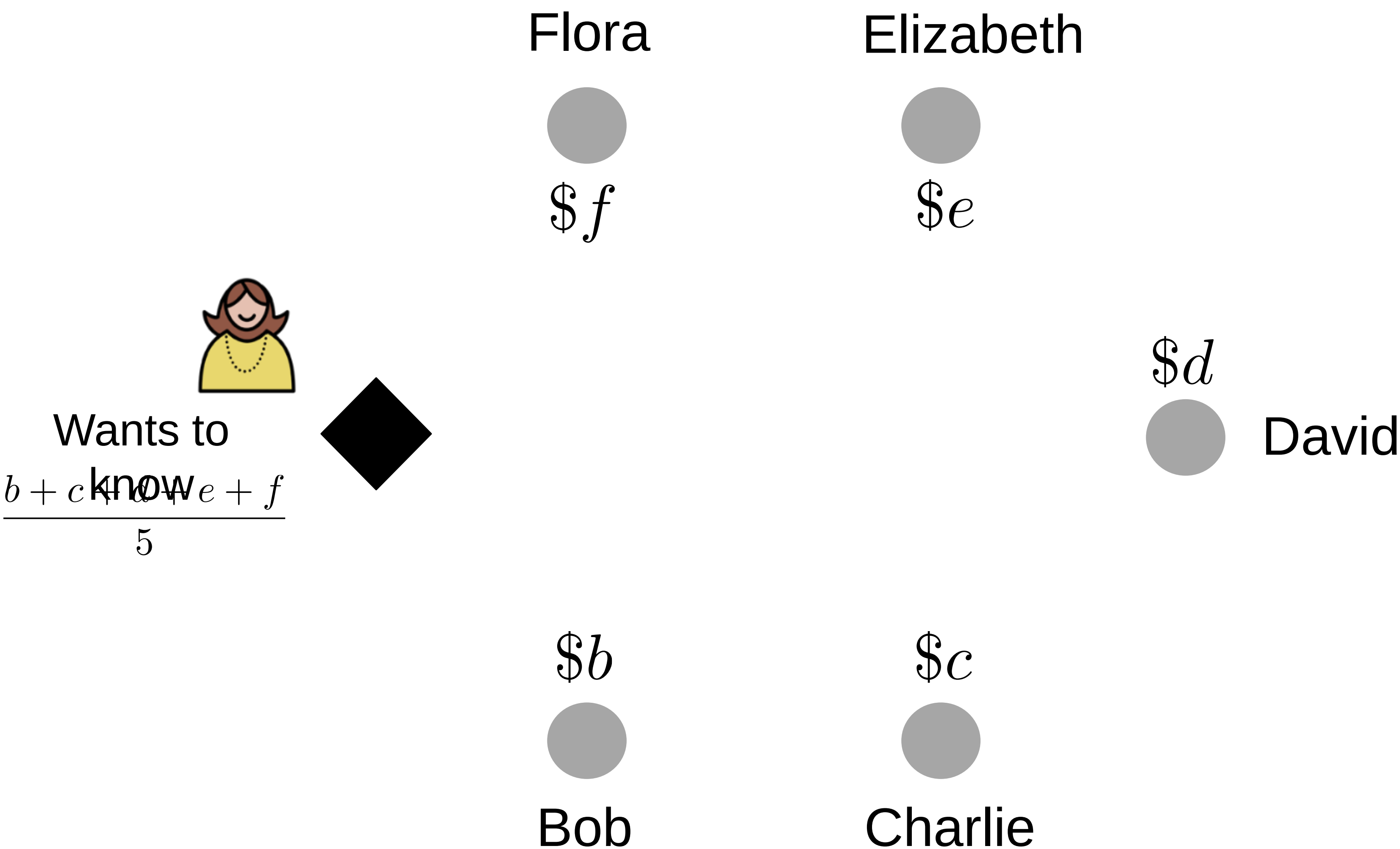
Privacy, Efficiency & Fault Tolerance in Aggregate Computations on Massive Star Networks

Rane, Freudiger, Brito, Uzun

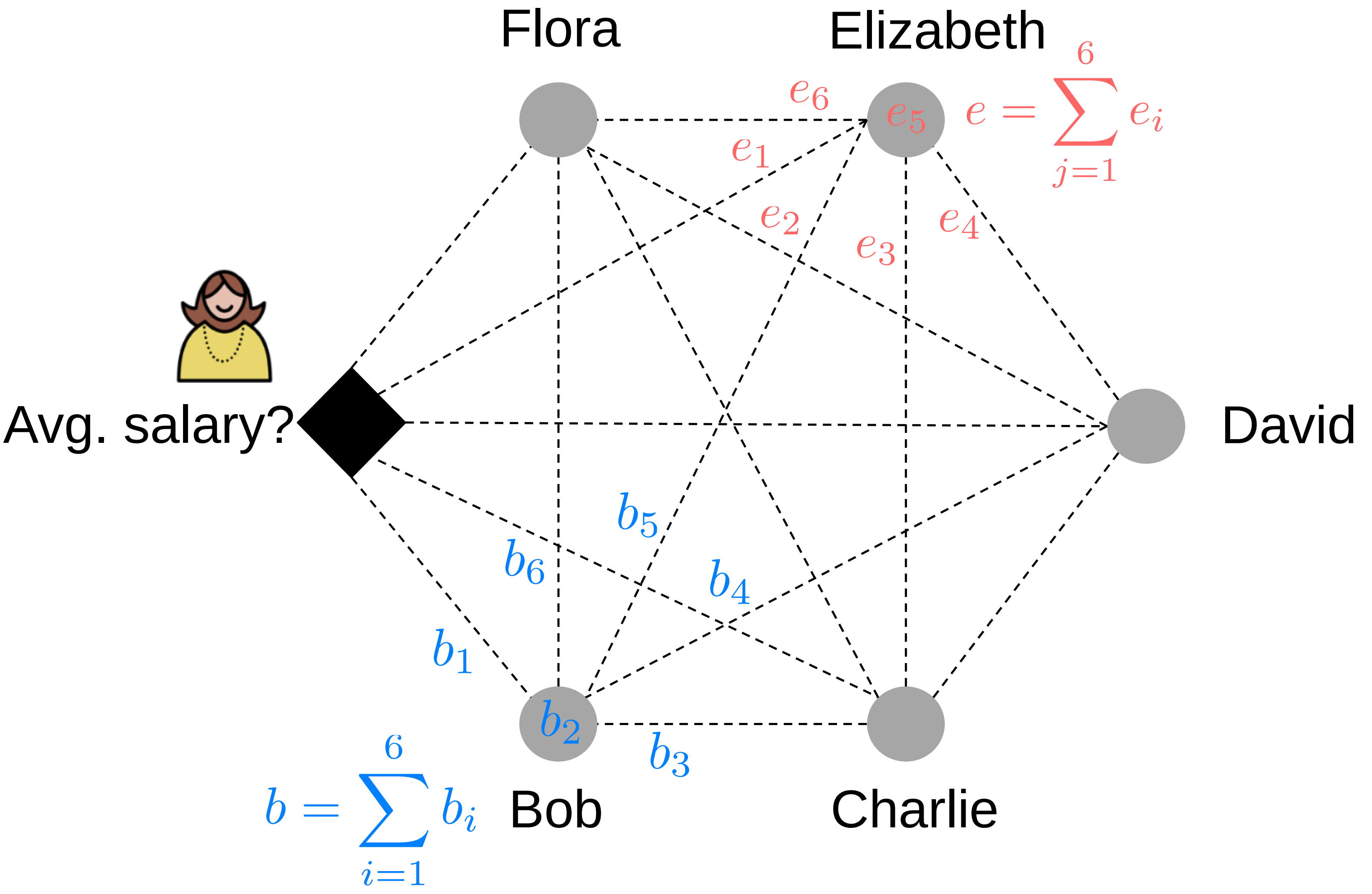
parc | WIFS | 2015

A Crypto Puzzle

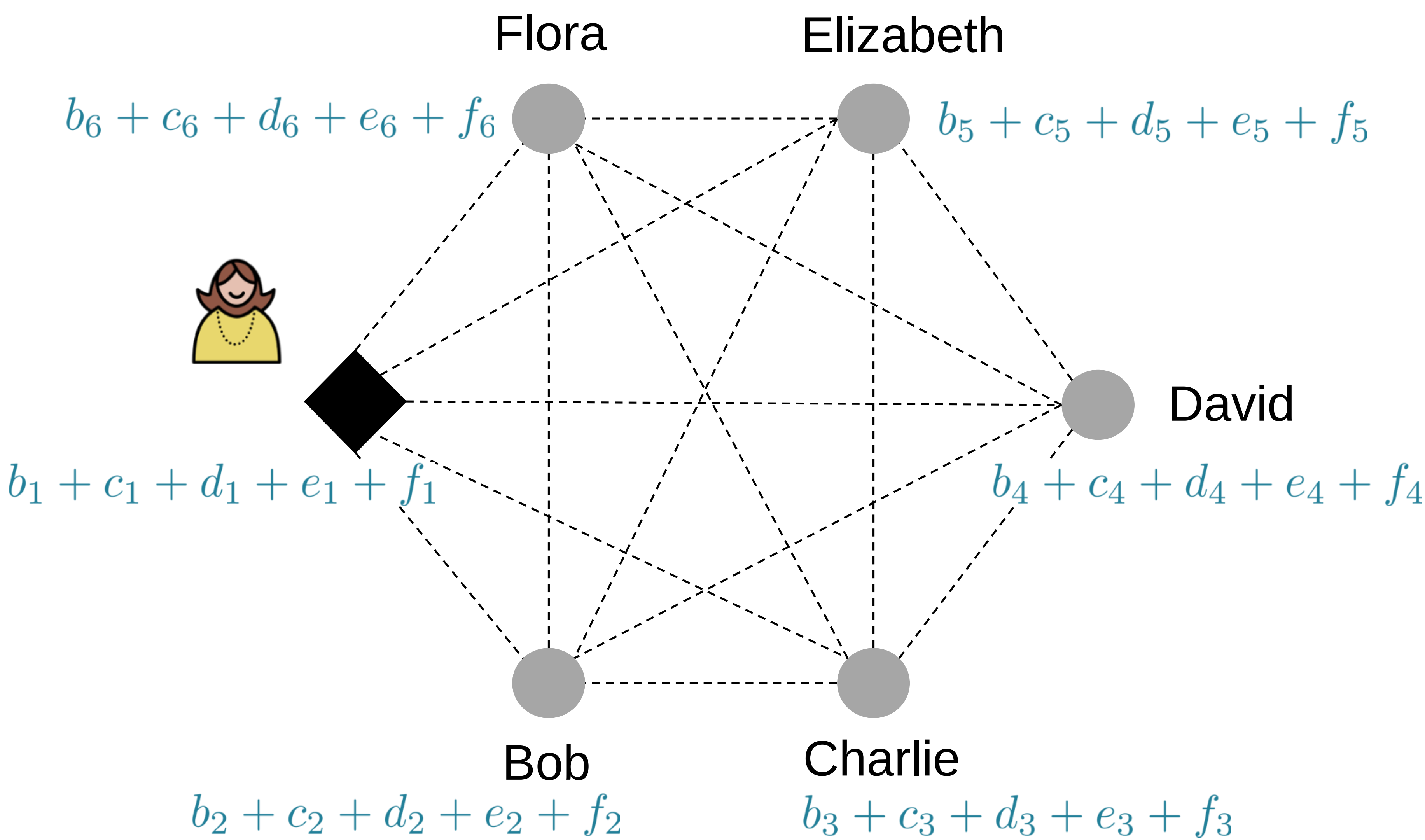


http://www.cartalk.com/content/coney-island-crab-cake-company

Allow people to gossip

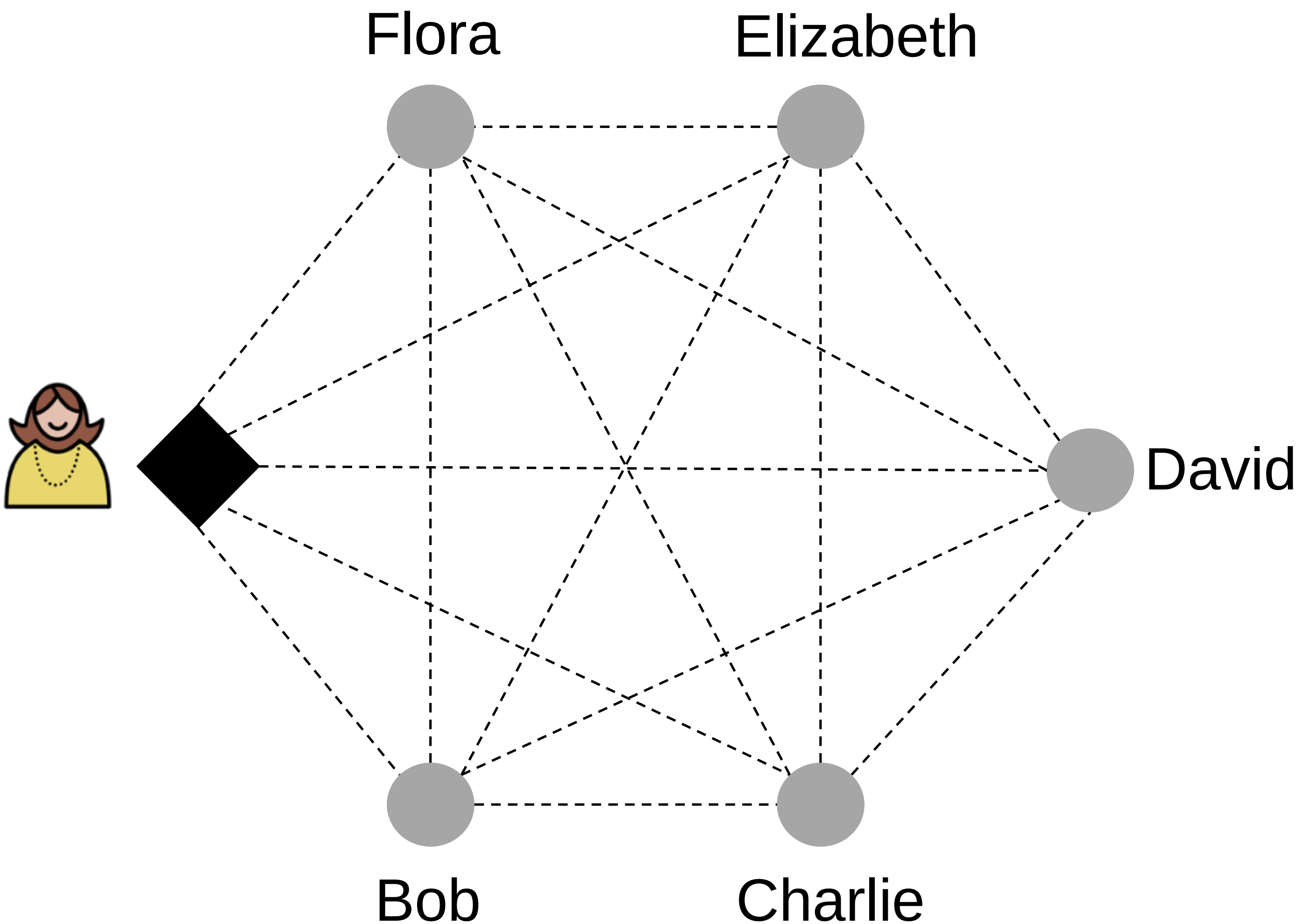


Additive Secret Sharing



sum, then avg.

What if people can only talk to Alice?



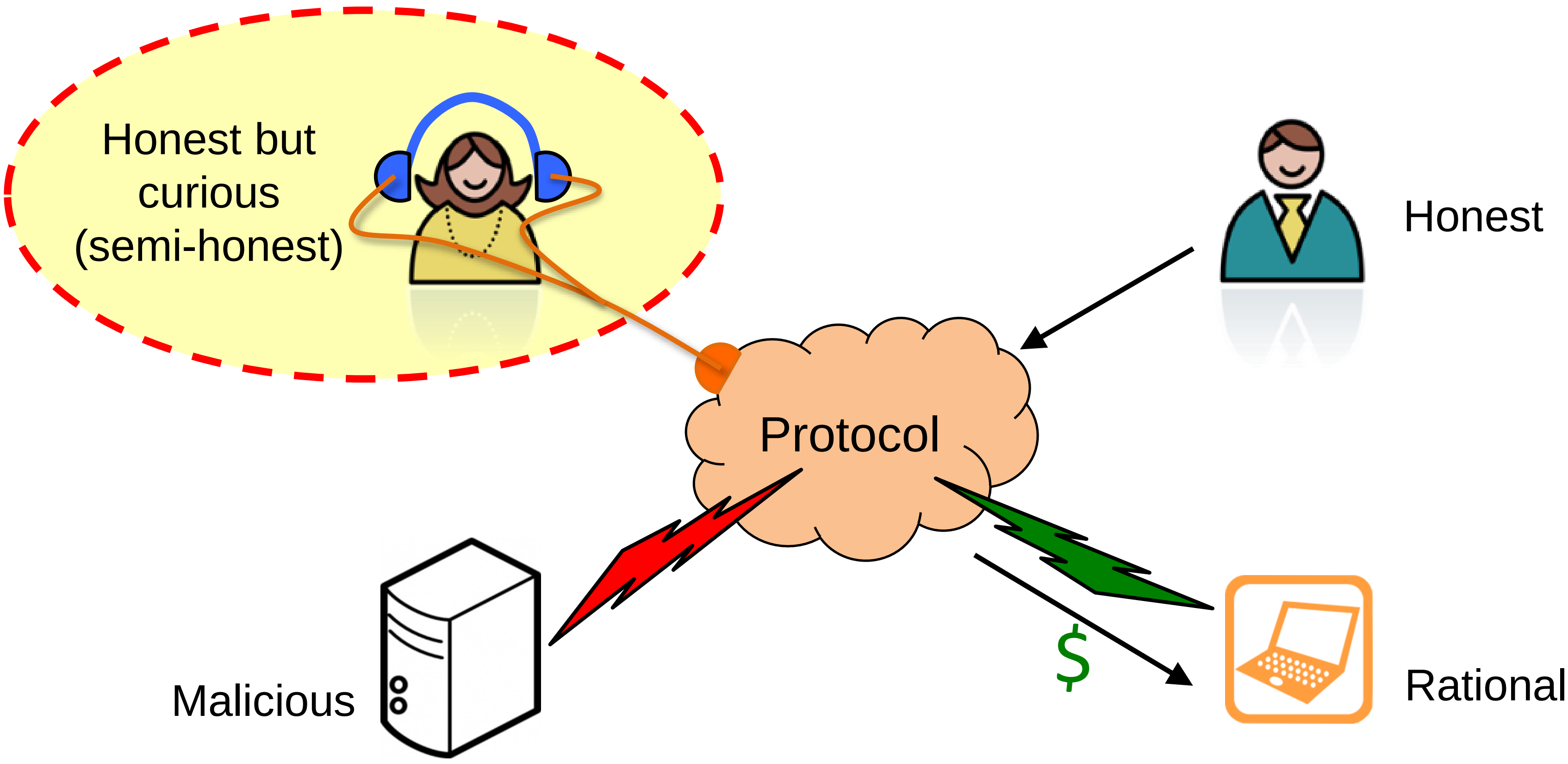
Applications

- Electronic voting
- Smart power grids
- Studying browsing behavior
- IoT analytics
  - Smart homes
  - Wearable devices
- Social Networks
- ... & many more

Existing aggregation solutions

[Erkin, Troncoso-Pastoriza, Lagendijk, Gonzalez, 2012]

Review: Semi-honest Adversary



Review: Homomorphic Encryption

$$
+\;\begin{array}{|c|}\hline x \\ \hline y \\ \hline z \\ \hline \end{array}
$$

$$
\overline{}
$$

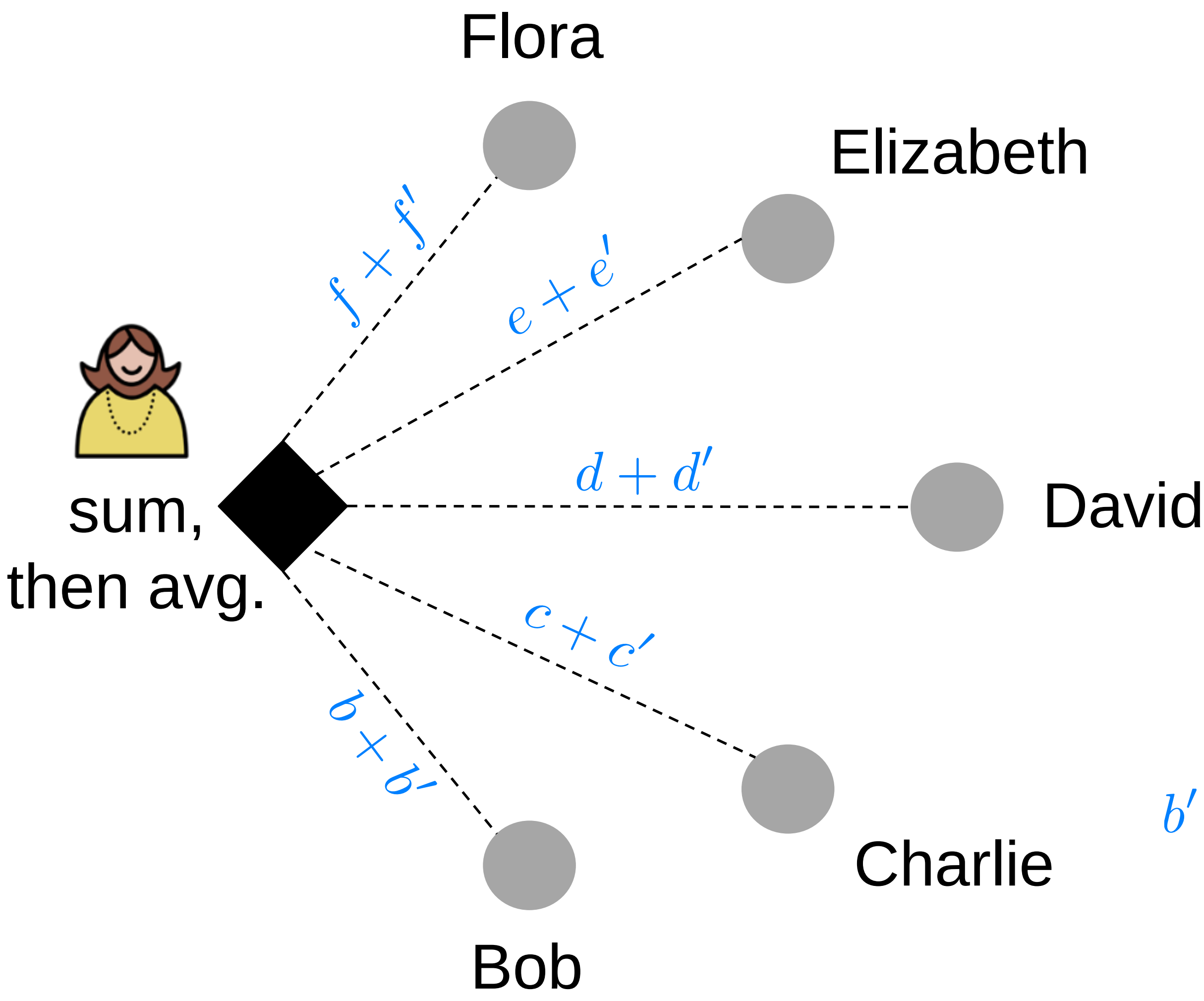
$$
S = x + y + z
$$

$$
\times\;\begin{array}{|c|}\hline E(x) \\ \hline E(y) \\ \hline E(z) \\ \hline \end{array}
$$

$$
\begin{aligned}
E(S) &= E(x)E(y)E(z) \\
&= E(x + y + z)
\end{aligned}
$$

[Paillier, 1999] [Damgard-Jurik, 2001] [El Gamal, 1985] [Gentry, 20

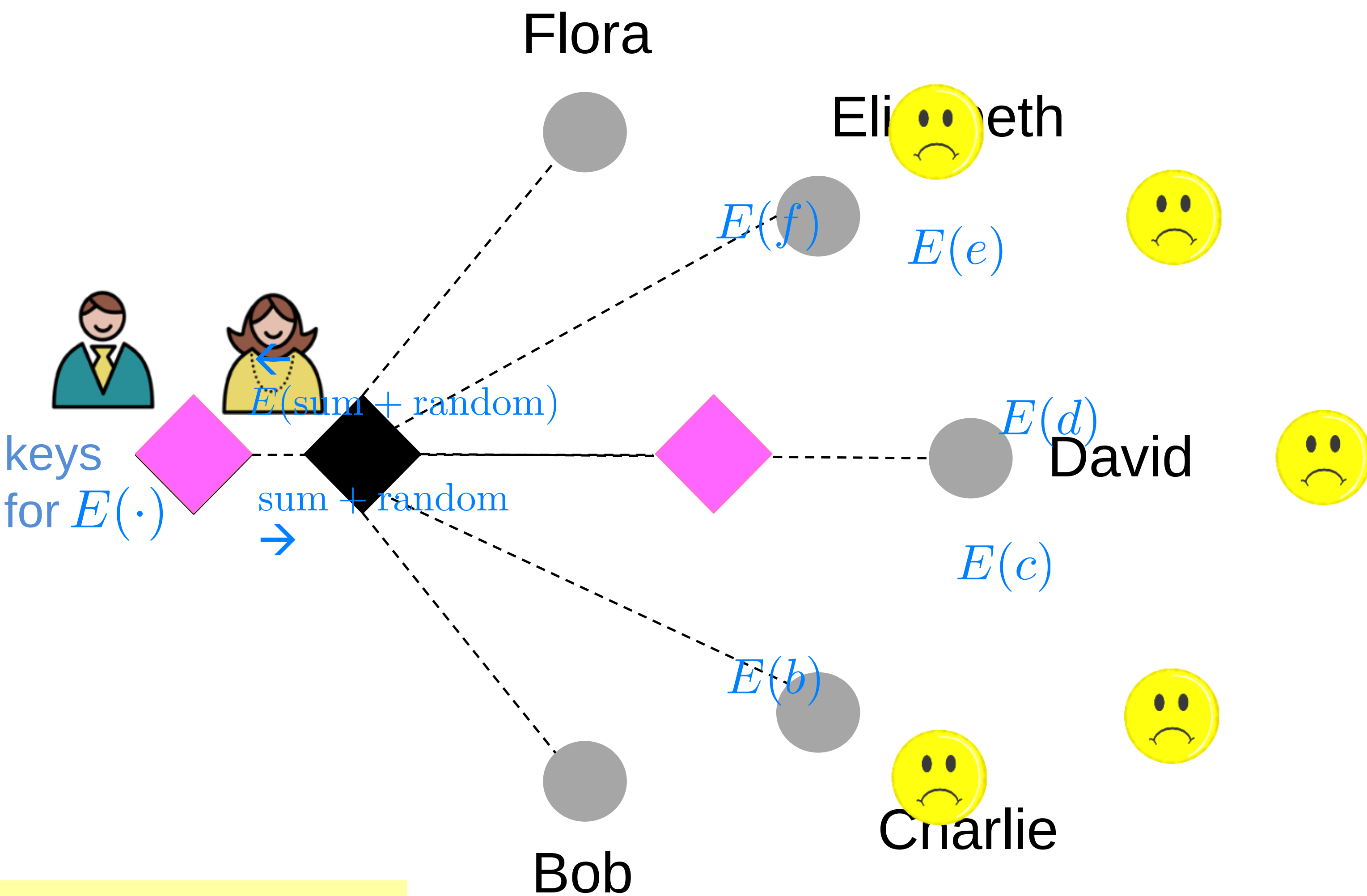
Soln #1: Let there be a Genie



$b' + c' + d' + e' + f'$
$= 0$

[Shi et al., 2011] [Chan et al., 2012] [Bilogrevic et al., 2014]
Related Approach: [Erkin, Tusdik, 2012]

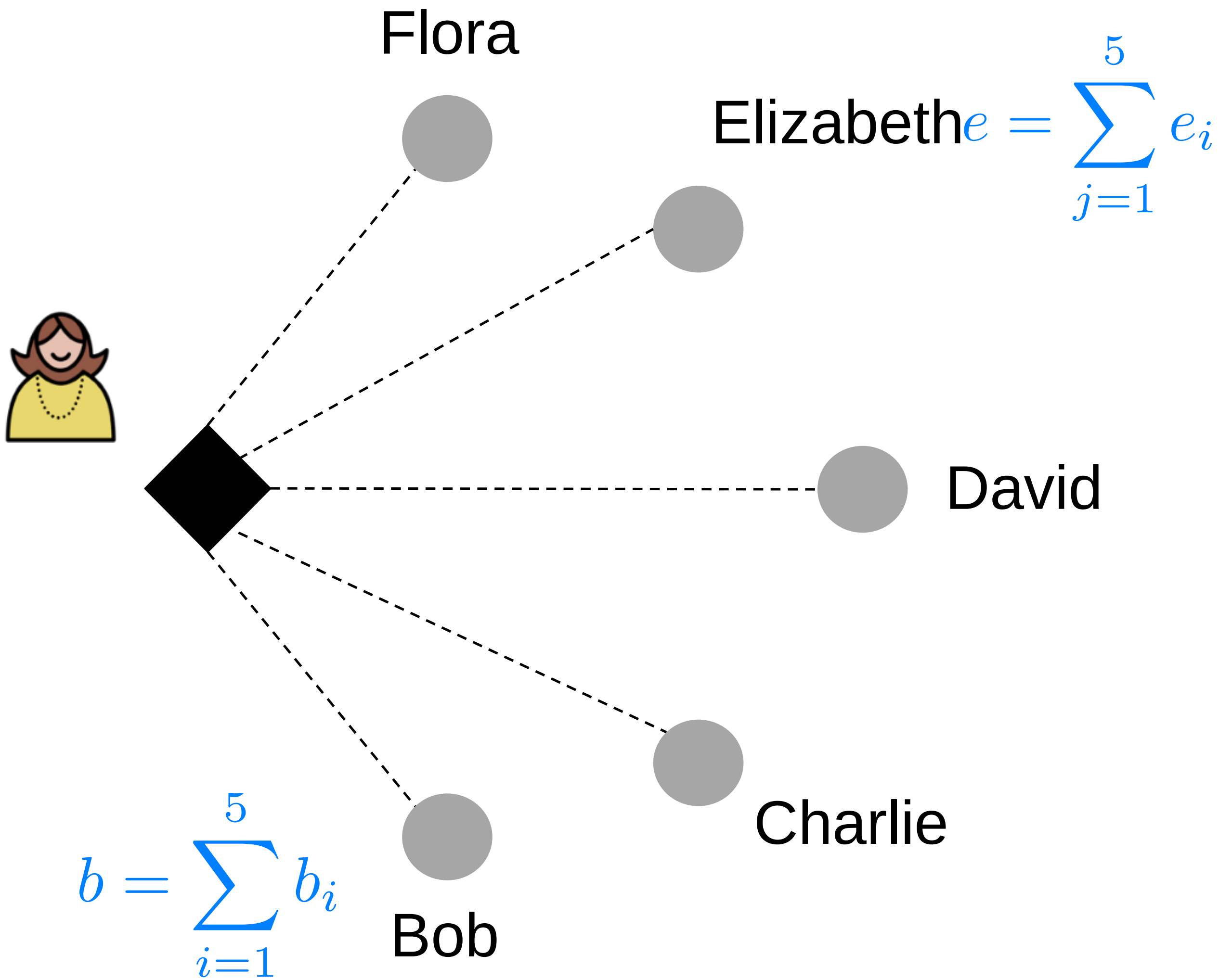
Soln #2: Untrusted Key Manager



Everyone can encrypt.
Only KM can decrypt.

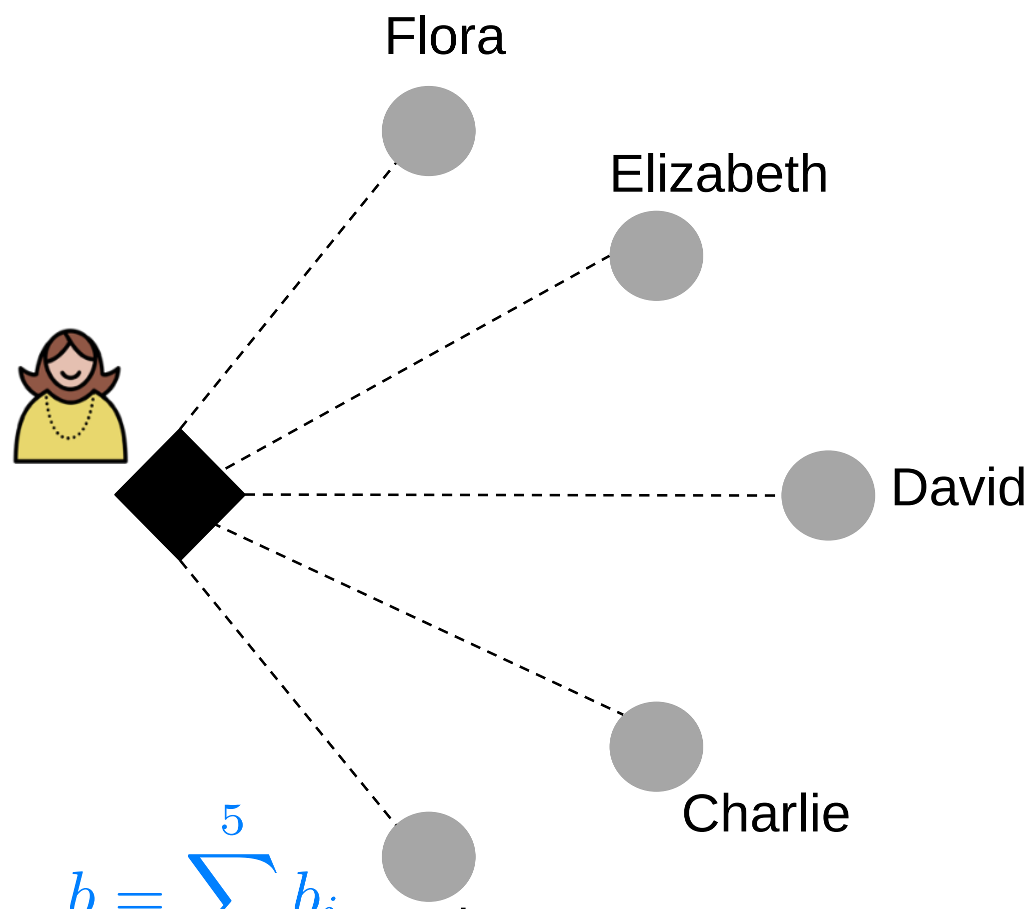
[Jawurek, Kerschbaum,2012]

Soln #3: Secret Sharing + Homomorphic Encryption



Assume, everyone knows everyone's public encryption keys, so David can encrypt with Bob's public key, etc.

Bob	Charlie	David	Elizabeth	Flora
$[b_1]$	$[b_2]$	$[b_3]$	$[b_4]$	$[b_5]$
$[c_1]$	$[c_2]$	$[c_3]$	$[c_4]$	$[c_5]$
$[d_1]$	$[d_2]$	$[d_3]$	$[d_4]$	$[d_5]$
$[e_1]$	$[e_2]$	$[e_3]$	$[e_4]$	$[e_5]$
$[f_1]$	$[f_2]$	$[f_3]$	$[f_4]$	$[f_5]$
$[q_1]$	$[q_2]$	$[q_3]$	$[q_4]$	$[q_5]$



$$b = \sum_{i=1}^{5} b_i$$

Book-keeping with additive shares

Alice requests decryptions q_1, q_2, q_3, q_4, q_5 from parties.

By construction, $q_1 + q_2 + q_3 + q_4 + q_5$
$= b + c + d + e + f$ done!

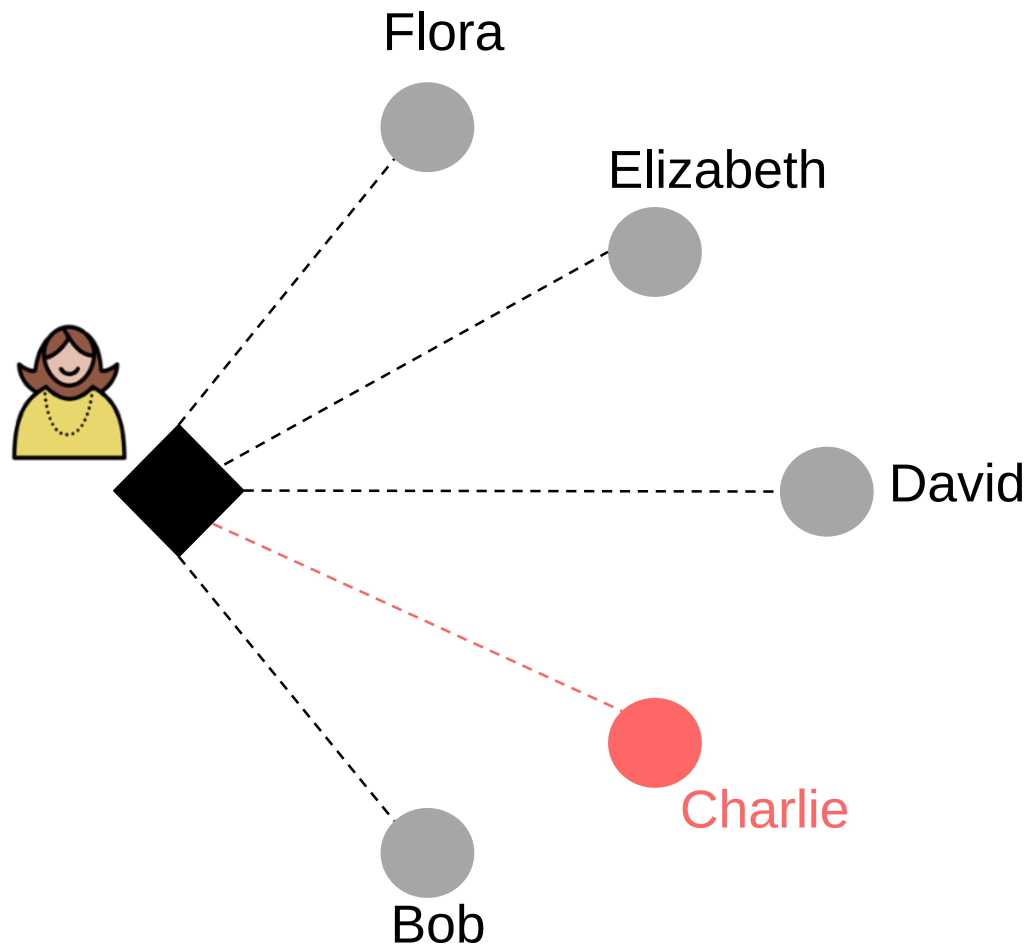
Collusion resistance → To compromise Bob, *all* other parties are forced to collude.

[Garcia, Jacobs, 2011]

Drawback: Not fault tolerant

Bob	Charlie	David	Elizabeth	Flora
b_1	b_2	b_3	b_4	b_5
c_1	c_2	c_3	c_4	c_5
d_1	d_2	d_3	d_4	d_5
e_1	e_2	e_3	e_4	e_5
f_1	f_2	f_3	f_4	f_5
q_1	q_2	q_3	q_4	q_5

H+



... the secret sharing approach breaks down.

Completel
y.

Shamir Secret Sharing [1979]

Bob

$$b(x) = b + b_1 x + b_2 x^2 + b_3 x^3 \mod \beta$$

Coefficients chosen at random from 0 to β - 1

Observe, $b(0) = b$

Bob evaluates his polynomial at x = 1, 2, 3, 4, 5

Elizabeth

$$e(x) = e + e_1 x + e_2 x^2 + e_3 x^3 \mod \beta$$

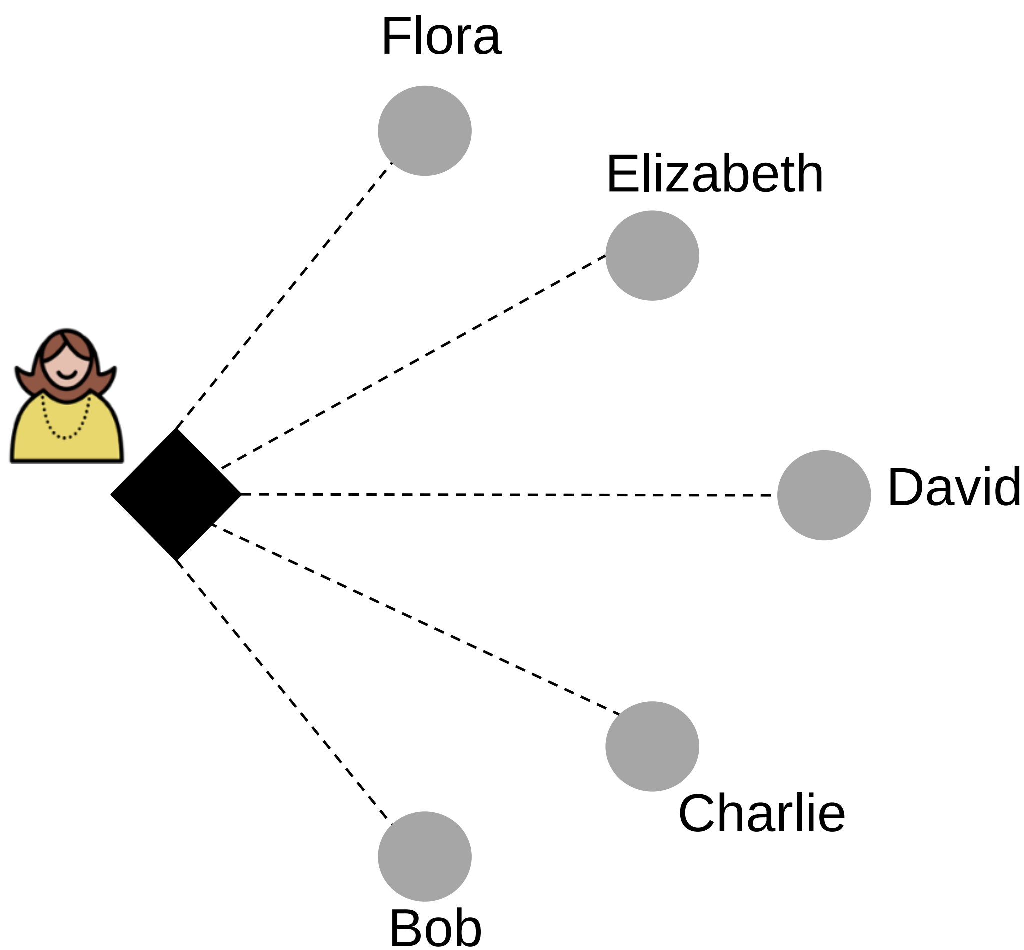
Coefficients chosen at random from 0 to β - 1

Again, $e(0) = e$

She evaluates her polynomial at x = 1, 2, 3, 4, 5

Assume, everyone knows everyone's public encryption keys, so David can encrypt with Bob's public key, etc.

Bob	Charlie	David	Elizabeth	Flora
$[b(1)]$	$[b(2)]$	$[b(3)]$	$[b(4)]$	$[b(5)]$
$[c(1)]$	$[c(2)]$	$[c(3)]$	$[c(4)]$	$[c(5)]$
$[d(1)]$	$[d(2)]$	$[d(3)]$	$[d(4)]$	$[d(5)]$
$[e(1)]$	$[e(2)]$	$[e(3)]$	$[e(4)]$	$[e(5)]$
$[f(1)]$	$[f(2)]$	$[f(3)]$	$[f(4)]$	$[f(5)]$
$[q(1)]$	$[q(2)]$	$[q(3)]$	$[q(4)]$	$[q(5)]$



Alice requests decryptions of $q(1)$ $q(2)$ $q(3)$ $q(4)$ $q(5)$

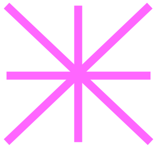
Evaluations of $q(x) = q + q_1 x + q_2 x^2 + q_3 x^3$

where, $q = b + c + d + e + f$

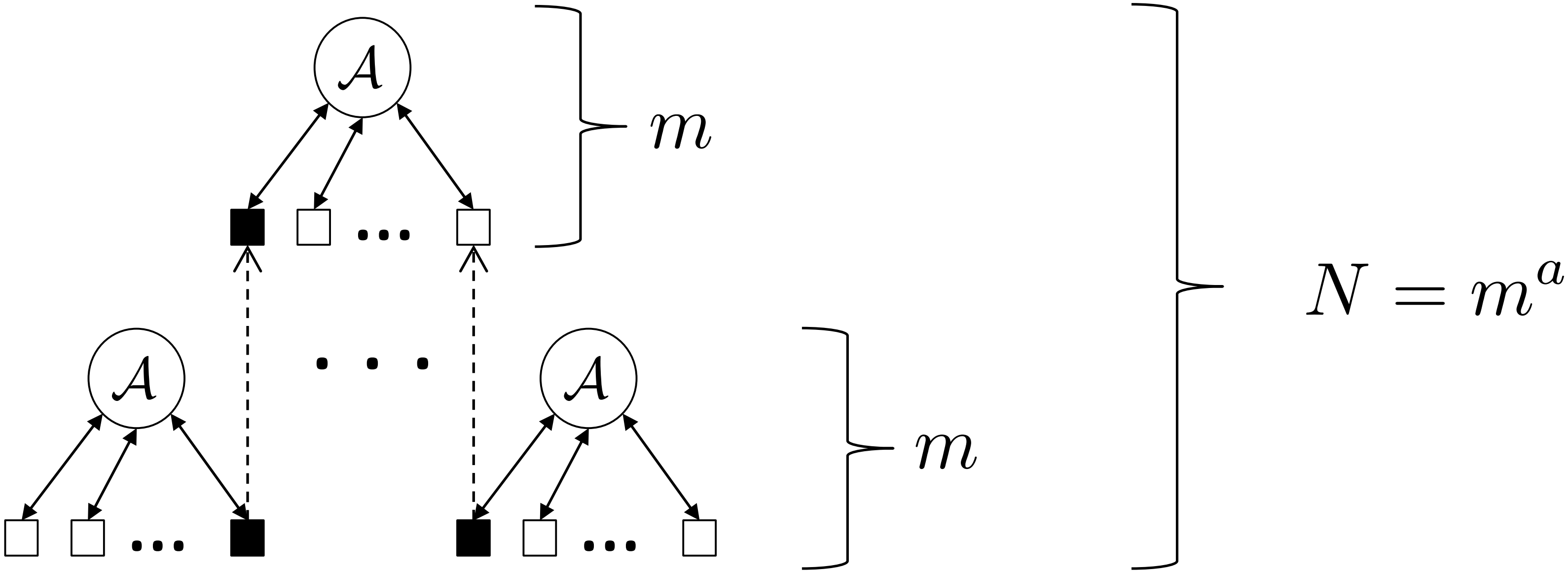
Putting x = 1, 2, ..., 5, Alice has 5 equations in 4 unknowns.
From any 4 equations, she can obtain q and divide by 5. Done!

Fault tolerance → Any *one* person can leave after distributing the polynomial secrets. Can generalize this.

Complexity at Aggregator

			
# calculations	O(m)	O(m)	O(m^2)
# transmissions	O(1)	O(1)	O(m)
Collusion resistance	Yes	No	Yes
Fault tolerance	No	Yes	Yes

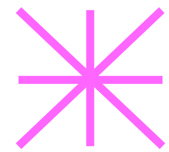
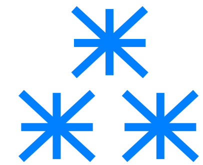
Complexity with Logical Hierarchy



No. of cohorts = $m^{a-1} + m^{a-2} + \ldots + m^2 + m + 1 = \dfrac{m^a - 1}{m - 1}$

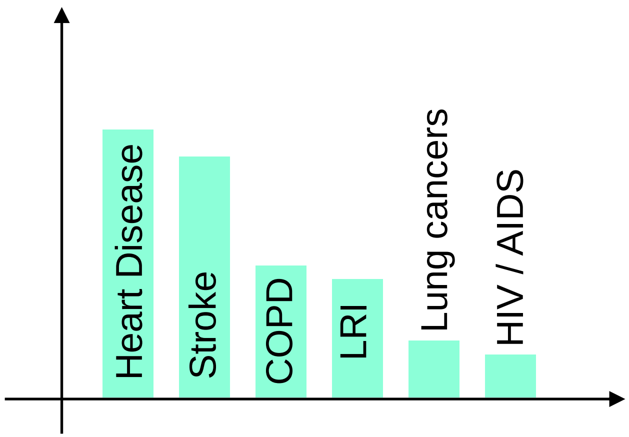
Effective Complexity = $O\left(m^2 \dfrac{m^a - 1}{m - 1}\right) \equiv O(Nm) \equiv \boxed{O\left(N^{1+\frac{1}{a}}\right)}$

Complexity

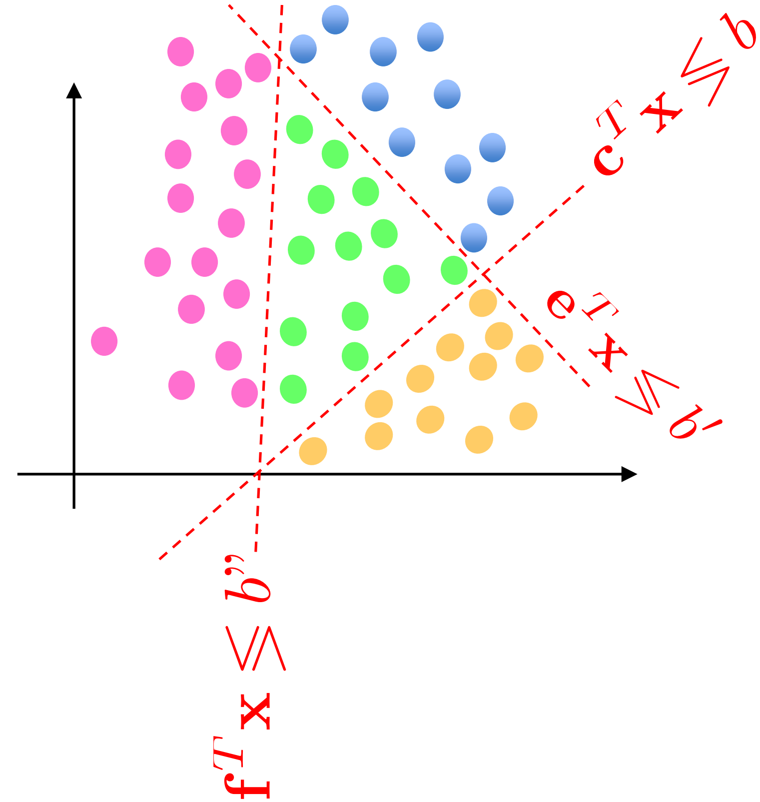
				
# calculations	$O(N)$	$O(N)$	$O(N^2)$	$O(N^{1+\varepsilon})$
# transmissions	$O(1)$	$O(1)$	$O(N)$	$O(N)$
Collusion resistance	Yes	No	Yes	Yes
Fault tolerance	No	Yes	Yes	Yes

More interesting computations

Histograms



Linear Classifiers



Summary

- Aggregation under constraints on privacy, network topology and fault tolerance for strict stat topology needs $O(N^2)$
- With hierarchical approach, can reduce the overhead down to $O(N^{1+\epsilon})$
- Tradeoffs among collusion resistance and fault tolerance.
- **Future work:** What other expressive computations are (efficiently) possible in star networks?