Rate-1 Quantum Fully Homomorphic Encryption

Orestis Chardouvelis [1] Nico Döttling [2] Giulio Malavolta [3]

[1]National Technical University of Athens

[2]CISPA Helmholtz Center for Information Security

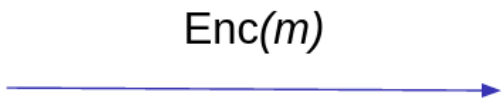
[3]Max Planck Institute for Security and Privacy

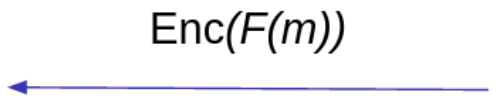
TCC 2021

Table of Contents

Fully Homomorphic Encryption Scheme

A FHE scheme allows Alice to encrypt some message m such that later Bob (holding any function F) can compute $\mathrm{Enc}(F(m))$.



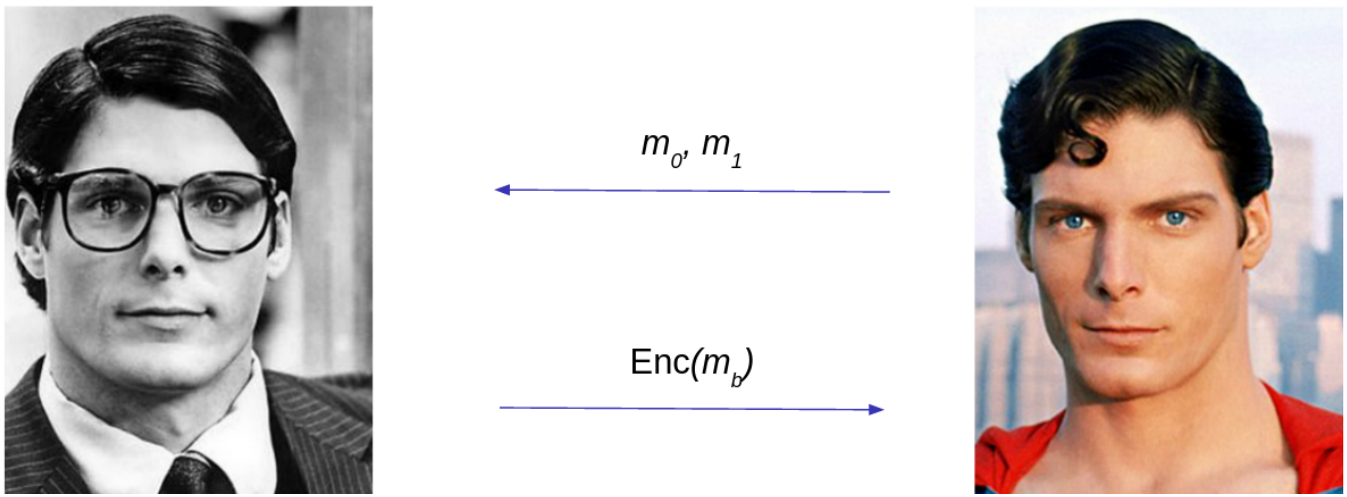


Fully Homomorphic Encryption Scheme

Semantic Security

- Semantic Security: Alice's input m must be hidden in an indistinguishability sense.

$$\mathrm{FHE.Enc}(pk, m_0) \approx_c \mathrm{FHE.Enc}(pk, m_1)$$



Fully Homomorphic Encryption Scheme

Circuit Privacy

Circuit Privacy: Bob's message must be statistically independent of F, conditioned on the output $F(m)$.

Fully Homomorphic Encryption Scheme

Circuit Privacy

Circuit Privacy: Bob's message must be statistically independent of F, conditioned on the output $F(m)$.

- **Semi-Honest Circuit Privacy**: Statistical circuit privacy is required to hold only for well-formed messages from Alice (pk and ciphertext).

vs

- **Malicious Circuit Privacy**: Statistical circuit privacy holds for any arbitrary message from Alice.

Fully Homomorphic Encryption Scheme

Circuit Privacy

Circuit Privacy: Bob's message must be statistically independent of F, conditioned on the output $F(m)$.

- **Semi-Honest Circuit Privacy**: Statistical circuit privacy is required to hold only for well-formed messages from Alice (pk and ciphertext).

vs

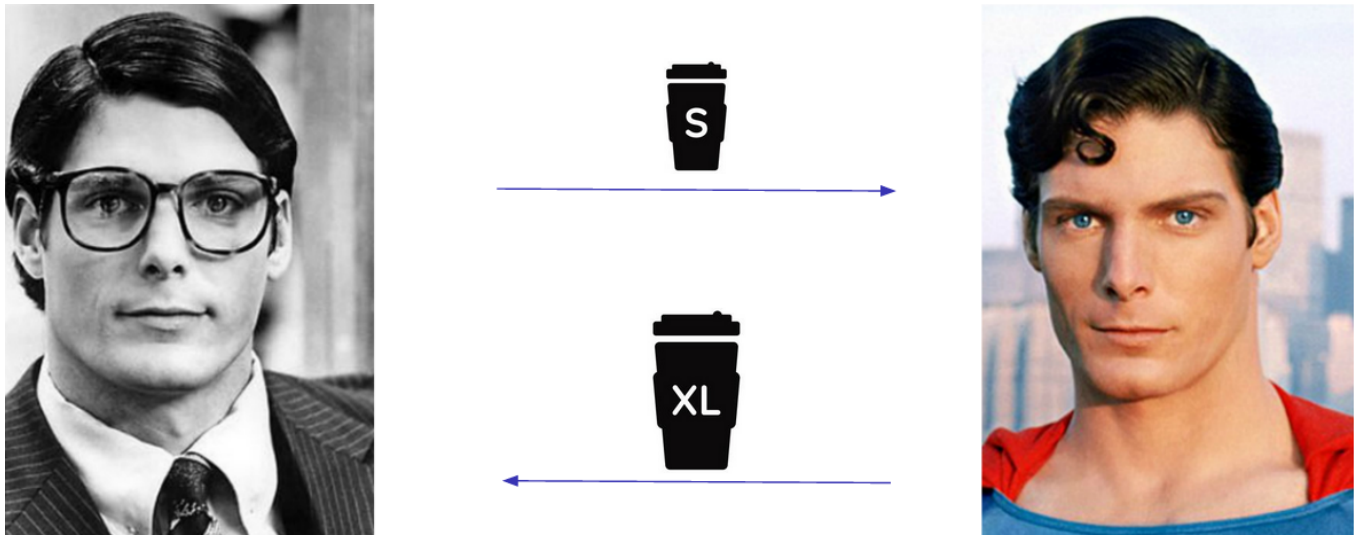
- **Malicious Circuit Privacy**: Statistical circuit privacy holds for any arbitrary message from Alice.

Malicious circuit privacy in classical FHE

Any classical FHE scheme can be converted into one with malicious circuit privacy [OPP14].

Fully Homomorphic Encryption Scheme

Communication Complexity



Ensure that communication overhead introduced for security doesn't nullify the efficiency of outsourcing computations.

Fully Homomorphic Encryption Scheme

Communication Complexity

- Communication complexity should be compact (independent of the size of the circuit).

Fully Homomorphic Encryption Scheme

Communication Complexity

- Communication complexity should be compact (independent of the size of the circuit).
- Useful in applications such as:
  - secure function evaluation
  - encrypted databases
  - private information retrieval [CGKS95]

Fully Homomorphic Encryption Scheme

Communication Complexity

- Communication complexity should be compact (independent of the size of the circuit).
- Useful in applications such as:
  - secure function evaluation
  - encrypted databases
  - private information retrieval [CGKS95]
- Best communication complexity approaches that of the insecure protocol (where Alice sends her input m in plain), assuming the hardness of LWE [BDGM19].

Fully Homomorphic Encryption Scheme

Rate

- Rate denotes the message-to-ciphertext ratio.

Fully Homomorphic Encryption Scheme

Rate

- Rate denotes the message-to-ciphertext ratio.
- Rate ρ: $\frac{\text{size of } F(m)}{\text{size of FHE.Eval}(F,m)} \geq \rho$.

Fully Homomorphic Encryption Scheme

Rate

- Rate denotes the message-to-ciphertext ratio.
- Rate ρ: $\frac{\text{size of } F(m)}{\text{size of FHE.Eval}(F,m)} \geq \rho$.
- Rate-1 schemes asymptotically approach rate $\rho = 1$.

Quantum FHE Scheme

In a Quantum FHE scheme Alice can encrypt a quantum state $|\psi\rangle$ whereas Bob (holding any unitary U) can compute

$\text{Enc}(|\psi\rangle)$

$\text{Enc}(U(|\psi\rangle))$

Quantum FHE Scheme

In a Quantum FHE scheme Alice can encrypt a quantum state $|\psi\rangle$ whereas Bob (holding any unitary U) can compute

$\text{Enc}(|\psi\rangle)$

$\text{Enc}(U(|\psi\rangle))$

Communication complexity with a quantum output?

Results

We construct quantum FHE in a malicious setting with communication complexity:

$$(|\,|\psi\rangle\,| + |C(|\psi\rangle)|) \cdot (1 + o(1))$$

Results

We construct quantum FHE in a malicious setting with communication complexity:

$$(|\,|\psi\rangle\,| + |C(|\psi\rangle)|) \cdot (1 + o(1))$$

Maliciously Circuit Private Quantum FHE

Assuming the quantum hardness of LWE, there exists a maliciously circuit private (levelled) QFHE scheme

Results

We construct quantum FHE in a malicious setting with communication complexity:

$$(|\,|\psi\rangle\,| + |C(|\psi\rangle)|) \cdot (1 + o(1))$$

Maliciously Circuit Private Quantum FHE

Assuming the quantum hardness of LWE, there exists a maliciously circuit private (levelled) QFHE scheme

Rate-1 Quantum FHE

Assuming the quantum hardness of LWE, there exists a (levelled) QFHE scheme with rate-1.

Table of Contents

Classical Techniques for Quantum FHE

Interference

Elements of a superposition representing the same bit string but with opposite amplitudes must cancel out.

Classical Techniques for Quantum FHE

Interference

Elements of a superposition representing the same bit string but with opposite amplitudes must cancel out.

Example

- Hadamard Transformation:

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \; H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Classical Techniques for Quantum FHE

Interference

Elements of a superposition representing the same bit string but with opposite amplitudes must cancel out.

Example

- Hadamard Transformation:

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \; H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

- $H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle$

Classical Techniques for Quantum FHE

Interference

Elements of a superposition representing the same bit string but with opposite amplitudes must cancel out.

Example

- Hadamard Transformation:

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \; H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

- $H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle$

- $\frac{1}{2}(|Enc(0)\rangle + |Enc(1)\rangle + |Enc(0)\rangle - |Enc(1)\rangle)$

Quantum One-Time Pad

- Solve using Quantum One-Time Pad [BJ15,Mah18,Bra18].

Quantum One-Time Pad

- Solve using Quantum One-Time Pad [BJ15,Mah18,Bra18].
- Pauli Operators:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Quantum One-Time Pad

- Solve using Quantum One-Time Pad [BJ15,Mah18,Bra18].
- Pauli Operators:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

- For a superposition $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ we sample $\text{otk} = (x, z) \in \{0,1\}^2$ and implement the QOTP as

$$\text{QOTP}(\text{otk}, |\phi\rangle) \equiv X^x Z^z |\phi\rangle = \alpha |x\rangle + (-1)^z \beta |1 \oplus x\rangle$$

Quantum FHE [Mah18]

$X^x Z^z |\psi\rangle$, $Enc(x,z)$

$X^{x'} Z^{z'} U |\psi\rangle$, $Enc(x',z')$

Quantum FHE

Mahadev Protocol

- Classical homomorphic computation along with a dependent quantum computation.

Quantum FHE

Mahadev Protocol

- Classical homomorphic computation along with a dependent quantum computation.
- $\begin{array}{c} X^x Z^z |\psi\rangle \\ \mathsf{Enc}(x,z) \end{array} \xrightarrow{U} \begin{array}{c} X^{x'} Z^{z'} U |\psi\rangle \\ \mathsf{Enc}(x',z') \end{array}$

Quantum FHE

Mahadev Protocol

- Classical homomorphic computation along with a dependent quantum computation.
- $$\begin{array}{c} X^x Z^z |\psi\rangle \\ \mathrm{Enc}(x,z) \end{array} \xrightarrow{U} \begin{array}{c} X^{x'} Z^{z'} U |\psi\rangle \\ \mathrm{Enc}(x',z') \end{array}$$
  - Clifford Gates: $U\, X^x Z^z |\psi\rangle = X^{x'} Z^{z'} U |\psi\rangle$.
  - Toffoli Gate: quantum operation dependent on the classically encrypted keys.

Quantum FHE

Mahadev Protocol

- Classical homomorphic computation along with a dependent quantum computation.
- $$\begin{array}{c} X^x Z^z |\psi\rangle \\ \mathrm{Enc}(x,z) \end{array} \xrightarrow{U} \begin{array}{c} X^{x'} Z^{z'} U |\psi\rangle \\ \mathrm{Enc}(x',z') \end{array}$$
  - Clifford Gates: $U\, X^x Z^z |\psi\rangle = X^{x'} Z^{z'} U |\psi\rangle$.
  - Toffoli Gate: quantum operation dependent on the classically encrypted keys.
- Quantum Capable FHE Scheme: A classical FHE that can be used to evaluate quantum circuits.

Quantum FHE

Properties of Interest

- The scheme has hybrid ciphertexts consisting of:
  - a Quantum OTP state.
  - a classical encryption of the completely classical *otk*.
- The classical component of the ciphertext satisfies (semi-honest) circuit privacy.

Quantum FHE

Our Contribution

Maliciously Circuit Private QFHE

We lift the protocol from the semi-honest to the malicious setting, providing security for any choice of Alice's first message.

Quantum FHE

Our Contribution

Maliciously Circuit Private QFHE

We lift the protocol from the semi-honest to the malicious setting, providing security for any choice of Alice's first message.

Rate-1 QFHE

We construct a QFHE scheme with nearly optimal ciphertext expansion.

Table of Contents

Existing QFHE Rate

- Rate ρ (Mahadev's scheme):

$$\frac{|C(|\psi\rangle)|}{|\mathsf{QFHE.QEval}\,(pk, C, |\phi\rangle)|} = \frac{\ell}{\ell + \text{size of HE keys}} \geq \rho$$

Existing QFHE Rate

- Rate ρ (Mahadev's scheme):

$$\frac{|C(|\psi\rangle)|}{|\mathsf{QFHE.QEval}\,(pk, C, |\phi\rangle)|} = \frac{\ell}{\ell + \text{size of HE keys}} \geq \rho$$

- Classical FHE is not rate-1.

- Overall Inverse Polynomial Rate!

Failed Approach

- Shrink classical information.

Failed Approach

- Shrink classical information.
- Sample $seed \leftarrow\$ \{0,1\}^{\lambda}$ for PRG.

Failed Approach

- Shrink classical information.
- Sample $seed \leftarrow\$ \{0,1\}^{\lambda}$ for PRG.
- Compute $\mathsf{QOTP}(\mathsf{PRG}(seed), |\psi\rangle), \mathsf{QEnc}(pk, seed)$

Failed Approach

- Shrink classical information.
- Sample $seed \leftarrow\$ \{0,1\}^{\lambda}$ for PRG.
- Compute QOTP(PRG($seed$), $|\psi\rangle$), QEnc(pk, $seed$)
- After homomorphic evaluation new one-time key :(

Failed Approach

- Shrink classical information.
- Sample $seed \leftarrow\$ \{0,1\}^{\lambda}$ for PRG.
- Compute QOTP(PRG($seed$), $|\psi\rangle$), QEnc(pk, $seed$)
- After homomorphic evaluation new one-time key :(

- Stuck with FHE.Enc(pk, otk), where two classical bits are necessary to encrypt a qubit.

Spooky Interactions [BDGM19]

- Some FHE schemes pack k classical bits $(m_1, \ldots, m_k)$ in ciphertexts of the form $c = (\boldsymbol{c}_0, c_1, \ldots, c_k) \in \mathbb{Z}_q^{n+1} \times \{0,1\}^k$.

Spooky Interactions [BDGM19]

- Some FHE schemes pack k classical bits $(m_1, \ldots, m_k)$ in ciphertexts of the form $c = (\boldsymbol{c}_0, c_1, \ldots, c_k) \in \mathbb{Z}_q^{n+1} \times \{0,1\}^k$.
- The last k-bits of the ciphertexts are *non-locally* correlated with the secret key sk.
- Spooky Decryption:

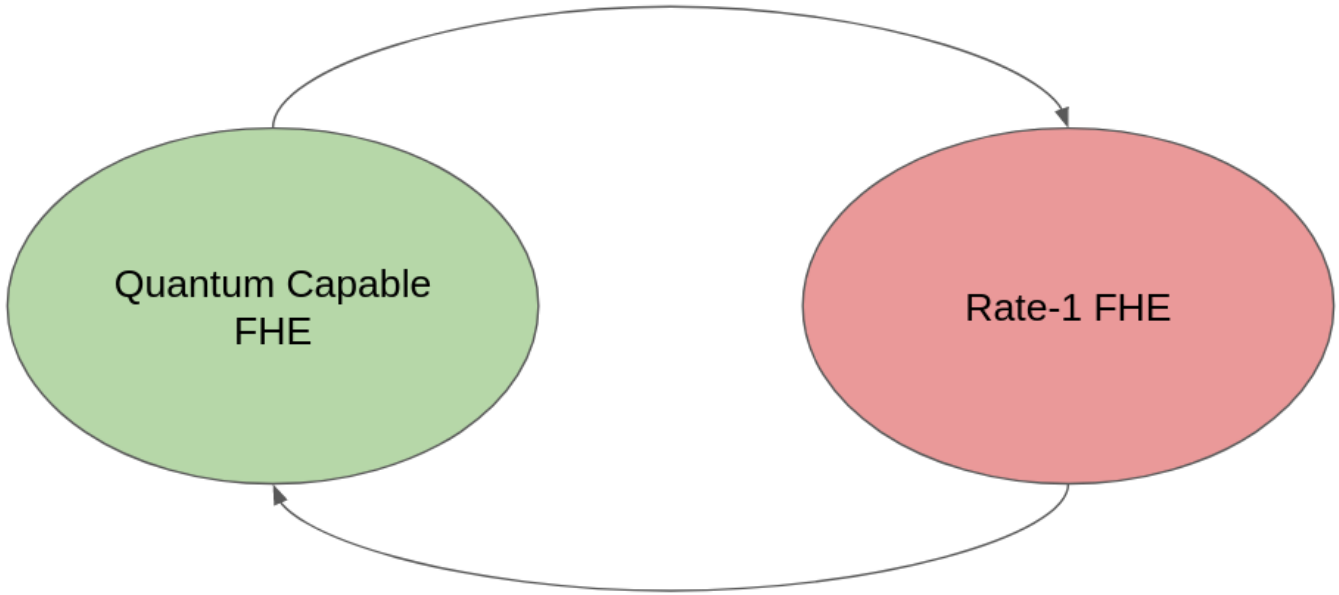
$$\mathsf{Dec}(sk, c) = F(sk, \boldsymbol{c}_0) \oplus (c_1, \ldots, c_k)$$

Construction

- Use spooky encryption scheme to get a Rate-1 form.

Construction

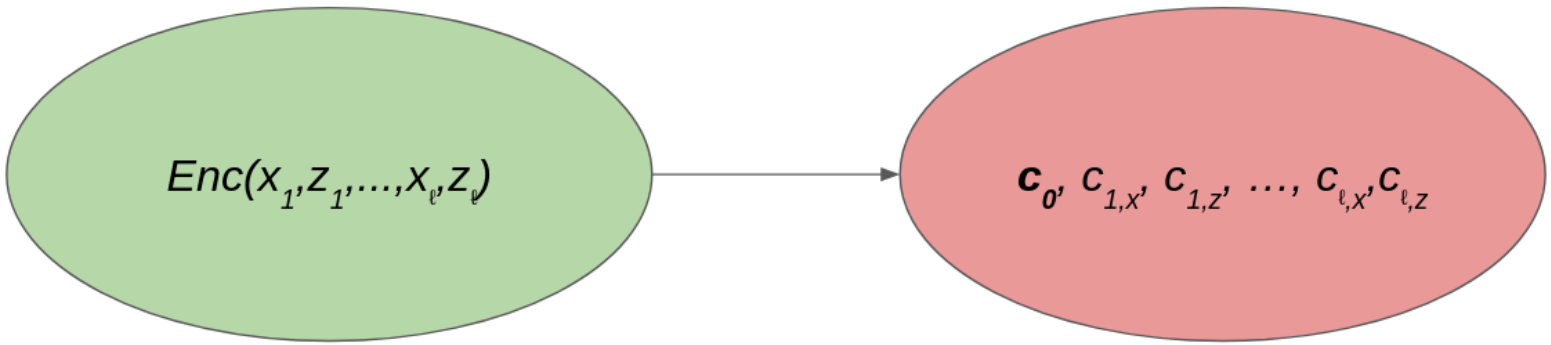
- Use spooky encryption scheme to get a Rate-1 form.



- Use the quantum capable FHE to perform homomorphic evaluations and the rate-1 to store the classical information.

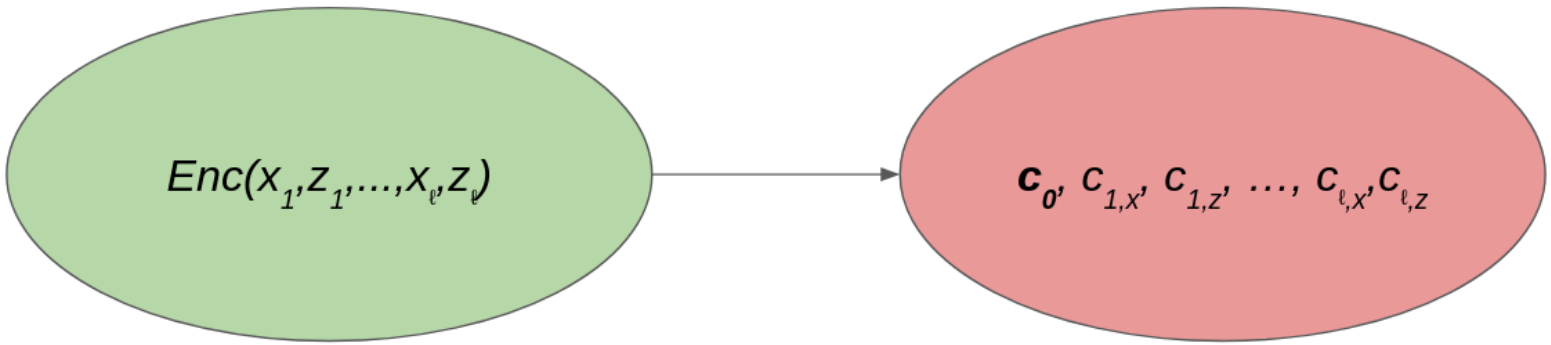
QFHE Construction

- Convert Enc(pk, otk) into an FHE ciphertext with spooky decryption via bootstrapping:



QFHE Construction

- Convert $\mathrm{Enc}(pk, otk)$ into an FHE ciphertext with spooky decryption via bootstrapping:



- Return $\boldsymbol{c}_0$ and $\bigotimes_{i\in[l]} (X^{c_{i,x}} Z^{c_{i,z}}) \cdot \mathrm{QOTP}(\mathrm{otk}, |\psi\rangle)$.

QFHE Construction

- Alter the one time key: $x_i, z_i \rightarrow x_i \oplus c_{i,x}, z_i \oplus c_{i,z}$

QFHE Construction

- Alter the one time key: $x_i, z_i \rightarrow x_i \oplus c_{i,x}, z_i \oplus c_{i,z}$
- The result of the function F is:

$$\begin{aligned} F(sk, \boldsymbol{c}_0) &= \mathrm{Dec}(sk, c) \oplus (c_{1,x}, c_{1,z}, \ldots, c_{\ell,x}, c_{\ell,z}) \\ &= (x_1, z_1, \ldots, x_\ell, z_\ell) \oplus (c_{1,x}, c_{1,z}, \ldots, c_{\ell,x}, c_{\ell,z}) \\ &= \text{the updated one time key} \end{aligned}$$

QFHE Construction

Rate

- Evaluated Plaintext $|\psi\rangle$: ℓ-qubit state.

QFHE Construction

Rate

- Evaluated Plaintext $|\psi\rangle$: ℓ-qubit state.
- Compressed Evaluated Ciphertext:
  - quantum information: ℓ-qubit state $|\phi\rangle$.
  - classical information: $\boldsymbol{c}_0$.

QFHE Construction

Rate

- Evaluated Plaintext $|\psi\rangle$: ℓ-qubit state.
- Compressed Evaluated Ciphertext:
  - quantum information: ℓ-qubit state $|\phi\rangle$.
  - classical information: $\boldsymbol{c}_0$.

$$\rho(\lambda) = \frac{\ell}{\text{size of } \boldsymbol{c}_0 + \ell} = 1 - \frac{\text{size of } \boldsymbol{c}_0}{\text{size of } \boldsymbol{c}_0 + \ell}.$$

QFHE Construction

Rate

- Evaluated Plaintext $|\psi\rangle$: ℓ-qubit state.
- Compressed Evaluated Ciphertext:
  - quantum information: ℓ-qubit state $|\phi\rangle$.
  - classical information: $\boldsymbol{c}_0$.

$$\rho(\lambda) = \frac{\ell}{\text{size of } \boldsymbol{c}_0 + \ell} = 1 - \frac{\text{size of } \boldsymbol{c}_0}{\text{size of } \boldsymbol{c}_0 + \ell}.$$

- By setting the parameters accordingly, the rate asymptotically approaches 1, assuming standard LWE.

Non-Generic Approach

- Construct a different classical FHE scheme.

Non-Generic Approach

- Construct a different classical FHE scheme.

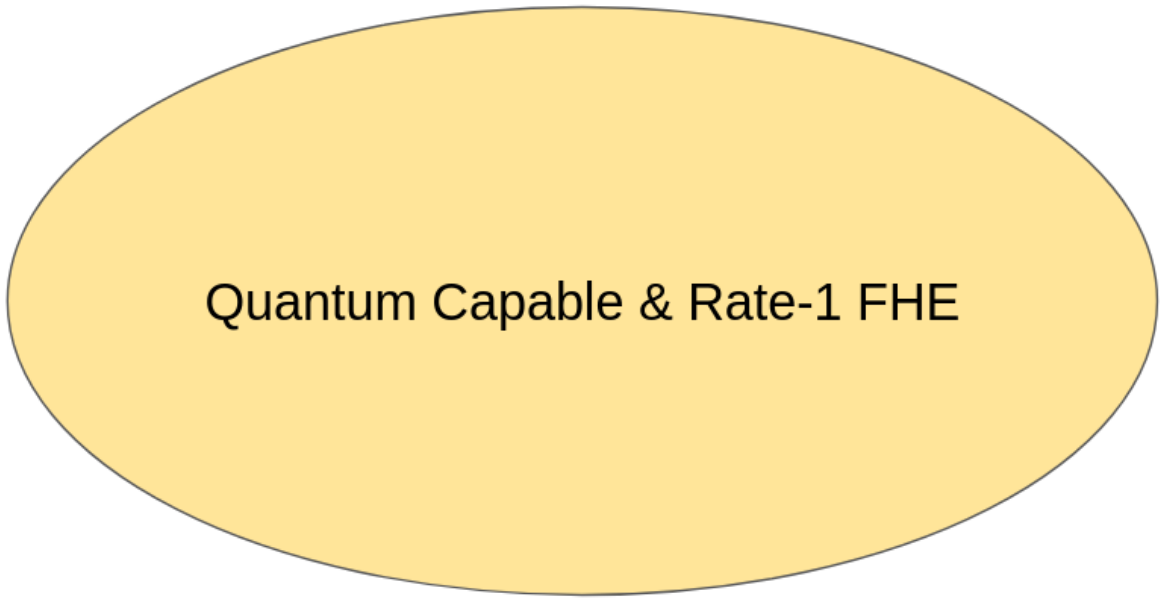


Table of Contents

Conclusion

- We construct maliciously circuit private rate-1 quantum FHE.

Conclusion

- We construct maliciously circuit private rate-1 quantum FHE.

  For any QFHE with a hybrid ciphertext form we:

  - Lift the protocol from semi-honest to maliciously circuit private FHE.
  - Get optimal (rate-1) communication complexity.

Conclusion

- We construct maliciously circuit private rate-1 quantum FHE.

  For any QFHE with a hybrid ciphertext form we:

  - Lift the protocol from semi-honest to maliciously circuit private FHE.
  - Get optimal (rate-1) communication complexity.

- https://eprint.iacr.org/2020/1454
  Orestis Chardouvelis, Nico Döttling and Giulio Malavolta.