CASE

A New Frontier in Public-Key Authenticated Encryption

Shashank Agrawal
Coin-Base

Shweta Agrawal
IIT Madras

Manoj Prabhakaran
IIT Bombay

Rajeev Raghunath
IIT Bombay

Jayesh Singla
IIT Bombay

TCC 2023

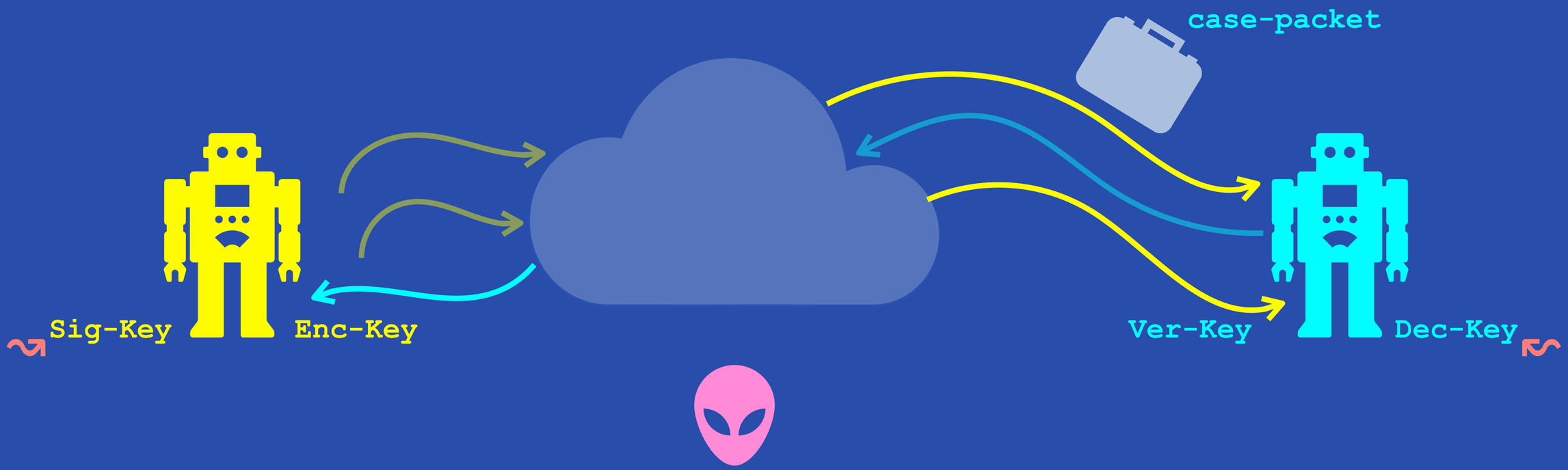
Outline

What is CASE

Active Agents Framework

A CASE construction

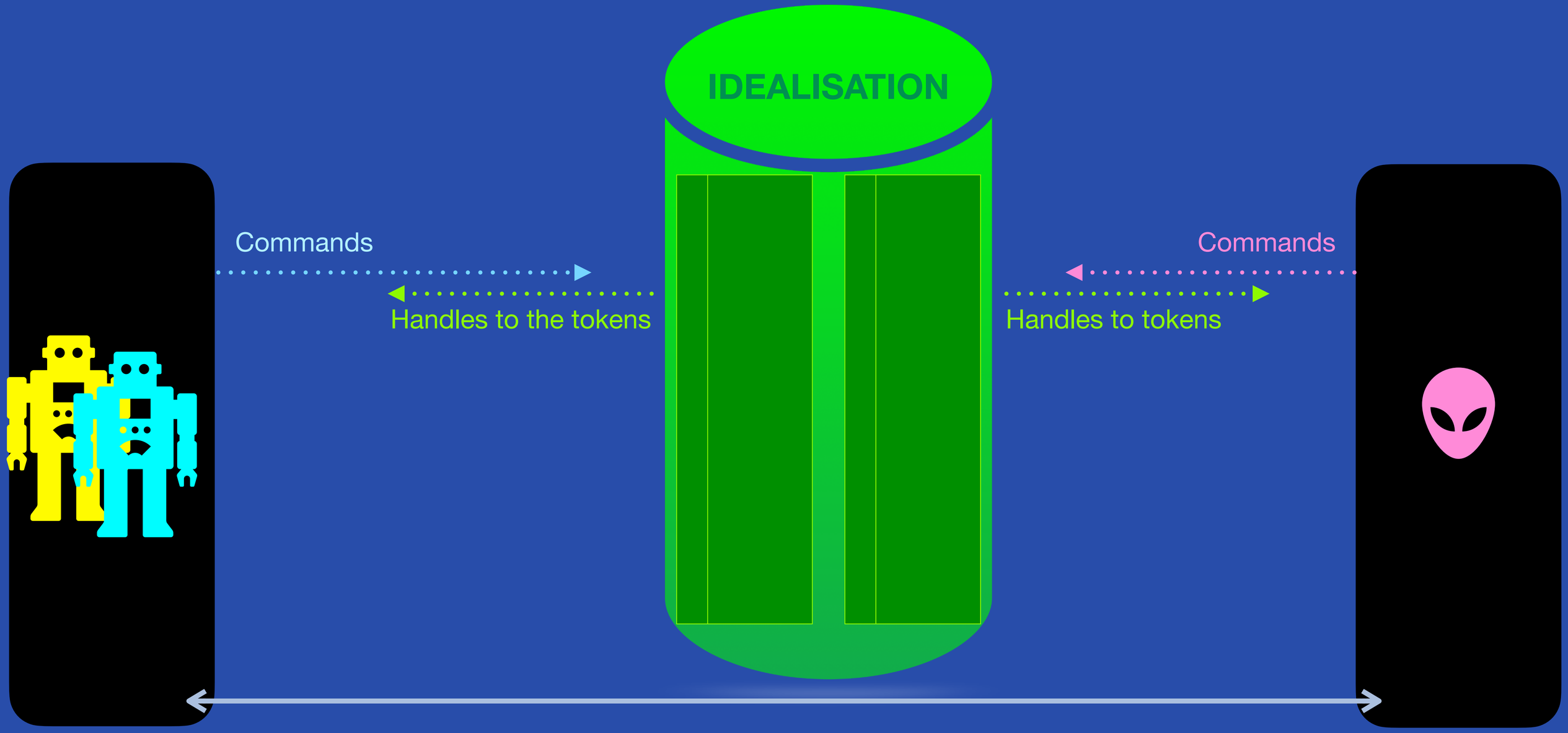
Completely Anonymous Signed Encryption



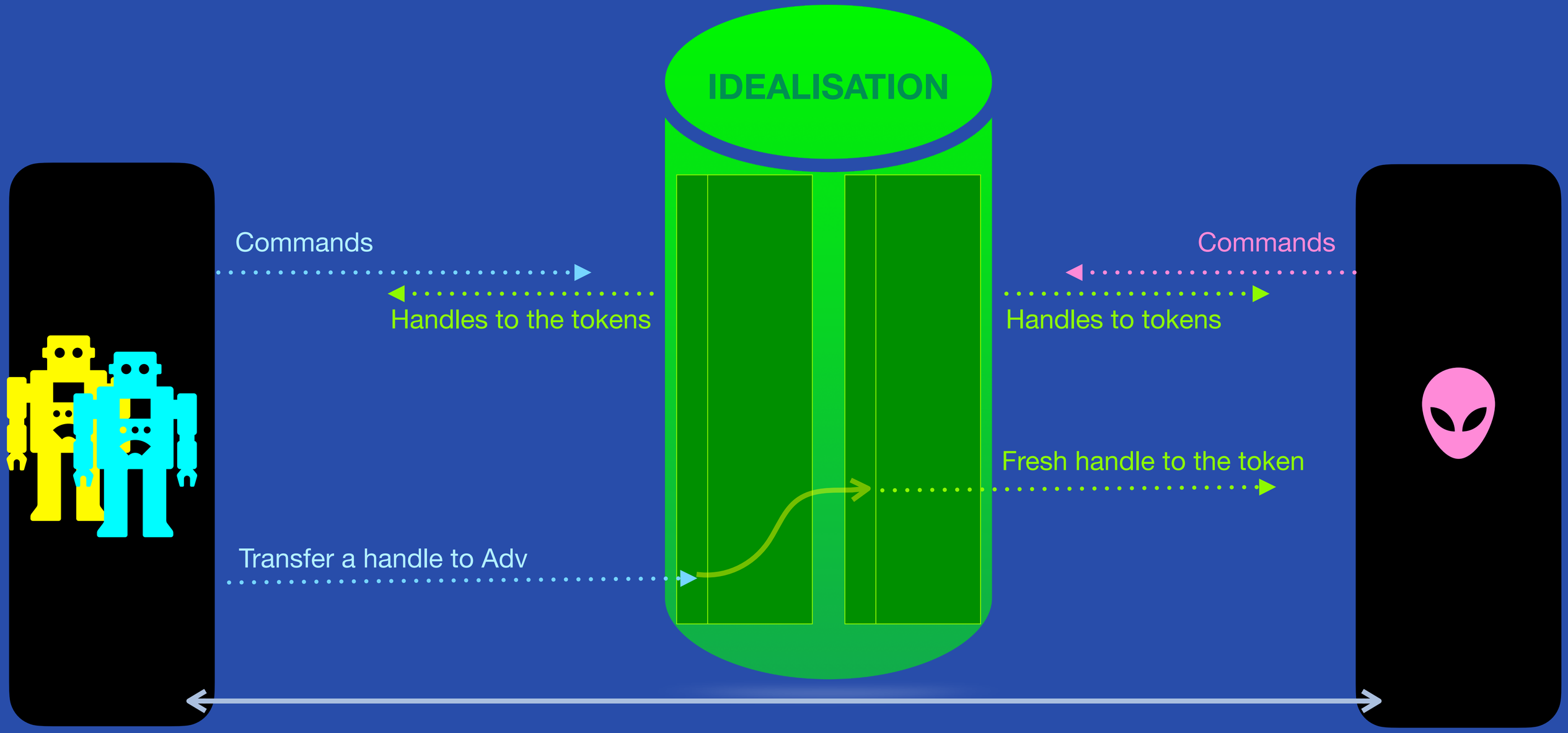
Goal: A public-key authenticated encryption scheme that is as idealised as possible!

Improve on *Signcryption* in terms of security

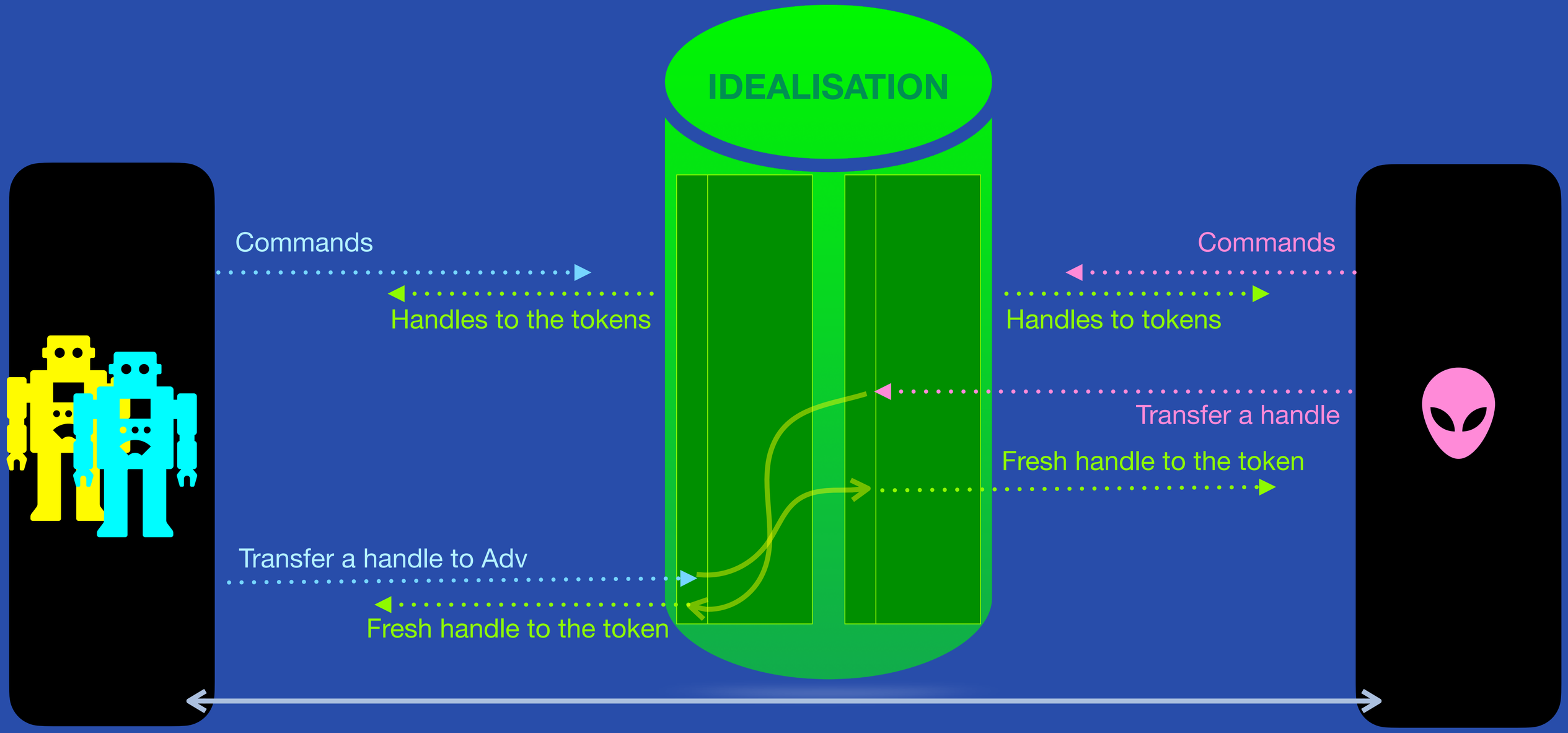
Completely Anonymous Signed Encryption



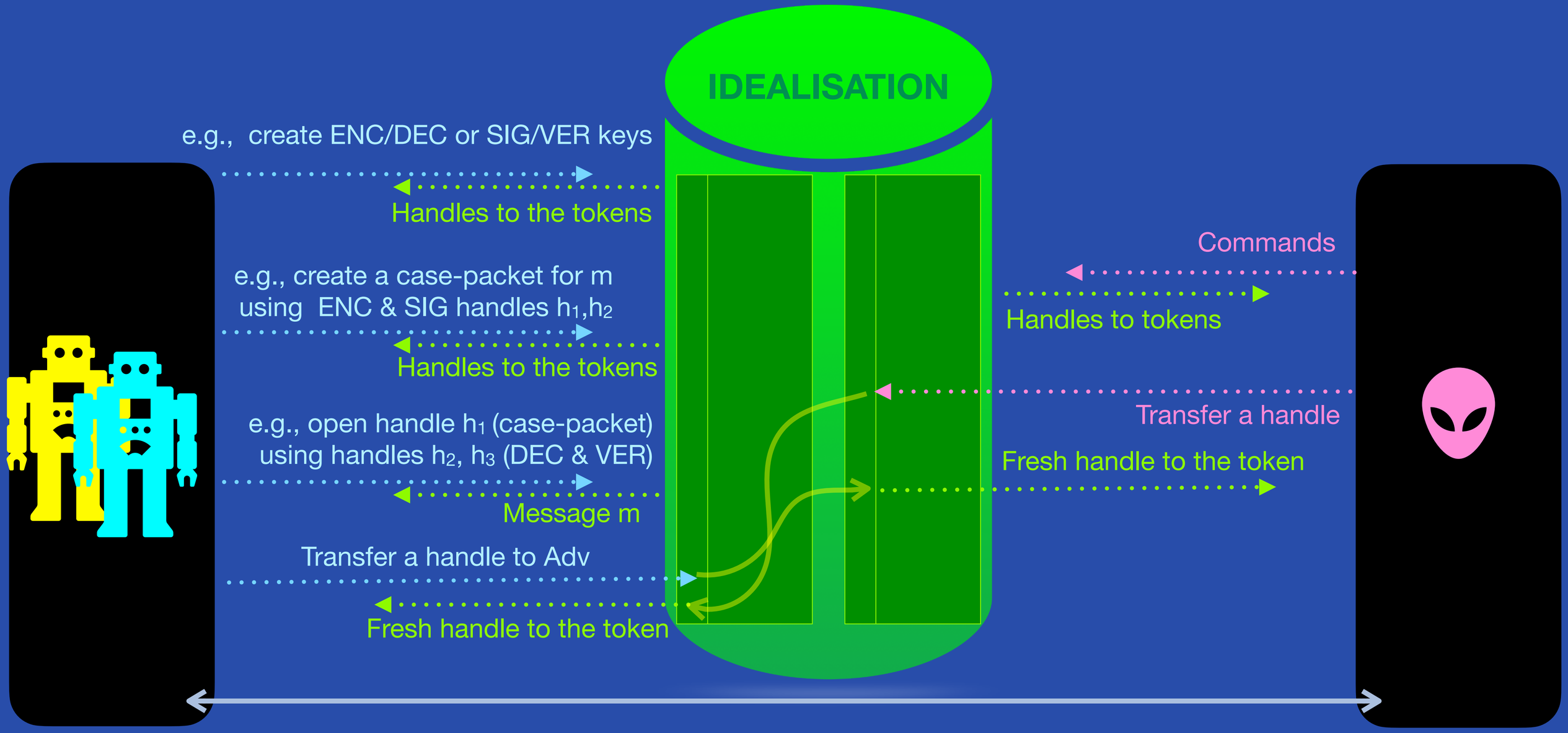
Completely Anonymous Signed Encryption



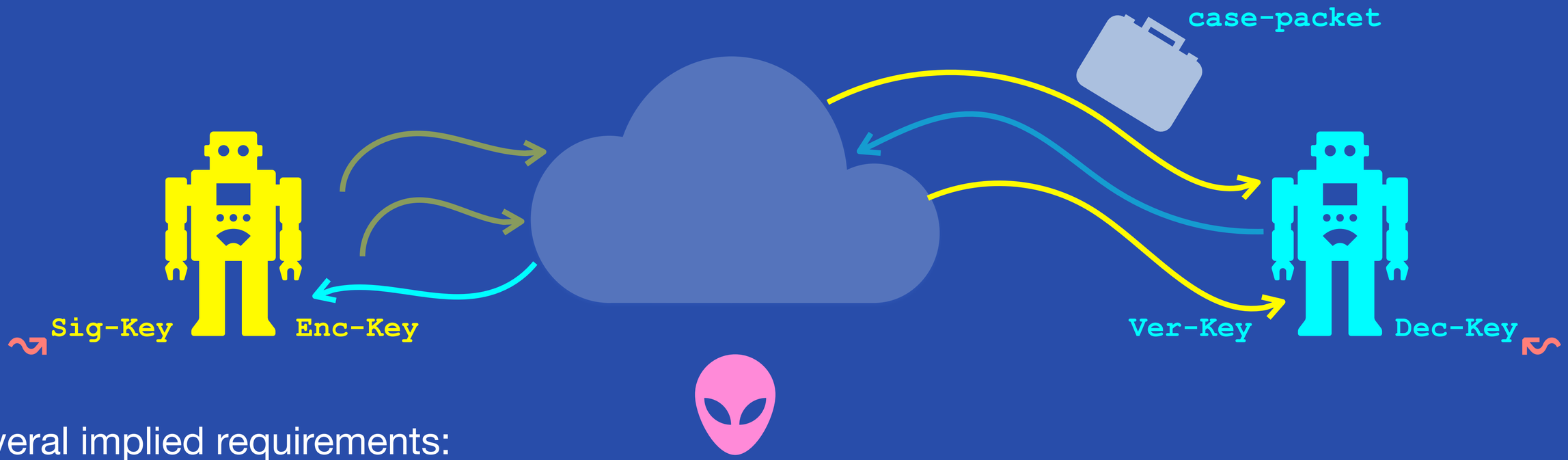
Completely Anonymous Signed Encryption



Completely Anonymous Signed Encryption



Completely Anonymous Signed Encryption



Several implied requirements:

- Cannot construct a case-packet that is decrypted by a Dec-Key unless Enc-Key given
- Without Dec-Key cannot tell who the sender or recipient is, nor what the message is
- Even with Dec-Key, without Ver-Key cannot tell if two case-packets have the same signer
- Even malicious objects (keys or case-packets) accepted from the adversary, behave ideally:
  - Two case-packets generated independently are unlikely to be equal
  - One case-packet can be decrypted/verifed by at most one dec-key/ver-key
- …

Completely Anonymous Signed Encryption

Chosen Objects Attack (COA) Security

1. **Correctness** of accepted objects
2. **Total Hiding** (a la Anonymous CCA secure encryption)
   - Can't tell between case-packets prepared using (m_0,Sig-Key_0) and (m_1,Sig-Key_1), with only blackbox access to decryption oracle (except on the challenge case-packet). Sig-Keys can be malicious (but accepted).
3. **Sender Anonymity**
   - Can't tell between case-packets prepared using (m_0,Sig-Key_0) and (m_1,Sig-Key_1), with only blackbox access to oracles for encasement with SK_0 and SK_1 and verification with VK_0 and VK_1 (except on the challenge case-packet). Enc-Key can be malicious.
4. **Strong Unforgeability**: Without Sig-Key, can't produce a new case-packet that verifies
5. **Unpredictability**: Case-packets have high min-entropy, even if Enc-Key/Sig-Key malicious.
6. **Existential Consistency**: Uniqueness of secret-keys/message behind public-keys/case-packet

Outline

Is COA security comprehensive?

What is CASE

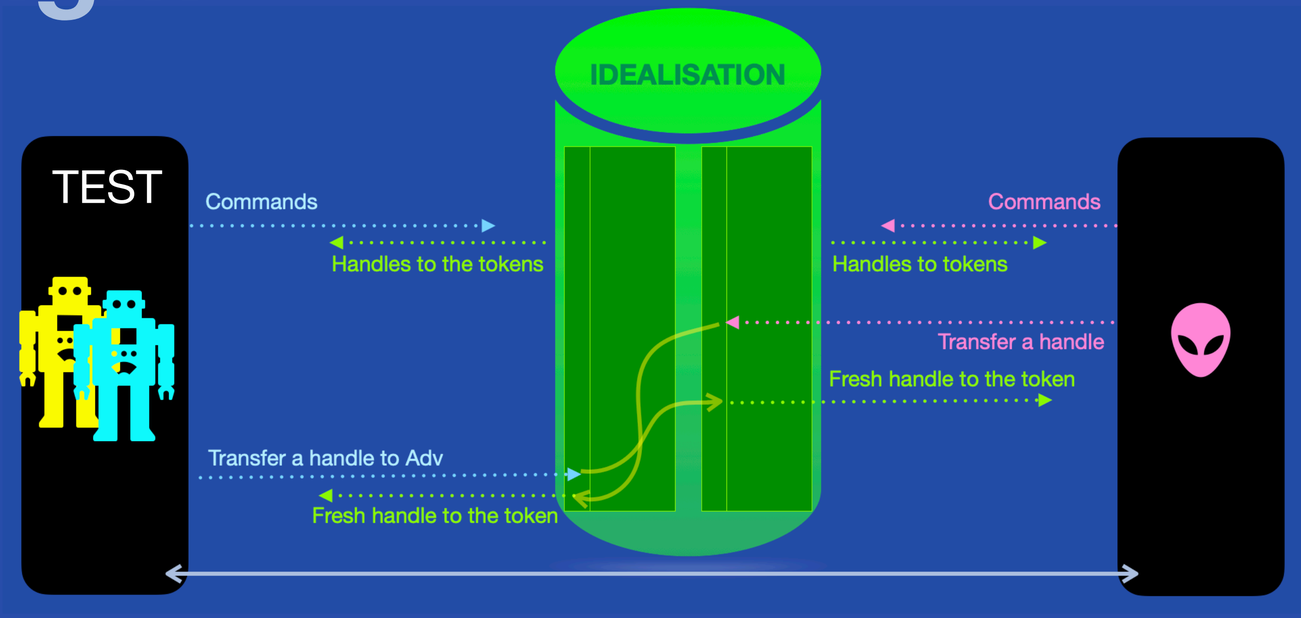
COA Security

Active Agents Framework

A CASE construction

A REAL/IDEAL Paradigm

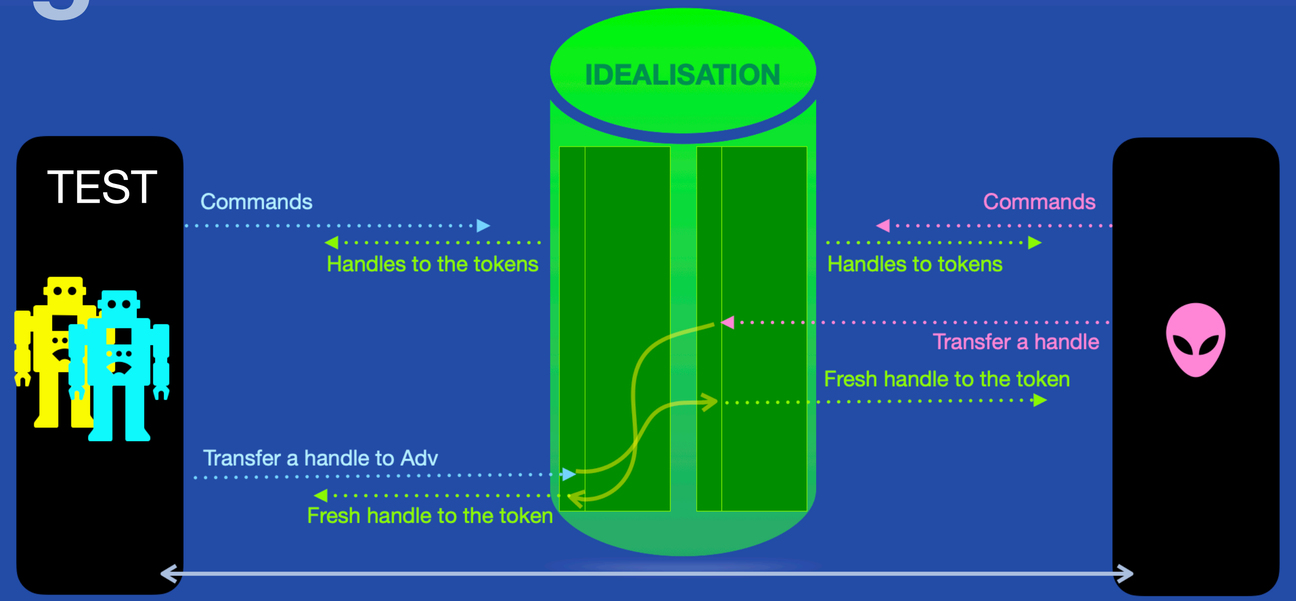
- Ideal CASE is easy to define



A REAL/IDEAL Paradigm

- Ideal CASE is easy to define

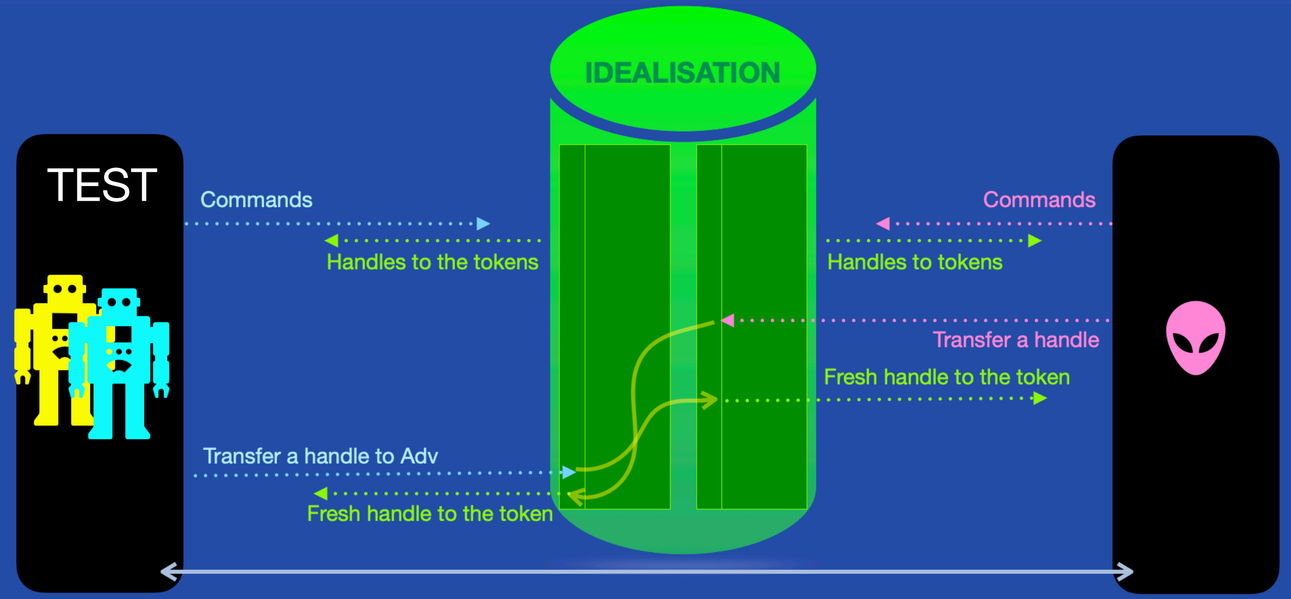
What does it mean to be *like Ideal?*



- Simulation-based definitions turn out to be impossible!

Active Agents Framework

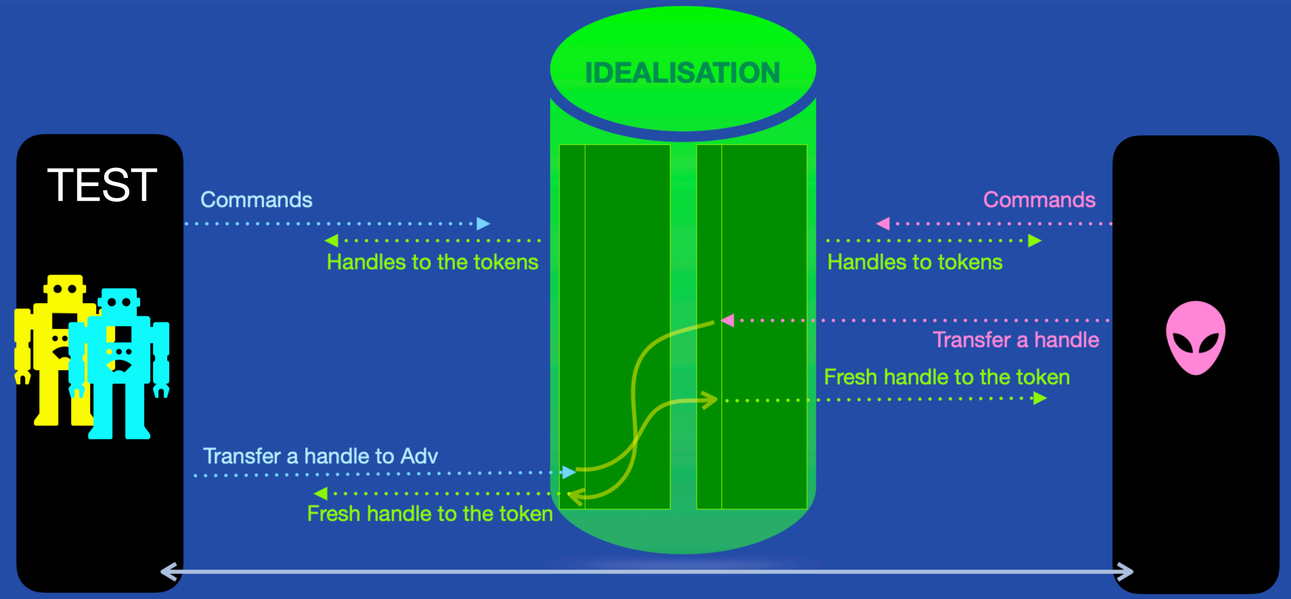
What does it mean to be *like Ideal?*



Indistinguishability Preserving (IND-PRE) security: If Test(0) vs. Test(1) is indistinguishable in the ideal execution, it should remain so in the real execution

Active Agents Framework

What does it mean to be *like Ideal?*

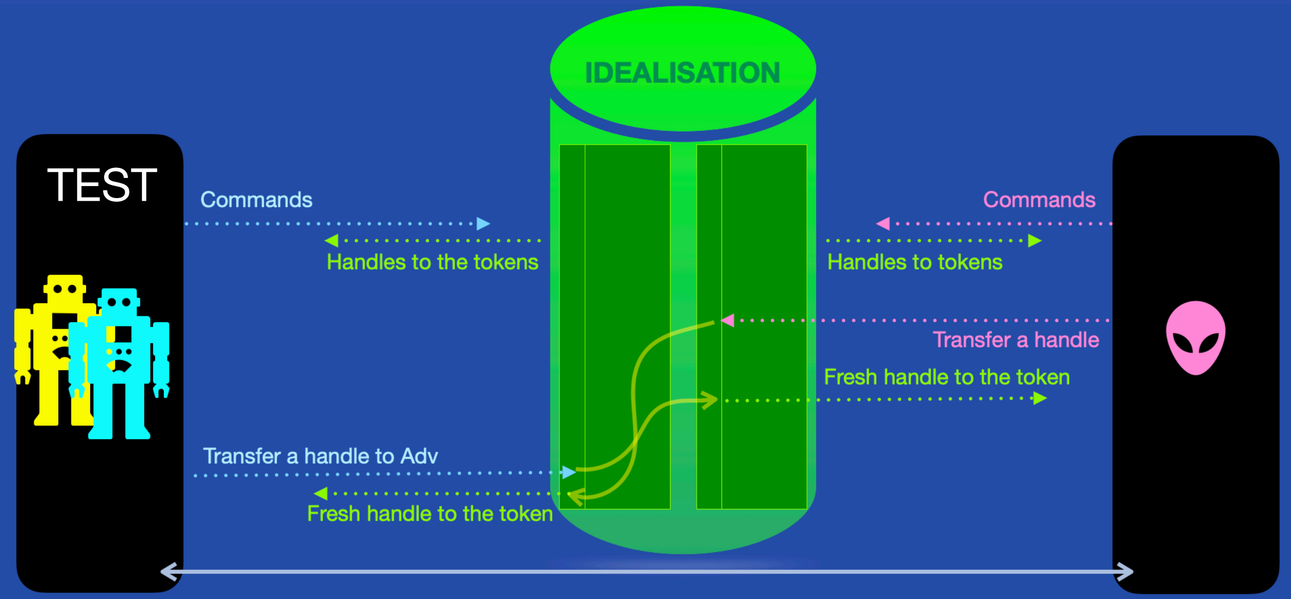


Indistinguishability Preserving (IND-PRE) security: If Test(0) vs. Test(1) is indistinguishable in the ideal execution, it should remain so in the real execution

- From the Cryptographic Agents Framework [AAP15, APY16]
- *New* in Active Agents: allow adversary to transfer handles to Test

Active Agents Framework

What does it mean to be *like Ideal?*



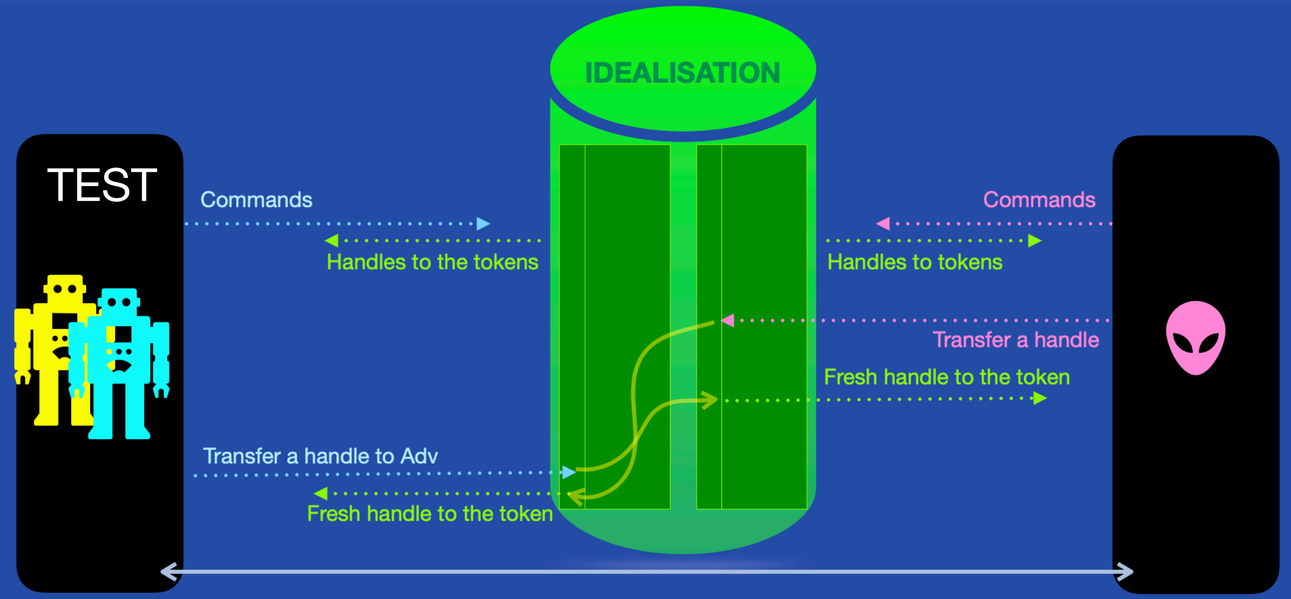
Indistinguishability Preserving (IND-PRE) security: If Test(0) vs. Test(1) is indistinguishable in the ideal execution, it should remain so in the real execution

- Still impossible! Relax a little:
  - Limit to **Δ-Tests** which use the Test-bit only to decide what is transferred, and otherwise have no secrets
  - In the IDEAL, restrict to **statistical** indistinguishability

Active Agents Framework

What does it mean to be *like Ideal?*

Δ-s-IND-PRE



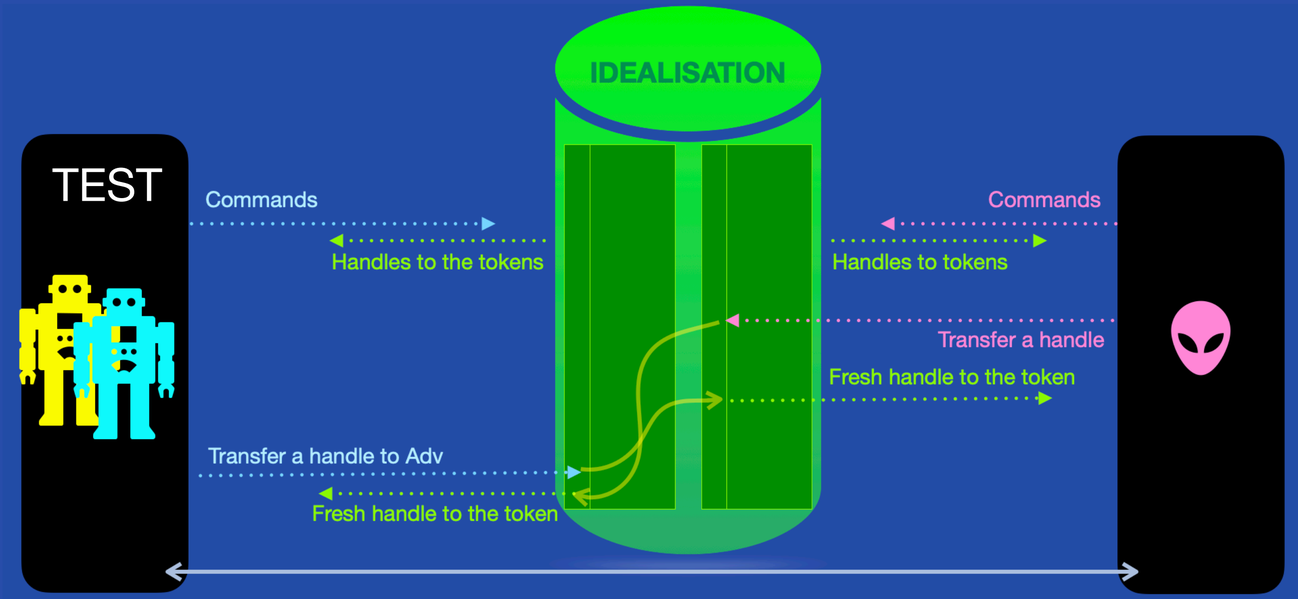
Indistinguishability Preserving (IND-PRE) security: If Test(0) vs. Test(1) is indistinguishable in the ideal execution, it should remain so in the real execution

- Still impossible! Relax a little:
  - Limit to **Δ-Tests** which use the Test-bit only to decide what is transferred, and otherwise have no secrets
  - In the IDEAL, restrict to **statistical** indistinguishability

Active Agents Framework

What does it mean to be *like Ideal?*

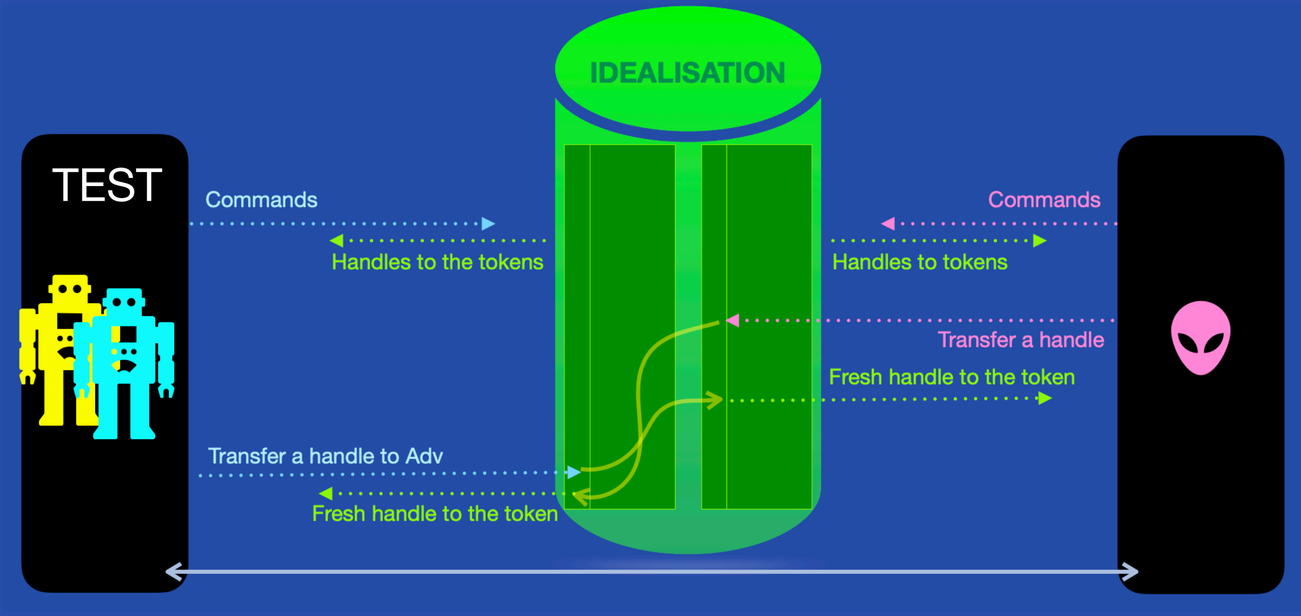
Δ-s-IND-PRE



- Covers all reasonable (i.e., ideally hiding) indistinguishability experiments at once
  - e.g., for PKE, subsumes CCA, Anon-CCA, etc.
- Not over-fitting to a particular primitive like encryption or signature

CASE in the Active Agents Framework

1. **Correctness**
2. **Total Hiding**
3. **Sender Anonymity**
4. **Strong Unforgeability**
5. **Unpredictability**
6. **Existential Consistency**



Main Theorem

COA-secure CASE ⇒ Δ-s-IND-PRE secure CASE

Outline

Is COA security comprehensive?

Is it achievable?

What is CASE

COA Security

Active Agents Framework

Δ-s-IND-PRE Security

A CASE construction

Constructing a CASE Scheme

Quasi-Deterministic
Anon-CCA
PKE

Constructing a CASE Scheme

Quasi-Deterministic
Anon-CCA
PKE

Cramer-Shoup
Encryption
(Based on DDH)

QD property:
$\mathsf{Enc}_{PK}(m; r) = (\tau, c)$
where $\tau = \mathsf{Encode}_{PK}(r)$
fixes r

Constructing a CASE Scheme

Quasi-Deterministic Anon-CCA PKE

COA-secure Quasi-Deterministic PKE

Cramer-Shoup Encryption (Based on DDH)

QD property:

$\mathsf{Enc}_{PK}(m; r) = (\tau, c)$

where $\tau = \mathsf{Encode}_{PK}(r)$

fixes r

Constructing a CASE Scheme

Quasi-Deterministic Anon-CCA PKE

COA-secure Quasi-Deterministic PKE

Existentially Consistent Anonymous Signatures

Cramer-Shoup Encryption (Based on DDH)

QD property:

$\mathsf{Enc}_{PK}(m; r) = (\tau, c)$

where $\tau = \mathsf{Encode}_{PK}(r)$

fixes r

Constructing a CASE Scheme

Cramer-Shoup
Encryption
(Based on DDH)

QD property:

$\mathsf{Enc}_{PK}(m; r) = (\tau, c)$

where $\tau = \mathsf{Encode}_{PK}(r)$

fixes r

Constructing a CASE Scheme

Quasi-Deterministic Anon-CCA PKE

COA-secure Quasi-Deterministic PKE

Existentially Consistent Anonymous Signatures

COA-secure CASE

Cramer-Shoup Encryption (Based on DDH)

QD property:

$\mathsf{Enc}_{PK}(m; r) = (\tau, c)$

where $\tau = \mathsf{Encode}_{PK}(r)$

fixes r

<u>By adding Existential Consistency</u>

Enc-Key has a *fully binding* commitment to Dec-Key

Ciphertext has a *fully binding* commitment to Enc-Key which can be opened on decrypting

Constructing a CASE Scheme

Quasi-Deterministic Anon-CCA PKE

Cramer-Shoup Encryption (Based on DDH)

QD property:
$\mathsf{Enc}_{PK}(m; r) = (\tau, c)$
where $\tau = \mathsf{Encode}_{PK}(r)$
fixes r

COA-secure Quasi-Deterministic PKE

By adding Existential Consistency

Enc-Key has a *fully binding* commitment to Dec-Key

Ciphertext has a *fully binding* commitment to Enc-Key which can be opened on decrypting

Existentially Consistent Anonymous Signatures

By adding an encryption layer and Existential Consistency

Use a COA-secure QD-PKE whose Dec-Key in Ver-Key

Sign m and encoding of randomness in the PKE

Encrypt the signature. Include a commitment to Ver-Key which can be opened on decrypting.

COA-secure CASE

Constructing a CASE Scheme

Quasi-Deterministic Anon-CCA PKE

COA-secure Quasi-Deterministic PKE

Existentially Consistent Anonymous Signatures

COA-secure CASE

Cramer-Shoup Encryption (Based on DDH)

QD property:

$\mathrm{Enc}_{PK}(m; r) = (\tau, c)$

where $\tau = \mathrm{Encode}_{PK}(r)$ fixes r

<u>By adding Existential Consistency</u>

Enc-Key has a *fully binding* commitment to Dec-Key

Ciphertext has a *fully binding* commitment to Enc-Key which can be opened on decrypting

<u>By adding an encryption layer and Existential Consistency</u>

Use a COA-secure QD-PKE whose Dec-Key in Ver-Key

Sign m and encoding of randomness in the PKE

Encrypt the signature. Include a commitment to Ver-Key which can be opened on decrypting.

<u>Start Encrypting-Sign-Finish Encrypting</u>

Sign using ECAS, encrypt using COA QD-PKE

Sign m and encoding of randomness in the COA QD-PKE

Then finish encrypting m and signature

Constructing a CASE Scheme

Quasi-Deterministic Anon-CCA PKE

Cramer-Shoup Encryption (Based on DDH)

QD property:
$\mathrm{Enc}_{PK}(m; r) = (\tau, c)$
where $\tau = \mathrm{Encode}_{PK}(r)$
fixes r

COA-secure Quasi-Deterministic PKE

By adding Existential Consistency

Enc-Key has a *fully binding* commitment to Dec-Key

Ciphertext has a *fully binding* commitment to Enc-Key which can be opened on decrypting

Existentially Consistent Anonymous Signatures

By adding an encryption layer and Existential Consistency

Use a COA-secure QD-PKE whose Dec-Key in Ver-Key

Sign m and encoding of randomness in the PKE

Encrypt the signature. Include a commitment to Ver-Key which can be opened on decrypting.

COA-secure CASE

Start Encrypting-Sign-Finish Encrypting

Sign using ECAS, encrypt using COA QD-PKE

Sign m and encoding of randomness in the COA QD-PKE

Then finish encrypting m and signature

Hybrid

Use SKE & Hash

Encase keys and hash of SKE cipher-text

Outline

Is COA security comprehensive?

Is it achievable?

What is CASE

COA Security

Active Agents Framework

Δ-s-IND-PRE Security

A CASE construction

Quite practical!

Thank You!