Communication Efficient Perfectly Secure VSS and MPC in Asynchronous Networks with Optimal Resilience

AFRICACRYPT 2010

Arpita Patra (IIT Madras)

Ashish Choudhury (IIT Madras)

Prof. C. Pandu Rangan (IIT Madras)

The Main Contribution

- Perfectly secure Asynchronous Verifiable Secret Sharing
  - Carried out among n parties
  - At most t parties can be actively corrupted by a computationally unbounded adversary
  - Possible iff $n \geq 4t + 1$
- [BH07]: Most communication efficient perfectly secure AVSS with $n = 4t + 1$
  - Generates t-sharing of ℓ secrets
  - $O(\ell n^2 \log |F|)$ bits of private communication
- This paper: A new perfectly secure AVSS with $n = 4t + 1$
  - Generates d-sharing of ℓ secrets, for any $t \leq d \leq 2t$
  - $O(\ell n^2 \log |F|)$ bits of private communication

The Main Contribution Contd …

- Application of our new AVSS:
  - Optimally resilient Perfectly secure Asynchronous Multiparty Computation Protocol with $n = 4t + 1$
  - Communicates $O(n^2 \log |F|)$ bits per multiplication gate

- [BH07]: Most communication efficient perfectly secure AMPC with $n = 4t + 1$
  - Communicates $O(n^3 \log |F|)$ bits per multiplication gate

Verifiable Secret Sharing (VSS) [CGMA85]

- Extends Secret Sharing [Sha79, Bla79] to the case of active corruption
- n parties $P = \{P_1, \ldots, P_n\}$, dealer D (e.g., $D = P_1$)
- t corrupted parties (possibly including D) $\rightarrow \mathcal{A}_t$

- Sharing Phase
  - D initially holds secret **s** and each party P_i finally holds some private information v_i --- share of s
  - $\mathcal{A}_t$ gets no information about s from the private information of corrupted parties

- Reconstruction Phase
  - Reconstruction function is applied to obtain $\mathbf{s} = Rec(v_1, \ldots, v_n)$

Asynchronous Networks

- No global clock in the system
- The communication channels have arbitrary, yet finite delay (i.e the messages will reach eventually)
- A_t schedules all messages in the network
  - ➢ Only schedules the messages of honest parties
- Inherent Difficulty: Cannot distinguish between a slow sender and a corrupted sender
- Cannot wait to receive messages from all the parties
  - ➢ Messages of t potentially honest parties ignored
- Techniques from synchronous world cannot be adapted

AVSS and Its Requirements

- Any AVSS scheme (Sh, Rec) for sharing a secret s satisfies the following

- Termination

  (1) If D is honest, then all honest parties eventually terminate Sh.

  (2) If D is corrupted and some honest party terminates Sh, then all honest parties eventually terminate Sh

  (3) If honest parties terminate Sh and some honest party initiates Rec, then all honest parties eventually terminate Rec

AVSS Requirements Contd …

- Correctness

  (1) If D is honest, all honest parties output s at the end of Rec, irrespective of behavior of corrupted parties

  (2) If D is corrupted and some honest party terminates Sh, then there is a unique s* which is fixed, such that all honest parties output s* at the end of Rec

- Also known as Strong Commitment

AVSS Requirements Contd …

- Secrecy

  If D is honest and no honest party has begun Rec then adversary gets no information about secret s

Types of AVSS

- Perfect AVSS :
  - Satisfies termination, correctness and secrecy property without any error
  - Possible iff $n \geq 4t + 1$

- Statistical AVSS :
  - Satisfies termination and correctness with probability $1 - 2^{-\Omega(k)}$: k is the error parameter
  - Possible iff $n \geq 3t + 1$

- This paper : Perfect AVSS with $n = 4t + 1$

d-Sharing

- A value s is said to be d-shared by a dealer $D \in P$ if:
  - D selects a random degree-d polynomial $f(x)$, where $f(0) = s$
  - D hands over $s_i = f(i)$ to every party $P_i \in P$
  - s_i --- i^{th} share of s
  - $[s_1, s_2, \ldots, s_n]$ --- d-sharing of s, denoted as $[s]_d$

- Typically VSS/AVSS is used to generate t-sharing in synchronous/asynchronous setting
  - One of the main tools used in MPC/AMPC

Existing Perfect AVSS vs Our Perfect AVSS with $n = 4t + 1$

Ref.	Type of Sharing	# of Shared Secrets	Communication Complexity
[BCG93]	t-Sharing	1	$O(n^3 \log\|F\|)$
[BH07]	t-Sharing	ℓ	$O(\ell n^2 \log\|F\|)$
This Article	d-Sharing $t \leq d \leq 2t$	ℓ	$O(\ell n^2 \log\|F\|)$

Advantage of d-sharing Over t-sharing

- In the context of MPC:
  - Evaluation of multiplication gate becomes very simple with the help of 2t-sharing [DN07, BH07]

- In other applications:
  - With t-sharing, only constant coefficient of the sharing polynomial will be information theoretically secure
  - With d-sharing, (d + 1 - t) coefficients of the sharing polynomial will be information theoretically secure
  - Can be useful to implement common coin primitive, which is used for designing Asynchronous Byzantine Agreement Protocols

Tool Used in Our Protocol

Finding (n, t)-Star in a Graph

- Definition: (n, t)-star
  - $G = (V, E)$ is an undirected graph, $V = P = \{P_1, \ldots, P_n\}$
  - (C, D), where $C \subseteq D \subseteq P$ is called (n, t)-star in G if:
    - ❑ $|C| \geq (n - 2t)$, $|D| \geq (n - t)$
    - ❑ For every $P_j \in C$ and $P_k \in D$, the edge $(P_j, P_k) \in E$
- Algorithm for finding (n, t)-star in a graph [BCG93]
  - Outputs either (n, t)-star or the message star not found
  - If G has a clique of size $(n - t)$ then always outputs star

Idea Behind AVSS Protocol of [BCG93, BH07]

Sharing Phase : $n = 4t + 1$

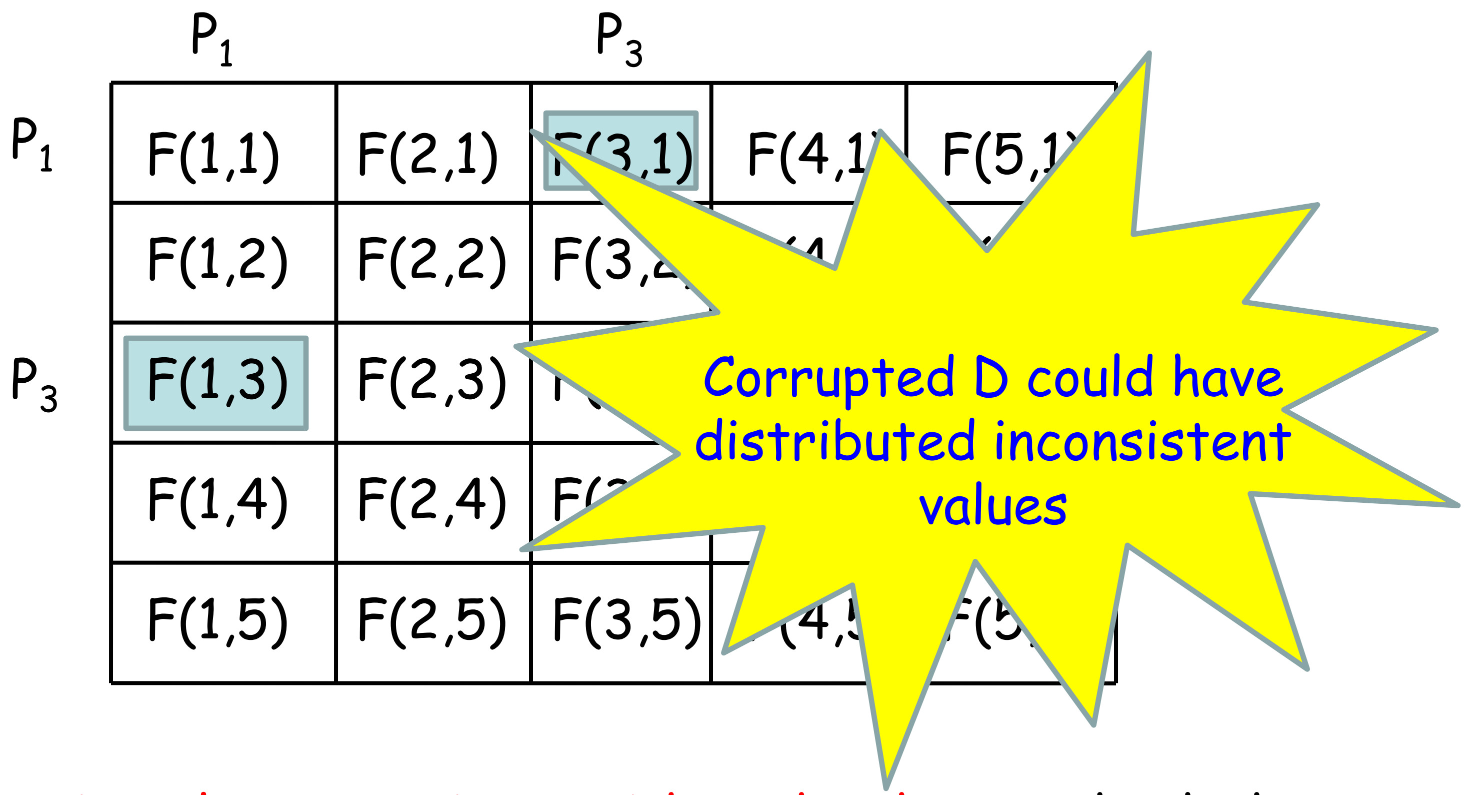
- D selects a random bi-variate polynomial $F(x,y)$ of degree t in both x and y, such that $F(0,0) = s$
- D privately sends $f_i(x) = F(x, i)$ and $g_i(y) = F(i,y)$ to party P_i

F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)	$f_1(x)$
F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)	
F(1,3)	F(2,3)	F(3,3)	F(4,3)	F(5,3)	
F(1,4)	F(2,4)	F(3,4)	F(4,4)	F(5,4)	
F(1,5)	F(2,5)	F(3,5)	F(4,5)	F(5,5)	
$g_1(y)$					

$\searrow$ $n = 5, t = 1$

Idea Behind AVSS Protocol of [BCG93, BH07]

Sharing Phase : $n = 4t + 1$



- Parties privately communicate with each other to check the consistency of the values distributed by D
- Party P_i privately sends to P_j the following:
  - $f_{ij} = f_i(j) = F(j, i)$
  - $g_{ij} = g_i(j) = F(i, j)$

Idea Behind AVSS Protocol of [BCG93, BH07]

Sharing Phase : $n = 4t + 1$

F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)
F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)
F(1,3)	(2,3)	F(3	F(4	F(5,3)
F(1,4)	F(2,4	[illegible]	[illegible]	4)
F(1,5)	F(2	[illegible]	[illegible]	[illegible]

Ideally $f_i(j) = g_j(i)$
And
$g_i(j) = f_j(i)$
Should hold

- Party P_j on receiving f_{ij} and g_{ij} from party P_i, checks:
  - $f_{ij} \overset{?}{=} g_j(i)$
  - $g_{ij} \overset{?}{=} f_j(i)$
- If both the test passes, P_j A-casts OK(P_j, P_i) signal

Idea Behind AVSS Protocol of [BCG93, BH07]

Sharing Phase : n = 4t + 1

F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)
F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)
F(1,3)	F(2,3)	F(3,3)	F(4,3)	F(5,3)
F(1,4)	F(2,4	F(3	F(4,4)	F(5,
F(1,	[illegible]	[illegible]	[illegible]	F(5,

- Party P_j on receiving f_{ij} and g_{ij} from P_i, checks:
  - $\overset{?}{=}$ ... $g_{ij} \overset{?}{=} f_j(i)$
  - ...asses,
  - ...ional

If D has behaved honestly then the set of honest parties will eventually form STAR

All honest parties will eventually agree on same STAR (if it exists)

- Lo... ch party)
  - ➢ Construct graph G = (V, E), where $V = \{P_1, \ldots, P_n\}$ and $(P_i, P_j) \in E$ if P_i has A-cast $OK(P_i, P_j)$ and P_j has A-cast $OK(P_j, P_i)$
  - ➢ Keep applying Find-Star algorithm on G till some STAR (C, D) is obtained

Idea Behind AVSS Protocol of [BCG93, BH07]

Sharing Phase : $n = 4t + 1$

F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)
F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)
F(1,3)	F(2,3)	F(3,3)	F(4,3)	F(5,3)
F(1,4)	F(2,4)	F(3,4)	F(4,4)	F(5,4)
F(1,5)	F(2,5)	F(3,5)	F(4,5)	F(5,5)

- Property of STAR: for each $P_i \in C$ and $P_j \in D$, P_i has A-cast OK(P_i, P_j) and P_j has A-cast OK(P_j, P_i)

- P

D has committed some meaningful bi-variate polynomial and hence secret

- The polynomials (row and column) of the define a unique bi-variate polynomial of deg Why ?
- Honest parties in C and D have checked that th r ro and column polynomial are pair-wise consistent
- $(n - 2t - t) = t + 1$ honest parties in C and $(n - t - t) = 2t + 1$ honest parties in D --- Defines a unique bi-variate of degree t in x and y

Idea Behind AVSS Protocol of [BCG93, BH07]

Sharing Phase : n = 4t + 1

$\mathcal{C} = \{P_1, P_2, P_3\}$

$\rightarrow$ $\mathcal{D} = \{P_1, P_2, P_3, P_4\}$

Consistent with bi-variate defined by honest parties in STAR

t-sharing of s $\longrightarrow$ of + 1 share-share could be corupted

)	F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)
2(0)	F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)
$f_3(0)$	F(1,3)	F(2,3)	F(3,3)	F(4,3)	F(5,3)
~~$f_4(0)$~~	F(1,4)	F(2,4)	F(3,4)	F(4,4)	F(5,4)
~~$f_5(0)$~~	F(1,5)	F(2,5)	F(3,5)	F(4,5)	F(5,5)

- Each $P_j \notin \mathcal{C}$, outputs reconstructs $f_j(0)$ with the honest parties in STAR ($\mathcal{C}$, $\mathcal{D}$)
  - P_j applies ONLINE share-share $g_i(j)$'s received from the P_i's in --t t o t + 1 share-share could be corrupted

ONLINE RS error correction is possible

Unsuccessful Extension of AVSS Protocol of [BCG93, BH07] to Generate d-Sharing, for $d > t$

- To generate d-sharing, Dealer will select bi-variate polynomial $F(x, y)$ of degree d in x and degree t in y
  - ➢ $f_i(x) = F(x, i)$: degree d, $g_i(y) = F(i, y)$: degree t
- If (C, D) is a STAR in the OK graph, then:
  - ➢ $f_i(x)$ polynomials of honest parties in C define $F(x, y)$
  - ➢ $g_i(y)$ polynomials of honest parties in D define $F(x, y)$
- s can be d-shared only by degree d polynomial $F(x, 0) = f_0(x)$
  - ➢ Each honest $P_i \in D$ already possess $g_i(0) = f_0(i)$
  - ➢ If $P_i \notin D$, then parties in C cannot help P_i to get $g_i(0) = f_0(i)$

❑ Only $2t + 1$ parties in C. So OEC will not work, as it requires $3t + 1$ parties to reconstruct t degree $g_i(y)$

Our Approach for Generating d-Sharing, Where $t \leq d \leq 2t$, $n = 4t + 1$

- The sharing phase of our AVSS is divided into sequence of following three phases:
  - Distribution Phas D distributes informatio to parties
  - rificat a agree nt on CO Pha
    - P iste ation
    - se set of 3t + 1 a s ed RE, h pe s
  - Generati n of d sharing Phase:
    - Executed only if CORE is agreed upon in last phase
    - Parties perform computation on data received only from parties in CORE during second phase to complete d-sharing

All three phases will eventually terminate if D i honest

If some honest party terminates all three phases then every other honest party will also eventually do so

Our Approach for Generating d-Sharing, Where $t \leq d \leq 2t$, $n = 4t + 1$

Distribution Phase

- D selects a random bi-variate polynomial $F(x,y)$ of degree d in both x and degree t in y, such that $F(0,0) = s$
- D privately sends $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$ to P_i
  - Row Polynomial: $f_i(x)$ of degree d
  - Column Polynomial: $p_i(y)$ of degree t

Our Approach for Generating d-Sharing, Where $t \leq d \leq 2t$, $n = 4t + 1$

Verification and Agreement on CORE Phase

- The goal of this phase is to check the existence of a set of parties called CORE

- If a CORE exists then every honest party will agree on CORE, where CORE is defined as follows

➢ CORE is a set of at least $3t + 1$ parties such that:

❑ row polynomials of the honest parties in CORE define a unique bivariate polynomial say, $F'(x, y)$ of degree- (d, t)

❑ Moreover, if D is honest then $F'(x, y) = F(x, y)$ where $F(x, y)$ was selected by D

Our Approach for Generating d-Sharing

Generation of d-sharing Through CORE

➢ CORE is a set of at least 3t + 1 parties such that:

❑ row polynomials of the honest parties in CORE define a unique bivariate polynomial say, $F'(x, y)$, of degree- (d, t)

F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)
F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)
F(1,3)	F(2,3)	F(3,3)	F(4,3)	F(5,3)
F(1,4)	F(2,4)	F(3,4)	F(4,4)	F(5,4)
F(1,5)	F(2,5)	F(3,5)	F(4,5)	F(5,5)

$t = 1, n = 5, d = 2$

$\rightarrow$ CORE = $\{P_1, P_2, P_3, P_4\}$

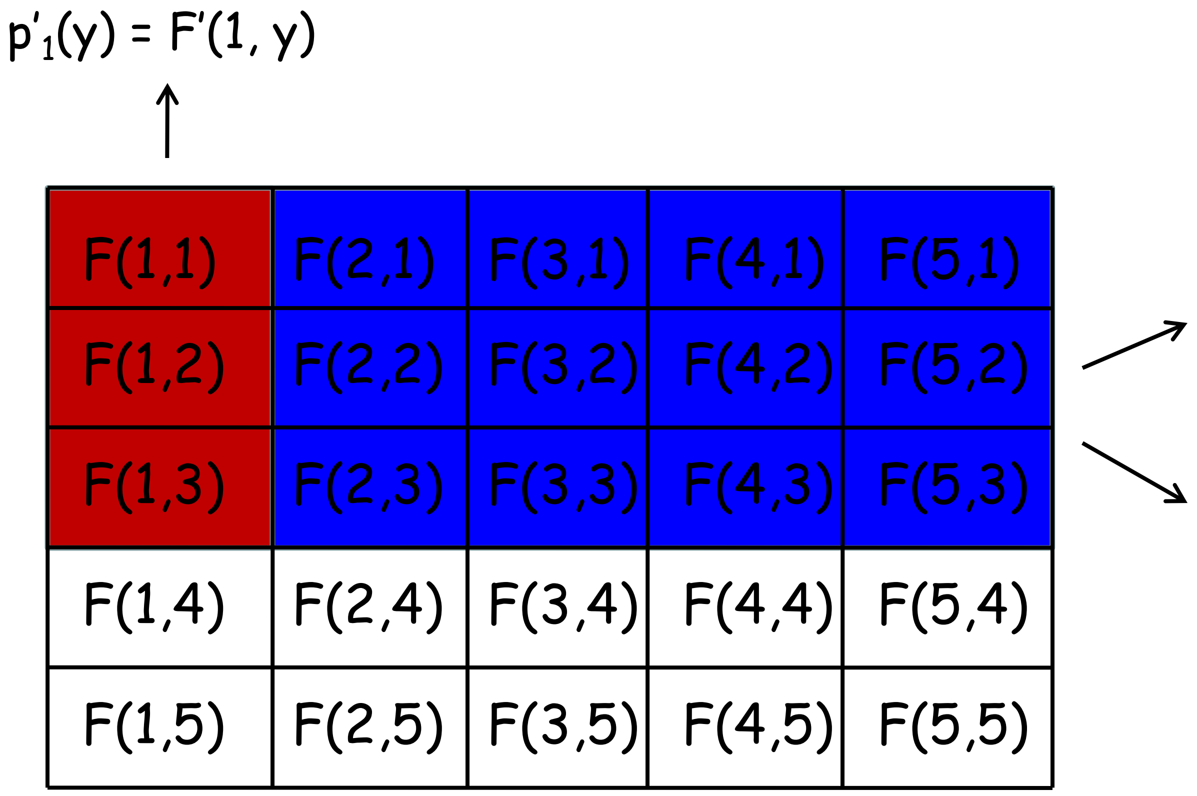
$\rightarrow$ $\{P_1, P_2, P_3\}$: Honest parties in CORE

Their row polynomials define $F'(x, y)$

Our Approach for Generating d-Sharing

Generation of d-sharing Through CORE

- j^{th} point on row polynomials of honest parties in CORE define degree-t column polynomial $p'_j(y) = F'(j, y)$



$p'_1(y) = F'(1, y)$

F(1,1)	F(2,1)	F(3,1)	F(4,1)	F(5,1)
F(1,2)	F(2,2)	F(3,2)	F(4,2)	F(5,2)
F(1,3)	F(2,3)	F(3,3)	F(4,3)	F(5,3)
F(1,4)	F(2,4)	F(3,4)	F(4,4)	F(5,4)
F(1,5)	F(2,5)	F(3,5)	F(4,5)	F(5,5)

$t = 1, n = 5, d = 2$

CORE = $\{P_1, P_2, P_3, P_4\}$

$\{P_1, P_2, P_3\}$: Honest parties in CORE

Their row polynomials define $F'(x, y)$

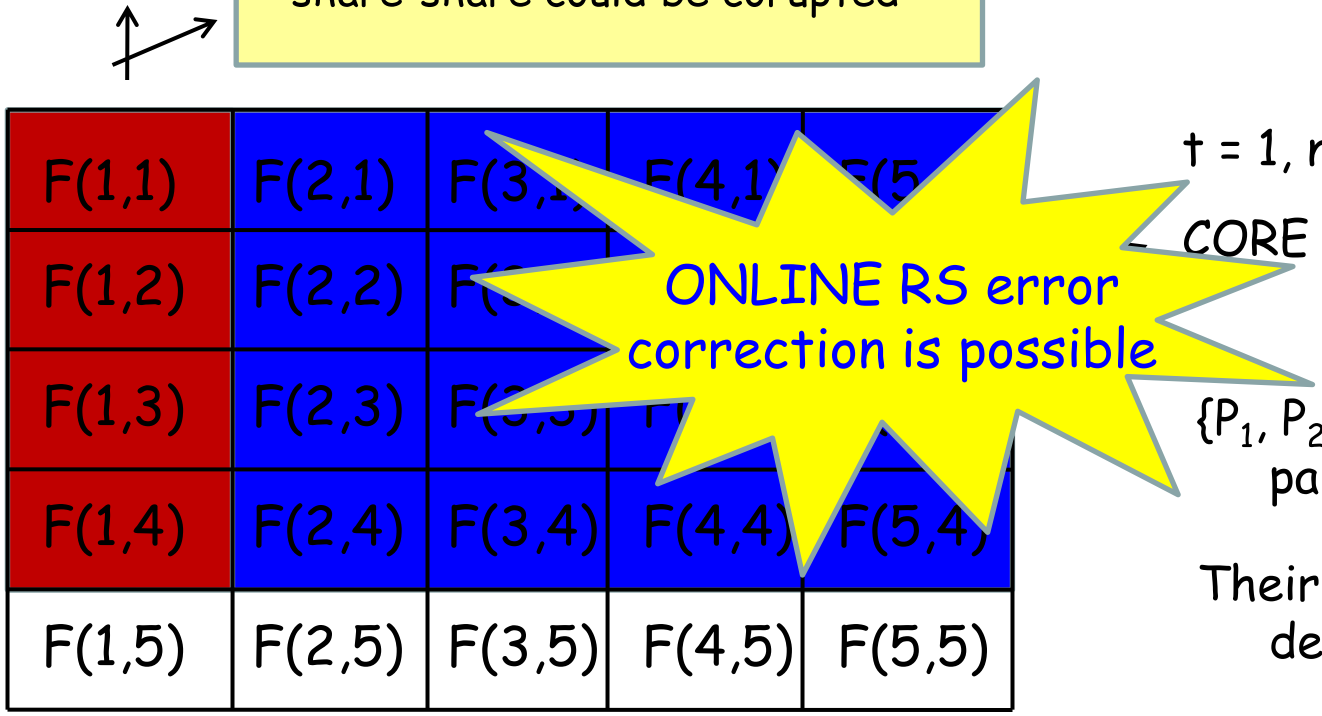
Our Approach for Generating d-Sharing

Generation of d-sharing Through CORE

- As $|CORE| \geq 3t + 1$, each $P_i \in CORE$ can send $f'_i(j) = F'(j, i)$ to P_j
- P_j can apply OEC on $f'_i(j)$'s to reconstruct $p'_j(y)$ and hence $p'_j(0)$

$p'_1(y) = F'(1, y)$

t out of 3t + 1
share-share could be corupted



ONLINE RS error correction is possible

t = 1, n = 5, d = 2

CORE = $\{P_1, P_2, P_3, P_4\}$

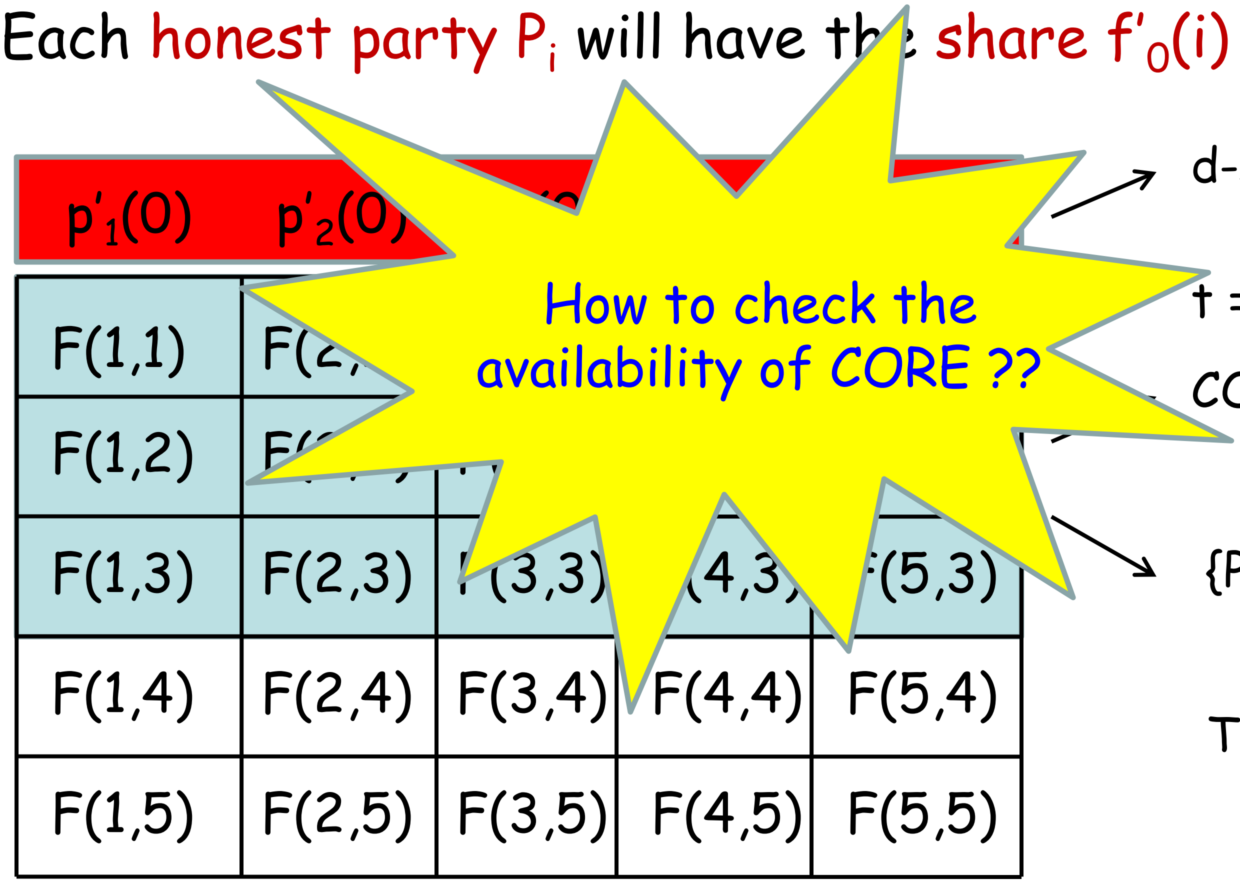
$\{P_1, P_2, P_3\}$: Honest parties in CORE

Their row polynomials define $F'(x, y)$

Our Approach for Generating d-Sharing

Generation of d-sharing Through CORE

- Secret $s' = F'(0, 0)$ will be d-shared using degree-d polynomial $f'_0(x) = F'(x, 0)$
- Each honest party P_i will have the share $f'_0(i) = p'_i(0)$ of s'



d-sharing of s

$t = 1, n = 5, d = 2$

$CORE = \{P_1, P_2, P_3, P_4\}$

$\{P_1, P_2, P_3\}$: Honest parties in CORE

Their row polynomials define $F'(x, y)$

Our Approach for Generating d-Sharing

Outline of Verification and Agreement on CORE Phase

- Parties privately exchange common values on their row and column polynomial and accordingly A-ca st OK signals
- Using the O signals, OK graph is c structured
- Applying FIND-S D alg m , a sequence of distinct STARs are c
- Claim: Each S ivariate polynomial
- We check whethe m any STAR
  - ➢ Using inter cially C component
- Claim: If C componen has + 1 honest parties then CORE can be generate rom STAR
- Claim: If D is honest then ventually C component of some STAR will have 2t + 1 honest parties

Generating a sequence of STARs is required as we do not know which STAR has 2t + 1 honest parties in its C component

Checking Whether CORE Can be Generated from STAR

- Let (C, D) be some STAR
  - ➢ Row polynomials of honest parties in C define F′(x, y) of degree-(d, t)
- Idea: Try to find how many ther row polynomials ie on F′(x, y)
  - ➢ list t all such P whos n polyno l is p se consistent with the polyn ls + 1 st F
    - ❑ Claim: T)
      - ❖ Co h row polynom
  - ➢ li s ent with the colu at + pa s in F – List E
    - ❑ Claim: The row olynom al of each P_j E lie o F′(x, y)
      - ❖ Row polynomial of P_j is of degree-d and is paiwise consistent with column polynomial of at least d + 1 honest parties in F

If |E| ≥ 3t + 1 then E is CORE

This process has to be repeated for every distinct STAR in OK graph

Reconstruction Phase of Our AVSS

- Let s be a secret which is d-shared among n parties using degree-d polynomial $f(x)$, where $t \leq d \leq 2t$ and $n = 4t + 1$

- Party $P_i \in P$ wants to privately reconstruct s

  - Each $P_j \in P$ privately sends s_j, the j^{th} share of s to P_i

  - P_i applies OEC on received shares to reconstruct s

  - [BCG93]: Any secret which is d-shared can be reconstructed using OEC if $t \leq d \leq 2t$ and $n = 4t + 1$

Designing AMPC Using Our AVSS

(t, 2t)-Sharing

- A secret s is said to be (t, 2t)-shared if:
  - s is t-shared as well as 2t-shared

Protocol for Generating (t, 2t)-Sharing

- Dealer D t-shares secret s using degree-t polynomial f(x)
  - Let $[s_1, \ldots, s_n]$ be the corresponding shares
- Dealer (2t – 1)-shares random r using (2t-1)-degree polynomial R(x)
  - Let $[r_1, \ldots, r_n]$ be the corresponding shares
- $g(x) = f(x) + x\,R(x)$ will be 2t-degree polynomial sharing s
  - $s_i + i\,r_i$: corresponding i^{th} share

Overview of Our AMPC Protocol

- Our AMPC follows the approach of [BH07] and is a sequence of following three phases:

1. Preparation Phase:

   - (t, 2t)-sharing of $\ell = c_M + c_R$ random values are generated
   - c_M and c_R are number of multiplication and random gates in the arithmetic circuit
   - Each party (t, 2t)-shares $(c_M + c_R) / (n - 2t)$ secrets
   - Parties execute *ACS* protocol to identify a set of $(n - t)$ parties *C* who have done the sharing
   - Sharing done by at least $(n - 2t)$ parties in *C* is random
   - Parties apply Vandermonde matrix on the sharings done by the parties in *C* to generate $c_M + c_R$ random sharings

Overview of Our AMPC Protocol

- Our AMPC follows the approach of [BH07] and is a sequence of following three phases:

2. Input Phase:

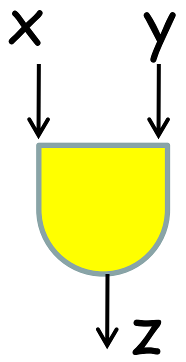
   - Each party t-shares their input using our AVSS
   - Parties execute ACS to agree on a set of $(n - t)$ parties I who have done the sharing
   - Only the inputs of the parties in C will be considered for circuit evaluation

Overview of Our AMPC Protocol

- Our AMPC follows the approach of [BH07] and is a sequence of following three phases:

3. Computation Phase:

- Linear gates evaluated locally due to linearity of t-sharing
- Multiplication : We follow approach of [DN07, BH07]



- Given $[x]_t$ and $[y]_t$, compute $[z]_t$
- Let $[r]_{(t, 2t)}$ be the associated $(t, 2t)$-sharing
- Parties compute $[\Lambda]_{2t} = [x]_t [y]_t + [r]_{2t}$

- parties publicly reconstruct Λ and define default $[\Lambda]_t$

- parties compute $[z]_t = [\Lambda]_t - [r]_t$

Conclusion

- We have designed communication efficient perfect AVSS and perfect AMPC with optimal resilience

- Our protocols outperform the existing protocols in terms of communication complexity

- Our AVSS can generate d-sharing of ℓ secrets concurrently for any d in the range $t \leq d \leq 2t$

   ➢ Explore several interesting features of STAR which were not explored earlier

- Our protocol shares ℓ secrets concurrently

   ➢ Significantly better than ℓ parallel executions of protocol sharing single secret

References

- [BCG93]: M. Ben-Or, R. Canetti, and O. Goldreich. Asynchronous secure computation. In STOC, pp 52–61, 1993.
- [BH07]: Z. Beerliov´a-Trub´ıniov´a and M. Hirt. Simple and efficient perfectly-secure asynchronous MPC. In ASIACRYPT, pages 376–392, 2007.
- [CGMA85]: B. Chor, S. Goldwasser, S. Micali and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In STOC, pp 383–395, 1985.
- [DN07]: I. Damgard and J. B. Nielsen. Scalable and unconditionally secure multiparty computation. In CRYPTO, pages 572–590, 2007.

Thank You
www.jillwlang.com