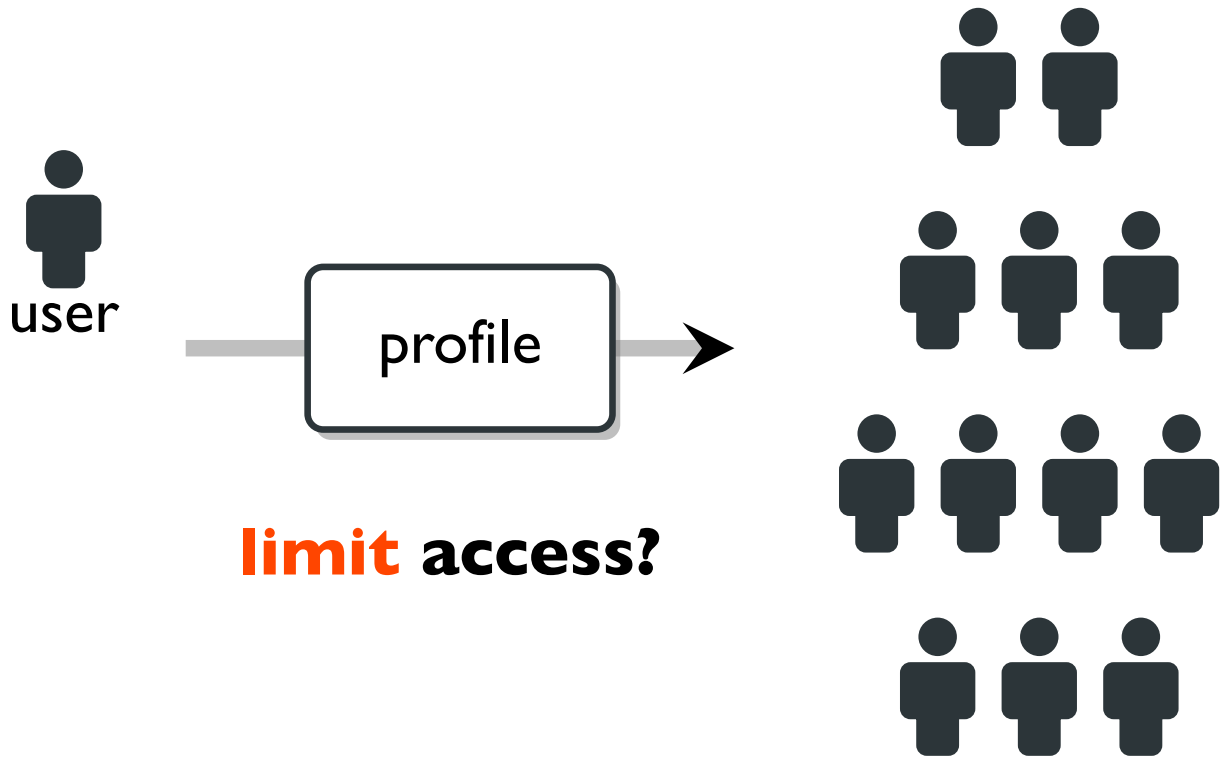
Attribute-Based Encryption & **Information-Theoretic** Crypto

Hoeteck Wee (**ENS**)

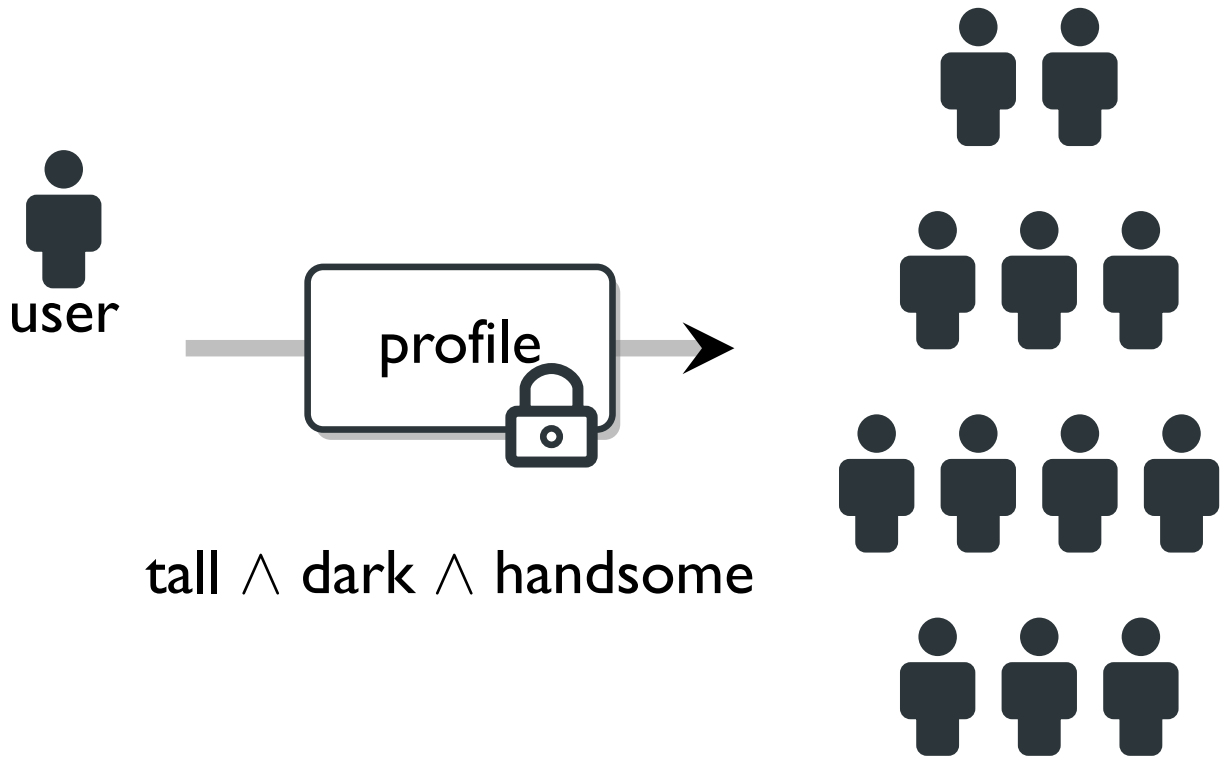
dating + big data

user

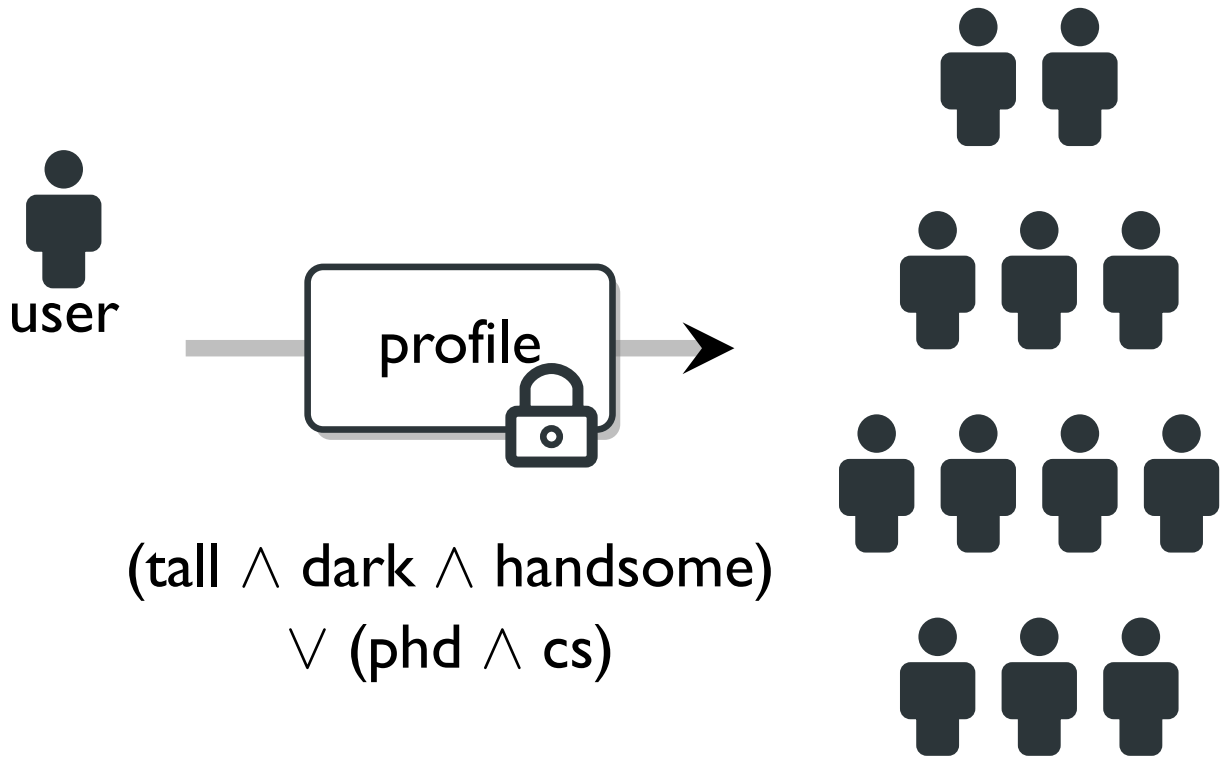
dating + big data



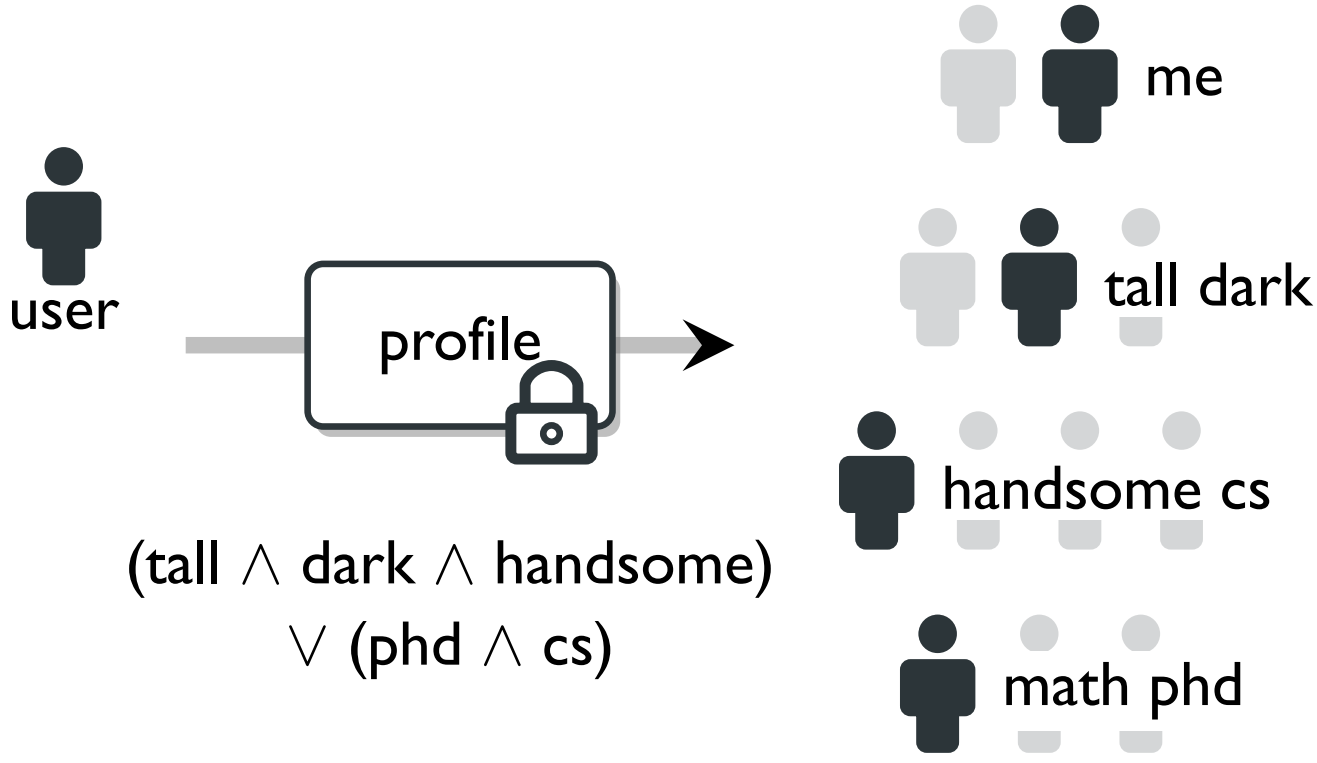
dating + big data



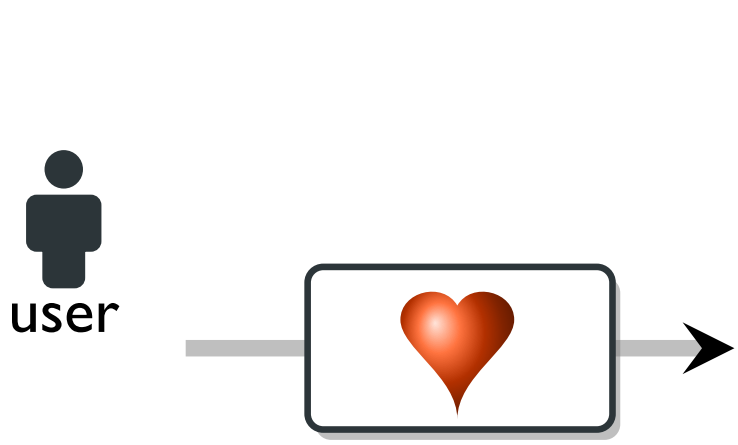
dating + big data



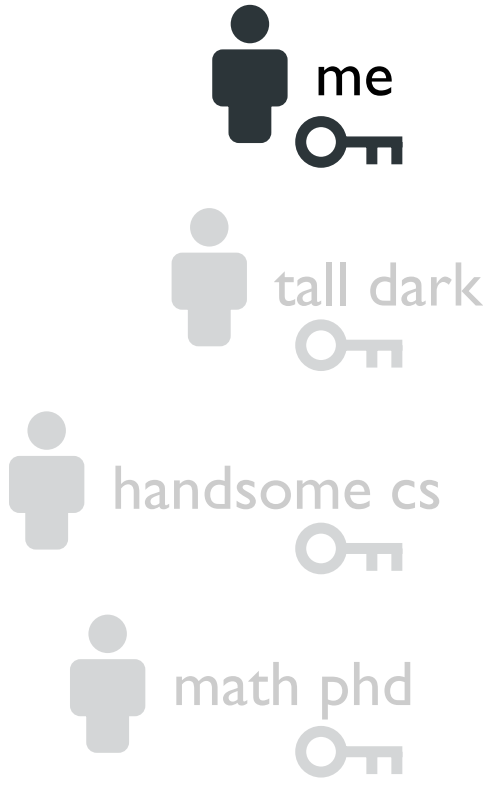
dating + big data



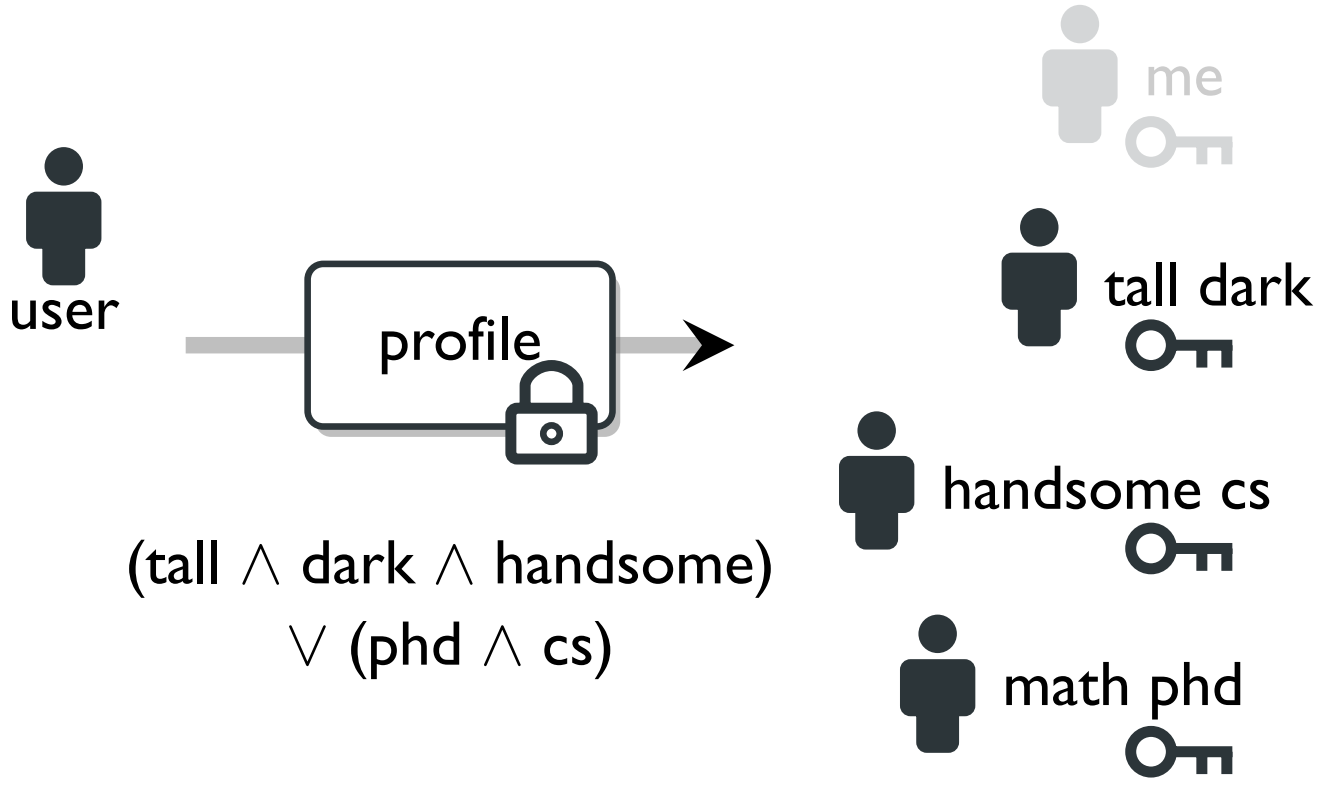
dating + big data



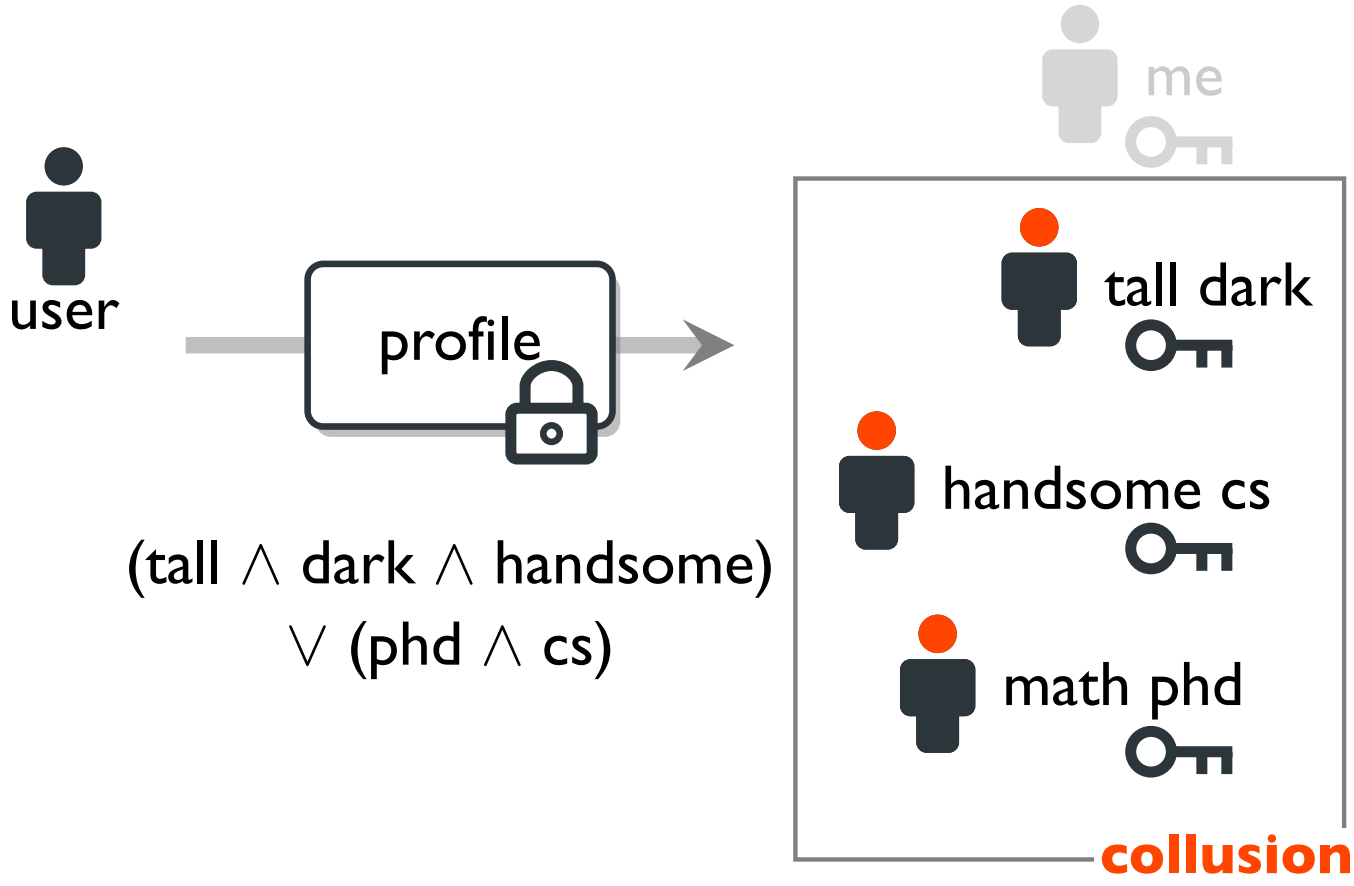
(tall ∧ dark ∧ handsome)
∨ (phd ∧ cs)



dating + big data

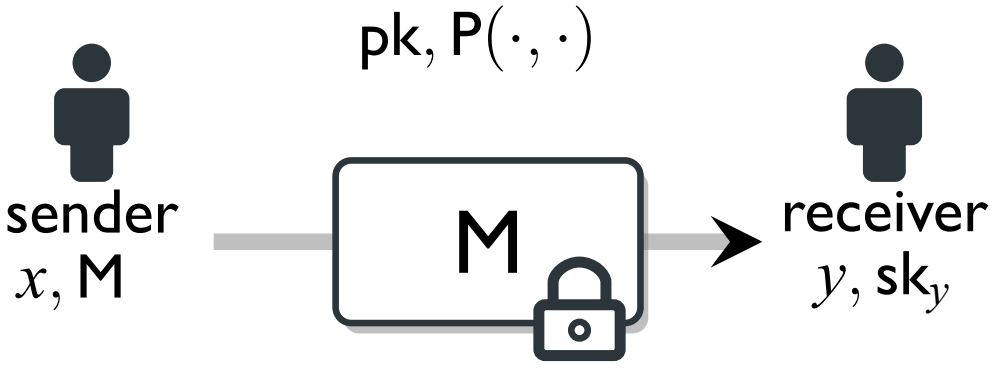


dating + big data



attribute-based encryption

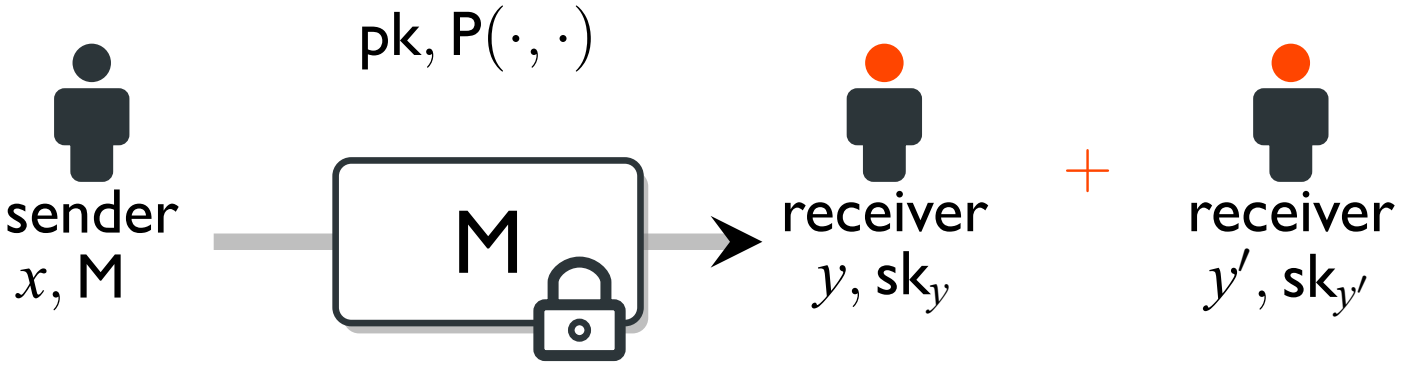
[GPSW06,SW05]



learns M $\Leftrightarrow$ $\mathsf{P}(x, y) = 1$

attribute-based encryption

[GPSW06,SW05]

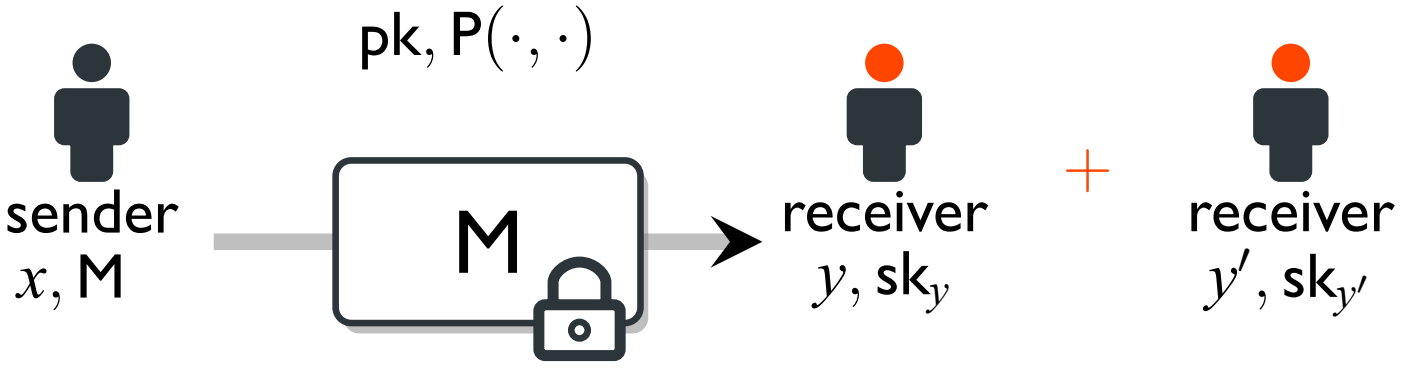


learns M $\Leftrightarrow$ $P(x, y) = 1$

security against **collusions**

attribute-based encryption

[GPSW06,SW05]



learns M $\Leftrightarrow$ $P(x,y)=1$

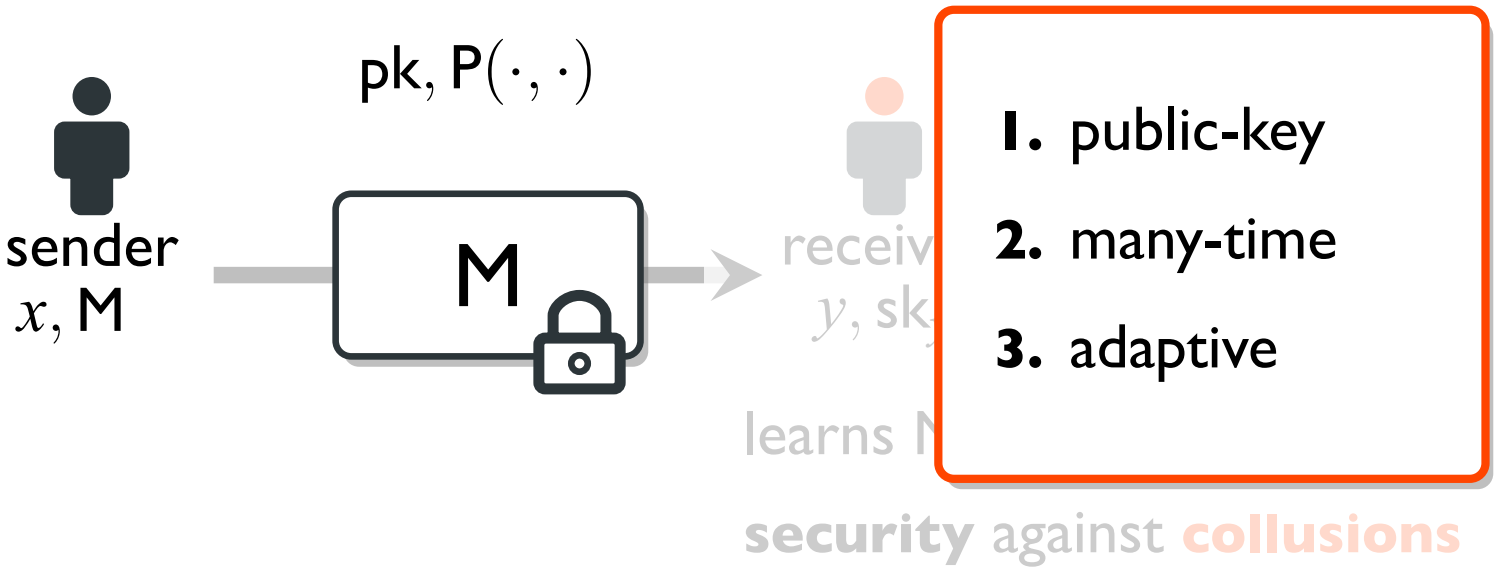
security against **collusions**

prior works.

[BF01, CHK04, BB04, GPSW06, W09, LW10, LOSTW10, OT10, ..., GVW13]

attribute-based encryption

[GPSW06,SW05]



prior works.

[BF01, CHK04, BB04, GPSW06, W09, LW10, LOSTW10, OT10, ..., GVW13]

this **talk**

information-theoretic

1. private-key
2. one-time
3. non-adaptive

attribute-based enc

1. public-key
2. many-time
3. adaptive

this **talk**

information-theoretic

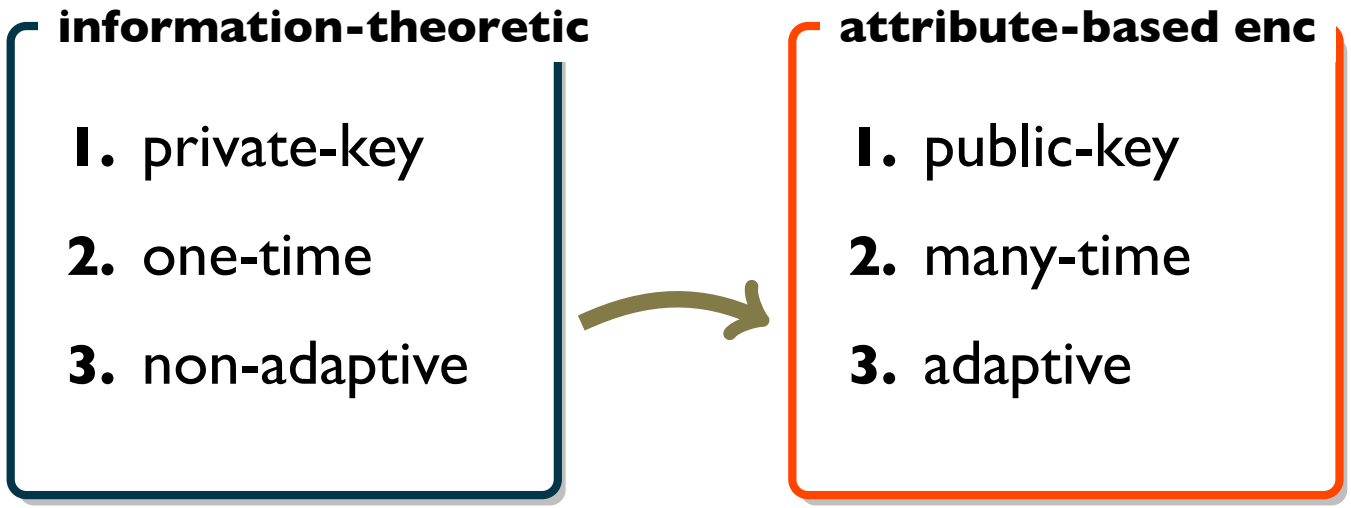
1. private-key
2. one-time
3. non-adaptive

attribute-based enc

1. public-key
2. many-time
3. adaptive

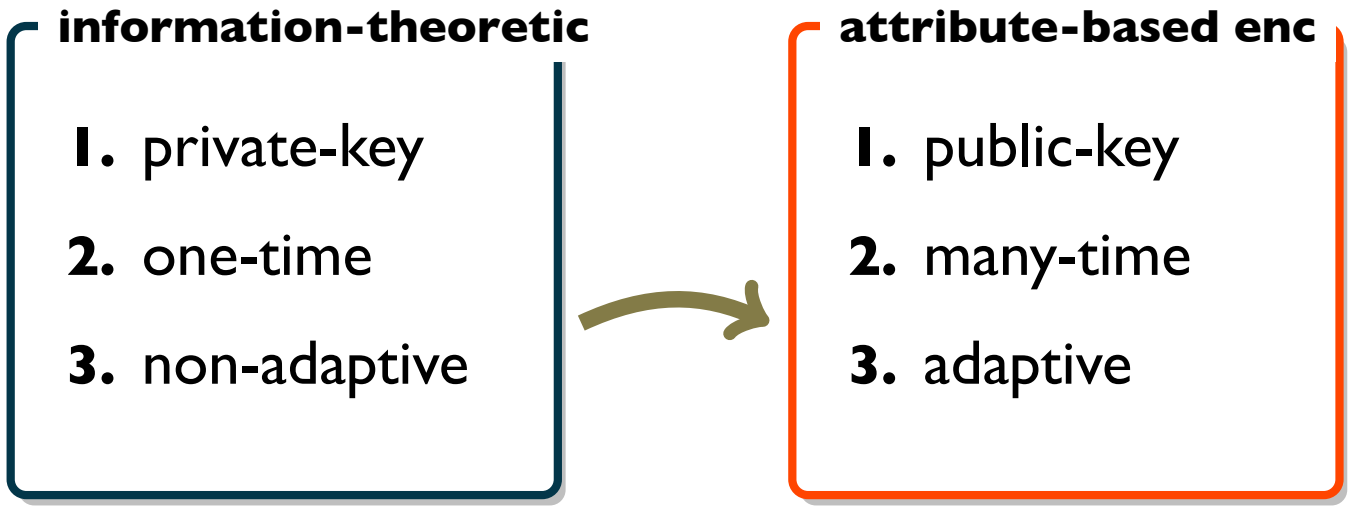
1. **conditional disclosure of secrets** & examples

this **talk**



1. **conditional disclosure of secrets** & examples
2. **compiler** based on DDH in bilinear groups

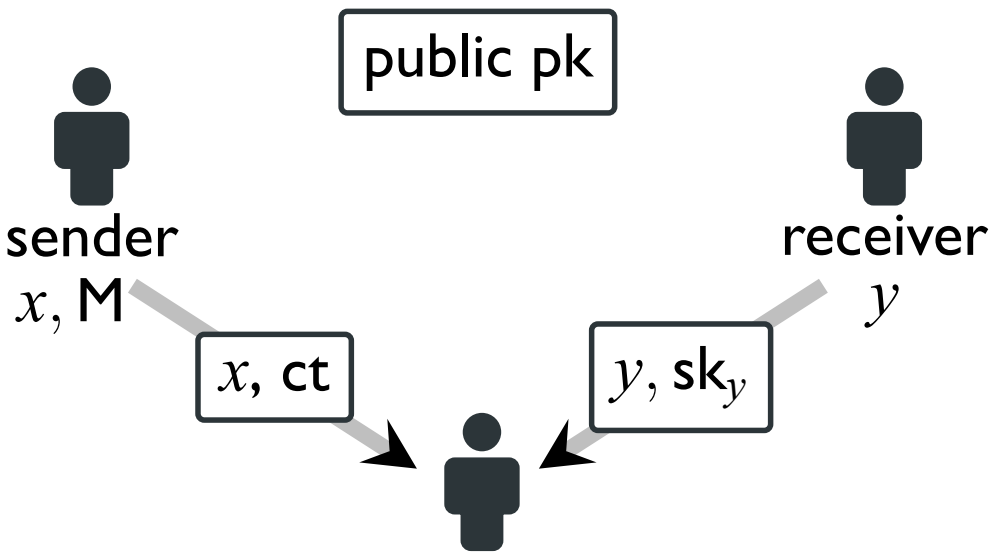
this **talk**



1. **conditional disclosure of secrets** & examples
2. **compiler** based on DDH in bilinear groups
3. new **lower bounds**

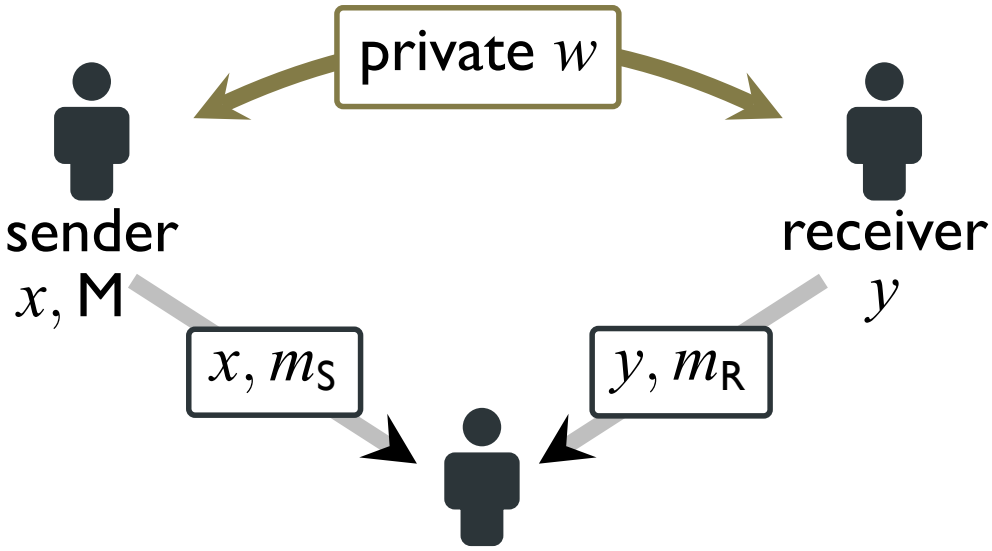
attribute-based encryption

[GPSW06,SW05]



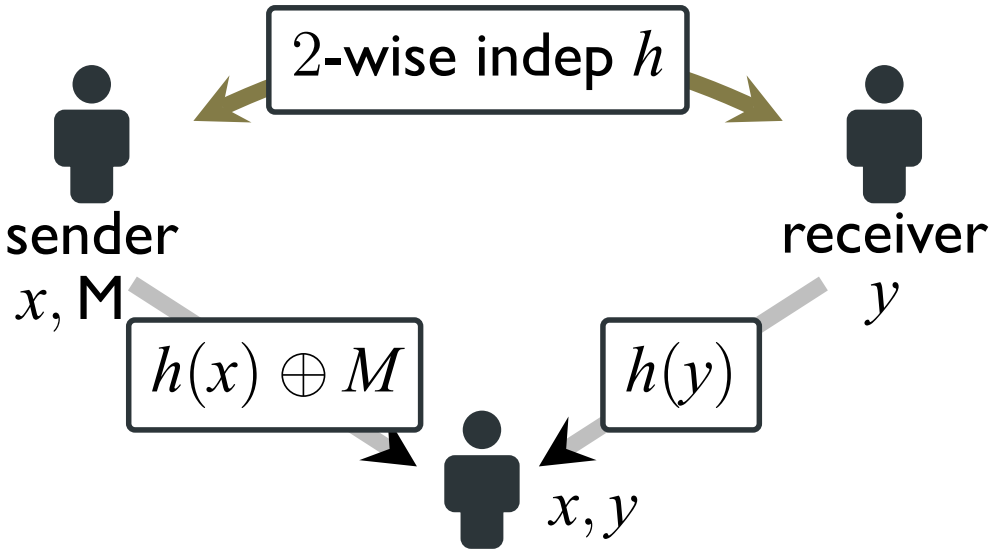
learns M $\Leftrightarrow$ $\mathsf{P}(x, y) = 1$

conditional disclosure of secrets [GIKM00,FKN94]



learns M $\Leftrightarrow$ P$(x, y) = 1$

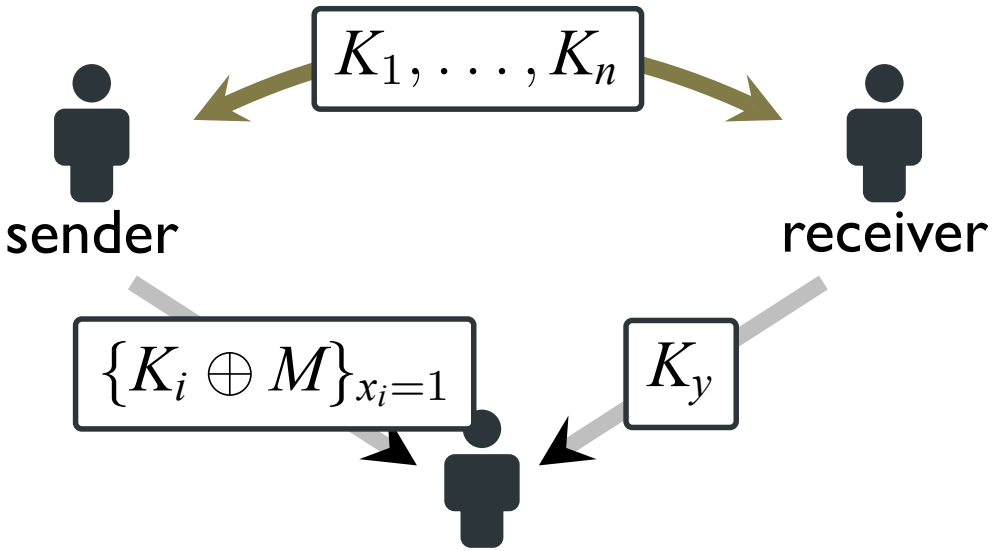
conditional disclosure of secrets EXAMPLES



learns M $\Leftrightarrow$ $\mathsf{P}(x, y) = 1$

equality. $\mathsf{P}(x, y) = (x \stackrel{?}{=} y)$

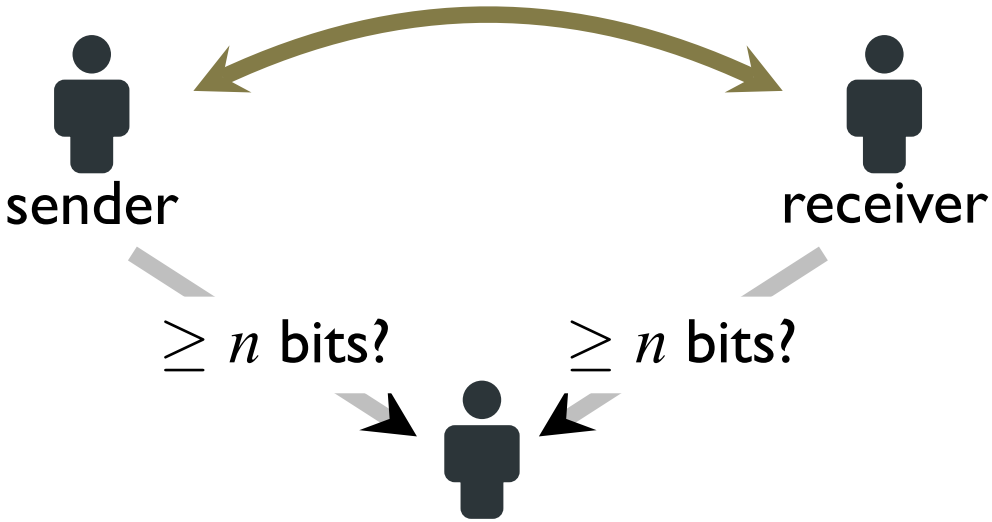
conditional disclosure of secrets EXAMPLES



learns M $\Leftrightarrow$ $\mathsf{P}(x, y) = 1$

index. $\mathsf{P}(x, y) = x_y, \ |x| = n, y \in [n]$

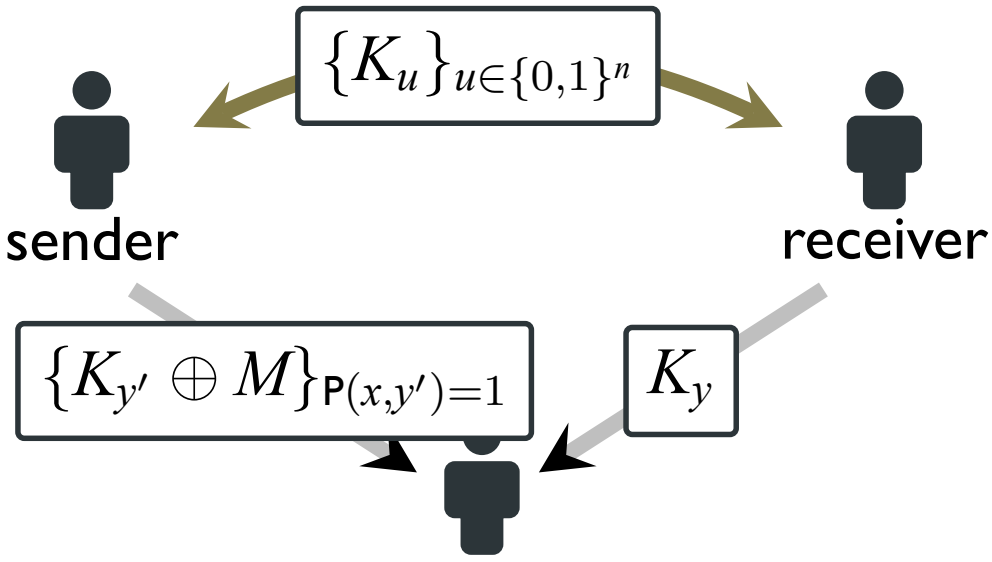
conditional disclosure of secrets EXAMPLES



learns M $\Leftrightarrow$ P$(x, y) = 1$

any P with n-bit inputs

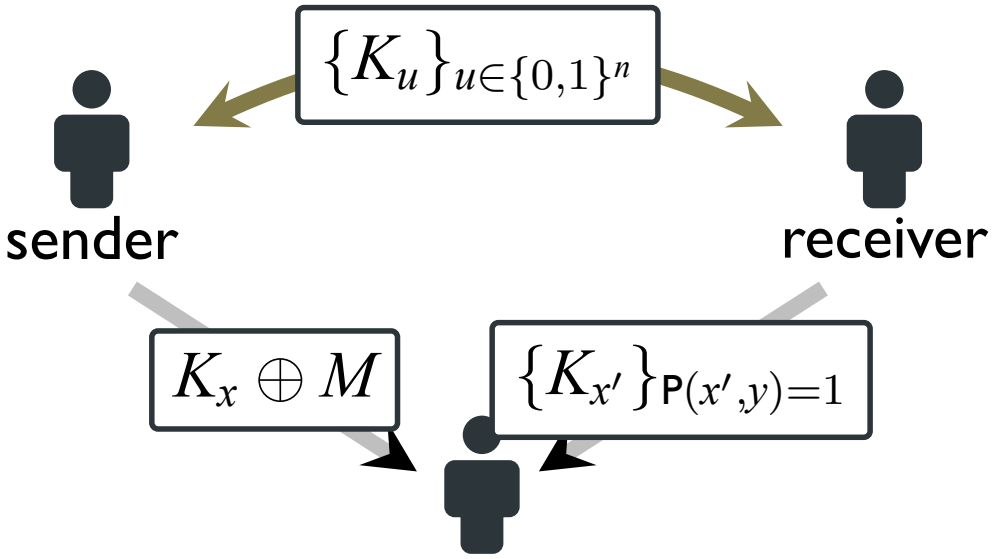
conditional disclosure of secrets EXAMPLES



learns M $\Leftrightarrow$ $\mathsf{P}(x, y) = 1$

any P with n-bit inputs

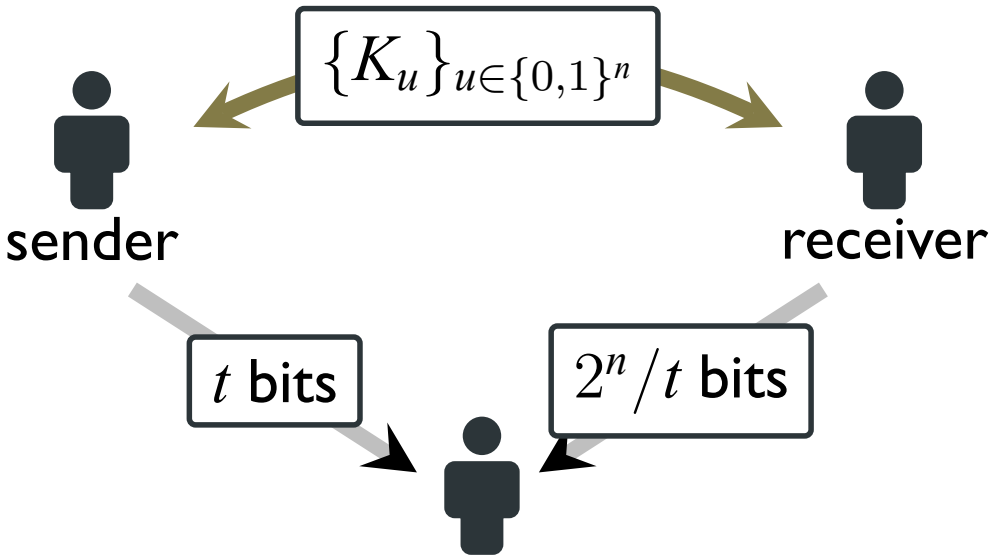
conditional disclosure of secrets EXAMPLES



learns M $\Leftrightarrow$ $\mathsf{P}(x,y) = 1$

any P with n-bit inputs

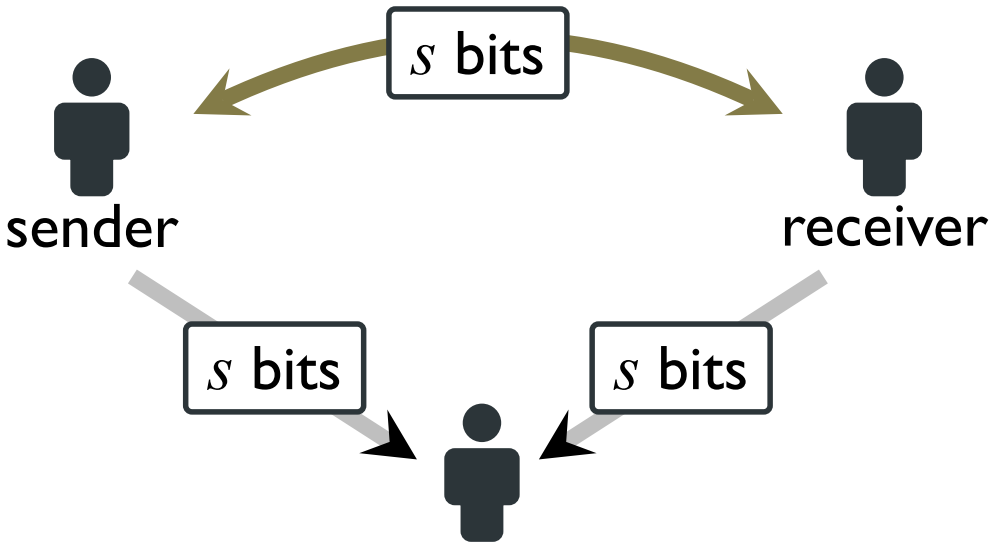
conditional disclosure of secrets EXAMPLES



learns M $\Leftrightarrow$ P$(x, y) = 1$

any P with n-bit inputs

conditional disclosure of secrets EXAMPLES

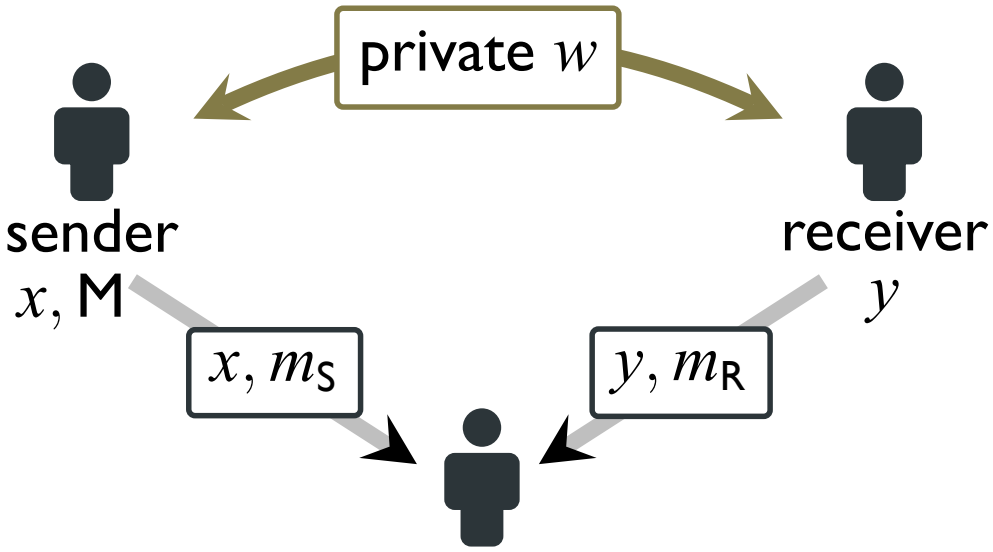


learns M $\Leftrightarrow$ P$(x, y) = 1$

NC^1 formula size s

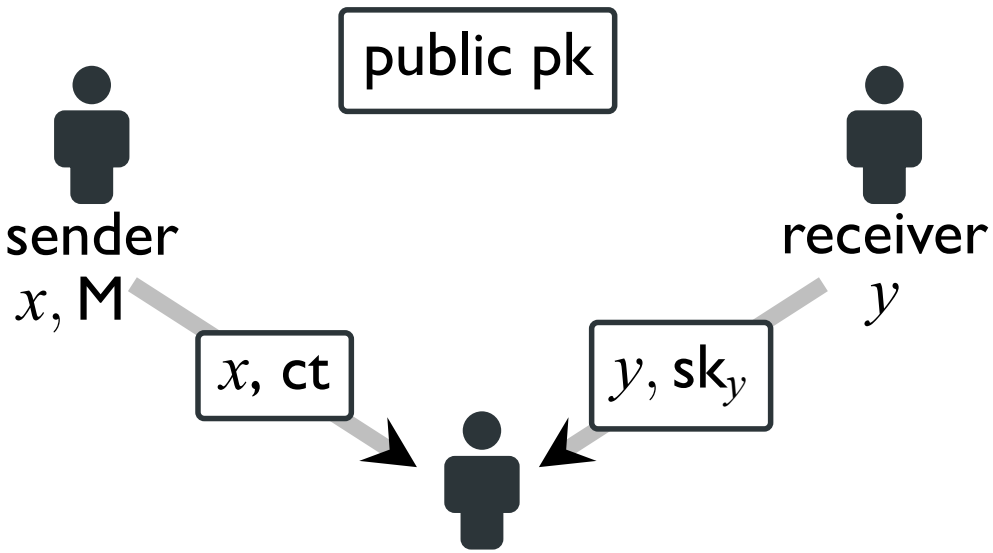
compiler: CDS $\mapsto$ ABE

[W14, Chen Gay W15]



compiler: CDS $\mapsto$ ABE

[W14, Chen Gay W15]



$$(w, m_{\mathsf{S}}, m_{\mathsf{R}}) \mapsto (\mathsf{pk}, \mathsf{ct}, \mathsf{sk}_y)$$

compiler: CDS $\mapsto$ ABE

(1) $w \mapsto \mathbf{W}_1, \mathbf{W}_2, \ldots$

compiler: CDS $\mapsto$ ABE

(1) $w \mapsto \mathbf{W}_1, \mathbf{W}_2, \ldots$

(2) pk $:=$

compiler: CDS $\mapsto$ ABE

(1) $w \mapsto \mathbf{W}_1, \mathbf{W}_2, \ldots$

(2) pk $:=$

"in the exponent" over bilinear groups

compiler: CDS $\mapsto$ ABE

(1) $w \mapsto \mathbf{W}_1, \mathbf{W}_2, \ldots$

(2) pk $:=$

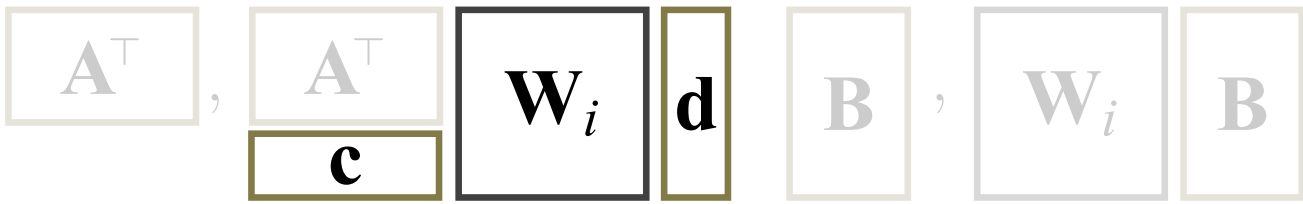
"in the exponent" over bilinear groups

proof. $\mathbf{W}_i$ has entropy given pk

compiler: CDS $\mapsto$ ABE

(1) $w \mapsto \mathbf{W}_1, \mathbf{W}_2, \ldots$

(2) pk :=



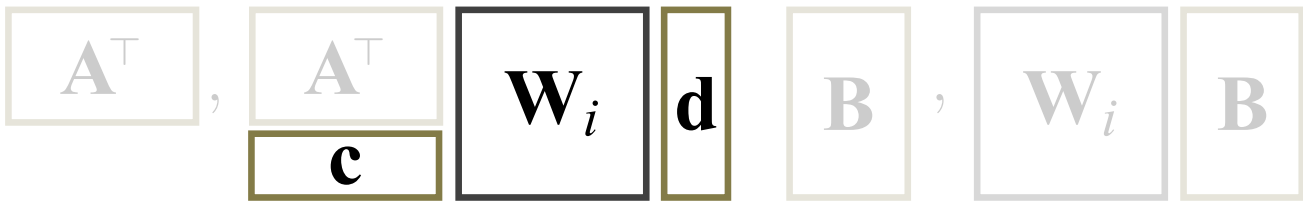
"in the exponent" over bilinear groups

proof. $\mathbf{W}_i$ has entropy given pk

compiler: CDS $\mapsto$ ABE

(1) $w \mapsto \mathbf{W}_1, \mathbf{W}_2, \ldots$

(2) pk :=

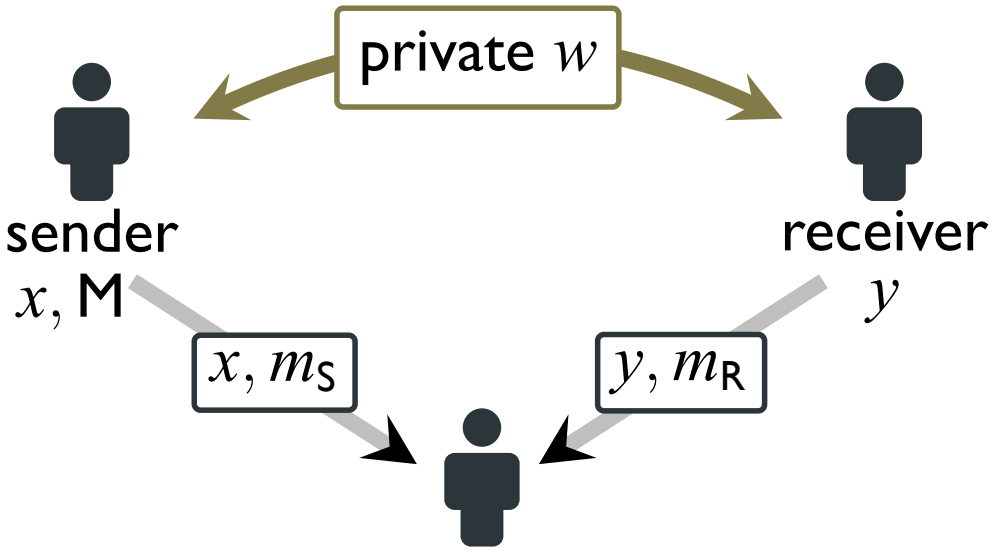


"in the exponent" over bilinear groups

proof. $\mathbf{W}_i$ has entropy given pk = CDS private key

lower bounds

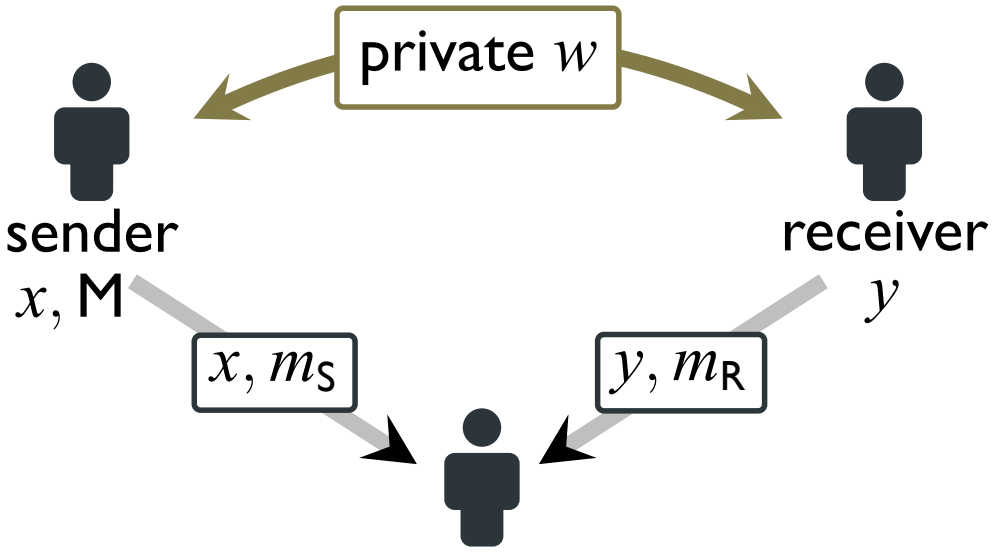
[Gay Kerenidis W15]



Q. how much **communication** (as a function of P)?

lower bounds

[Gay Kerenidis W15]

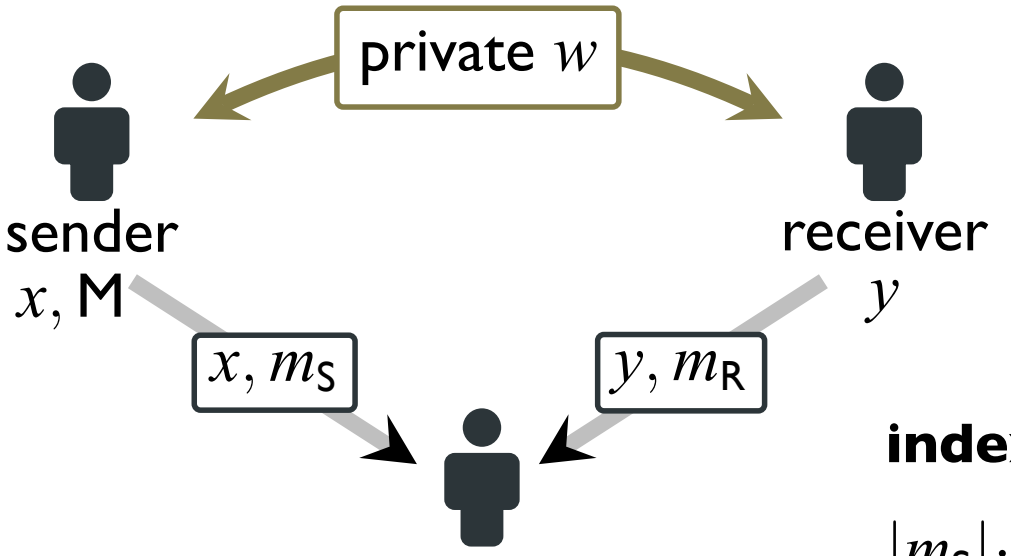


informal.

$$|m_S| + |m_R| \geq \sqrt{\text{communication complexity of } P}$$

lower bounds

[Gay Kerenidis W15]



index, prefix:

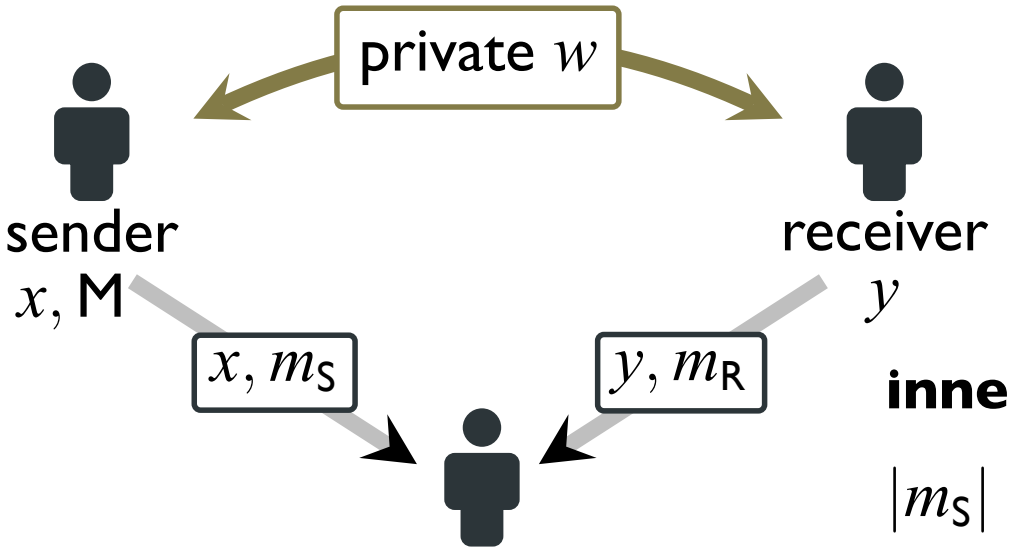
$|m_S| \cdot |m_R| \geq n$ if $|m_S| \leq \sqrt{n}$

informal.

$|m_S| + |m_R| \geq \sqrt{\text{communication complexity of } P}$

lower bounds

[Gay Kerenidis W15]



inner product:

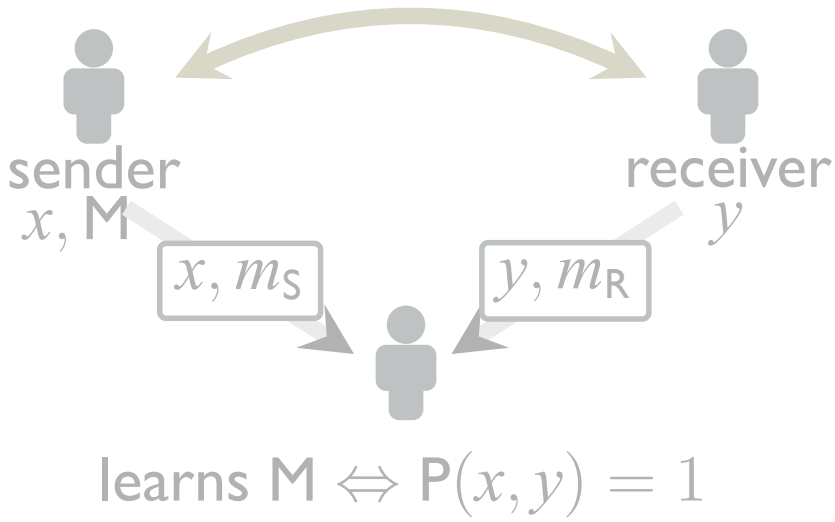
$$|m_S| = \Omega(n) \text{ if } |m_R| = O(1)$$

$$|m_R| = \Omega(n) \text{ if } |m_S| = O(1)$$

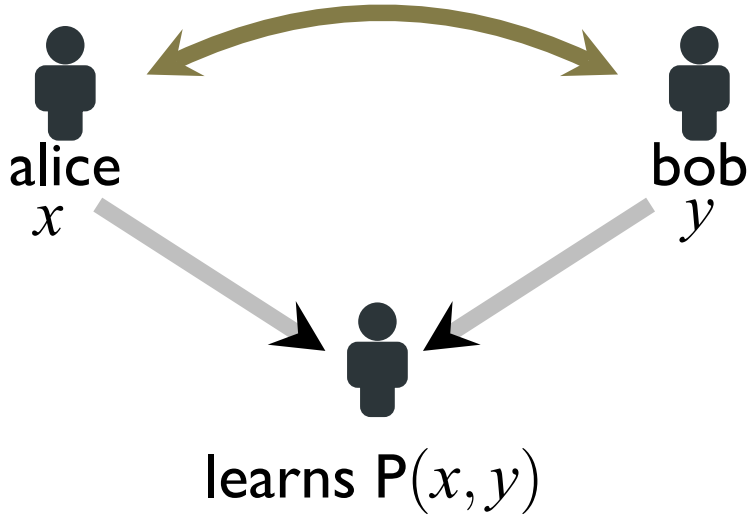
informal.

$$|m_S| + |m_R| \geq \sqrt{\text{communication complexity of } P}$$

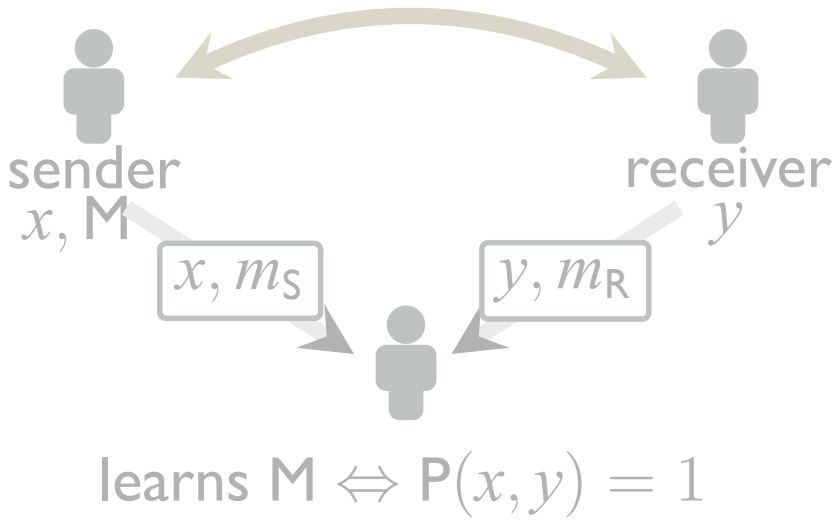
proof strategy



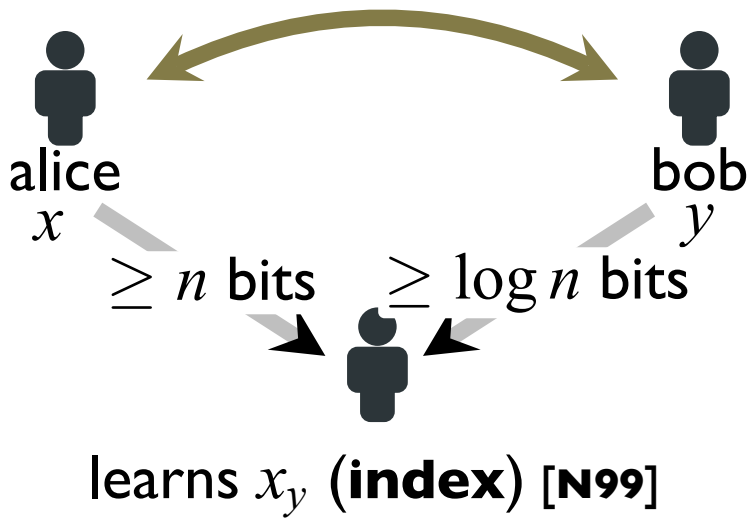
communication complexity [Y82]



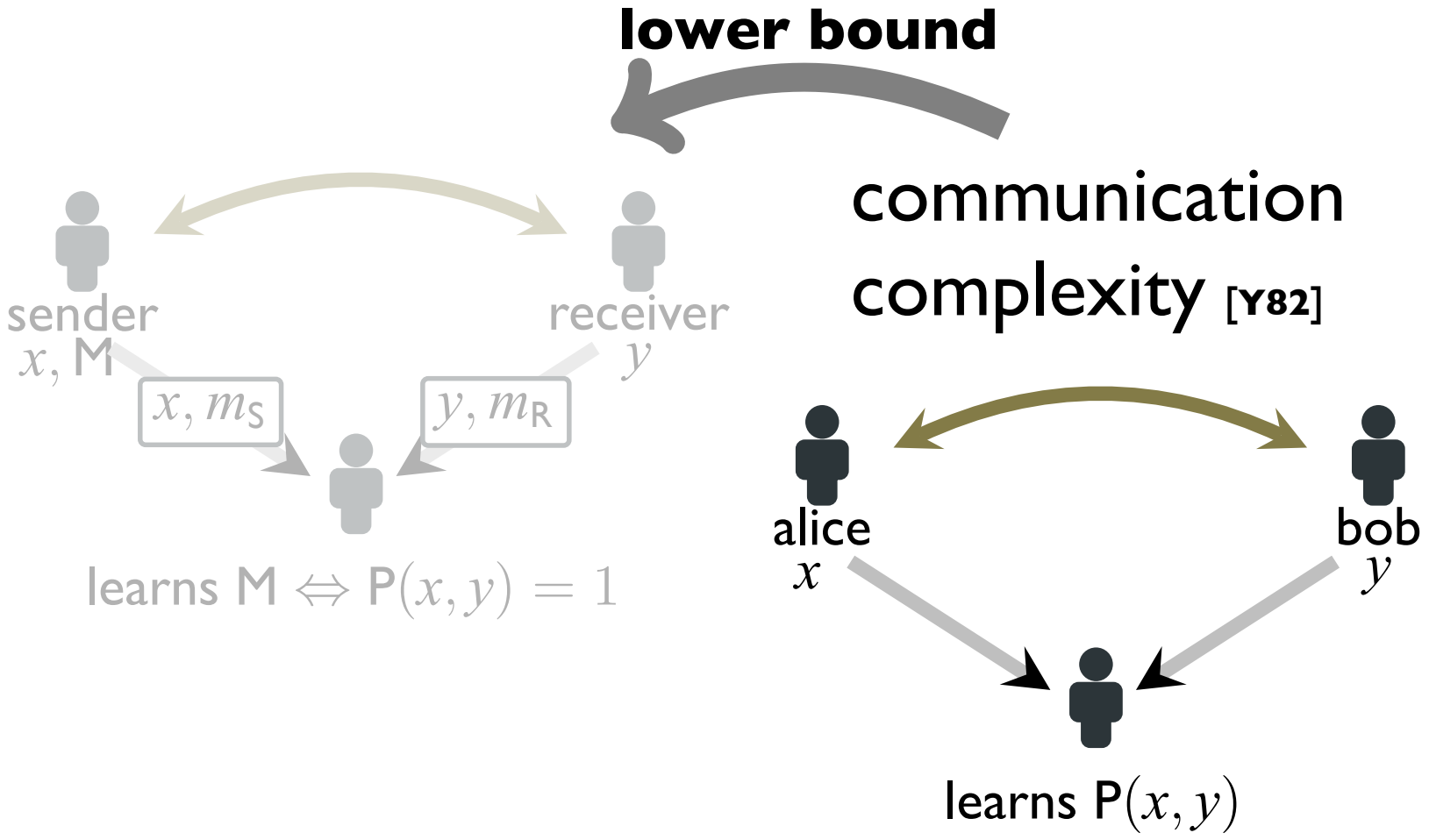
proof strategy



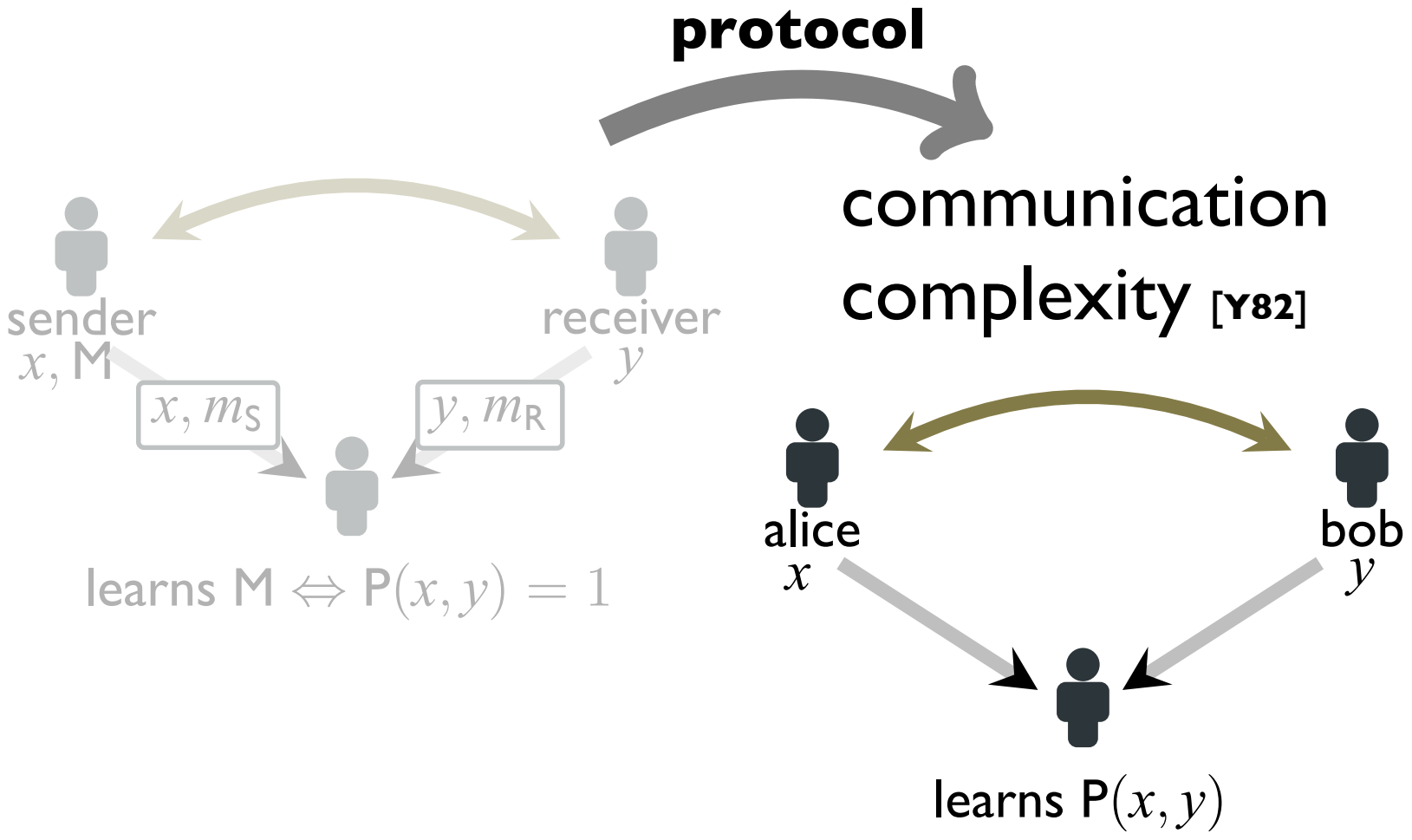
communication complexity **[Y82]**



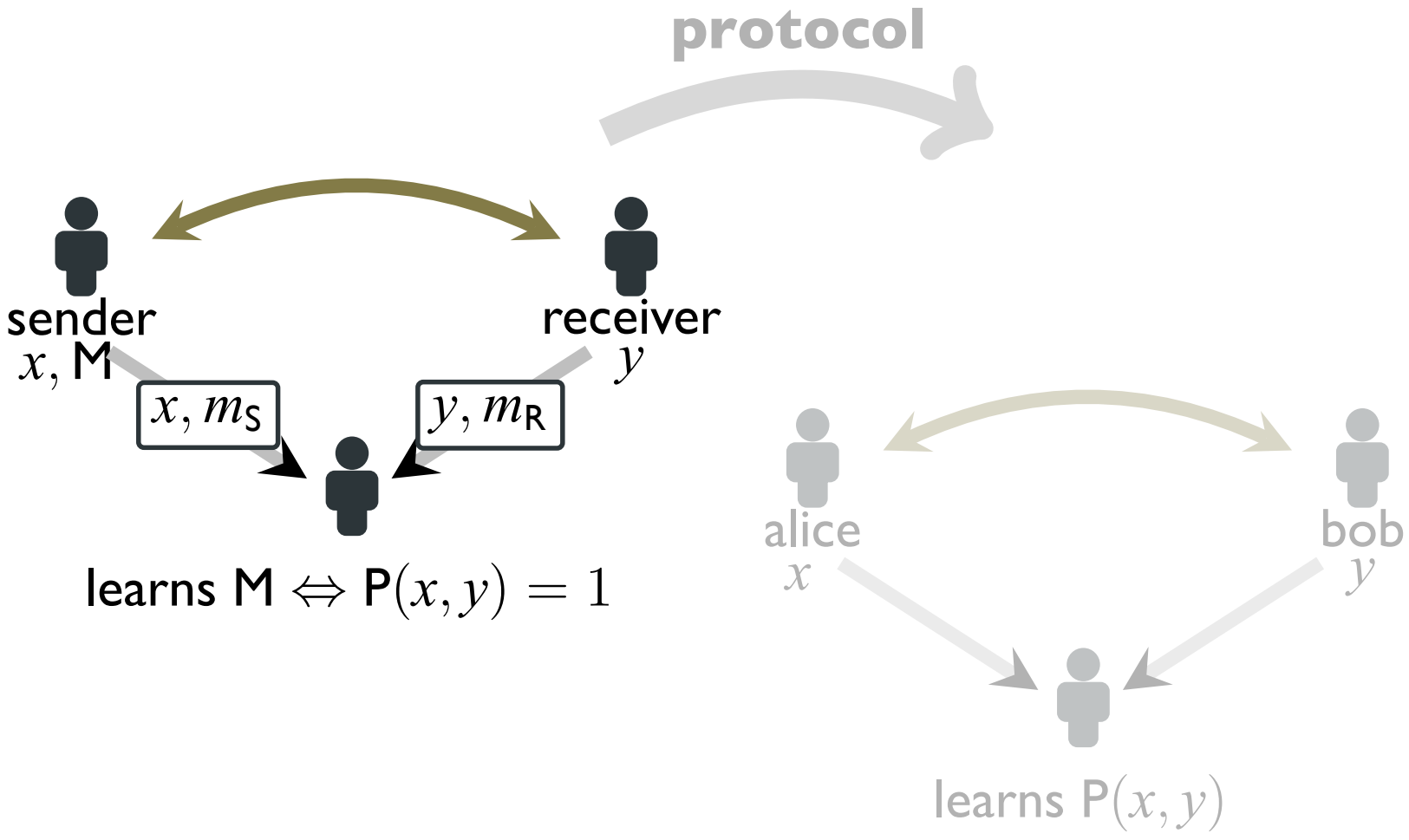
proof strategy



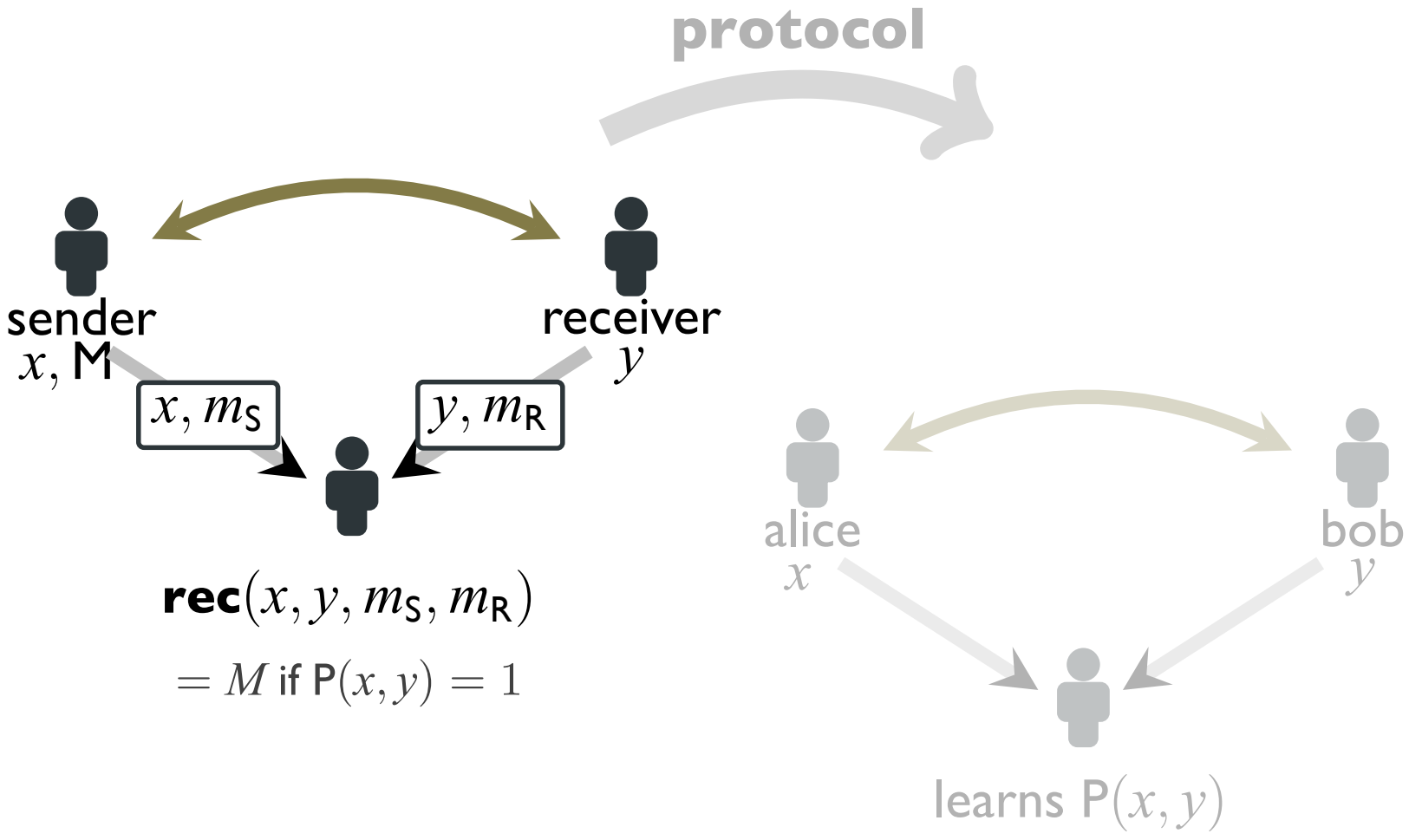
proof strategy



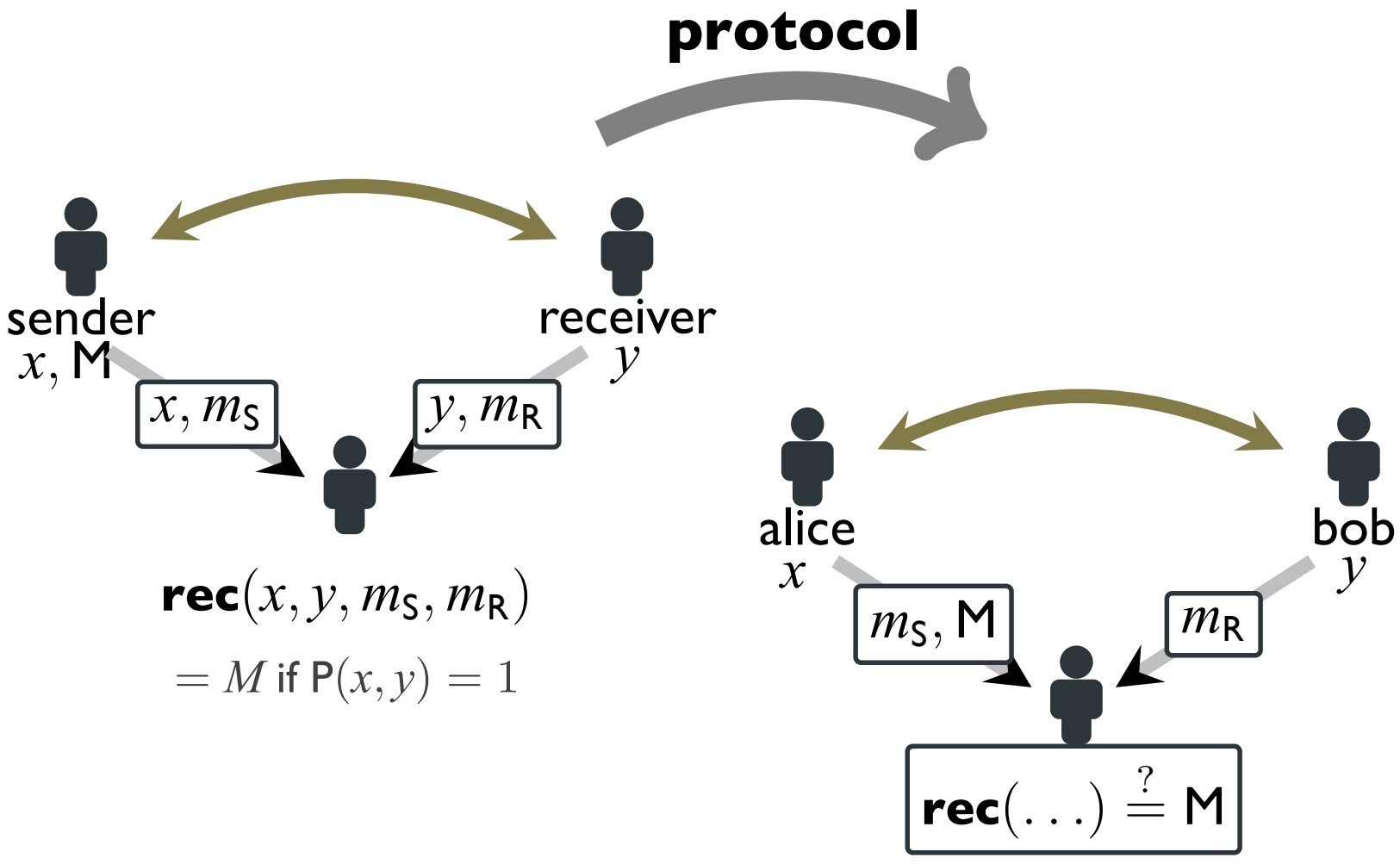
proof strategy



proof strategy



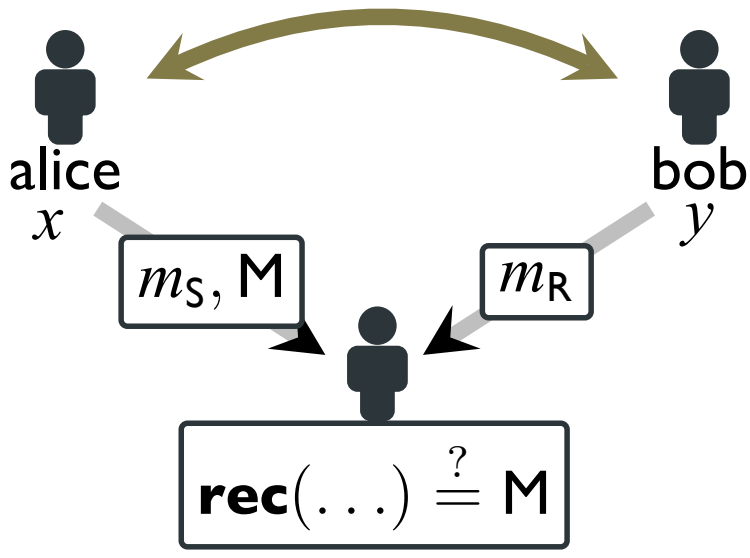
proof – first idea



proof – first idea

$$\textbf{rec}(x, y, m_S, m_R) = M \text{ if } \mathsf{P}(x, y) = 1$$

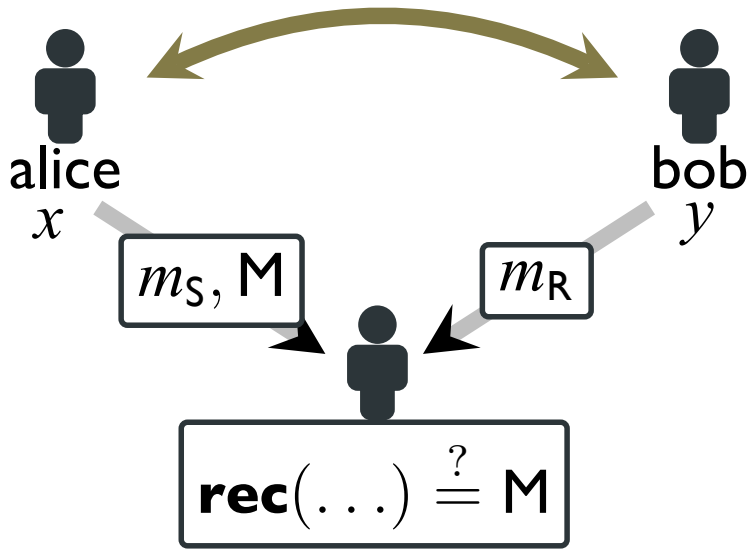
pf. $\Pr[\textbf{rec}(\ldots) = \mathsf{M}] \leq \frac{1}{2}$ if $\mathsf{P}(x, y) = 0$



proof – first idea

thm? $|m_S| + |m_R| + 1 \geq \mathsf{cc}(\mathsf{P})$

$\mathbf{rec}(x, y, m_S, m_R)$
$= M$ if $\mathsf{P}(x, y) = 1$



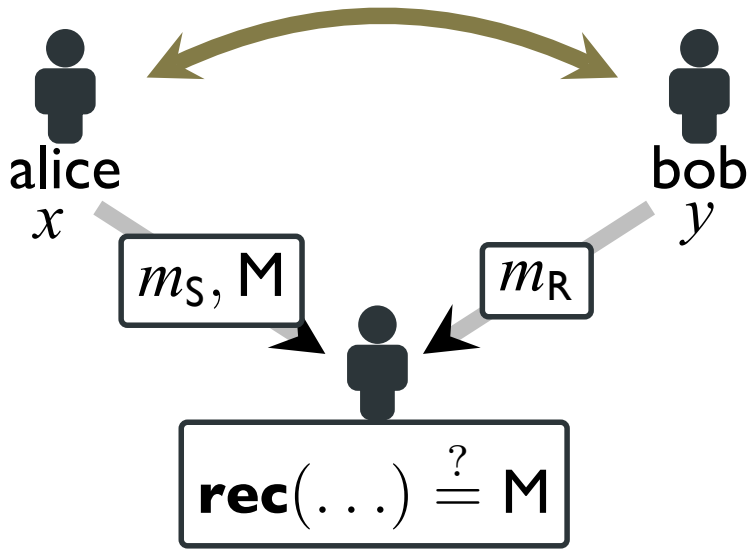
proof – first idea

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $P(x, y) = 1$

thm? $|m_S| + |m_R| + 1 \geq cc(P)$

problem. which (x, y)?

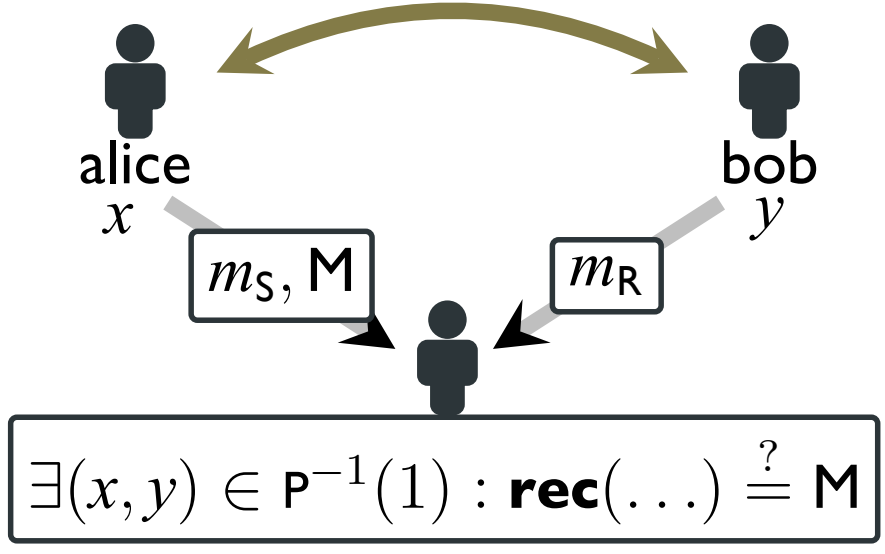


proof – first idea

thm? $|m_S| + |m_R| + 1 \geq \mathsf{cc}(\mathsf{P})$

problem. which (x, y)?

$\mathbf{rec}(x, y, m_S, m_R)$
$= M$ if $\mathsf{P}(x, y) = 1$



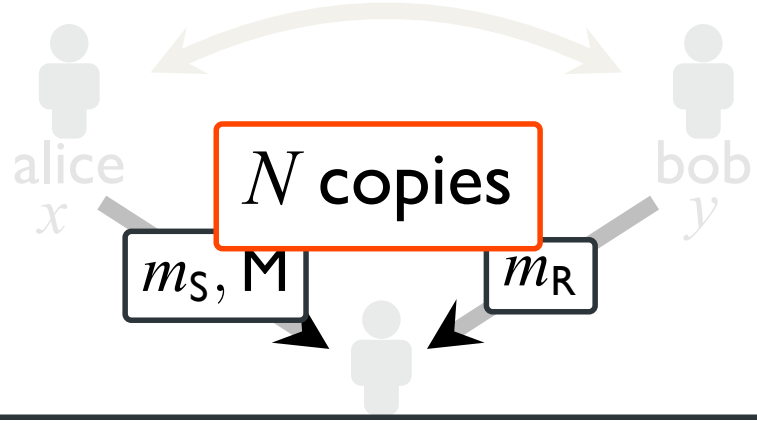
proof – second idea

thm? $|m_S| + |m_R| + 1 \geq \mathsf{cc}(\mathsf{P})$

pf. $\Pr[\mathbf{rec}(\ldots) = \mathsf{M}] \leq \frac{1}{2^N}$

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$



$\exists (x, y) \in \mathsf{P}^{-1}(1) : \forall i, \mathbf{rec}(\ldots) \stackrel{?}{=} \mathsf{M}$

proof – second idea

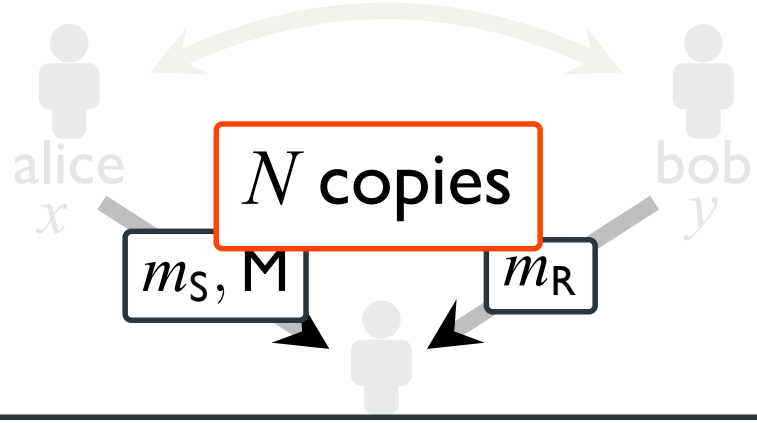
thm. $N\big(|m_S| + |m_R| + 1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log |\mathsf{P}^{-1}(1)|$

+ union bound

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$



$\exists (x, y) \in \mathsf{P}^{-1}(1) : \forall i, \mathbf{rec}(\ldots) \stackrel{?}{=} \mathsf{M}$

proof – second idea

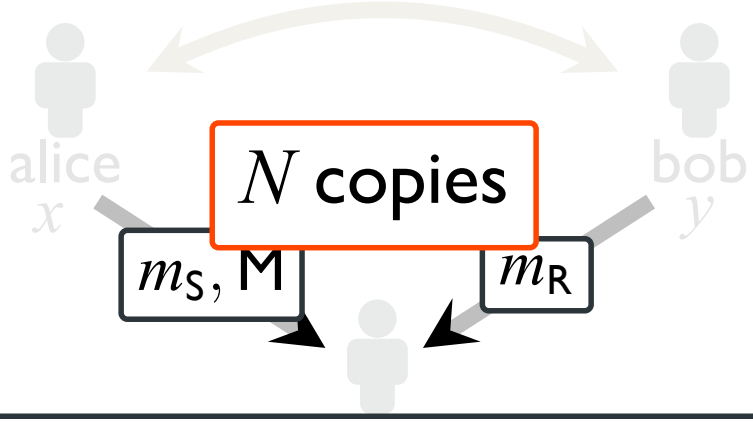
$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$

thm. $N\big(|m_S| + |m_R| + 1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log |\mathsf{P}^{-1}(1)|$

x $|\mathsf{P}^{-1}(1)| \approx 2^n, \mathsf{cc}(\mathsf{P}) \leq 2n$



$\exists (x, y) \in \mathsf{P}^{-1}(1) : \forall i, \mathbf{rec}(\ldots) \stackrel{?}{=} \mathsf{M}$

proof – third idea

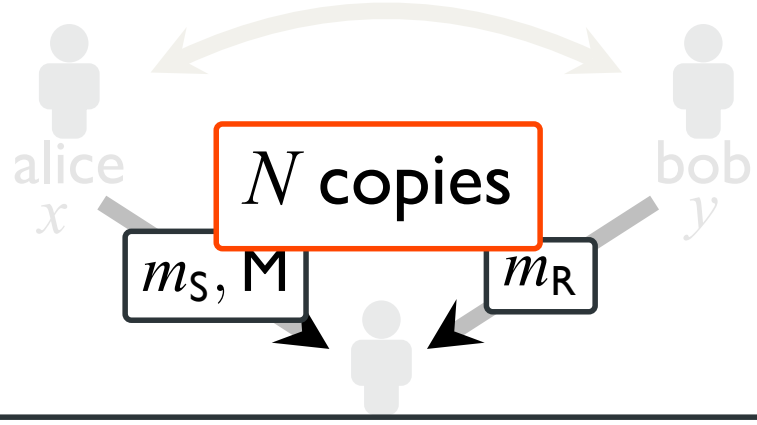
thm. $N\big(|m_S| + |m_R| + 1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log |\#\mathbf{rec}^*|$

x $|\mathsf{P}^{-1}(1)| \approx 2^n, \mathsf{cc}(\mathsf{P}) \leq 2n$

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$



$\mathbf{rec}^* : \{0,1\}^{|m_S|+|m_R|} \to \{0,1\}$

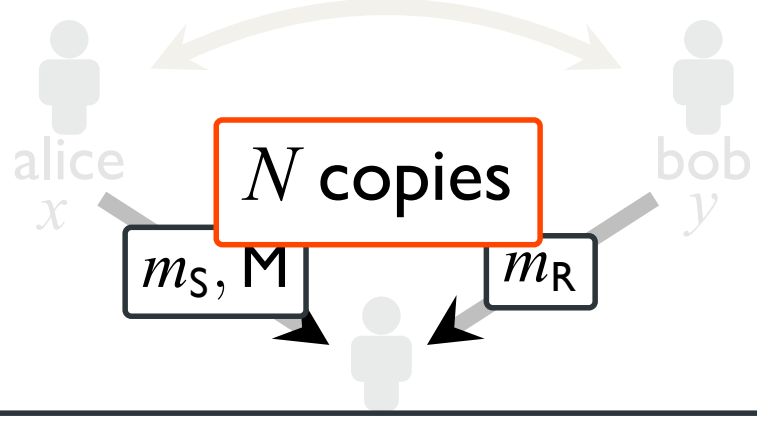
$\exists \mathbf{rec}^* : \forall i, \mathbf{rec}^*(m_S^i, m_R^i) \stackrel{?}{=} \mathsf{M}$

proof – third idea

thm. $N\big(|m_S| + |m_R| + 1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log |\#\mathbf{rec}^*| \leq 2^{|m_S|+|m_R|}$

x $|\mathsf{P}^{-1}(1)| \approx 2^n, \mathsf{cc}(\mathsf{P}) \leq 2n$



$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$

$\mathbf{rec}^* : \{0,1\}^{|m_S|+|m_R|} \to \{0,1\}$ $\quad \exists \mathbf{rec}^* : \forall i, \mathbf{rec}^*(m_S^i, m_R^i) \stackrel{?}{=} \mathsf{M}$

proof – third idea

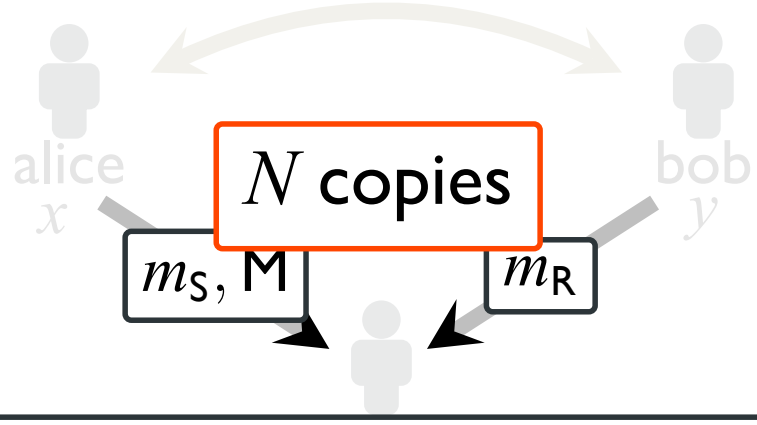
thm. $N\big(|m_S| + |m_R| + 1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log |\#\mathbf{rec}^*| \leq 2^{|m_S|+|m_R|}$

$\Rightarrow |m_S| + |m_R| = \Omega(\log \mathsf{cc}(\mathsf{P}))$

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$



$\mathbf{rec}^* : \{0,1\}^{|m_S|+|m_R|} \to \{0,1\}$ $\quad \exists \mathbf{rec}^* : \forall i, \mathbf{rec}^*(m_S^i, m_R^i) \stackrel{?}{=} \mathsf{M}$

proof – third idea

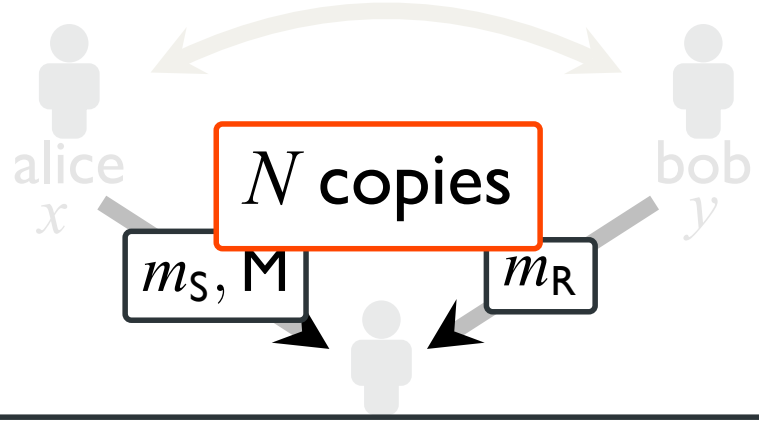
thm. $N\big(|m_S| + |m_R| + 1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log |\#\mathbf{rec}^*| \leq |m_S| + |m_R|$

for linear $\mathbf{rec}^*$

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$



$\mathbf{rec}^* : \{0,1\}^{|m_S|+|m_R|} \to \{0,1\}$ $\quad \exists \mathbf{rec}^* : \forall i, \mathbf{rec}^*(m_S^i, m_R^i) \stackrel{?}{=} \mathsf{M}$

proof – third idea

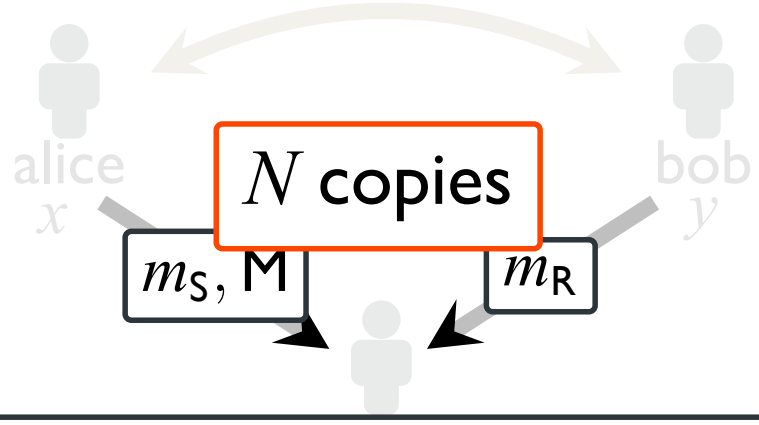
thm. $N\big(|m_S|+|m_R|+1\big) \geq \mathsf{cc}(\mathsf{P})$

pf. $N = \log|\#\mathbf{rec}^*| \leq |m_S|+|m_R|$

for linear $\mathbf{rec}^* \Rightarrow \Omega(\sqrt{\mathsf{cc}(\mathsf{P})})$

$\mathbf{rec}(x, y, m_S, m_R)$

$= M$ if $\mathsf{P}(x, y) = 1$



$\mathbf{rec}^* : \{0,1\}^{|m_S|+|m_R|} \to \{0,1\}$ $\quad \exists \mathbf{rec}^* : \forall i, \mathbf{rec}^*(m_S^i, m_R^i) \stackrel{?}{=} \mathsf{M}$

conclusion

today. **attribute-based** encryption +

information-theoretic crypto

conclusion

today. **attribute-based** encryption +

information-theoretic crypto

open questions.

– compiler from lattice assumptions?

– other compilers [KW15, KPW15]?

conclusion

today. **attribute-based** encryption +

information-theoretic crypto

open questions.

– **non-linear** reconstruction [BI01, VV15]?

– tight bounds for **inner product**?

– **multi-bit** secrets [C94, BGW99, BBPT14]?

// the end