Access Control Encryption for Equality, Comparison, and More

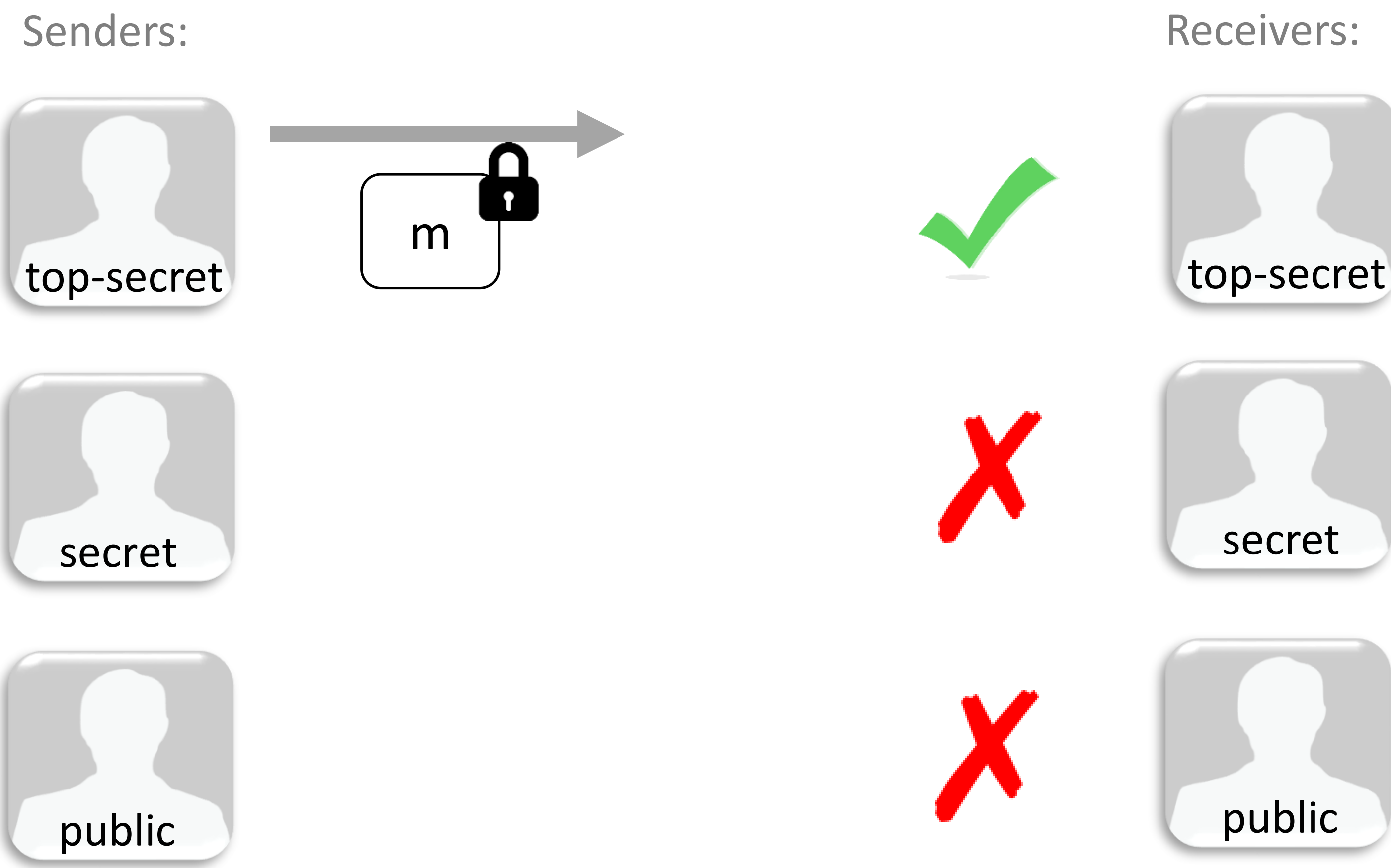
Georg Fuchsbauer, ENS

Romain Gay, ENS

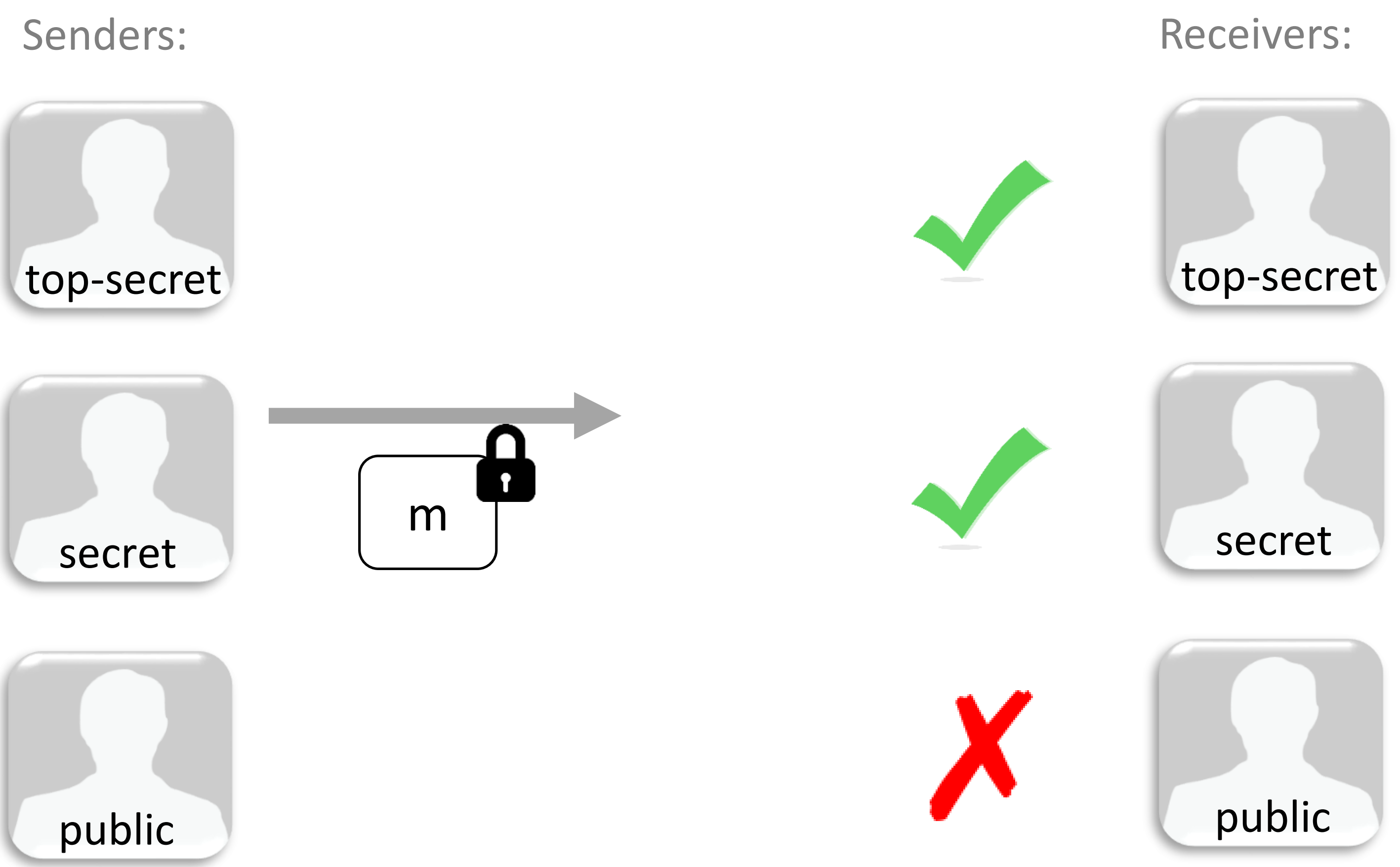
Lucas Kowalczyk, Columbia University

Claudio Orlandi, Aarhus university

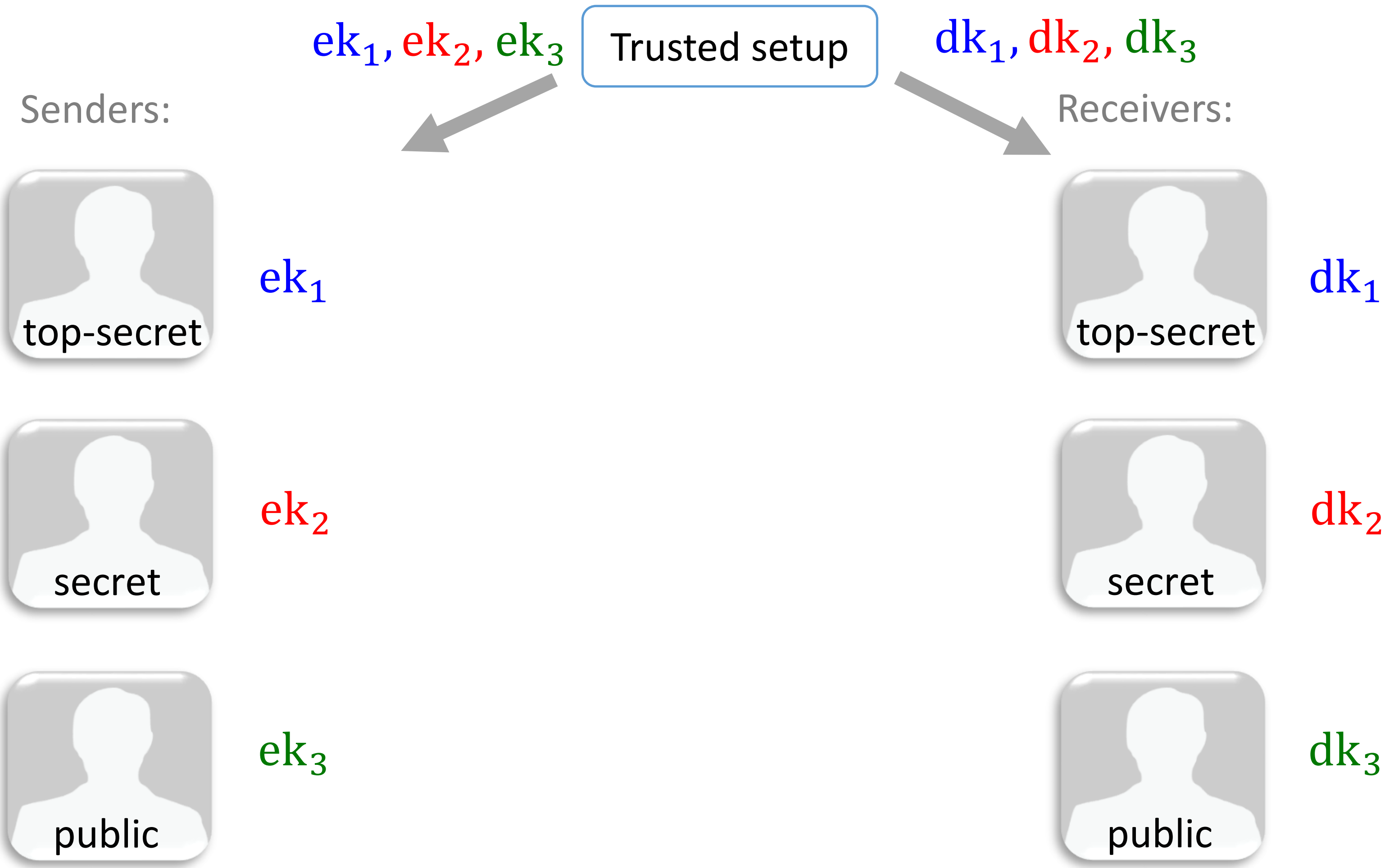
ACE [Damgård, Haagh, Orlandi 16]



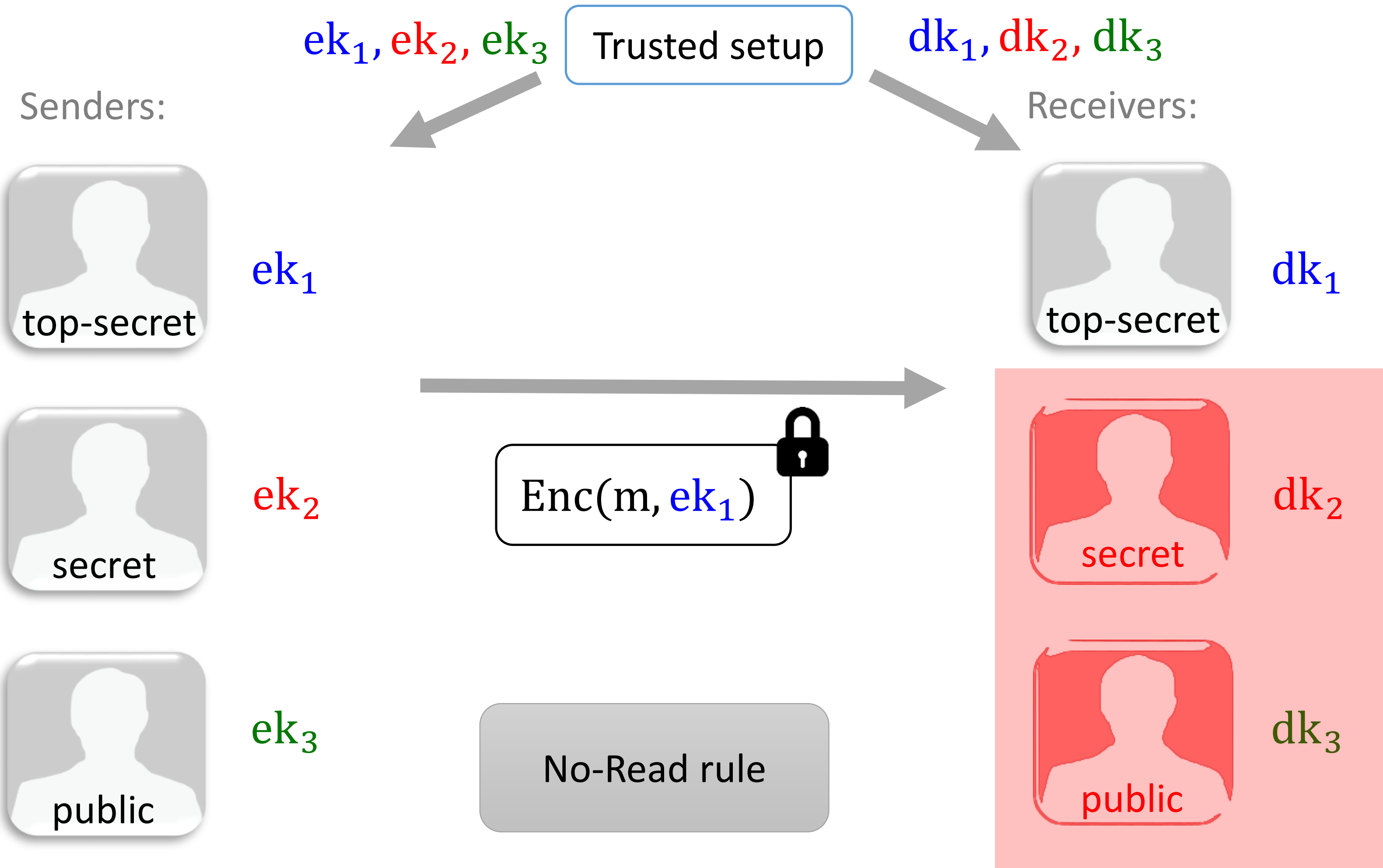
ACE [Damgård, Haagh, Orlandi 16]



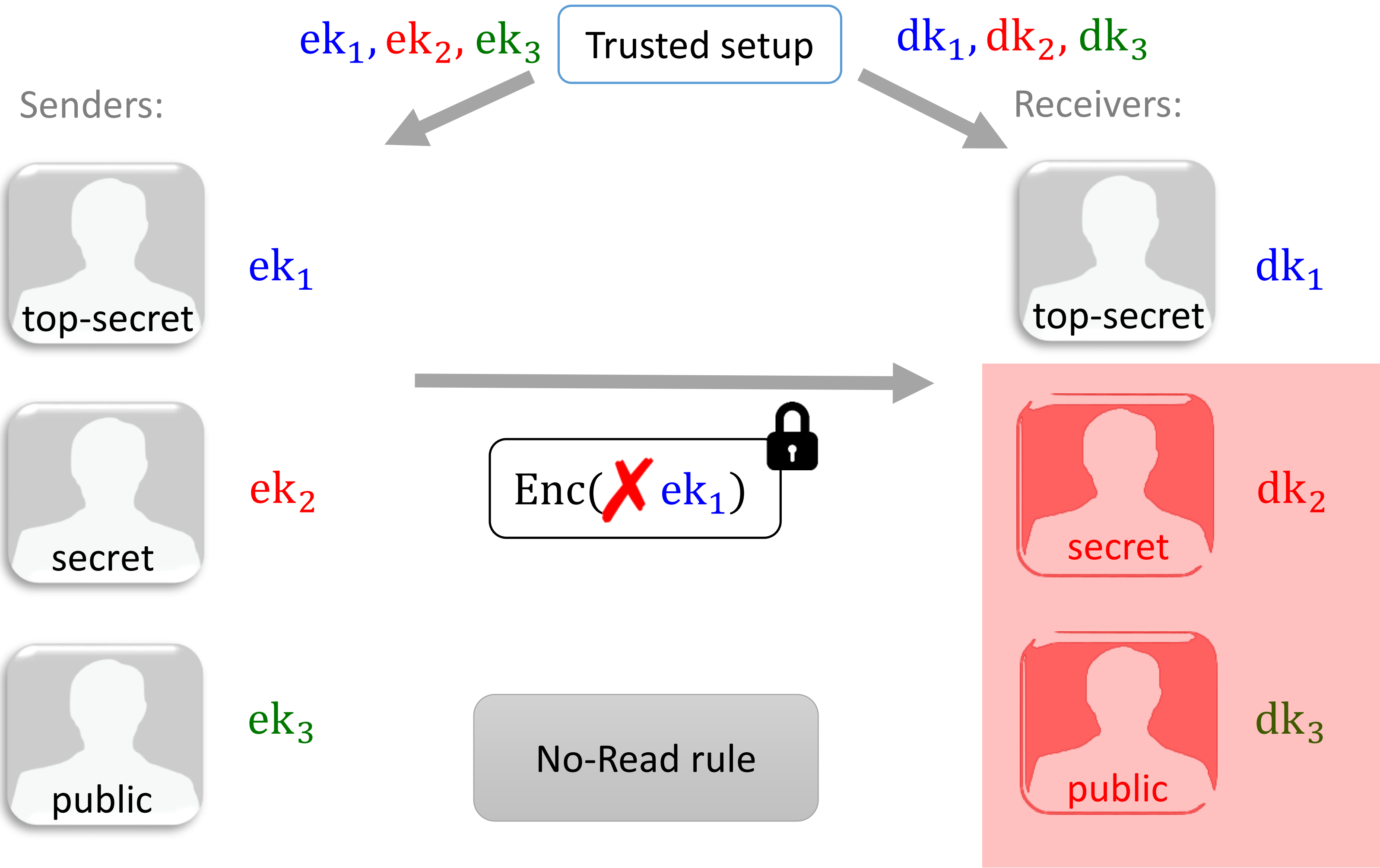
ACE [Damgård, Haagh, Orlandi 16]



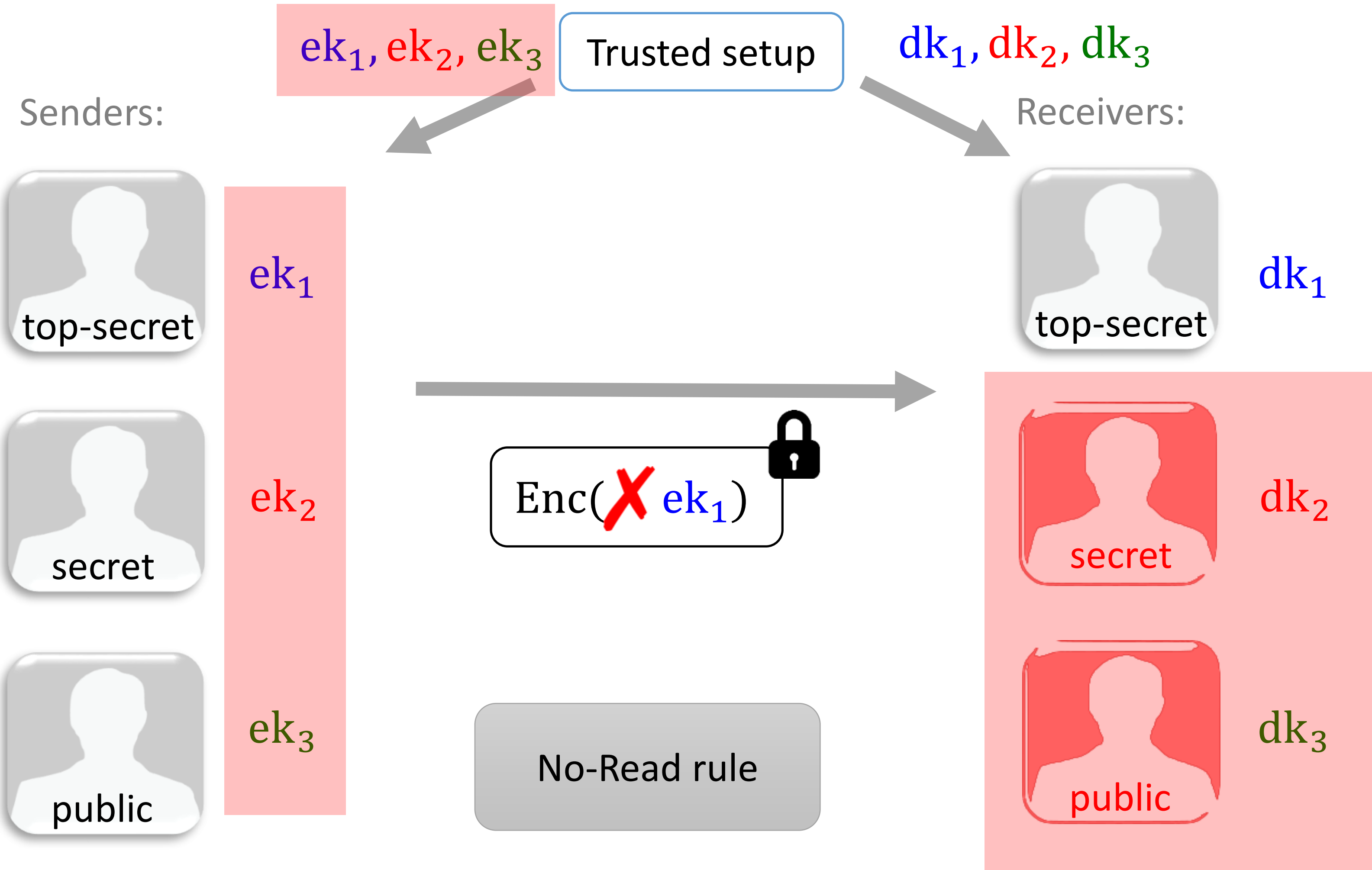
ACE [Damgård, Haagh, Orlandi 16]



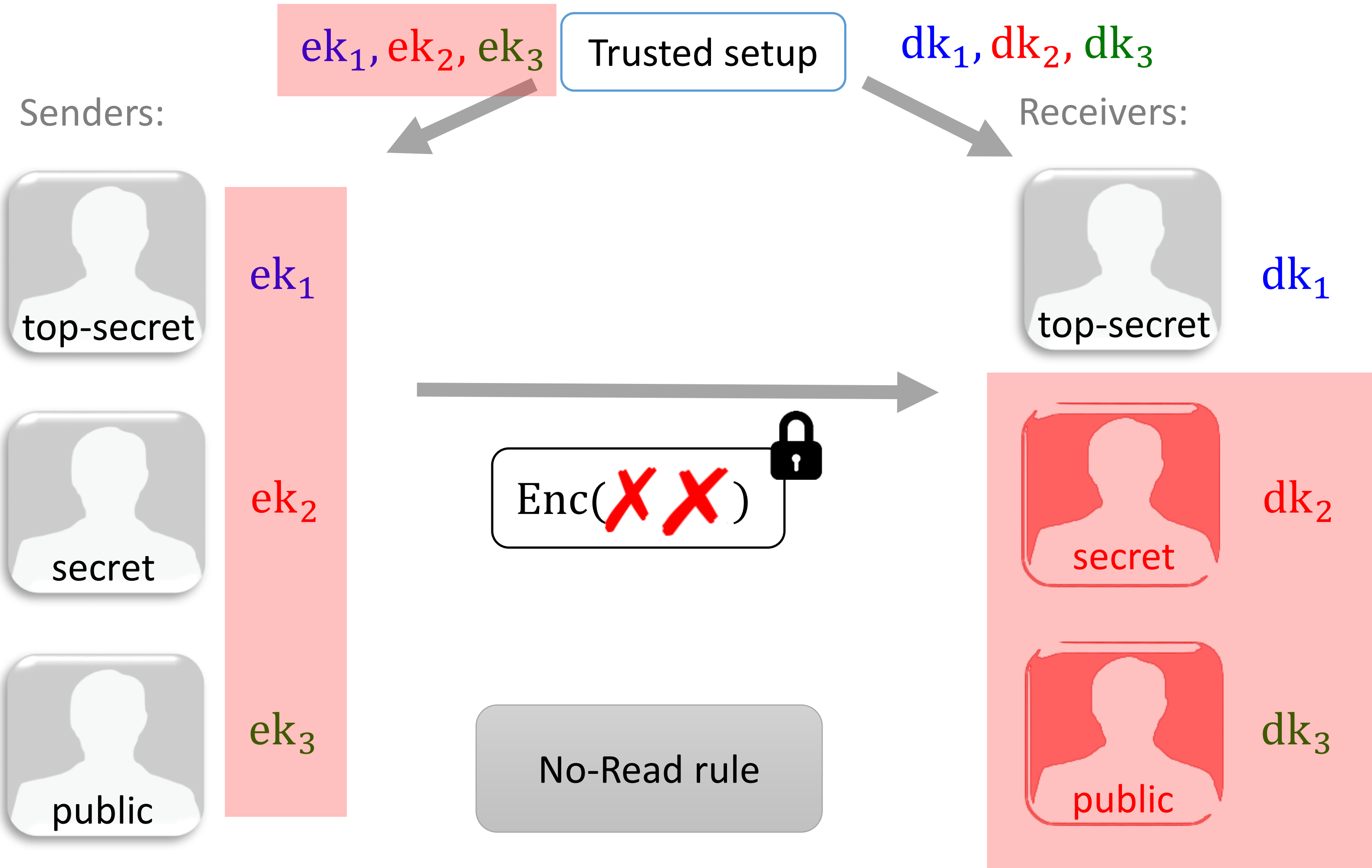
ACE [Damgård, Haagh, Orlandi 16]



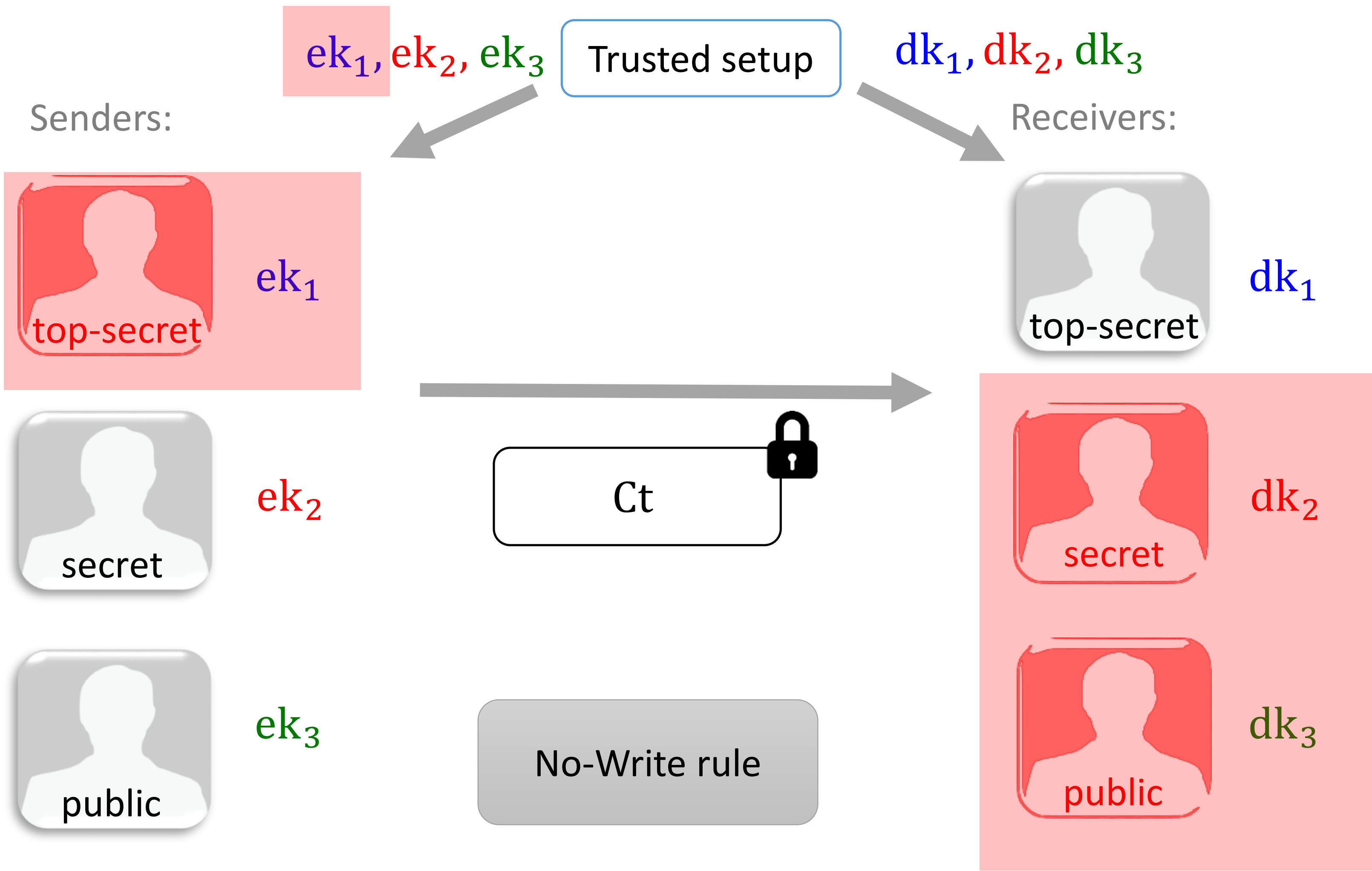
ACE [Damgård, Haagh, Orlandi 16]



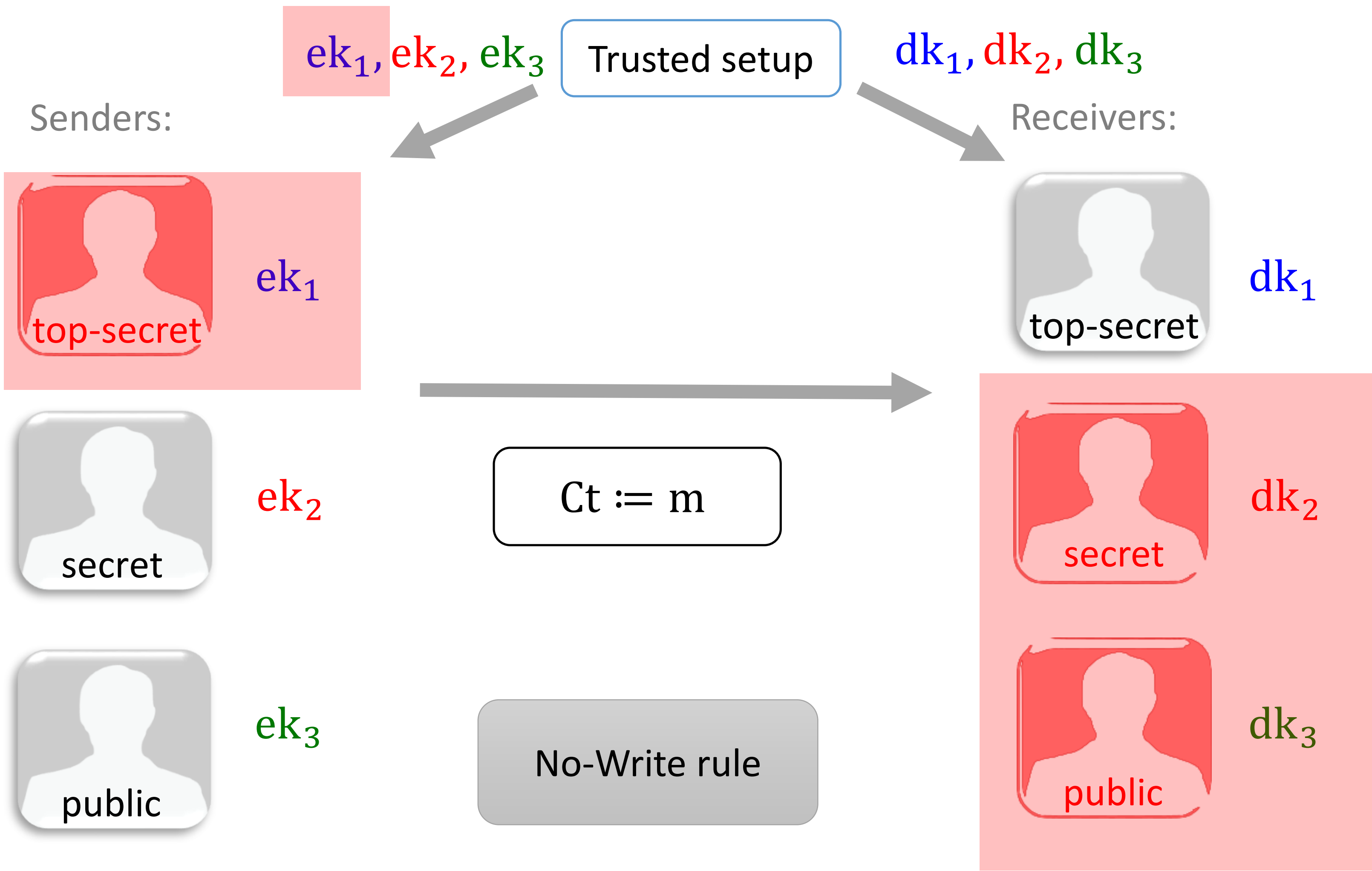
ACE [Damgård, Haagh, Orlandi 16]



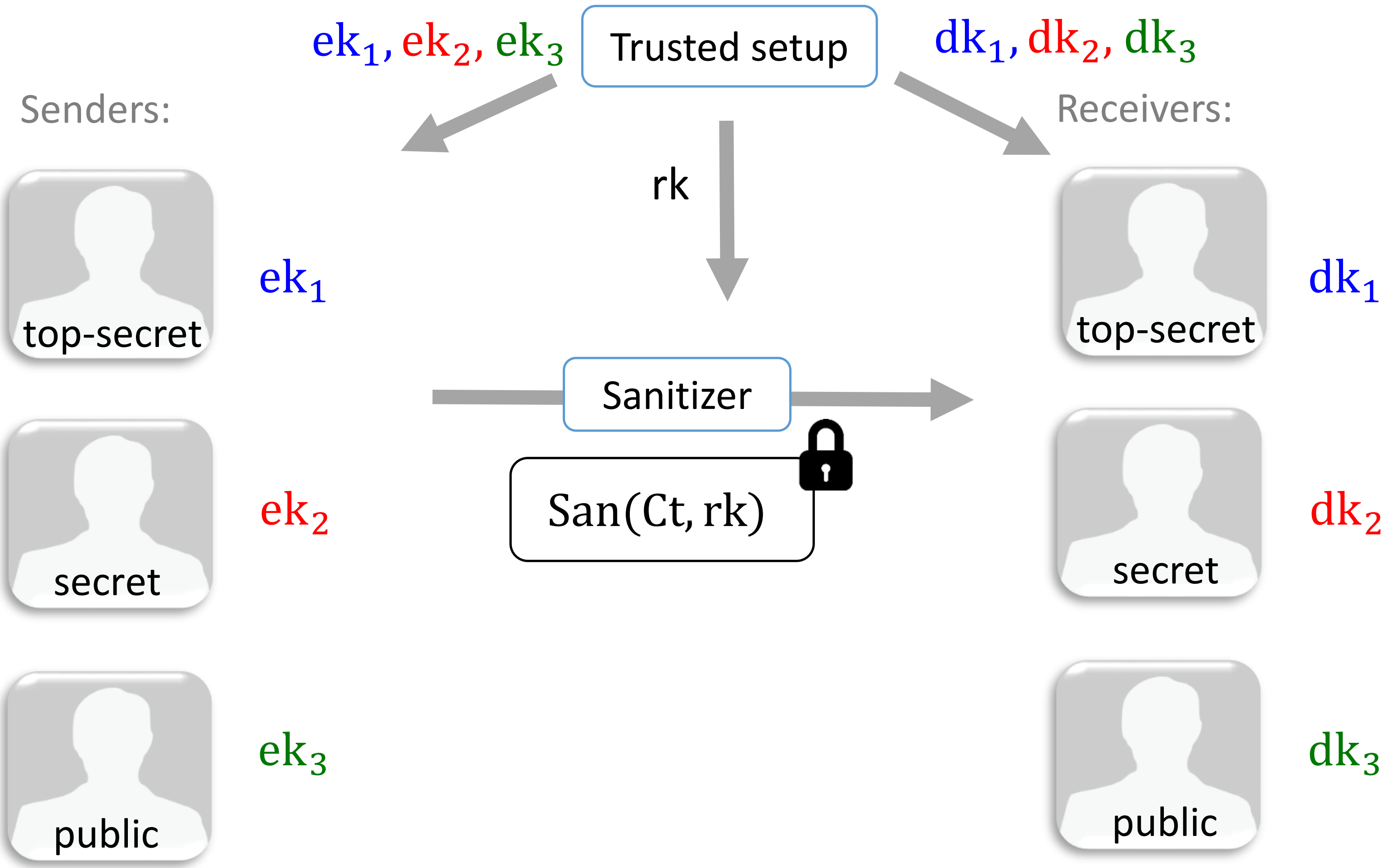
ACE [Damgård, Haagh, Orlandi 16]



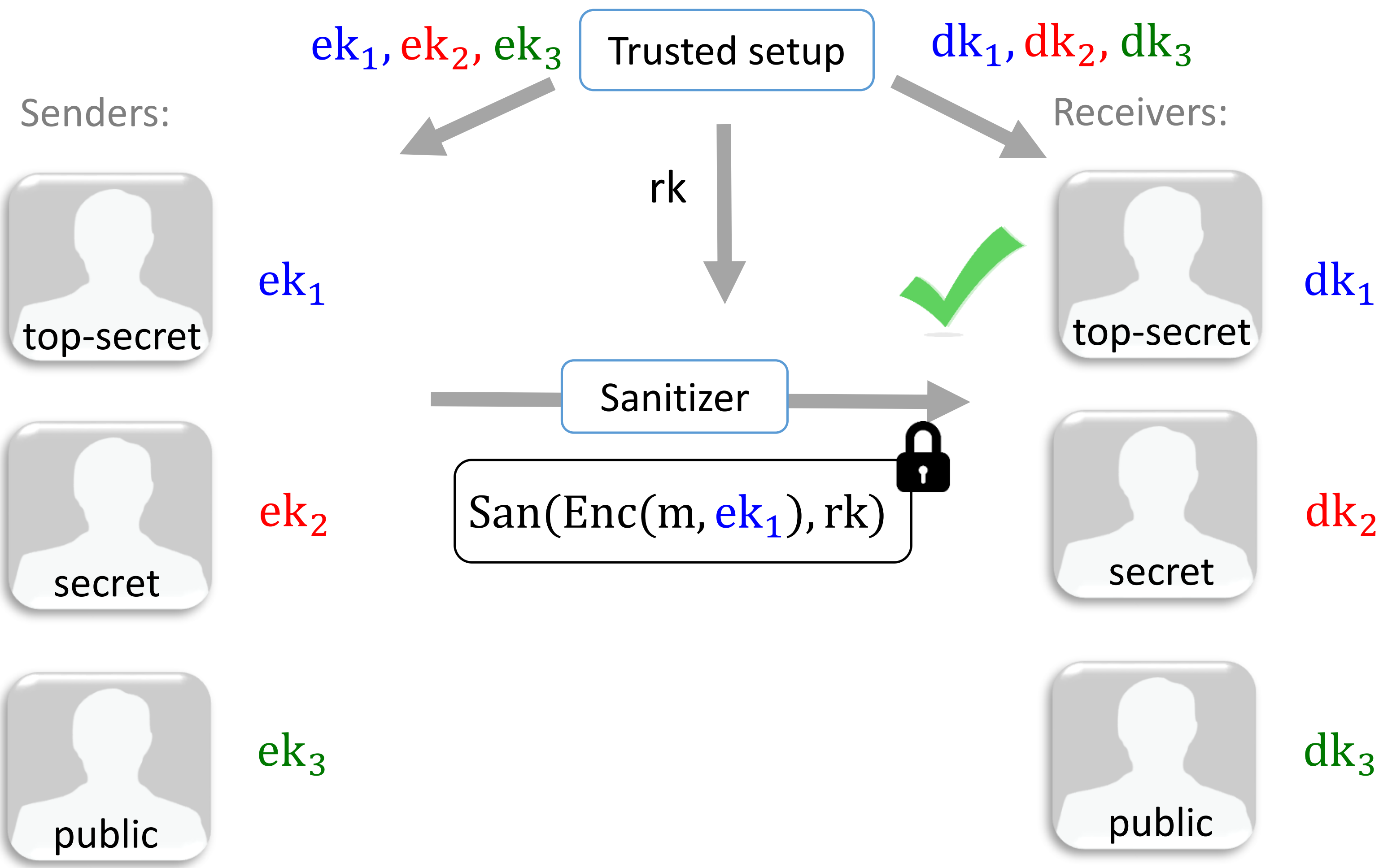
ACE [Damgård, Haagh, Orlandi 16]



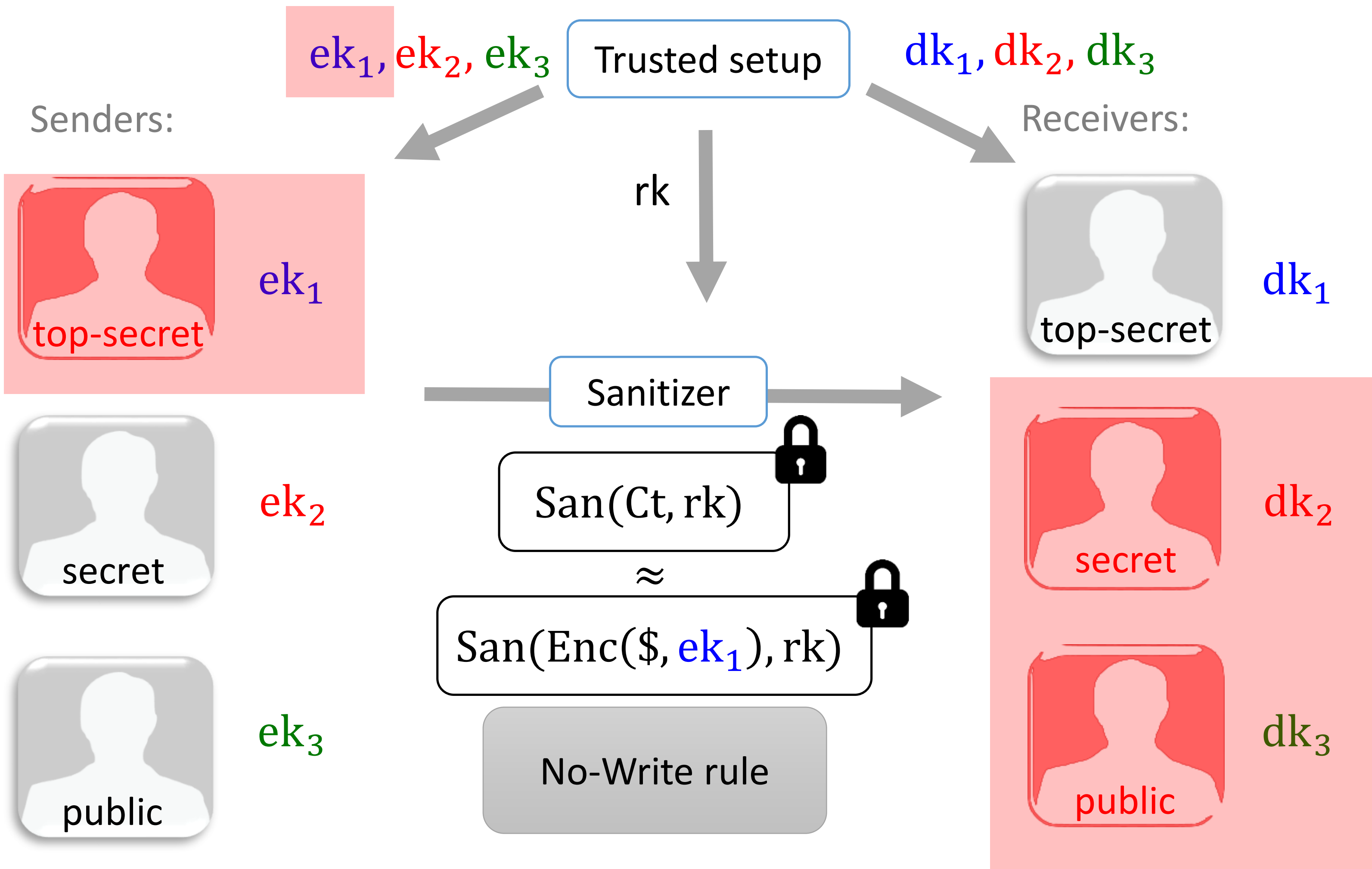
ACE [Damgård, Haagh, Orlandi 16]



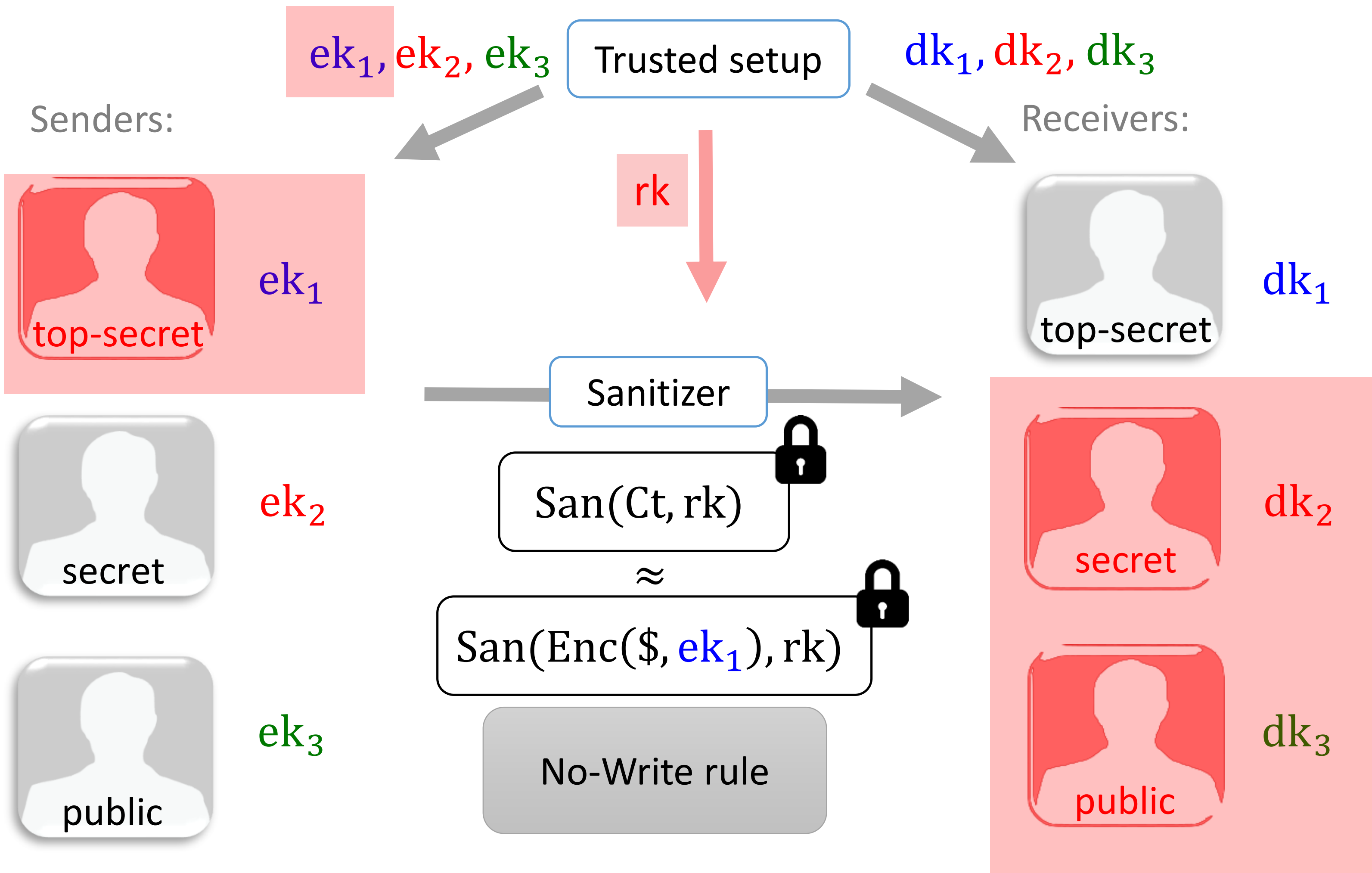
ACE [Damgård, Haagh, Orlandi 16]



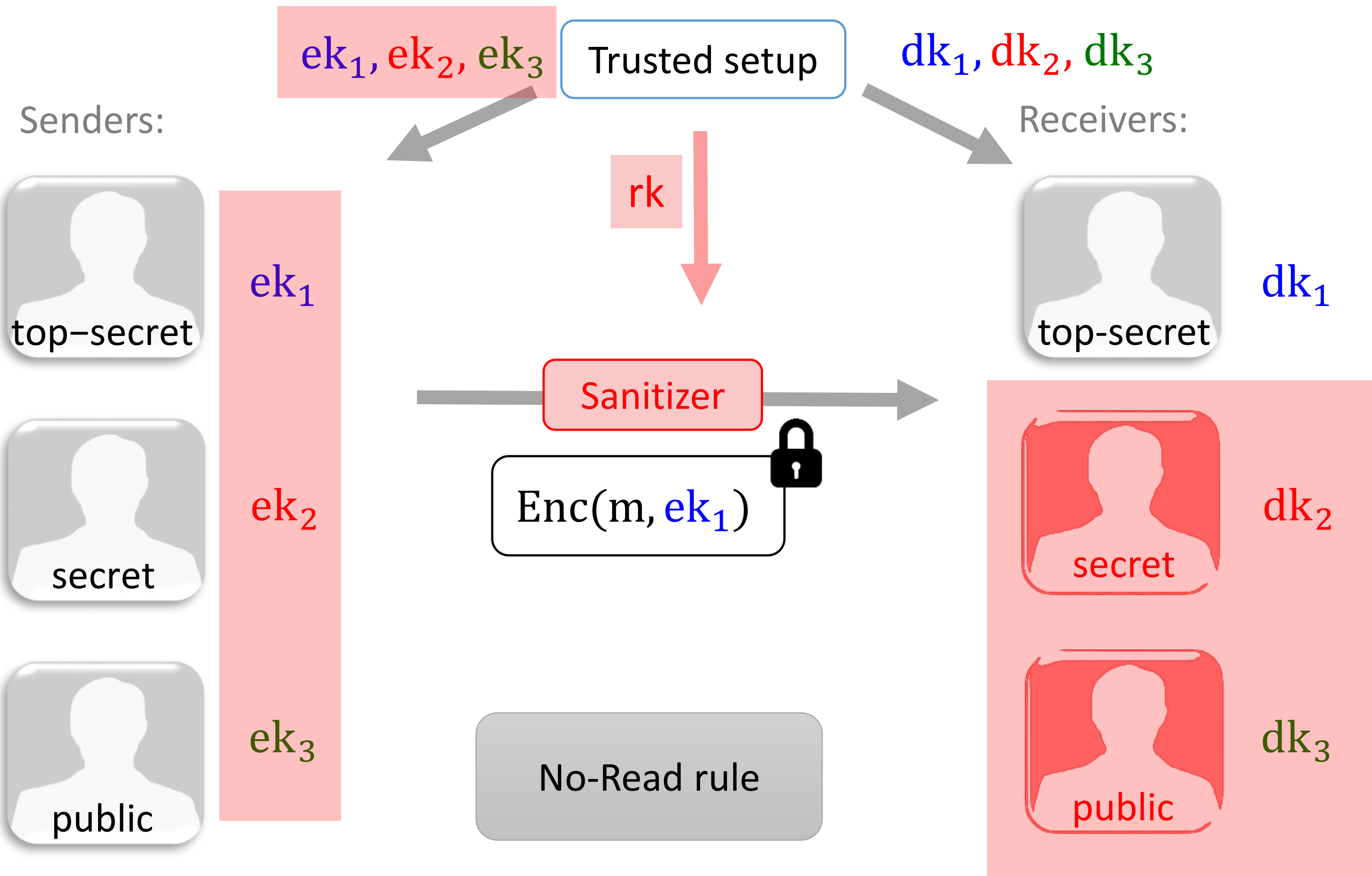
ACE [Damgård, Haagh, Orlandi 16]



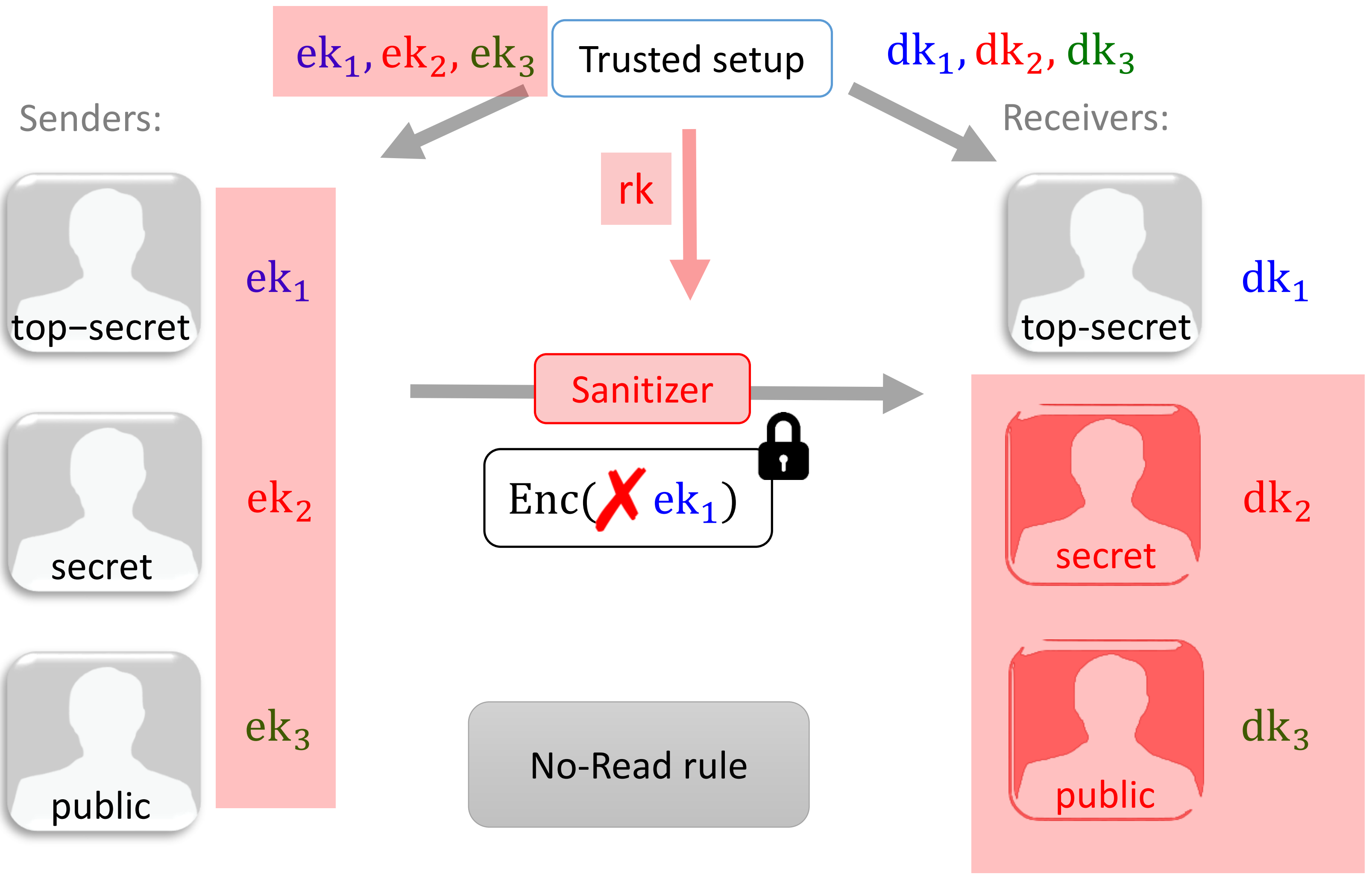
ACE [Damgård, Haagh, Orlandi 16]



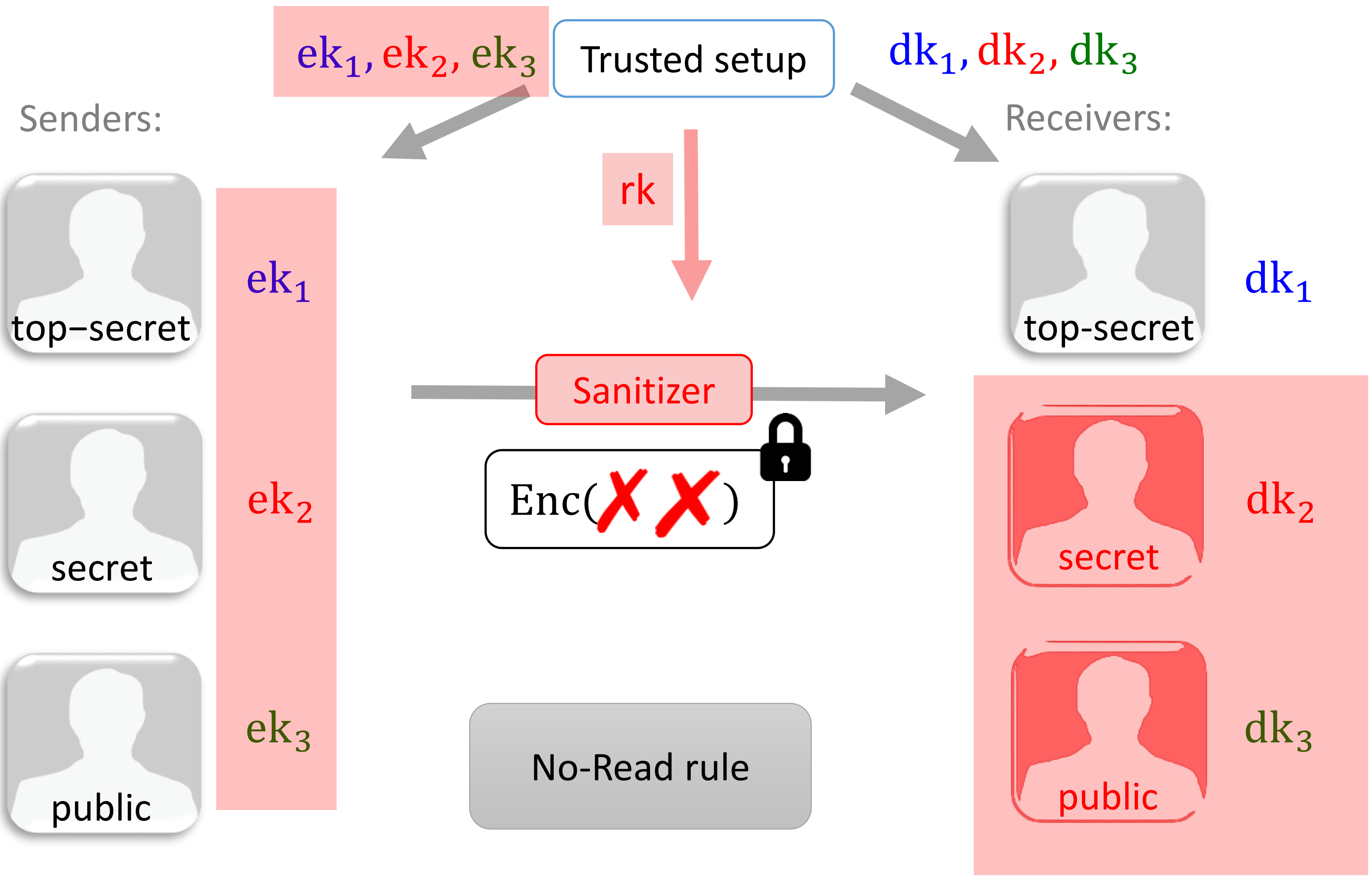
ACE [Damgård, Haagh, Orlandi 16]



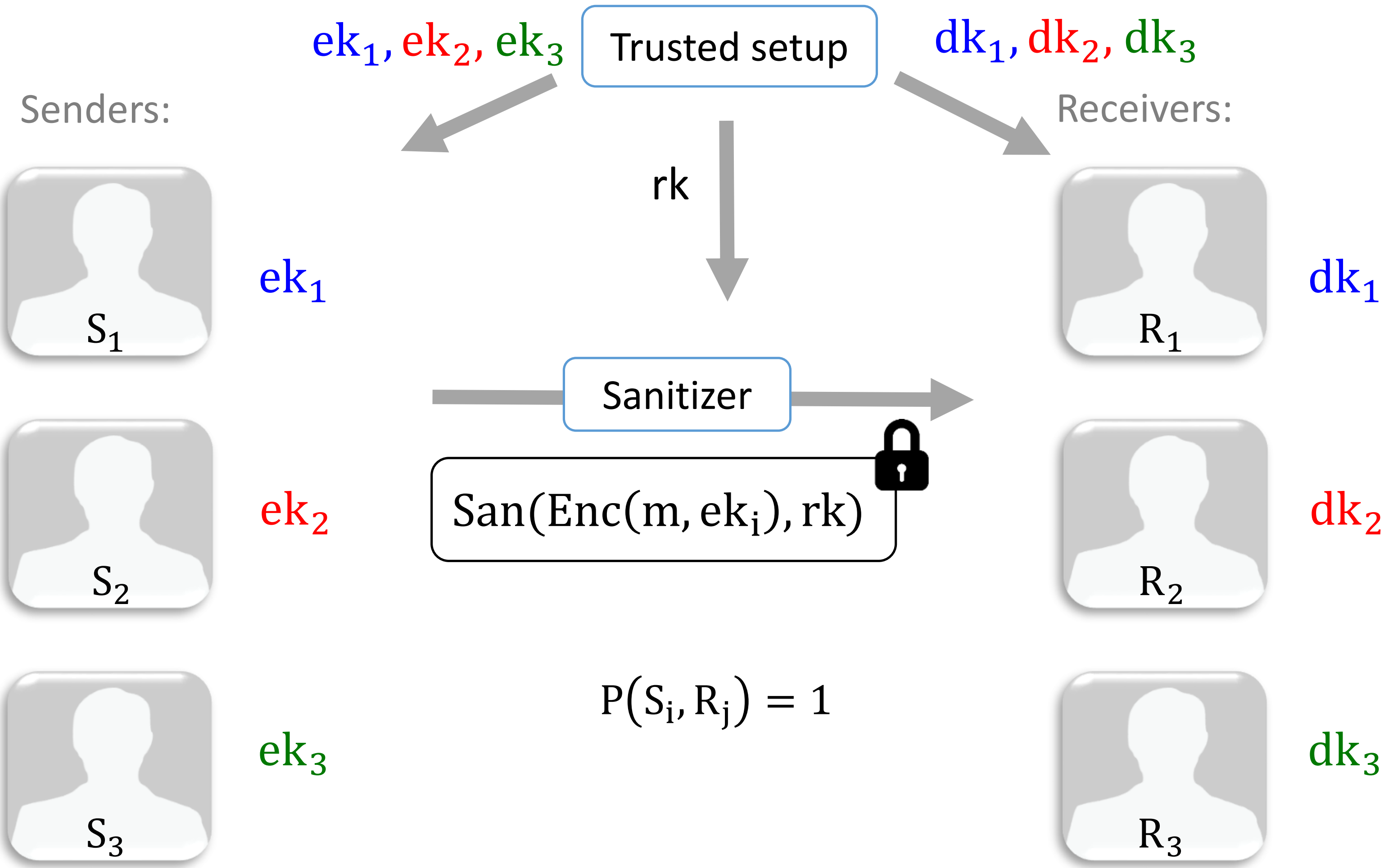
ACE [Damgård, Haagh, Orlandi 16]



ACE [Damgård, Haagh, Orlandi 16]



ACE [Damgård, Haagh, Orlandi 16]



Previous works

For predicates $\mathrm{P}: \{0,1\}^{\mathrm{n}} \times \{0,1\}^{\mathrm{n}} \rightarrow \{0,1\}$

Construction:	Predicate:	Ct size:	Assumption:	Practical:
[DHO 16]	any	$O(2^n)$	DDH or DCR	✗
[DHO 16]	any	poly(n)	iO	✗

Our work

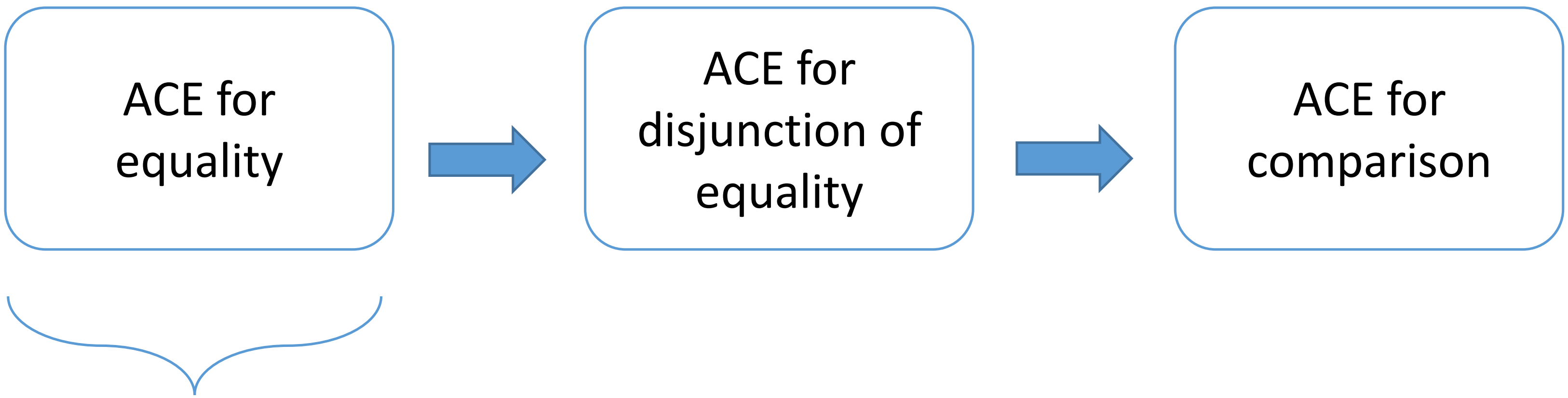
For predicates $\mathrm{P}: \{0,1\}^{\mathrm{n}} \times \{0,1\}^{\mathrm{n}} \rightarrow \{0,1\}$

Construction:	Predicate:	Ct size:	Assumption:	Practical:
[DHO 16]	any	$O(2^n)$	DDH or DCR	✗
[DHO 16]	any	poly(n)	iO	✗
Our work	$\mathrm{P_{eq}}, \mathrm{P_{comp}}$	$O(n)$	SXDH	✓

$$\mathrm{P_{eq}}(\mathrm{i}, \mathrm{j}) = 1 \text{ iff } \mathrm{i} = \mathrm{j}$$

$$\mathrm{P_{comp}}(\mathrm{i}, \mathrm{j}) = 1 \text{ iff } \mathrm{i} \geq \mathrm{j}$$

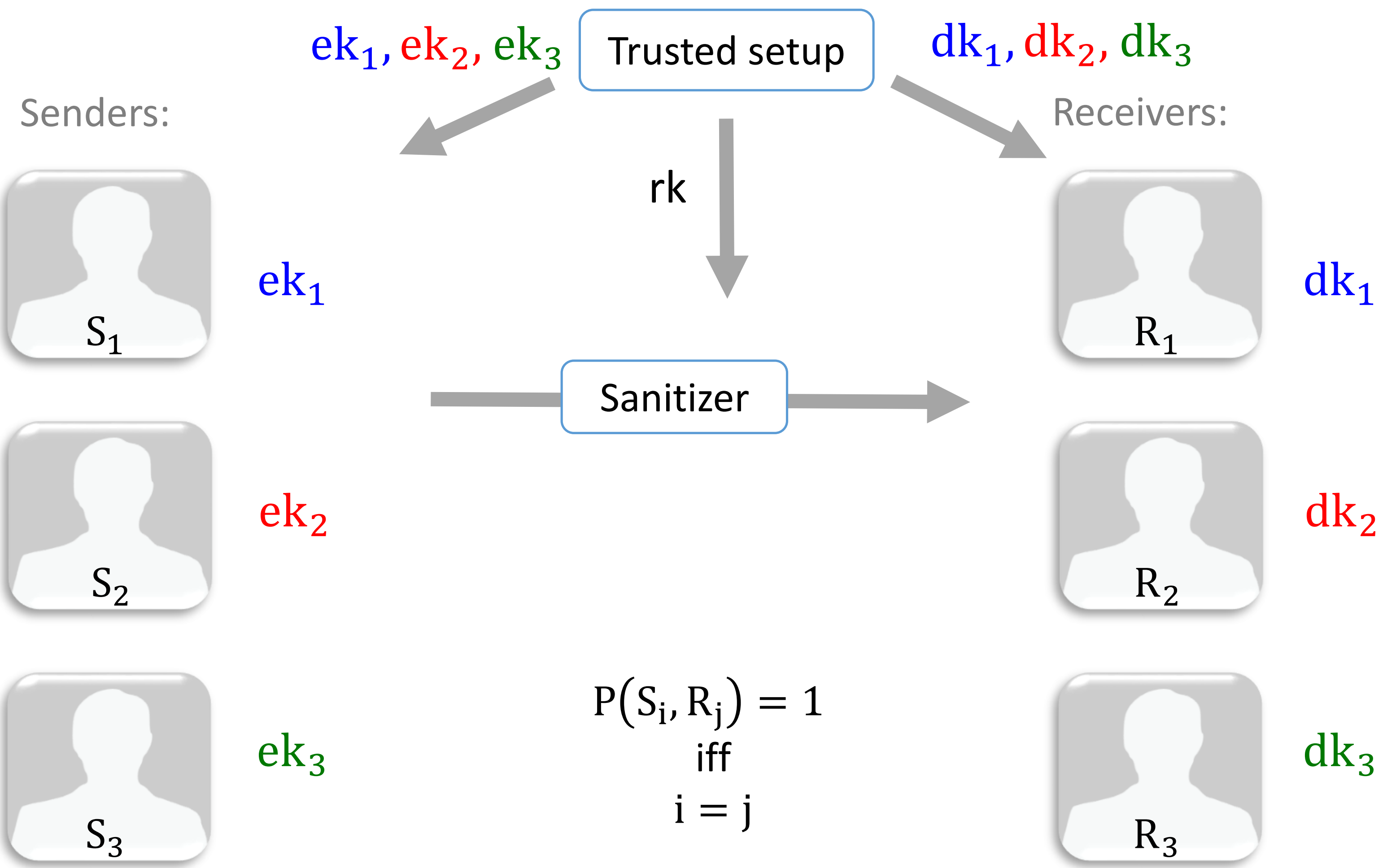
Outline



1. ACE for equality from [DHO 16]

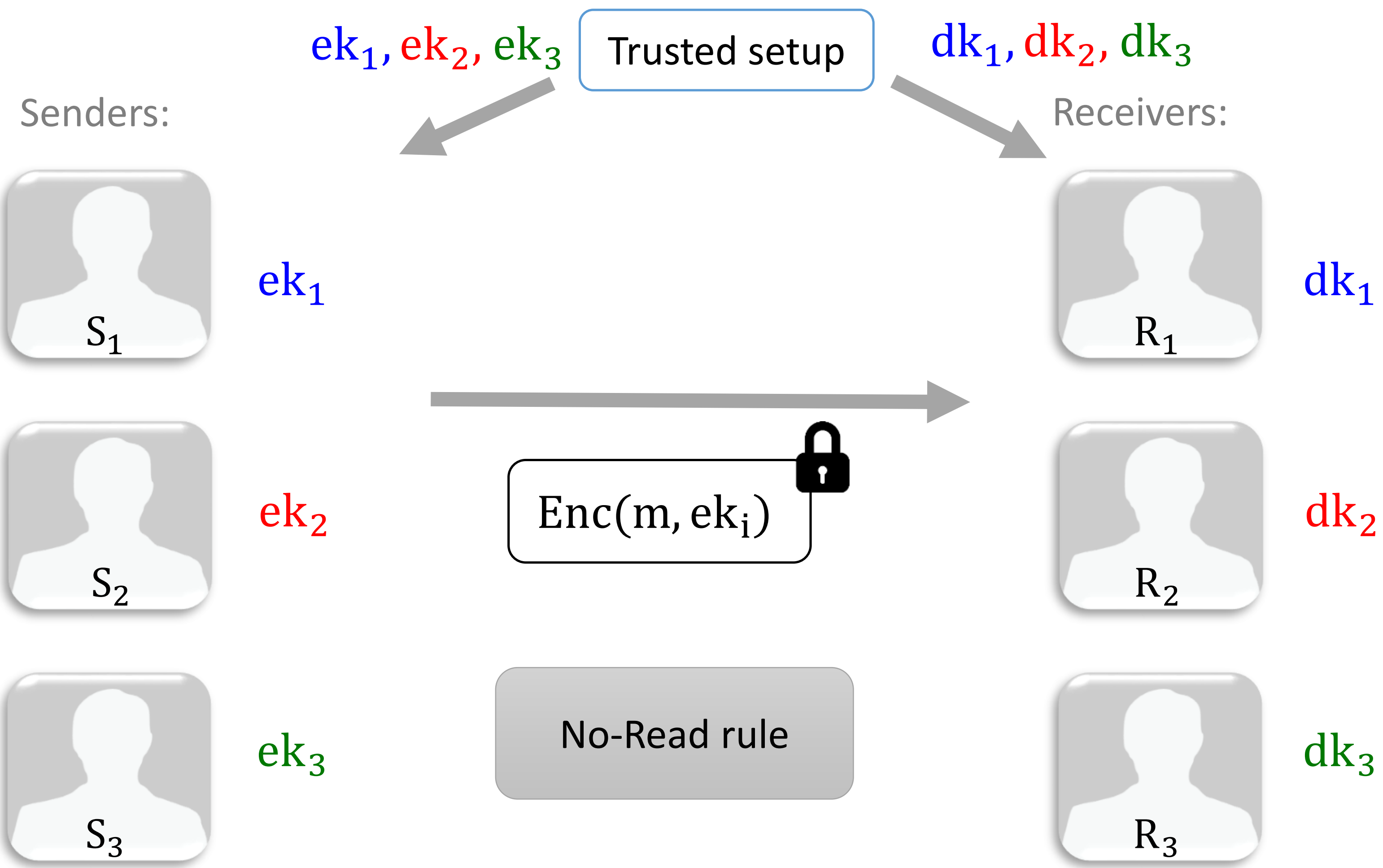
2. New ACE for equality

ACE for equality: DHO 16



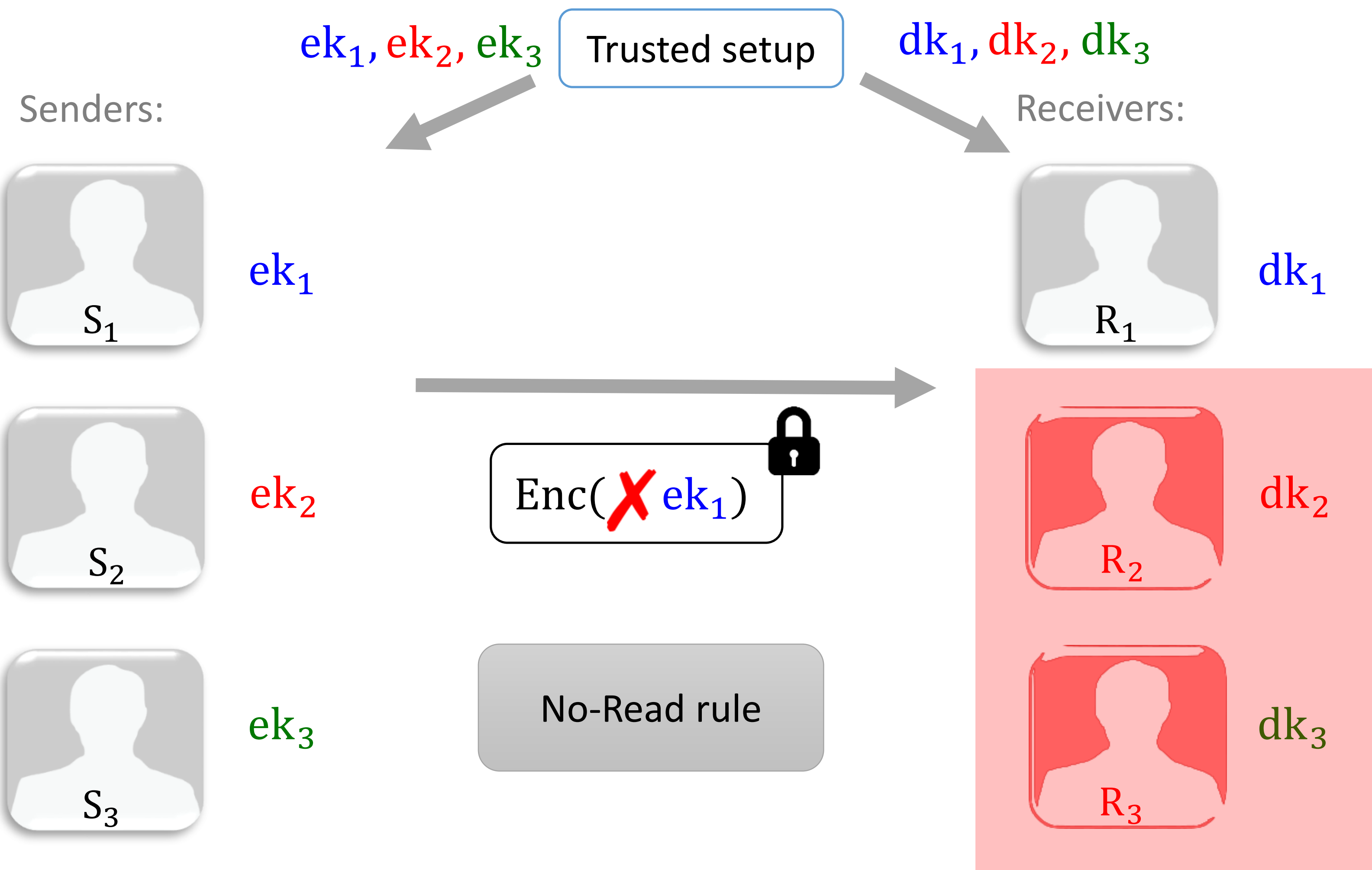
ACE for equality: DHO 16

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Private Key Encryption



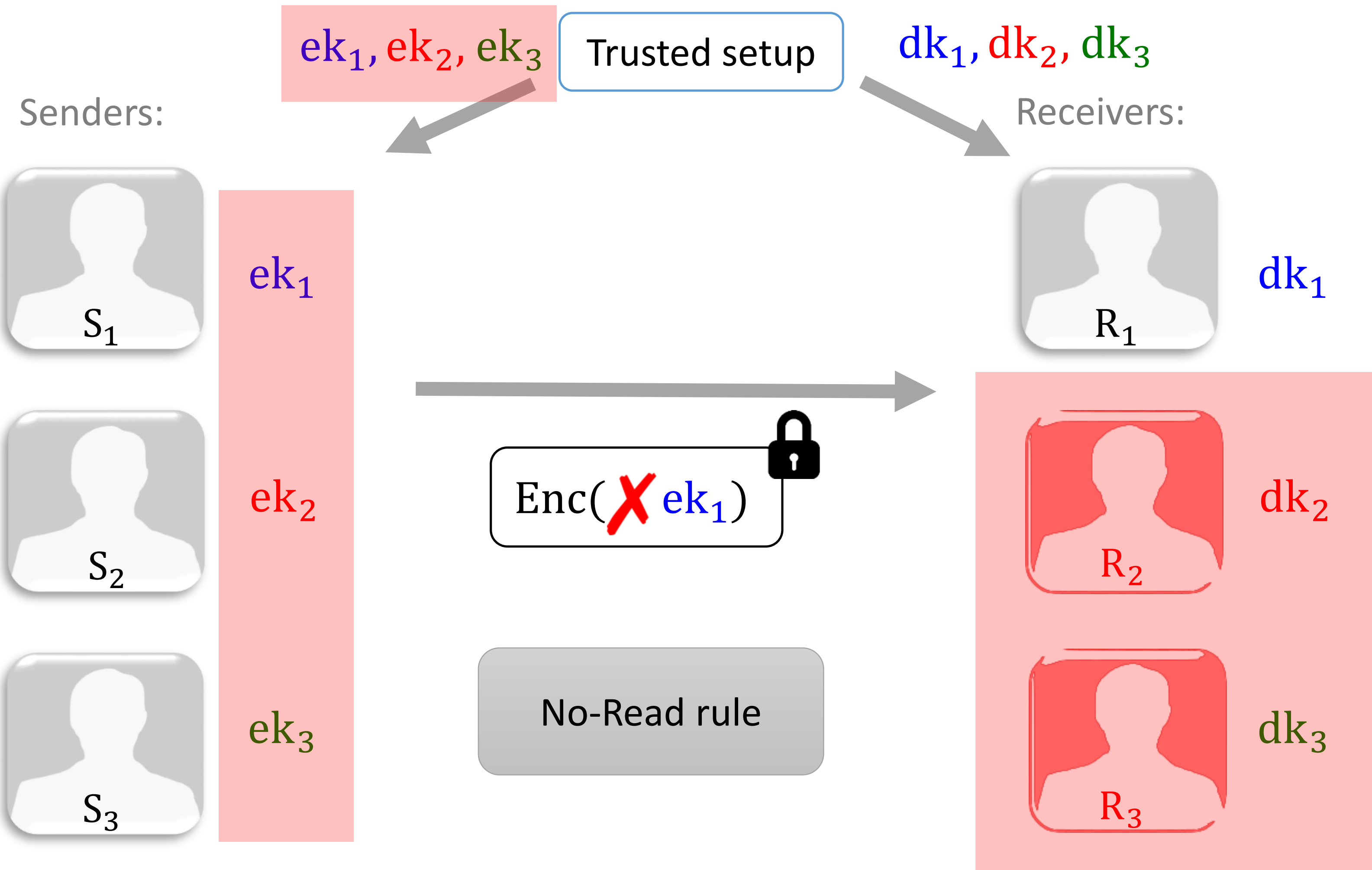
ACE for equality: DHO 16

$(ek_i, dk_i) \leftarrow \text{Private Key Encryption}$



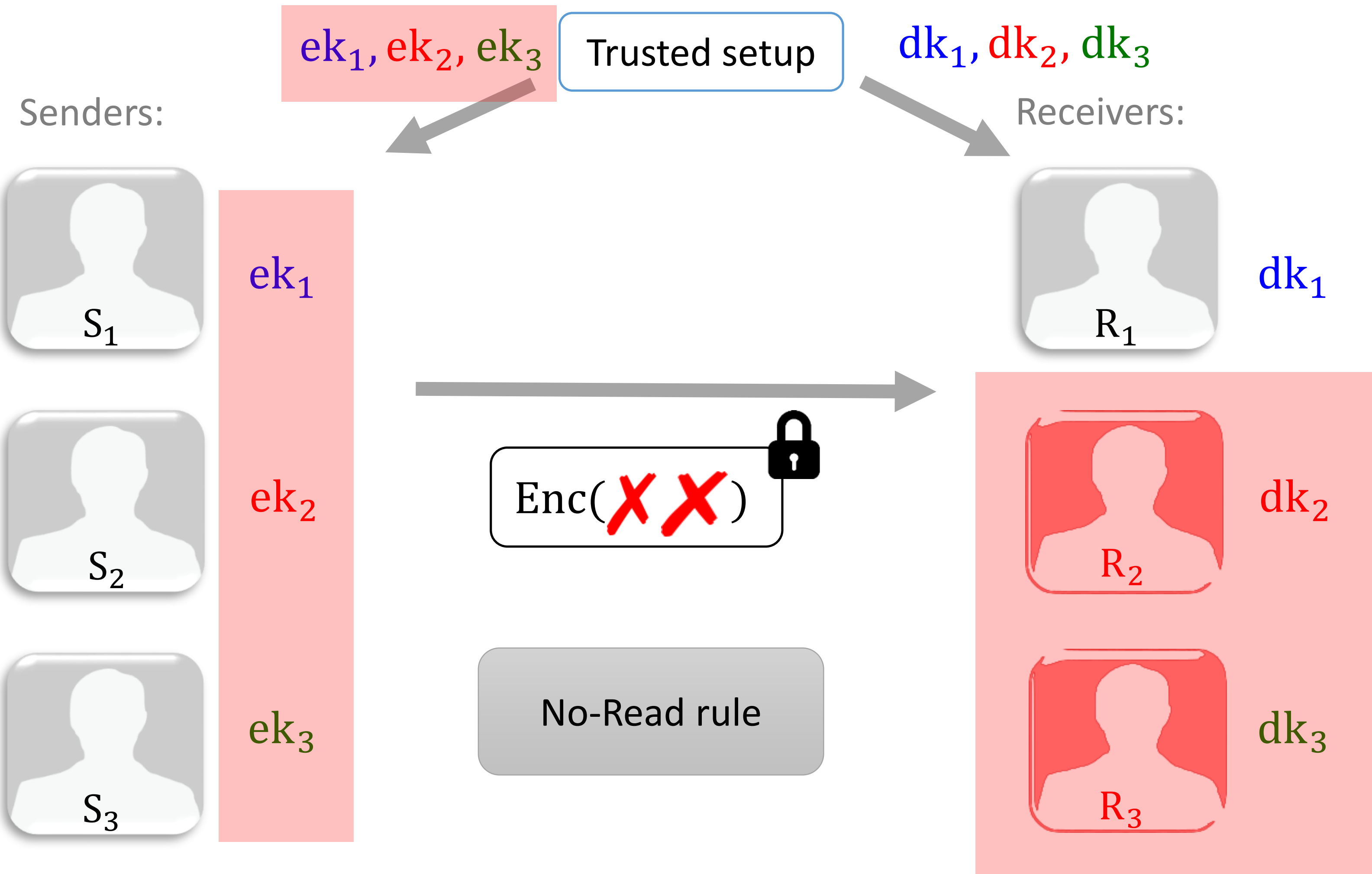
ACE for equality: DHO 16

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Public Key Encryption



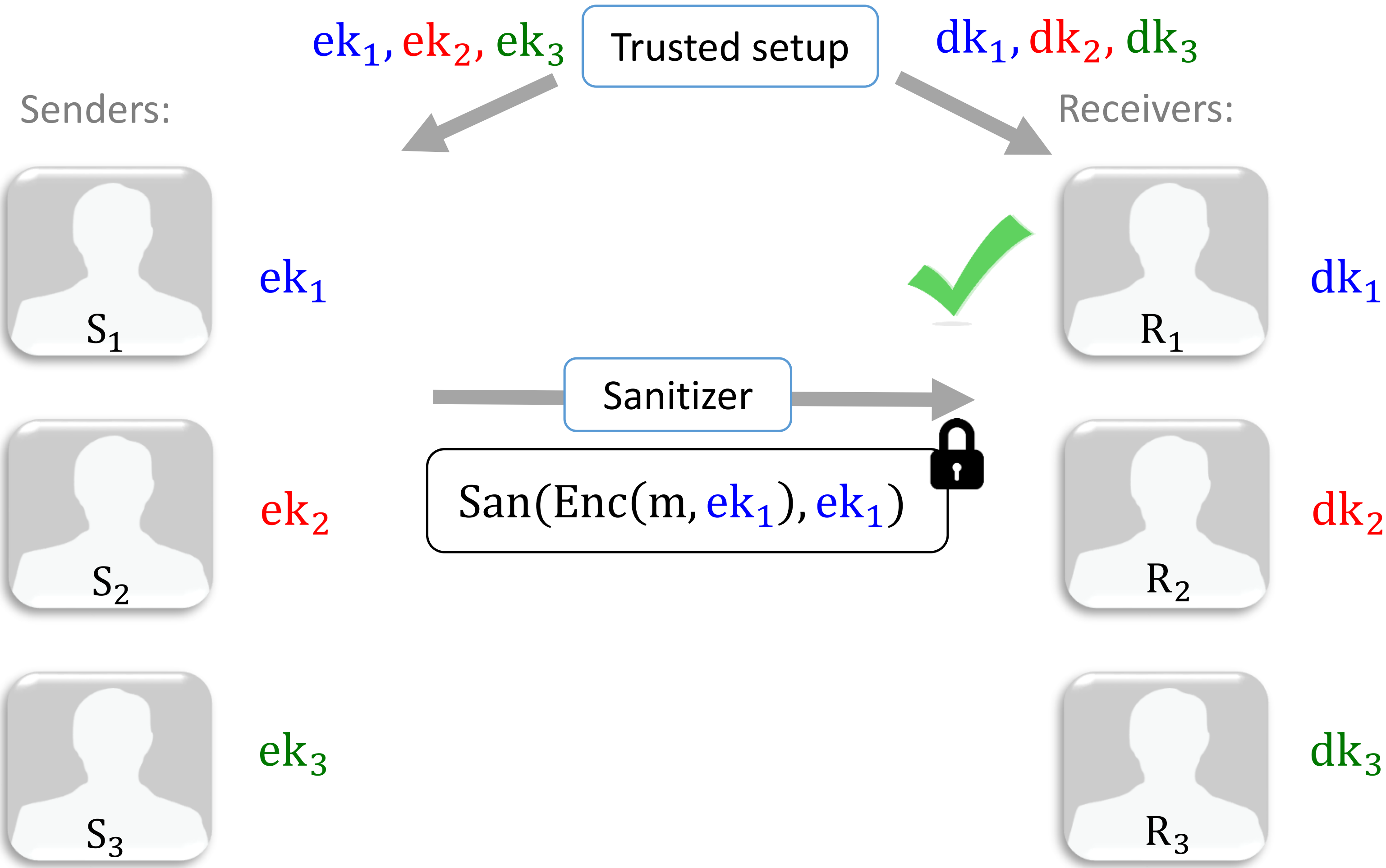
ACE for equality: DHO 16

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous Public Key Encryption



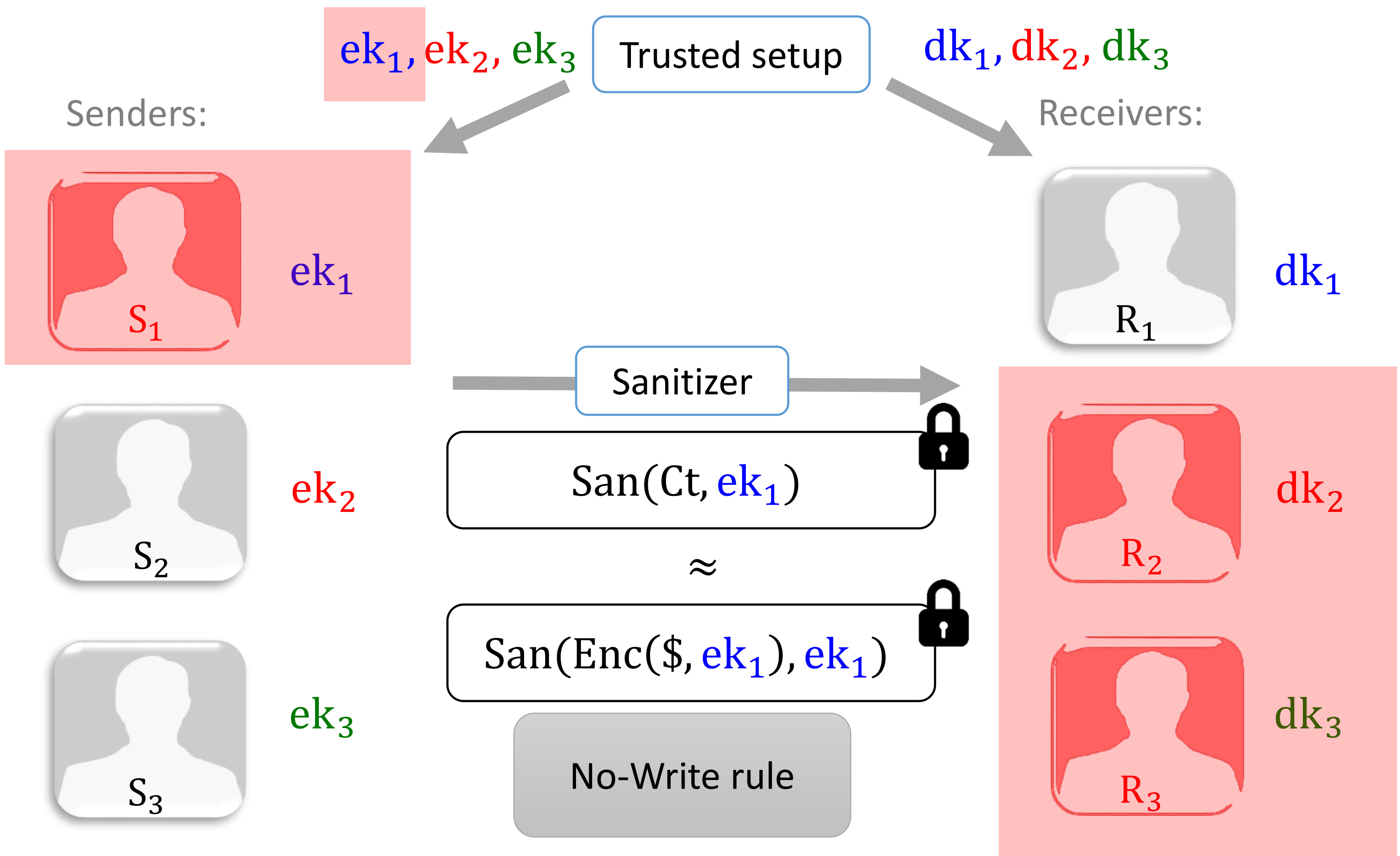
ACE for equality: DHO 16

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Sanitizable Anonymous Public Key Encryption



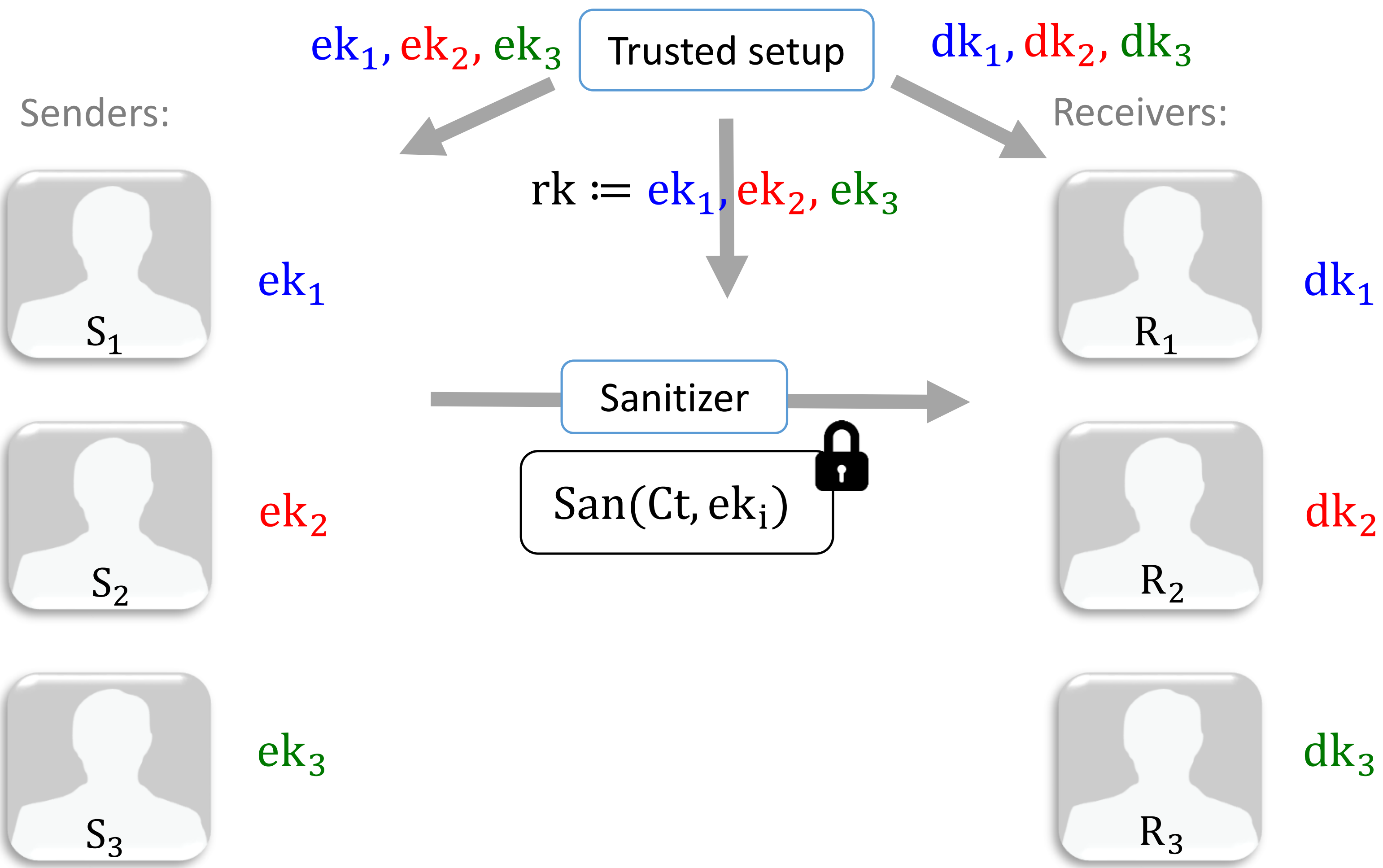
ACE for equality: DHO 16

$(\mathrm{pk_i}, \mathrm{dk_i}) \leftarrow$ Sanitizable Anonymous Public Key Encryption

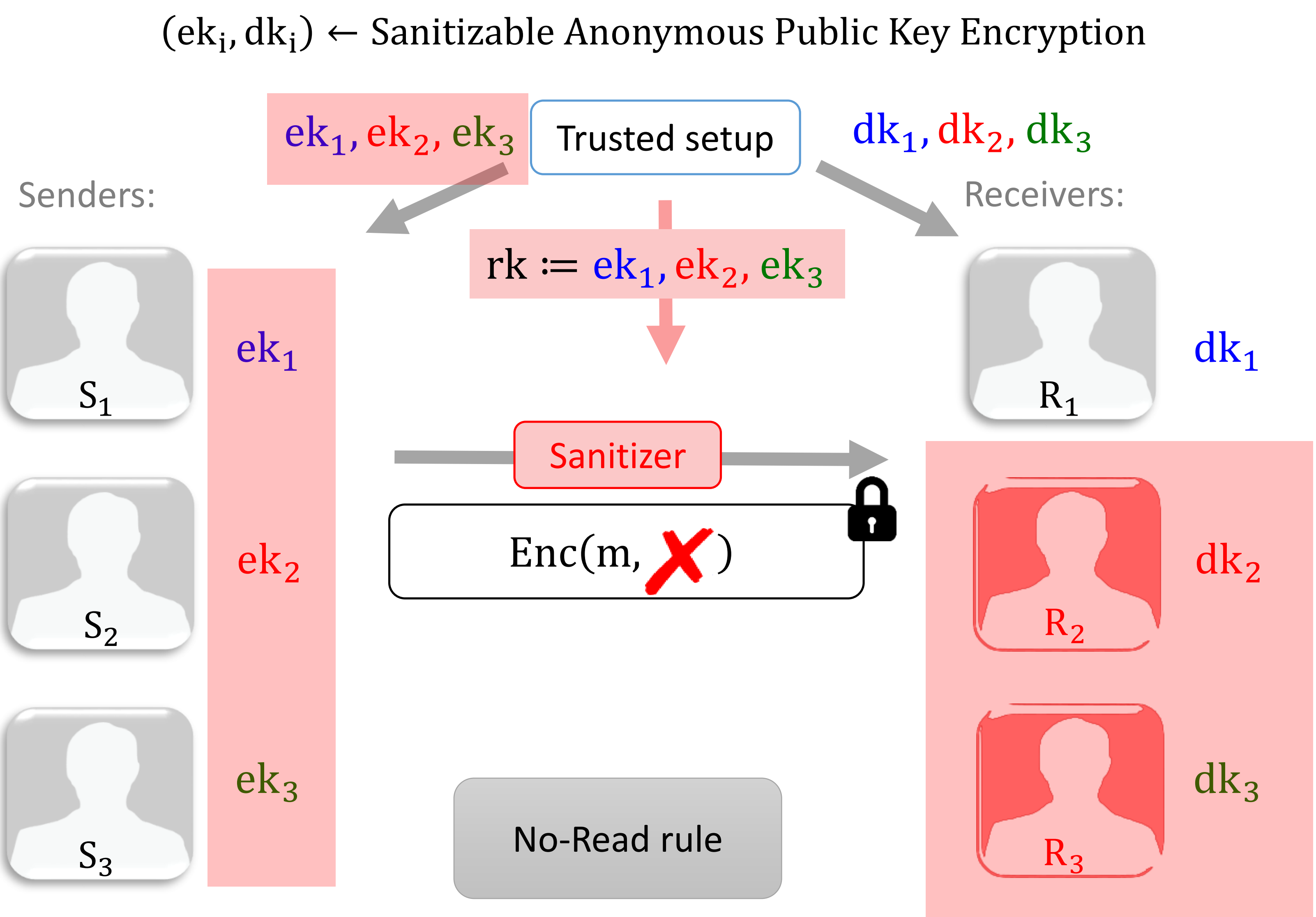


ACE for equality: DHO 16

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Sanitizable Anonymous Public Key Encryption

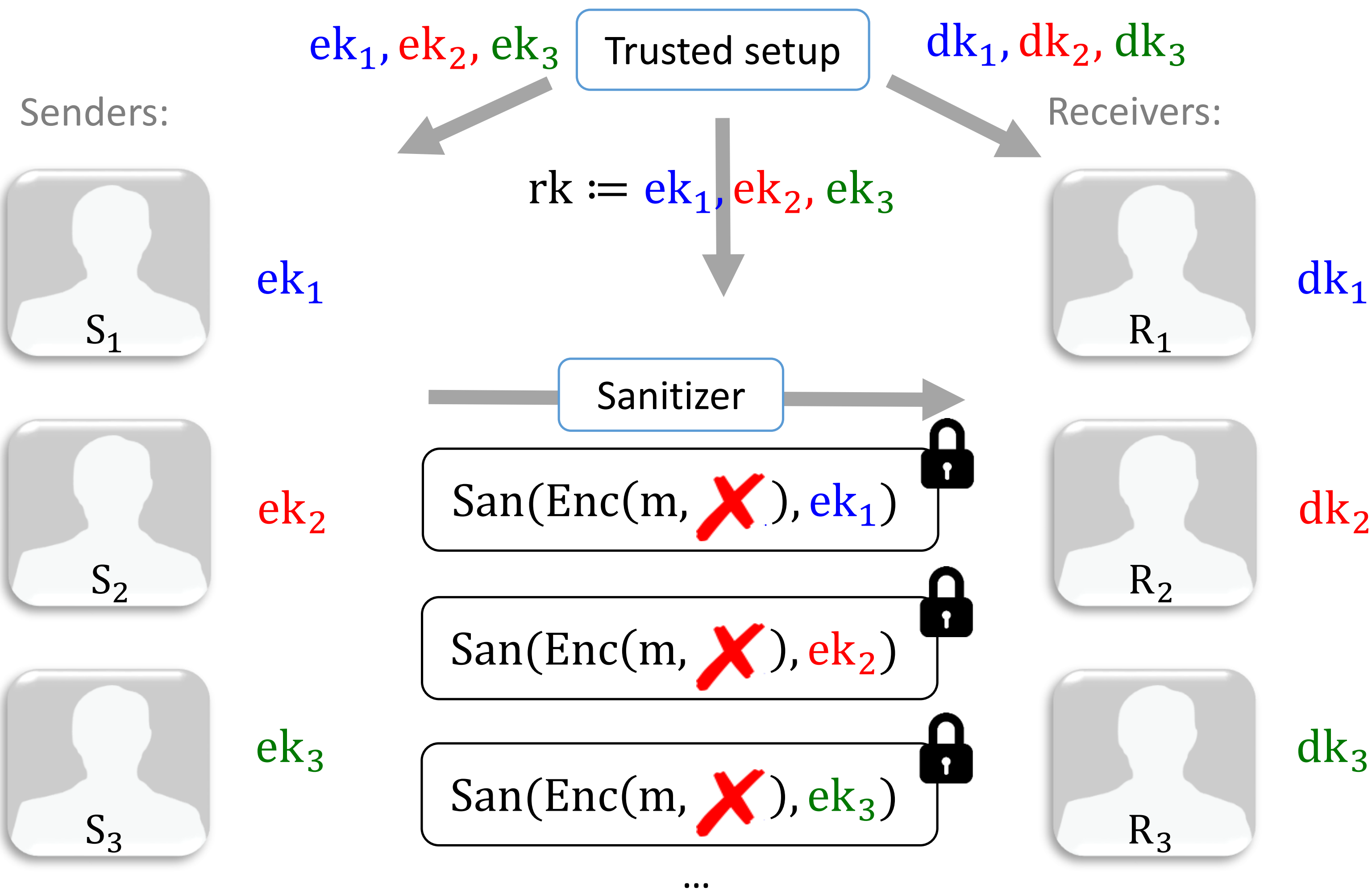


ACE for equality: DHO 16



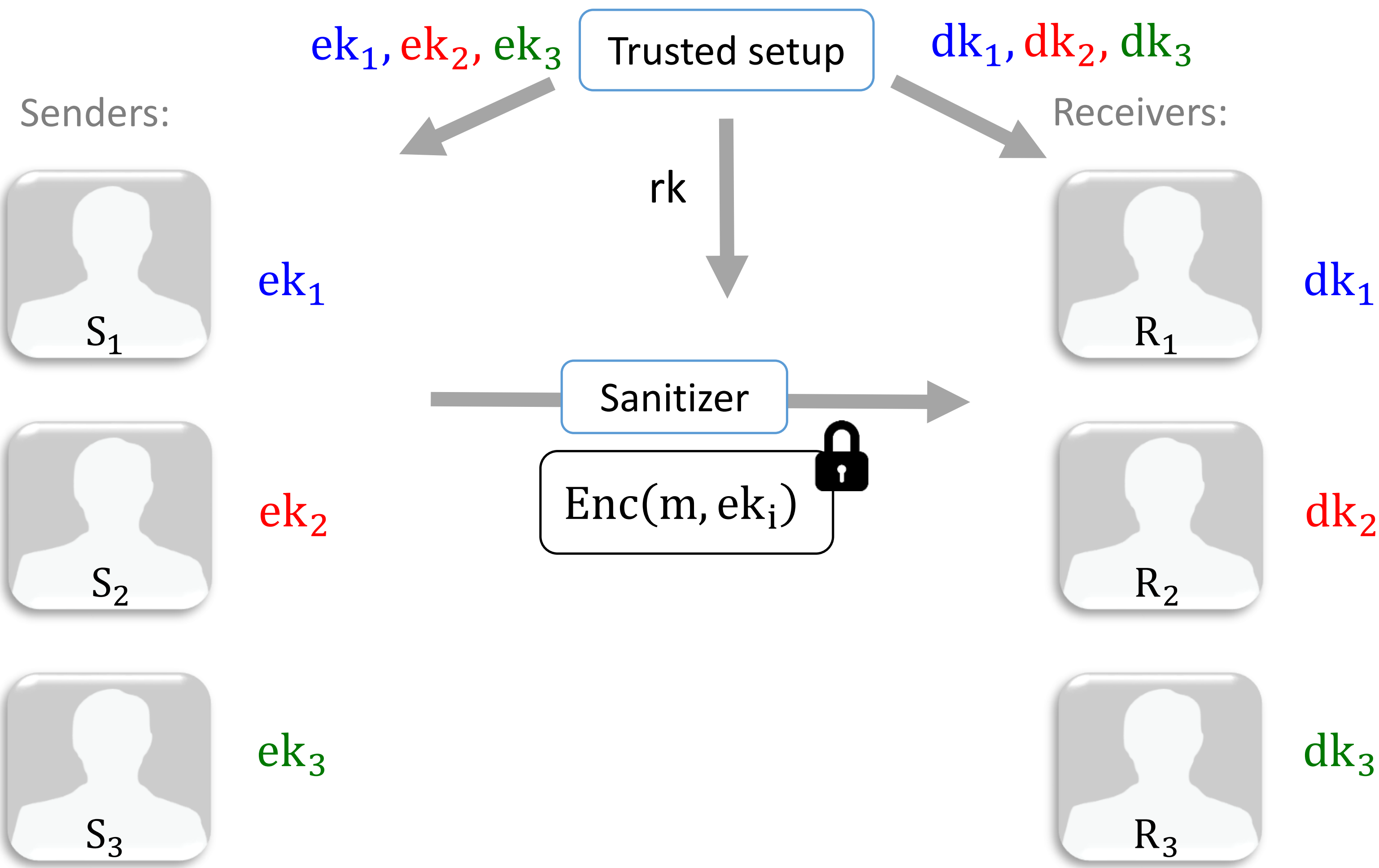
ACE for equality: DHO 16

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Sanitizable Anonymous Public Key Encryption



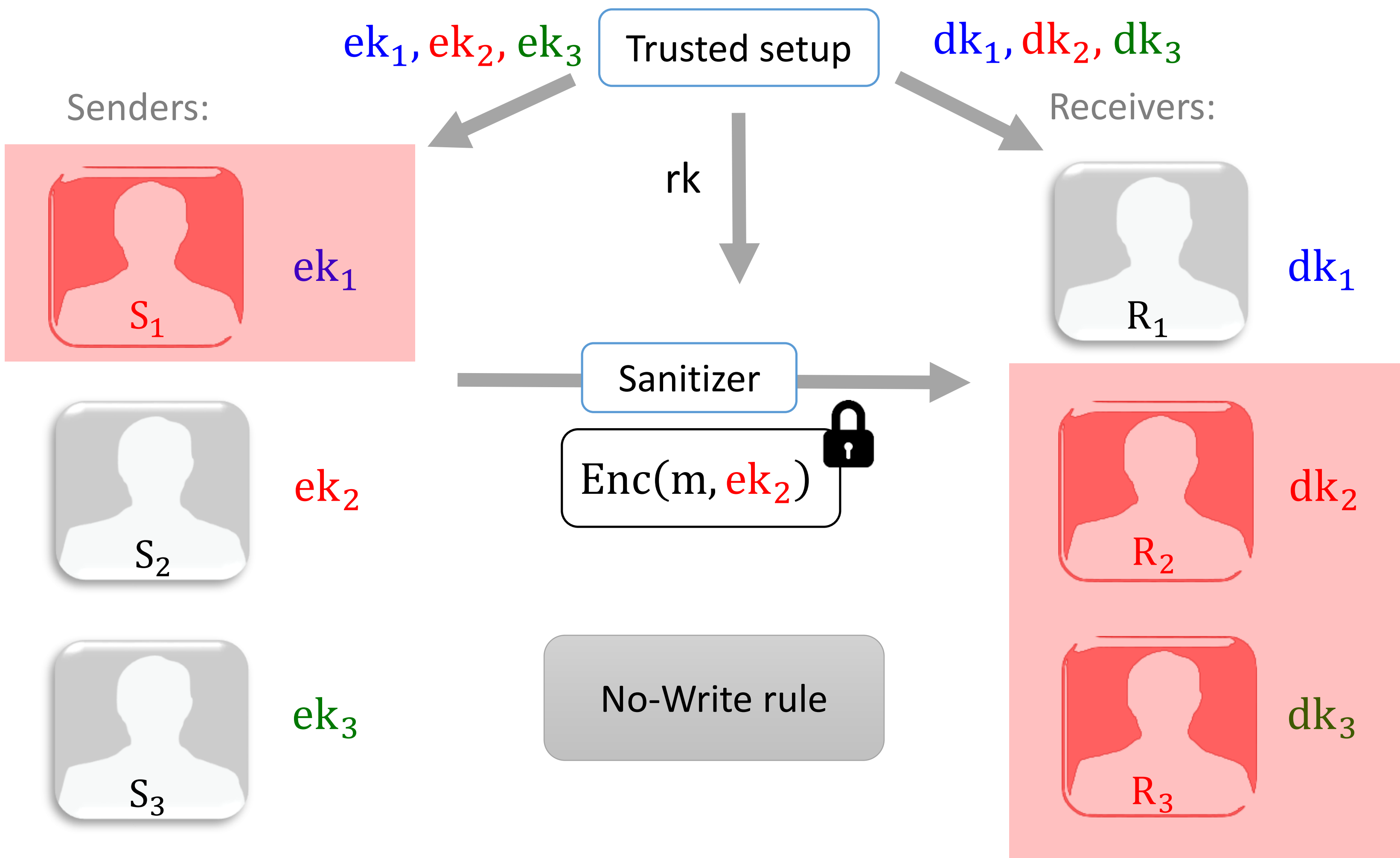
New ACE for equality

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous PKE



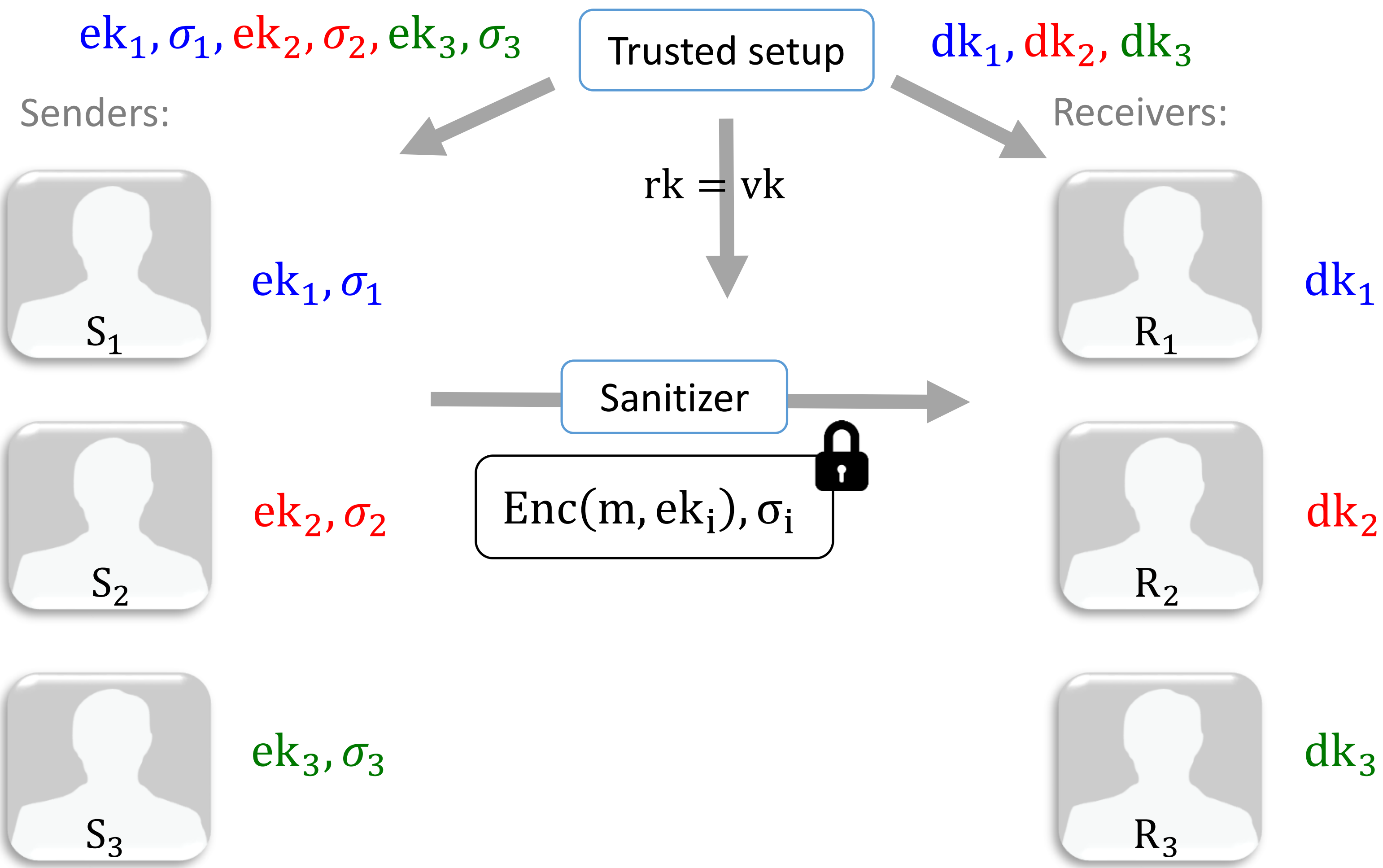
New ACE for equality

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous PKE



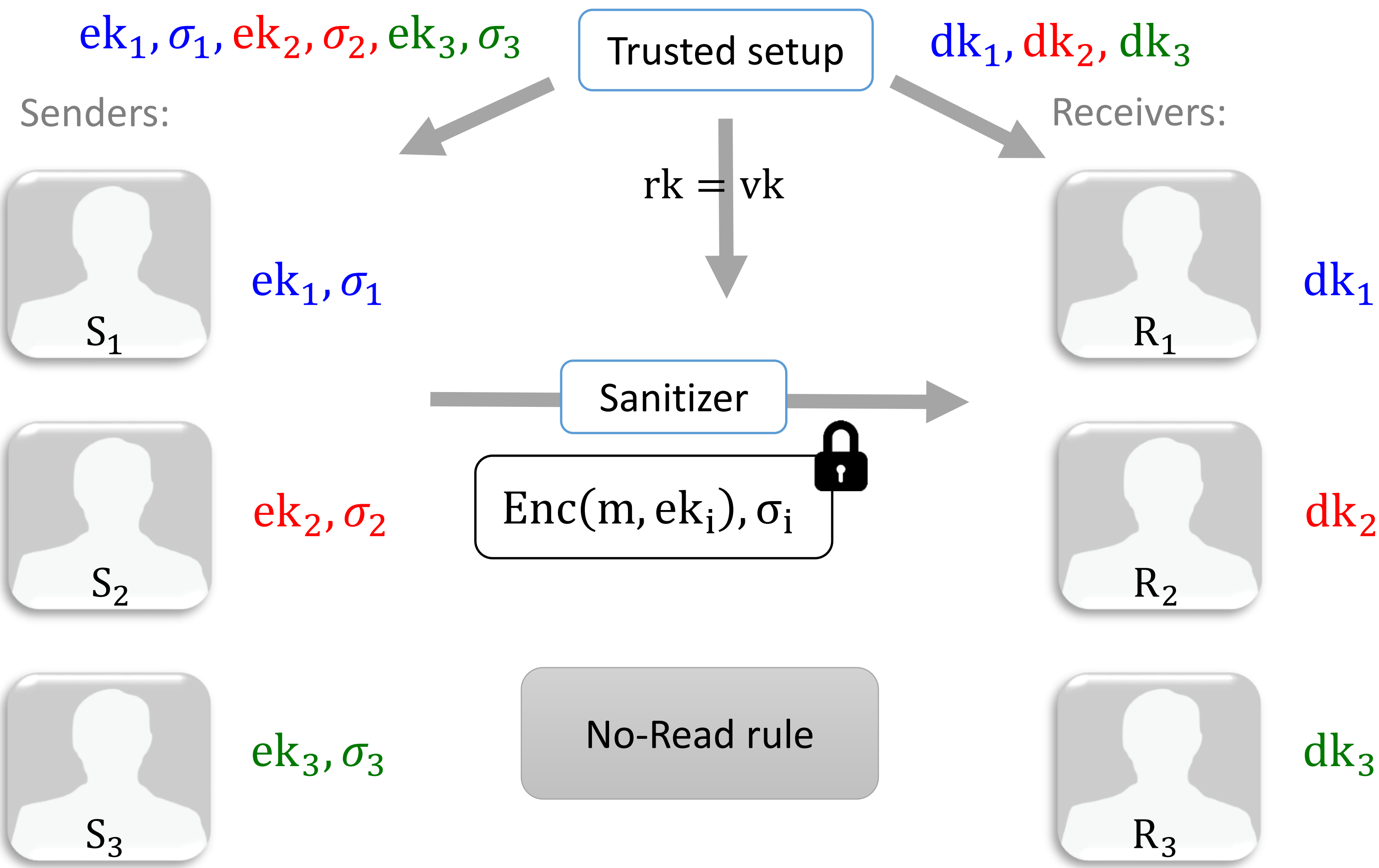
New ACE for equality

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous PKE, $\sigma_i = \mathrm{Sign}(\mathrm{ek_i})$



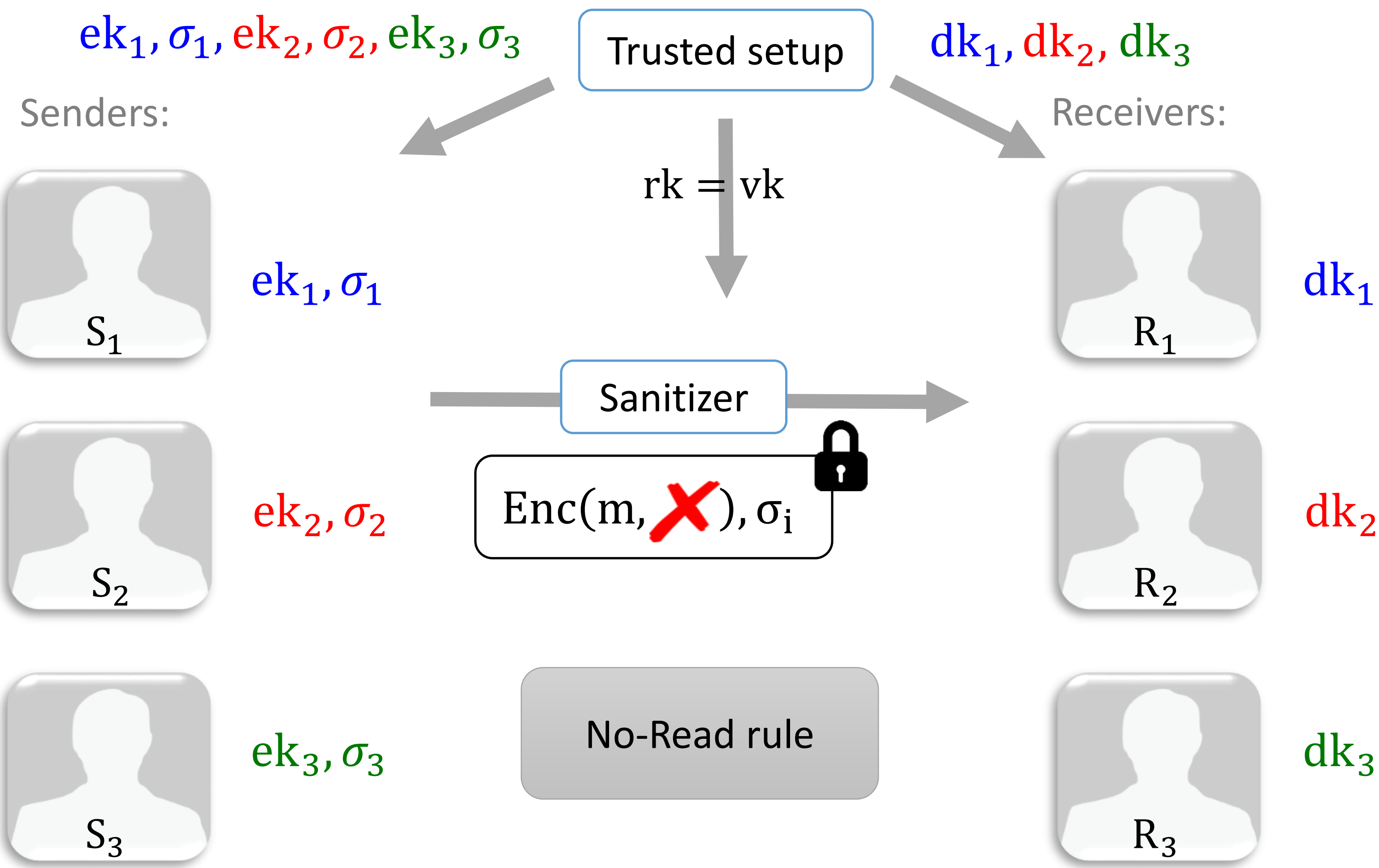
New ACE for equality

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous PKE, $\sigma_i = \mathrm{Sign}(ek_i)$



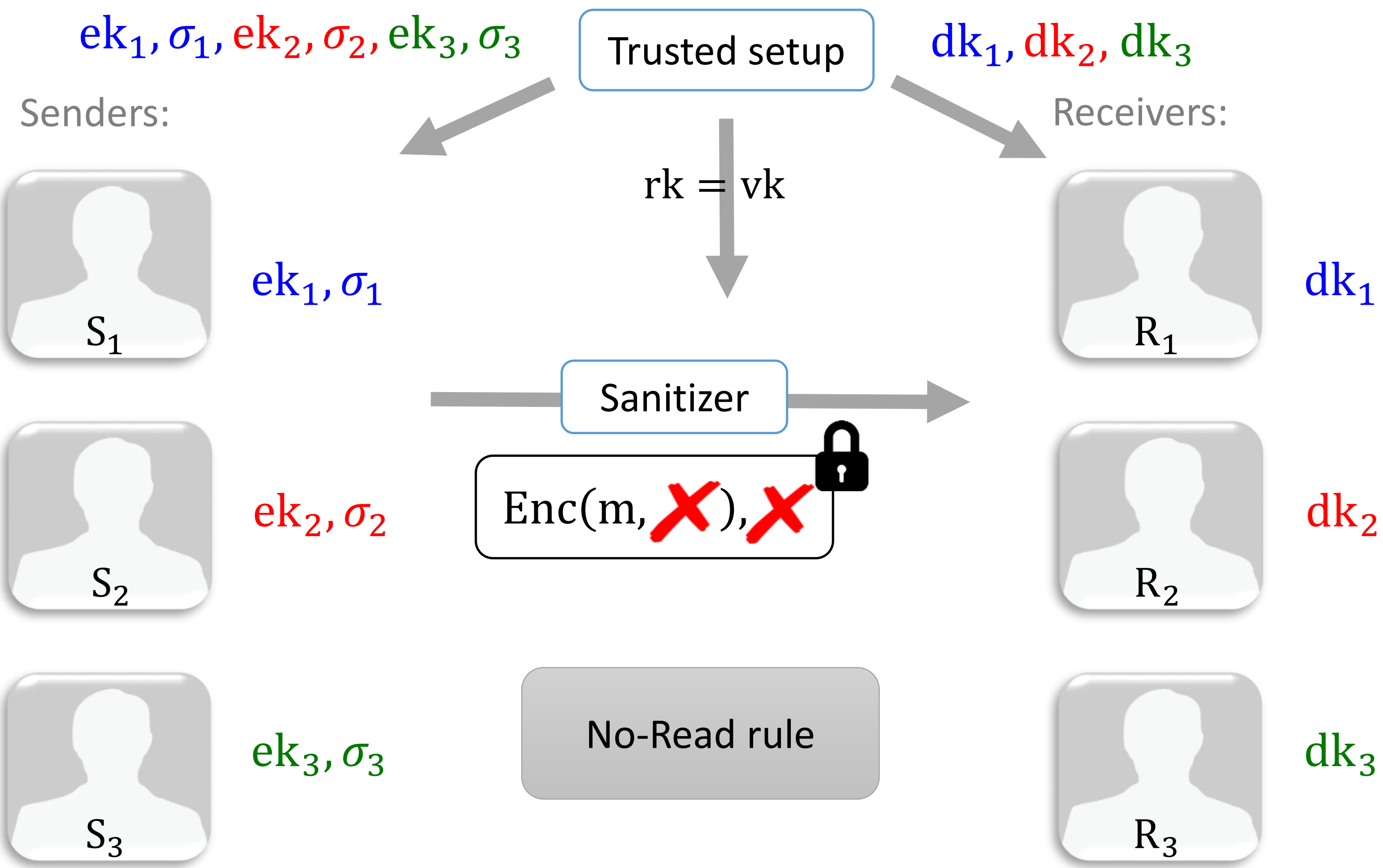
New ACE for equality

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous PKE, $\sigma_\mathrm{i} = \mathrm{Sign}(e\mathrm{k_i})$



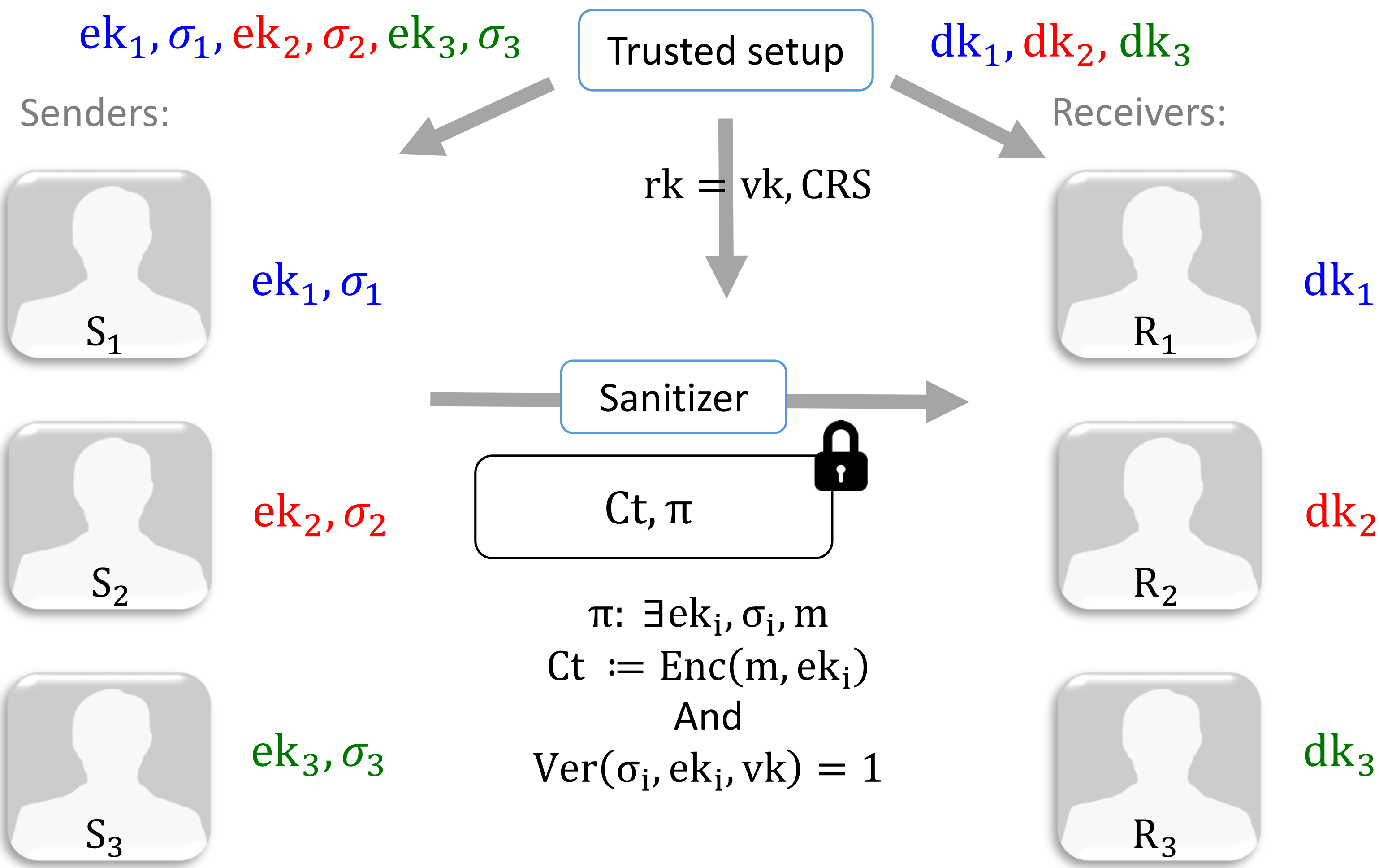
New ACE for equality

$$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow \text{Anonymous PKE}, \quad \sigma_\mathrm{i} = \mathrm{Sign}(e\mathrm{k_i})$$



New ACE for equality

$(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ Anonymous PKE, $\sigma_i = \mathrm{Sign}(\mathrm{ek_i}), \mathrm{CRS} \leftarrow \mathrm{NIZK}$



Concrete ACE for equality

- $(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ (Rerandomizable)Anonymous PKE: El Gamal
- NIZK: Groth Sahai [GS 12]
- $\sigma_\mathrm{i} = \mathrm{Sign}(\mathrm{ek_i})$: Structure preserving signature

SPS:	$\mathrm{ek_i}$:	ct:	Assumption:
[KPW 12]	$7\mathbb{G}_1 + 1\mathbb{G}_2$	$34\mathbb{G}_1 + 16\mathbb{G}_2$	SXDH
[AGHO 11]	$3\mathbb{G}_1 + 1\mathbb{G}_2$	$20\mathbb{G}_1 + 14\mathbb{G}_2$	GGM

Concrete ACE for equality

- $(\mathrm{ek_i}, \mathrm{dk_i}) \leftarrow$ (Rerandomizable)Anonymous PKE: El Gamal
- NIZK: Groth Sahai [GS 12]
- $\sigma_\mathrm{i} = \mathrm{Sign}(\mathrm{ek_i})$: Structure preserving signature

SPS:	$\mathrm{ek_i}$:	ct:	Assumption:
[KPW 12]	$7\mathbb{G}_1 + 1\mathbb{G}_2$	$34\mathbb{G}_1 + 16\mathbb{G}_2$	SXDH
[AGHO 11]	$3\mathbb{G}_1 + 1\mathbb{G}_2$	$20\mathbb{G}_1 + 14\mathbb{G}_2$	GGM

SPS-EQ:	$\mathrm{ek_i}$:	ct:	Assumption:
[FHS 15]	$3\mathbb{G}_1 + 1\mathbb{G}_2$	$6\mathbb{G}_1 + 1\mathbb{G}_2$	GGM

Conclusion

Construction:	Predicate:	Ct size:	Assumption:	Practical:
[DHO 16]	any	$O(2^n)$	DDH or DCR	✗
[DHO 16]	any	poly(n)	iO	✗
Our work	$\mathrm{P_{eq}}, \mathrm{P_{comp}}$	$O(n)$	SXDH	✓

Conclusion

Construction:	Predicate:	Ct size:	Assumption:	Practical:
[DHO 16]	any	$O(2^n)$	DDH or DCR	✗
[DHO 16]	any	$\mathrm{poly}(n)$	iO	✗
Our work	$\mathrm{P_{eq}}, \mathrm{P_{comp}}$	$O(n)$	SXDH	✓
Open	$\mathrm{P_{eq}}, \mathrm{P_{comp}}$	$\mathrm{poly}(n)$	DDH	✓

Conclusion

Construction:	Predicate:	Ct size:	Assumption:	Practical:
[DHO 16]	any	$O(2^n)$	DDH or DCR	✗
[DHO 16]	any	$\mathrm{poly}(n)$	iO	✗
Our work	$\mathrm{P}_{\mathrm{eq}}, \mathrm{P}_{\mathrm{comp}}$	$O(n)$	SXDH	✓
Open	$\mathrm{P}_{\mathrm{eq}}, \mathrm{P}_{\mathrm{comp}}$	$\mathrm{poly}(n)$	DDH	✓
Open	any	$\mathrm{poly}(n)$	standard	✓

Conclusion

Construction:	Predicate:	Ct size:	Assumption:	Practical:
[DHO 16]	any	$O(2^n)$	DDH or DCR	✗
[DHO 16]	any	poly(n)	iO	✗
Our work	$\mathrm{P_{eq}}, \mathrm{P_{comp}}$	$O(n)$	SXDH	✓
Open	$\mathrm{P_{eq}}, \mathrm{P_{comp}}$	poly(n)	DDH	✓
Open	any	poly(n)	standard	✓

Thank you!

Any questions?