Keyword Search on Encrypted Data

RUI ZHANG

Motivation

Secure Integration of Public Key Encryption with Keyword Search (PEKS) and Public Key Encryption (PKE)

Results

❖ A formal model of PEKS/PKE

❖ A simple, generic construction of PEKS/PKE based on tag-KEM/DEM

❖ Some interesting applications/extensions

Integration of PEKS and PKE

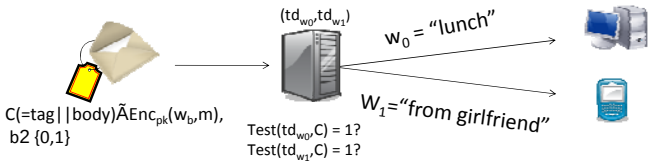
❖ Ciphertexts are produced with specific keywords

❖ Example

o Routing on encrypted emails

➢Encrypted Email = tag || encrypted mail body

➢A mail gateway (with trapdoor td_w produced by the Receiver) can test whether "tag" contains information of w



Security of the Integrated System

➢ PEKS + PKE

➔Individually secure components may NOT result in a secure system!

➔E.g.: Data privacy may not hold if chosen ciphertext attack is considered. (Pointed out by [BSS06])

➢ Security Notions

✓ Data privacy

• Semantic security against adaptive chosen ciphertext and chosen keyword attack

✓Keyword Privacy

• Indistinguishability against adaptive chosen ciphertext and chosen keyword attack

The Proposed Scheme

$\mathsf{Kg}(1^k)$ $(pk_1, sk_1) \leftarrow \mathsf{PEKSkg}(1^k)$; $(pk_2, sk_2) \leftarrow \mathsf{TKkg}(1^k)$; $pk = (pk_1, pk_2)$; $sk = (sk_1, sk_2)$; return (pk, sk);	$\mathsf{Dec}(sk, c)$ $sk = (sk_1, sk_2)$; $c = (\tau, \psi, \chi)$; $dk \leftarrow \mathsf{TKdec}(sk_2, \psi, \tau\|\chi)$; $m \leftarrow \mathsf{DEMdec}(dk, \chi)$; return m;
$\mathsf{Enc}(pk, w, m)$ $pk = (pk_1, pk_2)$; $\tau \leftarrow \mathsf{PEKSenc}(pk_1, w)$; $(dk, \eta) \leftarrow \mathsf{TKkey}(pk_2)$; $\chi \leftarrow \mathsf{DEMenc}(dk, m)$; $\lambda \leftarrow (\tau\|\chi)$; $\psi \leftarrow \mathsf{TKenc}(\eta, \lambda)$; $c \leftarrow (\tau, \psi, \chi)$; return c;	$\mathsf{Td}(sk, w)$ $sk = (sk_1, sk_2)$; $t_w \leftarrow \mathsf{PEKStd}(sk_1, w)$; return t_w; $\mathsf{Test}(t_w, c)$ $c = (\tau, \psi, \chi)$; $b \leftarrow \mathsf{PEKStest}(t_w, \tau)$; return b;

For each algorithm of PEKS/PKE, we require it should terminate and return "⊥" (denoting "abnormal termination"), if any of its sub-algorithms terminates abnormally.

Fig. 1. Generic Construction of PEKS/PKE

Construction Idea:

❖Anonymous IBE + tag-KEM/DEM
❖Well understood and standard components)

Applications and Extensions:

✓ Efficient Instantiation with Gentry-PEKS and KD-PKE

✓ Threshold decryption

✓ Hierarchical Keywords