Principle of ShaftStop

shaftstop.fhe@gmail.com

www.shaftstop.com

Table Defines Operator

- In binary space, if the encryption scheme is static, we can define an encryption scheme as below:
  - *Enc(0, Key)* = 你 = C_1
  - *Enc(1, Key)* = 好 = C_2
- We can give the following table *T* in advance:

$$\begin{vmatrix} 你你 & 你好 \\ 你好 & 好你 \end{vmatrix}$$

- This table defines an operator $\oplus$ in cipher space, which is $C_i \oplus C_j = T_{ij}$.

A Very Simple FHE Scheme

- For the integer numbers in [0,9], if the encryption scheme is static, there are 10 cipher-texts totally: $C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9$
- The secret key owner can calculate out two sets of data as below:

  $g_{add}(C_i, C_j) = Enc(Dec(C_i, Key) + Dec(C_j, Key), Key) = C_{ij\_add}$

  $g_{mul}(C_i, C_j) = Enc(Dec(C_i, Key) * Dec(C_j, Key), Key) = C_{ij\_mul}$

  $g_{add}(C_i, C_j)$ and $g_{mul}(C_i, C_j)$ define addition and multiplication operators in cipher space.

  Obviously, $g_{add}(C_i, C_j)$ and $g_{mul}(C_i, C_j)$ are both have 100 elements.
- By using $g_{add}(C_i, C_j)$ and $g_{mul}(C_i, C_j)$, any 3rd party can execute addition and multiplication operations on encrypted data. These two sets are called ***Computational Dictionary***, denoted as $G=\{g_{add}(C_i, C_j), g_{mul}(C_i, C_j)\}$.
- Unfortunately, this simple FHE scheme can only serve a very small space of cipher-text.

Extend the Plain-text Space

- For B_i in [0,255], the cipher space is S_{256} and the volume of $\boldsymbol{G}$ is $2*256^2=131072$.
- We can use 2 such integers $B^2=(B_i, B_j)$ to represent a larger integer B_i+B_j*256, which ranges from 0~65535. And $C_i=Enc(B_i,Key)$, $E_{256}=Enc(256,Key)$, $E_{256}^2=Enc(256^2,Key)$, $G=\{g_{add},g_{mul}\}$.

  $$C^2=Enc(B^2,Key)=Enc(B_i+B_j*256,Key)=Enc(B_i,Key)\oplus Enc(B_j,Key)\odot E_{256}=C_i\oplus C_j\odot E_{256}$$

  For the addition operation:

  $$C^2{}_1\oplus C^2{}_2=(C_{i1}\oplus C_{j1}\odot E_{256})\oplus(C_{i2}\oplus C_{j2}\odot E_{256})=C_{i3}\oplus C_{j3}\odot E_{256}=C^2{}_3$$

  where $C_{i3}=g_{add}(C_{i1},C_{i2})$, $C_{j3}=g_{add}(C_{j1},C_{j2})$

  For the multiplication operation:

  $$C^2{}_1\odot C^2{}_2=(C_{i1}\oplus C_{j1}\odot E_{256})\odot(C_{i2}\oplus C_{j2}\odot E_{256})$$

  $$=C_{i1}C_{i2}\oplus(C_{i1}C_{j2}\oplus C_{i2}C_{j1})\odot E_{256}\oplus C_{j1}C_{j2}\odot E_{256}^2=C_{i4}\oplus C_{j4}\odot E_{256}\oplus C_{k4}\odot E_{256}^2=C^3{}_4$$

  where $C_{i4}=g_{mul}(C_{i1},C_{i2})$, $C_{j4}=g_{add}(g_{mul}(C_{i1},C_{j2}),g_{mul}(C_{i2},C_{j1}))$, $C_{k4}=g_{mul}(C_{j1},C_{j2})$
- Through this way, B^n can be handled. But this scheme is still static which is unsafe.

Dynamic Mode

- Things become more complicated when dynamic property is concerned.
- Because the cipher space S is very large for dynamic scheme, the ***Computational Dictionary G*** cannot be listed pratically.
- Suppose P is in [0, 255], the cipher of a specific encryption scheme is $Enc(P,Key)=(C_1,C_2)$, where C_1 is in S_{256} and C_2 is in S.
- Give tow mappings M_1: $S_{256} \rightarrow S_{256}$, M_2: $S_{256} \rightarrow S$, where $C_1=M_1(P)$ and $C_2=M_2(C_1)$
- If we could find some function F which makes the following equations true:
  - $P = F(C_1, C_2)$
  - $F(C_{11}, C_{21}) \oplus F(C_{12}, C_{22}) = F(C_{11} \oplus C_{12}, M_2(C_{11} \oplus C_{12}))$
  - $F(C_{11}, C_{21}) \odot F(C_{12}, C_{22}) = F(C_{11} \odot C_{12}, M_2(C_{11} \odot C_{12}))$
- Thus, (F, M_1, M_2, Key, G) can construct a dynamic FHE scheme on [0,255].

ShaftStop Scheme

- Consider: $P = a_1 \cdot f(x_1) \cdot z_1 + a_2 \cdot f(x_2) \cdot z_2$

  Where $x_1, x_2 \in \mathbf{Z}$ and $P, a_1, a_2, z_1, z_2 \in \mathbf{R}$;

  $f()$: $\mathbf{Z_D} \rightarrow \mathbf{R \backslash 0}$ is continuous and differentiable on a finite and bounded domain of definition $\mathbf{Z_D}$.

  $A=(a_1, a_2)$ and $X=(x_1, x_2)$ compose the cipher-text, $C=(A, X)$;

  $f()$ and $Z=(z_1, z_2)$ compose the secret key, $Key=(f, Z)$.

- G is defined as: $\begin{cases} g_{add}(x_1, x_2, c) = \dfrac{f(x_1) + c \cdot f(x_2)}{f(h_1(x_1, x_2))} \\ g_{mul}(x_1, x_2) = \dfrac{f(x_1) \cdot f(x_2)}{f(h_2(x_1, x_2))} \end{cases} \Rightarrow \begin{cases} f(x_1) + c \cdot f(x_2) = g_{add}(x_1, x_2, c) \cdot f(h_1(x_1, x_2)) \\ f(x_1) \cdot f(x_2) = g_{mul}(x_1, x_2) \cdot f(h_2(x_1, x_2)) \end{cases}$

  Where $h1(), h_2()$: $\mathbf{Z_D^2} \rightarrow \mathbf{Z_D}$, and $g_{add}, g_{mul} \in \mathbf{R}$.

- For anyone holds G, the addition and multiplication operations on $f(x)$ can be executed, without knowing the expression of $f()$.

Homomorphism

$$C_1 + C_2$$

$$= [a_{11} \cdot f(x_{11}) \cdot y_1 + a_{12} \cdot f(x_{12}) \cdot y_2] + [a_{21} \cdot f(x_{21}) \cdot y_1 + a_{22} \cdot f(x_{22}) \cdot y_2]$$

$$= a_{11} \cdot [f(x_{11}) + \frac{a_{21}}{a_{11}} \cdot f(x_{21})] \cdot y_1 + a_{12} \cdot [f(x_{12}) + \frac{a_{22}}{a_{12}} \cdot f(x_{22})] \cdot y_2$$

$$= a_{11} \cdot g_1(x_{11}, x_{21}, \frac{a_{21}}{a_{11}}) \cdot f[h_1(x_{11}, x_{21})] \cdot y_1 + a_{12} \cdot g_1(x_{12}, x_{22}, \frac{a_{22}}{a_{12}}) \cdot f[h_1(x_{12}, x_{22})] \cdot y_2$$

$$= a_{31} \cdot f(x_{31}) \cdot y_1 + a_{32} \cdot f(x_{32}) \cdot y_2$$

$$= C_3$$

$$C_1 \cdot C_2$$

$$= [a_{11} \cdot f(x_{11}) \cdot y_1 + a_{12} \cdot f(x_{12}) \cdot y_2] \cdot [a_{21} \cdot f(x_{21}) \cdot y_1 + a_{22} \cdot f(x_{22}) \cdot y_2]$$

$$= a_{11} \cdot a_{21} \cdot f(x_{11}) \cdot f(x_{21}) \cdot y_1^2 + [a_{11} \cdot a_{22} \cdot f(x_{11}) \cdot f(x_{22}) + a_{12} \cdot a_{21} \cdot f(x_{12}) \cdot f(x_{21})] \cdot y_1 \cdot y_2 + a_{12} \cdot a_{22} \cdot f(x_{12}) \cdot f(x_{22}) \cdot y_2^2$$

$$= a_{11} \cdot a_{21} \cdot g_2(x_{11}, x_{21}) \cdot f[h_2(x_{11}, x_{21})] \cdot y_1^2 + [a_{11} \cdot a_{22} \cdot g_2(x_{11}, x_{22}) \cdot f[h_2(x_{11}, x_{22})] + a_{12} \cdot a_{21} \cdot g_2(x_{12}, x_{21}) \cdot f[h_2(x_{12}, x_{21})]] \cdot y_1 \cdot y_2$$

$$+ a_{12} \cdot a_{22} \cdot g_2(x_{12}, x_{22}) \cdot f[h_2(x_{12}, x_{22})] \cdot y_2^2$$

$$= a_{31} \cdot f(x_{31}) \cdot y_1^2 + [a'_{32} \cdot f(x'_{32}) + a''_{32} \cdot f(x''_{32})] \cdot y_1 \cdot y_2 + a_{33} \cdot f(x_{33}) \cdot y_2^2$$

$$= a_{31} \cdot f(x_{31}) \cdot y_1^2 + a'_{32} \cdot g_1(x'_{32}, x''_{32}, \frac{a'_{32}}{a''_{32}}) \cdot f[h_1(x'_{32}, x''_{32})] \cdot y_1 \cdot y_2 + a_{33} \cdot f(x_{33}) \cdot y_2^2$$

$$= a_{31} \cdot f(x_{31}) \cdot y_1^2 + a_{32} \cdot f(x_{32}) \cdot y_1 \cdot y_2 + a_{33} \cdot f(x_{33}) \cdot y_2^2$$

$$= C_4$$

Security Analysis

- Since the domain of definition of *f()* is finite and bounded, a set of variable *Y* can be used to replace *f()*, where:

$$Def_f = \{x_i \mid i \in I\}, Y = \{y_i = f(x_i) \mid i \in I\}$$

- Then the encryption formula is:

$$P = a_1 \cdot y_1 \cdot z_1 + a_2 \cdot y_2 \cdot z_2$$

- The scheme changes into a Multivariate Quadratic (**MQ**) Problem, which is proven to be NP-Complete.
- Moreover, when re-define *f()* as *f()*: $\mathbf{R_D \rightarrow R \backslash 0}$, the domain of definition becomes infinite, which makes it impossible to attack the scheme by solving the equation set.
- This improvement can make ShaftStop more secure.

Real version of $f()$: $\mathbf{R_D} \rightarrow \mathbf{R}\backslash 0$

- For the real version, the domain of definition of $f()$ is $\mathbf{R_D}$, which has infinite values of x_i.
- If $f()$ is continuous and differentiable everywhere, let $x_0 \in \mathbf{R_D}$, there should exists a range δ and $x_1 = x_0 + \delta$, which satisfies the following condition:
  - For any $x_0 < x < x_1$, $|f(x_0) + [f(x_1) - f(x_0)]/(x_1 - x_0) * (x - x_0) - f(x)| < \varepsilon$, where $\varepsilon > 0$ is small enough.
- In this case, we can use a linear interpolation algorithm to match $f()$ on a discreted set X, where the distance between any two nearby points is less than δ. In the other word, we can use two discreted set X and $F = \{f(x_i) | x_i \in X\}$ to represent $f()$, rather than using the analytic expression.
- The more gentle the curve of $f()$ is, the larger δ could be, and the number of points in set X is less, which also makes F be smaller.
- According to the definition, the computational dictionary $G = \{g_{add}(x_i, x_j, c), g_{mul}(x_i, x_j)\}$ is also continuous and differentiable, where g_{add}: $\mathbf{R_D}^3 \rightarrow \mathbf{R}$, g_{mul}: $\mathbf{R_D}^2 \rightarrow \mathbf{R}$.
- G can also be discreted in the similar way, and be represented as two discreted mappings.

Conclusions

- ShaftStop is a FHE scheme.
- Computation Dictionary G is the key-point to execute operations on cipher space.
- This scheme can be proven to be IND-CPA Secure.
- The commercial version of ShaftStop has already been developed, the advanced propetries include:

  Asymmetric sheme; Integrity checking for ciphertext; Stronger security against various attack modes; Controllable accuracy and volumn of ciphertext; Binary mode; Division operation; Cipher comparation; Cipher simplification; Secret key switch; Cipher delivery; etc.

End