Practical continuous leakage-resilient CCA secure identity-based encryption

Yanwei ZHOU, Bo YANG

Frontiers of Computer Science, DOI: 10.1007/s11704-019-8140-2

Problems & Ideas

- The cryptography construction with bounded leakage resilience may not be able to hold their claimed security in the continuous leakage setting.
  - In the real word, an adversary can make continuous leakage attacks.
  - A cryptography scheme proved in the bounded leakage model cannot keep its original security in the actual application.
- The previous IBE schemes with continuous leakage resilience either only achieve CPA security or obtain selective identity CCA security.
  - The CPA security be proved in the standard model.
  - The CCA security can only be obtained in the selective identity security model.

Main Contributions

- In this paper, we focus on the construction of CCA secure continuous leakage-resilient IBE scheme.
  - We allow continuous leakage of the private key of user. In other words, our proposal can keep its claimed security in the continuous leakage setting.
  - The leakage parameter is independent of the plaintext space and has a constant size. That is, our construction has better leakage resilience, even if the length of encrypted message is long.
  - An adversary cannot obtain any leakage on the private key of user from the corresponding given ciphertext, i.e., all elements in the ciphertext are random in the adversary's view.

Better Performances

Table 1 Comparison of Basic Parameters with Previous Works

	$\mathcal{SK}_{Len}$	C_{Len}	$Assumption$	$SecLev$	$\mathcal{U}_{\lambda}$	$\mathcal{L}_{Model}$
LR-IBE-Li	$2\|G\| + 2\|p\|$	$3\|G\| + l_m + l_t$	q-ABDHE	CCA	$\log p - l_m - \omega(\log \kappa)$	BLM
LR-IBE-Sun	$3\|G\| + 3\|p\|$	$4\|G\| + \|p\|$	q-ABDHE	CCA	$\log p - \omega(\log k)$	BLM
CLR-IBE-Zhou	$4\|G\|$	$2\|G\| + 2\|G_T\| + \|p\|$	DBDH	CCA	$2\log p - \omega(\log \kappa)$	CLM
Our Scheme Π_{New}	$2\|G\| + 2\|p\|$	$2\|G\| + 4\|G_T\| + \|p\|$	q-ABDHE	CCA	$3\log p - \omega(\log \kappa)$	CLM

(1) Let l_t be the length of randomness seed, l_m the length of message and $|p|$ the length of element in $\mathbb{Z}_p^*$. Let $|G|$, $|G_T|$ be the length of element in the group G and G_T, respectively.
(2) Let BLM be the bounded leakage model, and CLM the continuous leakage model.

Table 2 Comparison of Computation Efficiency with Previous Works

	KeyGen	Enc	Dec
LR-IBE-Li	$4E_s$	$1E_s + 2E_d + 1E_e + 1E_{Ext}$	$2E_d + 2E_e + 1E_{Ext}$
LR-IBE-Sun	$6E_s$	$1E_s + 3E_d + 3E_e$	$2E_s + 2E_d + 2E_e$
CLR-IBE-Zhou	$2E_s + 2E_s$	$2E_s + 2E_d$	$2E_d + 4E_e$
Our Scheme Π_{New}	$2E_d$	$4E_s + 2E_d$	$3E_s + 3E_d + 2E_e$

Let E_{Ext} be the cost of the randomness extractor operation, E_s the cost of sigle exponentiation operation, E_d the cost of double exponentiation operation and E_e the cost of the pairing operation.