KLVY

A1 The [Mah18] QFHE scheme

- $\mathrm{Enc}(|\psi\rangle) = \left(Z^\theta X^\chi |\psi\rangle,\ \text{classical encryptions of } \chi \text{ \& } \theta \right)$

i.e. $\mathrm{Enc}(|\psi\rangle) = \left(Z^\theta X^\chi |\psi\rangle,\ \{\hat{x}_i, \hat{\theta}_i\}_{i \in [\ell]} \right)$

ℓ = # qubits.

- Suppose, we want to evaluate a circuit C on $\mathrm{Enc}(|\psi\rangle)$ & obtain $\mathrm{Enc}(C|\psi\rangle)$.

This is done by the "Eval" procedure.

$$\mathrm{Eval}_C\left(\mathrm{Enc}|\psi\rangle, |0^t\rangle\right)$$

- We proceed gate-by-gate.

– for each gate in C,

suppose the gate implements $U \otimes \mathbb{I}$ (constantly many qubits; rest).

Then, Eval_C homomorphically evaluates

(i) the gate by applying $U' \otimes \mathbb{I}$ to its padded state (i.e. w/ $|0^t\rangle$ padded), where U' acts on original gate & plus the aux (init. to $|0\rangle$),

(ii) updating the classical ciphertexts to encrypt the "correspo"

–/–

KLVY

A1 The [Mah18] QFHE scheme.

- $\mathrm{Enc}(|\psi\rangle) = \left(Z^\theta X^x |\psi\rangle, \text{classical encryptions of } x \text{ \& } \theta \right)$

i.e. $\mathrm{Enc}(|\psi\rangle) = \left(Z^\theta X^x |\psi\rangle, \{\hat{x}_i, \hat{\theta}_i\}_{i \in [\ell]} \right)$

ℓ : # qubits.

- Suppose, we want to evaluate a circuit C on $\mathrm{Enc}(|\psi\rangle)$ & obtain $\mathrm{Enc}(C|\psi\rangle)$.

This is done by the "Eval" procedure.

$$\mathrm{Eval}_C\left(\mathrm{Enc}|\psi\rangle, |0^t\rangle\right)$$

- We proceed gate-by-gate.

  - for each gate in C,

    suppose the gate implements $U \otimes \mathbb{I}$ (constantly many qubits / rest).

Then, Eval_C homomorphically evaluates

(i) the gate by applying $U' \otimes \mathbb{I}$ to its padded state (i.e. w/ $|0^t\rangle$ padded), where U' acts on original gate & plus the aux (init. to $|0\rangle$),

(ii) updating the classical ciphertexts to encrypt the "correspon"-

Reminder:

- Suppose C is a Clifford gate. (instead of a general circuit).

- It holds that $\forall\ P_1, P_2$ in the Pauli grp. $\exists\ P_3, P_4$ in the Pauli grp s.t.

$$C(P_1 \otimes P_2) C^\dagger = P_3 \otimes P_4 .$$

$\Rightarrow \forall\ x, z, \exists\ x', z'$ s.t.

$$C Z^z X^x |\psi\rangle = Z^{z'} X^{x'} C |\psi\rangle .$$

└

- (Therefore) for all Clifford gates, Eval_C simply applies the gate & updates the classical encryptions of z, x to z', x'.

(NB: z' & x' can depend on z, x & the gate).

- The Toffoli gate, T, is more involved & uses the additional aux qubits.

Why?

Reminder: $T(\underbrace{Z^{z_1} X^{x_1} \otimes Z^{z_2} X^{x_2} \otimes Z^{z_3} X^{x_3}}_{\text{"}} |\psi\rangle) =$

$T(\quad\text{"}\quad) T^\dagger T |\psi\rangle$

$CNOT_{13}^{x_1}\ CNOT_{23}^{x_1} (\mathbb{1} \otimes H)\ CNOT_{12}^{z_3} (\mathbb{1} \otimes H)$

$\Big(Z^{z_1 + x_1 z_3 + x_1 x_2 z_3} X^{x_1} \otimes Z^{z_2 + x_1 z_3 + x_2 z_3} X^{x_2} \otimes Z^{z_3} X^{x_1 x_2 + x_3} \Big) T |\psi\rangle$

not clear which gate is the Hadamard action

where CNOT_{ij}^{s} is the "encrypted CNOT operation"

applied to the i,j^{th} qubits where

s indicates whether or not

CNOT is applied.

Clearly, in addition to the Paulis, there are corrections — to the idea we used w/ Cliffords is not enough.

How Eval_C implements T gates.

(i) applies T & updates the classical ciphertexts encoding the pads to be consistent w/

$$Z^{\delta_1 + x_2\delta_3} X^{x_1} \otimes Z^{\delta_2 + x_1\delta_3} X^{x_3} \otimes Z^{\delta_3} X^{x_1 x_2 + x_3}$$

(just as we did for Cliffords)

(ii) applies a correction to undo the

$$\mathrm{CNOT}_{13}^{x_2}\ \mathrm{CNOT}_{23}^{x_1}\ (\mathbb{I}\otimes H)\ \mathrm{CNOT}_{12}^{\delta_3}\ (\mathbb{I}\otimes H)$$

piece NB: $\mathbb{I}\otimes H$ is easily corrected by applying it again!

NB2: $\mathrm{CNOT}_{ij}\ \mathrm{CNOT}_{ij} = \mathbb{I}$.

NB3: To correct the CNOT part, Eval_C needs to apply CNOT, controlled on a classical FHE Enc of a bit s.

This is the main tech. achievement of [Mah 18].

& relies on aux qubits.

⌜ LWE allows us to do the following

Specifically, Mahadev uses an encryption scheme (associated with NTCF) w/ the following prop.

given encryption $\hat{\mathcal{S}}$ of a bit c,

(i) one can efficiently compute

$f_0, f_1 : \{0,1\}^* \to \mathcal{Y}$ s.t.

$\forall \quad (x_0, r_0), (x_1, r_1) \in \{0,1\} \times \mathcal{R}$

which is a claw (i.e. $f_0(x_0, r_0) = f_1(x_1, r_1)$),

it holds that $x_0 \oplus x_1 = 1$.

(ii) one can also compute the encryption of the trapdoor corresponding to the pair (f_0, f_1) (allows one to invert)

⌞

Procedure for applying the encrypted $CNOT^{\mathcal{S}}$ operation on a 2-qubit state

$$|\Psi\rangle = \sum_{a,b \in \{0,1\}} \alpha_{ab} |a, b\rangle,$$

given $\hat{\mathcal{S}}$

1. Classically, compute a description of the claw-free pair (f_0, f_1) corresponding to $\hat{\mathcal{S}}$.

2. Use the aux. qubits to entangle $|\Psi\rangle$ w/ a random claw for f_0, f_1 by computing

$$\sum_{\substack{a,b,\mu\in\{0,1\}\\ s\in R}} \alpha_{ab}\,|ab\rangle|\mu\, s\rangle|f_a(\mu,s)\rangle$$

& measuring the last register to obtain $y \in \mathcal{Y}$.

Let (μ_0, s_0), (μ_1, s_1) be the two pre-images of y,

i.e. $f_0(\mu_0, s_0) = f_1(\mu_1, s_1) = y$.

Then, the remaining state is

$$\sum_{a,b\in\{0,1\}} \alpha_{ab}\,|ab\rangle\,|\mu_a\, s_a\rangle.$$

3. XOR μ_a into the second register, i.e.

$$\sum_{ab\in\{0,1\}} \alpha_{ab}\,|a, b\oplus\mu_0\rangle\,|\mu_a\, s_a\rangle =$$

$(\because \mu_0\oplus\mu_1 = s)$

$$\sum_{a,b\in\{0,1\}} \alpha_{ab}\,(\mathbb{1}\otimes X^{\mu_0})\,|a,\, b+a\cdot s\rangle\,|\mu_a s_a\rangle =$$

(by def^n $CNOT^s_{12}$)

$$\sum_{a,b\in\{0,1\}} \alpha_{ab}\,(\mathbb{1}\otimes X^{\mu_0})\,CNOT^s_{12}\,|a,b\rangle\,|\mu_a s_a\rangle$$

4. Remove the entangled register $|\mu_a\, s_a\rangle$ by applying Hadamards:

$$\sum_{\substack{a,b,d_0\in\{0,1\}^l\\ d\in\{0,1\}^l}} \alpha_{ab}\,(\mathbb{1}\otimes X^{\mu_0})\,CNOT^s_{12}\,|ab\rangle\;(-1)^{(d_0 d)\cdot(\mu_a s_a)}\,|d_0\, d\rangle$$

5. Measure register $|d_0 d\rangle$ to get

$$(\mathbb{1}\otimes X^{\mu_0})\,\mathrm{CNOT}^{S}_{12} \sum_{ab\in\{0,1\}} (-1)^{(d_0 d)\cdot(\mu_0 s_0)} \alpha_{ab}|ab\rangle =$$

$$(-1)^{(d_0 d)(\mu_0 s_0)} \quad (\mathbb{1}\otimes X^{\mu_0})\,\mathrm{CNOT}^{S}_{12} \left(\sum_{b\in\{0,1\}} \alpha_{0b}|0,b\rangle + \right.$$

$$\left. (-1)^{(d_0 d)\cdot((\mu_0 s_0)\oplus(\mu_1 s_1))} \sum_{b\in\{0,1\}} \alpha_{1b}|1,b\rangle \right) =$$

$$(-1)^{(d_0 d)(\mu_0 s_0)} \left(\mathbb{1}\otimes X^{\mu_0}\right)\mathrm{CNOT}^{S}_{12} \left(Z^{(d_0 d)\cdot((\mu_0 s_0)\oplus(\mu_1 s_1))} \otimes \mathbb{1} \right)$$

$$\left(\sum_{ab\in\{0,1\}} \alpha_{ab}|ab\rangle \right) =$$

$$(-1)^{(d_0 d)(\mu_0 s_0)} \left(Z^{(d_0 d)\cdot((\mu_0 s_0)\oplus(\mu_1 s_1))} \otimes X^{\mu_0} \right) \mathrm{CNOT}^{S}_{12} \left(\sum_{\substack{ab \\ \in\{0,1\}}} \alpha_{ab}|ab\rangle \right)$$

6. Finally, use the (classical) encryption of the trapdoor for (f_0, f_1) to homomorphically evaluate

$$(d_0\ d)\cdot((\mu_0 s_0)\oplus(\mu_1 s_1)) \quad \& \quad \mu_0\, s_0$$

& update the classical encryptions of the Pauli pads.