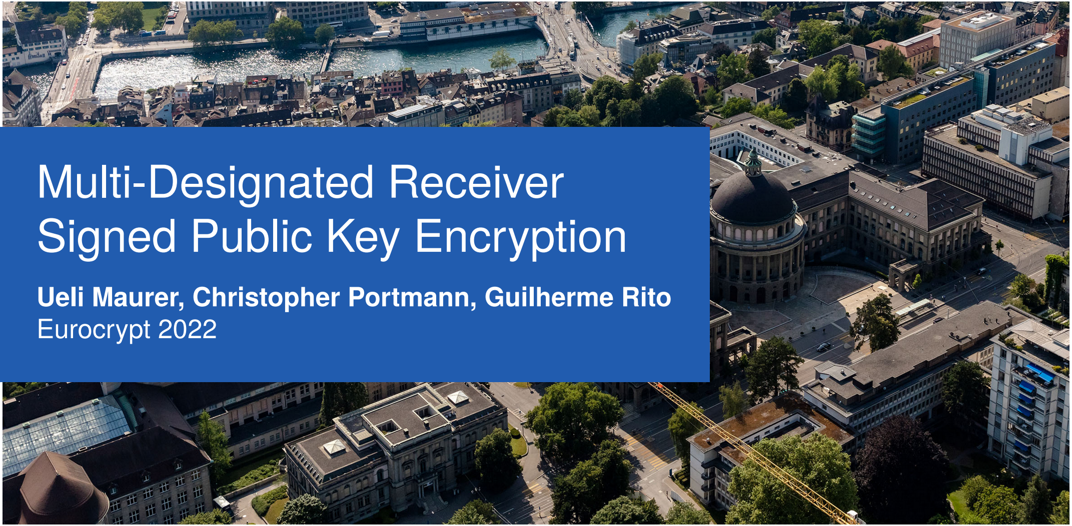
ETH zürich



Multi-Designated Receiver Signed Public Key Encryption

Ueli Maurer, Christopher Portmann, Guilherme Rito

Eurocrypt 2022

Outline

1. Contributions
2. Public Key Encryption for Broadcast (PKEBC)
3. PKEBC Scheme Construction
4. Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE)
5. MDRS-PKE Scheme Construction

1. Contributions

1. Contributions

New types of Public Key Encryption (PKE) schemes:

- Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE);
- Public Key Encryption for Broadcast (PKEBC);

1. Contributions

New types of Public Key Encryption (PKE) schemes:

- Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE);
- Public Key Encryption for Broadcast (PKEBC);

Constructions of both schemes from **standard assumptions**;

1. Contributions

New types of Public Key Encryption (PKE) schemes:

- Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE);
- Public Key Encryption for Broadcast (PKEBC);

Constructions of both schemes from **standard assumptions**;

MDRS-PKE scheme yields Multi-Designated Verifier Signature scheme (MDVS) with Privacy of Identities;

The only prior construction is based on **Verifiable Functional Encryption** [1].

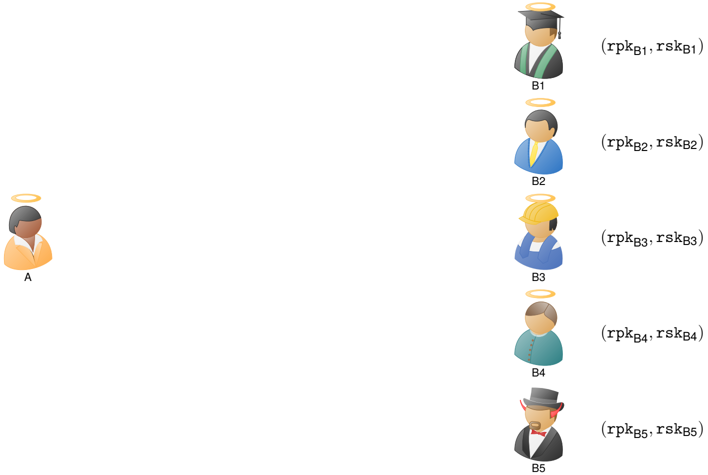
[1] Damgård et al. (TCC '20).

Outline

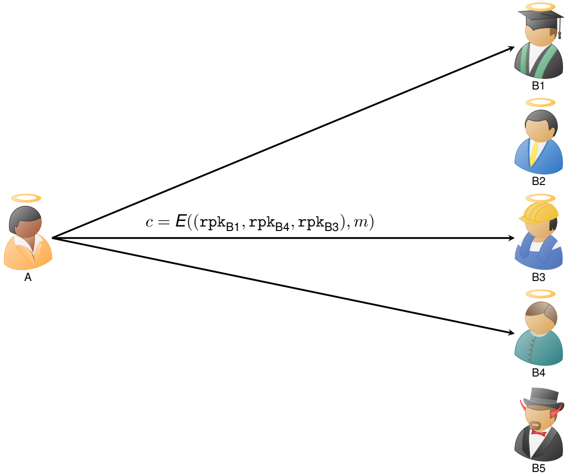
1. Contributions
2. Public Key Encryption for Broadcast (PKEBC)
3. PKEBC Scheme Construction
4. Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE)
5. MDRS-PKE Scheme Construction

2. PKEBC — Syntax

2. PKEBC — Syntax


B1
$(\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rsk}_{\mathsf{B1}})$
B2
$(\mathtt{rpk}_{\mathsf{B2}}, \mathtt{rsk}_{\mathsf{B2}})$
A
B3
$(\mathtt{rpk}_{\mathsf{B3}}, \mathtt{rsk}_{\mathsf{B3}})$
B4
$(\mathtt{rpk}_{\mathsf{B4}}, \mathtt{rsk}_{\mathsf{B4}})$
B5
$(\mathtt{rpk}_{\mathsf{B5}}, \mathtt{rsk}_{\mathsf{B5}})$

2. PKEBC — Syntax



$(\mathtt{rpk}_{B1}, \mathtt{rsk}_{B1})$

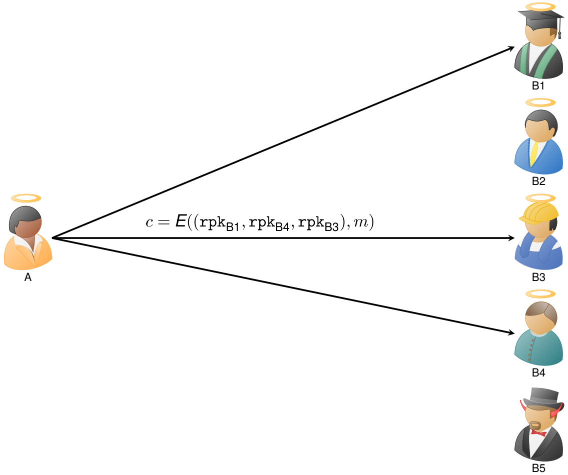
$(\mathtt{rpk}_{B2}, \mathtt{rsk}_{B2})$

$(\mathtt{rpk}_{B3}, \mathtt{rsk}_{B3})$

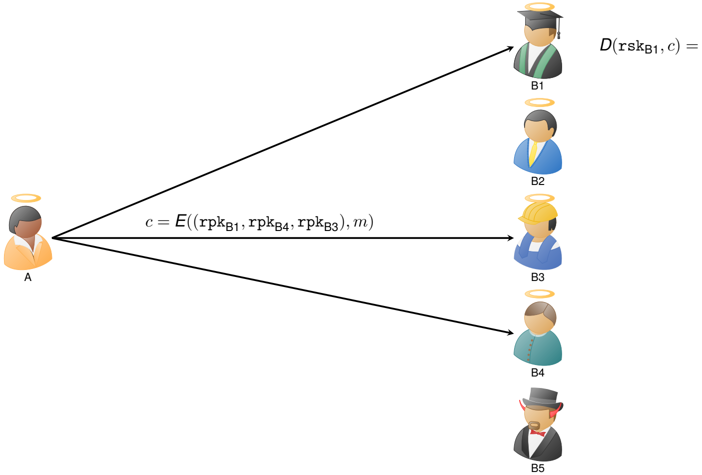
$(\mathtt{rpk}_{B4}, \mathtt{rsk}_{B4})$

$(\mathtt{rpk}_{B5}, \mathtt{rsk}_{B5})$

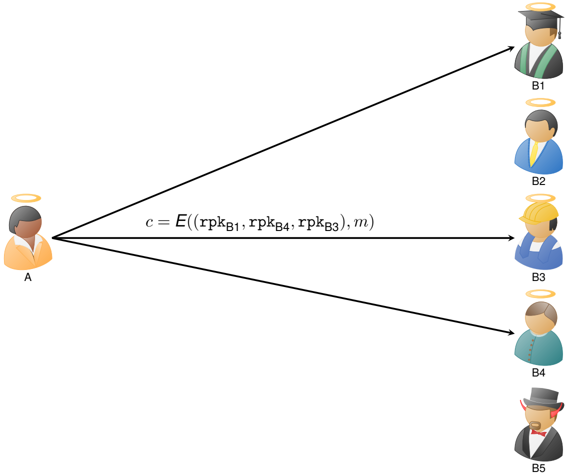
2. PKEBC — Syntax



2. PKEBC — Syntax

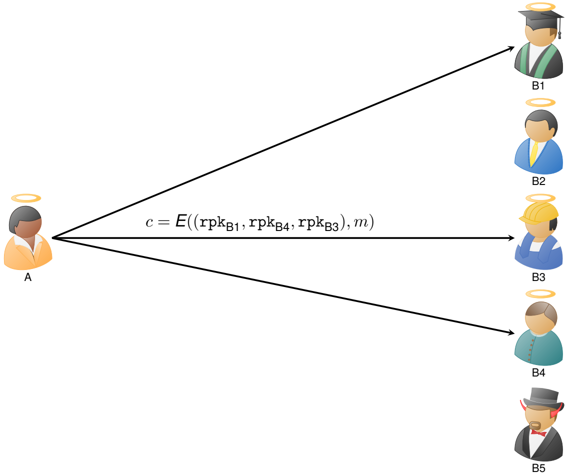


2. PKEBC — Syntax



$D(\mathtt{rsk}_{B1}, c) = ((\mathtt{rpk}_{B1}, \mathtt{rpk}_{B4}, \mathtt{rpk}_{B3}), m)$

2. PKEBC — Syntax



$D(\mathtt{rsk}_{\mathsf{B1}}, c) = ((\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B4}}, \mathtt{rpk}_{\mathsf{B3}}), m)$

Syntax of decryption:

- Only $\mathtt{rsk}_{\mathsf{B1}}$ is needed;
- Outputs vector of receivers' $\mathtt{rpk}$.

2. PKEBC — Security Notions

Consistency

Robustness

Confidentiality (IND-CCA-2 security)

2. PKEBC — Security Notions

Consistency

Robustness

Confidentiality (IND-CCA-2 security)

+ Anonymity (IK-CCA-2 security)

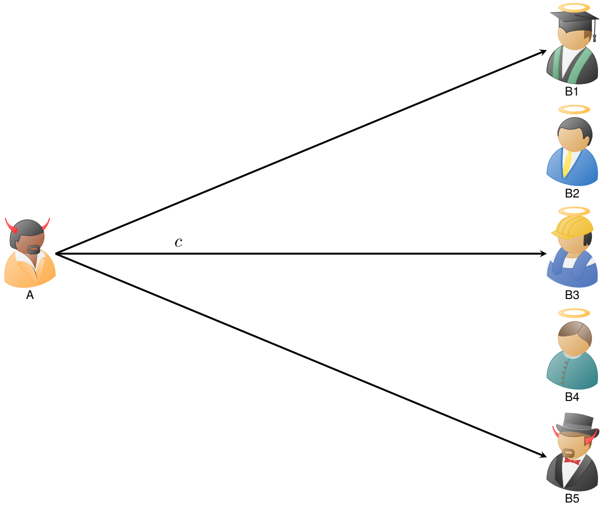
2. PKEBC — Consistency

A

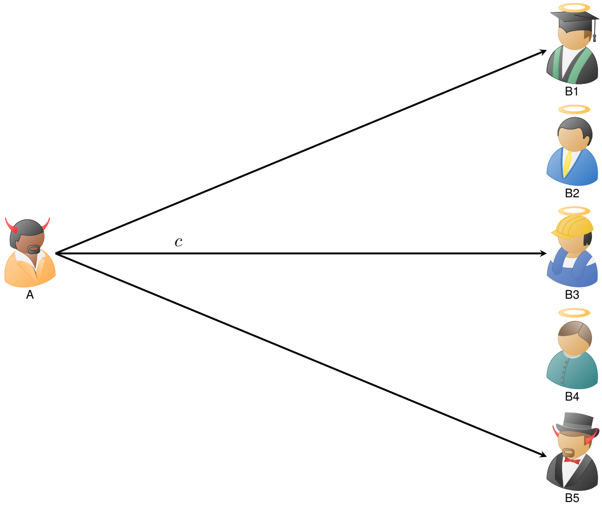
2. PKEBC — Consistency

2. PKEBC — Consistency

2. PKEBC — Consistency

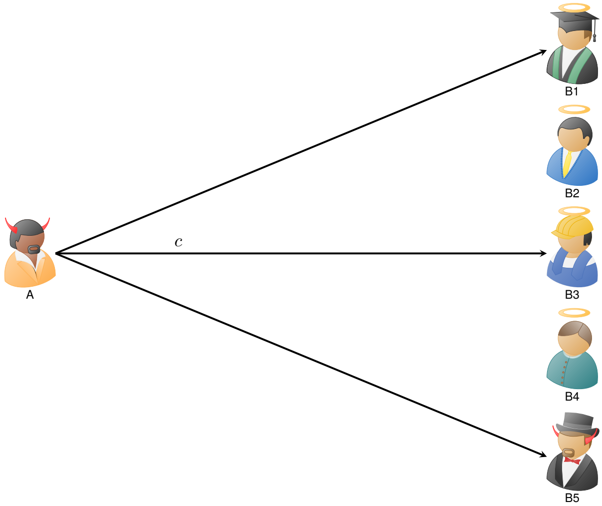


2. PKEBC — Consistency



$D(\mathtt{rsk}_{\mathsf{B1}}, c) = ((\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B3}}, \mathtt{rpk}_{\mathsf{B5}}), m)$

2. PKEBC — Consistency



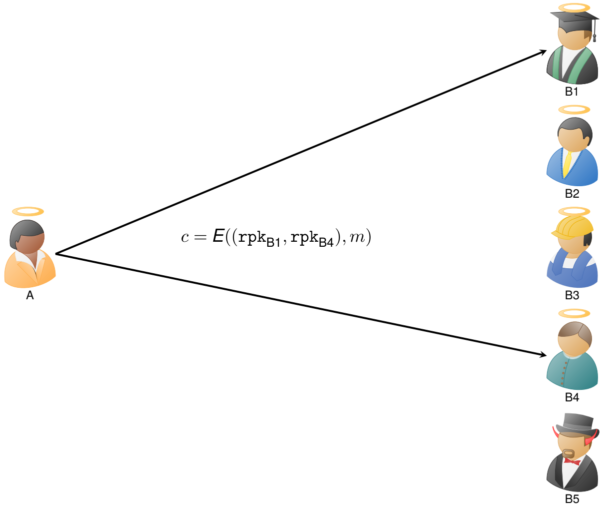
$D(\mathtt{rsk}_{\mathsf{B1}}, c) = ((\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B3}}, \mathtt{rpk}_{\mathsf{B5}}), m)$

$D(\mathtt{rsk}_{\mathsf{B3}}, c) = ((\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B3}}, \mathtt{rpk}_{\mathsf{B5}}), m)$

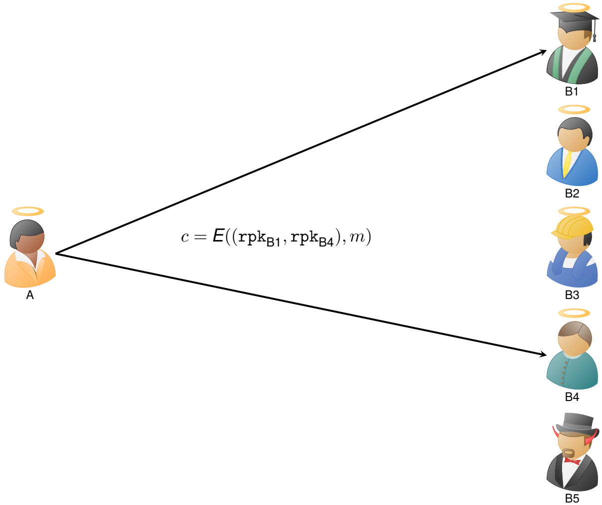
2. PKEBC — Robustness

2. PKEBC — Robustness

2. PKEBC — Robustness

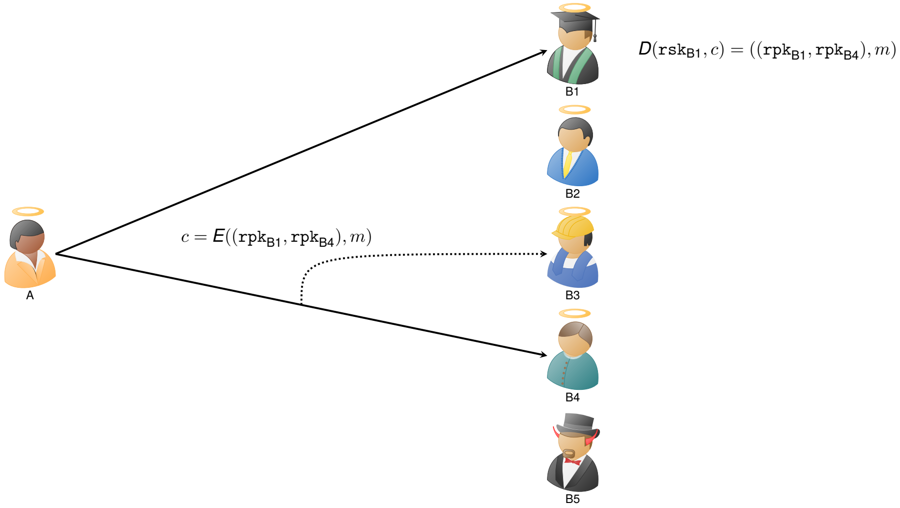


2. PKEBC — Robustness

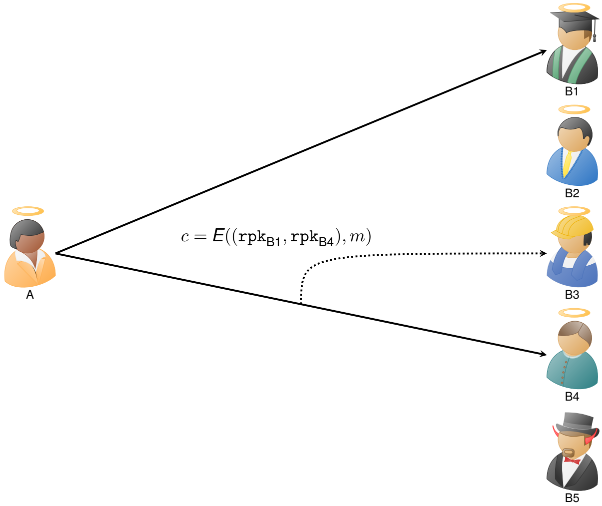


$D(\texttt{rsk}_{\mathsf{B1}}, c) = ((\texttt{rpk}_{\mathsf{B1}}, \texttt{rpk}_{\mathsf{B4}}), m)$

2. PKEBC — Robustness



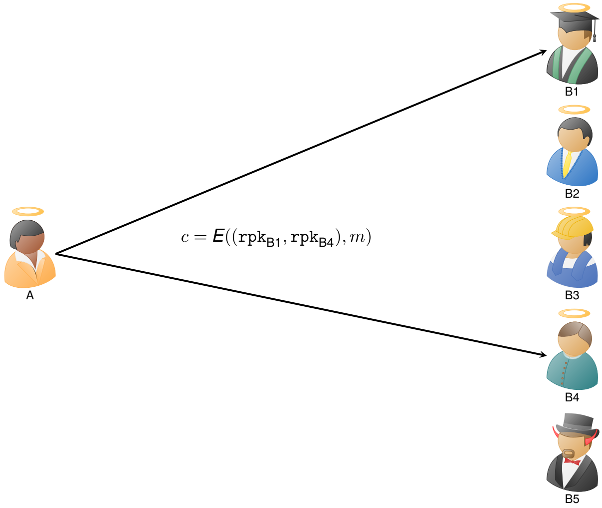
2. PKEBC — Robustness



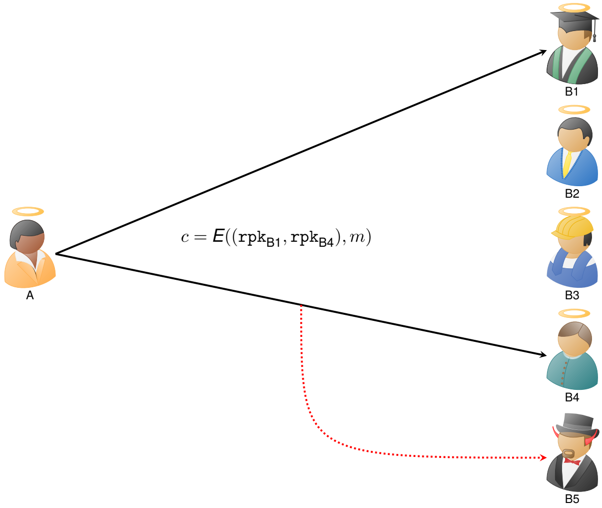
$D(\mathtt{rsk}_{B1}, c) = ((\mathtt{rpk}_{B1}, \mathtt{rpk}_{B4}), m)$

$D(\mathtt{rsk}_{B3}, c) = \perp$

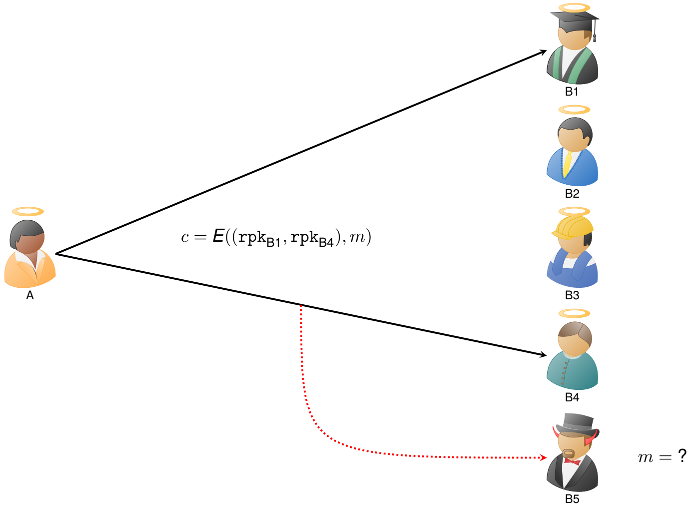
2. PKEBC — Confidentiality (IND-CCA-2 Security)



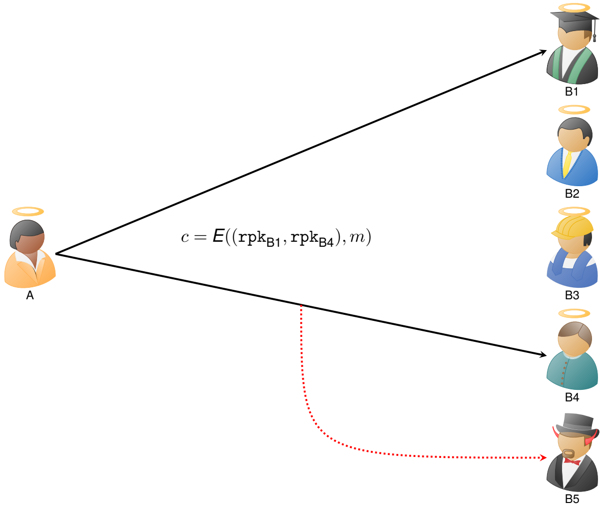
2. PKEBC — Confidentiality (IND-CCA-2 Security)



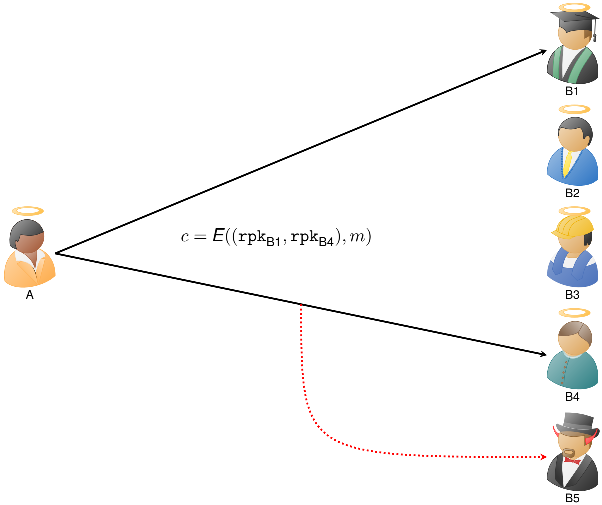
2. PKEBC — Confidentiality (IND-CCA-2 Security)



2. PKEBC — Anonymity (IK-CCA-2 Security)

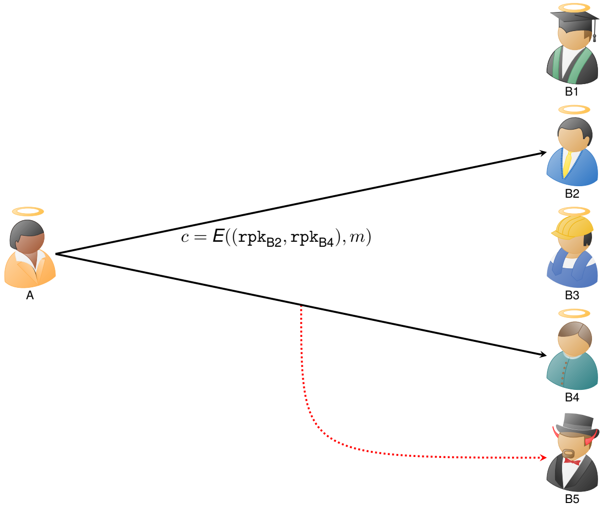


2. PKEBC — Anonymity (IK-CCA-2 Security)



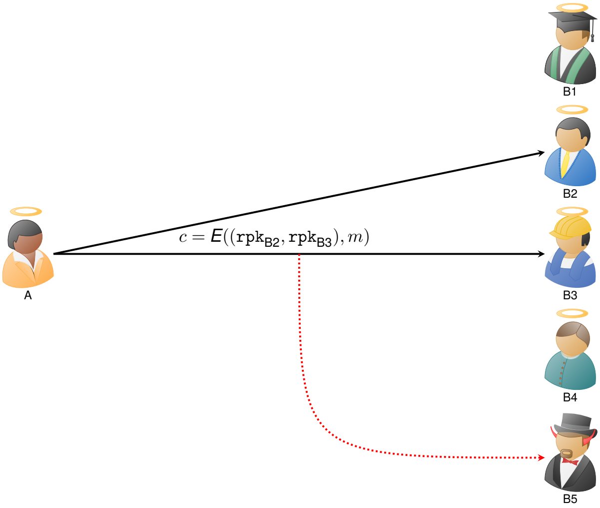
Are the (two) receivers of c $(B1, B4)$?

2. PKEBC — Anonymity (IK-CCA-2 Security)



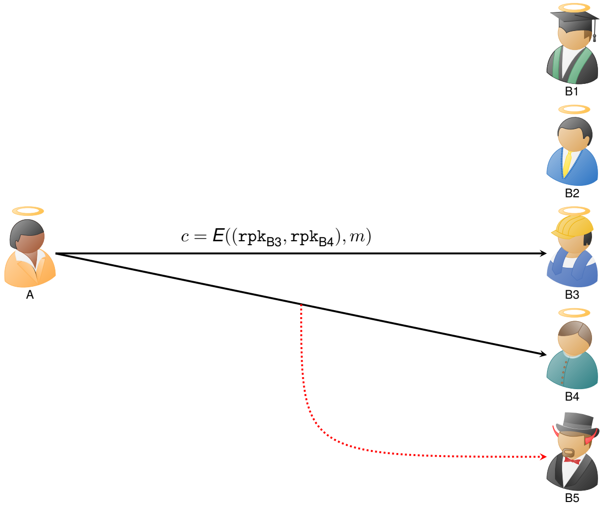
Are the (two) receivers of c $(B2, B4)$?

2. PKEBC — Anonymity (IK-CCA-2 Security)



Are the (two) receivers of c $(B2, B3)$?

2. PKEBC — Anonymity (IK-CCA-2 Security)



Are the (two) receivers of c $(B3, B4)$?

Outline

1. Contributions
2. Public Key Encryption for Broadcast (PKEBC)
3. PKEBC Scheme Construction
4. Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE)
5. MDRS-PKE Scheme Construction

3. PKEBC Scheme Construction Roadmap

Recall Naor-Yung's IND-CCA-1 PKE scheme construction [2];

Generalization to (non IK-CCA-2 secure) PKEBC scheme;

Making the PKEBC scheme IK-CCA-2 secure.

[2] Naor and Yung (STOC '90).

3. Naor-Yung's PKE Scheme

Building blocks:

- (IND-CPA secure) PKE scheme CPA $= (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$;
- NIZK $= (\mathit{Gen}_{\mathit{CRS}}, \mathit{Prv}, \mathit{Vfy})$;

3. Naor-Yung's PKE Scheme

Building blocks:

- (IND-CPA secure) PKE scheme CPA $= (\textit{Gen}, \textit{Enc}, \textit{Dec})$;
- NIZK $= (\textit{Gen}_{\textit{CRS}}, \textit{Prv}, \textit{Vfy})$;

Construction of IND-CCA-1 secure PKE scheme $\Pi = (\textit{Gen}, \textit{Enc}, \textit{Dec})$:

$\Pi.\textit{Gen}$:

$$\Big((\mathtt{pk}_0, \mathtt{sk}_0), (\mathtt{pk}_1, \mathtt{sk}_1)\Big) \leftarrow (\text{CPA}.\textit{Gen}, \text{CPA}.\textit{Gen});$$

$$\mathtt{crs} \leftarrow \text{NIZK}.\textit{Gen}_{\textit{CRS}};$$

$$\text{Output } \Big(\mathtt{pk} := (\mathtt{crs}, \mathtt{pk}_0, \mathtt{pk}_1), \mathtt{sk} := (\mathtt{sk}_0, \mathtt{pk})\Big).$$

3. Naor-Yung's PKE Scheme

$\Pi.\textit{Enc}(\texttt{pk} := (\texttt{crs}, \texttt{pk}_0, \texttt{pk}_1), m)$:

$(c_0, c_1) \leftarrow (\text{CPA}.\textit{Enc}_{\texttt{pk}_0}(m), \text{CPA}.\textit{Enc}_{\texttt{pk}_1}(m))$;

$p \leftarrow$ NIZK.*Prv*$\big($$\texttt{crs}$,

$\texttt{stmt} :=$ "There is a message m such that c_0 and c_1 are encryptions of m under $\texttt{pk}_0$ and $\texttt{pk}_1$, resp.",

$\texttt{w} := (m,$ Encryption Randomness$)\big)$;

Output (p, c_0, c_1).

3. Naor-Yung's PKE Scheme

$\Pi.$*Enc*$(\mathtt{pk} \coloneqq (\mathtt{crs}, \mathtt{pk}_0, \mathtt{pk}_1), m)$:

$(c_0, c_1) \leftarrow (\text{CPA.}\textit{Enc}_{\mathtt{pk}_0}(m), \text{CPA.}\textit{Enc}_{\mathtt{pk}_1}(m))$;

$p \leftarrow$ NIZK.*Prv*$\big(\mathtt{crs},$

$\mathtt{stmt} \coloneqq$ "There is a message m such that c_0 and c_1 are encryptions of m under $\mathtt{pk}_0$ and $\mathtt{pk}_1$, resp.",

$\mathtt{w} \coloneqq (m,$ Encryption Randomness$)\big)$;

Output (p, c_0, c_1).

$\Pi.$*Dec*$(\mathtt{sk} \coloneqq (\mathtt{sk}_0, \mathtt{pk}), c \coloneqq (p, c_0, c_1))$:

Output $\perp$ if NIZK.*Vfy*$\big(\mathtt{crs}, \mathtt{stmt}, p\big)$ = invalid;

$m \leftarrow$ CPA.*Dec*$_{\mathtt{sk}_0}(c_0)$;

Output m otherwise.

3. Naor-Yung's PKE Scheme

$\Pi.$*Enc*$(\mathtt{pk} := (\mathtt{crs}, \mathtt{pk}_0, \mathtt{pk}_1), m)$:

$(c_0, c_1) \leftarrow (\text{CPA.}\textit{Enc}_{\mathtt{pk}_0}(m), \text{CPA.}\textit{Enc}_{\mathtt{pk}_1}(m))$;

$p \leftarrow$ NIZK.*Prv*$\big(\mathtt{crs},$

$\mathtt{stmt} :=$ "There is a message m such that c_0 and c_1 are encryptions of m under $\mathtt{pk}_0$ and $\mathtt{pk}_1$, resp.",

$\mathtt{w} := (m,$ Encryption Randomness$)\big)$;

Output (p, c_0, c_1).

$\Pi.$*Dec*$(\mathtt{sk} := (\mathtt{sk}_0, \mathtt{pk}), c := (p, c_0, c_1))$:

Output $\perp$ if NIZK.*Vfy*$\big(\mathtt{crs}, \mathtt{stmt}, p\big)$ = invalid;

$m \leftarrow$ CPA.*Dec*$_{\mathtt{sk}_0}(c_0)$;

Output m otherwise.

Simulation Sound NIZK $\Rightarrow$ PKE scheme is IND-CCA-2 secure [3].

[3]: Sahai, FOCS '99

3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

Π.***Setup***:

$\mathtt{crs} \leftarrow$ NIZK.*Gen*$_{CRS}$;
Output $\mathtt{crs}$;

Π.*Gen*:

$\Big((\mathtt{pk}_0, \mathtt{sk}_0), (\mathtt{pk}_1, \mathtt{sk}_1)\Big) \leftarrow$ (CPA.*Gen*, CPA.*Gen*);
$\cancel{\mathtt{crs} \leftarrow \text{NIZK}.\mathit{Gen}_{CRS};}$
Output $\Big(\mathtt{rpk} := (\mathtt{pk}_0, \mathtt{pk}_1), \mathtt{rsk} := (\mathtt{sk}_0, \mathtt{rpk})\Big)$.

3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

$\Pi.\mathit{Enc}(\mathtt{pp} := \mathtt{crs}, \vec{v} := \big(\mathtt{rpk}_1 := (\mathtt{pk}_{1,0}, \mathtt{pk}_{1,1}), \ldots, \mathtt{rpk}_{|\vec{v}|} := (\mathtt{pk}_{|\vec{v}|,0}, \mathtt{pk}_{|\vec{v}|,1})\big), m)$:

$(c_{\boldsymbol{j},0}, c_{\boldsymbol{j},1}) \leftarrow (\mathsf{CPA}.\mathit{Enc}_{\mathtt{pk}_{\boldsymbol{j},0}}(m), \mathsf{CPA}.\mathit{Enc}_{\mathtt{pk}_{\boldsymbol{j},1}}(m))$ **, for each $\boldsymbol{j} \in \{1, \ldots, |\vec{v}|\}$**

$p \leftarrow \mathsf{NIZK}.\mathit{Prv}\big(\mathtt{crs},$

$\mathtt{stmt} :=$ "There is a message m such that **for all $\boldsymbol{j} \in \{1, \ldots, |\vec{v}|\}$, and all $\boldsymbol{b} \in \{0, 1\}$, $c_{\boldsymbol{j},\boldsymbol{b}}$ is an encryption of m under $v_{\boldsymbol{j},\boldsymbol{b}}$.**",

$\mathtt{w} := (m,$ Encryption Randomness$)\big)$;

Output $(p, \vec{c} := \big((c_{1,0}, c_{1,1}), \ldots, (c_{|\vec{v}|,0}, c_{|\vec{v}|,1})\big), \boldsymbol{\vec{v}})$.

3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

$\Pi.\mathit{Enc}(\mathtt{pp} := \mathtt{crs}, \vec{v} := \big(\mathtt{rpk}_1 := (\mathtt{pk}_{1,0}, \mathtt{pk}_{1,1}), \ldots, \mathtt{rpk}_{|\vec{v}|} := (\mathtt{pk}_{|\vec{v}|,0}, \mathtt{pk}_{|\vec{v}|,1})\big), m)$:

$(c_{j,0}, c_{j,1}) \leftarrow (\mathsf{CPA}.\mathit{Enc}_{\mathtt{pk}_{j,0}}(m), \mathsf{CPA}.\mathit{Enc}_{\mathtt{pk}_{j,1}}(m))$ **, for each $j \in \{1, \ldots, |\vec{v}|\}$**

$p \leftarrow \mathsf{NIZK}.\mathit{Prv}\big(\mathtt{crs},$

$\mathtt{stmt} :=$ "There is a message m such that **for all $j \in \{1, \ldots, |\vec{v}|\}$, and all $b \in \{0, 1\}$, $c_{j,b}$ is an encryption of m under $v_{j,b}$.**",

$\mathtt{w} := (m, \text{Encryption Randomness})\big)$;

Output $(p, \vec{c} := \big((c_{1,0}, c_{1,1}), \ldots, (c_{|\vec{v}|,0}, c_{|\vec{v}|,1})\big), \vec{v})$.

$\Pi.\mathit{Dec}(\mathtt{pp} := \mathtt{crs}, \mathtt{rsk} := (\mathtt{sk}_0, \mathtt{rpk}), c := (p, \vec{c} := \big((c_{1,0}, c_{1,1}), \ldots, (c_{|\vec{v}|,0}, c_{|\vec{v}|,1})\big), \vec{v}))$:

Output $\perp$ if $\mathsf{NIZK}.\mathit{Vfy}\big(\mathtt{crs}, \mathtt{stmt}, p\big)$ = invalid;

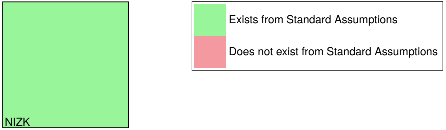
Let $i \in \{1, \ldots, |\vec{v}|\}$ be (the least number) such that $v_i = \mathtt{rpk}$;

Output $\perp$ if there is no such i;

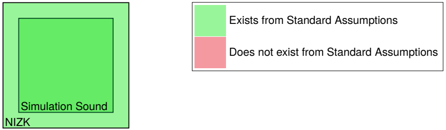
$m \leftarrow \mathsf{CPA}.\mathit{Dec}_{\mathtt{sk}_0}(c_{i,0})$;

Output $(\vec{v}, m)$ otherwise.

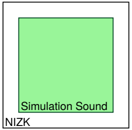
3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

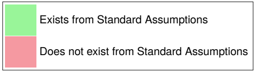


3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

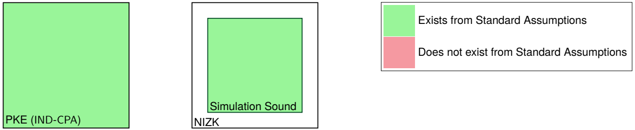


3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)

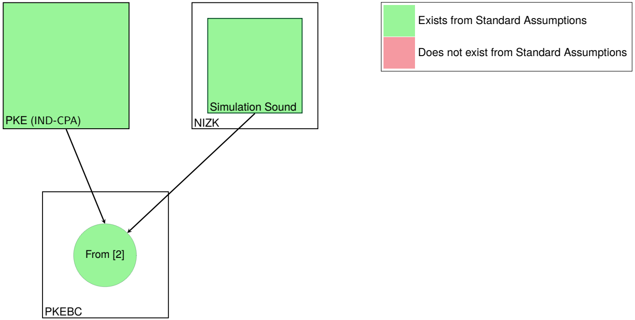




3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)



3. Naor-Yung Scheme's Trivial Generalization (Non IK-CCA-2 Secure)



3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

Main idea:

Add a (Binding) Commitment to $\vec{v}$ (vector of receivers' public keys) and m;

3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

Main idea:

Add a (Binding) Commitment to $\vec{v}$ (vector of receivers' public keys) and m;

Encrypt $\vec{v}$, m and commitment's randomness to each receiver;

3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

Building Blocks:

- (Statistically Binding) Commitment scheme CS $= (Gen_{CRS}, Commit, Verify)$;
- (IND-CPA and IK-CPA secure) PKE scheme CPA $= (Gen, Enc, Dec)$;
- (Simulation Sound) NIZK $= (Gen_{CRS}, Prv, Vfy)$.

3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

$\Pi.\textit{Setup}$:

$\mathtt{crs}_{\mathsf{NIZK}} \leftarrow \mathsf{NIZK}.\mathit{Gen}_{\mathit{CRS}}$;
$\mathtt{crs}_{\mathsf{CS}} \leftarrow \mathsf{CS}.\mathit{Gen}_{\mathit{CRS}}$;
Output $(\mathtt{crs}_{\mathsf{NIZK}}, \mathtt{crs}_{\mathsf{CS}})$;

$\Pi.\textit{Gen}$:

$\Big((\mathtt{pk}_0, \mathtt{sk}_0), (\mathtt{pk}_1, \mathtt{sk}_1)\Big) \leftarrow (\mathsf{CPA}.\mathit{Gen}, \mathsf{CPA}.\mathit{Gen})$;
Output $\Big(\mathtt{rpk} \coloneqq (\mathtt{pk}_0, \mathtt{pk}_1), \mathtt{rsk} \coloneqq (\mathtt{sk}_0, \mathtt{rpk})\Big)$.

3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

$\Pi.\mathit{Enc}(\mathtt{pp} := (\mathtt{crs}_{\mathsf{NIZK}}, \mathtt{crs}_{\mathsf{CS}}), \vec{v} := \big(\mathtt{rpk}_0 := (\mathtt{pk}_{1,0}, \mathtt{pk}_{1,1}), \ldots, \mathtt{rpk}_{|\vec{v}|} := (\mathtt{pk}_{|\vec{v}|,0}, \mathtt{pk}_{|\vec{v}|,1})\big), m)$:

$\mathtt{comm} \leftarrow \mathsf{CS}.\mathit{Commit}(\mathtt{crs}_{\mathsf{CS}}, (\vec{v}, m); \rho)$;

$(c_{j,0}, c_{j,1}) \leftarrow (\mathsf{CPA}.\mathit{Enc}_{\mathtt{pk}_{j,0}}(\rho, \vec{v}, m), \mathsf{CPA}.\mathit{Enc}_{\mathtt{pk}_{j,1}}(\rho, \vec{v}, m))$, for each $i \in \{1, \ldots, |\vec{v}|\}$;

$p \leftarrow \mathsf{NIZK}.\mathit{Prv}\big(\mathtt{crs}_{\mathsf{NIZK}},$

$\mathtt{stmt} :=$ "There is a message m, **a vector $\vec{v}$ and a sequence** ρ such that:

for all $i \in \{1, \ldots, |\vec{v}|\}$, $b \in \{0, 1\}$, $c_{i,b}$ is an encryption of $(\rho, \vec{v}, m)$ under $v_{i,b}$,

and $\mathtt{comm} = \mathsf{CS}.\mathit{Commit}(\mathtt{crs}_{\mathsf{CS}}, (\vec{v}, m); \rho)$.",

$\mathtt{w} := (m, \vec{v}, \rho,$ Encryption Randomness$)\big)$;

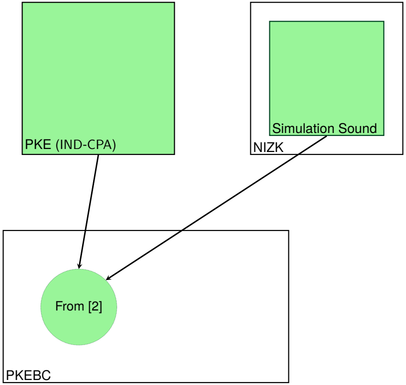
Output $(\mathtt{comm}, p, \vec{c})$.

3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction

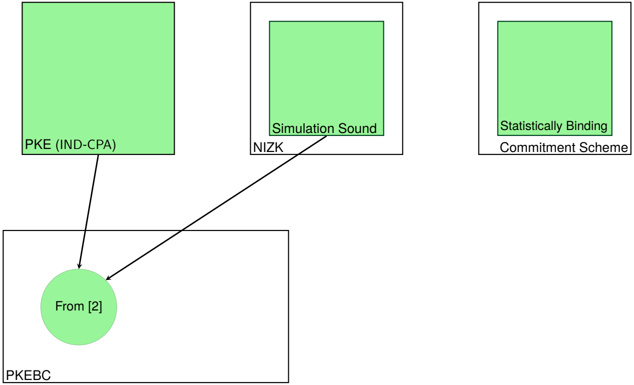
$\Pi.\textit{Dec}(\texttt{pp} := (\texttt{crs}_{\mathsf{NIZK}}, \texttt{crs}_{\mathsf{CS}}), \texttt{rsk} := (\texttt{sk}_0, \texttt{rpk}), c := (\texttt{comm}, p, \vec{c}))$:

Output $\perp$ if NIZK.*Vfy*$\big(\texttt{crs}, \texttt{stmt}, p\big)$ = invalid;
Find the least $i \in \{1, \ldots, |\vec{v}|\}$ with
$(\rho, \vec{v}, m) \leftarrow$ CPA.*Dec*$_{\texttt{sk}_0}(c_{i,0})$ satisfying:
$(\rho, \vec{v}, m) \neq \perp$;
$v_i = \texttt{rpk}$;
$c.\texttt{comm} =$ CS.*Commit*$(\texttt{crs}_{\mathsf{CS}}, (\vec{v}, m); \rho)$;
Output $\perp$ if there is no such i;
Output $(\vec{v}, m)$ otherwise.

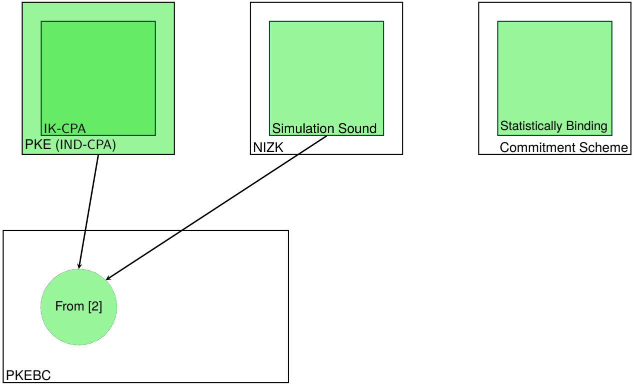
3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction



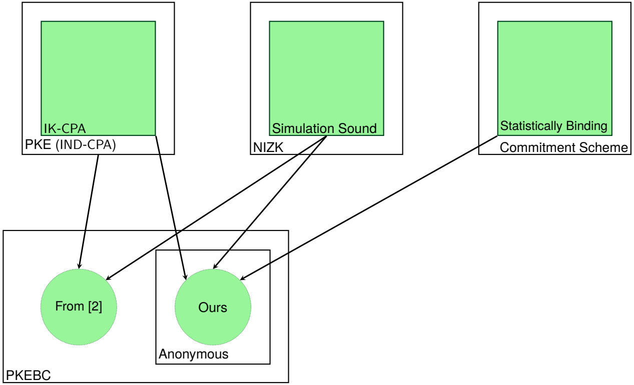
3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction



3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction



3. Our (IK-CCA-2 Secure) PKEBC Scheme Construction



Outline

1. Contributions
2. Public Key Encryption for Broadcast (PKEBC)
3. PKEBC Scheme Construction
4. Multi-Designated Receiver Signed Public Key Encryption (MDRS-PKE)
5. MDRS-PKE Scheme Construction

4. MDRS-PKE — Syntax

$(\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rsk}_{\mathsf{B1}})$

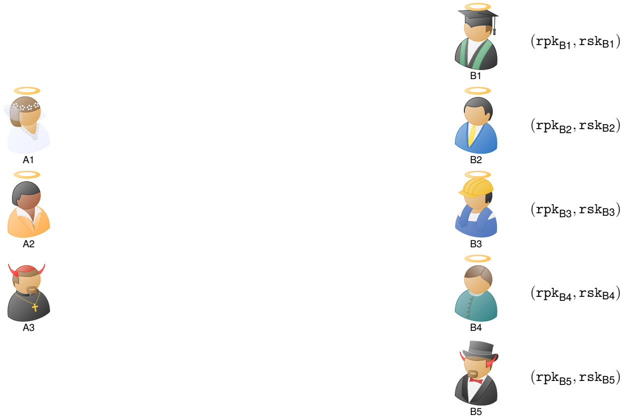
$(\mathtt{rpk}_{\mathsf{B2}}, \mathtt{rsk}_{\mathsf{B2}})$

$(\mathtt{rpk}_{\mathsf{B3}}, \mathtt{rsk}_{\mathsf{B3}})$

$(\mathtt{rpk}_{\mathsf{B4}}, \mathtt{rsk}_{\mathsf{B4}})$

$(\mathtt{rpk}_{\mathsf{B5}}, \mathtt{rsk}_{\mathsf{B5}})$

4. MDRS-PKE — Syntax

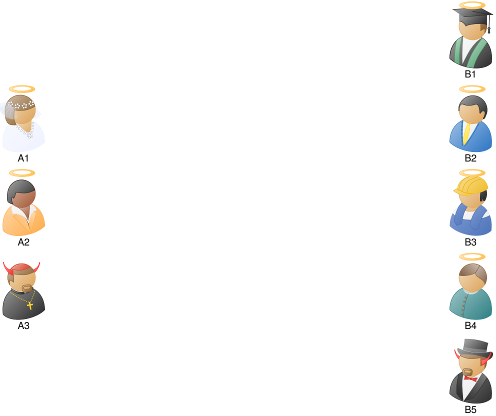


4. MDRS-PKE — Syntax

$(\texttt{spk}_{A1}, \texttt{ssk}_{A1})$

$(\texttt{spk}_{A2}, \texttt{ssk}_{A2})$

$(\texttt{spk}_{A3}, \texttt{ssk}_{A3})$



$(\texttt{rpk}_{B1}, \texttt{rsk}_{B1})$

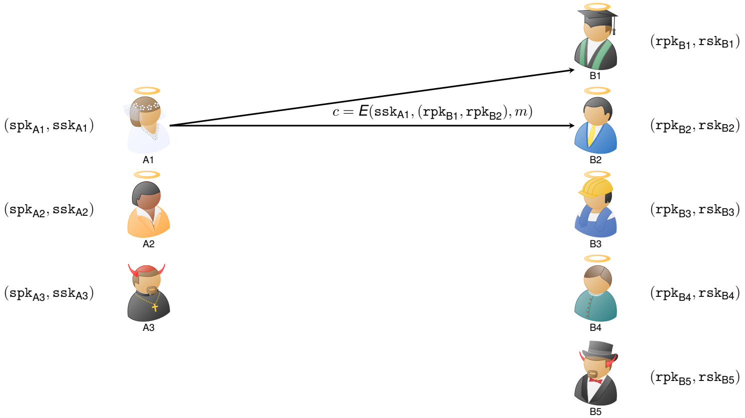
$(\texttt{rpk}_{B2}, \texttt{rsk}_{B2})$

$(\texttt{rpk}_{B3}, \texttt{rsk}_{B3})$

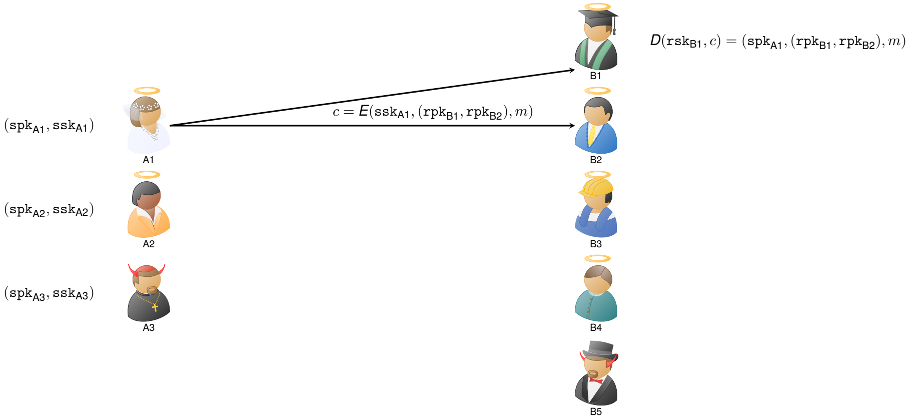
$(\texttt{rpk}_{B4}, \texttt{rsk}_{B4})$

$(\texttt{rpk}_{B5}, \texttt{rsk}_{B5})$

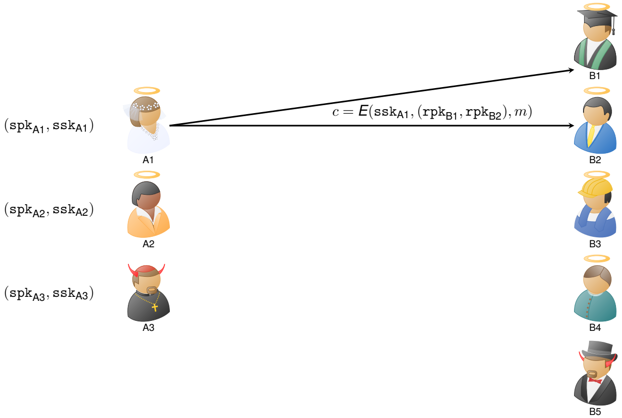
4. MDRS-PKE — Syntax



4. MDRS-PKE — Syntax



4. MDRS-PKE — Syntax



$D(\mathtt{rsk}_{B1}, c) = (\mathtt{spk}_{A1}, (\mathtt{rpk}_{B1}, \mathtt{rpk}_{B2}), m)$

Syntax of decryption:

- Only $\mathtt{rsk}_{B1}$ is needed;
- Outputs sender's $\mathtt{spk}$ and vector of receivers' $\mathtt{rpk}$.

4. MDRS-PKE — Security Notions

Off-The-Record

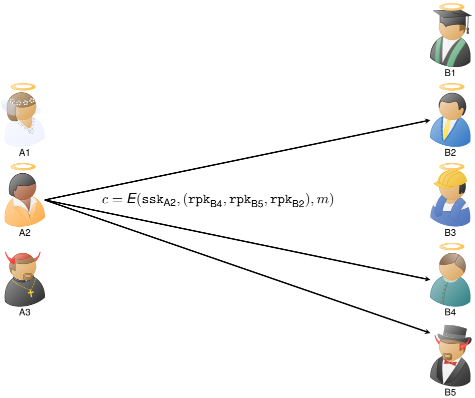
Unforgeability

Consistency

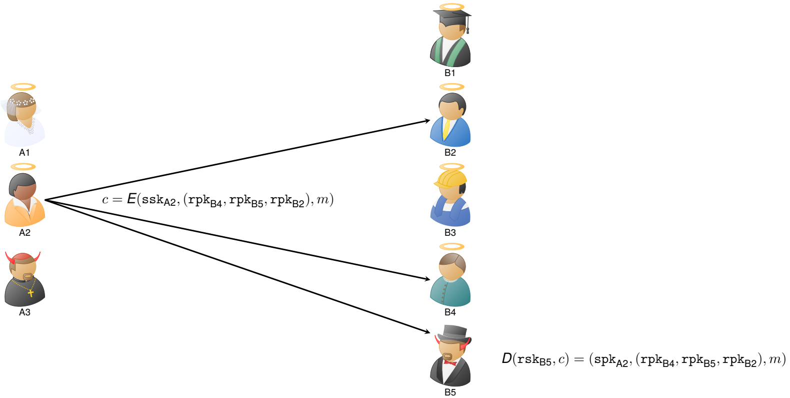
Confidentiality (IND-CCA-2 security)

+ Anonymity (IK-CCA-2 security)

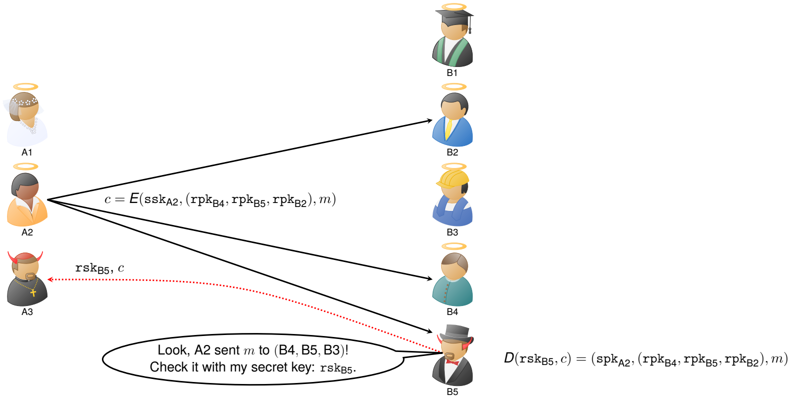
4. MDRS-PKE — Off-The-Record



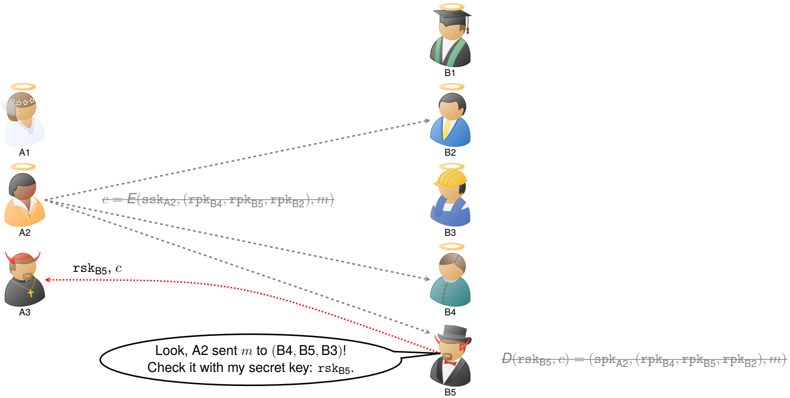
4. MDRS-PKE — Off-The-Record



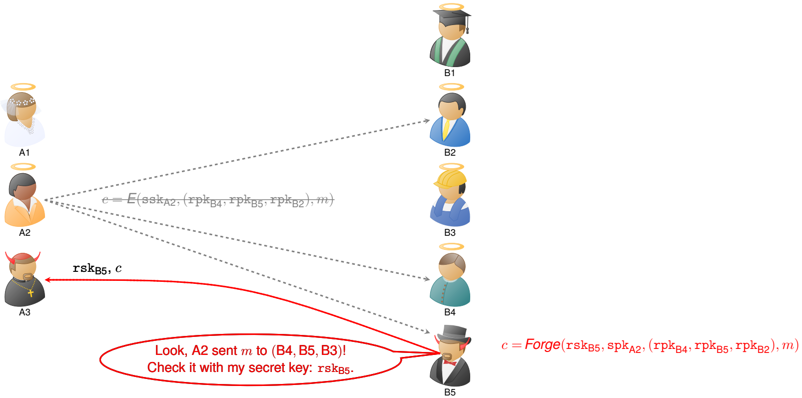
4. MDRS-PKE — Off-The-Record



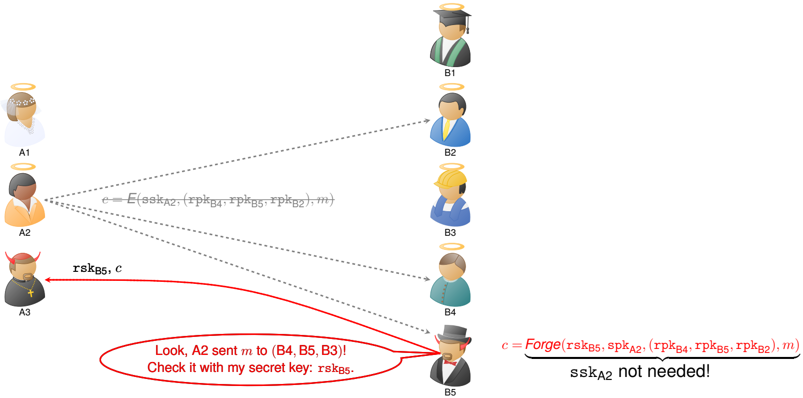
4. MDRS-PKE — Off-The-Record



4. MDRS-PKE — Off-The-Record



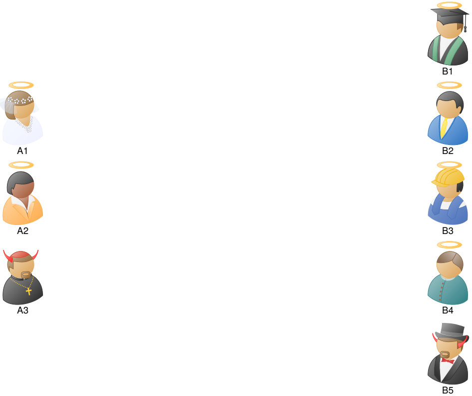
4. MDRS-PKE — Off-The-Record



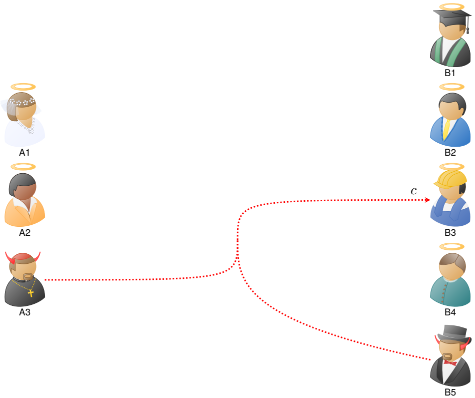
4. MDRS-PKE — Off-The-Record

$$c = \underbrace{\textit{Forge}(\mathtt{rsk}_{B5}, \mathtt{spk}_{A2}, (\mathtt{rpk}_{B4}, \mathtt{rpk}_{B5}, \mathtt{rpk}_{B2}), m)}_{\mathtt{ssk}_{A2} \text{ not needed!}}$$

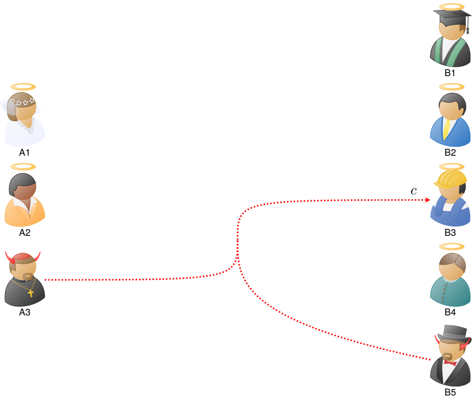
4. MDRS-PKE — Authenticity (Existential Unforgeability)



4. MDRS-PKE — Authenticity (Existential Unforgeability)



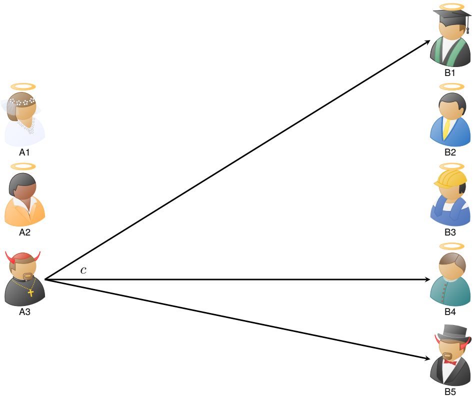
4. MDRS-PKE — Authenticity (Existential Unforgeability)



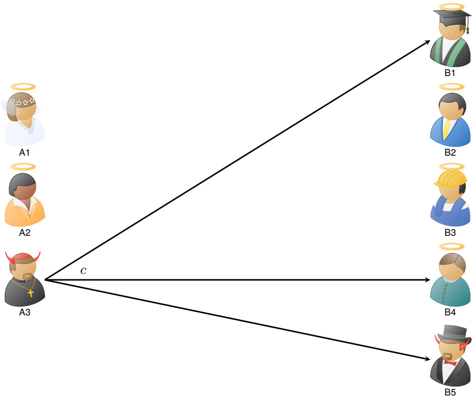
$D(\texttt{rsk}_{\mathsf{B3}}, c) = \perp$, or $D(\texttt{rsk}_{\mathsf{B3}}, c) = (\texttt{spk}, \vec{v}, m)$ and for every (honest) sender Ai, either $\texttt{spk} \neq \texttt{spk}_{\mathsf{Ai}}$ or Ai sent m to $\vec{v}$ before.

4. MDRS-PKE — Consistency

4. MDRS-PKE — Consistency

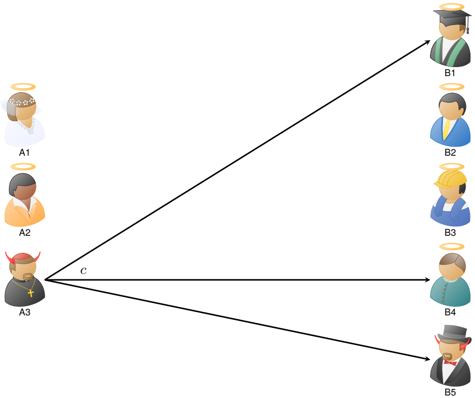


4. MDRS-PKE — Consistency



$D(\mathtt{rsk}_{\mathsf{B1}}, c) = (\mathtt{spk}_{\mathsf{X}}, (\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B4}}, \mathtt{rpk}_{\mathsf{B5}}), m)$

4. MDRS-PKE — Consistency

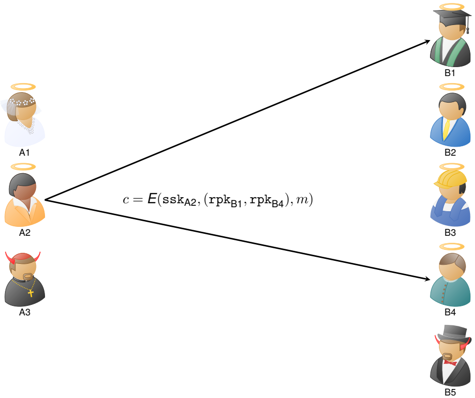


$D(\mathtt{rsk}_{\mathsf{B1}}, c) = (\mathtt{spk}_{\mathsf{X}}, (\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B4}}, \mathtt{rpk}_{\mathsf{B5}}), m)$

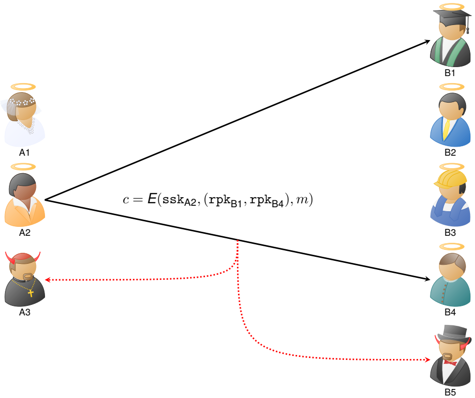
$D(\mathtt{rsk}_{\mathsf{B4}}, c) = (\mathtt{spk}_{\mathsf{X}}, (\mathtt{rpk}_{\mathsf{B1}}, \mathtt{rpk}_{\mathsf{B4}}, \mathtt{rpk}_{\mathsf{B5}}), m)$

4. MDRS-PKE — Confidentiality (IND-CCA-2 Security)

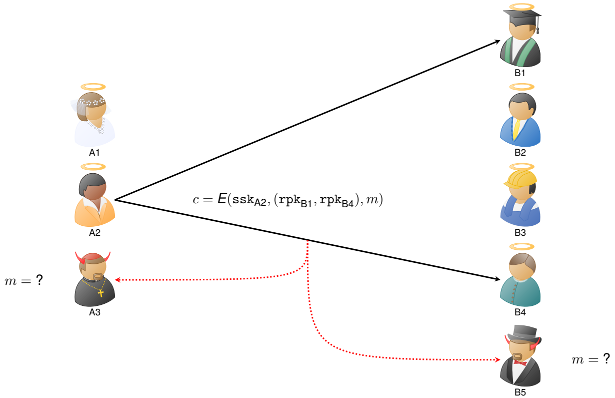
4. MDRS-PKE — Confidentiality (IND-CCA-2 Security)



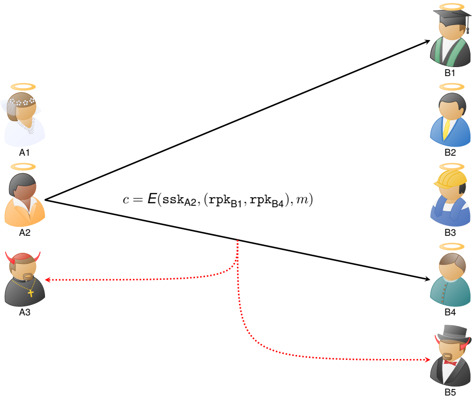
4. MDRS-PKE — Confidentiality (IND-CCA-2 Security)



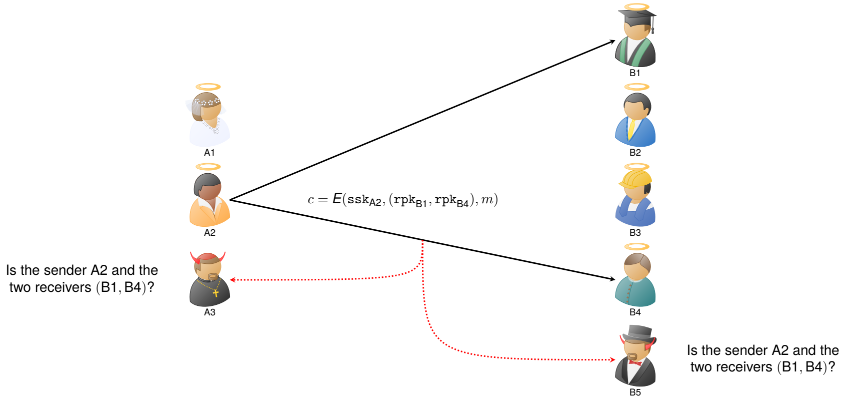
4. MDRS-PKE — Confidentiality (IND-CCA-2 Security)



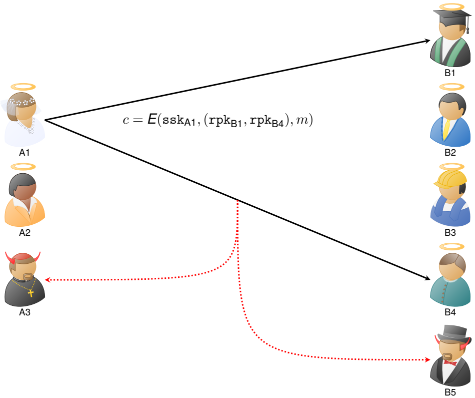
4. MDRS-PKE — Anonymity (IK-CCA-2 Security)



4. MDRS-PKE — Anonymity (IK-CCA-2 Security)



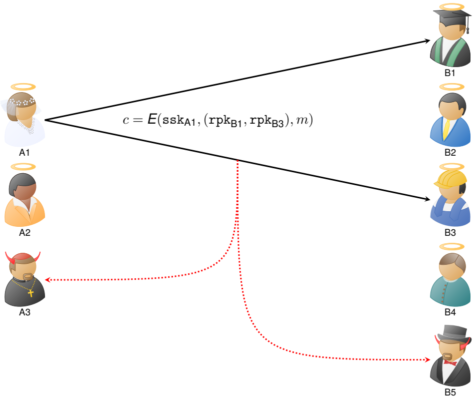
4. MDRS-PKE — Anonymity (IK-CCA-2 Security)



Is the sender A1 and the two receivers $(\mathsf{B1}, \mathsf{B4})$?

Is the sender A1 and the two receivers $(\mathsf{B1}, \mathsf{B4})$?

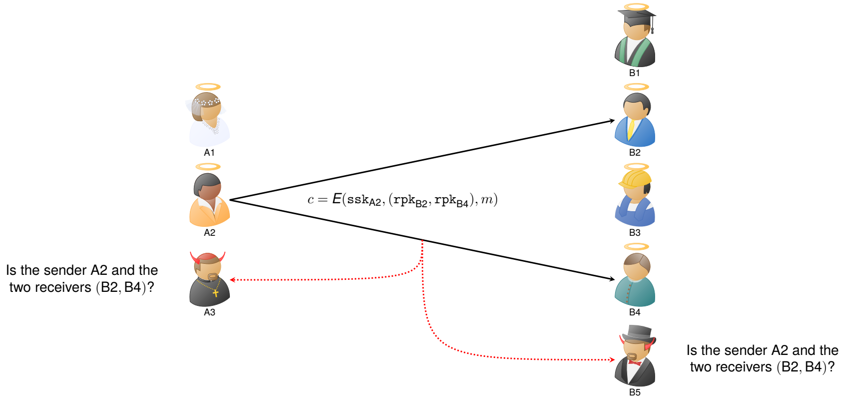
4. MDRS-PKE — Anonymity (IK-CCA-2 Security)



Is the sender A1 and the two receivers $(\mathsf{B1}, \mathsf{B3})$?

Is the sender A1 and the two receivers $(\mathsf{B1}, \mathsf{B3})$?

4. MDRS-PKE — Anonymity (IK-CCA-2 Security)



Outline

5. Our MDRS-PKE Scheme Construction

5. Our MDRS-PKE Scheme Construction

Building Blocks:

- MDVS $= (\textit{Setup}, \textit{Gen}_{\mathsf{Sig}}, \textit{Gen}_{\mathsf{Vrf}}, \textit{Sign}, \textit{Vfy})$;
- (IK-CCA-2 secure) PKEBC $= (\textit{Setup}, \textit{Gen}_{\mathsf{Snd}}, \textit{Gen}_{\mathsf{Rcv}}, \textit{Enc}, \textit{Dec})$;

5. Our MDRS-PKE Scheme Construction

Building Blocks:

- MDVS $= (\mathit{Setup}, \mathit{Gen}_{\mathsf{Sig}}, \mathit{Gen}_{\mathsf{Vrf}}, \mathit{Sign}, \mathit{Vfy})$;
- (IK-CCA-2 secure) PKEBC $= (\mathit{Setup}, \mathit{Gen}_{\mathsf{Snd}}, \mathit{Gen}_{\mathsf{Rcv}}, \mathit{Enc}, \mathit{Dec})$;

Main idea: “Sign-then-Encrypt”

5. Our MDRS-PKE Scheme Construction

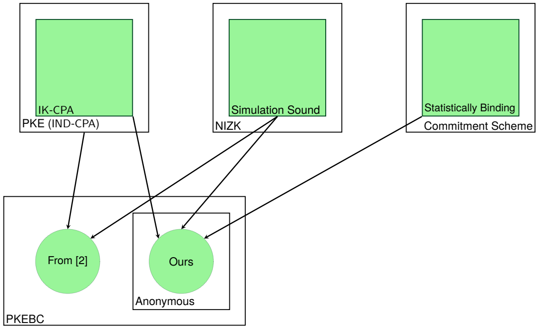
Building Blocks:

- MDVS $= (\textit{Setup}, \textit{Gen}_{\mathsf{Sig}}, \textit{Gen}_{\mathsf{Vrf}}, \textit{Sign}, \textit{Vfy})$;
- (IK-CCA-2 secure) PKEBC $= (\textit{Setup}, \textit{Gen}_{\mathsf{Snd}}, \textit{Gen}_{\mathsf{Rcv}}, \textit{Enc}, \textit{Dec})$;

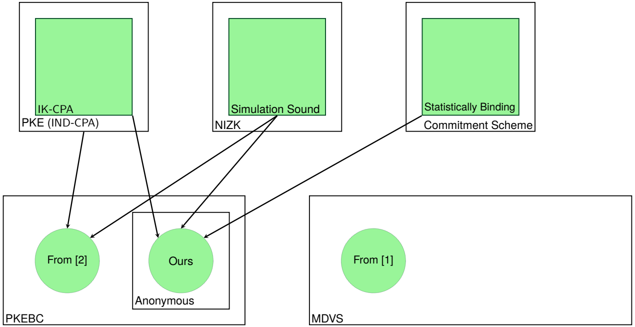
Main idea: "Sign-then-Encrypt"

Use MDVS to sign vector of receivers and message;
Then, use PKEBC to encrypt the sender's and all receivers' public keys, message and the signature.

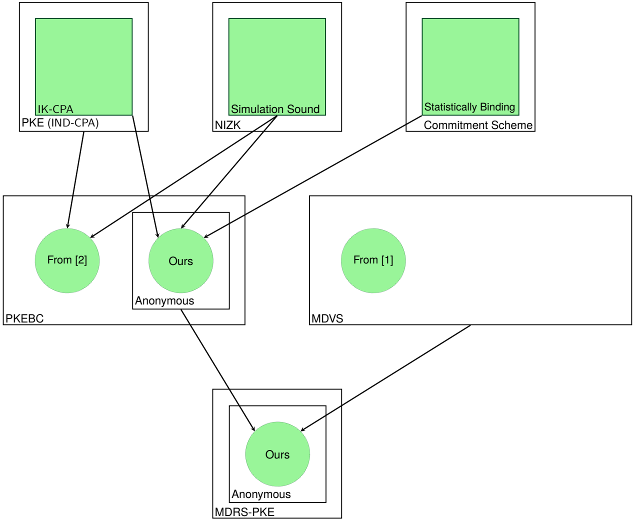
5. Our MDRS-PKE Scheme Construction



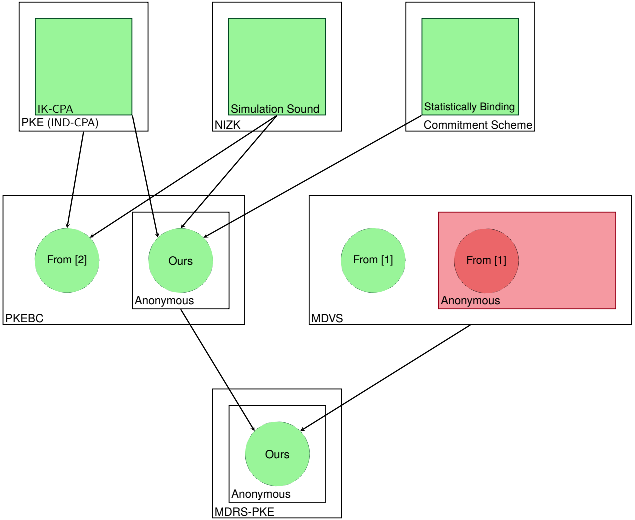
5. Our MDRS-PKE Scheme Construction



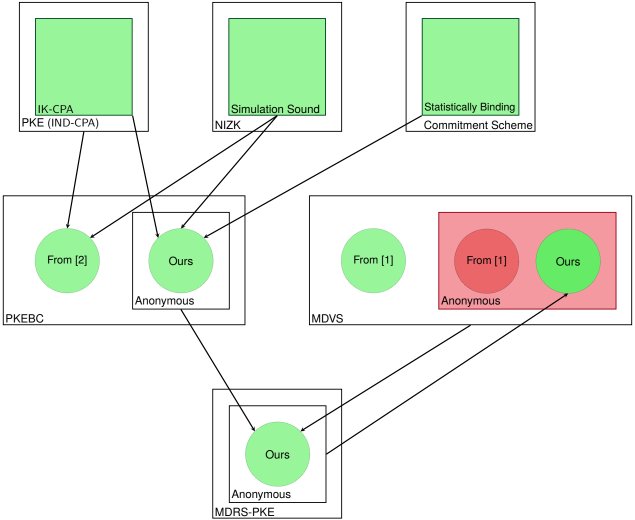
5. Our MDRS-PKE Scheme Construction



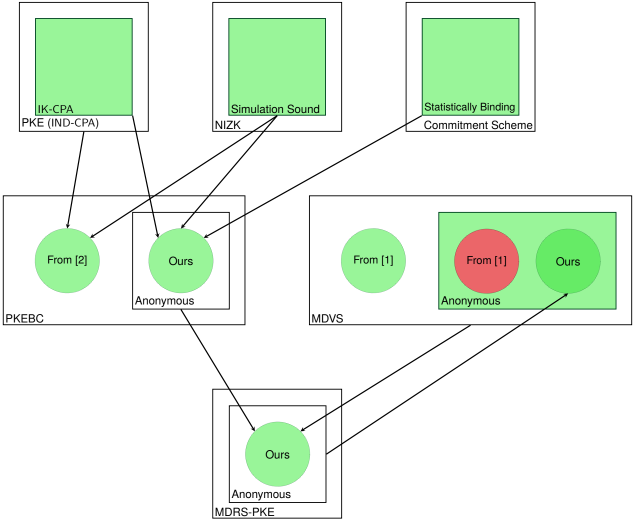
5. Our MDRS-PKE Scheme Construction



5. Our MDRS-PKE Scheme Construction



5. Our MDRS-PKE Scheme Construction



Thank you!

Bibliography

[1] Ivan Damgård, Helene Haagh, Rebekah Mercer, Anca Nitulescu, Claudio Orlandi, and Sophia Yakoubov.
Stronger security and constructions of multi-designated verifier signatures.
In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part II*, volume 12551 of *LNCS*, pages 229–260. Springer, Heidelberg, November 2020.

[2] Moni Naor and Moti Yung.
Public-key cryptosystems provably secure against chosen ciphertext attacks.
In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.

[3] Amit Sahai.
Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security.
In *40th FOCS*, pages 543–553. IEEE Computer Society Press, October 1999.

Outline

6. Full MDRS-PKE construction

6. MDRS-PKE Scheme Construction

MDRS-PKE.*Setup*:

$\mathtt{pp}_{\text{MDVS}} \leftarrow$ MDVS.*Setup*(1^k);
$\mathtt{pp}_{\text{PKEBC}} \leftarrow$ PKEBC.*Setup*(1^k);
Output $\mathtt{pp} = (\mathtt{pp}_{\text{MDVS}}, \mathtt{pp}_{\text{PKEBC}})$;

MDRS-PKE.*Gen*$_{Snd}(\mathtt{pp} = (\mathtt{pp}_{\text{MDVS}}, \mathtt{pp}_{\text{PKEBC}}))$:

$(\mathtt{spk}_{\text{MDVS}}, \mathtt{ssk}_{\text{MDVS}}) \leftarrow$ MDVS.*Gen*$_{Sig}(\mathtt{pp}_{\text{MDVS}})$;
Output $(\mathtt{spk} := \mathtt{spk}_{\text{MDVS}}, \mathtt{ssk} := (\mathtt{spk}, \mathtt{ssk}_{\text{MDVS}}))$;

MDRS-PKE.*Gen*$_{Rcv}(\mathtt{pp} = (\mathtt{pp}_{\text{MDVS}}, \mathtt{pp}_{\text{PKEBC}}))$:

$(\mathtt{vpk}_{\text{MDVS}}, \mathtt{vsk}_{\text{MDVS}}) \leftarrow$ MDVS.*Gen*$_V(\mathtt{pp}_{\text{MDVS}})$;
$(\mathtt{rpk}_{\text{PKEBC}}, \mathtt{rsk}_{\text{PKEBC}}) \leftarrow$ PKEBC.*Gen*$(\mathtt{pp}_{\text{PKEBC}})$;
Output $\Big(\mathtt{rpk} := (\mathtt{vpk}_{\text{MDVS}}, \mathtt{rpk}_{\text{PKEBC}}), \mathtt{rsk} := \big(\mathtt{rpk}, (\mathtt{vsk}_{\text{MDVS}}, \mathtt{rsk}_{\text{PKEBC}})\big)\Big)$;

6. MDRS-PKE Scheme Construction

MDRS-PKE.*Enc*$(\mathtt{ssk}_i := (\mathtt{spk}_i, \mathtt{ssk}_{\mathsf{MDVS}\,i}), \vec{v} := \big(\mathtt{rpk}_1, \ldots, \mathtt{rpk}_{|\vec{v}|}\big), m)$:
(where $\mathtt{rpk}_i := (\mathtt{vpk}_{\mathsf{MDVS}\,i}, \mathtt{rpk}_{\mathsf{PKEBC}\,i})$)

Let $\vec{v}_{\mathsf{PKEBC}} = (\mathtt{rpk}_{\mathsf{PKEBC}\,1}, \ldots, \mathtt{rpk}_{\mathsf{PKEBC}\,|\vec{v}|})$;
Let $\vec{v}_{\mathsf{MDVS}} = (\mathtt{vpk}_{\mathsf{MDVS}\,1}, \ldots, \mathtt{vpk}_{\mathsf{MDVS}\,|\vec{v}|})$;
$\sigma \leftarrow$ MDVS.*Sign*$(\mathtt{ssk}_{\mathsf{MDVS}\,i}, \vec{v}_{\mathsf{MDVS}}, (\vec{v}_{\mathsf{PKEBC}}, m))$;
Output PKEBC.*Enc*$\big(\vec{v}_{\mathsf{PKEBC}}, (\mathtt{spk}_i, \vec{v}_{\mathsf{MDVS}}, m, \sigma)\big)$;

6. MDRS-PKE Scheme Construction

$$\text{MDRS-PKE.}\textit{Dec}(\mathtt{rsk}_j := \big(\mathtt{rpk}_j, (\mathtt{vsk}_{\text{MDVS}\,j}, \mathtt{rsk}_{\text{PKEBC}\,j})\big), c)\text{:}$$
$$(\text{where } \mathtt{rpk}_j := (\mathtt{vpk}_{\text{MDVS}\,j}, \mathtt{rpk}_{\text{PKEBC}\,j}))$$

$\big(\vec{v}_{\text{PKEBC}}, (\mathtt{spk}_i, \vec{v}_{\text{MDVS}}, m, \sigma)\big) \leftarrow \text{PKEBC.}\textit{D}(\mathtt{rsk}_{\text{PKEBC}\,j}, c)$;
Output $\perp$ if $\big(\vec{v}_{\text{PKEBC}}, (\mathtt{spk}_i, \vec{v}_{\text{MDVS}}, m, \sigma)\big) = \perp$ or $|\vec{v}_{\text{PKEBC}}| \neq |\vec{v}_{\text{MDVS}}|$;
Let $\vec{v} = \big((v_{\text{MDVS}\,1}, v_{\text{PKEBC}\,1}), \ldots, (v_{\text{MDVS}\,|\vec{v}_{\text{PKEBC}}|}, v_{\text{PKEBC}\,|\vec{v}_{\text{PKEBC}}|})\big)$;
Output $\perp$ if $\mathtt{rpk}_j \notin \vec{v}$ or MDVS.*Vfy*$(\mathtt{spk}_i, \mathtt{vsk}_{\text{MDVS}\,j}, \vec{v}_{\text{MDVS}}, (\vec{v}_{\text{PKEBC}}, m), \sigma) \neq \mathtt{valid}$;
Output $(\mathtt{spk}_i, \vec{v}, m)$;