ISC 2026 · INFORMATION SECURITY CONFERENCE



CRSF

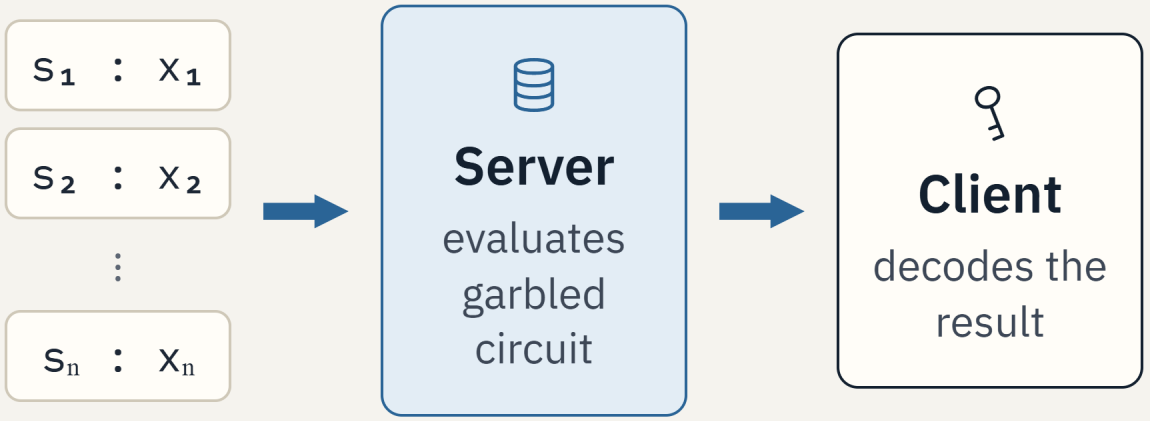
Collusion-Resilient Privacy-Preserving Sensor Fusion with Byzantine-Robust Participation

Chao Yin[1] [2], Haihong Tian[3], Zheng Yang[3], Haibin Zhang[4] [5], Fabio Massacci[1] [6], **Chenglu Jin[2]**

[1] VU Amsterdam · [2] CWI Amsterdam · [3] Southwest University · [4] Yangtze Delta Region Institute of Tsinghua University · [5] Jiaxing Key Laboratory of Artificial Intelligence and Cyber Resilience · [6] University of Trento

SETTING

Privacy-preserving sensor fusion



Input privacy
Server sees no readings and no result.

Robustness
Malicious sensors cannot bias the result.

Output delivery
Client always gets the result if sensors and server don’t collude.

BACKGROUND

How a garbled gate works

AND gate

a	b	c
0	0	0
0	1	0
1	0	0
1	1	1



garble

Garbled table, rows shuffled

Ciphertext	Server has A^1, B^0
$\mathrm{Enc}(A^1, B^1 ; C^1)$	✗
$\mathrm{Enc}(A^0, B^1 ; C^0)$	✗
$\mathrm{Enc}(A^1, B^0 ; C^0)$	opens → C^0
$\mathrm{Enc}(A^0, B^0 ; C^0)$	✗

1 · Garble

Encrypt each output label under its input labels.

2 · Evaluate

One label per input opens exactly one row.

3 · Decode

Only the client maps labels to bits.

BACKGROUND

Garbled circuits and FreeXOR

Wire	bit 0	bit 1
w_1	W_1^0	$W_1^0 \oplus \Delta$
w_2	W_2^0	$W_2^0 \oplus \Delta$
output	Y^0	$Y^0 \oplus \Delta$

The server holds one label per wire and never learns its bit.

Obliviousness

One label reveals nothing about its bit.

Authenticity

No one can forge a different valid output.

FreeXOR: gain and price

XOR gates are free, but all wires share one Δ. Two labels of a wire reveal it.

BASELINE

PG: garbled-circuit sensor fusion (CCS 2024)[1]



What PG achieves

Privacy, fault tolerance and guaranteed output, together.

What it trusts

One server decides who counts; all wires share one Δ.

[1] C. Jin et al. PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery. ACM CCS 2024.

Who does what in PG

Offline · client

0 Shares a seed with each sensor → σ^0, σ^1

1 Garbles the fusion circuit (one Δ)

2 Garbles checking and filter gates

Online

3 **Sensor → server:** σ^x for each bit

4 **Server:** checking gates

5 **Client → server:** Hon or Mal label

6 **Server:** filter gates, fusion circuit

7 **Server → client:** output labels

Step 0: each sensor knows **both** σ^0 and σ^1 of its own wires.

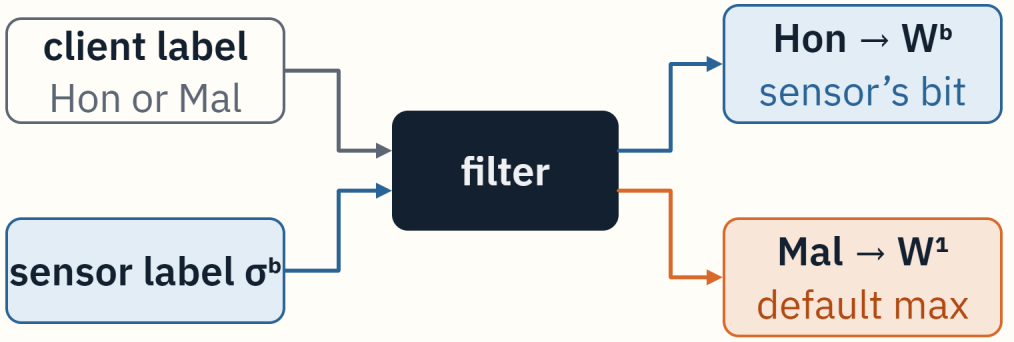
Checking gates and filter gates

Checking gate Checks that a sensor's labels are well-formed and valid.

Filter gate

A server–client protocol: the server claims the admitted sensors; the client releases the matching label.

Nobody checks the claim, but however it reports, the server gets only one output label.



σ labels don't use Δ, but W labels do: Hon label + both σ → both W^0, W^1.

THREAT MODEL

A stronger adversary: sensors collude with a server

One adversary controls some sensors and one server, and pools their views.

Collusion is well documented in sensing systems.

PG's guarantees don't cover it.

Party	Assumption
Sensors	Many corrupted; faulty + absent stay below the fusion threshold
Servers	4 servers, at most 1 Byzantine
Client	Semi-Honest
Network	Sensor → server synchronous; servers partially synchronous
Adversary	Corrupted sensors and server share all views and coordinate the behaviours

LIMITATION 1 · REQUIRES COLLUSION

A colluding sensor leaks the global offset Δ

STEP 1

Server says the colluding sensor passed.

STEP 2

Client releases the Hon-branch labels.

STEP 3

Sensor knows σ^0 and σ^1: evaluate twice → W^0, W^1.

STEP 4

XOR the two labels:

$$W^0 \oplus W^1 = \Delta$$

Privacy broken

Δ turns any label into its complement: honest inputs leak.

Integrity broken

Output labels ⊕ Δ still decode, to a flipped result.

LIMITATION 2 · COLLUSION MAKES IT PRECISE

One server alone decides who participates

WHAT THE SENSORS SUBMIT



WHAT A COLLUDING SERVER ADMITS



Example: 7 sensors, fewer than 1/3 may be faulty. × = dropped.

4 / 7

count as faulty: 2 malicious kept, 2 honest dropped

Above 1/3: the result can be steered.

Colluding: drops exactly the honest sensors.

CRSF at a glance

1 An honest submission cannot be dropped.

2 Servers can rebuild only the agreed label.

0 **Offline:** client garbles; per-server filter gates

1 **Submit:** sensors sign, send to all 4 servers

2 **Agree:** PBFT decides (Hon, r_i) or Mal

3 **Check:** checking gates → status vector u

4 **Release:** 3 matching u → one label branch

5 **Share:** filter gates output shares of W

6 **Rebuild:** 3 shares → W, then validated

7 **Evaluate:** fusion circuit; 3 matching outputs

Four servers, at most one Byzantine. **Blue** steps realize principle 1, **orange** steps principle 2.

MECHANISM 1 · AGREEMENT

Evidence-supported agreement

1. **Signed submissions**
   Sensor signs H(r) per server, sends to all 4.
2. **Signed reports**
   After T_sub: each server reports Sub or NoSub.
3. **Evidence rule**
   3 reports; ≥ 2 matching r → (Hon, r), else Mal.
4. **PBFT**
   Backups reject outcomes not derived from evidence.

Why an honest sensor can't be dropped

It reaches every honest server in time.

Any 3 reports hold ≥ 2 honest copies of r.

So a Mal proposal is invalid.

PBFT: all honest servers agree.

Agreement under attack: four cases

Honest sensor, Byzantine primary

Backups reject Mal; silence → view change.

→ **(Hon, r)**

Honest sensor, Byzantine backup

Any evidence set holds 2 honest Sub reports.

→ **(Hon, r)**

Equivocating sensor

Sends r to some servers, r′ to others.

→ **(Hon, r) or Mal, same everywhere**

Silent or late sensor

Nothing arrives before T_sub.

→ **Mal (default value)**

So: no honest sensor is dropped, the remaining malicious ones stay within the tolerated bound, and all honest servers agree on who participates.

MECHANISM 2 · THRESHOLD LABELS

Threshold-protected circuit-input labels

Server_1
gate on the agreed σ^b
→ share of W^b

Server_2
gate on the agreed σ^b
→ share of W^b

Server_3
gate on the agreed σ^b
→ share of W^b

Server_4 · Byzantine
gate fed both σ^0 and σ^1
→ shares of W^b, W^{1-b}

(3, 4) threshold

3 or 4 shares → the full label

1 or 2 shares → nothing at all

Coalition's view of one wire

Label	Shares held	Learns
W^b (agreed)	4 of 4	W^b, needed anyway
W^{1-b} (other)	1 of 4	nothing

$\Delta = W^b \oplus W^{1-b}$ needs both labels, so Δ stays hidden.

Who sends what, online

Phase	From → to	Payload
Submit	sensor → 4 servers	label vector r + signature
Report	backups → primary	signed Sub / NoSub reports
Agree	primary ↔ backups	pre-prepare + evidence, prepare, commit
Status	servers → client	status vector u
Release	client → each server	one branch of its filter labels
Share Reconstruction	servers ↔ servers	filter-gate output shares
Output	servers → client	output-label vector

Sensors send once; the client only votes, releases, decodes.

SECURITY

What CRSF guarantees

THEOREM 1

Privacy

The coalition learns nothing beyond public leakage: no honest inputs, no output.

THEOREM 2

Correctness with explicit abort

The client outputs $\perp$ or the correct result.

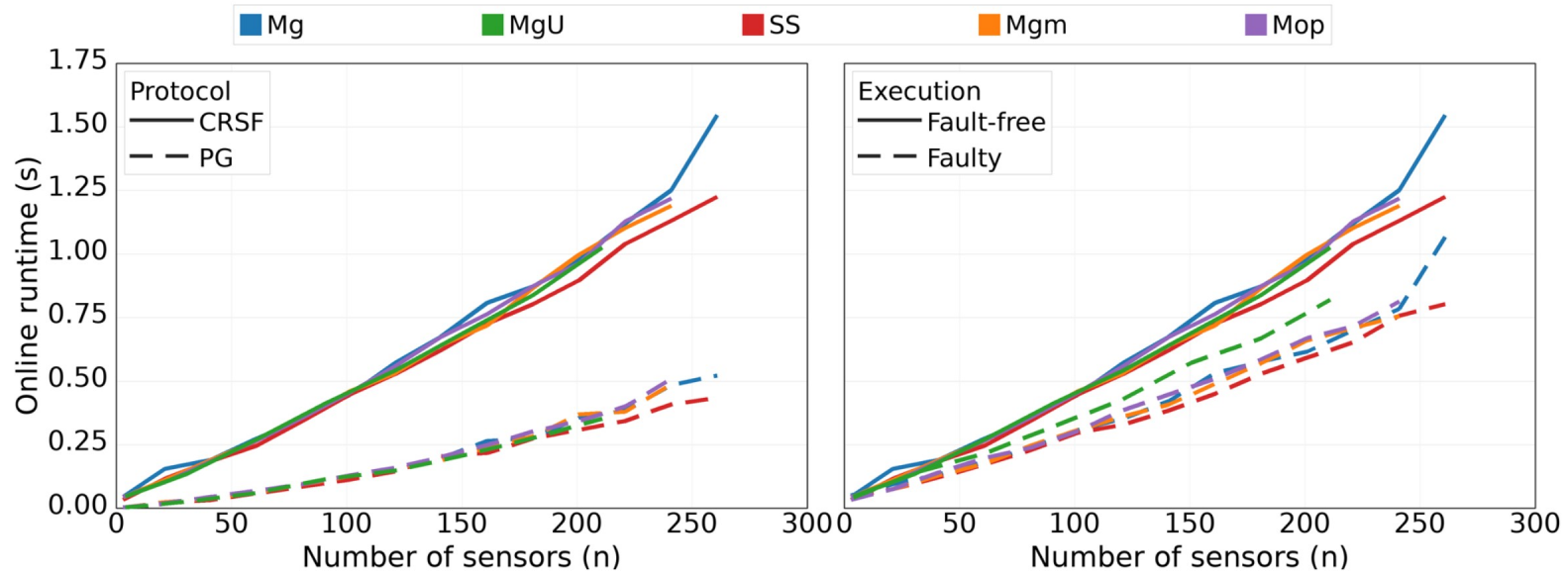
THEOREM 3

Liveness

The client eventually outputs the result or $\perp$.

EVALUATION

Online runtime vs. number of sensors



Left: CRSF (solid) vs. PG (dashed). Right: fault-free (solid) vs. faulty (dashed).

Setup

C++ · 5 GCP VMs · PG's 5 circuits · 3–261 sensors

Linear scaling

Linear in n with four servers.

Price of robustness

PG ≈ 0.5 s vs. CRSF ≈ 1.2–1.5 s at 261 sensors.

EVALUATION

Where the extra time goes

< 0.51 s
PBFT · 7.8–9.7 MB

< 0.14 s
Rebuild · 1.2–1.5 MB

1.0–1.5 s
Total · 211–261 sensors

Circuit	n	BFT agreement	Reconstruction	Total online
Mg	261	488.0	115.7	1546.0
MgU	211	426.4	122.9	1025.2
SS	261	506.5	138.2	1224.2
Mgm	241	481.7	128.6	1189.7
Mop	241	472.3	139.3	1217.8

Wall time in ms, largest tested instance per circuit (paper, Table 1).

SUMMARY

Collusion-resilient sensor fusion is practical

Problem: PG under collusion

Collusion leaks Δ and lets one server drop exactly the honest sensors.

Mechanism 1: Byzantine agreement

Signed evidence + PBFT: honest sensors can’t be dropped.

Mechanism 2: threshold labels

(3, 4)-shared labels: never two labels of one wire in the fusion circuit.

Guarantees and cost

Privacy, correctness, liveness; ≈ 1–1.5 s for 200+ sensors.

Chenglu Jin · CWI Amsterdam · chenglu.jin@cwi.nl

Questions?