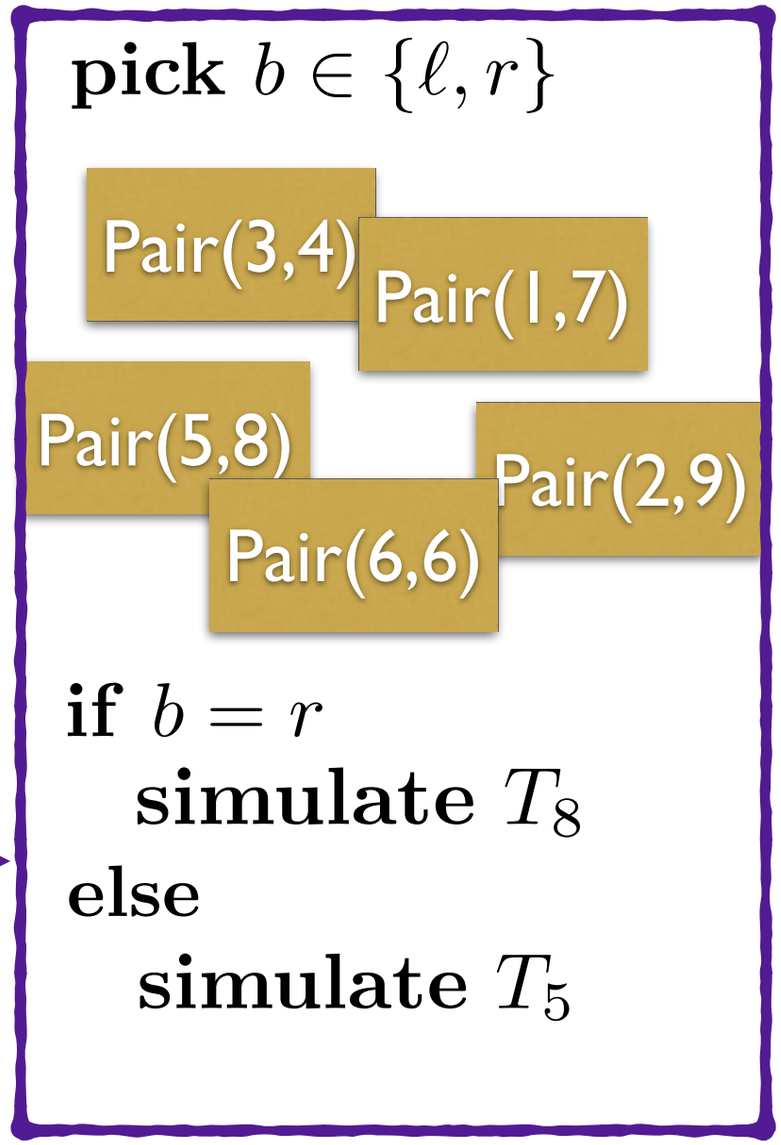
ACCESS CONTROL
PRIVACY

Adversary can pair tags

Draw(T_i, T_j)

b'

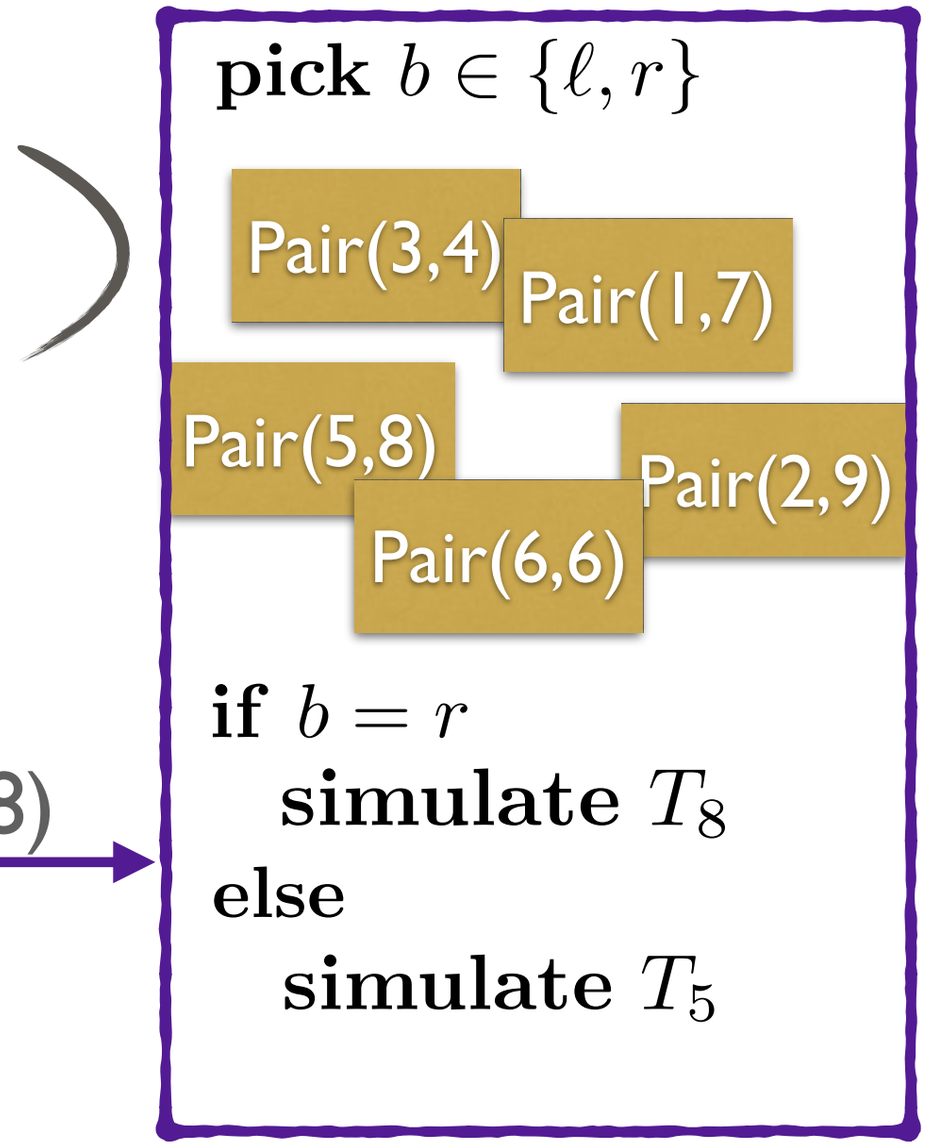
Pair(5,8)



ACCESS CONTROL
PRIVACY

Adversary can pair tags

Draw(T_i, T_j)



Pair(5,8)

b'

Adversary wins **if** $b' = b$

ACCESS CONTROL
PRIVACY

Adversary can pair tags

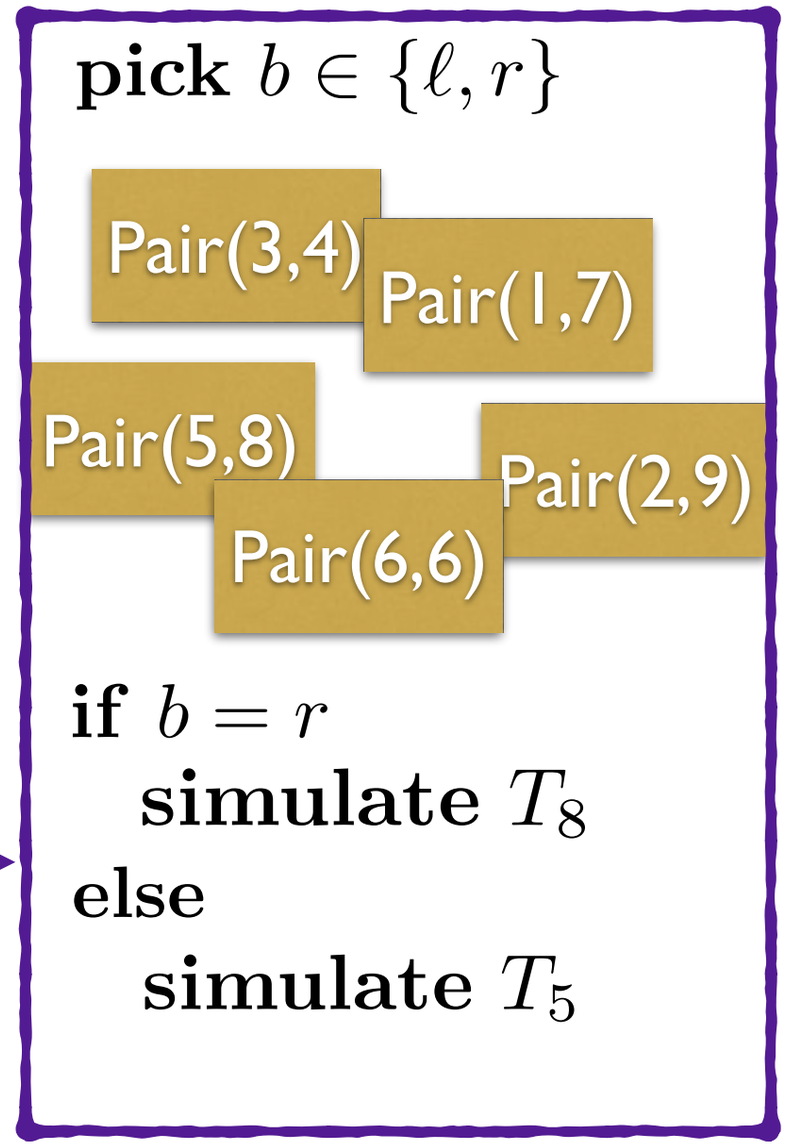
Draw(T_i, T_j)

- T_i and T_j are at the same location
- T_i and T_j have the same access privileges

b'

Adversary wins **if** $b' = b$

Pair(5,8)



OUTLINE

- ✓ EFFICIENT PUBLIC-KEY DB PROTOCOL
  - Introduction
  - Weak-authenticated Key Agreement
  - Eff-pkDB and its private variant
  - Comparison
- ✓ **ACCESS CONTROL WITH DB**
  - Introduction
  - Security and Privacy model for AC
  - **Our Framework**
  - Conclusion

AC WITH DB

OUR FRAMEWORK

Controller	Reader	Tag
$(\mathsf{sk}_C, \mathsf{pk}_C, DataB, B)$	(loc_R)	$(\mathsf{sk}_T, \mathsf{pk}_T, \mathsf{pk}_C, req)$

AC WITH DB

OUR FRAMEWORK

<u>Controller</u>

$(\mathsf{sk}_C, \mathsf{pk}_C, DataB, B)$

<u>Reader</u>

(loc_R)

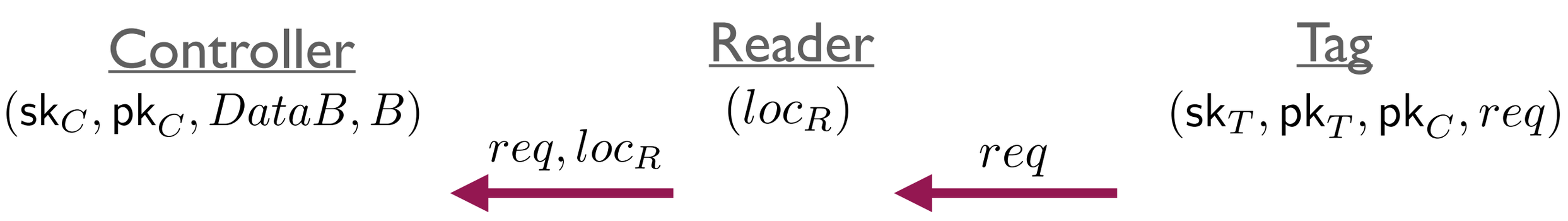
req

<u>Tag</u>

$(\mathsf{sk}_T, \mathsf{pk}_T, \mathsf{pk}_C, req)$

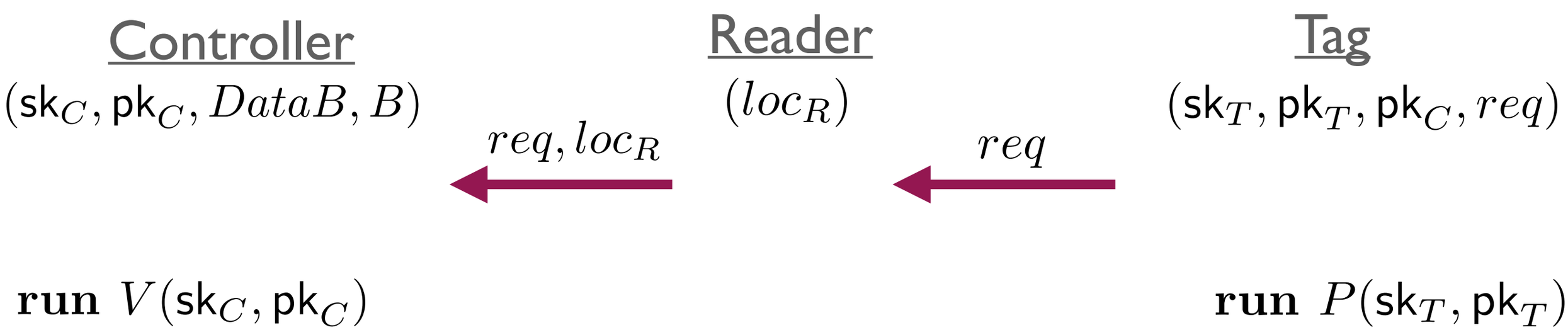
AC WITH DB

OUR FRAMEWORK



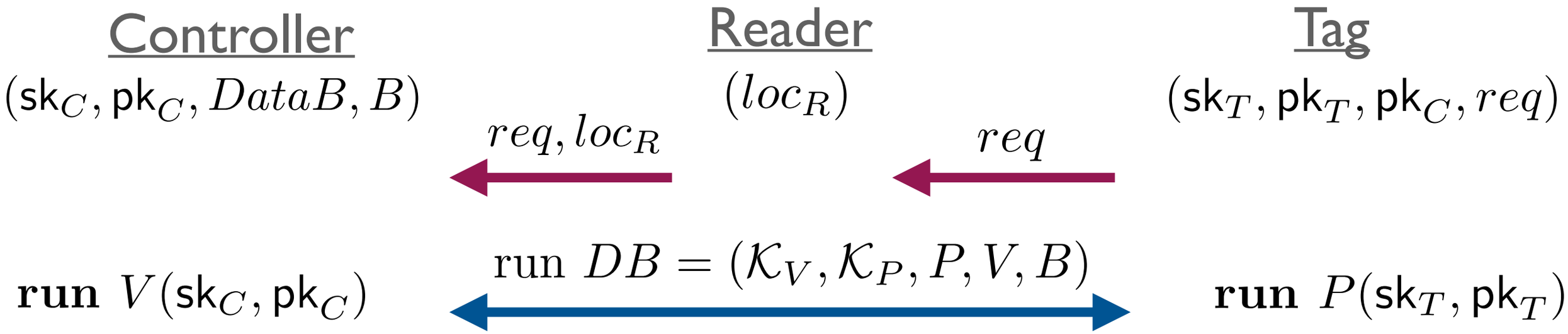
AC WITH DB

OUR FRAMEWORK



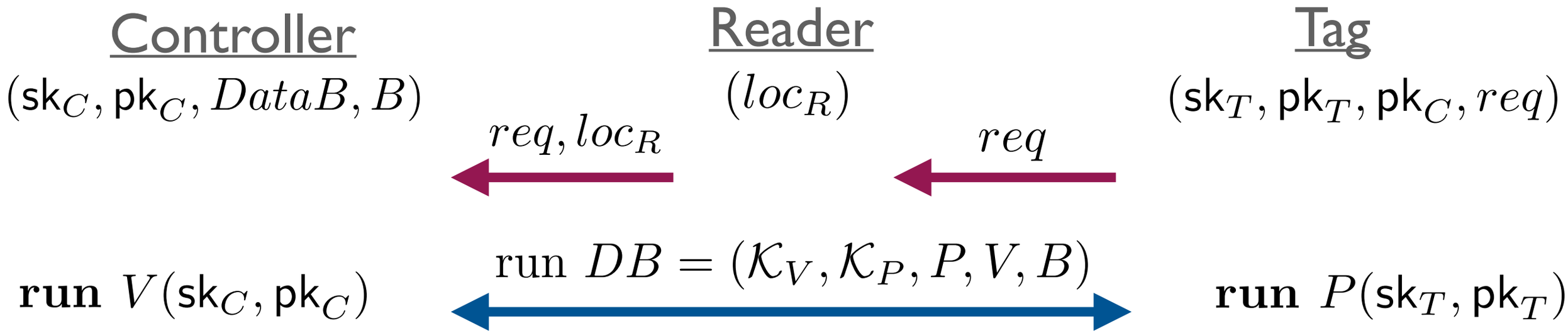
AC WITH DB

OUR FRAMEWORK



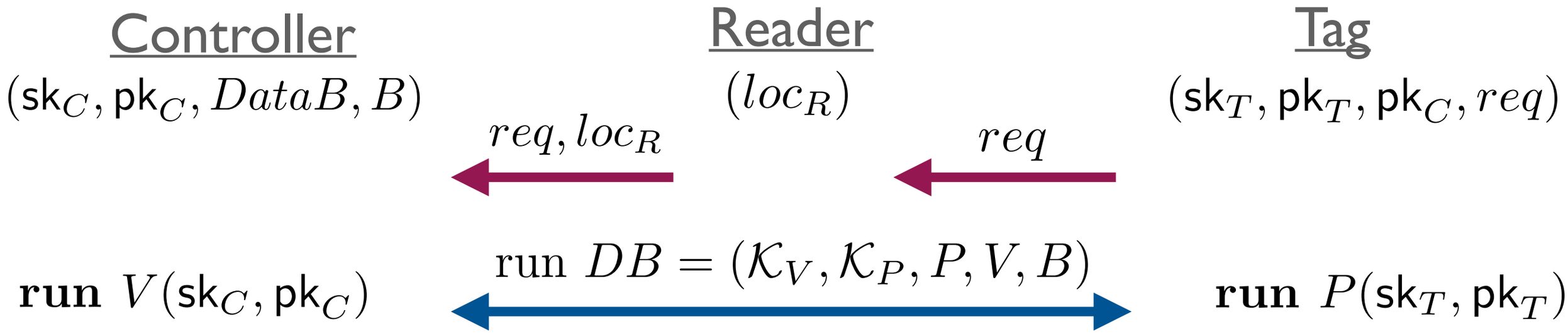
AC WITH DB

OUR FRAMEWORK



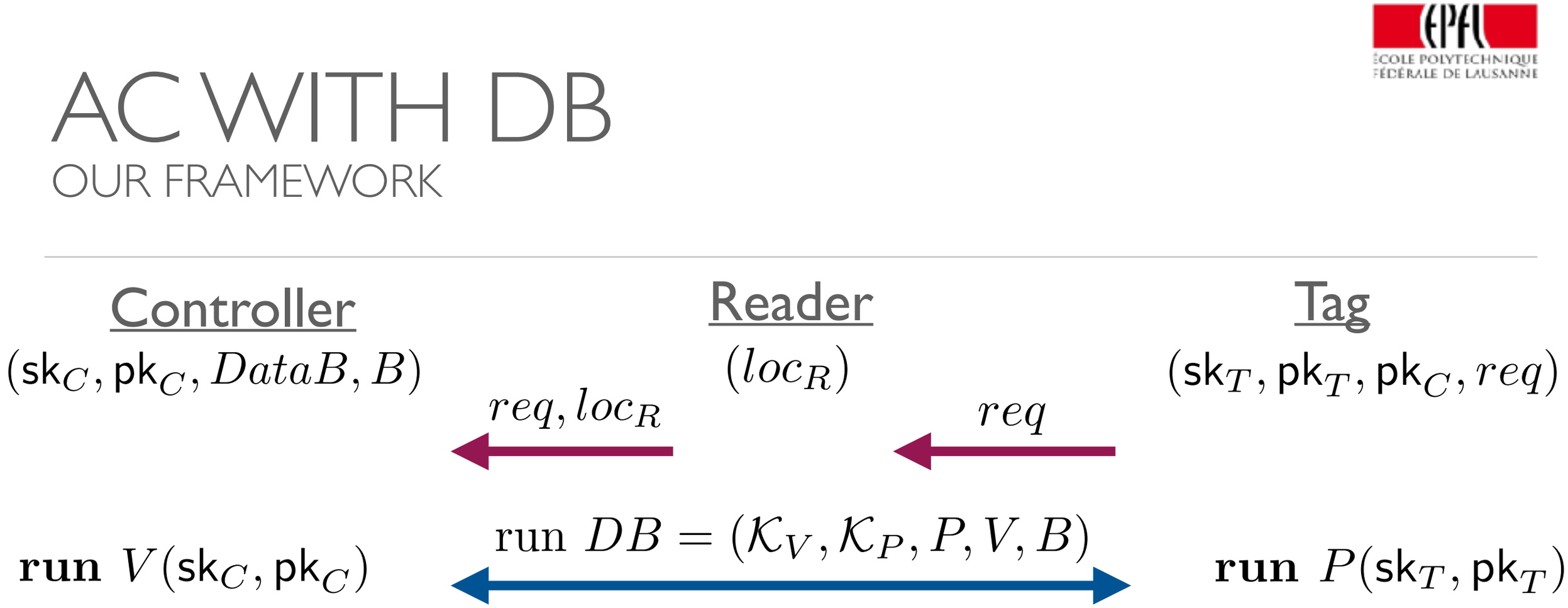
AC WITH DB

OUR FRAMEWORK



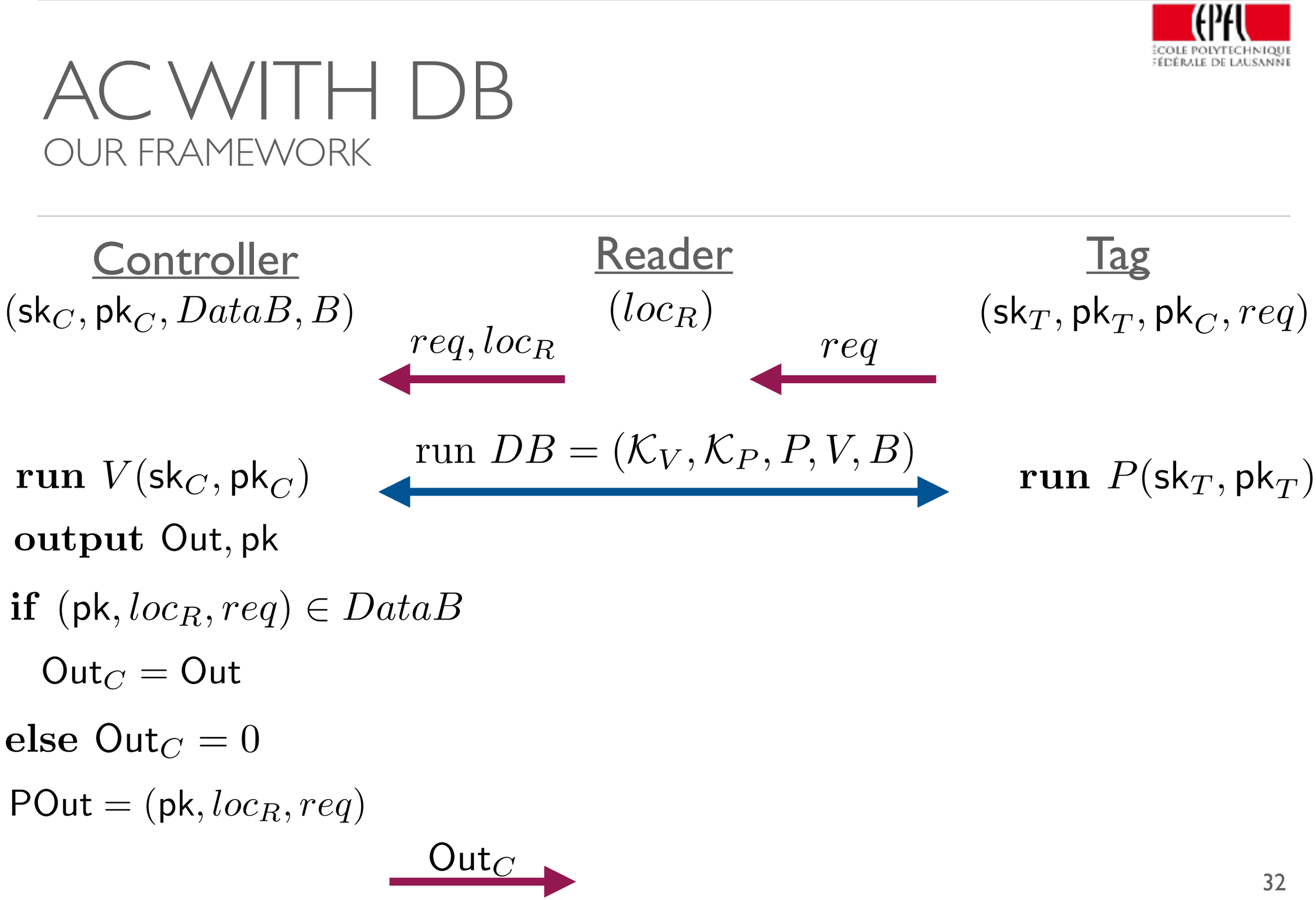
AC WITH DB

OUR FRAMEWORK



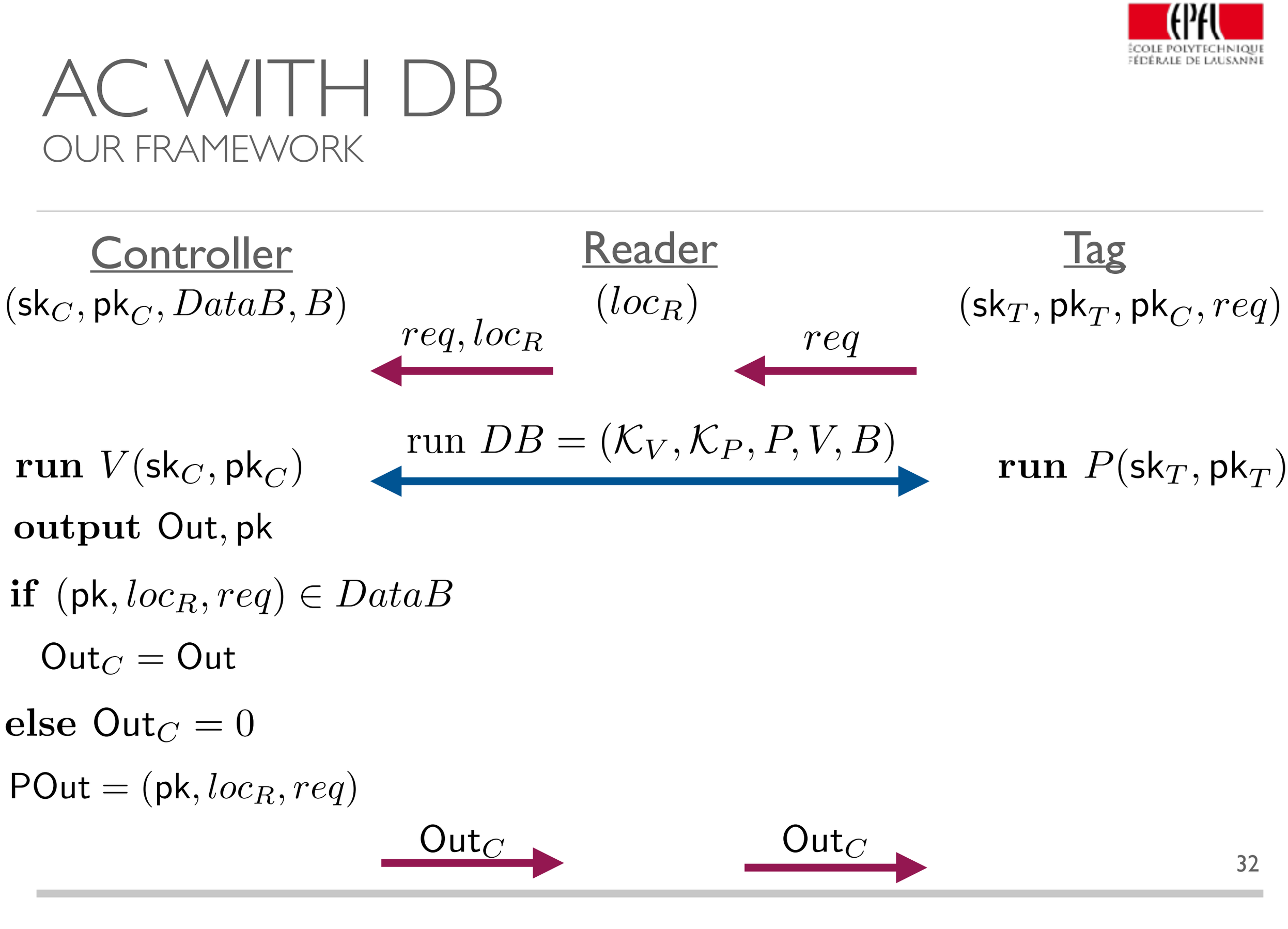
AC WITH DB

OUR FRAMEWORK



AC WITH DB

OUR FRAMEWORK



AC WITH DB

SECURITY AND PRIVACY OF OUR FRAMEWORK

SECURITY

Assuming that the DB protocol is **MiM-secure** and **DH-secure**, then an AC protocol with using this DB protocol with our framework is a secure AC protocol.

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

SECURITY AND PRIVACY OF OUR FRAMEWORK

SECURITY

Assuming that the DB protocol is **MiM-secure** and **DH-secure**, then an AC protocol with using this DB protocol with our framework is a secure AC protocol.

PRIVACY

Assuming that the DB protocol is **private** DB, then an AC protocol with our framework is private AC protocol when DataB is trivial.

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

SECURITY AND PRIVACY OF OUR FRAMEWORK

SECURITY

Assuming that the DB protocol is **MiM-secure** and **DH-secure**, then an AC protocol with using this DB protocol with our framework is a secure AC protocol.

PRIVACY

Assuming that the DB protocol is **private** DB, then an AC protocol with our framework is private AC protocol when DataB is trivial.

empty or contains all possible triplets

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$

run $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$ →

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ ↔ $DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ ↔ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$ →

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ ↔ $DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ ↔ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

AC Protocol using DB' with our framework

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$ →

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ ↔ $DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ ↔ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

AC Protocol using DB' with our framework

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$ →

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ ↔ $DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ ↔ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

AC Protocol using DB' with our framework

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$ →

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ ↔ $DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ ↔ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

AC Protocol using DB' with our framework

pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$

$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$

Pair(1,2)

AC Protocol using DB' with our framework

pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$

$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$

run $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

AC Protocol using DB' with our framework

Pair(1,2)

pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

R

T

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ $\quad DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ $\quad$ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

AC Protocol using DB' with our framework

Pair(1,2)

pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

R $\longrightarrow$ T

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ $\quad DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ $\quad$ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

Pair(1,2)

AC Protocol using DB' with our framework

R $\quad flag = 0$ $\quad flag = 1$ $\quad T$

pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$ $\quad DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$ $\quad$ **run** $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

Pair(1,2)

AC Protocol using DB' with our framework

R $\quad flag = 0$ $\quad flag = 1$ $\quad T$

Out_R

pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

PRIVACY

$$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B) \longrightarrow DB' = (\mathcal{K}_P, \mathcal{K}_V, P', V', B)$$

$V'(\mathsf{sk}_V, \mathsf{pk}_V)$

$flag = 0$

$flag$

$P'(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

if $flag = 1$ **and** pk_P is odd

$\mathcal{K}_P \rightarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

$(\mathsf{sk}_P, \mathsf{pk}_P) \leftarrow (\mathsf{sk}'_P, \mathsf{pk}'_P)$

run $P(\mathsf{sk}_P, \mathsf{pk}_P, \mathsf{pk}_V)$

run $V(\mathsf{sk}_V, \mathsf{pk}_V)$

$DB = (\mathcal{K}_P, \mathcal{K}_V, P, V, B)$

Pair(1,2)

AC Protocol using DB' with our framework

R

$flag = 0$ $flag = 1$

Out_R

T

if $\mathsf{Out}_R = 1$
  output $b' = \ell$
else
  output $b' = r$

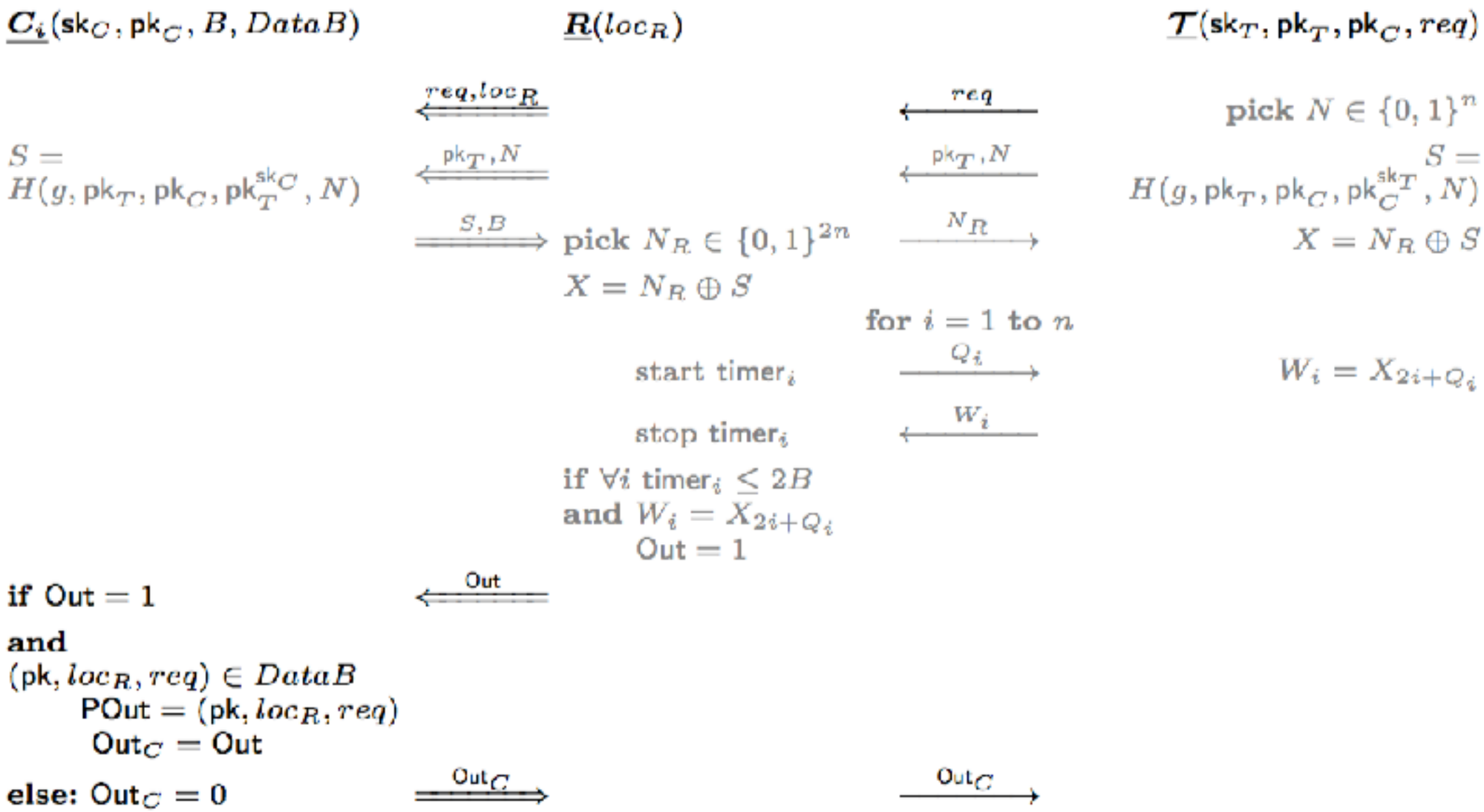
pk_1 is odd pk_2 is even

$DataB = \{(\mathsf{pk}_1, loc_R, req), (\mathsf{pk}_2, loc_R, req)\}$

*Handan Kılınç and Serge Vaudenay. Contactless Access Control based on Distance bounding. In ISC, 2017

AC WITH DB

EFF-AC (AN INSTANTIATION OF OUR FRAMEWORK)



OUTLINE

- ✓ EFFICIENT PUBLIC-KEY DB PROTOCOL
  - Introduction
  - Weak-authenticated Key Agreement
  - Eff-pkDB and its private variant
  - Comparison
- ✓ **ACCESS CONTROL WITH DB**
  - Introduction
  - Security and Privacy model for AC
  - Our Framework
  - **Conclusion**

CONCLUSION

- We define an integrated security model for AC including identification, access control, and distance bounding.
- We give a framework that clarifies how to use a secure DB to construct a secure AC in our new security model.
- We show that the same framework can be used to achieve privacy in AC with restrictions on the database of AC system.

CONCLUSION

- We define an integrated security model for AC including identification, access control, and distance bounding.
- We give a framework that clarifies how to use a secure DB to construct a secure AC in our new security model.
- We show that the same framework can be used to achieve privacy in AC with restrictions on the database of AC system.

**'Secure Contactless Payment' will appear in ACISP 2018*

EFF-PKDB WITH SIM-TF

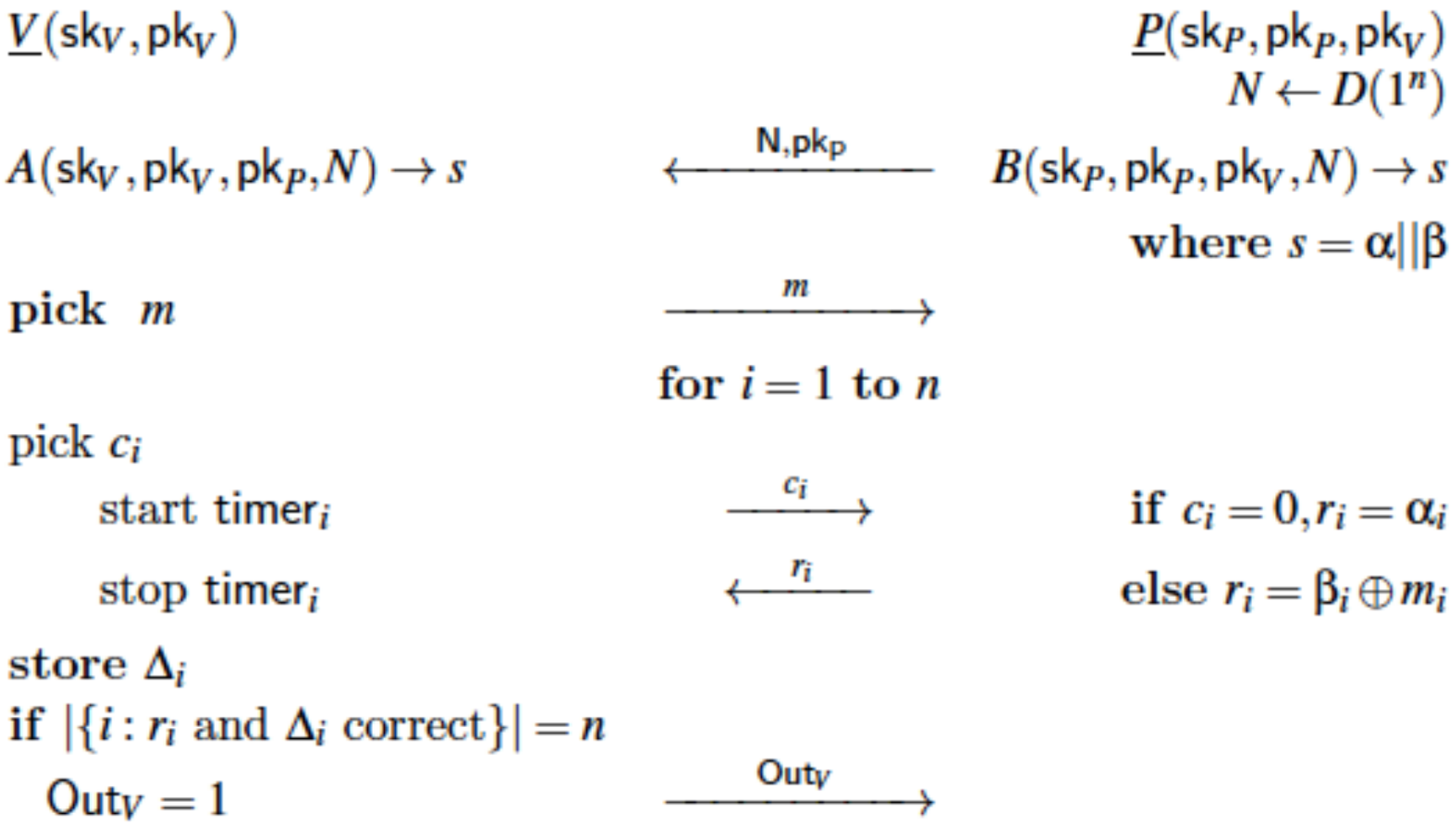


Figure 4.6 – Eff-pkDB with Sim-TF security