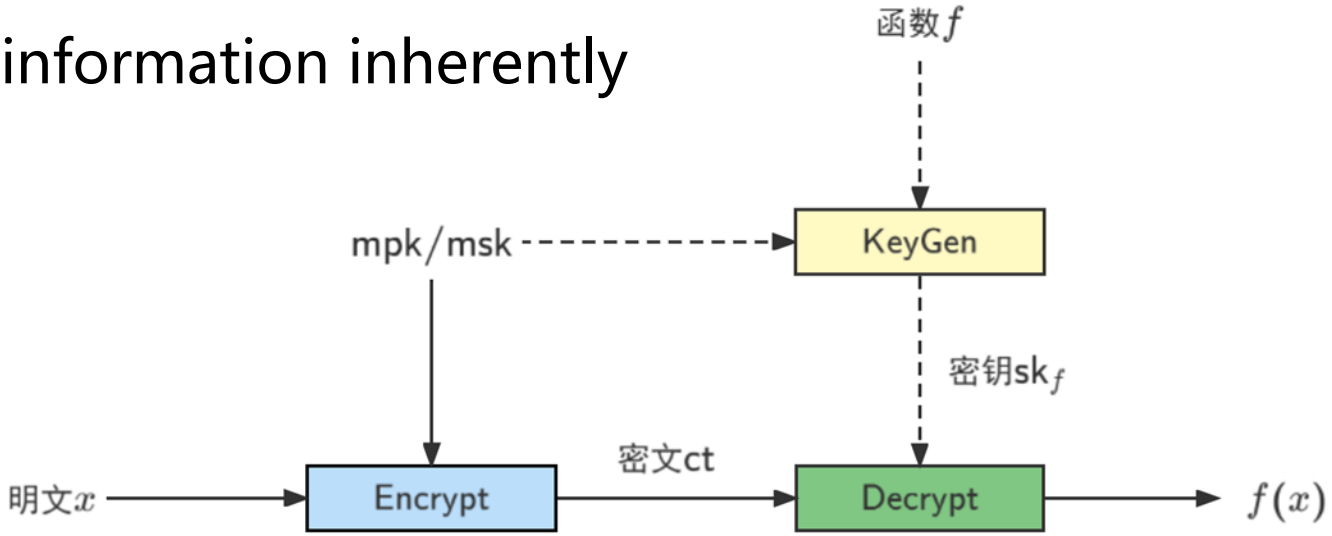
Partially-Hiding Functional Encryption for degree-2 polynomials with Fine-Grained Access Control

Haifeng QIAN, Cheng LIN, Qiaohan CHU, Jie CHEN

Frontiers of Computer Science, DOI: 10.1007/s11704-023-3461-6

- Problem: FE sk_f leak information inherently



- Previous works:

  [ACGU20] inner-product FE with access control (ciphertext-policy)

  [NPP22] FE for Inner Products with access control (dual notion: key-policy)

- Idea: Can we construct FE with access control for more complex function, i.e. quadratic function ???

[ACGU20] Abdalla M, Catalano D, Gay R, Ursu B. Inner-product functional encryption with fine-grained access control. In: ASIACRYPT. 2020, 467–497
[NPP22]Nguyen K, Phan D H, Pointcheval D. Multi-client functional encryption with fine-grained access control. In: ASIACRYP. 2022,95–125

Main Contributions

- Two partially-hiding functional encryption schemes with access control
- Security relies on the reduction from FE for quadratic functions to that for linear functions

Table 1 Comparison of prior PHFE schemes related with our constructions.

Schemes	Functionality	Security	Assumption
[Wee17]	PHFE for linear functions	SA-SIM	MDDH
[Wee20]	PHFE for linear functions	SA-SIM	MDDH
[Wee20]	PHFE for degree-2	SA-SIM	bi-k-Lin
[ACGU20]	IPFE with access control	SEL-SIM	DDH
[NPP22]	IPFE with access control	SEL-IND	SXDH
ours1	PHFE for linear functions with access control	SA-SIM	MDDH
ours2	PHFE for degree-2 with access control	SA-SIM	bi-k-Lin

[1] PHFE stands for partially-hiding FE, IPFE stands for inner-product FE. (SEL, SA, IND, SIM) stands for selective security, semi-adaptive security, indistinguishability-based, simulation-based. SXDH stands for Symmetric eXternal Diffie Hellman, k-Lin is more well-studied than bi-k-Lin because the latter need groups $\mathbb{G}_1, \mathbb{G}_2$ simultaneously.

[Wee17] Wee H. Attribute-hiding predicate encryption in bilinear groups, revisited. In: TCC. 2017, 206–233
[Wee20] Wee H. Functional encryption for quadratic functions from k-lin, revisited. In: TCC. 2020, 210–228