

[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 2 日

本日の講義の内容

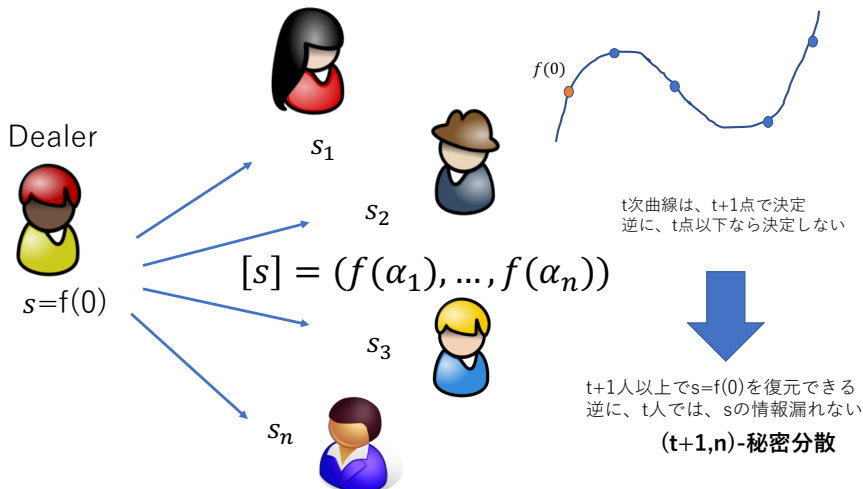
① Shamir 秘密分散 (復習)

② 能動的安全性に向けて

③ Reed-Solomon 符号

Shamir 秘密分散

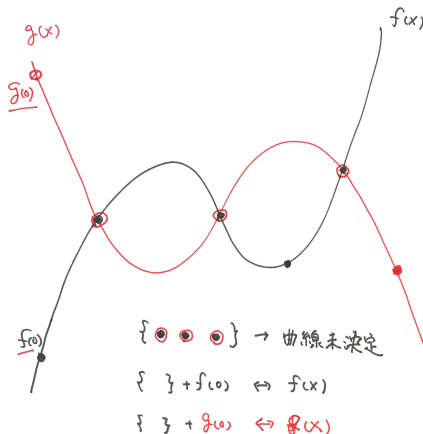
Dealer は、多項式 f を $s = f(0)$ かつ $\deg(f) = t$ となる条件でランダムに選ぶ。秘密を分割して参加者間で保持。 t 人では秘密が全く漏れない。 $t + 1$ 人以上で秘密を復元できる。



多項式の決定から

$f(X)$ の決定 $\iff$ 曲線の $\deg(f) + 1$ 点の決定

- $(f(0)$ 以外の) $\deg(f)$ 点が漏れる $\implies$ 秘密 $f(0)$ の情報全くなし
- $\deg(f) + 1$ 点を公開 $\implies f(X)$ が決定するので $f(0)$ が決定



Shamir 秘密分散 (formal)

Shamir 秘密分散 $SS = (\text{Share}, \text{Recon}, \Gamma_{t+1,n})$. $\alpha_1, \dots, \alpha_n \in K$ はシステムで予め定められた異なる値。

Shamir SS

- $\text{Share}(s)$:

- $a_0 := s$ の条件のもと K 係数のランダムな t 次多項式 $f(X) = \sum_{i=0}^t a_i X^i$ を選ぶ。

$$f(X) \leftarrow_R K[X] \quad \text{such that} \quad \deg(f) = t \text{ and } a_0 = s.$$

- $[s] = (f(\alpha_1), \dots, f(\alpha_n))$ を出力する。
- $\text{Recon}(S_Q)$ ($S_Q = \{f(\alpha_i) | i \in Q \text{ s.t. } Q \in \Gamma_{t+1,n}\}$): s を出力。

$$s = \sum_{i \in Q} \lambda_{i,Q} f(\alpha_i) \text{ where } \lambda_{i,Q} = \prod_{j \in Q \setminus \{i\}} \left(\frac{\alpha_j}{\alpha_j - \alpha_i} \right).$$

Reconstruction vector $(\lambda_{1,Q}, \dots, \lambda_{\#Q,Q})$ は、 S_Q のみで決定することに注意

某企業の例

- 関数を回路 (= 専用チップ) に直して実現するのは不便。またループが可変にあるようなものに向かない。
- 回路で MPC が実現できる (feasibility result) から、高級言語で MPC を実現へ $\implies$ 高級言語の関数一つ一つを (高速な) MPC 計算に作り直す。関数の品揃えを増やしている。
- 実現で悩んでいる難しい関数がまだまだ多数存在する。
- 今の所、Passive Case を中心に開発が進んでいる。

本日の講義の内容

① Shamir 秘密分散 (復習)

② 能動的安全性に向けて

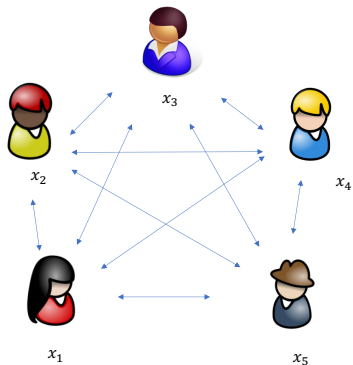
③ Reed-Solomon 符号

安全性モデル

大雑把に言うと、現実が、理想と同じ、または十分近くなれば安全という。

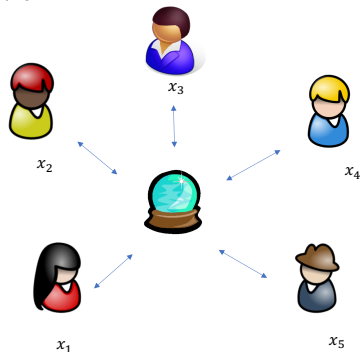
現実のプロトコル

互いに通信し計算結果を得る



理想状態

各自の秘密を  に預けると計算結果を返してくれる



Adversary (攻撃者)

- Passive Adversary (aka semi-honest or honest-but-curious).
 - 受動的攻撃者
 - 正規のプロトコルからは逸脱しないが、プロトコルから得た情報から正直な参加者の秘密情報を得ようとする
- Active Adversary
 - 能動的攻撃者
 - プロトコルから逸脱しても良い。正直な参加者の秘密情報を得ようとする事と、プロトコルを失敗に終わらせようとする。
 - さらに、static case と adaptive case が存在する。
 - static adversary: プロトコルが始まる前に不正者が固定されている
 - adaptive adversary: プロトコル中に正直な参加者を corrupt して、今までの情報を得た上に不正者として操ることができる

知られている結果

不正者数 (Adversary が corrupt できる参加者数) に応じた結果

	Passive	Active w/ broadcast	Active w/o broadcast
情報理論的安全	$< \frac{n}{2}$	$< \frac{n}{3}$	$< \frac{n}{3}$
統計的安全	$< \frac{n}{2}$	$< \frac{n}{2}$	$< \frac{n}{3}$
計算量的安全	n	$< \frac{n}{2}$	$< \frac{n}{2}$

ただし、 $n > 2$.

- 情報理論的安全: Real と Ideal の分布が完全に同じ
- 統計的安全: Real と Ideal の分布の差がわずかな統計的差しかない。
- 計算量的安全: 多項式時間制限の Environment $\mathcal{Z}$ では、識別できないぐらいしか、Real と Ideal の分布に違いはない。

Secure MPC against Active Adversaries

- 参加者: $P_1, \dots, P_n$.
- 各 P_i への秘密の入力: $x_i \in \{0, 1\}^\lambda$
- 全参加者への入力: 関数 $F : \{0, 1\}^{n\lambda} \rightarrow \{0, 1\}^*$.
- 各 P_i への出力: $F(x_1, \dots, x_n)$.
- パラメータ: t, n ($t < n/3$)
- 不正者: Active, $\mathcal{A}_{t,n} (\triangleq \{A \subset \{1, \dots, n\} \mid \#A \leq t\})$.

Theorem

There is an efficient MPC protocol to evaluate any efficiently computable function F such that the following conditions hold:

- (Perfect Correctness) All honest players receive $F(x_1, \dots, x_n)$ with prob. 1.*
- (Perfect Privacy) Any (statically) active $\mathcal{A}_{t,n}$ -adversary with $t < n/3$ learns no information beyond $\{x_i\}_{i \in \mathcal{A}_{t,n}}$ and $F(x_1, \dots, x_n)$ from executing the protocol regardless of their computing power and memory.*

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ならない。

- 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、全てのシェアが正しいことを前提に復元される (解決策：今日の話)。
- 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：来週)。

本日の講義の内容

① Shamir 秘密分散 (復習)

② 能動的安全性に向けて

③ Reed-Solomon 符号

$(n, t+1)$ -線型符号とは、 n 次元ベクトル空間の $t+1$ 次元部分空間である。 $K = \mathbb{F}_q$ (元の個数が q 個の有限体) とする。 $\alpha_1, \dots, \alpha_n \in K$ ($\alpha_i \neq \alpha_j$ for $i \neq j$) とする。

Reed-Solomon (RS) 符号

$f \in K[X]$, $\deg(f) \leq t$ となる多項式から作られる次の符号語

$$(f(\alpha_1), \dots, f(\alpha_n))$$

の全体からなる集合を、 $(n, t+1)$ -Reed-Solomon 符号と言う。

$$\text{i.e., } C^{\text{RS}} = \{(f(\alpha_1), \dots, f(\alpha_n)) \mid f \in K[X] \text{ s.t. } \deg(f) \leq t\}.$$

$(n, t+1)$ -RS 符号は $(n, t+1)$ -線型符号

線型符号

線型符号のこと

- 線型符号 C は、 K 上ベクトル空間の部分ベクトル空間であるので、

$$c, c' \in C, \quad a, b \in K \quad \implies \quad ac + bc' \in C.$$

つまり、符号語の線形和は符号語。

- 任意の相異なる符号語 c, c' と (ハミング) 重み τ 以下の任意の (エラー) ベクトル e, e' に対して、必ず

$$c + e \neq c' + e'$$

なら、 τ 個誤り訂正可能 (τ -error correcting) という。

- 線型符号の最小距離 d は、非零の最小の符号語のハミング重みに等しい
- 線型符号誤り訂正可能 (最大) 数は、 $\tau < \frac{d}{2}$ の最大値。

- $v \in K^n$ のハミング重み: $w_H(v) \triangleq \# \text{ of } \{v_i \neq 0 \text{ for } v = (v_1, \dots, v_n)\}$.
- v と w 間のハミング距離: $d_H(v, w) \triangleq w_H(v - w)$.
- 符号の最小距離: 二つの符号間のハミング距離の最小値.
 $d = \min\{d_H(c, c') \mid \forall c, c' \in C \text{ s.t. } c \neq c'\}$

Theorem

$(n, t+1)$ -Reed-Solomon 符号の最小距離は $n - t$ ($(n, t+1)$ -線型符号の最小距離の上界)。ここから誤り訂正可能最大数は $\tau < \frac{n-t}{2}$ なる τ の最大値。

Proof.

RS 符号語が $\mathbf{f} = (f(\alpha_1), \dots, f(\alpha_n))$ であることを頭に入れ、

$$\text{非零の符号 } \mathbf{f} \in C^{\text{RS}} \iff f(x) = 0 \text{ の零点が } t \text{ 個以下}$$

何故ならば、 $\deg(f) \leq t$ より $t+1$ 点以上の零点があると $f \equiv 0$ 。よって、

$$f(x) = 0 \text{ の零点が } t \text{ 個以下} \iff w_H(\mathbf{f}) \geq n - t$$

これから、最小距離 $d = n - t$ が導かれる。さらに、 $w_H(\mathbf{e}) < (n - t)/2$ なら、

$$\forall \mathbf{c}, \mathbf{c}' \in C^{\text{RS}}, \forall \mathbf{e}, \mathbf{e}' (w_H(\mathbf{e}), w_H(\mathbf{e}') < (n - t)/2) \implies \mathbf{c} + \mathbf{e} \neq \mathbf{c}' + \mathbf{e}'.$$



RS-符号の復号 (その1)

Shamir SS の不正者が $1/3$ 未満の場合の Reconstruction の具体的手法に相当。

- 符号語 $\mathbf{f} = (f(\alpha_1), \dots, f(\alpha_n))$ where $\deg(f) \leq t$ and $n \geq 3t + 1$.
- エラー付き $\hat{\mathbf{f}} = (y_1, \dots, y_n) = \mathbf{f} + \mathbf{e}$ where $W_H(\mathbf{e}) \leq t$
- Goal: $\hat{\mathbf{f}}$ から $\mathbf{f}$ に復号する

Welch/Berlekamp Algorithm

- $Q(X, Y) \triangleq f_0(X) - f_1(X)Y$
- $Q(\alpha_i, y_i) = 0$ for $i = 1, \dots, n$
- $\deg(f_0) \leq 2t$ and $\deg(f_1) \leq t$
- $f_1(0) = 1$

となる $f_0(X), f_1(X)$ を求め、 $f(X) = \frac{f_0(X)}{f_1(X)}$ として出力。

$W_H(\mathbf{e}) \leq t$ かつ、 $n \geq 3t + 1$ ならこのような f_0, f_1 は存在し、さらに $f(X) = \frac{f_0(X)}{f_1(X)}$ を満たす。

RS-符号の復号（その2）

f_0, f_1 の存在証明.

$y_i = f(\alpha_i) + e_i$ で、 $e_i \neq 0$ は高々 t 個なので、 f_0, f_1 は次のように存在する。
 $B = \{i \mid e_i \neq 0\}$ とおく。定義より、 $\#B \leq t$.

$$k(X) = \frac{\prod_{i \in B} (X - \alpha_i)}{\prod_{i \in B} (-\alpha_i)}$$

とおく。

- $f_0(X) = k(X)f(X)$,
- $f_1(X) = k(X)$

とおくと、 $f_1(0) = 1$, $\deg(f_0) \leq 2t$, $\deg(f_1) \leq t$. さらに、 $i = 1, \dots, n$ に対して、

$$Q(\alpha_i, y_i) = f_0(\alpha_i) - f_1(\alpha_i)y_i = k(\alpha_i)(f(\alpha_i) - y_i) = 0.$$

よって、 f_0, f_1 は存在。

RS-符号の復号（その3）

- $f_0(X) = a_0 + a_1X + \dots + a_{2t}X^{2t}$
- $f_1(X) = 1 + b_1X + \dots + b_tX^t$

$Q(\alpha_i, y_i) = f_0(\alpha_i) - f_1(\alpha_i)y_i = 0$ for $i = 1, \dots, n$ から、以下の未知変数 $3t + 1$ の連立一次方程式を解く。

$$\begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \cdots & \alpha_1^{2t} & -y_1 & -y_1\alpha_1 & \cdots & -y_1\alpha_1^t \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \cdots & \cdots & \alpha_n^{2t} & -y_1 & -y_n\alpha_n & \cdots & -y_n\alpha_n^t \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{2t} \\ 1 \\ b_1 \\ \vdots \\ b_t \end{pmatrix}$$

RS-符号の復号 (その4)

- $\hat{Q}(X) = Q(X, f(X))$ と定義する。すると $\deg(\hat{Q}) \leq 2t$.
- $W_H(\mathbf{e}) \leq t$ より、 $y_i = f(\alpha_i)$ となる点が少なくとも $n - t$ 個ある。
- よって、 $n - t$ 個の (α_i) で、 $\hat{Q}(\alpha_i) = 0$.
- $n \geq 3t + 1$ より、 $\deg(\hat{Q}) \leq 2t < n - t$. よって、

$$\deg(\hat{Q}) \equiv 0.$$

- よって、

$$f_0(X) - f_1(X)f(X) \equiv 0.$$

- よって、

$$f(X) = \frac{f_0(X)}{f_1(X)}.$$