2015年7月9日

Shamirによる多項式秘密分散法の理論と実装

@elliptic_shiho

1　自己紹介

- 緑川 志穂 (@elliptic_shiho)
- どこにでも居る高校1年生
- 暗号学, 楕円曲線, セキュリティ, ...

2　最初に

- 正直CTFは関係ないです
- 暗号理論の初歩みたいな感じです
- こういう世界も有るのか〜程度に思っていただければ
- 数式アレルギーな方は言っていただければある程度噛み砕いた解説をその都度やるので言ってください!

3　最初に

- 本当は属性ベース暗号というものをやる予定でした
- しかし、準備の量があまりに多くて断念...
- 楕円曲線, ペアリング, IDベース暗号等のキーワードにびびっと来た方はぜひ調べてみてください

4　(k, n) 閾値法

- セキュリティスペシャリストなんかでお馴染み
- 秘密のデータをn個に分散、k個集まると復号できる
- 名前だけは色々と聞くと思います $\rightarrow$ しかし!!

5 (k, n) 閾値法

- 意外に実装が難しい?
- 数時間考えた程度では出てこない
- 今回は多項式を使った方法を紹介します

6　理論

- RSA**の開発で有名な** A. Shamir **による** (k, n) **閾値法の理論です**
- **なかなかに面白い**

7　理論

- 秘密の数sに対して(k, n)閾値法を適用するには次のようにします
- まず、$k-1$個の$r_j \in \mathbb{F}_p (j < k)$をランダムに選ぶ
- $r_0 := s$として、$k-1$次多項式

$$f(x) := \sum_{u=0}^{k-1} r_u x^u \tag{1}$$

を定義する。

8　理論

- 適当なn個の異なる数値$x_1, \ldots, x_n \in \mathbb{F}_p \setminus \{0\}$を用意する
- $y_j := f(x_j)$をそれぞれ計算して、j番目の人に(x_j, y_j)を渡す。
- 渡した後は、sと$f(x)$を消去する。

9　理論

- ???**何が嬉しいのか**???
- **先ほどの** (x_j, y_j) **を考える**
- $\longrightarrow$ **適当な** x **とそれで多項式を** evalute **した結果のペア**

10　理論

- 一般に、$k-1$次方程式は$k-1$個の点が決まると方程式の係数を決定できる
- つまり$r_0 = s$を復元可能
- 結果、n個の秘密分散に成功したことになる

11　理論

- どのように$k-1$個の点から係数を決定するのか
  - 面白い方法があります
- Lagrange係数$\Delta_{u,S}(x)$を

$$\Delta_{u,S}(x) := \prod_{j \in S \setminus \{u\}} \frac{x-j}{u-j} \tag{2}$$

  と定義する
- 式(2)を、Lagrangeの補完多項式という

12　理論

- どのように使うのか?
- 実際に元の関数を復元するには、

$$f(x) = \sum_{u \in S} f(u) \Delta_{u,S}(x) \tag{3}$$

  を計算することで復元できる。
- 式変形部分に関してはスライドの都合上やりませんが、一度やってみると面白いですよ

13　理論

- この方法で多項式補完をするには、k個の異なる(x_j, y_j)が存在する必要がある
- つまり、$k-1$個以下の異なる(x_j, y_j)しか存在する場合は補完出来ない
  $\rightarrow$結果的に(k, n)閾値法として使うことが可能となる

14　実装

- **実装してみました**
- **言語は**Python w/sage

15　実装

コード実演

https://gist.github.com/elliptic-shiho/06ed8ac99e754d21cd38

secret.sage

16　実装

- **ちょっと応用してCTFの問題を作りました**
  s01.elliptic-shiho.xyz/ctf/problem/44
- **良ければ解いてみてください**

17　まとめ

- (k, n) **閾値法の実装をした**
- Lagrange **の補完多項式を利用することで** n **次関数** $f(x)$ **を** $y_j = f(x_j)$ **で生成される** n **個の値のペア** (x_j, y_j) **から補完することができる**

おわり