BGW Verifiable Secret Sharing

2020/6/28 藤﨑@ JAIST

1 BGW VSS

Ben-Or/Goldwasser/Wigderson Verifiable Secret Sharing 方式 [1] とその証明。Shamir の秘密分散では、Dealer（以下 D）が正直な場合、$P_1, \ldots, P_n$ に $f(\alpha_1), \ldots, f(\alpha_n)$ がそれぞれ配られ、不正者数 t が $n/3$ 未満 ($n \geq 3t+1$) であれば、Reed-Solomon 符号の (Welch/Berlekamp) 復号によりもとの多項式 $f(X)$ が復元でき、それゆえ D の秘密 $s = f(0)$ が正しく復元できる。

$$\hat{f}(\alpha_i) = f(\alpha_i) + e_i \text{ s.t. } W_H(\boldsymbol{e}) \leq t \quad \Longrightarrow \quad \text{Reconstruct } f(X)$$

しかし、D が不正者であった場合これは成り立たない。D が正直であっても不正者であっても、プロトコルが受理 (accept) された場合は、秘密分散が必ず正しく行われている方式として、検証可能秘密分散方式がある。

BGW VSS の Reconstruction と Privacy の証明は、[2] を参考にしている。

1.1 Bivariable Symmetric Polynomial

K を有限体。次のような K 係数の二変数対称多項式を考える。

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

such that $\deg_X(F) = \deg_Y(F) = t$ and, for all $0 \leq i, j \leq t$, $r_{i,j} = r_{j,i}$. 全ての i, j に対して、$F(\alpha_i, \alpha_j) = F(\alpha_j, \alpha_i)$ が成立することに注意。

- $\alpha_1, \ldots, \alpha_n \in K$: 全て異なる値.
- $f(X) \triangleq F(X, 0)$: D's real sharing polynomial.
- $f_i(X) \triangleq F(X, \alpha_i)$: P_i's verification 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 $f(X)$.

以下、常に不正な参加者の集合を $\mathcal{A}_{t,n}$ とし ($\#\mathcal{A}_{t,n} = t$)、$n \geq 3t+1$. よって、正直な参加者の集合を H とすると、$\#H = n - t \geq 2t+1$. また、有限体 K と $\alpha_1, \ldots, \alpha_n \in K$ はシステム共通のパラメータであり、$\#K > n$ かつ、$\alpha_1, \ldots, \alpha_n$ は全て異なる値である。

1.2 Distribution Phase

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 1.1 章の $s = r_{00}$ となる二変数対称多項式 $F(X,Y) = \sum_{i,j=1}^{t} r_{i,j} X^i Y^j$ をランダムに

選ぶ。すなわち、$s = F(0,0)$. D は、各 P_i $(i = 1, \ldots, n)$ に検証多項式 $f_i(X) = F(X, \alpha_i)$ を（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[*1]、Step 9 でプロトコルが受理されるまで復活しない。
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。D が不正をしていなければ $s_i = f_i(0) = F(0, \alpha_i) = F(\alpha_i, 0) = f(\alpha_i)$. 各 P_i は、$s_{ij} = f_i(\alpha_j)$ を（秘密通信で）P_j $(j \in \{1, \ldots, n\} \backslash \{i\})$ に送る。
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。D が不正をしていなければ $s_{ij} = f_i(\alpha_j) = F(\alpha_j, \alpha_i) = F(\alpha_i, \alpha_j) = f_j(\alpha_i) = s_{ji}$. 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。
5. D は、各 $(\text{dispute}, i, j)$ に対して、$\hat{s}_{ij}$ $(= F(\alpha_i, \alpha_j))$ を broadcast する。
6. $(\text{dispute}, i, j)$ に対して broadcast された $\hat{s}_{ij}$ を、P_i と P_j はそれぞれ $\hat{s}_{ij} = s_{ij} (= f_i(\alpha_j))$ と $\hat{s}_{ij} = s_{ji} (= f_j(\alpha_i))$ 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、$\hat{f}_i(X)$ $(= f_i(X))$ を broadcast する。
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。

注釈 1　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。

注釈 2　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。

1.3 Reconstruction

正直な $n - t$ 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。

2 Perfect Reconstruction

定理 3　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 $f(X)$ の点 $f(\alpha_i)$ をもつ。$n \geq 3t+1$ で、$\#H = n - t \geq 2t+1$ より Reconstruction で秘密

[*1] broadcast channel を仮定していない場合は、Byzantine algorithm で broadcast を実現する（$n > 3t$ より可能）.

$f(0)$ が常に正しく復元できる。

2.1 D が正直な場合

D が正直な場合の定理 3 の証明を考える。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 $f_i(0) = f(\alpha_i)$ が成り立つ。 ■

2.2 D が不正者の場合

以下、D を不正者とする。まず次の重要な lemma を考える。

Lemma 4 $f_1(X), \ldots, f_p(X) \in K[X]$ 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、

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

となる。

Claim 5 $p = t+1$ の時、Lemma 4 は成立する。

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。□

Claim 6 $p > t+1$ の時、Lemma 4 は成立する。

$Q = \{1, \ldots, t+1\}$ とする。$i \in Q$ に対しては、Claim 5 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、$f_j(X) = \boldsymbol{x}^T R \boldsymbol{\mu_j}$ $(j \notin Q)$. □

以下、上述の補題を使い D が不正者の場合の定理 3 の証明を示す。

- 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、$H = C \sqcup \bar{C}$.

と定義する。このとき、

Claim 7　Step 6 で、プロトコルが終了しない場合、$\#C \geq t + 1$.

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、

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

が成り立つ。□

Step 4 で、$i, j \in C$ に対して、$f_i(\alpha_j) = f_j(\alpha_i)$ が成り立っている（$i = j$ のときは、プロトコルでは調べないが常に成り立つので ok)。この時点でプロトコルが終了しないとしたら、accuse した参加者は高々 t 人であるから、Claim 7 より $\#C \geq t + 1$ である。よって、Lemma 4 より、全ての $i \in C$ に対して、 二変数対称多項式 $F(X, Y) = \boldsymbol{x}^T R \boldsymbol{y}$ が存在して、$f_i(X) = \boldsymbol{x}^T R \boldsymbol{\mu_i}$ 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、

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

$f_i(\alpha_j) = \boldsymbol{\mu_j}^T R \boldsymbol{\mu_i} = (\boldsymbol{\mu_j}^T R \boldsymbol{\mu_i})^T = \boldsymbol{\mu_i}^T R^T \boldsymbol{\mu_j} = \boldsymbol{\mu_i}^T R \boldsymbol{\mu_j}$. $\hat{f}_j(\alpha_i) = \boldsymbol{\mu_i}^T \hat{\boldsymbol{f}}_{\boldsymbol{j}}$ とおけて、Claim 6 より、$\hat{\boldsymbol{f}}_{\boldsymbol{j}} = R\boldsymbol{\mu_j}$. よって、

$$\hat{f}_j(X) = \boldsymbol{x}^T R \boldsymbol{\mu_j} \qquad \text{for all } j \in \bar{C}$$

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、

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

が成り立つ。$F(X, Y)$ が対称多項式より、$f_i(0) = F(0, \alpha_i) = F(\alpha_i, 0) = f(\alpha_i)$. ■

3 Perfect Privacy

定理 8　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。

$\hat{F}(X,Y)$ 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、$\left(\prod_{j\in\mathcal{A}_{t,n}}(Y-\alpha_j)\right) \mid g(X,Y)$ 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、$\left(\prod_{j\in\mathcal{A}_{t,n}}(X-\alpha_j)\right) \mid g(X,Y)$ 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。

別の書き方をすれば、$F(X,Y)$ を一様ランダムに選んだときの $F(0,0)$ は、K 上を一様ランダムであるが、(5) を満足する $F(X,Y)$ を一様ランダムに選んでも、$F(0,0)$ の分布は K 上一様ランダムになる。

$$\Pr_{F(X,Y)\leftarrow D}[F(0,0) = s \mid f_j(X) = F(X,\alpha_j) \text{ for } \forall P_j \in \mathcal{A}_{t,n}] = \Pr_{F(X,Y)\leftarrow D}[F(0,0) = s] = \frac{1}{|K|}.$$

参考文献

[1] 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.

[2] Ronald Cramer, Ivan Damgård, and Jesper Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.