Secure Multiparty Computation:

Using Information-Theoretic MPC with No Honest Majority

Yuval Ishai
Technion

Message of this talk

- IT MPC is useful even when there is no honest majority!
- Establishes unexpected connections between different areas in cryptography
- New results for ZK and MPC with no honest majority
- New application domains for IT MPC

Allison

Research interests:
- zero-knowledge proofs
- efficient two-party protocols

Bernard

Research interests:
- information-theoretic cryptography
- honest-majority MPC

some relevance →

← no relevance?

Allison

Bernard

Research interests:

- zero-knowledge proofs
- efficient two-party protocols

Research interests:

- information-theoretic cryptography
- honest-majority MPC

Want to hear about my latest and coolest VSS protocol?

what a dork…

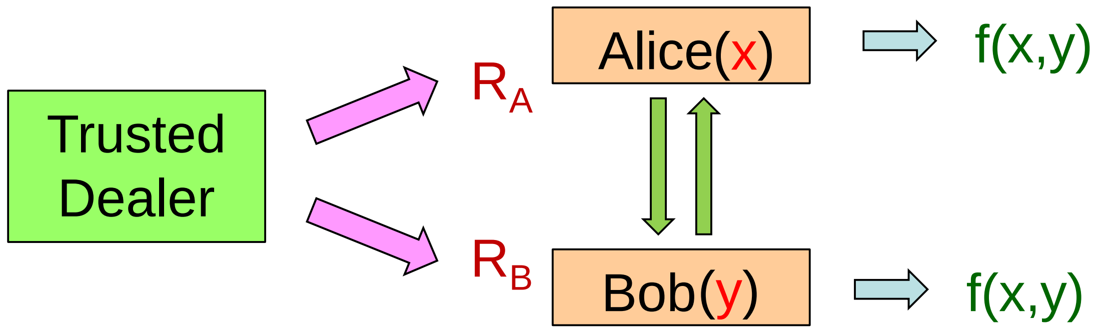
Helping make the match

- Add to Allison's world a simple ideal functionality
  - Ideal commitment oracle for ZK (Com-hybrid model)
  - Ideal OT oracle for general protocols (OT-hybrid model)
  - … or even a general source of correlated randomness
- Makes unconditional (and UC) security possible
  - Analogous to secure channels in Bernard's world
- Why should Allison be happy?
  - Generality: Com or OT can be realized in a variety of models, under a variety of assumptions
  - Efficiency: Correlated randomness can be generated offline. Com or OT can be realized with little overhead
    - Cheap preprocessing: fast OT […,PVW08], faster OT extension [Bea96,IKNP03…,BCGIKRS19]

MPC with
Correlated Randomness

Dealer-Aided Protocol

[I-Kushilevitz-Meldgaard-Orlandi-Paskin13]



- Correlated randomness:
  - Set G[x',y'] = f[x'-dx, y'-dy] for random dx, dy
  - Secret-share G into G_A,G_B
  - Alice gets R_A=(G_A,dx) Bob gets R_B=(G_B,dy)
- Protocol on inputs (x,y):
  - Alice sends x'=x+dx, Bob sends y'=y+dy
  - Alice sends z_A= G_A[x',y'], Bob sends z_B= G_B[x',y']
  - Parties output $z=z_A+z_B$

Dealer-Aided Protocol

- The good:
  - Perfect security
  - Great online communication
- The bad:
  - Exponential size randomness and storage
- Can we use less randomness?
  - Yes if f has small circuit complexity
  - Idea: process f gate-by-gate
  - Coming up…

Dealer-Aided Protocol

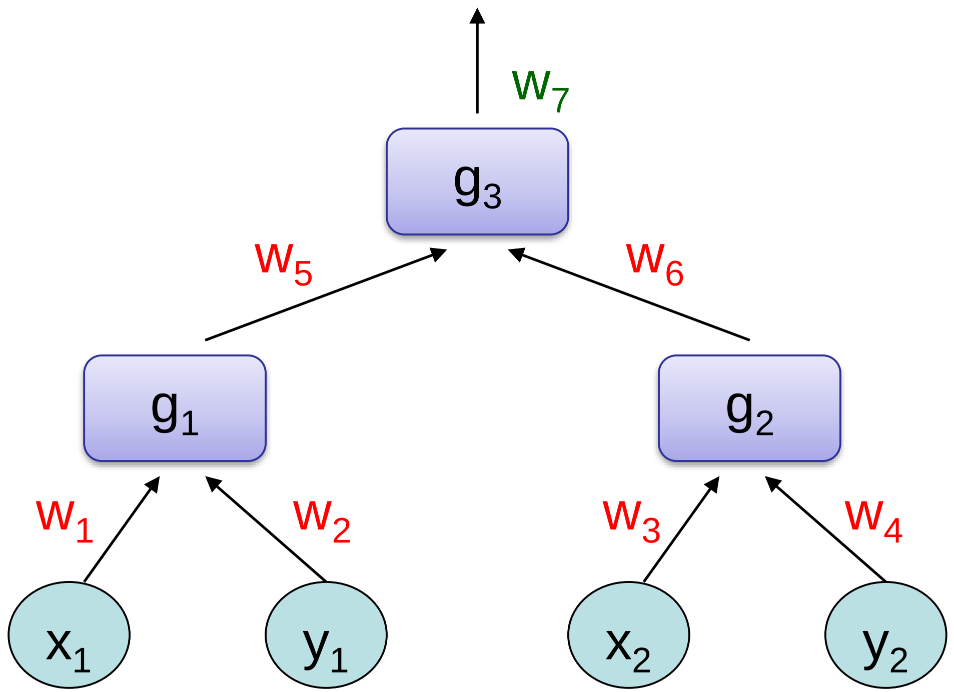
- The good:
  - Perfect security
  - Great online communication
- The bad:
  - Exponential size randomness and storage
- Can we use less randomness for every f?

Dealer-Aided Protocol

- The good:
  - Perfect security
  - Great online communication
- The bad:
  - Exponential size randomness and storage
- Can we use less randomness for every f?
  - Yes!
  - Upper bound: $2^{O\sim(\sqrt{k})}$ [Beimel-I-Kumaresan-Kushilevitz14]
  - Two-way relation with to 3-server IT PIR [Chor-Goldreich-Kushilevitz-Sudan95,Yekhanin07,Efremenko09]
  - Best known lower bound: $\Omega(k)$

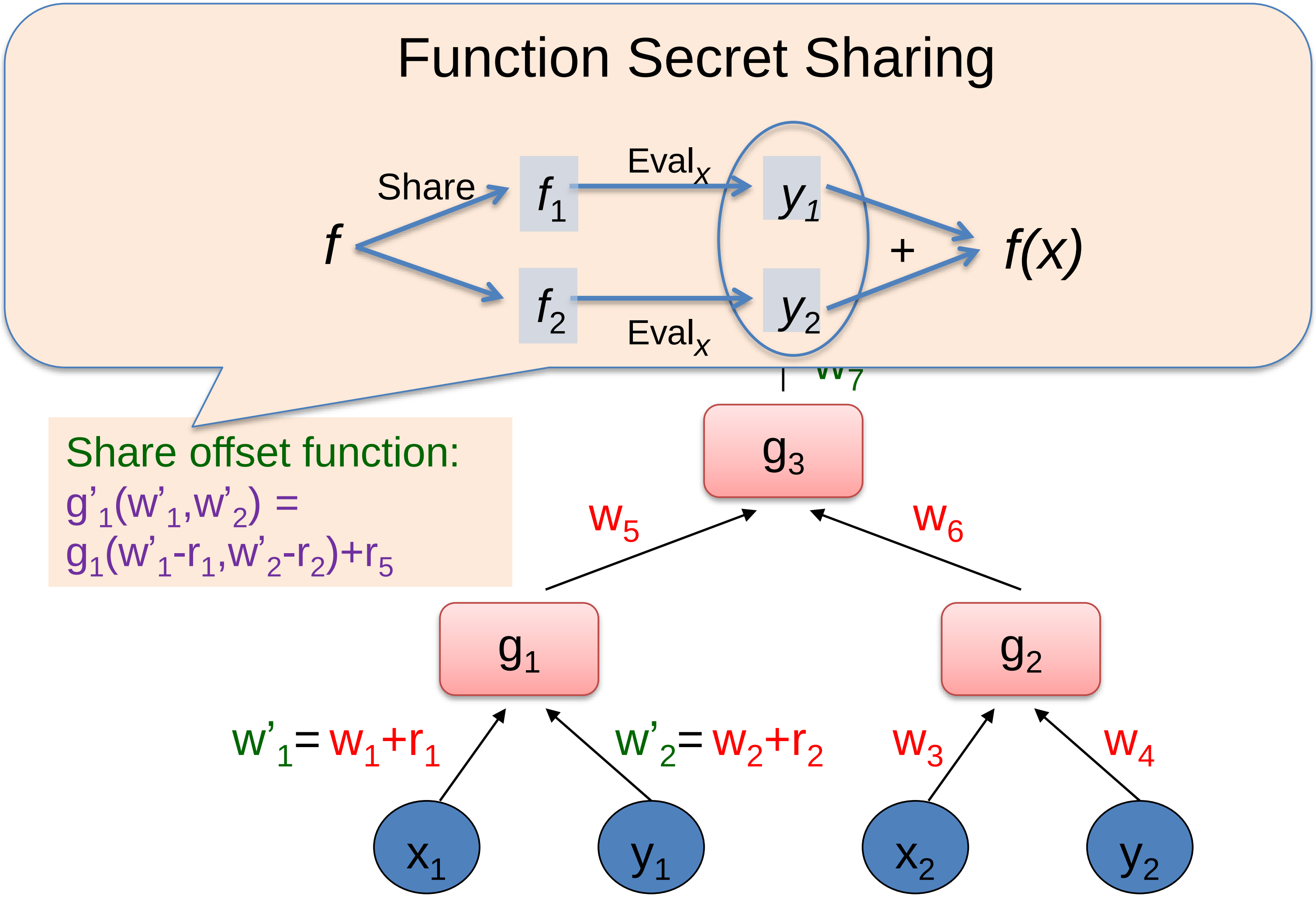
From Truth-Tables to Circuits

[Beaver95, Damgård-Nielsen-Nielsen-Ranellucci17, Boyle-Gilboa-I19]



- Dealer prepares a random mask r_i for every wire w_i.
- Sends to each party masks of its input wires
- Reveals masks of output wires

cuits



- Dealer prepares a random mask r_i for every wire w_i.
- Sends to each party masks of its input wires
- Reveals masks of output wires

From Truth-Tables to Circuits

Gate type	Offset class	FSS
Arbitrary	All functions	Additively share truth-table
Ring multiplication	Degree-2 poly. in 2 variables	Additively share 4 coefficients (compressible to 1)
Equality, Greater-than, ReLU, Bit-decompos Spline,…	Point functions, Union of intervals	Efficient PRG-based constructions [Boyle-Gilboa-I16]

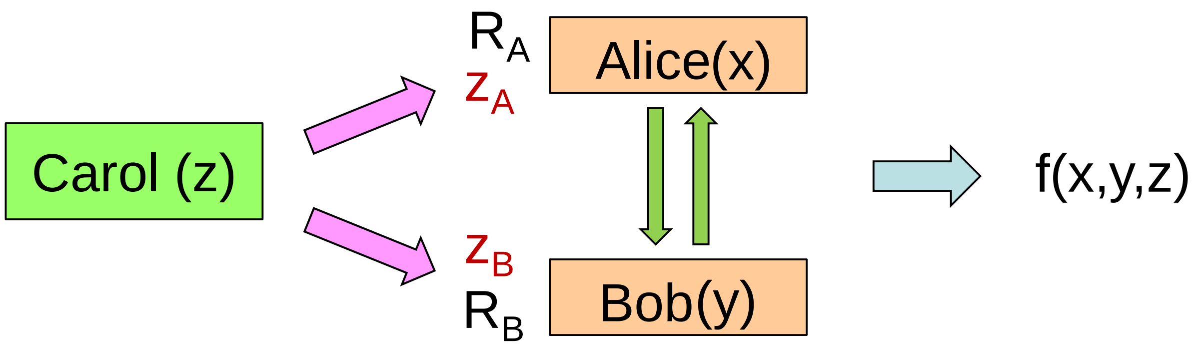
Almost in scope of school…

Features of Circuit-Based Protocol

- Online computation near-optimal for standard gates
  - Meets ideal “small overhead” goal over very fast networks
- Easy to extend to n>2 parties and active adversary [Bendlin-Damgård-Orlandi-Zakarias11, Damgård-Pastro-Smart-Zakarias12]
  - Using simple homomorphic MAC
  - Serves as basis for the “SPDZ” line of protocols
- What about the dealer?
  - Emulate via a secure MPC protocol
    - Offline, input-independent preprocessing, simple functionality
    - New techniques for efficient MPC with “silent preprocessing” […, Boyle-Couteau-Gilboa-I-Kohl-Scholl19, …]
  - Coming up: dealer-free protocols

Dealer-free MPC for f(x,y,z)

- Define $f'((x,z_A),(y,z_B)) = f(x,y,z_A+z_B)$



Alternative protocol for passive 3-party honest-majority MPC

Can be generically bootstrapped to efficient n-party MPC using recursive player virtualization and log-depth threshold formulas [Hirt-Maurer01,Cohen-I-Damgård-Kolker-Raz-Rothblum13, Kozachinskiy-Podolskii20]

Helping make the match

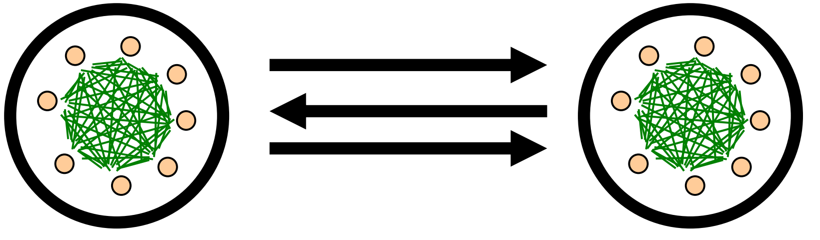
- Add to Allison’s world a simple ideal functionality
  - Ideal commitment oracle for ZK (Com-hybrid model)
  - Ideal OT oracle for general protocols (OT-hybrid model)
  - … or even general s… of … ted randomness
- Ma… …ity possible
  - … s world
- … a variety of models,
- … can be generated offline
- Co… …ed with little overhead
  - Chea… reprocessing: fast OT […,PVW08], faster OT extension [Bea9… NP03…,BCGIKRS19]

A high level idea:

- Run MPC “in the head”.
- Commit to generated views.
- Use consistency checks to ensure honest majority.

- Still: Why should Bernard’s research be relevant?

MPC in the Head



Back to the 1980s

- Zero-knowledge proofs for NP [GMR85,GMW86]
- Computational MPC with no honest majority [Yao86, GMW87]
- Unconditional MPC with honest majority [BGW88, CCD88, RB89]
- Unconditional MPC with no honest majority assuming ideal OT [Kilian88]

- Are these unrelated?

Passive vs. Active Attacks

- Security against active attacks is much more challenging.
  - Life is easier when everyone follows instructions…
  - Even more challenging with no honest majority
    - VSS, error-correcting codes are not directly applicable
- Natural goal:
  passive security → active security

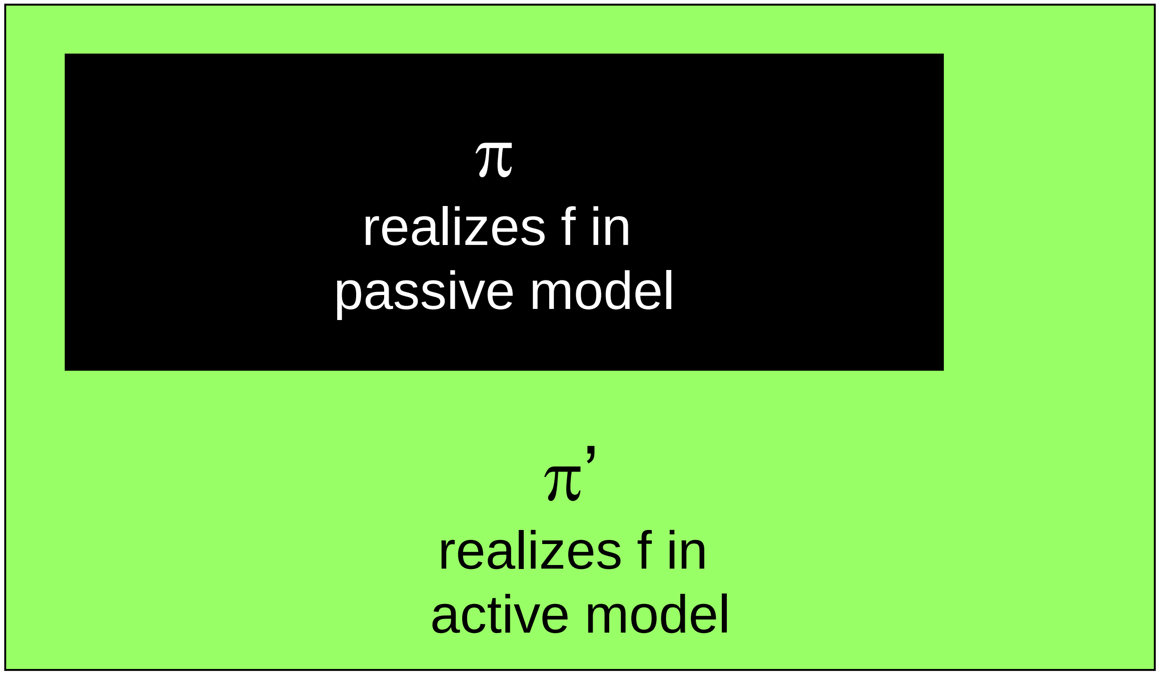
- Major research effort in cryptography

GMW Paradigm

[Goldreich-Micali-Wigderson87]

- GMW compiler:
  - Passive-secure π → active-secure π' with abort (over broadcast)
  - Uses ZK proofs to prove "sticking to protocol"
  - Typically does not apply to IT-MPC protocols
    - Exception: Niv's talk!
- Non-black-box: ZK proofs in π' involve code of π
  - Typically "impractical"
  - Not applicable when π uses an oracle
    - Functionality oracle: secure channels, OT
    - Crypto primitive oracle: black-box PRG
    - Arithmetic oracle: black-box field, ring, non-abelian group,…
- Can these limitations be avoided?

A dream goal



- Possible for some fixed f
  - e.g., OT [IKLP06,Hai08]
- Impossible for general f
  - e.g., ZK functionalities [IKOS07]

IKOS Compiler

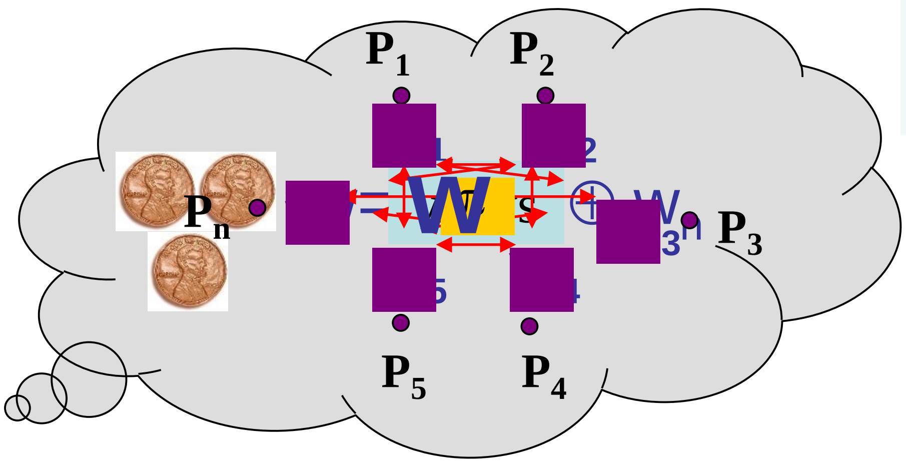
[I-Kushilevitz-Ostrovsky-Sahai07]

- Goal: ZK proof for an NP-relation R(x,w)
  - Completeness
  - Soundness
  - Zero-knowledge

- Towards using MPC:
  - define n-party functionality
    $f(x; w_1,\ldots,w_n) = R(x, w_1 \oplus \ldots \oplus w_n)$
  - use any 2-secure, perfectly correct protocol π for f
    - security in passive model
    - honest majority when $n \geq 5$
    - black-box use of π

Passive MPC → ZK

Given MPC protocol π for
$f(x; w_1,\ldots,w_n) = R(x, w_1 \oplus \ldots \oplus w_n)$



accept iff output=1
&
V_i, V_j are consistent

Prover

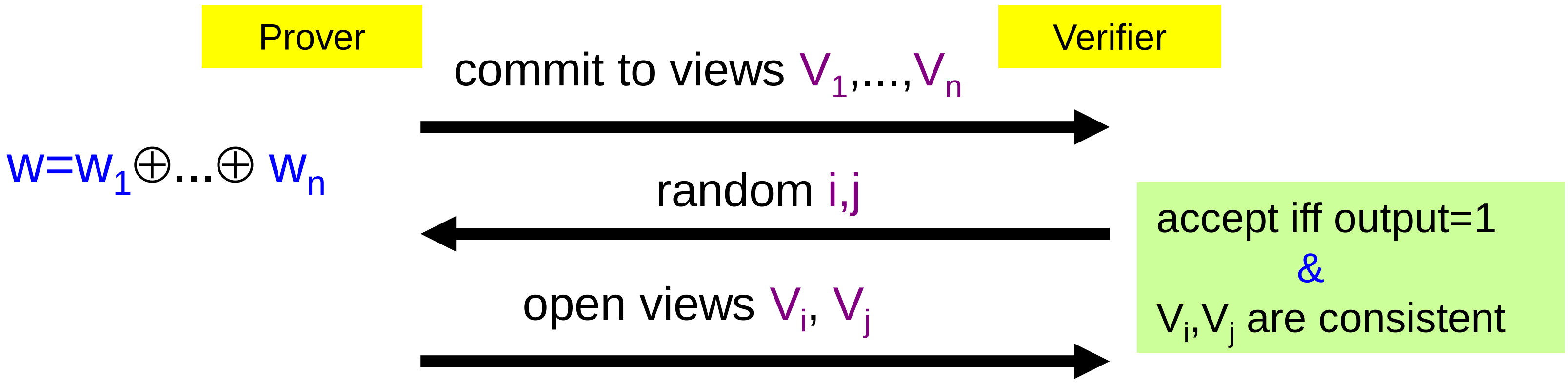
Verifier

commit to views $V_1,\ldots,V_n$ →

random i,j ←

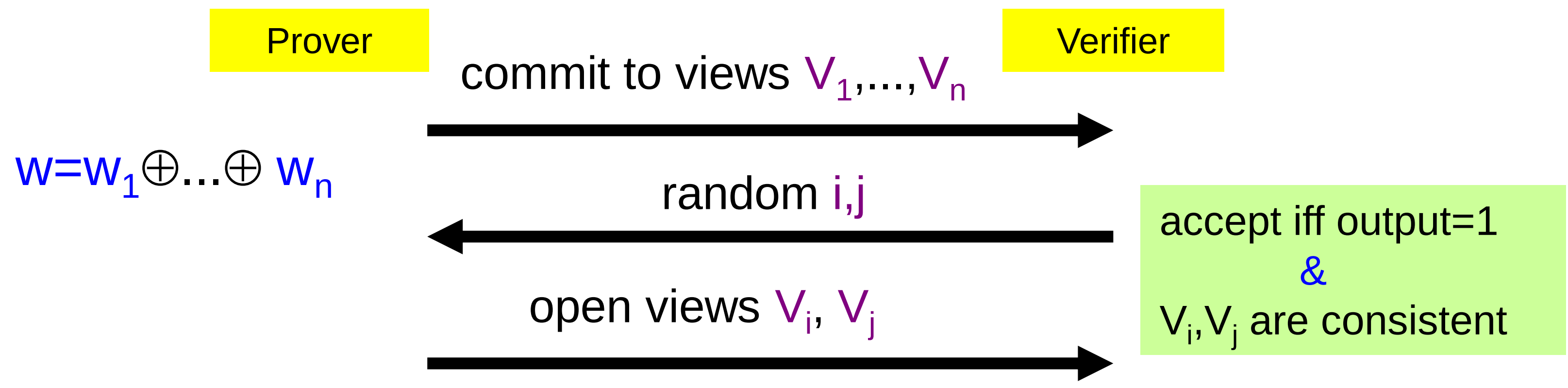
open views V_i, V_j →

Analysis



- Completeness: √
- Zero-knowledge: by 2-security of π and randomness of w_i, w_j.
  (Note: enough to use w_1,w_2,w_3)

Analysis



- **Soundness:** Suppose $R(x, w)=0$ for all w.

  ➔ either (1) $V_1,\ldots,V_n$ consistent with protocol π

  or (2) $V_1,\ldots,V_n$ not consistent with π

  (1) $\Rightarrow$ outputs=0 (perfect correctness)

  $\Rightarrow$ Verifier rejects

  (2) $\Rightarrow$ for some (i,j), V_i,V_j are inconsistent.

  $\Rightarrow$ Verifier rejects with prob. $\geq 1/n^2$.

Extensions

- Use OT-based MPC
  - Check consistency of OT inputs and outputs
  - In fact, can use F-based MPC
- Use 1-secure MPC
  - Open one view and one incident channel
- Directly get 2^{-s} soundness error via active-secure honest-majority MPC
- Realize Com using OWF

Applications

- Simple ZK proofs using:
  - (2,5) or (1,3) semi-honest MPC [BGW88,CCD88,Mau02]
  - (2,3) or (1,2) semi-honest MPC^{OT} [Yao86,GMW87,GV87,GHY87, HV16]
  - Practical [Giacomelli-Madsen-Orlandi16,CDG+17,KKW18]

    ➔ post-quantum signatures!

- ZK proofs with O(|C|) communication
  - (n/5,n) malicious MPC based on AG codes [CC06,DI06,IKOS07]

- Hitting the circuit-size barrier?
  - Sublinear ZK for special tasks: linear algebra, non-abelian groups,…
  - Even for general circuits ~ $|C|^{1/2}$ communication

    Ligero [Ames-Hazay-I-Venkitasubramaniam17]

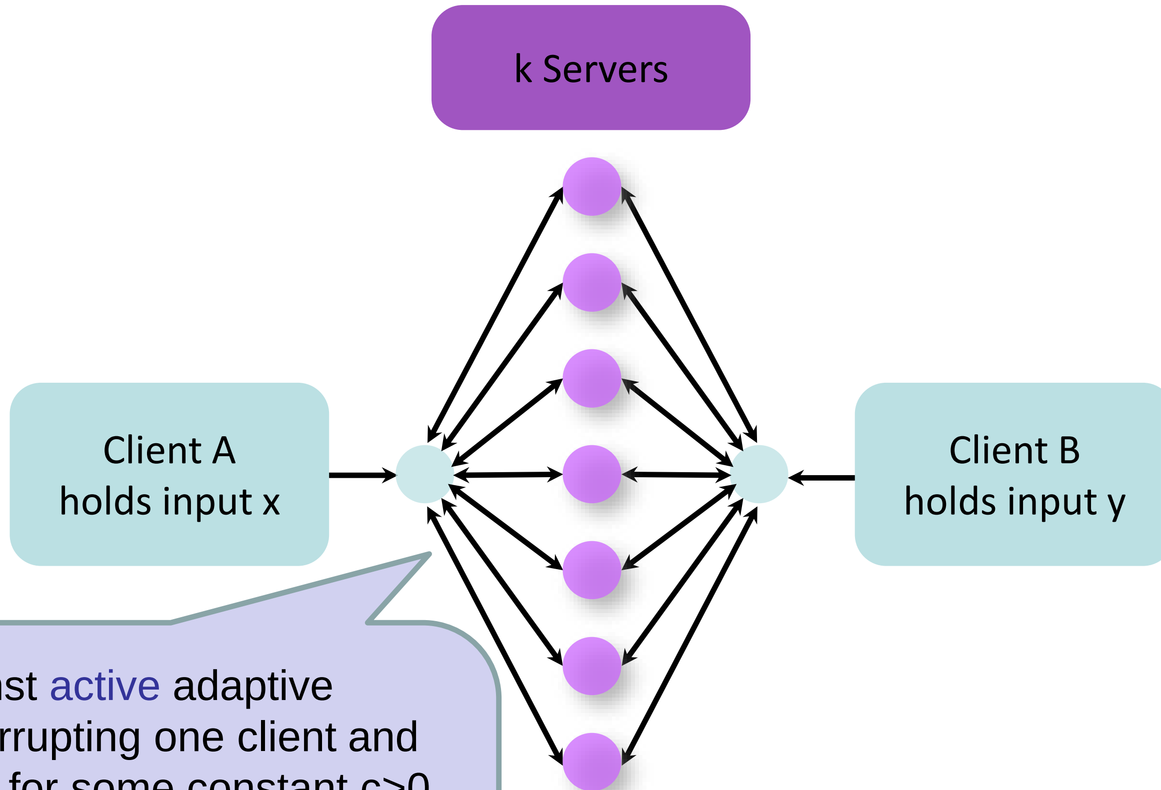
IPS Compiler

[I-Prabhakaran-Sahai08]

- Goal: active-secure 2-party protocol
- Idea: combine two types of “easy” protocols:
  - Outer protocol:
    honest-majority active-secure MPC
  - Inner protocol:
    passive-secure 2-party protocol
    - possibly in OT-hybrid model

- Both are considerably easier than our goal
- Both can have information-theoretic security

Outer protocol



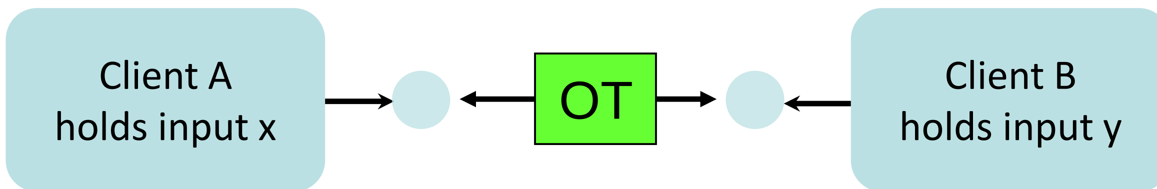
Secure against active adaptive adversary corrupting one client and t=ck servers, for some constant c>0.

Security with abort suffices.

Straight-line simulation.

Example: “BGW-lite”

Inner protocol



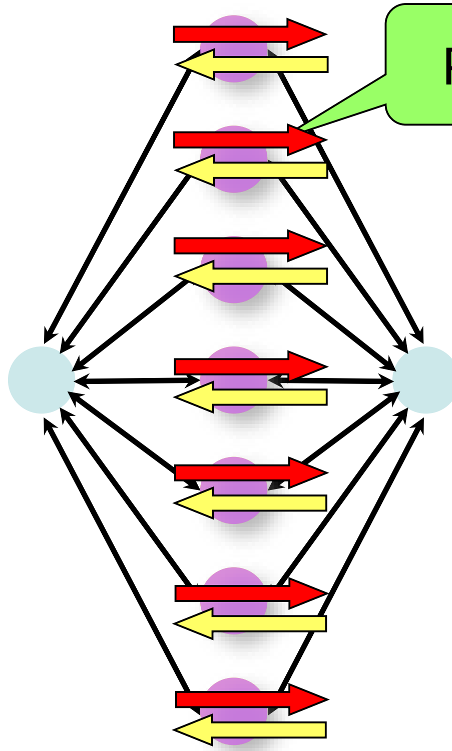
Secure against passive adversary

(Adaptive security w/erasures)

Example: “GMW-lite”

Combining the two protocols

oblivious watch lists



Player virtualization

outer protocol for f

Applications

- Revisiting the classics
  - BGW-lite + GMW-lite ➔ Kilian
- Efficient MPC with no honest majority
  - O(1) bits per gate in OT-hybrid model (+ additive term)
- Constant-round MPC^{OT} (t<n) using black-box PRG
  - Extending 2-party "cut-and-choose" Yao
- Constant-rate b.b. reduction of OT to semi-honest OT
- Secure arithmetic computation over black-box fields/rings/groups
- Practical arithmetic 2PC from black-box passive-OLE: Leviosa [Hazay-I-Marcedone-Venkitasubramaniam19]
  - ~x2 overhead over passive security

    …or even "better than passive" via lattice-based leaky OLE

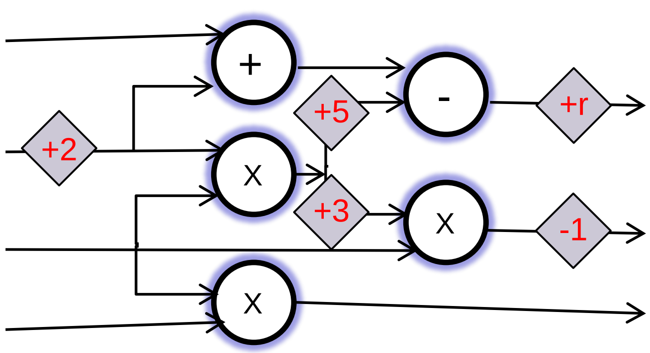
AMD Circuits

[Genkin-I-Prabhakaran-Sahai-Tromer14]

- Motivating observation: In “natural” passive-secure MPC protocols for evaluating an arithmetic circuit C, the effect of an active adversary corresponds to an additive attack on C.
  - Formally: the protocol perfectly realizes an augmented ideal functionality that allows for an additive attack.
  - Applies to all information-theoretic circuit evaluation protocols we know that achieve an optimal level of security (t<n/2 over point-to-point channels, t<n over OT/OLE)
  - Can be generalized to protocols with near-optimal security based on “packed secret sharing” [Genkin-I-Polychroniadou15]
- Active security can be achieved by applying passive-secure protocol to an “AMD circuit” C’ that resists additive attacks.
- Reduces protocol design to fault-tolerant circuit design

AMD Circuit for g

- Syntax: randomized arithmetic circuit
- Correctness: computes g (with probability 1)
- Security: “best possible security” against additive attacks
  - Every additive attack on circuit can be simulated by a (possibly randomized) additive attack on inputs and outputs alone
  - In presence of additive attacks, AMD circuit is “as good” as tamper-proof hardware for g



AMD Circuit Constructions

- Compile any C to an ε-secure C'
  - |C'|=O(|C|)
  - ε = O(1/|F|)

- Extension to block-AMD circuits

Applications

- Simplified feasibility results
  - Passive BGW88 → RB89 ($t<n/2$)
  - Passive GMW87 → Kil88/IPS09 ($t<n$, OLE-hybrid)
- Improved efficiency
  - Passive DN07 → Improved BFO12
    $t<n/2$, $O(n|C|+n^2)$ field elements
  - Passive GMW87 → Improved IPS09
    $t<n$, $O(|C|)$ OLE calls
  - Passive packed DN07 → Improved DIK10
- Practical protocols via lightweight AMD

  [Chida-Genkin-Hamada-Ikarashi-Kikuchi-Lindell-Nof18]