The Round Complexity of Verifiable Secret Sharing Re-Visited

CRYPTO 2009

Arpita Patra (IIT Madras)

Ashish Choudhary (IIT Madras)

Tal Rabin (IBM Research)

C. Pandu Rangan (IIT Madras)

Verifiable Secret Sharing (VSS)

- Fundamental building block in secure distributed computing
- Two phase (sharing and reconstruction) protocol
  - ➢ Carried out among n parties of which at most t parties could be actively corrupted
  - ➢ Sharing phase : a secret s is shared among n parties
  - ➢ Reconstruction phase : s is uniquely reconstructed

Round Complexity of VSS

- Studied in [GIKR01]
  - Assumed that protocols are error-free (perfect)
  - Lower bound : perfect VSS with 3 rounds of sharing
    is possible iff $n \geq 3t + 1$
    (1 round of reconstruction)
- Our Result:
  - Existing lower bound can be circumvented by allowing a negligible error probability
  - Statistical VSS with 2 rounds of sharing is possible iff $n \geq 3t + 1$
    (2 rounds of reconstruction)
    - 1 round of reconstruction if A_t is non-rushing

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) → A_t

- Sharing Phase
  - D initially holds secret **s** and each party P_i finally holds some private information v_i --- share of s
  - A_t gets no information about s from the private information of corrupted parties
- Reconstruction Phase
  - Reconstruction function is applied to obtain

    $\mathbf{s} = Rec(v_1, \ldots, v_n)$

VSS Requirements

- Secrecy
  - If D is honest, then A_t has no information about secret **s** during the Sharing phase
- Correctness
  - If D is honest, then secret **s** will be correctly reconstructed during reconstruction phase
- Strong Commitment
  - If D is corrupted, then at the end of sharing phase, there exists a unique s*, such that s* will be reconstructed in reconstruction phase, irrespective of the behavior of corrupted parties

Types of VSS

- Perfect
  - Without any error

- Statistical
  - Negligible error probability of $\in = 2^{-\Omega(k)}$ in Correctness and Strong Commitment
  - No compromise in Secrecy

Communication Model and Definitions

- Synchronous, fully connected network of pair-wise secure channels + broadcast channel
- Rushing and adaptive active adversary A_t
- All computation and communication done over a finite field $F = GF(2^k)$, where k is security parameter
- Without loss of generality, k = poly(n)
- **Round complexity:** Number of communication rounds in the Sharing phase [GIKR01, FGGPS06, KKK08]
- **Efficiency:** Total computation and communication is polynomial in n, k and size of the secret.

Our Results vs [GIKR01, FGGPS06]

Summary of existing results for perfect VSS

# Rounds	Characterization	Efficient?	Optimal Rounds?	Optimal Fault Tolerance?
1	t = 1; n ≥ 5 No protocol for t > 1	Yes	Yes	Yes
2	n ≥ 4t + 1 , t ≥1	Yes	Yes	Yes
3	**n ≥ 3t + 1 , t ≥1**	**Yes**	**Yes**	**Yes**

Summary of our results for statistical VSS

# Rounds	Characterization	Efficient?	Optimal Rounds?	Optimal Fault Tolerance?
1	t = 1; n ≥ 4 No protocol for t > 1	Yes	Yes	Yes
2	**n ≥ 3t + 1 , t ≥ 1**	**Yes**	**Yes**	**Yes**

- Conclusion: the existing lower bounds can be circumvented by allowing negligible error probability

Overview of Our 2 Round $(3t + 1, t)$ Statistical VSS

- We follow the structure of the VSS protocols of [RB89, FGGPS06, KKK08]
  - ➢ We first design a 2 round $(3t + 1, t)$ statistical WSS
  - ➢ Our 2 round $(3t + 1, t)$ statistical WSS is used as a black-box to design our 2 round $(3t + 1, t)$ statistical VSS
- Novelty of our protocol : specific design of the WSS component and the way we use it for VSS

Weak Secret Sharing (WSS) [RB89]

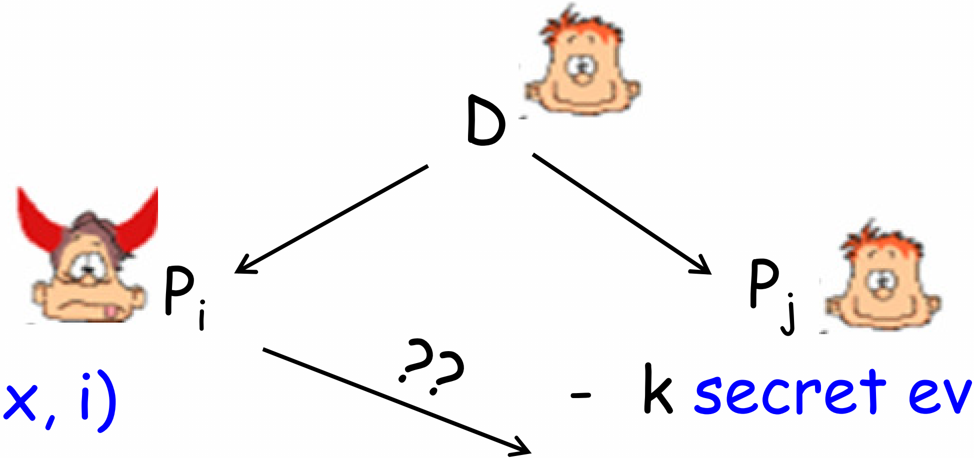
- Used as a black-box in our VSS
- Secrecy and Correctness : same as in VSS
- Instead of Strong Commitment, satisfies Weak Commitment

- Weak Commitment
  - If D is corrupted, then at the end of sharing phase, there exists a unique s*, such that during reconstruction phase either s* or NULL will be reconstructed

- Perfect WSS : no error
- Statistical WSS : negligible error of $2^{-\Omega(k)}$ in correctness and weak commitment

Idea of Our 2 Round $(3t + 1, t)$ Statistical WSS

- D selects $F(x, y)$, $\text{degree}(x) = nk + 1$, $\text{degree}(y) = t$, $F(0, 0) = s$
  - ➢ Note the asymmetry in $\text{degree}(x)$ and $\text{degree}(y)$



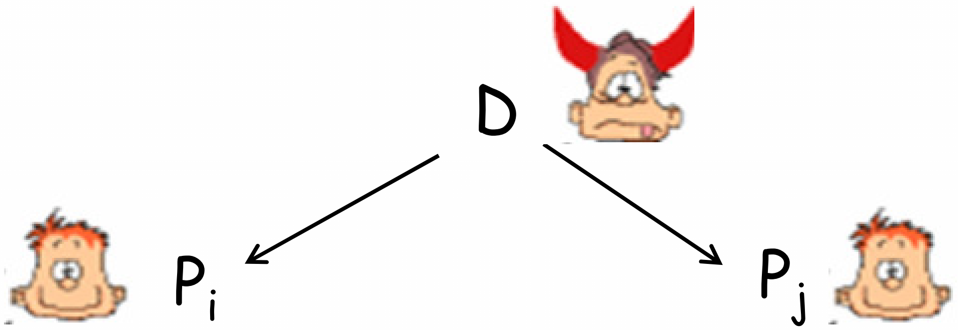
- $f_i(x) = F(x, i)$
- $\text{degree}(x) = nk + 1$

- k secret evaluation points
- $f_i(x)$ evaluated at these points

- Corrupted P_i revealing $f'_i(x) \neq f_i(x)$ will be caught by honest P_j with high probability

- $f'_i(x) \neq f_i(x)$ will match at one of the evaluation points of P_j with probability $(nk + 1) / |F| \approx 2^{-\Omega(k)}$

Idea of Our 2 Round (3t + 1, t) Statistical WSS Contd…



- $f_i(x)$

- $f'_i(x) \neq f_i(x)$ evaluated

k points

- P_i and P_j interact i d-choose to check the consist

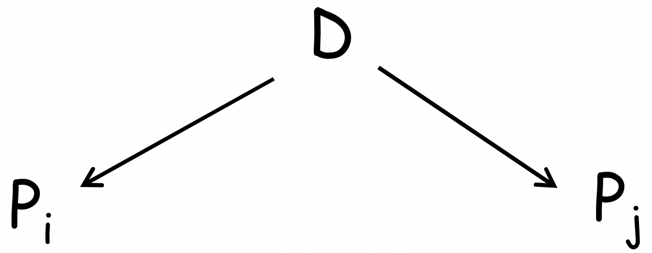
- Challenges in cut-and-cho

Only two rounds of sharing is allowed

- ➢ Should take only ONE round
- ➢ Adversary should not get additional information about s if D is honest

Idea of 2 Round Statistical WSS Contd.

- **D's distribution before Cut-and-choose:**



D

P_i
- $f_i(x)$ and $r_i(x)$
- degree(x) = nk + 1
- $r_i(x)$: blinding polynomial

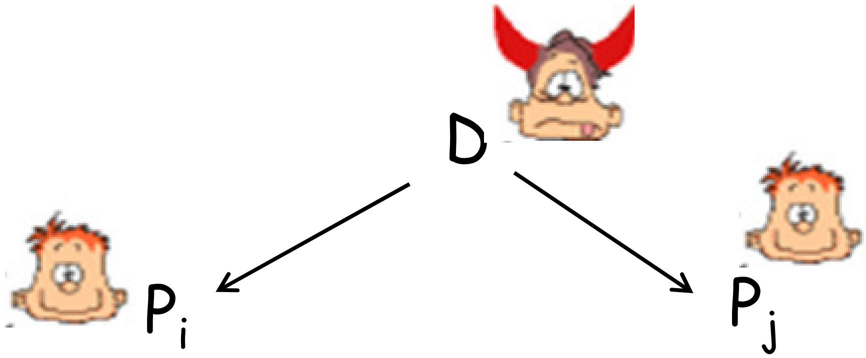
P_j
- k secret evaluation points
- $f_i(x)$ and $r_i(x)$ evaluated at these points

- **Cut-and-choose:**

- **P_i BROADCASTS:**
  - random $c_i \neq 0$
  - $g_i(x) = f_i(x) + c_i\, r_i(x)$

- **P_j BROADCASTS:**
  - random k/2 evaluation points out of k
  - evaluation of $f_i(x)$ and $r_i(x)$ at these k/2 points

Idea of Our 2 Round (3t + 1, t) Statistical WSS Contd…



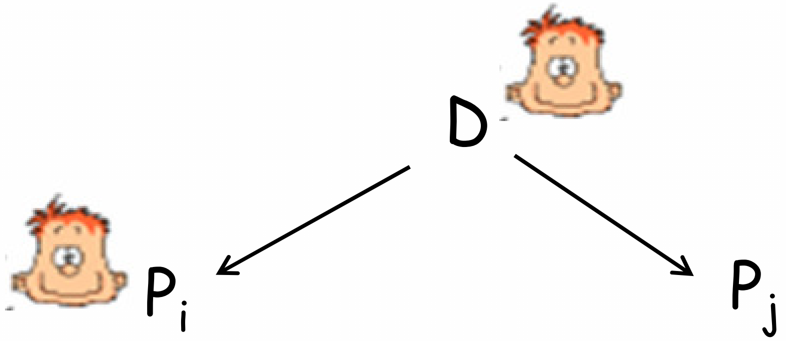
- **P_i Broadcasts:**
  - random $c_i \neq 0$
  - $g_i(x) = f_i(x) + c_i\, r_i(x)$

- **P_j Broadcasts:**
  - random k/2 evaluation points out of k
  - evaluation of $f_i(x)$ and $r_i(x)$ at these k/2 points

- If the k/2 values exposed by P_j satisfies $g_i(x)$, then except with probability $1/\ C(k, k/2) \approx 2^{-\Omega(k)}$, at least one of the remaining k/2 values of $f_i(x)$ possessed by P_j indeed lie on $f_i(x)$

➢ P_j randomly selects k/2 evaluations points for exposing

Idea of Our 2 Round (3t + 1, t) Statistical WSS Contd…



- **P_i Broadcasts:**
  - random $c_i \neq 0$
  - $g_i(x) = f_i(x) + c_i\, r_i(x)$

- **P_j Broadcasts:**
  - random k/2 evaluation points out of k
  - evaluation of $f_i(x)$ and $r_i(x)$ at these k/2 points

- Adversary will have no information about $f_i(0) = F(0, i)$

  - degree($f_i(x)$) = $nk + 1 = (3t + 1)k + 1$
  - Total number of points on $f_i(x)$ known by adversary is $[\ kt + (2t + 1)\ k/2\ ] < (nk + 1)$

Statistical VSS, 2 Round Sharing, 2 Round Reconstruction, n = 3t + 1

Overall Idea

- **Almost follows the same idea as [FGGPS06, KKK08]**
  - D selects a symmetric bivariate polynomial F(x, y) of degree t in x, y with F(0, 0) = s and sends $f_i(y) = F(i, y)$ to P_i
  - P_i executes sharing phase of 2 Round WSS to share a random degree-t polynomial $g_i(y)$ --- WSS^{P_i}
  - Parties perform pair-wise consistency checking of their common values on F(x, y) using $g_i(y)$ polynomials for masking
  - Though there is no third round to resolve conflict as in [FGGPS06, KKK08], our VSS achieve all the properties of statistic VSS.

Statistical VSS with Only 1 Round of Broadcast

- We can modify the VSS protocol so that it uses broadcast channel in ONLY ONE ROUND throughout the protocol
  - Minimum number of rounds in which broadcast channel is used --- [KKK08]
  - Idea: To modify the underlying WSS such that it does only private communication during reconstruction phase

Statistical VSS --- 1 Round of Reconstruction

- If the adversary is non-rushing, then two rounds of reconstruction can be merged into single round
  - If the adversary is non-rushing, then the reconstruction of underlying WSS can be done in one round.
  - The reconstruction phase of the VSS is simply the execution of reconstruction phase of underlying WSS

Our Other Results
(To Appear in Full Version of Paper)

- 3-Round efficient statistical WSS with n = 2t + 1
- 3-Round efficient statistical VSS with n = 3 and t = 1
- 4-Round in-efficient statistical VSS with n = 2t + 1
- 5-Round efficient statistical VSS with n = 2t + 1
- The current best statistical VSS with n = 2t + 1 is due to [CDD+99], which takes more than 5 rounds

Open Problems

- [GIKR01, FGGPS06, KKK08] --- perfect VSS with 3 Rounds of sharing and n = 3t + 1

Total = 4 rounds

- This Paper --- sharing
  and 2 round of reconstruction with n = 3t + 1

- Open Problem I: what is the total round complexity
  (sharing + reconstruction) of VSS with
  n = 3t + 1

- This Paper --- error probability only in correctness and
  strong commitment

- Open Problem II: What is the effect on the round complexity of VSS considering error probability in secrecy as well

Thank You

References

[Shamir79]: A. Shamir. How to share a secret. *Communications of the ACM, 22(11):612-613, 1979.*

[CGMA85]: B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In Proc. of STOC 1985, pages 383–395, 1985.

[RB89]: T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In STOC, pages 73–85, 1989.

[GIKR01]: Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. The round complexity of verifiable secret sharing and secure multicast. In STOC, pages 580–589, 2001.

[FGGPS06]: M. Fitzi, J. Garay, S. Gollakota, C. Pandu Rangan, and K. Srinathan. Round-optimal and efficient verifiable secret sharing. In Proc. of TCC 2006, pages 329–342, 2006.

References

[KKK08]: J. Katz, C. Koo, and R. Kumaresan. Improving the round complexity of vss in point-to-point networks. Cryptology ePrint Archive, Report 2007/358. Also in Proc. of ICALP 2008.

Another View of Computation in 2 Round WSS

- We can view the computation done by D during sharing phase as follows:
  - D shares a degree-t polynomial g(y) using WSS
  - For this, D selects a random bi-variate F(x,y) as in WSS protocol, such that F(0, y) = g(y)
  - The polynomial g(y) is the degree-t polynomial used by D to share s = g(0) = F(0, 0)
  - The polynomial g(y) is not completely random, but preserves the secrecy of only its constant term

Statistical VSS, 2 Round Sharing, n = 3t + 1

Sharing Phase, 2 Rounds

- **Round 1:**
  - D selects a symmetric bivariate polynomial F(x, y) of degree t in x, y with F(0, 0) = s and sends $f_i(y) = F(i, y)$ to P_i
  - P_i executes Round 1 of sharing phase of 2 Round WSS to share a random degree-t polynomial $g_i(y)$ --- WSS^{P_i}
- **Round 2:**
  - Party P_i broadcasts

    - $h_i(y) = f_i(y) + g_i(y)$ - $a_{ji} = f_j(i) + g_j(i) = f_i(j) + g_j(i)$
  - The parties execute Round 2 of sharing phase of each WSS^{P_i}. Let $WSS\text{-}SH_i$ denote the SH created in WSS^{P_i}.

Statistical VSS, 2 Round Sharing, n = 3t + 1

Sharing Phase, 2 Rounds

- **Local Computation (by Each Party) :**
  - P_i accepted by P_j if $h_i(j) = a_{ij}$
  - Accept
  - VSS-S
  - For $P_i \in$ $_i| \le$
    2t then r
  - If final |VSS-SH| ≤ 2t then discard D

- Protocol is similar to the 3 round perfect VSS of [FGGPR06, KKK08]
- Instead of doing verification point-wise, we do verification on polynomials
- No third round to resolve conflicts

Statistical VSS, 2 Round Sharing, n = 3t + 1

Properties of VSS-SH for Honest D

- **Recall --- Local Computation (by Each Party) :**
  - P_i is said to be accepted by P_j if $h_i(j) = a_{ij}$
  - Accept_i = set of all parties that accepted party P_i
  - VSS-SH $\leftarrow P_i$ if $|\text{Accept}_i| \geq 2t + 1$
  - For $P_i \in$ VSS-SH, if $|\text{VSS-SH} \cap \text{WSS-SH}_i \cap \text{Accept}_i| \leq 2t$ then remove P_i from VSS-SH
  - If final $|\text{VSS-SH}| \leq 2t$ then discard D

- All honest parties will be present in VSS-SH and so an honest D will not be discarded during sharing phase

- If a corrupted $P_i \in$ VSS-SH then $h_i(y) - g_i(y) = f_i(y) = F(i, y)$
  - There are at least (t + 1) honest parties in $(\text{WSS-SH}_i \cap \text{Accept}_i)$ who uniquely define $g_i(y)$ and $f_i(y)$

Statistical VSS, 2 Round Sharing, n = 3t + 1

Properties of VSS-SH for Corrupted D

- **Recall --- Local Computation (by Each Party) :**
  - P_i is said to be accepted by P_j if $h_i(j) = a_{ij}$
  - Accept_i = set of all parties that accepted party P_i
  - VSS-SH $\leftarrow P_i$ if $|\text{Accept}_i| \geq 2t + 1$
  - For $P_i \in$ VSS-SH, if $|\text{VSS-SH} \cap \text{WSS-SH}_i \cap \text{Accept}_i| \leq 2t$ then remove P_i from VSS-SH
  - If final $|\text{VSS-SH}| \leq 2t$ then discard D

- If honest parties in VSS-SH are not pair-wise consistent, then committed secret $s^* = \text{NULL}$
- If honest parties in VSS-SH are pair-wise consistent and defines $F^H(x, y)$, then committed secret is $s^* = F^H(0, 0)$
  - If corrupted $P_i \in$ VSS-SH then $h_i(y) - g_i(y) = F^H(i, y)$ as there are $(t + 1)$ honest parties in $(\text{WSS-SH}_i \cap \text{Accept}_i)$

Statistical VSS, 2 Round Sharing, n = 3t + 1

Reconstruction Phase, 2 Rounds

- **Round 1 and Round 2 :**
  - For each $P_i \in$ VSS-SH, run reconstruction phase of WSS^{P_i}
- **Local Computation (By Each Party) :**
  - Initialize VS
  - VSS-REC = V

- $h_i(y)$ publicly known during sharing phase
- $g_i(y)$ publicly reconstructed in WSS^{P_i}

  - For $P_i \in$ VSS-REC, define its share as $f_i(0) = h_i(0) - g_i(0)$
  - If shares of the parties in VSS-REC interpolate a degree-t polynomial f(x), then output s = f(0). Else output NULL

Statistical VSS, 2 Round Sharing, $n = 3t + 1$

Properties of VSS-REC

- An honest $P_i \in$ VSS-SH will be present in VSS-REC with high probability
  - $WSS^{P_i} \neq$ NULL with very high probability
- From the properties of VSS-SH and VSS-REC, the protocol satisfies $(1 - \in)$-correctness and $(1 - \in)$-strong commitment

Statistical VSS, 2 Round Sharing, n = 3t + 1

Perfect Secrecy of the Protocol

- If P_i is honest then $h_i(y) = f_i(y) + g_i(y)$ does not reveal any information about $f_i(0)$

  - Both $f_i(y)$ ar

  - WSS^{P_i} does not reveal any information about $g_i(0)$

Follows from the secrecy property of 2 Round WSS

- Secrecy now follows from the properties of bivariate polynomial of degree-t in x and y

Statistical VSS --- 1 Round of Reconstruction

- If the adversary is non-rushing, then two rounds of reconstruction can be collapsed into single round
  - The reconstruction phase of the VSS is simply the execution of reconstruction phase of underlying WSS
  - If the adversary is non-rushing, then the reconstruction of underlying WSS and hence overall VSS can be done in one round

Statistical VSS with Only 1 Round of Broadcast

- We can modify the VSS protocol so that it uses broadcast channel in ONLY ONE ROUND throughout the protocol

Minimum number of rounds in which broadcast is used [KKK08]

  - Ide lying WSS with the one which for reconstruction phase
  - I the end of WSS^{P_i}, all honest output SAME $g_i(y)$
  - If a corrupted $P_i \in$ VSS-SH, then at the end of WSS^{P_i}, each honest party will locally output either $g_i(y)$ or NULL, but nothing other than $g_i(y)$
- The resultant protocol will satisfy the properties of statistical VSS

Outline of the Talk

- Definition of VSS and WSS
- Existing Results and Outline of Our Results
- 2 Round (3t+1, t) Statistical WSS
- 2 Round (3t+1, t) Statistical VSS
- Open Problems

Verifiable Secret Sharing (VSS) [CGMA85]

- Extends secret sharing to the case of *active* corruptions
- A_t may actively corrupt at most t parties (possibly including the dealer D)
- Corrupted parties, incl. D may behave arbitrarily during the protocol

Statistical WSS and VSS

- Statistical WSS
  - Satisfies Correctness and Weak Commitment with probability $(1 - \in)$
  - $\in = 2^{-\Omega(k)}$ and k = security parameter
  - No compromise in Secrecy

- Statistical VSS
  - Satisfies Correctness and Strong Commitment with probability $(1 - \in)$
  - $\in = 2^{-\Omega(k)}$ and k = security parameter
  - No compromise in Secrecy

Existing results on Perfect VSS

- Perfect VSS (without any error) is (efficiently) achievable iff n > 3t [BGW88, DDWY90]

- Optimal fault tolerance --- (n = 3t + 1)
- Optimal number of sharing rounds --- 3
- Optimal number of rounds in which broadcast channel is used --- 1

al Fault
rance?

es

es

es

es

- Reconstruction phase of perfect VSS requires ONLY one round

- 3 Rou]

- [KKK0 ing
broadca

Our Results

- Statistical VSS possible iff n > 2t and broadcast channel is available [RB89] ---- nothing known about round complexity

- We the study of round complexity of statistical VSS

# Rounds	Characterization	Efficient?	Optimal	Optimal Fault Tolerance?
1				es
2				es

- Reconstruction phase of perfect VSS requires ONLY one round

- Our protocol requires TWO rounds of reconstruction

- If A_t is nor tion can be done in SINGLE rour

- Same as in [KKK08]

- Our protocols use broadcast channel in ONLY ONE round

Statistical WSS --- 1 Round of Reconstruction

- If the adversary is non-rushing, then two rounds of reconstruction can be coll

- Ensures CORRECTNESS property

  - ➢ Two rounds are required to force the rushing adversary to commit the $f_i(x)$ polynomials of corrupted parties before seeing the evaluation points of honest parties

  - ➢ If the adversary is non-rushing, then the task of both the rounds can be merged into a single round

Statistical WSS with 1 Round of Broadcast

- We can modify the protocol so that it uses broadcast channel in ONLY ONE ROUND throughout the protocol
  - Ide te communication
    nstruction phase
  - The correctness
    and perfec
  - The resultant p eak
    commitment but wi
  - Some honest party(ies) may output committed secret s* while some may output NULL

Minimum number of rounds
in which broadcast is used
[KKK08]

Privately

A corrupted P_i may reveal
different $f_i(x)$'s to each
honest party

Idea of Our 2 Round (3t + 1, t) Statistical WSS

- D selects F(x, y), degree(x) = nk + 1, degree(y) = t, F(0, 0) = s

➢ S

- D – ng

ught

- D – igh

- Con

$f_i($

➢ P_i and P_j in o knowledge using cut and choose

to check consis cy of $f_i(x)$ and evaluation of $f_i(x)$

All this is done in only 2 rounds of sharing

- Nowhere we need to reconstruct $f_i(x)$ polynomials.

Proof of the Properties of 2 Round WSS

- **CORRECTNESS: (D is hone**
  - All honest parties (at least 2t H - -- An honest D is not discarded
  - All honest parties will also be present in REC
  - If D is honest then with very high probability no corrupted party will be present in REC
    - ➢ A corrupted P_i broadcasts $f'_i(x) \neq f_i(x)$ in Round 1 of reconstruction phase --- no information about evaluation points of honest parties
    - ➢ Honest parties reveal their secret evaluation points and values ONLY in Round 2 of reconstruction phase
    - ➢ With high probability no honest party will re-accept P_i

- If D is honest then all honest parties will accept as well as re-accept each other

Proof of the Properties of 2 Round WSS

- **SECRECY: (D is honest)**
  - Let $P_1, \ldots, P_t$ be under the control of A_t
  - During Round 1 of sharing phase, A_t learns the following:
    - Polynomials $f_1(x), \ldots., f_t(x)$ and $r_1(x), \ldots., r_t(x)$
    - Kt points on $f_{t+1}(x), \ldots., f_n(x)$ and $r_{t+1}(x), \ldots., r_n(x)$
  - During Round 2 of sharing phase, A_t learns the following:
    - $\frac{k}{2}(2t+1)$ more points on $f_{t+1}(x$ $f (x)$ and r (x) $r (x)$
  - In total, A_t will learn $kt + \frac{k}{2}$ (2 x) and $r_{t+1}(x), \ldots., r_n(x)$
  - Degree of $f_{t+1}(x), \ldots., f_n(x)$ is $(nk + 1) > kt + \frac{k}{2}(2t+1)$
  - So $s = f_0(0)$ will be secure

- A_t cannot interpolate back $F(x, y)$

Proof of the Properties of 2 Round WSS

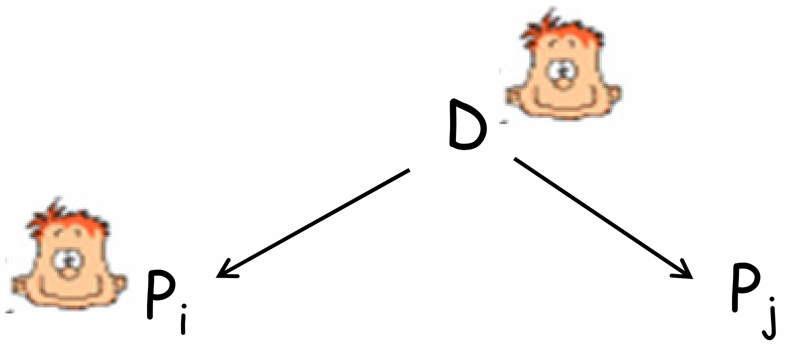
- WEAK COMMITMENT: (D is Corrupted and |SH| ≥ 2t+1)
  - Committed s* is constant term of the degree-t polynomial interpolated by the shares of HONEST parties in SH
  - s* = NULL if the shares of HONEST parties in SH does not interpolate a degree-t polynomial

- With very high probability, all HONEST parties in SH will be also present in REC

- In order that an HONEST P_i was present in SH but not present in REC, the foll
  - At lease one HONEST P_j a but did not re-accepted P_i
  - 2t+1 parties accepted P_i during sharing phase, but only t parties re-accepted P_i during reconstruction phase

- From the properties of cut-and-choose, this can happen with negligible probability

Idea of Our 2 Round (3t + 1, t) Statistical WSS Contd…



- **P_i Broadcasts:**
  - random $c_i \neq 0$
  - $g_i(x) = f_i(x) + c_i\, r_i(x)$

- **P_j Broadcasts:**
  - random k/2 evaluation points out of k
  - evaluation of $f_i(x)$ and $r_i(x)$ at these k/2 points

- Adversary will have no information about $f_i(0) = F(0, i)$
  - degree($f_i(x)$) = $nk + 1 = (3t + 1)k + 1$
  - Total number of points on $f_i(x)$ known by adversary is $kt + (2t + 1)\, k/2$

Statistical WSS, 2 Round Sharing, n = 3t + 1

Sharing Phase : 2 Rounds

- **Round 1:**

- D selects the following:

➢ F(x, y) --- degree of x = nk + 1, degree of y = t, F(0, 0) = s

➢ $r_1(x)$, …, $r_n(x)$ --- degree nk + 1, independent of F(x, y)

➢ nk random, distinct, non-zero secret evaluation points denoted as $\alpha_{i,1}, \ldots, \alpha_{i,k} : 1 \leq i \leq n$

- D sends to par

➢ $f_i(x) = F(x, i)$

➢ $a_{j,i,l} = f_j(\alpha_{i,l})$

k

➢ $f_i(0)$ --- i^{th} share of s

- If D is honest, then $f_i(0)$'s of honest parties lie on degree-t polynomial g(y) = F(0,y).
- In the reconstruction phase, s will be obtained by reconstructing g(y).

Statistical WSS, 2 Round Sharing, n = 3t + 1

Sharing Phase

- Round 2:
  - Party P_i broadcasts the following:
    - A random, non-zero value c_i
    - Polynomial $g_i(x) = f_i(x) + c_i\ r_i(x)$
    - A random subset of k/2 secret evaluation points $\alpha_{i, l_1}, \ldots, \alpha_{i, l_{k/2}}$ and the values $a_{j, i, l_1}, \ldots, a_{j, i, l_{k/2}}$ and $b_{j, i, l_1}, \ldots, b_{j, i, l_{k/2}}$

- Parties interact in zero knowledge fashion using cut-and-choose to find the consistency of $f_i(x)$ and evaluations of $f_i(x)$

- Local Computation by Each Party:
  - P_j accepts P_i if $g_i(\alpha_{j, l}) = a_{i, j, l} + c_i\ b_{i, j, l}$ for all l in the set of k / 2 secret points broadcasted by P_j in Round 2
  - SH $\leftarrow P_i$ if P_i is accepted by at least 2t + 1 parties
  - If |SH| ≤ 2t then discard D

Statistical WSS, 2 Round Sharing, $n = 3t + 1$

Reconstruction Phase, 2 Rounds

- **Round 1:**
  - Each $P_i \in SH$ broadcasts $f_i(x)$
- **Round 2:**
  - P_j broadcasts $\alpha_{j,l}$'s which were not broadcasted during sharing phase and $a_{i,j,l}$'s corresponding to these indices
- **Local Computation by Each Party:**
  - P_j re-accepts P_i if $f_i(\alpha_{j,l}) = a_{i,j,l}$ for any of the newly revealed secret evaluation points
  - $REC \leftarrow P_i$ if P_i is re-accepted by at least $t + 1$ parties
  - If the shares of the parties in REC interpolate a degree-t polynomial $g(y)$ then output $s = g(0)$. Else output NULL