lec 08

# Verifiable secret sharing (VSS)



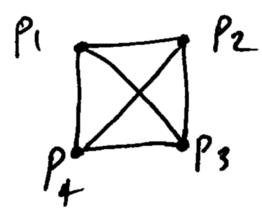
* players must be able to verify all computations
* a dishonest dealer must be detected during the sharing phase of the protocol
* corrupted players (compromised) should not be able to disrupt the protocol

---

(a) first unconditionally secure VSS → $t < n/3$

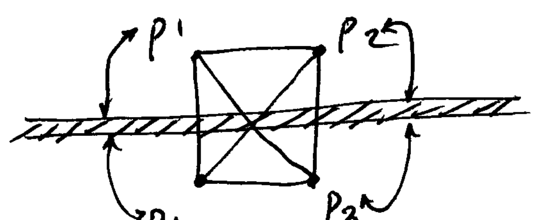
zero prob of error

private channels




(b) VSS where $t < n/2$ → private channels

broadcast channels




simpler (c) VSS where $t < n/4$ → private channels

broadcast channels

$\boxed{\text{sharing phase}}$ $|\nabla| \leq t-1 \leq \lfloor \frac{n-1}{4} \rfloor$ assumption

① The dealer "D" selects a symmetric bivariat polynomial $f(x,y) \in \mathbb{Z}_q[x,y]$ where $f(0,0) = \alpha$ secret

$$f(x,y) = \sum_{i=0}^{t-1} \sum_{j=0}^{t-1} a_{ij} x^i y^j \qquad a_{00} = \alpha \ , \ a_{ij} = a_{ji}$$

the dealer sends $f_i(x) = f(x, w^i)$ to $P_i$ for $1 \leq i \leq n$

"$w$ is a primitive root"

② $P_i$ and $P_j$ peform pairwise checks. That is, they verify that $\underbrace{f_i(w^j)}_{\text{share of } P_i} = \underbrace{f_j(w^i)}_{\text{share of } P_j}$. If $P_i$ finds that $f_i(w^j) \neq f_j(w^i)$ he broadcast the ordered pair $(i,j)$ to accuse $P_j$.

③ Each $P_i$, $1 \leq i \leq n$, computes a subset $T \subseteq \underbrace{\{1, \dots n\}}_{\text{identities}}$ such that any ordered pair $(i,j) \in T \times T$ is not broadcasted. If $|T| \geq n - \underbrace{(t-1)}_{\#\text{ of corrupted shares}}$, $P_i$ outputs $Ver_i = 1$, otherwise, $Ver_i = \phi$.

④ The secret sharing is accepted if at least $n - \underbrace{(t-1)}_{\#\text{ of corrupted shares}}$ players output $Ver_i = 1$, otherwise, the dealer is disqualified.

$\boxed{\text{Example:}}$ $n=9$, $q=13$, $b=2$, $w=2$

$t=3 \longrightarrow$ degree $=2$

① $f(x) = \underbrace{11}_{\alpha} + 3x + 3y + 4x^2 + 4y^2 + xy^2 + x^2y + 7xy + 9x^2y^2$

$P_1 \longrightarrow f_1(x) = f(x, 2^1) = 3x^2 + 8x + 7$

$P_2 \longrightarrow f_2(x) = f(x, 2^2) = 9x^2 + 8x + 9$

$P_3 \longrightarrow f_3(x) = f(x, 2^3) = 3x^2 + 6x + 5$

$P_4 \longrightarrow f_4(x) = f(x, 2^4) = 10x^2 + 7x + \underbrace{4}_{\text{true part of the shares}}$

$\vdots$

shares / shadows

② 2nd, 3rd

$f_3(x) = f_3(2^2) = 12$

$f_2(x) = f_2(2^3) = 12$

$$\begin{array}{c|cccc} & P_1 & P_2 & P_3 & P_4 \\ \hline P_1 & 0 & 9 & 3 & 6 \\ P_2 & 9 & 0 & 12 & 10 \\ P_3 & 3 & 12 & 0 & 11 \\ P_4 & 6 & 10 & 11 & 0 \end{array}$$

symmetric matrix

③ $Ver_1 = \emptyset$ or $1$

$Ver_2 = \emptyset$ or $1$

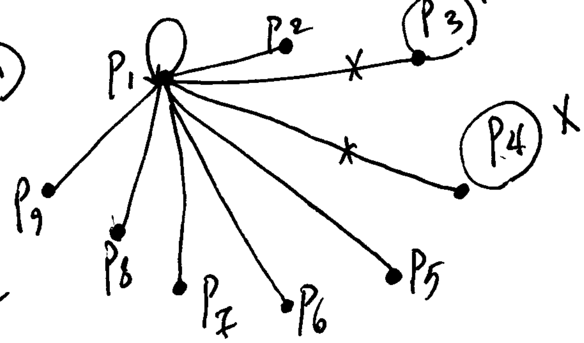
$Ver_3 = \emptyset$ or $1$

$Ver_4 = \emptyset$ or $1$

$\vdots \quad \vdots$

$\boxed{n-(t-1) = 7}$

(4.1)




$Ver_1 = 1$

$\vdots$

$P_3 \quad Ver_3 = \emptyset$

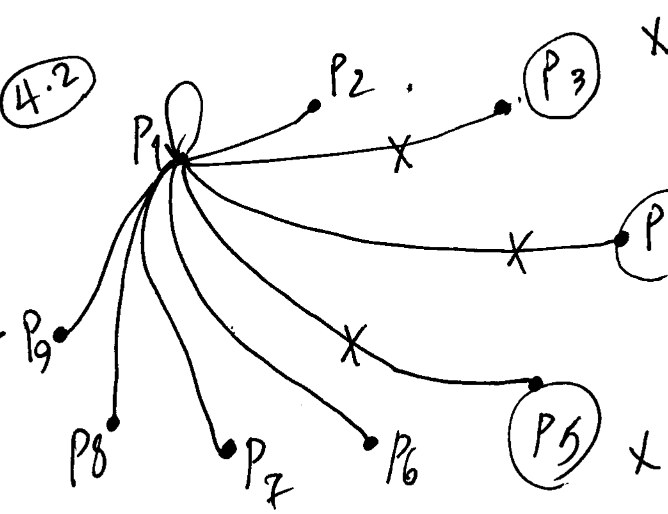
$P_4 \quad Ver_4 = \emptyset$

$\vdots$

④ $7 = Ver_i$ is equal to 1

dealer is qualified

(4.2)




$Ver_1 = \emptyset$

$\vdots$

$Ver_3 = 0$

$Ver_4 = 0$

$Ver_5 = 0$

$\vdots$

dealer is disqualified

## Recovery phase

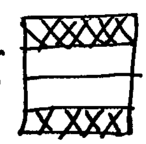
① Each player $\underbrace{P_i \text{ where } i \in T}_{\text{non-crropted players}}$ sends his share (or the constant term of his share) to a selected player $P_j$.

② player $P_j$ computes a polynomial $f_j(y)$ such that $f_j(w^i) = f_i(0)$ for at least $n-2(t-1)$ values of "$i$". He then computes the secret

$$f_j(0) = f(0,0)$$

→ $(t-1)$ corrupted shares might be excluded during the sharing phase
$(t-1)$ corrupted shares may exist during the recovery phase

during sharing ←
$\frac{1}{3}$ can be corrupted
during the recovery phase & error correction can be used to recover the secret correctly



**Example:** $P_1, P_2, P_3$

$$C_1 = \frac{0-2^2}{2^1-2^2} * \frac{0-2^3}{2^1-2^3} \pmod{13} \qquad C_2 = \frac{0-2^1}{2^2-2^1} * \frac{0-2^3}{2^2-2^3} \pmod{13}$$

$$C_3 = \frac{0-2^1}{2^3-2^1} * \frac{0-2^2}{2^3-2^2} \pmod{13}$$

$$\text{poly} = (3x^2+8x+7) * C_1 + (9x^2+8x+9) * C_2 + (3x^2+6x+5) * C_3 \pmod{13}$$

$$= \underbrace{11}_{\text{secret}} + ax + bx^2$$

## properties of this VSS scheme.

① If a good player (non-corrupted) $P_i$ outputs $Ver_i = \emptyset$ at the end of the sharing phase, every good player (non-corrupted) outputs $Ver_i = \emptyset$. If this occurs, then more than $(t-1)$ shares have been corrupted by bad players and a dishonest dealer. In this case, the protocol fails.

② If the dealer is honest, $Ver_i = 1$ for every good $P_i$ at the end of the sharing phase. In this situation, at most $(t-1)$ shares might be later corrupted by bad players.

③ If at least $n-(t-1)$ players $P_i$ output $Ver_i = 1$, then $\acute{\alpha} \in \mathbb{Z}_q$ will be reconstructed in the recovery phase (i.e., at most $t-1$ players have received incorrect shares from the dealer) and $\acute{\alpha} = \alpha$ if dealer is honest

seclecting correct secret

④ If $|Z| = q$, $\alpha$ is chosen randomly from $\mathbb{Z}_q$, and the dealer is honest, then any coalition of at most $(t-1)$ players cannot use Lagrange Int to recover the secret. They cannot also guess the value "$\alpha$" (secret) with a probability greater than $\frac{1}{q}$ at the end of the sharing phase.