Adaptively secure MPC in sublinear communication

Ran Cohen
BU & Northeastern

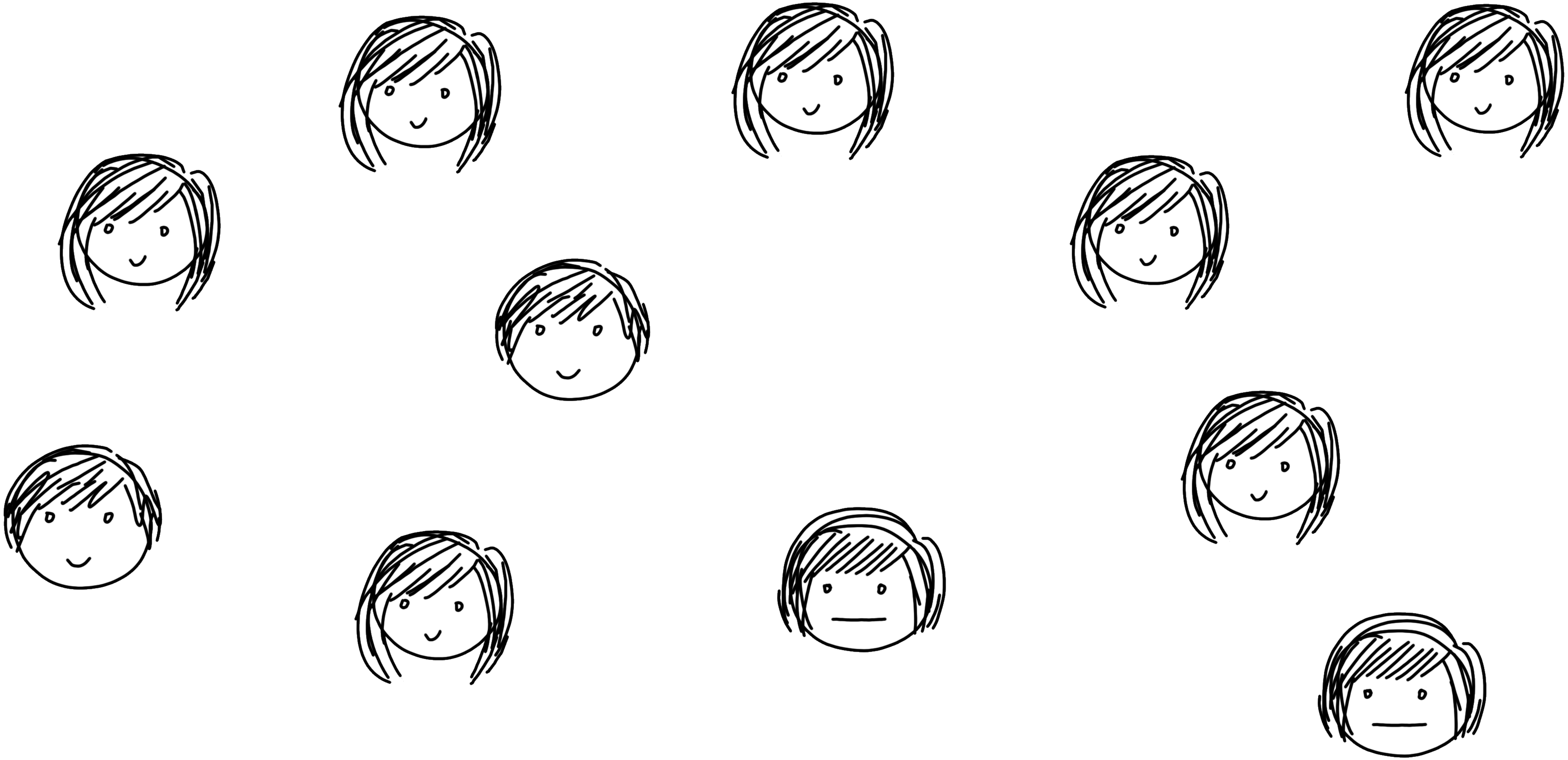
Daniel Wichs
Northeastern

abhi shelat
Northeastern

Static corruptions

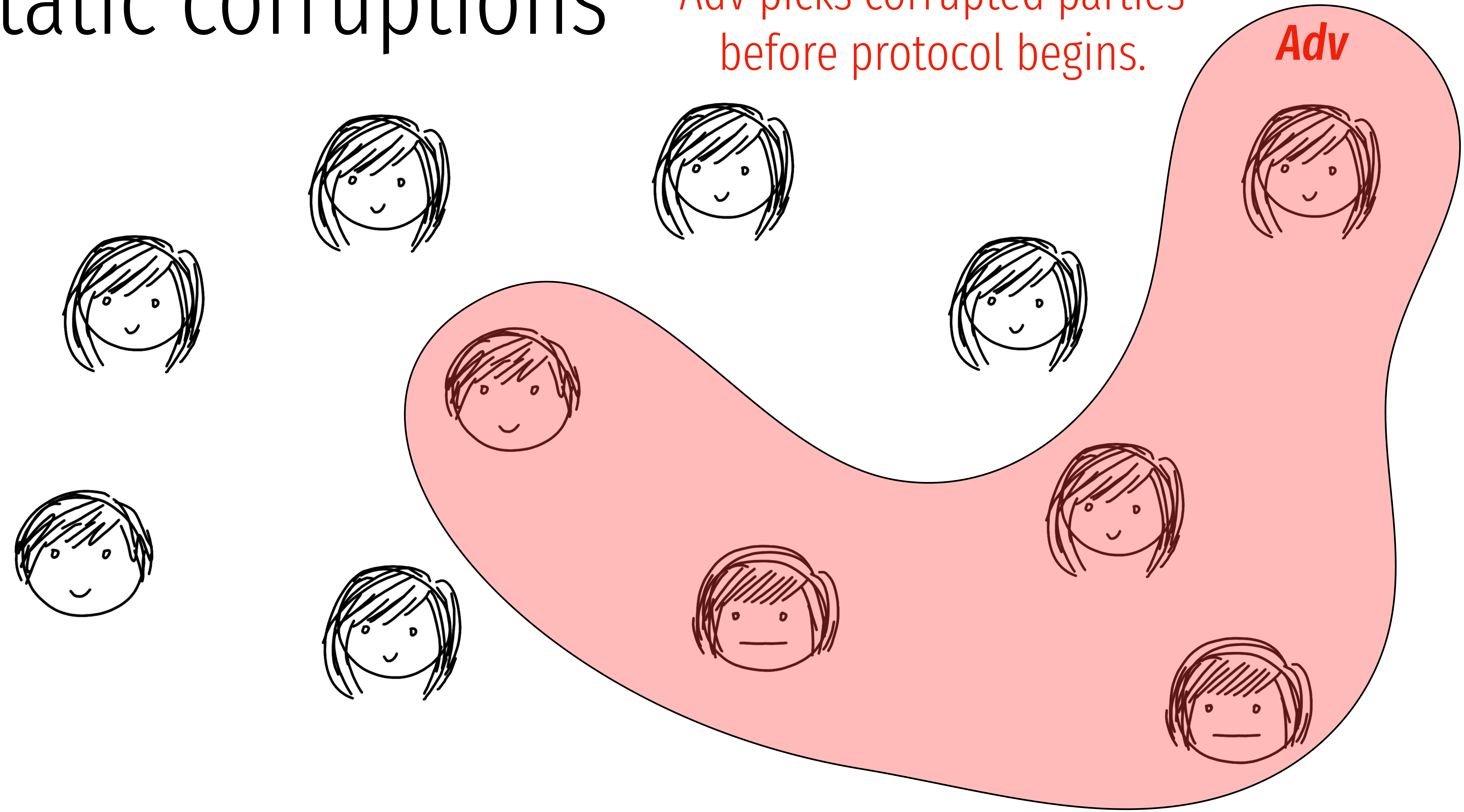
Adv picks corrupted parties before protocol begins.

Adv



Static corruptions

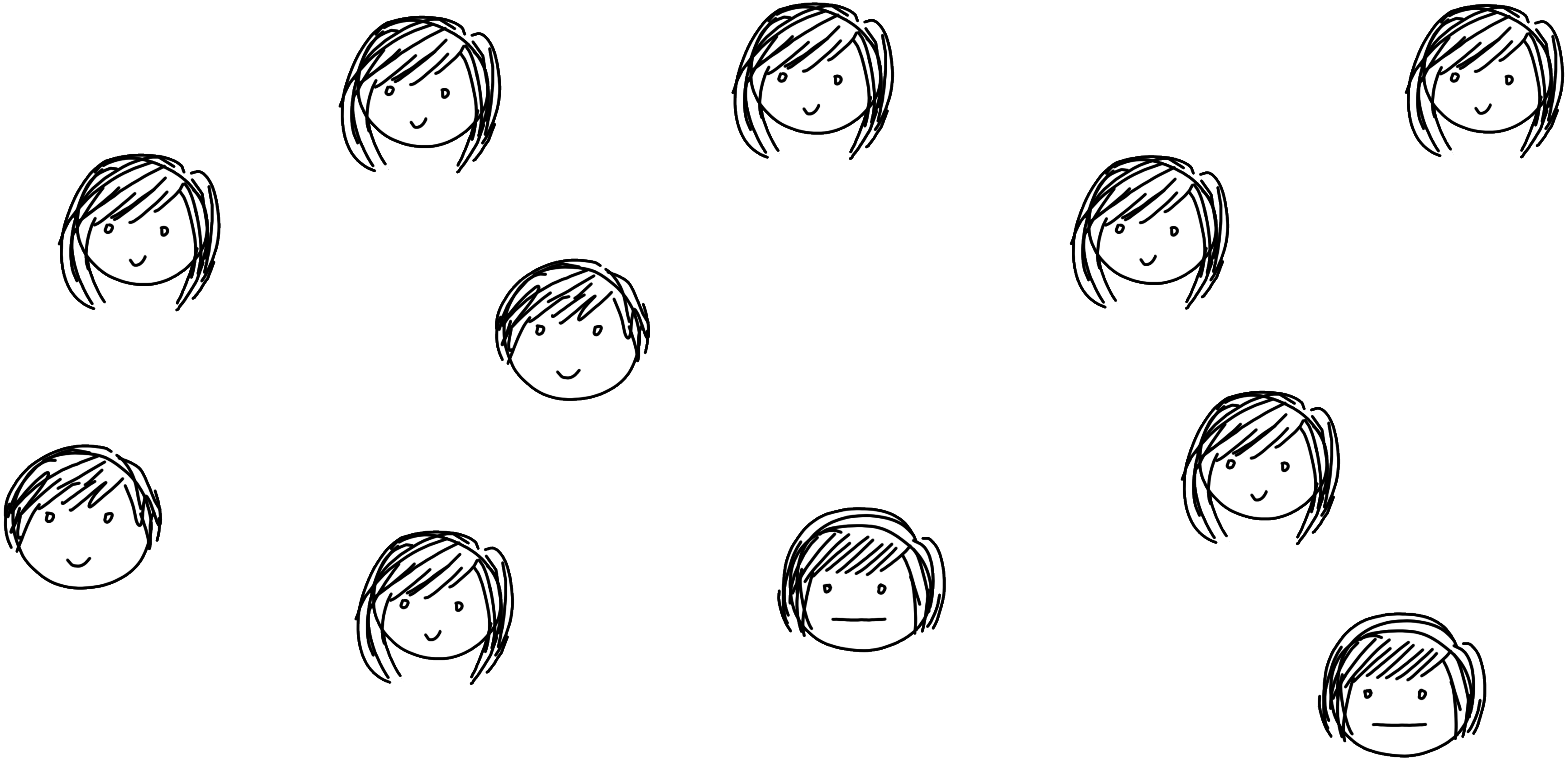
Adv picks corrupted parties before protocol begins.



Adaptive corruptions

Adv picks corrupted parties at any time.

Adv



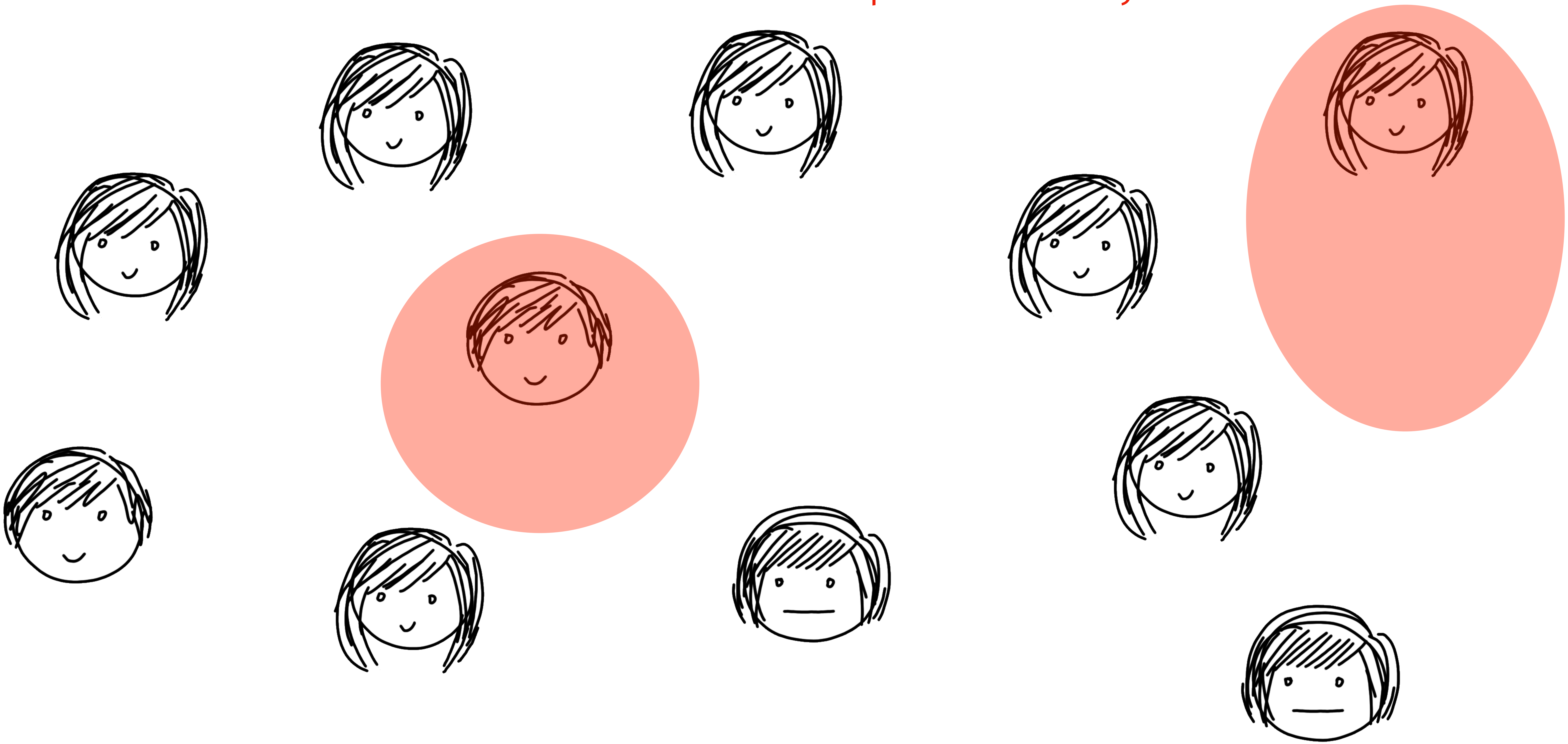
Adaptive corruptions

Adv picks corrupted parties at any time.

Adaptive corruptions

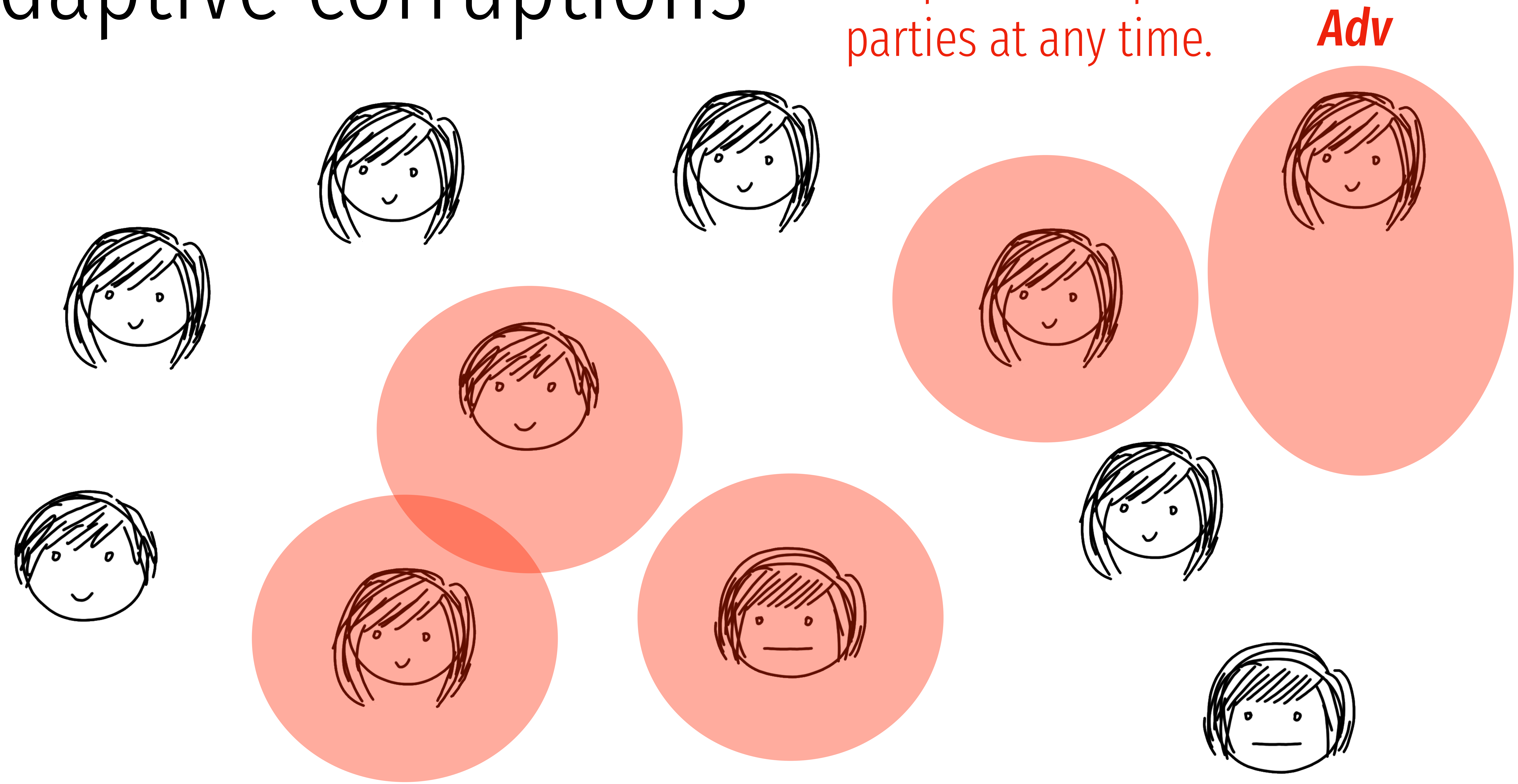
Adv picks corrupted parties at any time.

Adv



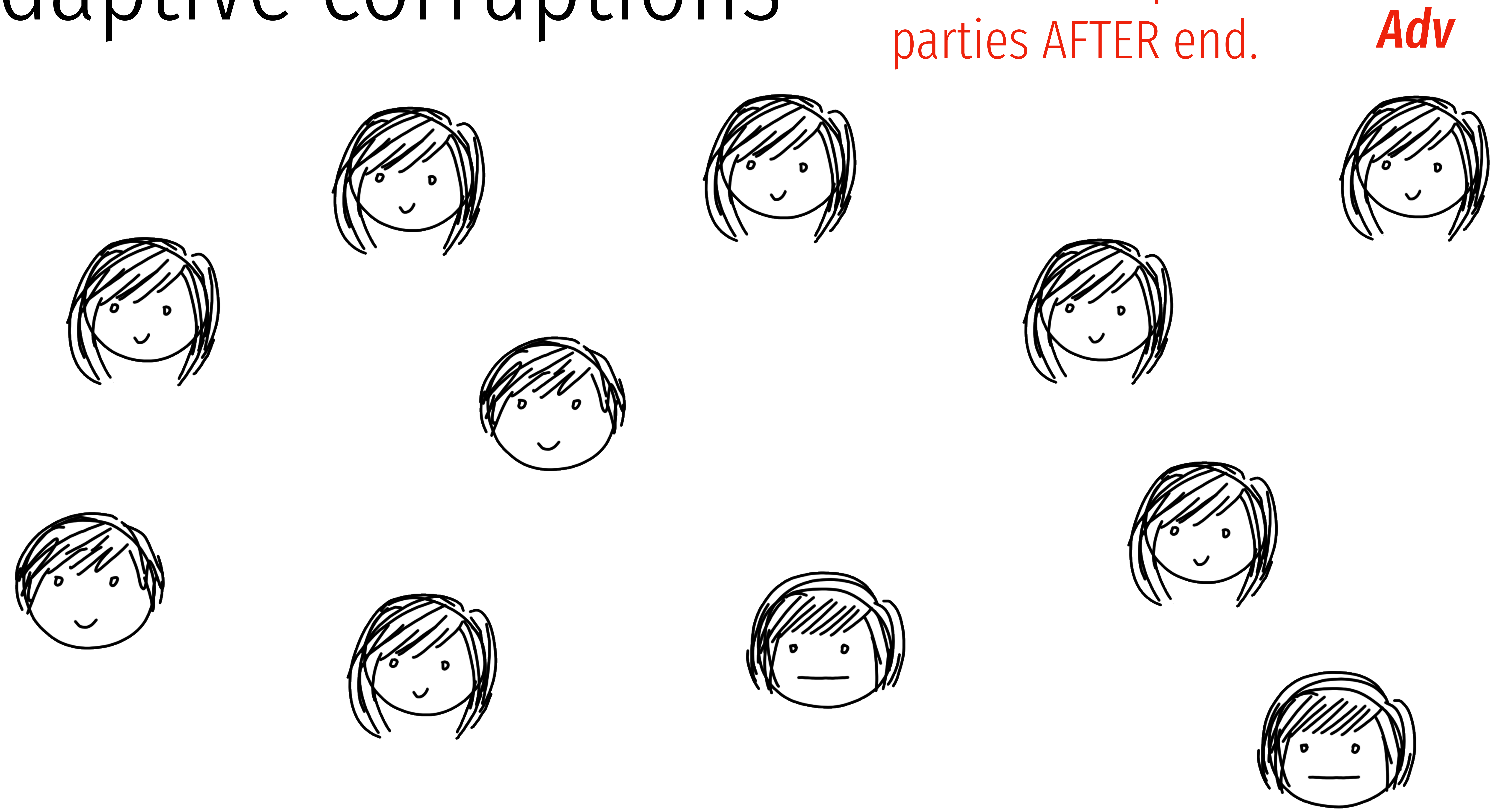
Adaptive corruptions

Adv picks corrupted parties at any time.



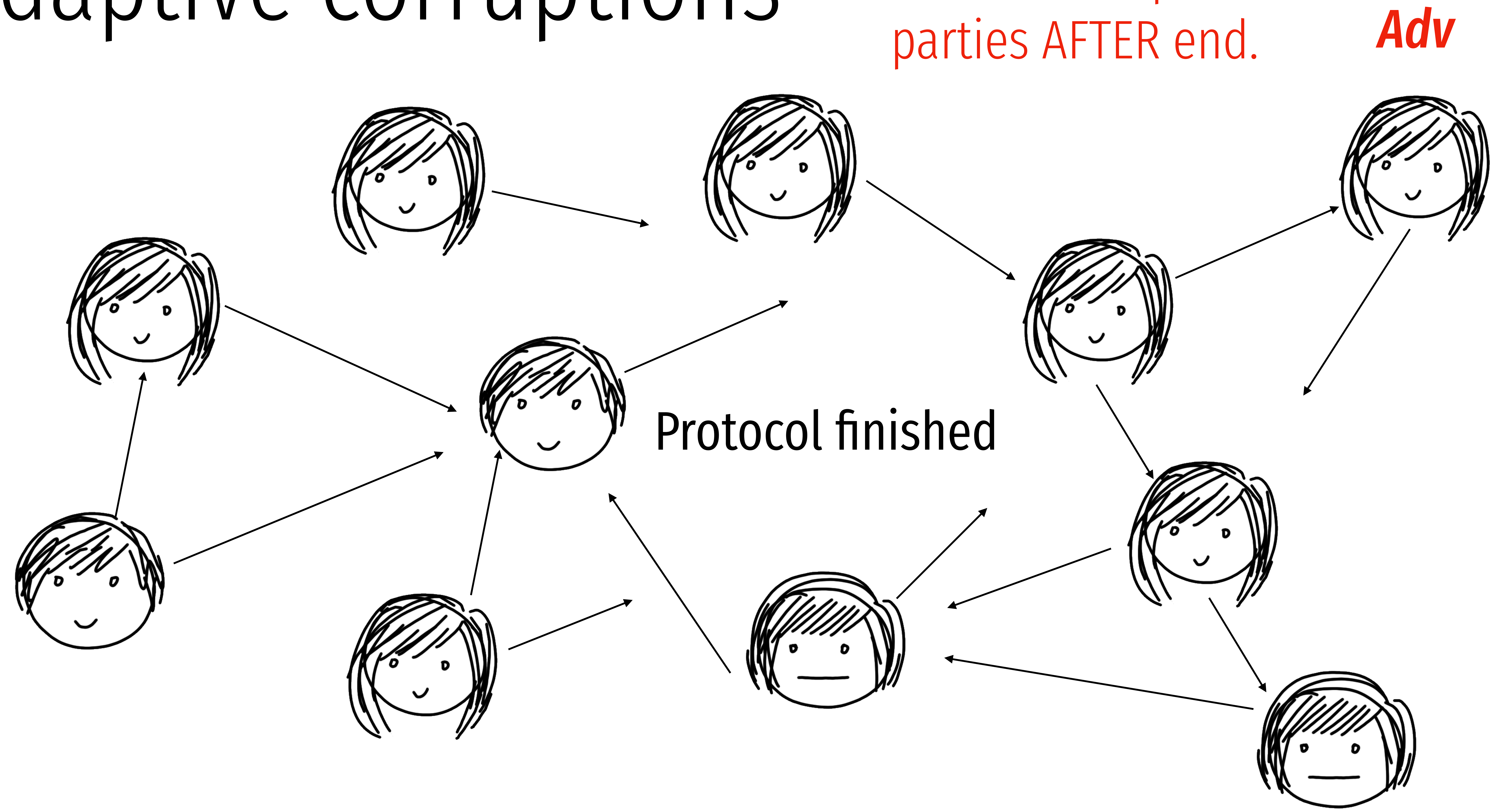
Adaptive corruptions

Adv can corrupt ALL parties AFTER end.



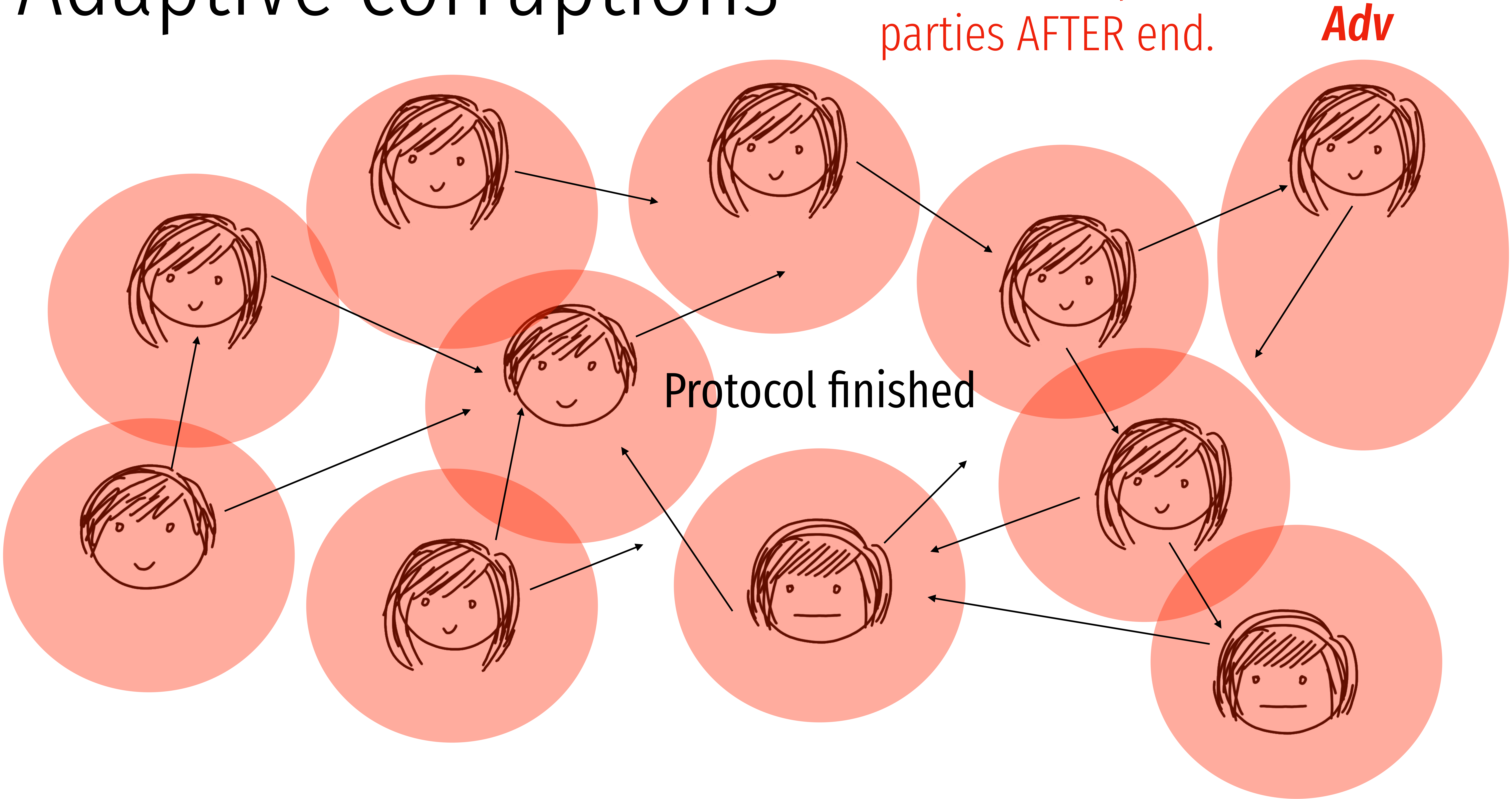
Adaptive corruptions

Adv can corrupt ALL parties AFTER end.



Adaptive corruptions

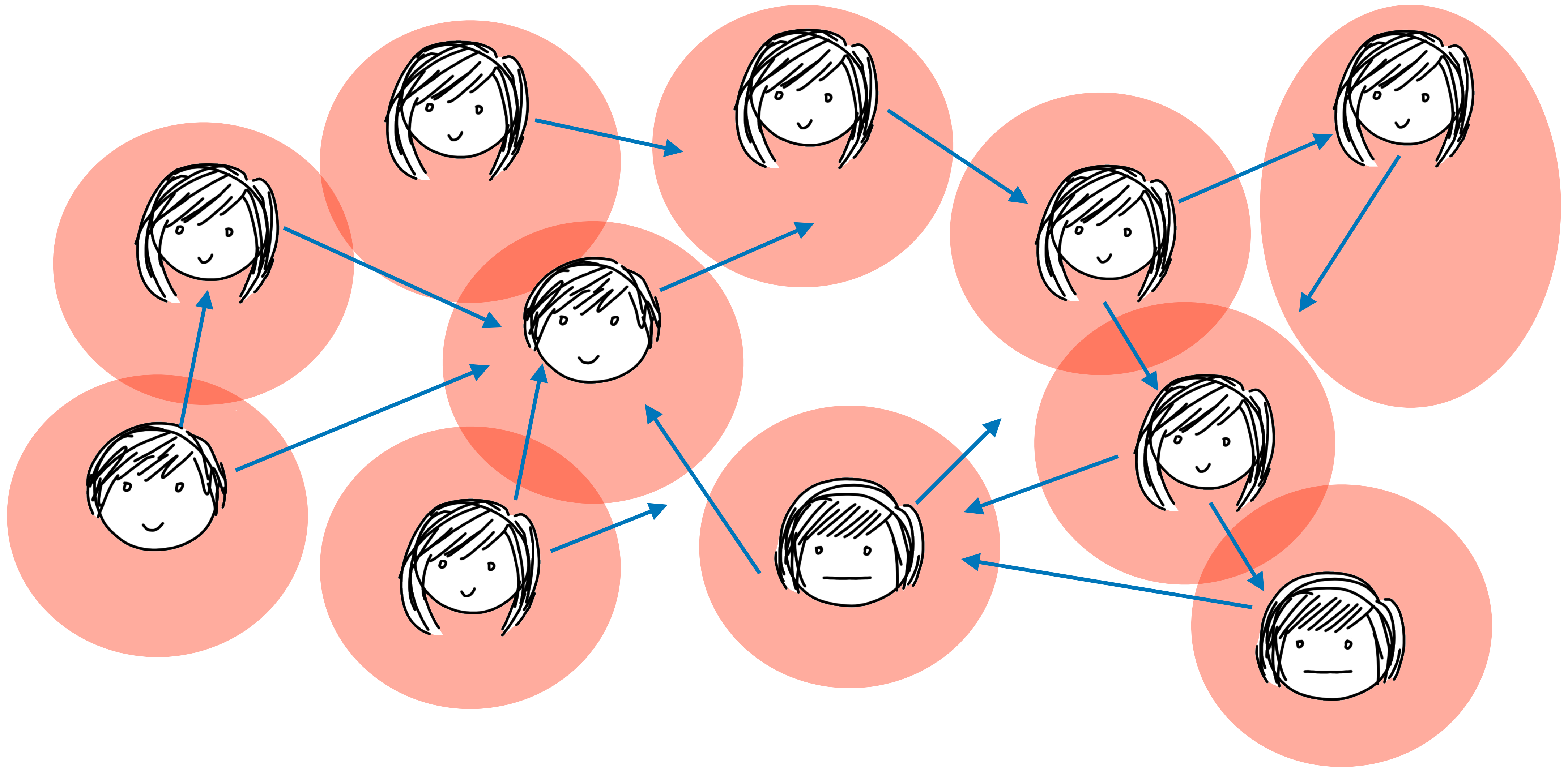
Adv can corrupt ALL parties AFTER end.



Adaptive corruptions

(without erasures)

Adv can corrupt ALL parties AFTER end.



Simulator S must produce transcript T without knowing inputs or outputs.

After corruption, S learns inputs and outputs.

S must explain transcript T by producing random tapes for each party!

At what cost adaptive security?

Partial history (static)

GMW'87
O(d) rounds
OT

BMR'90
O(1) rounds
OT

AJLTVW'12
2 rounds, comm
LWE, NIZK,
Threshold-PKI

GGHR'14
2 rounds
iO, NIZK, CRS

MW'16
2 rounds, comm
LWE, NIZK, CRS

GS'18 / BL'18
2 rounds
OT, CRS

QWW'18
2 rounds
comm & online work
Adaptive-LWE, NIZK, CRS

Partial history (static)

CLOS'02
O(d) rounds
OT, CRS

DKR'15 / CGP'15
O(1) rounds
iO, OT, RefStr

GP'15
2 rounds, o(C) comm
iO,DenEnc,O(C) Ref

CPV'17
O(1) rounds
OT, CRS

BLPV'18
2 rounds, |C|
OT, CRS

GMW'87
O(d) rounds
OT

BMR'90
O(1) rounds
OT

AJLTVW'12
2 rounds, comm
LWE, NIZK,
Threshold-PKI

GGHR'14
2 rounds
iO, NIZK, CRS

MW'16
2 rounds, comm
LWE, NIZK, CRS

GS'18 / BL'18
2 rounds
OT, CRS

QWW'18
2 rounds
comm & online work
Adaptive-LWE, NIZK, CRS

Partial history (static)

CLOS'02
O(d) rounds
OT, CRS

DKR'15 / CGP'15
O(1) rounds
iO, OT, RefStr

GP'15
2 rounds, o(C) comm
iO,DenEnc,O(C) Ref

CPV'17
O(1) rounds
OT, CRS

BLPV'18
2 rounds, |C|
OT, CRS

GMW'87
O(d) rounds
OT

BMR'90
O(1) rounds
OT

AJLTVW'12
2 rounds, comm
LWE, NIZK,
Threshold-PKI

GGHR'14
2 rounds
iO, NIZK, CRS

MW'16
2 rounds, comm
LWE, NIZK, CRS

GS'18 / BL'18
2 rounds
OT, CRS

QWW'18
2 rounds
comm & online work
Adaptive-LWE, NIZK, CRS

RB'89
O(d)
rounds

BMR'90
O(1) rounds
OWF

AJLTVW'12
4 rounds, comm
LWE, NIZK,
Threshold-PKI

GLS'15
2 rounds, comm
LWE, NIZK,
Threshold-PKI

ACGJ'18
3 rounds
PKE, Zaps

Partial history (static)

CLOS'02
O(d) rounds
OT, CRS

DKR'15 / CGP'15
O(1) rounds
iO, OT, RefStr

GP'15
2 rounds, o(C) comm
iO,DenEnc,O(C) Ref

CPV'17
O(1) rounds
OT, CRS

BLPV'18
2 rounds, |C|
OT, CRS

GMW'87
O(d) rounds
OT

BMR'90
O(1) rounds
OT

AJLTVW'12
2 rounds, comm
LWE, NIZK,
Threshold-PKI

GGHR'14
2 rounds
iO, NIZK, CRS

MW'16
2 rounds, comm
LWE, NIZK, CRS

GS'18 / BL'18
2 rounds
OT, CRS

QWW'18
2 rounds
comm & online work
Adaptive-LWE, NIZK, CRS

RB'89
O(d)
rounds

BMR'90
O(1) rounds
OWF

AJLTVW'12
4 rounds, comm
LWE, NIZK,
Threshold-PKI

GLS'15
2 rounds, comm
LWE, NIZK,
Threshold-PKI

ACGJ'18
3 rounds
PKE, Zaps

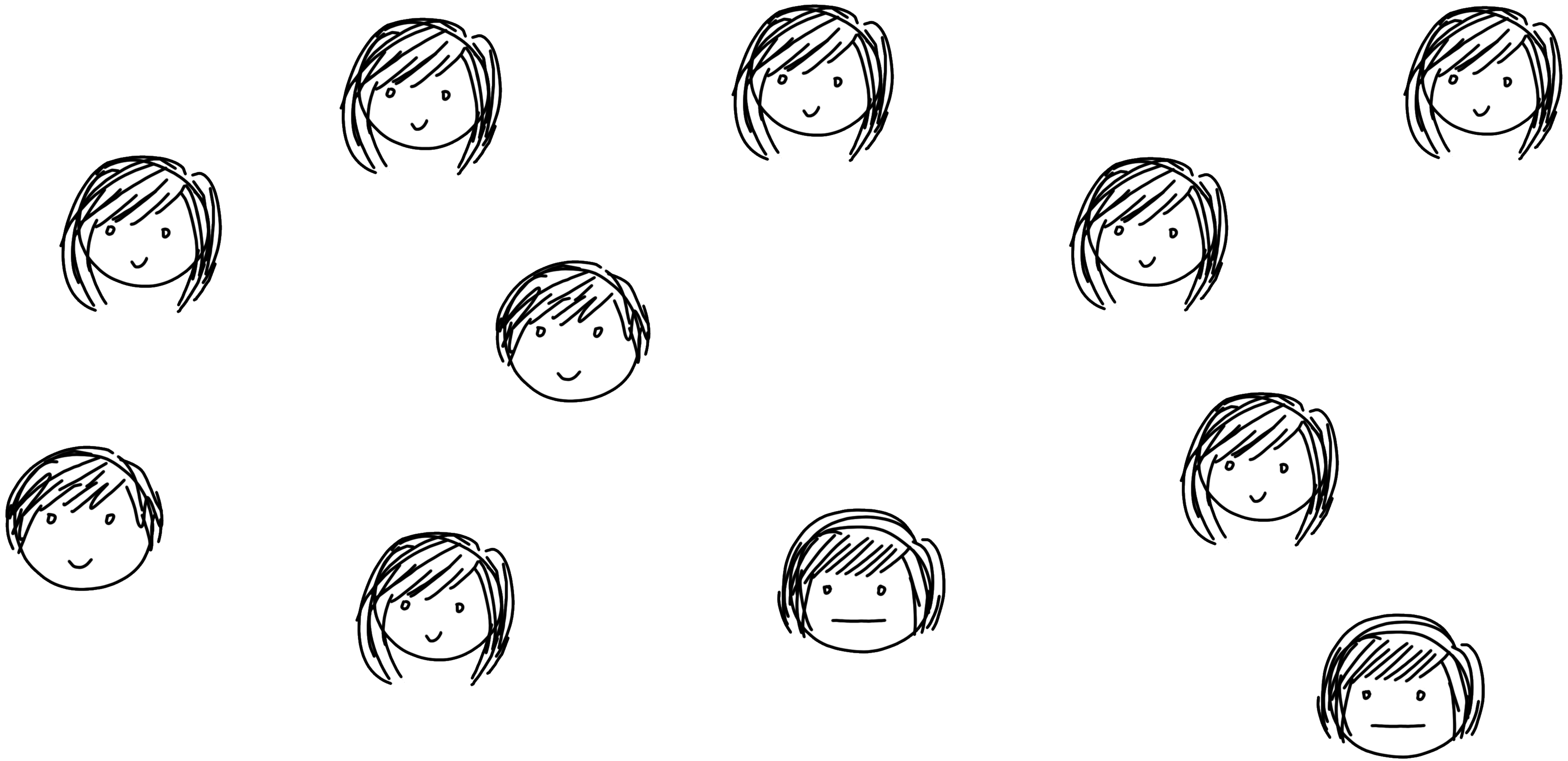
IPS'08
O(1) rounds
OT, CRS

DPR'16
3 rounds, o(C) comm
LWE, NIZK, Threshold-
PKI

CDDHR'99
O(d) rounds

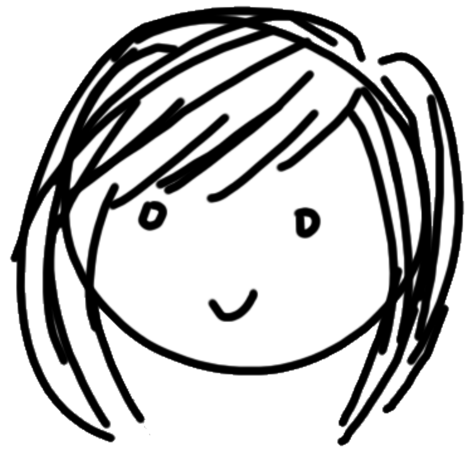
DI'05
O(1) rounds
OWF

Framework for 2-round sub-|C| MPC



Framework for 2-round sub-|C| MPC

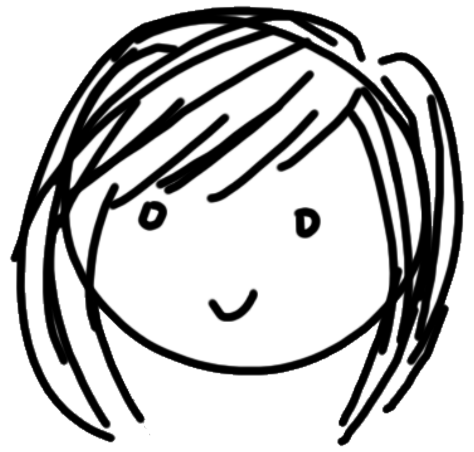
pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i; r)$

Framework for 2-round sub-|C| MPC

pk, sk_i

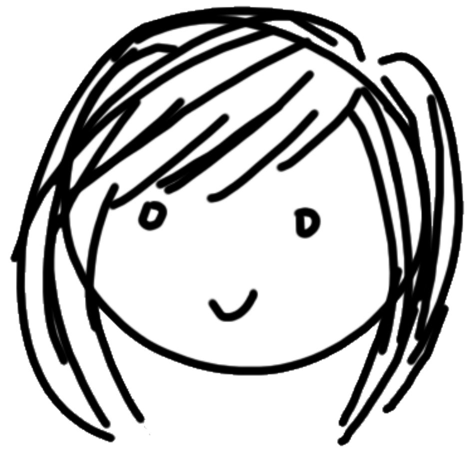


$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i; r)$

(receive c1,...,cn from everyone)

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i; r)$

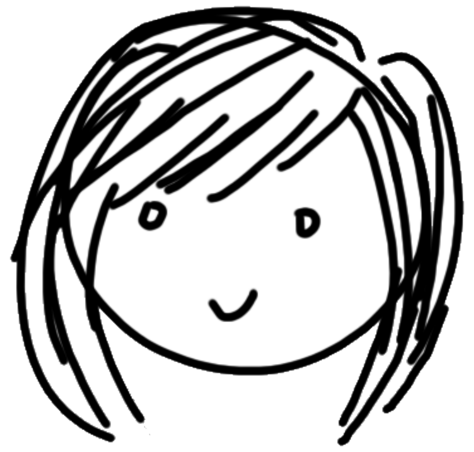
(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y)$

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i; r)$

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

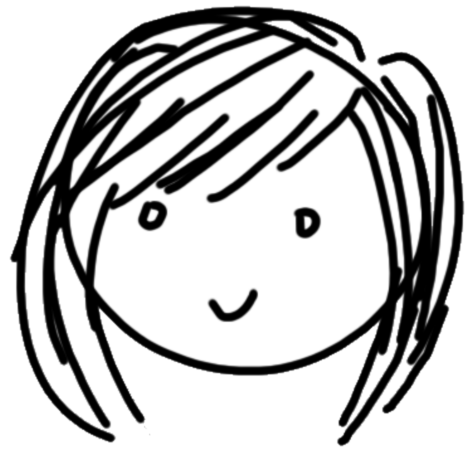
$d_i \leftarrow \mathrm{Dec}_{sk_i}(y)$

d_i

(receive d1,...,dn from everyone)

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i; r)$

(receive c1,…,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

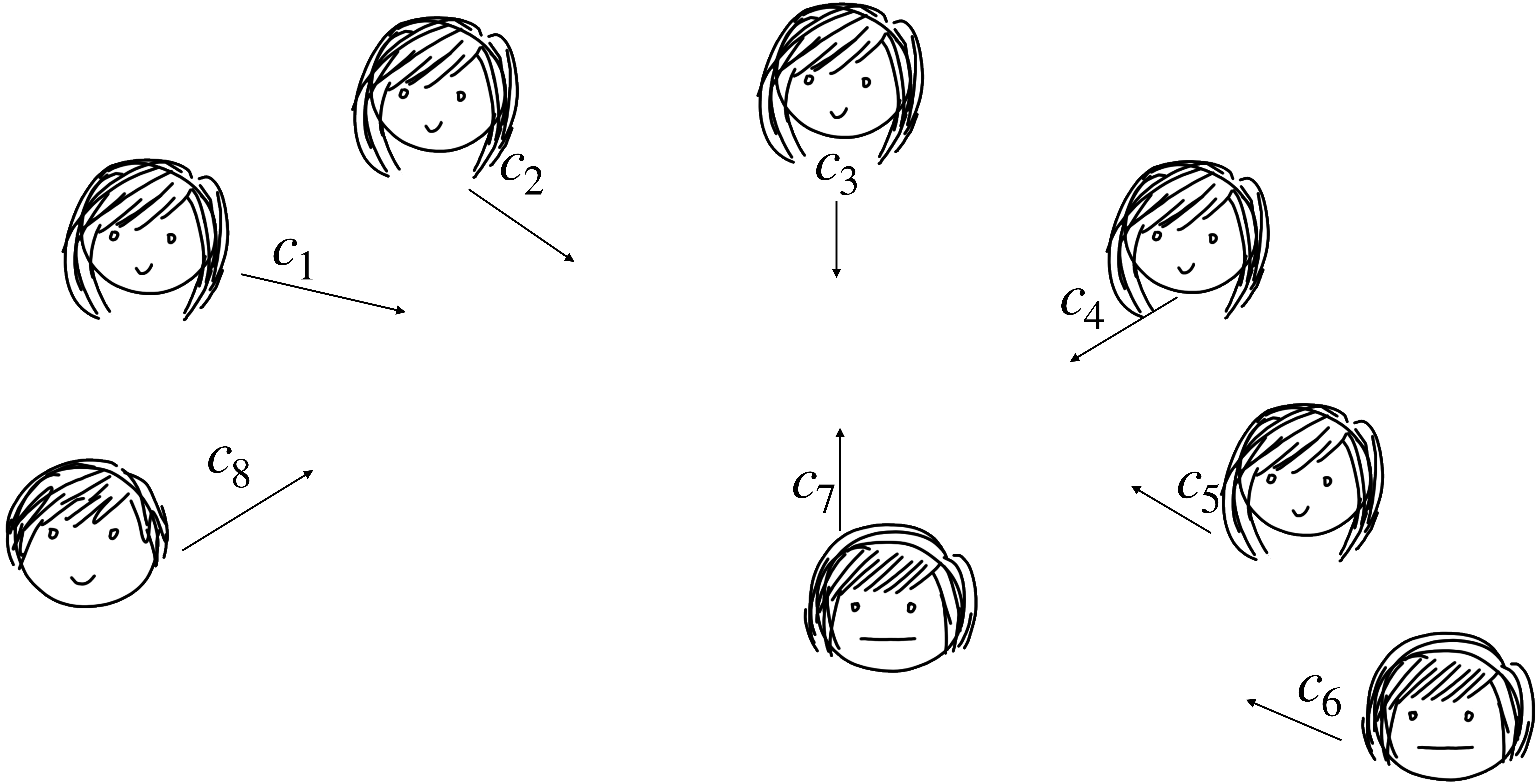
$d_i \leftarrow \mathrm{Dec}_{sk_i}(y)$

d_i

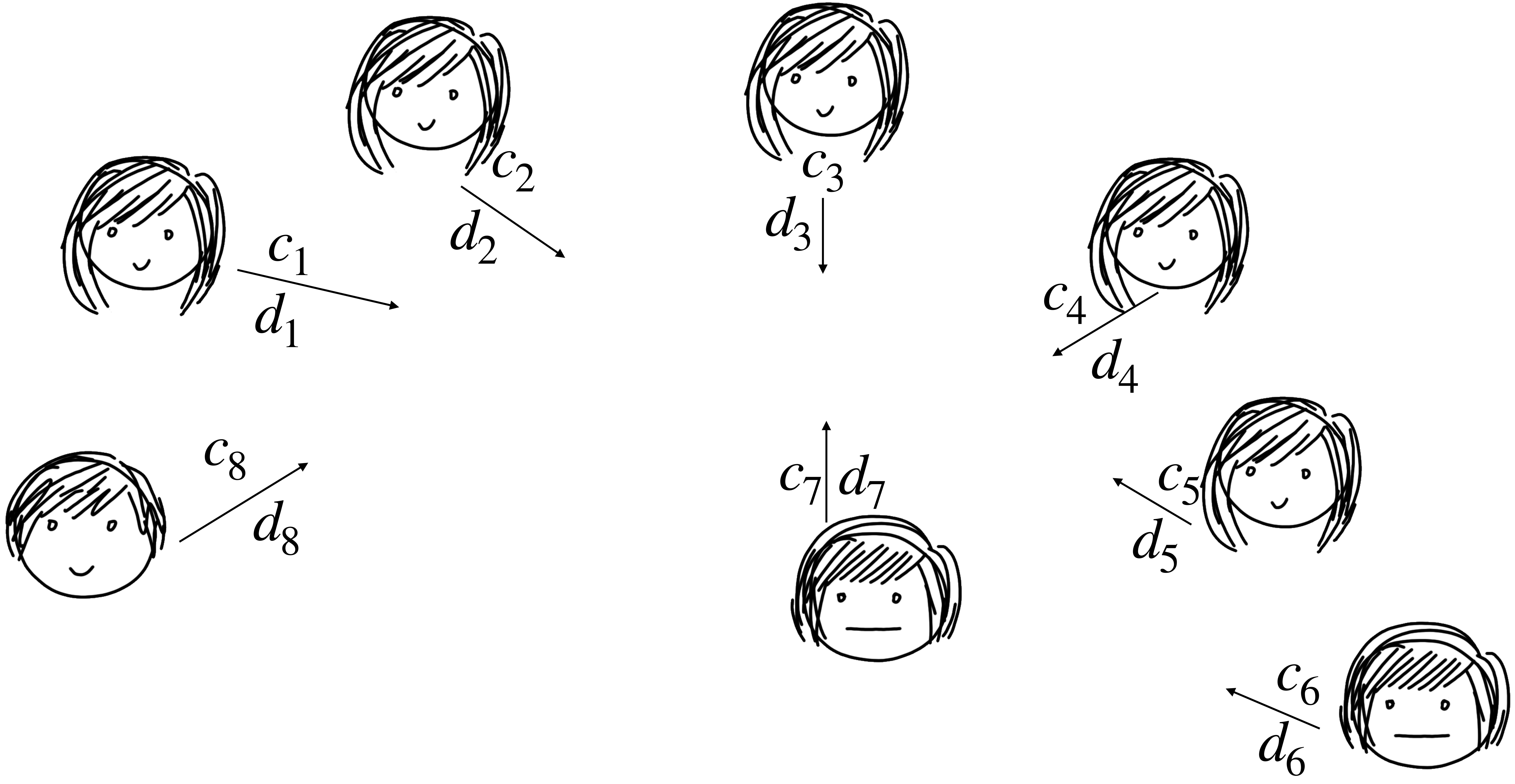
(receive d1,…,dn from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

Framework for 2-round sub-|C| MPC



Framework for 2-round sub-|C| MPC



Adaptive Secure FHE

(sk, pk) <—- Gen(1^k)
Enc, Dec, Eval as usual

$\underline{\mathsf{Ideal}_{\mathcal{A},\mathcal{S}}(k)}$

$$
\begin{aligned}
&(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k);\\
&(m_1, \ldots, m_\ell, \tau) \leftarrow \mathcal{A}_1(1^k);\\
&sk \leftarrow \mathcal{S}_2(s, m_1, \ldots, m_\ell);\\
&b \leftarrow \mathcal{A}_2(\tau, pk, c_1, \ldots, c_\ell, sk);\\
&\mathit{Return}\ b.
\end{aligned}
$$

Adaptive Secure FHE Impossible Katz-Thiruvengadam-Zhou

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$

$$c' \leftarrow \text{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Adaptive Secure FHE Impossible Katz-Thiruvengadam-Zhou

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$
$$c' \leftarrow \text{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Given input $m = (m_1, \ldots, m_\ell)$ compute f(m) as:

Adaptive Secure FHE Impossible

Katz-Thiruvengadam-Zhou

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$

$$c' \leftarrow \mathrm{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Given input $m = (m_1, \ldots, m_\ell)$ compute f(m) as:

$$sk \leftarrow \mathcal{S}_2(s, m_1, \ldots, m_\ell);$$

Adaptive Secure FHE Impossible

Katz-Thiruvengadam-Zhou

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$

$$c' \leftarrow \mathrm{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Given input $m = (m_1, \ldots, m_\ell)$ compute f(m) as:

$$sk \leftarrow \mathcal{S}_2(s, m_1, \ldots, m_\ell);$$

$$f(m) \leftarrow \mathrm{Dec}_{sk}(c')$$

Adaptive Secure FHE Impossible Katz-Thiruvengadam-Zhou

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$
$$c' \leftarrow \mathrm{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Given input $m = (m_1, \ldots, m_\ell)$ compute f(m) as:

$$sk \leftarrow \mathcal{S}_2(s, m_1, \ldots, m_\ell);$$
$$f(m) \leftarrow \mathrm{Dec}_{sk}(c')$$

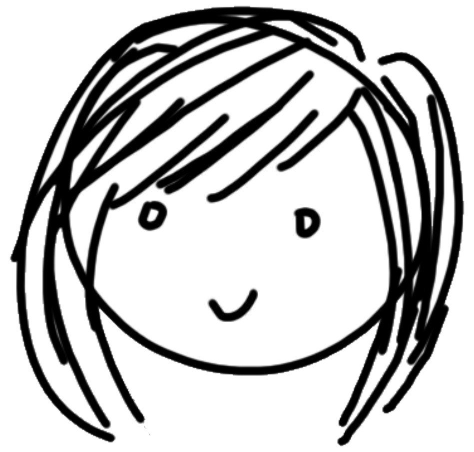
Size of circuit computing f is:

Impossibility of adaptive FHE

Erasures don't help

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i)$ Erase random coins.

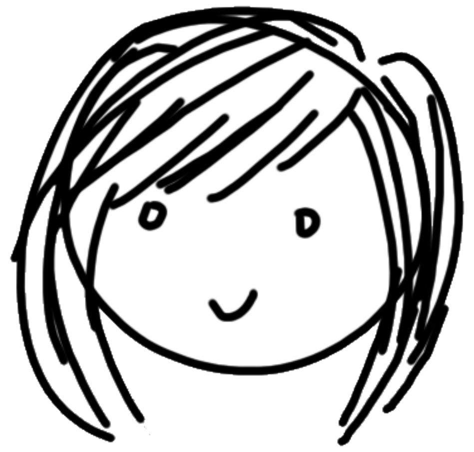
Erase sk_i.

(receive d1,...,dn from everyone)

$f(x_1, \ldots, x_n) \leftarrow \text{Combine}(d_1, \ldots, d_n)$

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i)$ Erase random coins.

(receive c1,...,cn from everyone)

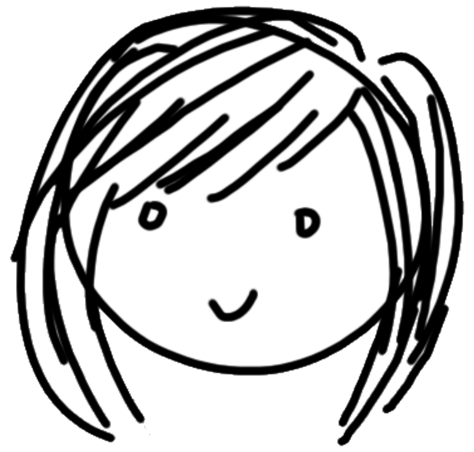
Erase sk_i.

(receive d1,...,dn from everyone)

$f(x_1, \ldots, x_n) \leftarrow \text{Combine}(d_1, \ldots, d_n)$

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i)$ Erase random coins.

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

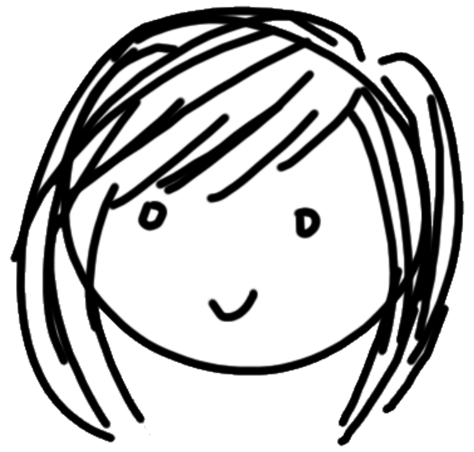
$d_i \leftarrow \mathrm{Dec}_{sk_i}(y)$ Erase sk_i.

(receive d1,...,dn from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

Framework for 2-round sub-|C| MPC

pk, sk_i



$c_i \leftarrow \mathsf{FHE.Enc}_{pk}(x_i)$ Erase random coins.

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y)$ Erase sk_i.

d_i

(receive d1,...,dn from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

Need new ideas for adaptive+succinct

Succinct
But not
Adaptive

Adaptive
but not
Succinct

Succinct
and
Adaptive

Laconic Function Evaluation (LFE)

Quach-Wee-Wichs'18

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, \mathsf{params})$$

Laconic Function Evaluation (LFE)

Quach-Wee-Wichs'18

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, \mathsf{params})$$

$$\mathsf{digest}_C \ = \ \mathsf{LFE.Compress}(\mathsf{crs}, C; r)$$

Laconic Function Evaluation (LFE)

Quach-Wee-Wichs'18

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, \mathsf{params})$$

$$\mathsf{digest}_C \;=\; \mathsf{LFE.Compress}(\mathsf{crs}, C; r)$$

$$\mathsf{ct} \;\leftarrow\; \mathsf{LFE.Enc}(\mathsf{crs}, \mathsf{digest}_C, x)$$

Laconic Function Evaluation (LFE)

Quach-Wee-Wichs'18

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, \mathsf{params})$$

$$\mathsf{digest}_C \;=\; \mathsf{LFE.Compress}(\mathsf{crs}, C; r)$$

$$\mathsf{ct} \;\leftarrow\; \mathsf{LFE.Enc}(\mathsf{crs}, \mathsf{digest}_C, x)$$

$$y = \mathsf{LFE.Dec}(\mathsf{crs}, C, r, \mathsf{ct})$$

LFE Avoids Impossibility

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, \mathsf{params})$$
$$\mathsf{digest}_C = \mathsf{LFE.Compress}(\mathsf{crs}, C; r)$$

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$
$$c' \leftarrow \mathrm{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Given input $m = (m_1, \ldots, m_\ell)$ compute f(m) as:

$$sk \leftarrow \mathcal{S}_2(s, m_1, \ldots, m_\ell);$$
$$f(m) \leftarrow \mathrm{Dec}_{sk}(c')$$

$$\mathsf{ct} \leftarrow \mathsf{LFE.Enc}(\mathsf{crs}, \mathsf{digest}_C, x)$$
$$y = \mathsf{LFE.Dec}(\mathsf{crs}, C, r, \mathsf{ct})$$

Fully Adaptive Succinct MPC

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, f.\mathsf{params})$$

Succinct

Fully Adaptive Succinct MPC

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, f.\mathsf{params})$$

Succinct

$$\mathsf{digest}_f = \mathsf{LFE.Compress}(\mathsf{crs}, C_f)$$

Fully Adaptive Succinct MPC

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, f.\mathsf{params})$$

Succinct

$$\mathsf{digest}_f = \mathsf{LFE.Compress}(\mathsf{crs}, C_f)$$

$$\mathcal{F}^{\mathsf{LFE.Enc}}_{\mathsf{sfe\text{-}abort}}(\mathsf{input}, \mathsf{sid}, (\mathsf{crs}, \mathsf{digest}_f, x_i, r_i)).$$

Fully Adaptive Succinct MPC

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, f.\mathsf{params})$$

Succinct

$$\mathsf{digest}_f = \mathsf{LFE.Compress}(\mathsf{crs}, C_f)$$

$$\mathcal{F}^{\mathsf{LFE.Enc}}_{\mathsf{sfe\text{-}abort}}(\mathsf{input}, \mathsf{sid}, (\mathsf{crs}, \mathsf{digest}_f, x_i, r_i)).$$

Benhamouda-Lin-Polychroniado-Muthu

C_f

Fully Adaptive Succinct MPC

$$\text{crs} \leftarrow \text{LFE.crsGen}(1^\kappa, f.\text{params})$$

Succinct

$$\text{digest}_f = \text{LFE.Compress}(\text{crs}, C_f)$$

$$\mathcal{F}^{\text{LFE.}\check{\text{E}}\text{nc}}_{\text{sfe-abort}}(\text{input}, \text{sid}, (\text{crs}, \text{digest}_f, x_i, r_i)).$$

Benhamouda-Lin-Polychroniado-Muthu

C_f

$$y = \text{LFE.Dec}(\text{crs}, C_f, \text{ct})$$ Erase ri.

Fully Adaptive Succinct MPC

$$\mathsf{crs} \leftarrow \mathsf{LFE.crsGen}(1^\kappa, f.\mathsf{params})$$

Succinct

$$\mathsf{digest}_f = \mathsf{LFE.Compress}(\mathsf{crs}, C_f)$$

$$\mathcal{F}_{\mathsf{sfe\text{-}abort}}^{\mathsf{LFE.\check{E}nc}}(\mathsf{input}, \mathsf{sid}, (\mathsf{crs}, \mathsf{digest}_f, x_i, r_i)).$$

Benhamouda-Lin-Polychroniado-Muthu

C_f

$$y = \mathsf{LFE.Dec}(\mathsf{crs}, C_f, \mathsf{ct})$$ Erase ri.

LFE is all-but-one adaptive secure.

Removing erasures

Explainability Compiler

Dachman-Soled—Katz-Rao'15

$$\mathsf{EC}(\mathrm{Alg}) \to (\widetilde{\mathrm{Alg}}, \mathsf{Explain})$$

Explainability Compiler

Dachman-Soled—Katz-Rao'15

$$\text{EC}(\text{Alg}) \rightarrow (\widetilde{\text{Alg}}, \text{Explain})$$

Poly-time overhead

Explainability Compiler

Dachman-Soled–Katz-Rao'15

$$\mathsf{EC}(\mathrm{Alg}) \to (\widetilde{\mathrm{Alg}}, \mathsf{Explain})$$

Poly-time overhead

Correctness: $\mathrm{Alg}(x) \approx \widetilde{\mathrm{Alg}}(x) \quad \forall x$

Explainability Compiler

Dachman-Soled—Katz-Rao'15

$$\text{EC}(\mathrm{Alg}) \rightarrow (\widetilde{\mathrm{Alg}}, \text{Explain})$$

Poly-time overhead

Correctness: $\mathrm{Alg}(x) \approx \widetilde{\mathrm{Alg}}(x) \quad \forall x$

For any input/output (x,y), **Explain** produces coins r s.t. ~Alg(x,r) = y

Explainability Compiler

Dachman-Soled—Katz-Rao'15

$$\mathsf{EC}(\mathrm{Alg}) \to (\widetilde{\mathrm{Alg}}, \mathsf{Explain})$$

Poly-time overhead

Correctness: $\mathrm{Alg}(x) \approx \widetilde{\mathrm{Alg}}(x) \quad \forall x$

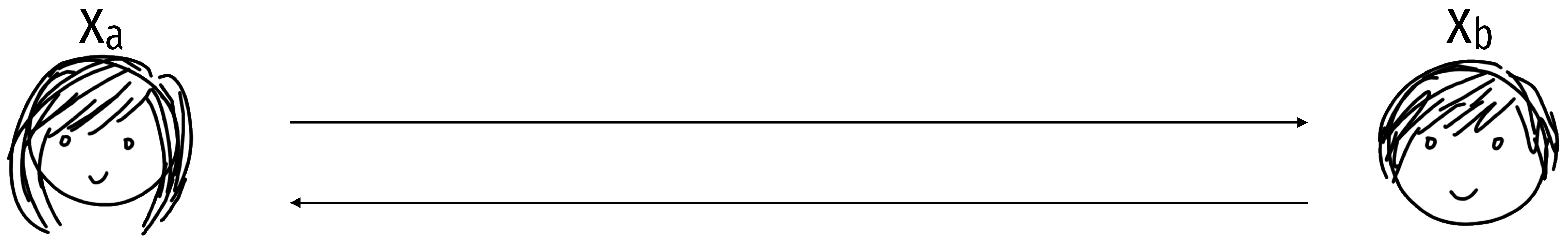
For any input/output (x,y), **Explain** produces coins r s.t. ~Alg(x,r) = y

Corollary A.7. *Assuming the existence of an indistinguishable obfuscator for* P/poly *and of one-way functions, both with sub-exponential security, there exists an explainability compiler with adaptive security for* P/poly.

Fully-adaptive summary

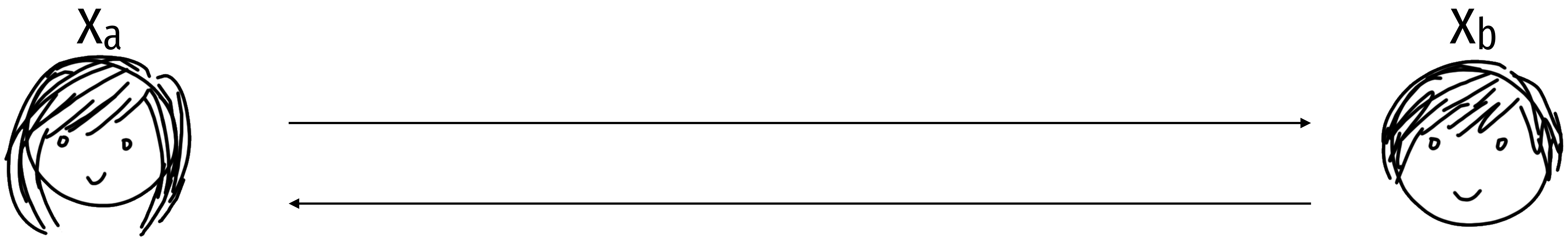
Protocol	Security (erasures)	Rounds	Communication	Online Computation	Setup size	Setup type	Assumption
MW [79]	static	2	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	$\text{poly}(\|C\|, \kappa)$	$\text{poly}(\kappa, d)$	CRS	LWE, NIZK
QWW [85] ABJMS [3]	static	2	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	$\text{poly}(\kappa, d)$	CRS	ALWE LWE
CLOS [24]	adaptive(no)	$O(d)$	$\|C\| \cdot \text{poly}(\kappa, n)$	$\text{poly}(\|C\|, \kappa)$	$\text{poly}(\kappa)$	CRS	TDP, NCE dense-crypto
GS [50]*	adaptive(no)	$O(d)$	$\|C\| \cdot \text{poly}(\kappa, n)$	$\text{poly}(\|C\|, \kappa)$	-	-	CRH TDP, NCE dense-crypto
DKR [40] CGP [27]	adaptive(no)	$O(1)$	$\|C\| \cdot \text{poly}(\kappa, n)$	$\text{poly}(\|C\|, \kappa)$	$\text{poly}(\|C\|, \kappa)$	Ref	OWF, iO
GP [49]	adaptive(no)	2	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, \kappa, n)$	$\text{poly}(\|C\|, \kappa)$	$\text{poly}(\|C\|, \kappa)$	Ref	OWF, iO
CPV [30]	adaptive(no)	$O(1)$	$\|C\| \cdot \text{poly}(\kappa, n)$	$\text{poly}(\|C\|, \kappa)$	$\text{poly}(\kappa)$	CRS	NCE dense-crypto
BLPV [13]	adaptive(no)	2	$\|C\| \cdot \text{poly}(\kappa, n)$	$\text{poly}(\|C\|, \kappa)$	$\text{poly}(\kappa)$	Ref	adaptive 2-round OT
This work	adaptive(yes) adaptive(no)	2	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	$\text{poly}(\kappa, d)$ $\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	CRS Ref	ALWE ALWE, iO

Alice-optimal



Alice learns $y = f(x_a, x_b)$

Alice-optimal



Alice learns $y = f(x_a, x_b)$

Comm: |xa| + |y|

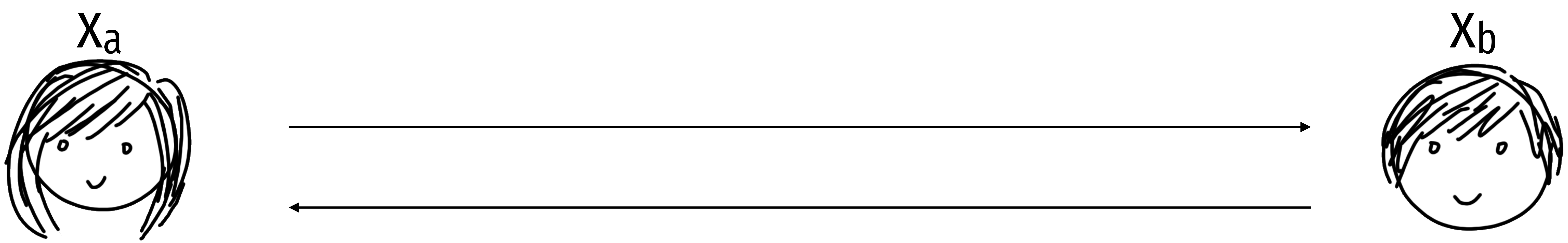
Comp: |f|

Comp: |xa| + |y|

Bob-optimal

Alice learns $y = f(x_a, x_b)$

Bob-optimal



Alice learns $y = f(x_a, x_b)$

Comp: $|f|$

Comm: $|x_b| + |y|$

Comp: $|x_b| + |y|$

Approach	**Security** (erasures)	**CRS**	**Communication** Alice	Bob	**Computation** Alice	Bob	**Assumptions**
GC [92]	static	-	ℓ_A	$\|f\|$	$\|f\|$	$\|f\|$	static OT
LOT [32]	static	$O(1)$	$O(1)$	$\|f\|$	$\|f\|$	$\|f\|$	DDH, etc.
FHE [52]	static	-	ℓ_A	ℓ_{out}	$\ell_A + \ell_{\mathsf{out}}$	$\|f\|$	LWE
LFE [85]	static	$O(1)$	$O(1)$	$\ell_B + \ell_{\mathsf{out}}$	$\|f\|$	$\ell_B + \ell_{\mathsf{out}}$	ALWE
equivocal GC [30]	adaptive (no)	-	ℓ_A	$\|f\|$	$\|f\|$	$\|f\|$	adaptive OT
This work	adaptive (yes)	$O(1)$	$O(1)$	$\ell_B + \ell_{\mathsf{out}}$	$\|f\|$	$\ell_B + \ell_{\mathsf{out}}$	ALWE
	adaptive (no)	$\ell_B + \ell_{\mathsf{out}}$	$O(1)$	$\ell_B + \ell_{\mathsf{out}}$	$\|f\|$	$\ell_B + \ell_{\mathsf{out}}$	ALWE and iO
	adaptive (yes)	$\|f\|$	$\|f\|$	$\ell_{\mathsf{out}} + o(\ell_B)$	$\|f\|$	$\|f\|$	impossible

Table 2: Comparison of two-message semi-honest protocols for $f : \{0,1\}^{\ell_A} \times \{0,1\}^{\ell_B} \to \{0,1\}^{\ell_{\mathsf{out}}}$. Alice talks first, Bob the second, and only Alice learns the output. For simplicity, multiplicative factors that are polynomial in the security parameter κ or the circuit depth d are suppressed.

At what cost lesser adaptive security?

Adaptive UC-NIZK

Groth-Ostrovsky-Sahai

Using bilinear pairings, Adaptive NIZK of size |C|*poly(k).

Succinct NIZK

Gentry-Groth-Ishai-Peikert-Sahai-Smith

NIZK crs

Prover(x,w)

sk,pk = FHE.Gen(r)

v_i = FHE.Enc_{pk}(w_i)

{v_i}, pi →

u* = FHE.$Eval_{pk}$(R,x,w_i,…w_i)

pi = Nizk{ FHE.Dec(sk,u*) = 1 }

Succinct + Adaptive NIZK ?

Homomorphic Trapdoor Function

Gorbunov-Vinod-Wichs

$$(pk, sk) \leftarrow \mathsf{HTDF.Gen}(1^k, 1^d)$$

$$f_{\mathsf{pk},x} : \mathcal{U} \to \mathcal{V}$$

$$\mathsf{HTDF.Inv}_{\mathsf{sk},x} : \check{\mathcal{V}} \to \mathcal{U}.$$

Homomorphic Trapdoor Function

Gorbunov-Vinod-Wichs

$$(pk, sk) \leftarrow \mathsf{HTDF.Gen}(1^k, 1^d)$$

$$f_{\mathsf{pk},x} : \mathcal{U} \to \mathcal{V},$$

$$\mathsf{HTDF.Inv}_{\mathsf{sk},x} : \mathcal{V} \to \mathcal{U}.$$

$$\mathsf{HTDF.Eval}^{\mathsf{in}}(g, (x_1, u_1), \ldots, (x_\ell, u_\ell))$$

$$v^* = \mathsf{HTDF.Eval}^{\mathsf{out}}(g, v_1, \ldots, v_\ell).$$

Impossibility doesn't apply to HTDF

$$(pk, c_1, \ldots, c_\ell, s) \leftarrow \mathcal{S}_1(1^k)$$

$$c' \leftarrow \mathrm{Eval}_{\mathsf{pk}}(C_f, c_1, \ldots, c_\ell)$$

Given input $m = (m_1, \ldots, m_\ell)$ compute f(m) as:

$$sk \leftarrow \mathcal{S}_2(s, m_1, \ldots, m_\ell);$$

$$f(m) \leftarrow \mathrm{Dec}_{sk}(c')$$

Size of circuit computing f is:

Succinct Adaptive NIZK

crs = HTDF.pk

Prover(x,w)

$v_i = \mathrm{HTDF}_{pk}(w_i)$

Succinct Adaptive NIZK

crs = HTDF.pk

Prover(x,w)

$v_i = \text{HTDF}_{pk}(w_i)$

$u^* = \text{HTDF.Eval}_{pk}(R,x,w_i,\ldots w_i)$

Succinct Adaptive NIZK

crs = HTDF.pk

Prover(x,w)

$v_i = HTDF_{pk}(w_i)$

$u^* = HTDF.Eval_{pk}(R,x,w_i,\ldots w_i)$

$v^* = HTDF.Eval_{pk}(R,x,v_i,..,v_i)$

Succinct Adaptive NIZK

crs = HTDF.pk

Prover(x,w)

v_i = $HTDF_{pk}(w_i)$

u* = $HTDF.Eval_{pk}(R,x,w_i,...w_i)$

v* = $HTDF.Eval_{pk}(R,x,v_i,..,v_i)$

pi = Adp-Nizk{$f_{pk}(u^*) = v^*$}

Succinct Adaptive NIZK

crs = HTDF.pk

Prover(x,w)

v_i = $HTDF_{pk}(w_i)$

$\{v_i\}$, pi →

u^* = $HTDF.Eval_{pk}(R,x,w_i,...w_i)$

v^* = $HTDF.Eval_{pk}(R,x,v_i,..,v_i)$

pi = Adp-Nizk$\{f_{pk}(u^*) = v^*\}$

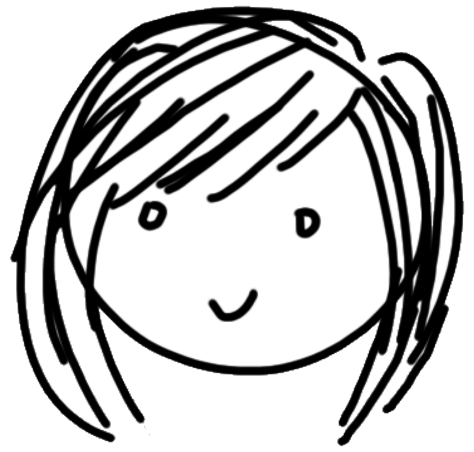
Adaptive NIZK

Protocol	Security (erasures)	CRS size	Proof size	Assumptions
Groth [60]	static	$\|C\| \cdot \text{poly}(\kappa)$	$\|C\| \cdot \text{poly}(\kappa)$	TDP
Groth [60]	static	$\|C\| \cdot \text{polylog}(\kappa) + \text{poly}(\kappa)$	$\|C\| \cdot \text{poly}(\kappa)$	Naccache-Stern
GOS [61]	adaptive (no)	$\text{poly}(\kappa)$	$\|C\| \cdot \text{poly}(\kappa)$	pairing based
Gentry [52]	adaptive (yes)	$\text{poly}(\kappa)$	$\|w\| \cdot \text{poly}(\kappa, d)$	LWE, NIZK
GGIPSS [56]	adaptive (yes)	$\text{poly}(\kappa)$	$\|w\| + \text{poly}(\kappa, d)$	LWE, NIZK
This work	adaptive (no)	$\text{poly}(\kappa)$	$\|w\| \cdot \text{poly}(\kappa, d)$	LWE, NIZK

Table 3: NIZK arguments with security parameter κ, for circuit size $|C|$, depth d, and witness size $|w|$.

All-but-one in 2 rounds

pk, sk_i



$c_i \leftarrow \mathsf{TEFHE.Enc}_{pk}(x_i), s = [0]$

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

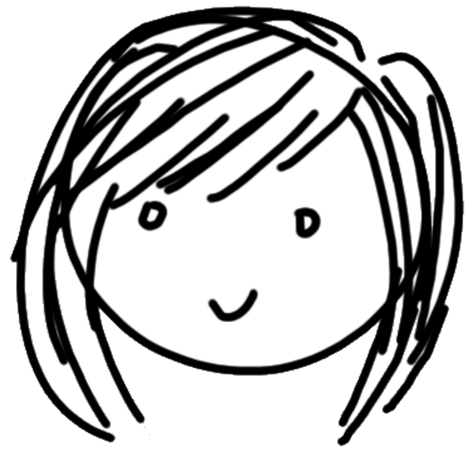
(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

+ Adaptive NIZK for malicious security

All-but-one in 2 rounds

pk, sk_i



$c_i \leftarrow \mathsf{TEFHE.Enc}_{pk}(x_i), s = [0]$

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$
$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

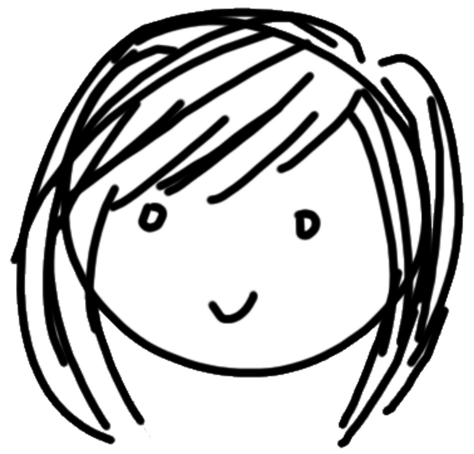
(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

+ Adaptive NIZK for malicious security

All-but-one in 2 rounds

pk, sk_i



$c_i \leftarrow \mathsf{TEFHE.Enc}_{pk}(x_i), s = [0]$

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

$d_i + s_i$

(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

+ Adaptive NIZK for malicious security

All-but-one corruptions

Protocol	Security	Rounds	Communication	Assumptions	Setup
AJLTVW [5]	static	2 3	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI CRS
MW [79]	static	2	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	LWE, NIZK	CRS
IPS [70]	adaptive	$O(1)$	$\|C\| + \mathrm{poly}(d, \log \|C\|, \kappa, n)$	OT-hybrid	-
GS [50]	adaptive	$O(1)$	$\|C\| + \mathrm{poly}(d, \log \|C\|, \kappa, n)$	CRH, TDP, NCE dense crypto	-
DPR [45]	adaptive	3	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI
This work	adaptive	2 4	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI CRS

Table 4: Comparison of maliciously secure MPC for $f : (\{0,1\}^{\ell_{\mathsf{in}}})^n \to \{0,1\}^{\ell_{\mathsf{out}}}$ represented by a circuit C of depth d, tolerating $n-1$ corruptions. $(*)$ The results in [50] only hold in the stand-alone model.

Honest majority results

Protocol	Security	Rounds	Communication	Assumptions	Setup
AJLTVW [5]	static	4 5	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI CRS
GLS [59]	static	2 3	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI CRS
ACGJ [4]	static	3	$\|C\| \cdot \text{poly}(\kappa, n)$	PKE and zaps	-
BJMS [6]	static	2 3	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, zaps, dense crypto	threshold PKI -
DI [41]	adaptive	$O(1)$	$\|C\| \cdot \text{poly}(\kappa, n)$	OWF	-
This work	adaptive	2 $O(1)$	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI -

Table 5: Comparison of maliciously secure MPC for $f : (\{0,1\}^{\ell_{\text{in}}})^n \to \{0,1\}^{\ell_{\text{out}}}$ represented by circuit C of depth d, in the honest-majority setting.

Open questions

Are erasures/io necessary for adaptive succinct MPC?

Protocol	Security (erasures)	Rounds	Communication	Online Computation	Setup size	Setup type	Assumption
MW [79]	static	2	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	$\mathrm{poly}(\kappa, d)$	CRS	LWE, NIZK
QWW [85] ABJMS [3]	static	2	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathrm{poly}(\kappa, d)$	CRS	ALWE LWE
CLOS [24]	adaptive(no)	$O(d)$	$\lvert C\rvert \cdot \mathrm{poly}(\kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	$\mathrm{poly}(\kappa)$	CRS	TDP, NCE dense-crypto
GS [50]*	adaptive(no)	$O(d)$	$\lvert C\rvert \cdot \mathrm{poly}(\kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	-	-	CRH TDP, NCE dense-crypto
DKR [40] CGP [27]	adaptive(no)	$O(1)$	$\lvert C\rvert \cdot \mathrm{poly}(\kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	Ref	OWF, iO
GP [49]	adaptive(no)	2	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, \kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	Ref	OWF, iO
CPV [30]	adaptive(no)	$O(1)$	$\lvert C\rvert \cdot \mathrm{poly}(\kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	$\mathrm{poly}(\kappa)$	CRS	NCE dense-crypto
BLPV [13]	adaptive(no)	2	$\lvert C\rvert \cdot \mathrm{poly}(\kappa, n)$	$\mathrm{poly}(\lvert C\rvert, \kappa)$	$\mathrm{poly}(\kappa)$	Ref	adaptive 2-round OT
This work	adaptive(yes) adaptive(no)	2	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathrm{poly}(\kappa, d)$ $\mathrm{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	CRS Ref	ALWE ALWE, iO

Open questions

Are erasures/io necessary for adaptive succinct MPC?

Are Ref strings/erasures necessary for fully adaptive succinct MPC?

Protocol	Security (erasures)	Rounds	Communication	Online Computation	Setup size	Setup type	Assumption
MW [79]	static	2	$\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	$\mathsf{poly}(\kappa, d)$	CRS	LWE, NIZK
QWW [85] ABJMS [3]	static	2	$\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathsf{poly}(\kappa, d)$	CRS	ALWE LWE
CLOS [24]	adaptive(no)	$O(d)$	$\lvert C \rvert \cdot \mathsf{poly}(\kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	$\mathsf{poly}(\kappa)$	CRS	TDP, NCE dense-crypto
GS [50]*	adaptive(no)	$O(d)$	$\lvert C \rvert \cdot \mathsf{poly}(\kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	-	-	CRH TDP, NCE dense-crypto
DKR [40] CGP [27]	adaptive(no)	$O(1)$	$\lvert C \rvert \cdot \mathsf{poly}(\kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	Ref	OWF, iO
GP [49]	adaptive(no)	2	$\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, \kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	Ref	OWF, iO
CPV [30]	adaptive(no)	$O(1)$	$\lvert C \rvert \cdot \mathsf{poly}(\kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	$\mathsf{poly}(\kappa)$	CRS	NCE dense-crypto
BLPV [13]	adaptive(no)	2	$\lvert C \rvert \cdot \mathsf{poly}(\kappa, n)$	$\mathsf{poly}(\lvert C \rvert, \kappa)$	$\mathsf{poly}(\kappa)$	Ref	adaptive 2-round OT
This work	adaptive(yes) adaptive(no)	2	$\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	$\mathsf{poly}(\kappa, d)$ $\mathsf{poly}(\ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, \kappa, n)$	CRS Ref	ALWE ALWE, iO

Open questions

Are erasures/io necessary for adaptive succinct MPC?

Are Ref strings/erasures necessary for fully adaptive succinct MPC?

Are setup relaxations possible for all-but-one adaptive succinct MPC?

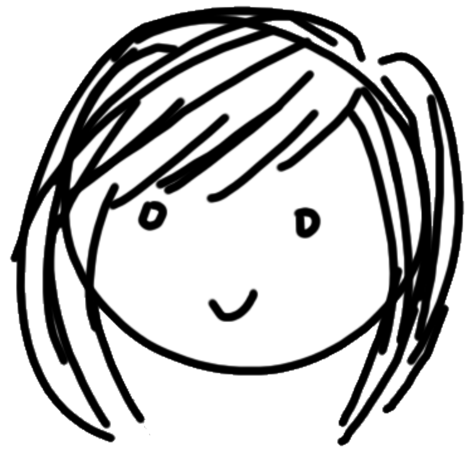
Protocol	Security	Rounds	Communication	Assumptions	Setup
AJLTVW [5]	static	2 3	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI CRS
MW [79]	static	2	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	CRS
IPS [70]	adaptive	$O(1)$	$\lvert C\rvert + \text{poly}(d, \log \lvert C\rvert, \kappa, n)$	OT-hybrid	-
GS [50]	adaptive	$O(1)$	$\lvert C\rvert + \text{poly}(d, \log \lvert C\rvert, \kappa, n)$	CRH, TDP, NCE dense crypto	-
DPR [45]	adaptive	3	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI
This work	adaptive	2 4	$\text{poly}(\ell_{\text{in}}, \ell_{\text{out}}, d, \kappa, n)$	LWE, NIZK	threshold PKI CRS

Table 4: Comparison of maliciously secure MPC for $f : (\{0,1\}^{\ell_{\text{in}}})^n \to \{0,1\}^{\ell_{\text{out}}}$ represented by a circuit C of depth d, tolerating $n-1$ corruptions. $(*)$ The results in [50] only hold in the stand-alone model.

All-but-one corruptions prior work

Damgard-Polychroniadou-Rao

pk, sk_i



$c_i \leftarrow \mathsf{EquivFHE.Enc}_{pk}(x_i)$

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

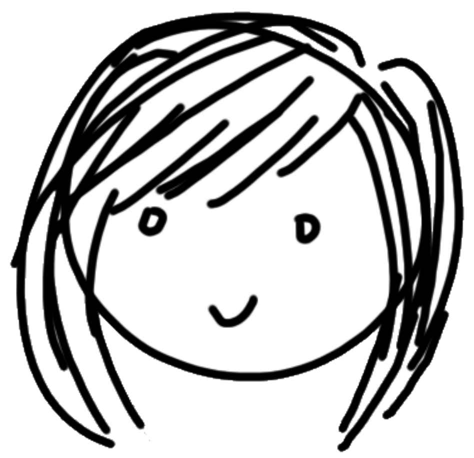
(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

All-but-one corruptions prior work

Damgard-Polychroniadou-Rao

pk, sk_i



$c_i \leftarrow \mathsf{EquivFHE.Enc}_{pk}(x_i)$

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

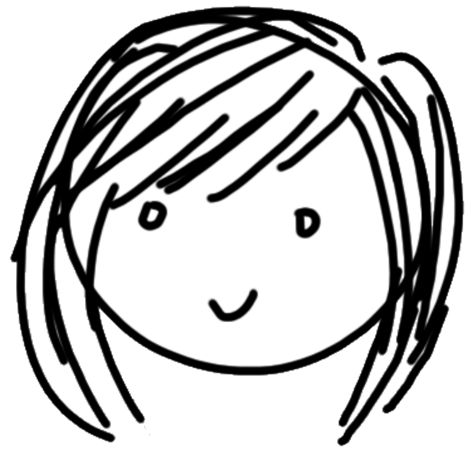
(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

All-but-one corruptions prior work

Damgard-Polychroniadou-Rao

pk, sk_i



$c_i \leftarrow \mathsf{EquivFHE.Enc}_{pk}(x_i)$

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

d_i

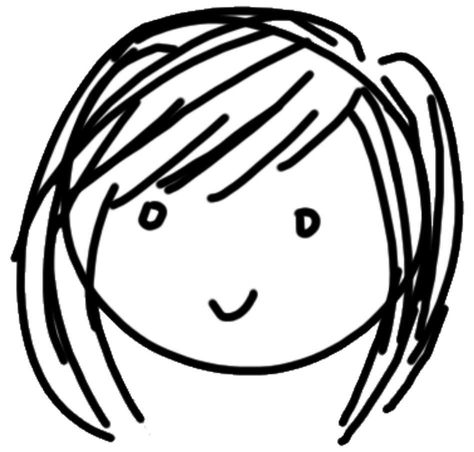
(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

All-but-one corruptions prior work

Damgard-Polychroniadou-Rao

pk, sk_i



$c_i \leftarrow \mathsf{EquivFHE.Enc}_{pk}(x_i)$ →

(receive c1,...,cn from everyone)

$y \leftarrow \mathsf{Eval}_{pk}(f, c_1, c_2, \ldots, c_n)$

$r_i \leftarrow \mathsf{EquivFhe.Enc}(0)$ →

$d_i \leftarrow \mathrm{Dec}_{sk_i}(y + r_i)$

d_i →

(receive from everyone)

$f(x_1, \ldots, x_n) \leftarrow \mathsf{Combine}(d_1, \ldots, d_n)$

Adaptive LWE

- *The Challenger picks k random matrices $A_i \leftarrow \mathbb{Z}_q^{n\times m}$ for $i \in [k]$, and sends them to $\mathcal{A}$.*
- *$\mathcal{A}$ adaptively picks $x_1, \ldots, x_k \in \{0,1\}$, and sends it to the Challenger.*
- *The Challenger samples $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ and computes for all $i \in [k]$*

$$\begin{cases} \boldsymbol{b}_i = \boldsymbol{s}^T(\boldsymbol{A}_i - x_i \cdot \boldsymbol{G}) + \boldsymbol{e}_i \text{ where } \boldsymbol{e}_i \leftarrow \chi^m, & \text{if } \beta = 0. \\ \boldsymbol{b}_i \leftarrow \mathbb{Z}_q^m, & \text{if } \beta = 1. \end{cases}$$

The Challenger also picks $\boldsymbol{A}_{k+1} \leftarrow \mathbb{Z}_q^{n\times m'}$ and computes

$$\begin{cases} \boldsymbol{b}_{k+1} = \boldsymbol{s}^T \boldsymbol{A}_{k+1} + \boldsymbol{e}_{k+1} \text{ where } \boldsymbol{e}_{k+1} \leftarrow \chi^{m'}, & \text{if } \beta = 0. \\ \boldsymbol{b}_{k+1} \leftarrow \mathbb{Z}_q^{m'}, & \text{if } \beta = 1. \end{cases}$$

The challenger sends $\boldsymbol{A}_{k+1}$ and $\{\boldsymbol{b}_i\}_{i\in[k+1]}$ to the adversary.

HTDF

- **Correctness.** Let $x_1, \ldots, x_\ell \in \{0,1\}$ and $v_i = f_{pk,x_i}(u_i)$ for $i \in [\ell]$. Then, for $u^* = \mathsf{HTDF.Eval}^{\mathsf{in}}(g, (x_1, u_1), \ldots, (x_\ell, u_\ell))$ and $v^* = \mathsf{HTDF.Eval}^{\mathsf{out}}(g, v_1, \ldots, v_\ell)$ it holds that $f_{pk,y}(u^*) = v^*$, where $y = g(x_1, \ldots, x_\ell)$.

- **Distributional equivalence of inversion.** For a bit $x \in \{0,1\}$, the tuple (pk, x, u, v) computed as $v = f_{\mathsf{pk},x}(u)$ for a random $u \leftarrow \mathcal{U}$ is statistically close to sampling $v \leftarrow \mathcal{V}$ at random and computing $u = \mathsf{HTDF.Inv}_{\mathsf{sk},x}(v)$.

- **Claw-free security.** Given the public key, no efficient adversary can come up with u and u' such that $f_{\mathsf{pk},0}(u) = f_{\mathsf{pk},1}(u')$ with more than a negligible probability.

Full adaptive case

Theorem 4.1 (Theorem 1.1, secure-erasures version, restated)**.** *Assume the existence of LFE schemes for* $\mathsf{P/poly}$*, of 2-round adaptively and maliciously secure OT, and of secure erasures, and let* $f : (\{0,1\}^{\ell_{\mathsf{in}}})^n \to \{0,1\}^{\ell_{\mathsf{out}}}$ *be an* n*-party function of depth* d*.*

Then, $\mathcal{F}^f_{\mathsf{sfe\text{-}abort}}$ *can be UC-realized tolerating a malicious, adaptive PPT adversary by a 2-round protocol in the common random string model. The size of the common random string is* $\mathrm{poly}(\kappa, d)$*, whereas the communication and online-computational complexity of the protocol are* $\mathrm{poly}(\kappa, \ell_{\mathsf{in}}, \ell_{\mathsf{out}}, d, n)$*.*