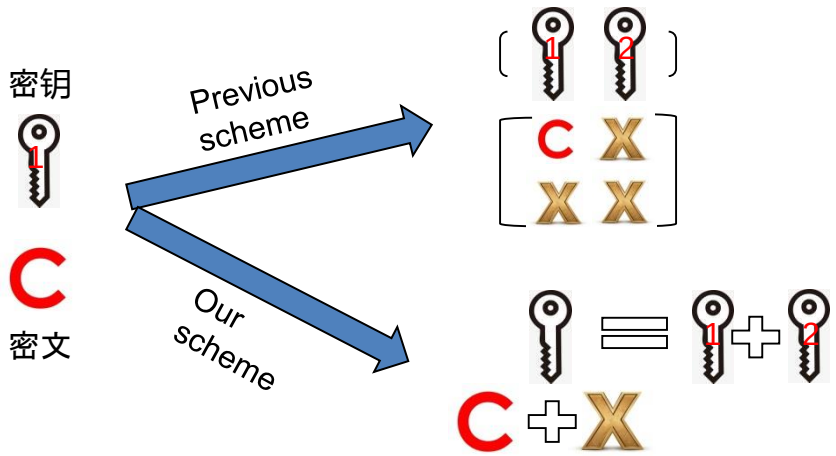
Multi-key FHE without Ciphertext-Expansion in Two-Server Model

Bingbing JIANG

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0479-5

Problems & Ideas

- In previous multi-key FHE schemes , the size of the ciphertext under multiple keys grows linearly or quadraticly with an increase in the number of the associated keys.
  - Expanding a ciphertext under a single key to a ciphertext under a set of keys with the same plaintext.
- Ideas: Can we construct a multi-key FHE scheme without ciphertext expansion?
  - Transform a ciphertext under a single key into a ciphertext under a ***sum*** of keys with the same plaintext.



Main Contributions

- **Comparison between our scheme and previous schemes**

Scheme	Standard Assumption	Growth Ratio
Lopez-Alt et al.	No	$O(n^{1+1/\varepsilon})$
CM15	Yes	$O(n^2)$
MW16	Yes	$O(n^2)$
BP16	Yes	O(n)
PS16#1	Yes	$O(n^2)$
PS16#2	Yes	O(n)
BHP17	Yes	$O(n^2)$
CZW17	Yes	O(n)
Our scheme	Yes	O(1)

1. Growth Ratio is that of the size of the new ciphertext and the original size.
2. n is the number of the associated keys.
3. ε is a parameter related to the security parameter.