3 者秘密計算

2 桁の数 $10a+b$ から秘密情報 $(x_1,x_2)=(a+1,b+1)$ を作る。3 人 P_1,P_2,P_3 で分散計算を行った結果を公開し、公開された 3 つの情報から秘密情報の積 $x_1\times x_2$ を取り出す。

積 $x_1\times x_2$ を考えるため、x_1,x_2 はそれぞれ 0 以外であるようにする為、$(x_1,x_2)=(a+1,b+1)$ と 1 を加えている。計算は有限体 $\mathbb{F}_{11}$ 上で考える。

P_1,P_2 の二人にそれぞれ x_1,x_2 を渡す。

P_1 は x_1 以外を知ることはなく P_2 は x_2 以外を知ることはない。P_3 は x_1,x_2 を知ることはない。

P_1,P_2 の二人はそれぞれ独自に 1 次多項式 $f_i(X)=x_i+c_iX$ を作る。c_i は P_1,P_2 の二人が勝手に決めほかに漏らすことはない。この多項式を使い、P_1 に $f_1(1),f_2(1)$ を渡し、P_2 に $f_1(2),f_2(2)$ を渡し、P_3 に $f_1(3),f_2(3)$ を渡す。

各 P_i はそれぞれで $y_i=f_1(i)\times f_2(i)$ を計算し y_1,y_2,y_3 がシェアとして公開される。

復号

公開された y_1,y_2,y_3 から復号を考える。

多項式 $f(X)=s+a_1X+a_2X^2$ とし、連立方程式 $y_i=f(i)$ を作り、その解 s,a_1,a_2 を求める。この時の s が $x_1\times x_2$ である。

具体的な復号手順

y_1,y_2,y_3 を得て次の連立方程式を作る。

$$\begin{cases} y_1=s+a_1+a_2 \\ y_2=s+2a_1+4a_2 \\ y_3=s+3a_1+9a_2 \end{cases} \Leftrightarrow \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ a_2 \end{pmatrix} \tag{1}$$

方程式を解くと $s,\ a_1,\ a_2$ が求まるので、この s が $x_1\times x_2$ である。

復号のために $f(X)$ を 2 次多項式としたが、これは P_1,P_2 が作った多項式 $f_1(X),f_2(X)$ が 1 次式であり、各 y_i は $y_i=f_1(i)\times f_2(i)$ と積をとったためである。この為、シェア y_i は 3 つ集めないと連立方程式を解けない。

実際に、各 y_i は次のような計算で作られる。

$$
\begin{aligned}
y_i =& f_1(i) \times f_2(i) && (2)\\
=& (x_1 + c_1 i)(x_2 + c_2 i) && (3)\\
=& x_1 x_2 + x_1 c_2 i + c_1 i x_2 + c_1 c_2 i^2 && (4)\\
=& x_1 x_2 + (x_1 c_2 + c_1 x_2) i + (c_1 c_2) i^2 && (5)
\end{aligned}
$$

その為、連立方程式の解は次の値となる。

$$(s, a_1, a_2) = (x_1 x_2, x_1 c_2 + c_1 x_2, c_1 c_2) \tag{6}$$

c_i は勝手に決めた値なので a_1, a_2 は何になるかわからないが、$f_i(X)$ の定数項を x_i と置けば必ず $s = x_1 x_2$ となる。
