[I486S]
暗号プロトコル理論

藤崎 英一郎

北陸先端科学技術大学院大学

2020 年 6 月 16 日

本日の講義の内容

1. 能動的攻撃者 (active adversary) 対策に向けて

2. 検証可能秘密分散 (VSS)

能動的攻撃者 (active adversary) 対策に向けて

Shamir の秘密分散法を使って能動的攻撃者に安全な MPC 計算を行う時、明らかに次のような問題を解決しなければいけない。

- 正直な Dealer （参加者の 1 人）により参加者に分配されたシェアを復元するとき、不正な参加者は嘘のシェアを皆の前に提示するかも知れない。Lagrange 多項式補間法では、全てのシェアーが正しいことを前提に復元される（解決策：先々週（線形符号））。
- Dealer が不正者の場合、t 次多項式 $f(X)$ 上にないシェアを参加者に配るかも知れない（解決策：今週（検証可能秘密分散））。

本日の講義の内容

1. 能動的攻撃者 (active adversary) 対策に向けて
2. 検証可能秘密分散 (VSS)

検証可能秘密分散 (VSS)

Ben-Or/Goldwasser/Wigderson [BGW88] の $(t+1, n)$-検証可能秘密分散 (Verifiable Secret Sharing) 方式 $(n \geq 3t+1)$

目的: Dealer D に秘密分散

$$[s] = (s_1, \ldots, s_n) = (f(\alpha_1), \ldots, f(\alpha_n))$$

を正しく実行させたい。

- Dealer D
- Players $P_1, \ldots, P_n$
- Perfect Privacy: Dealer が正直な場合、Dealer の秘密情報 $s \in K$ は、t 人以下の攻撃者 $\mathcal{A}_{t,n}$ に対して一切情報を与えない。
- Perfect Reconstruction: VSS 方式が参加者間で受理 (accept) された場合、正直な参加者 $P_{h_1}, \ldots, P_{h_{n-t}}$ は、t 次のある多項式 f の点 $(f(\alpha_{h_1}), \ldots, f(\alpha_{h_{n-t}}))$ をそれぞれもつ。
  $\Longrightarrow$ すなわち、正直な $t+1$ 人以上の参加者のみで、または n 人の中に不正者が t 人以下混じっていて、それを正直な参加者が認識できていなくても秘密 $f(0)$ を正しく復元できる。

BGW VSS

Dealer は、次のような二変数対称多項式を（ランダムに）選ぶ。

Bivariable Symmetric Polynomial

$$F(X,Y) = \sum_{i,j=0}^{t} r_{i,j} X^i Y^j \text{ where } r_{00} = s,$$

such that $\deg_X(F) = \deg_Y(F) = t$ and, for all i, j, $r_{i,j} = r_{j,i}$.

Notes:

- $F(\alpha_i, \alpha_j) = F(\alpha_j, \alpha_i)$ for all i, j.
- $f(X) \triangleq F(X, 0)$: real sharing polynomial.
- $s = F(0,0)$: real secret.
- $s_i = f(\alpha_i) = F(\alpha_i, 0) = F(0, \alpha_i)$: P_i's real share on $f(X)$.
- $f_i(X) \triangleq F(X, \alpha_i)$: P_i's verification polynomial.

BGW VSS (Distribution Phase) I

プロトコル実行中、D への accuse が $t+1$ 以上となった時点でプロトコルは拒絶され強制終了するものとする。

1. D は、$s = F(0,0)$ とし、検証多項式 $f_i(X) = F(X, \alpha_i)$ を P_i $(i = 1, \ldots, n)$ にそれぞれ（秘匿通信で）送る。
2. 各 P_i は、$\deg(f_i) \neq t$ の場合、(accuse, i, D) を broadcast*し、Step 9 でプロトコルが受理されるまで復活しない。

   *: broadcast channel を仮定していないが、Byzantine algorithm で broadcast を実現する（$n > 3t$ より可能).
3. $\deg(f_i) = t$ を確認できた P_i は $s_i = f_i(0)$ を s の自らのシェアと設定する。各 P_i は、$s_{ij} = f_i(\alpha_j)$ を（秘匿通信で）P_j $(j \in \{1, \ldots, n\} \backslash \{i\})$ に送る。

   D が不正をしていなければ $s_i = f_i(0) = F(0, \alpha_i) = F(\alpha_i, 0) = f(\alpha_i)$.
4. 各 P_i は、P_j $(j \in \{1, \ldots, n\} \backslash \{i\})$ から送られてきた s_{ji} に対して、$s_{ij} = s_{ji}$ であるかチェックする。各 P_i は、送られてきた s_{ji} に対して、$s_{ij} \neq s_{ji}$ となるものを発見した時、P_i は、$(\text{dispute}, i, j)$ を broadcast する。

   D, P_i, P_j が全て正直なら、$s_{ij} = f_i(\alpha_j) = F(\alpha_j, \alpha_i) = F(\alpha_i, \alpha_j) = f_j(\alpha_i) = s_{ji}$.
5. D は、各 $(\text{dispute}, i, j)$ に対して、$\hat{s}_{ij}$ を broadcast する。

   D が正直であれば、$\hat{s_{ij}} = F(\alpha_i, \alpha_j)$ である。

BGW VSS (Distribution Phase) II

6. (dispute, i, j) に対して broadcast された $\hat{s}_{ij}$ を、P_i と P_j はそれぞれ $\hat{s}_{ij} = s_{ij}$ と $\hat{s}_{ij} = s_{ji}$ であるかチェックする。もし、自分のものと一致しないとわかったら、その参加者（P_i とする）は、(accuse, i, D) を broadcast し、Step 9 でプロトコルが受理されるまで復活しない。
7. D は、これまでの全ての (accuse, i, D) に対して、$\hat{f}_i(X)$ を broadcast する。
   D が正直であれば、$\hat{f}_i(X) = f_i(X)$ である。
8. $\hat{f}_i(X)$ が broadcast されたとき、これまで accuse していない P_j は、$\deg(\hat{f}_i) = t$ と
$$s_{ji} = f_j(\alpha_i) = \hat{f}_i(\alpha_j)$$
   が成立するかチェックし、成立しなければ (accuse, j, D) を broadcast する。
9. これまでの accuse 数が合わせて t 以下の場合は、プロトコルは受理 (accept) され、これまでに accuse をした P_i も、$\hat{f}_i(X)$ を新たな自分の検証多項式とみなし $f_i(X) \triangleq \hat{f}_i(X)$ とおき、$s_i = f_i(0)$ を自分のシェアとする。

BGW VSS (Reconstruction Phase)

Reconstruction

正直な $n - t(\geq 2t + 1)$ 人の参加者は、Reed-Solomon 符号の復号により、$f(X)$ を復元することができ、$s = f(0)$ を復元できる。

- Step 6 で合計 accuse 数が $t + 1$ 以上になりプロトコルが強制終了されなければ、D が正直であろうとなかろうと、少なくとも $t + 1$ 人以上の正直な参加者間で t 次多項式 $f(X)$ が補間（秘密分散）される。
- プロトコルが受理された時、D が正直であろうとなかろうと、正直な全ての参加者間で t 次多項式 $f(X)$ が補間（秘密分散）される。

Perfect Reconstruction

Theorem

BGW VSS 方式が受理されたとき、全ての正直な参加者 $P_i \in H$ は、ある（同じ）t 次多項式 $f(X)$ の各点 $f(\alpha_i)$ をシェアとしてもつ。よって、$\#H = n - t \geq 2t + 1$ より *Reconstruction* で秘密 $f(0)$ が常に正しく復元できる。

定理 1 の証明（D が正直な場合）

D が正直であれば、正直な参加者 P_i は dispute をすることはあっても、accuse をすることはない。不正な参加者の数は t であるから、プロトコルは常に受理され、各 P_i は、$f_i(X)$ を保持し、D は正直なため
$f_i(0) = F(0, \alpha_i) = F(\alpha_i, 0) = f(\alpha_i)$ が成り立つ。 □

定理 1 の証明（D が不正者の場合）

D を不正者とし、C を Step 2 と Step 6 で accuse しない正直な参加者の集合とする。Step 6 で、プロトコルが終了しないとしたら、その時点で accuse した参加者の数は高々 t. よって、$\#C \geq n - \#\{\text{不正者}\} - \#\text{accuse} \geq n - t - t = n - 2t \geq t + 1$.

$$g(X) = \sum_{i \in C} \lambda_{i,C} f_i(X)$$

とおく。任意の $P_j \in H$ に対して、

$$\begin{aligned} g(\alpha_j) &= \sum_{i \in C} \lambda_{i,C} f_i(\alpha_j) \\ &= \sum_{i \in C} \lambda_{i,C} f_j(\alpha_i) \quad (\text{At Step 9: } f_i(\alpha_j) = f_j(\alpha_i) \text{ for all } i \in C, j \in H.) \\ &= f_j(0) \quad (deg(f_j) = t, \#C \geq t + 1 \Longrightarrow f_j(0).) \\ &= s_j. \end{aligned}$$

C に属する参加者は全員正直なので、$deg(f_i) = t$ より $deg(g) = t$. よって、正直な参加者 P_j は共通の t 次多項式 $g(X)$ の各点 $g(\alpha_j)$ を保持する。

定理 1 の別証明（D が不正者の場合）

まず次の lemma を考える。

Lemma

$f_1(X), \ldots, f_p(X) \in K[X]$ を p 個の体 K を係数とする t 次多項式。
$\alpha_1, \ldots, \alpha_p \in K$ は互いに異なる値とする。$p \geq t+1$ で、全ての
$i, j \in \{1, \ldots, p\}$ に対して、$f_i(\alpha_j) = f_j(\alpha_i)$ が成立するとすると、ある
$\deg_X(F) = \deg_Y(F) = t$ である二変数対称多項式 $F(X, Y)$ が存在して、

$$f_i(X) = F(X, \alpha_i) \quad \textit{for } i \in \{1, \ldots, p\}$$

となる。

$p = t + 1$ の場合

列ベクトル $\boldsymbol{x}$, $\boldsymbol{\mu_i}$ を $\boldsymbol{x} = (1, x, \ldots, x^t)^T$, $\boldsymbol{\mu_i} = (1, \alpha_i, \ldots, \alpha_i^t)^T$ と定義する。$f_i(X)$ の係数を要素とする列ベクトルを $\boldsymbol{f_i}$ とすると、$f_i(X) = \boldsymbol{x}^T \boldsymbol{f_i}$ と表せる。$\boldsymbol{\mu_1}, \ldots, \boldsymbol{\mu_{t+1}}$ が $t+1$ 次元ベクトル空間の独立なベクトルであり、$M \triangleq (\boldsymbol{\mu_1}, \ldots, \boldsymbol{\mu_{t+1}})$ は $(t+1) \times (t+1)$ の Van de monde 行列だから正則。よって、$(t+1) \times (t+1)$ 行列 $R = (\boldsymbol{f_1}, \ldots, \boldsymbol{f_{t+1}})M^{-1}$ とすると $(\boldsymbol{f_1}, \ldots, \boldsymbol{f_{t+1}}) = RM$. よって $\boldsymbol{f_i} = R\boldsymbol{\mu_i}$. すなわち

$$f_i(X) = \boldsymbol{x}^T R \boldsymbol{\mu_i} \qquad \text{where } i = 1, \ldots, t+1 \tag{1}$$

$f_i(\alpha_j) = f_j(\alpha_i)$ と、$f_j(\alpha_i) = f_j(\alpha_i)^T = (\boldsymbol{\mu_i}^T R \boldsymbol{\mu_j})^T = \boldsymbol{\mu_j}^T R^T \boldsymbol{\mu_i}$ より、

$$\boldsymbol{\mu_j}^T R \boldsymbol{\mu_i} = \boldsymbol{\mu_j}^T R^T \boldsymbol{\mu_i}. \tag{2}$$

これが、全ての $i, j \in \{1, \ldots, t+1\}$ に対して成り立つから、$M^T R M = M^T R^T M$. M は正則だから、$R = R^T$. これより、二変数対称多項式 $F(X, Y) = \boldsymbol{x}^T R \boldsymbol{y}$（ただし、$\boldsymbol{y} = (1, Y, \ldots, Y^t)^T$）が存在して $f_i(X) = F(X, \alpha_i) (= \boldsymbol{x}^T R \boldsymbol{\mu_i})$ となる。 □

$p > t+1$ の時

$Q = \{1, \ldots, t+1\}$ とする。$i \in Q$ に対しては、$p = t+1$ の場合から二変数対称多項式 $F(X, Y) = \boldsymbol{x}^T R \boldsymbol{y}$ $(R = R^T)$ が存在して $f_i(X) = \boldsymbol{x}^T R \boldsymbol{\mu_i}$ となる。ここで、

$$f_i(\alpha_j) = \boldsymbol{\mu_j}^T R \boldsymbol{\mu_i} = (\boldsymbol{\mu_j}^T R \boldsymbol{\mu_i})^T = \boldsymbol{\mu_i}^T R \boldsymbol{\mu_j}.$$

$j \notin Q$ の場合、$f_j(X) = \boldsymbol{x}^T \boldsymbol{f_j}$ とおく。

$$f_j(\alpha_i) = f_i(\alpha_j) \qquad \text{for all } i \in Q. \tag{3}$$

から、

$$\boldsymbol{\mu_i}^T \boldsymbol{f_j} = \boldsymbol{\mu_i}^T R \boldsymbol{\mu_j} \qquad \text{for all } i \in Q. \tag{4}$$

$M = (\boldsymbol{\mu_1}, \ldots, \boldsymbol{\mu_{t+1}})$ として、(4) から $M^T \boldsymbol{f_j} = M^T R \boldsymbol{\mu_j}$. M は正則なので、$\boldsymbol{f_j} = R \boldsymbol{\mu_j}$.
よって、$f_j(X) = \boldsymbol{x}^T R \boldsymbol{\mu_j}$ $(j \notin Q)$. □

D が不正者の場合の証明

- C: Step 2 と Step 6 で accuse しない正直な参加者の集合
- $\bar{C}$: Step 2 または Step 6 で accuse した正直な参加者の集合。すなわち、$H = C \sqcup \bar{C}$.

Step 6 で、プロトコルが終了しないとしたら、その時点で accuse した参加者の数は高々 t. よって、

$$\#C \geq n - \#\{\text{不正者}\} - \#\text{accuse} \geq n - t - t = n - 2t \geq t + 1.$$

Lemma 2 より、$i, j \in C$ に対して、$f_i(\alpha_j) = f_j(\alpha_i)$ から、全ての $i \in C$ に対して、$f_i(X) = \boldsymbol{x}^T R \boldsymbol{\mu_i}$ となる。$j \in \bar{C}$ は、$\hat{f}_i(X)$ を D から受け取るが、プロトコルが最終的に受理するならば、

$$\hat{f}_j(\alpha_i) = f_i(\alpha_j) \qquad \text{for all } i \in Q(\subset C).$$

Q は、C の任意の $\#Q = t + 1$ となる部分集合。すると $p > t + 1$ の場合と同様で、$\hat{f}_j(X) = \boldsymbol{x}^T R \boldsymbol{\mu_j}$ $(j \in \bar{C})$. これより、プロトコルが受理されるなら正直な参加者全員に対して、

$$f_i(X) = \boldsymbol{x}^T R \boldsymbol{\mu_i} = F(X, \alpha_i) \qquad \text{for all } i \in H.$$

よって、$f_i(0) = F(0, \alpha_i) = F(\alpha_i, 0) = f(\alpha_i)$. □

Perfect Privacy

Theorem

D が正直な場合、*Distribution Phase* を実行することで、不正者が得られる情報は $\{f_j(X) := F(X, \alpha_j) \,|\, P_j \in \mathcal{A}_{t,n}\}$ であり、そこから導き出される以上の情報は一切えられない。特に D の秘密情報 s は一切漏れない。

不正者はプロトコルから

$$\{f_j(X) = F(X, \alpha_j) \,|\, P_j \in \mathcal{A}_{t,n}\} \tag{5}$$

の t 個の t 次多項式の情報を得る。さらにプロトコルから正直な参加者の多項式 $f_i(X)$ の点 $f_i(\alpha_j)$ $(P_i \in H,, P_j \in \mathcal{A}_{t,n})$ の情報は得られるが、$f_j(\alpha_i) = f_i(\alpha_j)$ であるからすでに (5) で不正者が得ている情報である。以上が D が正直な場合不正者が得られる情報の全てであるが、このとき $s = F(0, 0)$ の情報がどの程度漏れるか考える。

Theorem 3 の証明 I

$\hat{F}(X,Y)$ を $\deg_X(\hat{F}) = \deg_Y(\hat{F}) = t$ なる対称多項式で、

$$\hat{F}(X,\alpha_j) = F(X,\alpha_j) \qquad \text{for all } P_j \in \mathcal{A}_{t,n} \tag{6}$$

を満たすとする。$\mathcal{A}_{t,n}$ からみると、$\hat{F}(X,\alpha_j) = F(X,\alpha_j)$ より、D が、$F(X,Y)$ を選んだのか、$\hat{F}(X,Y)$ を選んだのか全く区別がつかないはずである。以下、$F(0,0)$ と、$\hat{F}(0,0)$ は独立であることを示す。

$$g(X,Y) := \hat{F}(X,Y) - F(X,Y) \tag{7}$$

と定義する。全ての $P_j \in \mathcal{A}_{t,n}$ に対して、$g(X,\alpha_j) = 0$ より、$\left(\prod_{j\in\mathcal{A}_{t,n}}(Y-\alpha_j)\right) | g(X,Y)$ が成り立つ。また $g(X,Y)$ が対称多項式であることを考えると、$\left(\prod_{j\in\mathcal{A}_{t,n}}(X-\alpha_j)\right) | g(X,Y)$ も成り立つ。$g(X,Y)$ の次数を考えると、$g(X) := \prod_{j\in\mathcal{A}_{t,n}}\left(\frac{X-\alpha_j}{-\alpha_j}\right)$ とすれば、

$$g(X,Y) = \beta \cdot g(X)g(Y)$$

と表せる。ここでスカラー $\beta \in K$ は、どのような値であっても式 (6) を満たすため、$\hat{F}(0,0) = s + \beta$ は s に依存せず自由な値をとることができる。D は、$F(X,Y)$ も $\hat{F}(X,Y)$ も等確率で選ぶため、秘密情報 s は不正者に一切漏れない。

参考文献

[BGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson.

Completeness theorems for non-cyptographic fault-tolerant distributed computation.

In Janos Simon, editor, STOC '88, pages 1–10. ACM, 1988.