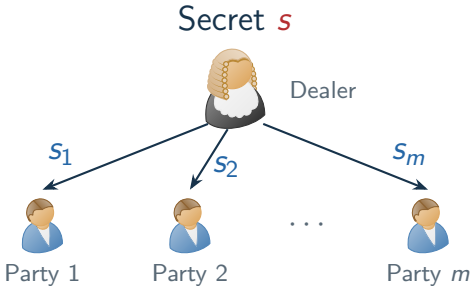
Local Leakage Resilience of Multiplication-Friendly Shamir Secret Sharing

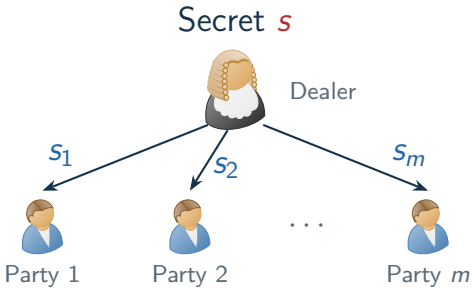
Jihun Hwang[1] Hemanta K. Maji[1]
Ilya D. Shkredov[2] Xiuyu Ye[1]

[1]Department of Computer Science, Purdue University
[2]Department of Mathematics, Purdue University

Shamir secret sharing



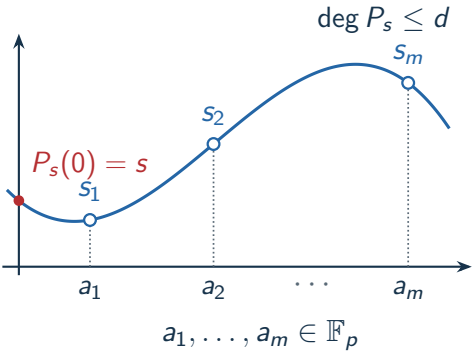
Shamir secret sharing



Independent uniform $R_1, \ldots, R_d \in \mathbb{F}_p$:

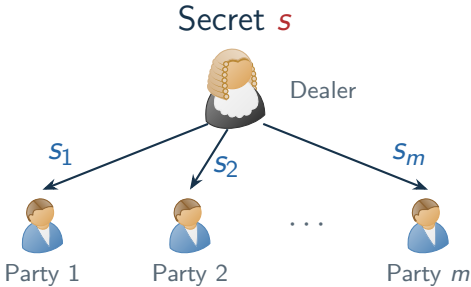
$$P_s(X) = s + R_1 X + \cdots + R_d X^d.$$

Party i receives $s_i = P_s(a_i)$.



Public, distinct, nonzero evaluation points in $\mathbb{F}_p$.

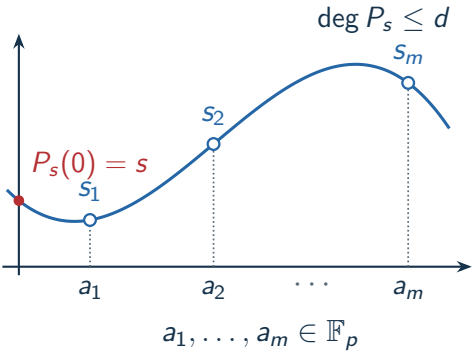
Shamir secret sharing



Independent uniform $R_1, \ldots, R_d \in \mathbb{F}_p$:

$$P_s(X) = s + R_1 X + \cdots + R_d X^d.$$

Party i receives $s_i = P_s(a_i)$.



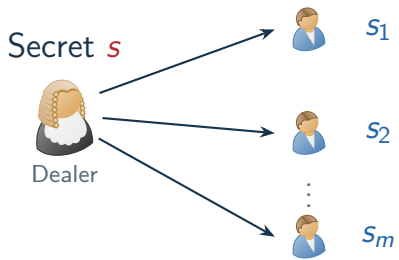
Public, distinct, nonzero evaluation points in $\mathbb{F}_p$.

Threshold scheme: all or nothing.

At most d full shares: no information. $d+1$ full shares: recover s.

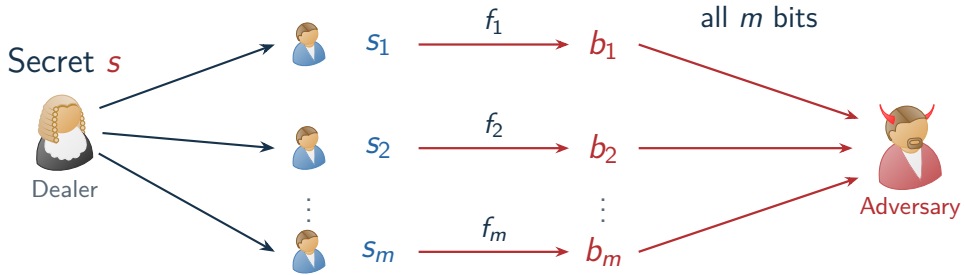
Local leakage

Side channel attacks can reveal **partial information**.



Local leakage

Side channel attacks can reveal **partial information**.

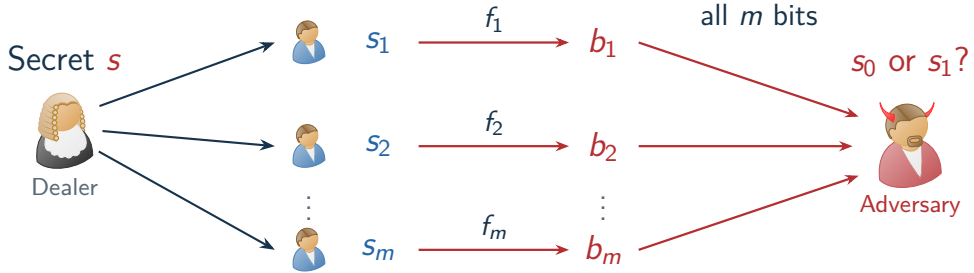


One arbitrary bit per share: $b_i = f_i(s_i), \quad f_i : \mathbb{F}_p \to \{0, 1\}$.

The functions may depend on all public evaluation points.

Local leakage

Side channel attacks can reveal **partial information**.



One arbitrary bit per share: $b_i = f_i(s_i), \quad f_i : \mathbb{F}_p \to \{0,1\}$.

The functions may depend on all public evaluation points.

Leakage resilience

From the leaked bits, the adversary cannot distinguish two secrets.

For every pair of secrets and every choice of local leakage functions.

Our problem

Is Shamir secret sharing resilient to one bit of local leakage from every share?

Fix the public tuple $a = (a_1, \ldots, a_m)$ and degree d. Same local functions in both worlds.



Goal: Worst-case leakage insecurity is small.

$$\mathsf{Insec}(a; d) := \max_{\substack{s_0, s_1 \in \mathbb{F}_p \\ f_1, \ldots, f_m : \mathbb{F}_p \to \{0,1\}}} \mathsf{SD}\left(\mathcal{L}^{a,\mathbf{f}}_{s_0}, \mathcal{L}^{a,\mathbf{f}}_{s_1}\right) \leq \epsilon$$

Prior work: lowering the threshold

m parties, degree d, and relative degree $c = d/m$.

Arbitrary one-bit leakage from every share, over prime fields.

Work	Sufficient cutoff
Benhamouda–Degwekar–Ishai–Rabin (2018)	$c > 0.907$
Maji–Paskin-Cherniavsky–Suad–Wang (2021)	$c > 0.8675$
Benhamouda–Degwekar–Ishai–Rabin (2021)	$c > 0.85$
Maji–Nguyen–Paskin-Cherniavsky–Wang (2022)	$c > 0.78$
Klein–Komargodski (2023)	$c > 0.69$
Kasser (TCC 2024)	$c > 0.668$

Can we go below $1/2$? Why does that matter?

Asymptotic cutoffs; field-size assumptions differ. Nguyen (2024) reaches every fixed positive rate for restricted leakage families, including almost all bit rules.

Why below one half?

Share secrets s and t using polynomials P, Q of degree at most d.



Party i

$$P(a_i) \cdot Q(a_i) = (PQ)(a_i)$$

Each party multiplies its own two shares.

$$\deg(PQ) \leq 2d \qquad (PQ)(0) = st$$

$$2d + 1 \leq m \iff d/m < 1/2$$

Enough evaluations to reconstruct the product polynomial.

A full protocol also handles degree reduction and privacy during the computation.

Why below one half?

Share secrets s and t using polynomials P, Q of degree at most d.



Party i

$$P(a_i) \cdot Q(a_i) = (PQ)(a_i)$$

Each party multiplies its own two shares.

$$\deg(PQ) \leq 2d \qquad (PQ)(0) = st$$

$$2d + 1 \leq m \iff d/m < 1/2$$

Enough evaluations to reconstruct the product polynomial.

Multiplication of shared values is a basic operation in MPC.

A full protocol also handles degree reduction and privacy during the computation.

Comparison with concurrent work

Arbitrary one-bit leakage. Let $n = \lceil \log_2 p \rceil$ be the field bit length.
m parties, degree d, and relative degree $c = d/m$.

Result	Relative degree	Public points	Field / party regime
Sun–Wootters Nguyen (2026)	$c > \frac{1}{2} - \delta$ absolute $\delta > 0$	Every valid tuple	Every prime $p > m$
Our quadratic result	Fixed $\frac{1}{3} < c < \frac{1}{2}$	Nearly every tuple	$\log p \gtrsim m^2 \log(2m)$
Our general result	Fixed $0 < c < \frac{1}{2}$	Nearly every tuple	$\log p \gtrsim m^{\Theta_\ell} \log(2m)$

For smaller fixed c, choose $\ell \geq 4$ with $1/\ell < c$; Θ_ℓ is a constant depending only on ℓ.

Comparison with concurrent work

Arbitrary one-bit leakage. Let $n = \lceil \log_2 p \rceil$ be the field bit length.
m parties, degree d, and relative degree $c = d/m$.

Result	Relative degree	Public points	Field / party regime
Sun–Wootters Nguyen (2026)	$c > \frac{1}{2} - \delta$ absolute $\delta > 0$	Every valid tuple	Every prime $p > m$
Our quadratic result	Fixed $\frac{1}{3} < c < \frac{1}{2}$	Nearly every tuple	$\log p \gtrsim m^2 \log(2m)$
Our general result	Fixed $0 < c < \frac{1}{2}$	Nearly every tuple	$\log p \gtrsim m^{\Theta_\ell} \log(2m)$

We reach every fixed positive rate below half, with random public points and larger fields.

For smaller fixed c, choose $\ell \geq 4$ with $1/\ell < c$; Θ_ℓ is a constant depending only on ℓ.

Further below half

What smaller c allows:

Larger local products

More factors can be multiplied locally before degree reduction.

More packing capacity

The same number of shares can carry more secrets,
with a lower full-share privacy threshold.

For packing, the relevant rate is the randomness fraction;
the total polynomial degree can remain near half.

Our result

Fix any $0 < c < 1/2$. For prime p, $n = \lceil \log_2 p \rceil$,set $m = \lfloor n^u \rfloor$, $d = \lfloor cm \rfloor$.

Choose a sufficiently small fixed $u > 0$ depending on c, and let $n \to \infty$.
Insecurity: the largest statistical distance between two secrets' leakage laws.

Arbitrary one-bit leakage

$$\mathbb{E}_a \, \mathrm{Insec}(a; d) \leq \left(\frac{2}{\pi}\right)^{(1-o(1))d}$$

a is uniform over ordered tuples of distinct, nonzero evaluation points.

Nearly every public tuple is secure, simultaneously
for every pair of secrets and every choice of local bit functions.

For $1/3 < c < 1/2$, any fixed $u < 1/2$ works. Smaller c needs smaller permitted u.

Sources: Reconstruction-based LSB attack: Maji et al., ITC 2022.

Our result

Fix any $0 < c < 1/2$. For prime p, $n = \lceil \log_2 p \rceil$,set $m = \lfloor n^u \rfloor$, $d = \lfloor cm \rfloor$.

Choose a sufficiently small fixed $u > 0$ depending on c, and let $n \to \infty$.
Insecurity: the largest statistical distance between two secrets' leakage laws.

Arbitrary one-bit leakage

$$\mathbb{E}_a \, \mathrm{Insec}(a; d) \leq \left(\frac{2}{\pi}\right)^{(1-o(1))d}$$

a is uniform over ordered tuples of distinct, nonzero evaluation points.

Nearly every public tuple is secure, simultaneously
for every pair of secrets and every choice of local bit functions.

Known LSB attack: $\mathrm{Insec}(a; d) \geq \left(\frac{2}{\pi}\right)^{d}$.

Optimal up to $o(d)$ in the exponent.

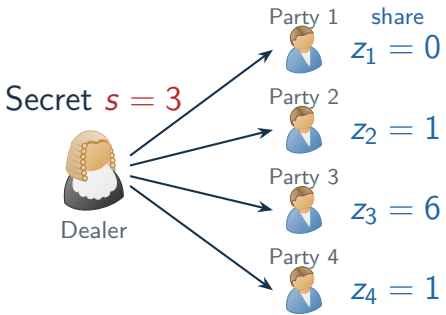
For $1/3 < c < 1/2$, any fixed $u < 1/2$ works. Smaller c needs smaller permitted u.

Sources: Reconstruction-based LSB attack: Maji et al., ITC 2022.

A four-party leakage experiment

$$\mathbb{F}_7, \qquad P_s(X) = s + AX + BX^2, \qquad A, B \xleftarrow{\$} \mathbb{F}_7$$

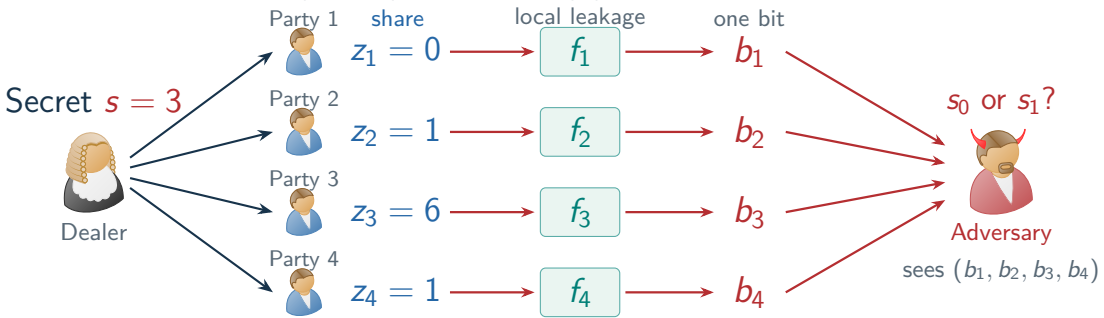
Public $a = (1, 2, 3, 4)$; shares $z_i = P_s(a_i)$. Snapshot: $s = 3$, $A = B = 2$.



A four-party leakage experiment

$$\mathbb{F}_7, \qquad P_s(X) = s + AX + BX^2, \qquad A, B \xleftarrow{\$} \mathbb{F}_7$$

Public $a = (1, 2, 3, 4)$; shares $z_i = P_s(a_i)$. Snapshot: $s = 3$, $A = B = 2$.

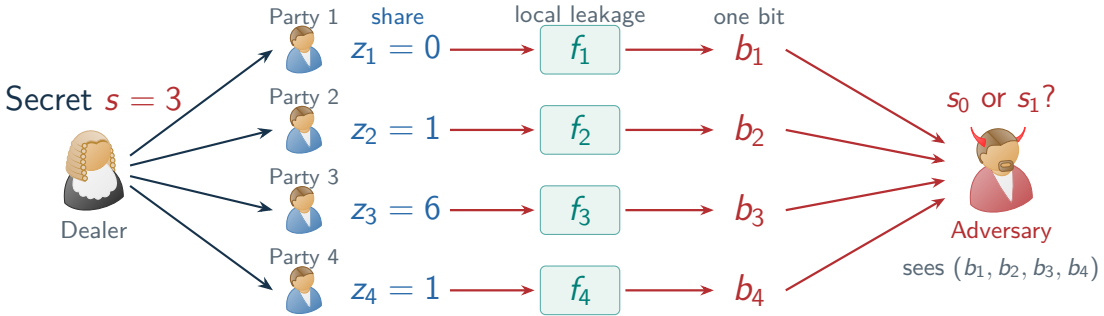


$$\Pr[b_i = 1 \mid z_i] = f_i(z_i), \qquad b_i \in \{0, 1\}$$

A four-party leakage experiment

$\mathbb{F}_7, \qquad P_s(X) = s + AX + BX^2, \qquad A, B \xleftarrow{\$} \mathbb{F}_7$

Public $a = (1, 2, 3, 4)$; shares $z_i = P_s(a_i)$. Snapshot: $s = 3$, $A = B = 2$.



$\phi_i(z) = e_7(u_i z + v_i z^2), \qquad f_i(z) = \frac{1+\mathrm{Re}\,\phi_i(z)}{2}$

$\Pr[b_i = 1 \mid z_i] = f_i(z_i), \qquad b_i \in \{0, 1\}$

u_i and v_i are fixed coefficients specifying party i's leakage rule.

One party: share, phase, leaked bit

$$\phi_i(z) = e_7(u_i z + v_i z^2), \qquad e_7(t) = \exp(2\pi i t/7)$$

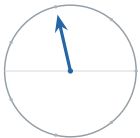
Fixed leakage coefficients $u_i, v_i \in \mathbb{F}_7$. Illustration at Party 2: $u_2 = v_2 = 1$.

Party 2



$z_2 = 1 \in \mathbb{F}_7$

2/7 turn



$\phi_2(1) = e_7(2)$

$$f_i(z) = \frac{1 + \operatorname{Re}\phi_i(z)}{2}$$

$f_2(1) \approx 0.389$

Probability of leaking 1

b_2

$b_2 \in \{0, 1\}$

The sampled bit is the observation; the clock explains its probability.
For the running calculation, we next specialize to linear phases ($v_i = 0$).

One party: share, phase, leaked bit

$$\phi_i(z) = e_7(u_i z + v_i z^2), \qquad e_7(t) = \exp(2\pi i t/7)$$

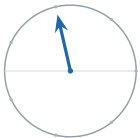
Fixed leakage coefficients $u_i, v_i \in \mathbb{F}_7$. Illustration at Party 2: $u_2 = v_2 = 1$.

Party 2



$z_2 = 1 \in \mathbb{F}_7$

2/7 turn



$\phi_2(1) = e_7(2)$

$$f_i(z) = \frac{1 + \operatorname{Re}\phi_i(z)}{2}$$

$f_2(1) \approx 0.389$

Probability of leaking 1

b_2

$b_2 \in \{0, 1\}$

$$f_i(z) = \tfrac{1}{2} + \tfrac{1}{4}\phi_i(z) + \tfrac{1}{4}\overline{\phi_i(z)}$$

Cosine leakage is a probability map built from two opposite phases.

The sampled bit is the observation; the clock explains its probability.
For the running calculation, we next specialize to linear phases ($v_i = 0$).

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. **Event probabilities are phase sums.**

From probabilities to phases

Given the shares, the coins are independent. Then average over the dealer's randomness.

$$\Pr_s[1111] = \mathbb{E}_{A,B}\left[\prod_{i=1}^{4} f_i(z_i)\right]$$

$$f_i = \frac{1}{2} + \frac{1}{4}\phi_i + \frac{1}{4}\overline{\phi_i}$$

Expanding the product gives a weighted sum of averaged phase products.

NEXT Expose the shared randomness that determines these averages.

Expose the shared randomness

$$P_s(X) = s + AX + BX^2 = s + XQ(X), \qquad Q(X) = A + BX$$

A, B are independent uniform elements of $\mathbb{F}_7$. Snapshot: $s = 3$, $A = B = 2$.

Party 1 

$z_1 = 0$

Party 2 

$z_2 = 1$

Party 3 

$z_3 = 6$

Party 4 

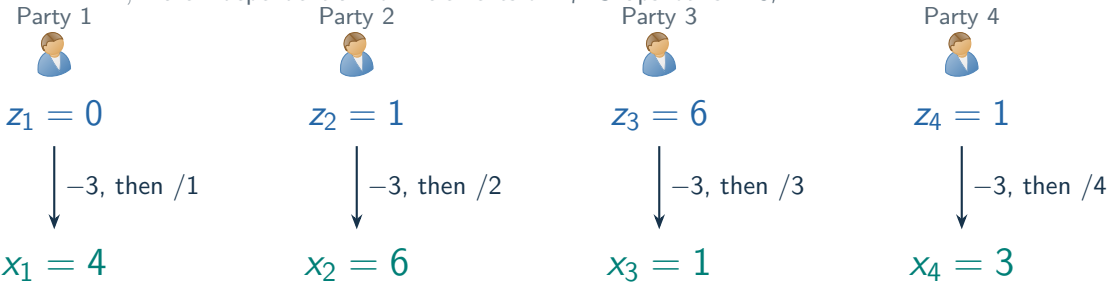
$z_4 = 1$

For fixed s, the rule becomes $g_{i,s}(x) = f_i(s + a_i x)$. The adversary does not subtract the secret. This four-party example illustrates the mechanism; it is not an instance of the asymptotic theorem.

Expose the shared randomness

$$P_s(X) = s + AX + BX^2 = s + XQ(X), \qquad Q(X) = A + BX$$

A, B are independent uniform elements of $\mathbb{F}_7$. Snapshot: $s = 3$, $A = B = 2$.



$$x_i = \frac{z_i - s}{a_i} = Q(a_i) = A + a_i B$$

We will analyze linear phases of these line-code inputs.

For fixed s, the rule becomes $g_{i,s}(x) = f_i(s + a_i x)$. The adversary does not subtract the secret.

This four-party example illustrates the mechanism; it is not an instance of the asymptotic theorem.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. **Normalize to expose randomness.**

One line behind the shares

For a fixed secret, subtract it and divide by each public evaluation point.

$$x_i = \frac{z_i - s}{a_i} = A + a_i B$$

$$g_{i,s}(x) = f_i(s + a_i x)$$

This changes variables only in our analysis. The leakage-event probability is unchanged.

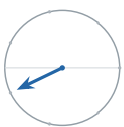
NEXT Find relations that hold for every intercept and slope.

A global relation locks a phase product

$$x_1 - 2x_2 + x_3 = 0 \qquad \text{for every } x_i = A + a_i B$$

$\kappa = (1, -2, 1, 0)$: $\sum_i \kappa_i = 0$ and $\sum_i a_i \kappa_i = 0$. $\kappa_i = u_i a_i$. All arithmetic is modulo 7.

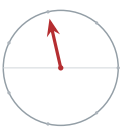
Party 1: $x_1 = 4$



4/7 turn

$e_7(x_1)$

Party 2: $x_2 = 6$



2/7 turn

$e_7(-2x_2)$

Party 3: $x_3 = 1$



1/7 turn

$e_7(x_3)$

Party 4: $x_4 = 3$



0/7 turn

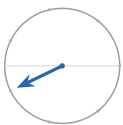
1

A global relation locks a phase product

$$x_1 - 2x_2 + x_3 = 0 \qquad \text{for every } x_i = A + a_i B$$

$\kappa = (1, -2, 1, 0)$: $\sum_i \kappa_i = 0$ and $\sum_i a_i \kappa_i = 0$. $\kappa_i = u_i a_i$. All arithmetic is modulo 7.

Party 1: $x_1 = 4$



4/7 turn

$e_7(x_1)$

Party 2: $x_2 = 6$



2/7 turn

$e_7(-2x_2)$

Party 3: $x_3 = 1$



1/7 turn

$e_7(x_3)$

Party 4: $x_4 = 3$



0/7 turn

1

$$\prod_i e_7(\kappa_i x_i) = e_7(0) = 1$$



The snapshot makes one full turn: $4 + 2 + 1 = 7$. The product stays 1 as A, B vary.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. **Relations fix phase products.**

Expand the actual probabilities

$$\Pr[1111] = \mathbb{E}[\textstyle\prod_i f_i(x_i)]$$

Expanding this product selects one term from each local function.

A fixed product must also occur

This product is one for every choice of the dealer's randomness.

$$x_1 - 2x_2 + x_3 = 0$$

$$\textstyle\prod_i e_7(\kappa_i x_i) = 1$$

$$\kappa = (1, -2, 1, 0)$$

It contributes only if each local expansion supplies its required phase with a nonzero coefficient.

NEXT Check whether each party supplies its required phase in this product.

A relation needs matching local frequencies

$f_1 = f_3 = f, \quad f_4 = 1, \qquad f(x) = \frac{1}{2} + \frac{1}{4}e_7(x) + \frac{1}{4}e_7(-x) = \frac{1+\cos(2\pi x/7)}{2}$

Expanding the product means choosing one term from each local function.

Party 1	Party 2	Party 3	Party 4
			
Required phases for $(1, -2, 1, 0)$			
$e_7(x_1)$	$e_7(-2x_2)$	$e_7(x_3)$	1
Filled dots: nonzero coefficients. Rings: required frequencies.			
			
Supplied	**Frequency -2 is missing**	Supplied	Constant supplied

Initially $f_2 = f$: its expansion has no $e_7(-2x)$ term.

This invariant product never appears in the expansion.

Only Party 2's leakage rule changes. The code and its global relation stay the same.

A relation needs matching local frequencies

$$f_1 = f_3 = f, \quad f_4 = 1, \qquad f(x) = \tfrac{1}{2} + \tfrac{1}{4}e_7(x) + \tfrac{1}{4}e_7(-x) = \tfrac{1+\cos(2\pi x/7)}{2}$$

Expanding the product means choosing one term from each local function.

Party 1	Party 2	Party 3	Party 4
Required phases for $(1, -2, 1, 0)$			
$e_7(x_1)$	$e_7(-2x_2)$	$e_7(x_3)$	1
Filled dots: nonzero coefficients. Rings: required frequencies.			
			
Supplied	**Now supplied**	Supplied	Constant supplied

Change only Party 2: $f_2(x) = \tfrac{1+\cos(4\pi x/7)}{2} = \tfrac{1}{2} + \tfrac{1}{4}e_7(2x) + \tfrac{1}{4}e_7(-2x)$.

Every party now supplies its phase: the product has nonzero weight.

Only Party 2's leakage rule changes. The code and its global relation stay the same.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. **Local support selects the terms.**

Two separate checks

1. Required terms appear locally.
2. Their product survives averaging.

Our chosen product passes both.

Each party supplies a factor

Its coefficient w is the product of the chosen local coefficients.

One term missing: $w = 0$

All terms present: $w \neq 0$

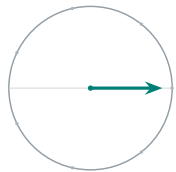
After changing Party 2, our chosen product occurs with nonzero weight and has average one.

NEXT Average the other available products to determine which survive.

Which products survive averaging?

Choose one supported frequency at each party, then average over A, B.

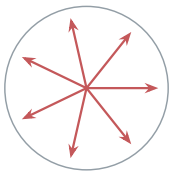
$(1, -2, 1, 0)$



Phase exponent is always 0.
Every product points in the same direction.

$$\mathbb{E}[\text{product}] = 1$$

$(1, 2, 1, 0)$



Phase exponent is $4A + B$.
Varying A visits all seven directions.

$$\mathbb{E}[\text{product}] = 0$$

Both tuples occur in the tuned cosine readouts. Only one satisfies both moment equations.
This exact zero statement concerns linear phases. Quadratic phases are treated separately.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. **Averaging filters linear phases.**

Two tests for a contribution

In this linear-phase example, a supported product averages to one exactly when both moments vanish.

$$\sum_i \kappa_i = 0, \qquad \sum_i a_i \kappa_i = 0$$

Otherwise its average is 0.

A term must occur locally and satisfy the global equations. Quadratic averages need a separate bound.

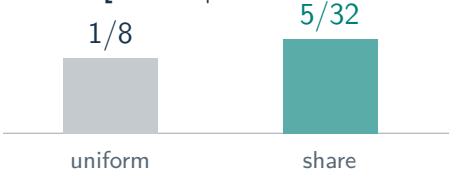
NEXT Add the coefficients of the products that survive.

Add the weights of the surviving products

Only three of the 27 expanded terms survive averaging.

Frequency tuple	Phase product	Coefficient (weight)
$(0,0,0,0)$	1	$\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot 1=\frac{1}{8}$
$(1,-2,1,0)$	$e_7(x_1-2x_2+x_3)=1$	$\frac{1}{4}\cdot\frac{1}{4}\cdot\frac{1}{4}\cdot 1=\frac{1}{64}$
$(-1,2,-1,0)$	$e_7(-x_1+2x_2-x_3)=1$	$\frac{1}{4}\cdot\frac{1}{4}\cdot\frac{1}{4}\cdot 1=\frac{1}{64}$

$$\Pr[1111 \mid \text{share from line}] = \frac{1}{8}+\frac{1}{64}+\frac{1}{64}=\frac{5}{32}$$



All-one event gap $1/32$

Party 4 always outputs one, so its constant coefficient is 1.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. **Surviving weights give event bias.**

From surviving terms to bias

Party 4 always outputs one. The zero tuple and the two supported relations contribute:

$$\frac{1}{8} + \frac{1}{64} + \frac{1}{64} = \frac{5}{32}$$

Independent inputs: $\frac{1}{8}$

The all-one event differs by one thirty-second. This compares code inputs with independent inputs.

NEXT Return to the original shares and compare two secrets under the same rules.

Return to the two secrets experiment

$$z_i = s + a_i x_i, \qquad x_i = A + a_i B$$

$$\Pr[b_i = 1 \mid z_i] = h_i(z_i) = \frac{1+\cos(2\pi\lambda_i z_i/7)}{2}, \qquad \lambda = (1, 6, 5, 0)$$

These rules stay fixed. Choose $\lambda_i = \kappa_i / a_i$, so $(\lambda_i a_i)_i = \kappa = (1, -2, 1, 0)$ modulo 7.

One party: the earlier phase gains a secret-dependent angle.

$$e_7(\lambda_i z_i) = \underbrace{e_7(\lambda_i s)}_{\text{depends on } s} \quad \underbrace{e_7(\kappa_i x_i)}_{\text{earlier phase}}$$

Return to the two secrets experiment

$$z_i = s + a_i x_i, \qquad x_i = A + a_i B$$

$$\Pr[b_i = 1 \mid z_i] = h_i(z_i) = \frac{1+\cos(2\pi\lambda_i z_i/7)}{2}, \qquad \lambda = (1, 6, 5, 0)$$

These rules stay fixed. Choose $\lambda_i = \kappa_i / a_i$, so $(\lambda_i a_i)_i = \kappa = (1, -2, 1, 0)$ modulo 7.

Across parties: the earlier cancellation still works.

$$\prod_i e_7(\lambda_i z_i) = e_7\big(s \textstyle\sum_i \lambda_i\big) \cdot 1 = e_7(5s)$$

The normalized phase product is 1. Only the secret-dependent angle remains.

Secret 0



Phase product $= 1$

Secret 3



Phase product $= e_7(1)$

These different angles survive averaging over the dealer's randomness.

Return to the two secrets experiment

$$z_i = s + a_i x_i, \qquad x_i = A + a_i B$$

$$\Pr[b_i = 1 \mid z_i] = h_i(z_i) = \frac{1+\cos(2\pi\lambda_i z_i/7)}{2}, \qquad \lambda = (1, 6, 5, 0)$$

These rules stay fixed. Choose $\lambda_i = \kappa_i / a_i$, so $(\lambda_i a_i)_i = \kappa = (1, -2, 1, 0)$ modulo 7.

Across parties: the earlier cancellation still works.

$$\prod_i e_7(\lambda_i z_i) = e_7\big(s \textstyle\sum_i \lambda_i\big) \cdot 1 = e_7(5s)$$

The normalized phase product is 1. Only the secret-dependent angle remains.

Secret 0



$\Pr[1111] = 5/32$

Secret 3



$\Pr[1111] = \frac{1}{8} + \frac{\cos(2\pi/7)}{32}$

Event gap: $\big(1 - \cos(2\pi/7)\big)/32 \approx 0.0118$

The adversary tests the all-one bit event; the clocks only explain its probability.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. Surviving weights give event bias.
7. **Surviving phases may retain secrets.**

A relation can carry the secret

The rules stay fixed; the remaining phase depends on the secret.

$$\Pr_s[1111] = \frac{1}{8} + \frac{e_7(5s) + e_7(-5s)}{64}$$

$$= \frac{1}{8} + \frac{\cos(2\pi \cdot 5s/7)}{32}.$$

We now compare two secrets under the same local rules. A bit-event gap lower-bounds statistical distance.

NEXT Organize families of relations by their coefficients at each party.

Two relations, viewed one party at a time

Return to the normalized line inputs: $x_i = A + a_i B, \quad a = (1, 2, 3, 4)$.

Coefficient-space toy: two linear relations, with one coefficient column per party.

	Party 1	Party 2	Party 3	Party 4
R_1	t_1	t_2	r_3	r_4
R_2	$2t_1$	$2t_2$	s_3	0
	y_1	y_2	y_3	y_4
	$V_1 = \mathrm{span}(w)$	$V_2 = \mathrm{span}(w)$	$V_3 = \mathbb{F}_7^2$	$V_4 = \mathrm{span}(1, 0)$

Assume these local coefficient spaces: $y_i \in V_i$, with $w = (1, 2)$.

$$\Sigma_i \, y_i = 0, \qquad \Sigma_i \, a_i y_i = 0$$

Both character products equal 1 for every line input.

These are two linear character relations, not the linear/quadratic coefficient pair.
This coefficient profile illustrates the mechanism; the general proof must obtain the constraints.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. Surviving weights give event bias.
7. Surviving phases may retain secrets.
8. **Local choices meet global equations.**

Local choices, global equations

In a new coefficient-space toy, each column belongs to an assumed local space.

$$y_i \in V_i$$

$$\sum_i y_i = 0, \qquad \sum_i a_i y_i = 0$$

The columns encode two linear character relations. The global equations couple the local choices.

NEXT Combine the global equations to force a constraint at each party.

One short row makes the constraints local

Use $\mathbf{h} = (2, -1)$ at every party. Set $\eta_i = \mathbf{h}^\mathsf{T} y_i$.

$\mathbf{h}^\mathsf{T} w = 2 \cdot 1 - 1 \cdot 2 = 0$

$\eta_1 = 0$ $\eta_2 = 0$ $\eta_3 = 2r_3 - s_3$ $\eta_4 = 2r_4$



Pale blue: locally allowed. Purple: common constraint. Teal: compatible direction. Finite-field schematics.

One short row makes the constraints local

Use $\mathbf{h} = (2, -1)$ at every party. Set $\eta_i = \mathbf{h}^\mathsf{T} y_i$.

$\mathbf{h}^\mathsf{T} w = 2 \cdot 1 - 1 \cdot 2 = 0$

$\eta_1 = 0$ $\quad$ $\eta_2 = 0$ $\quad$ $\eta_3 = 2r_3 - s_3$ $\quad$ $\eta_4 = 2r_4$

$$\eta_3 + \eta_4 = 0, \qquad 3\eta_3 + 4\eta_4 = 0$$

Subtract three times the first equation: $\eta_4 = 0$, then $\eta_3 = 0$.



Pale blue: locally allowed. Purple: common constraint. Teal: compatible direction. Finite-field schematics.

One short row makes the constraints local

Use $\mathbf{h} = (2, -1)$ at every party. Set $\eta_i = \mathbf{h}^\mathsf{T} y_i$.

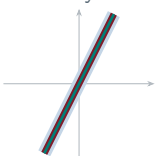
$\mathbf{h}^\mathsf{T} w = 2 \cdot 1 - 1 \cdot 2 = 0$

$\eta_1 = 0$ $\quad$ $\eta_2 = 0$ $\quad$ $\eta_3 = 2r_3 - s_3$ $\quad$ $\eta_4 = 2r_4$

$$\eta_3 + \eta_4 = 0, \qquad 3\eta_3 + 4\eta_4 = 0$$

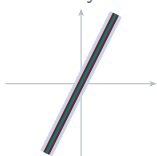
Subtract three times the first equation: $\eta_4 = 0$, then $\eta_3 = 0$.

Party 1



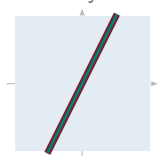
Line $\to$ same line

Party 2



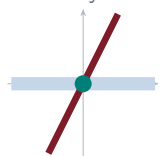
Line $\to$ same line

Party 3



Plane $\to$ line

Party 4



Horizontal line $\to \{0\}$

$2y_{i,1} - y_{i,2} = 0$ **at every party.**

Pale blue: locally allowed. Purple: common constraint. Teal: compatible direction. Finite-field schematics.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. Surviving weights give event bias.
7. Surviving phases may retain secrets.
8. Local choices meet global equations.
9. **A short row gives local constraints.**

From certificate to phase angles

$\mathbf{h} = (2, -1), \qquad \mathbf{h}^{\mathsf{T}} y_i \equiv 0 \pmod 7$

For normalized input $q \in \mathbb{F}_7$, multiply the equation by $q/7$:

$$\Theta_i(q) = \frac{q}{7}\, y_i \pmod 1$$

$$\downarrow$$

$$\mathbf{h}^{\mathsf{T}} \Theta_i(q) \equiv 0 \pmod 1$$

$$2\theta_{i,1} - \theta_{i,2} \equiv 0 \pmod 1$$

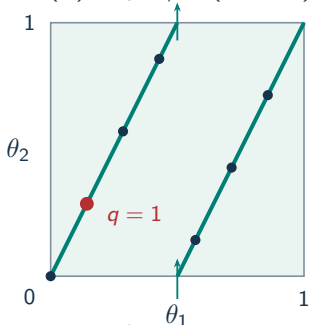
One angle now determines the pair.

NEXT Picture the allowed curve on the torus, then simplify the leakage readout.

A local equation confines the torus motion

Choose $(y_1, y_2, y_3, y_4) = (w, -2w, w, 0), \quad w = (1, 2).$

$\Theta_i(q) = y_i q/7 \pmod 1$ $\qquad H = \{(t, 2t) \pmod 1 : t \in \mathbb{R}/\mathbb{Z}\}$



Identify opposite edges.

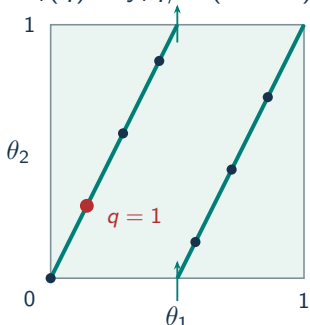
All four local orbits lie in H; party 4 stays at $(0, 0)$.

Party 1 visits seven points on a continuous carrier curve. Clocks are analysis tools.

A local equation confines the torus motion

Choose $(y_1, y_2, y_3, y_4) = (w, -2w, w, 0), \quad w = (1, 2)$.

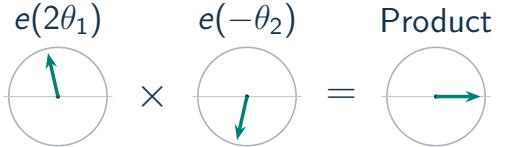
$\Theta_i(q) = y_i q/7 \pmod 1$



Identify opposite edges.

$$H = \{(t, 2t) \pmod 1 : t \in \mathbb{R}/\mathbb{Z}\}$$

At party 1, input $q = 1$:



$$e(2\theta_1)e(-\theta_2) = e(2\theta_1 - \theta_2) = 1$$

All four local orbits lie in H; party 4 stays at $(0, 0)$.

Party 1 visits seven points on a continuous carrier curve. Clocks are analysis tools.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. Surviving weights give event bias.
7. Surviving phases may retain secrets.
8. Local choices meet global equations.
9. A short row gives local constraints.
10. **Local phase orbits lie on a curve.**

Local phases lie on a curve

$$\Theta_i(q) = (t, 2t) \pmod 1$$

We need a bit probability at each angle pair. Define the **readout**:

$$C : (\mathbb{R}/\mathbb{Z})^2 \longrightarrow [0,1]$$

$$\Pr[b_i = 1 \mid x_i = q] = C\Big(\Theta_i(q)\Big)$$

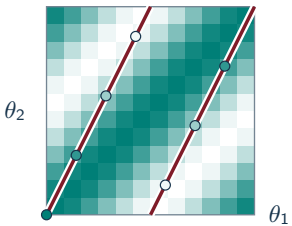
C comes from the leakage rule.
The curve tells us where to evaluate it.

NEXT Use the curve equation to express the same bit probability with one angle.

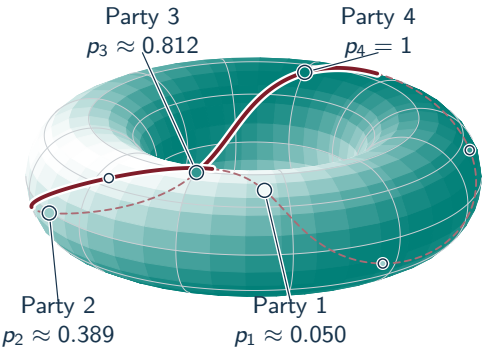
Restrict to the surviving curve

$$C(\theta_1, \theta_2) = \tfrac{1}{2} + \tfrac{1}{2}\cos\big(2\pi(\theta_2 - \theta_1)\big)$$

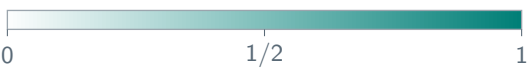
Readout on the torus



Flat view: identify opposite edges.



Probability of a leaked 1

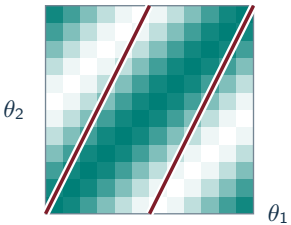


Same color: same probability. Purple: the surviving curve H.

Restrict to the surviving curve

$$C(\theta_1, \theta_2) = \tfrac{1}{2} + \tfrac{1}{2}\cos\big(2\pi(\theta_2 - \theta_1)\big)$$

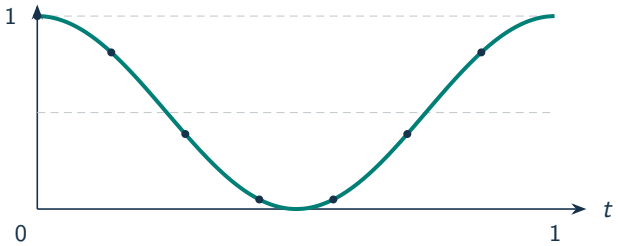
Readout on the torus



Darker: larger probability.
Purple: H.

restrict to H

$$C(t, 2t) = \tfrac{1}{2} + \tfrac{1}{2}\cos(2\pi t)$$

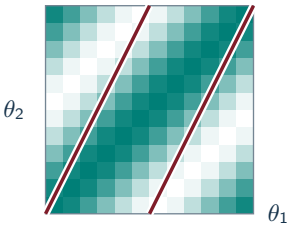


Displayed sets are local Fourier supports.

Restrict to the surviving curve

$$C(\theta_1, \theta_2) = \tfrac{1}{2} + \tfrac{1}{2}\cos\big(2\pi(\theta_2 - \theta_1)\big)$$

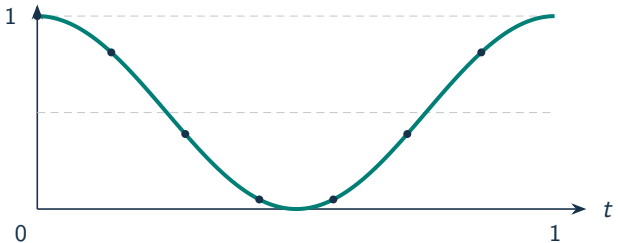
Readout on the torus



Darker: larger probability.
Purple: H.

restrict to H

$$C(t, 2t) = \tfrac{1}{2} + \tfrac{1}{2}\cos(2\pi t)$$



Use the same tuple $(w, -2w, w, 0)$.

Party 1	Party 2	Party 3	Party 4
$\{0, \pm 1\}$	$\{0, \pm 2\}$	$\{0, \pm 1\}$	$\{0\}$

We are back to the cosine rules analyzed earlier.

Displayed sets are local Fourier supports.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. Surviving weights give event bias.
7. Surviving phases may retain secrets.
8. Local choices meet global equations.
9. A short row gives local constraints.
10. Local phase orbits lie on a curve.
11. **Restricted readouts give cosines.**

Back to the cosine calculation

On the curve, the difference between the two angles is just the first angle.

$$C(t, 2t) = \frac{1 + \cos(2\pi t)}{2}$$

Frequencies: $1,\ -2,\ 1,\ 0$

The chosen columns recover exactly our tuned cosine rules. We can reuse the earlier phase calculation.

NEXT Identify the extra work needed to handle arbitrary leakage functions.

What the example explains

Global relations constrain local geometry; the surviving waves carry the bias.

Relations

$$\sum y_i = 0$$
$$\sum a_i y_i = 0$$

→

Local constraints



$(2, -1)y_i = 0$

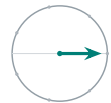
→

Torus readout



→

Surviving weight



add Fourier weights

The toy analyzes one event. The theorem bounds statistical distance, uniformly over every local leakage rule.

What the example explains

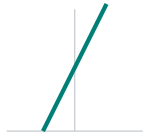
Global relations constrain local geometry; the surviving waves carry the bias.

Relations

$$\sum y_i = 0$$
$$\sum a_i y_i = 0$$

→

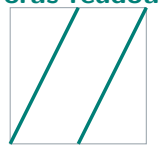
Local constraints



$(2, -1)y_i = 0$

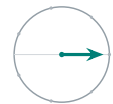
→

Torus readout



→

Surviving weight



add Fourier weights

What the full proof adds

Approximate arbitrary leakage by structured probability maps.

Produce short certificates and control the total weight of many relations.

The toy analyzes one event. The theorem bounds statistical distance, uniformly over every local leakage rule.

Takeaway: the proof so far

From local probabilities to leakage resilience.

1. Event probabilities are phase sums.
2. Normalize to expose randomness.
3. Relations fix phase products.
4. Local support selects the terms.
5. Averaging filters linear phases.
6. Surviving weights give event bias.
7. Surviving phases may retain secrets.
8. Local choices meet global equations.
9. A short row gives local constraints.
10. Local phase orbits lie on a curve.
11. Restricted readouts give cosines.
12. **Control all rules and outputs.**

From the toy to the theorem

The full proof first approximates arbitrary leakage by structured functions.

Structure $\longrightarrow$ local constraints

$\longrightarrow$ statistical-distance bound

Short certificates simplify the readouts. Quantitative estimates control all surviving contributions and outputs.

NEXT Return to the theorem in the multiplication-friendly degree range.

Leakage resilience below one half

$$0 < c < \tfrac{1}{2}, \quad n = \lceil \log_2 p \rceil, \quad m = \lfloor n^u \rfloor, \quad d = \lfloor cm \rfloor$$

p prime; fixed $u > 0$ sufficiently small depending on c; $n \to \infty$.

$$\mathbb{E}_a \, \mathrm{Insec}(a; d) \leq \left(\frac{2}{\pi}\right)^{(1-o(1))d}$$

Uniform distinct, nonzero public points; optimal up to $o(d)$ in the exponent.

Nearly every tuple works for every secret pair and every local bit rule.

Small positive degree rates are possible with suitable public points and sufficiently large fields.

Leakage resilience below one half

$$0 < c < \tfrac{1}{2}, \quad n = \lceil \log_2 p \rceil, \quad m = \lfloor n^u \rfloor, \quad d = \lfloor cm \rfloor$$

p prime; fixed $u > 0$ sufficiently small depending on c; $n \to \infty$.

$$\mathbb{E}_a \, \mathrm{Insec}(a; d) \leq \left(\frac{2}{\pi}\right)^{(1-o(1))d}$$

Uniform distinct, nonzero public points; optimal up to $o(d)$ in the exponent.

Nearly every tuple works for every secret pair and every local bit rule.

Structure the leakage
Arbitrary bit rules
$\longrightarrow$ structured functions

$\longrightarrow$

Constrain it locally
Global equations
$\longrightarrow$ local constraints

$\longrightarrow$

Bound the leakage bias
Control total weights
across all output events

Multiplication-friendly Shamir sharing
can resist one bit of leakage from every share.

Small positive degree rates are possible with suitable public points and sufficiently large fields.