

Searchable Encryption

陳榮傑

交通大學資工系

Cryptanalysis Lab

2012/03/29

Searchable Encryption

kw : keyword



Alice

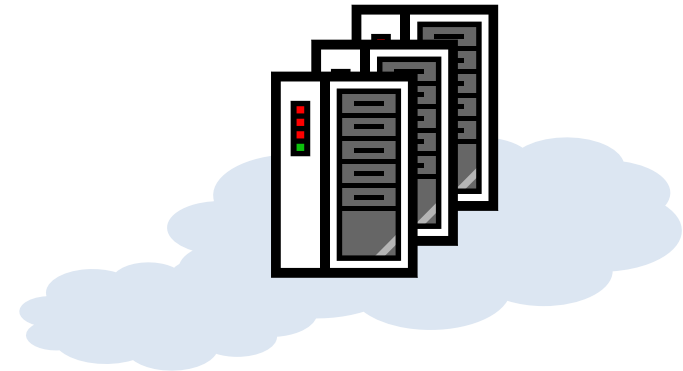
Encrypt:

- Encrypted data
- $PEKS(kw)s$



Search kw:

- $Trapdoor(kw')$

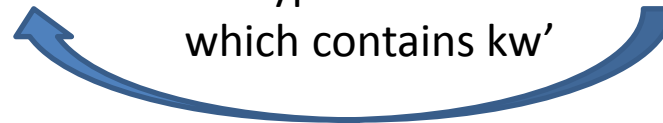


Test:

for each file
tests PEKS
(using pairing-based
cryptography)

Reply:

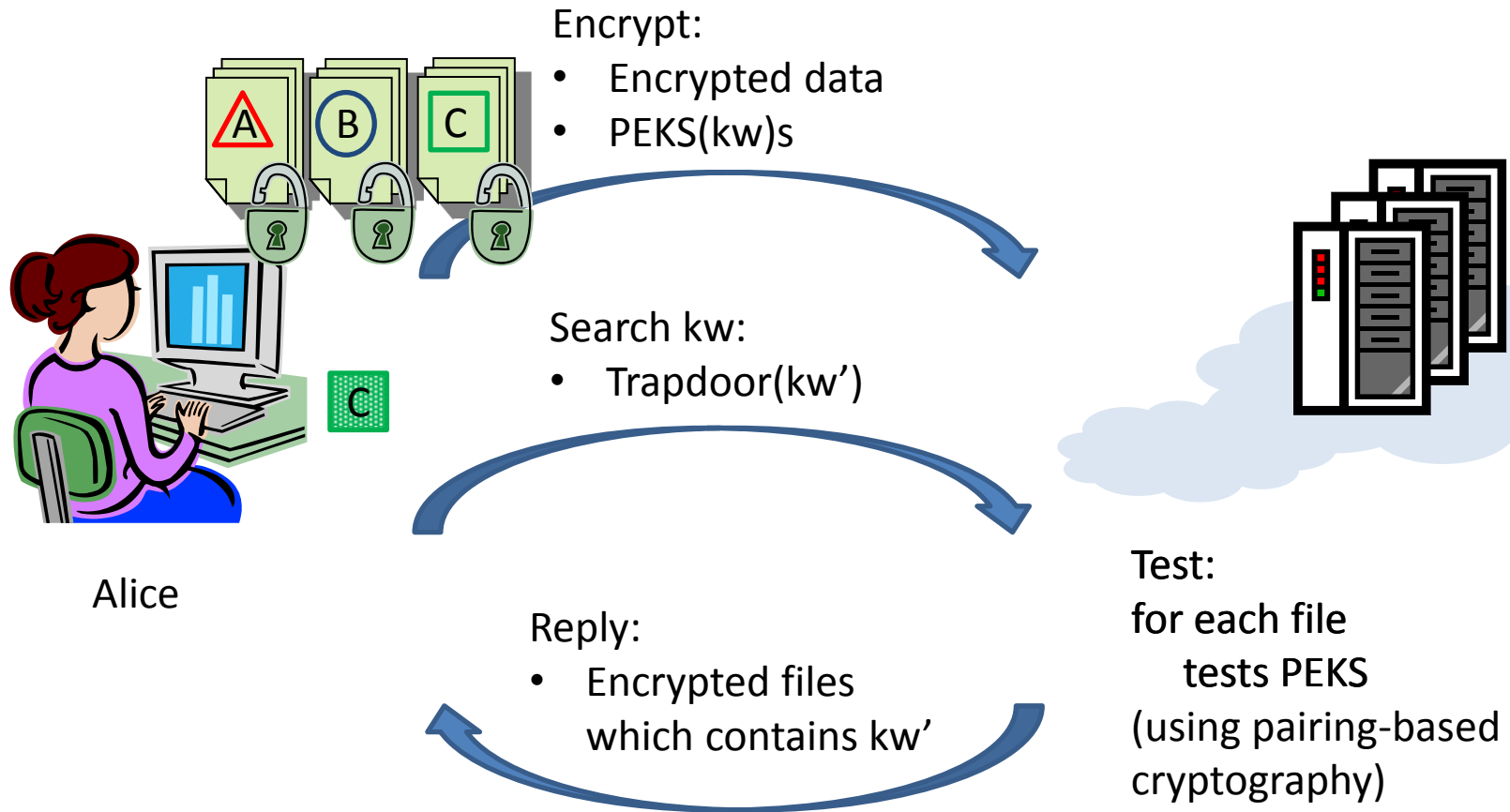
- Encrypted files
which contains kw'



Server gains no knowledge about kw or the file content stored on the Cloud Storage

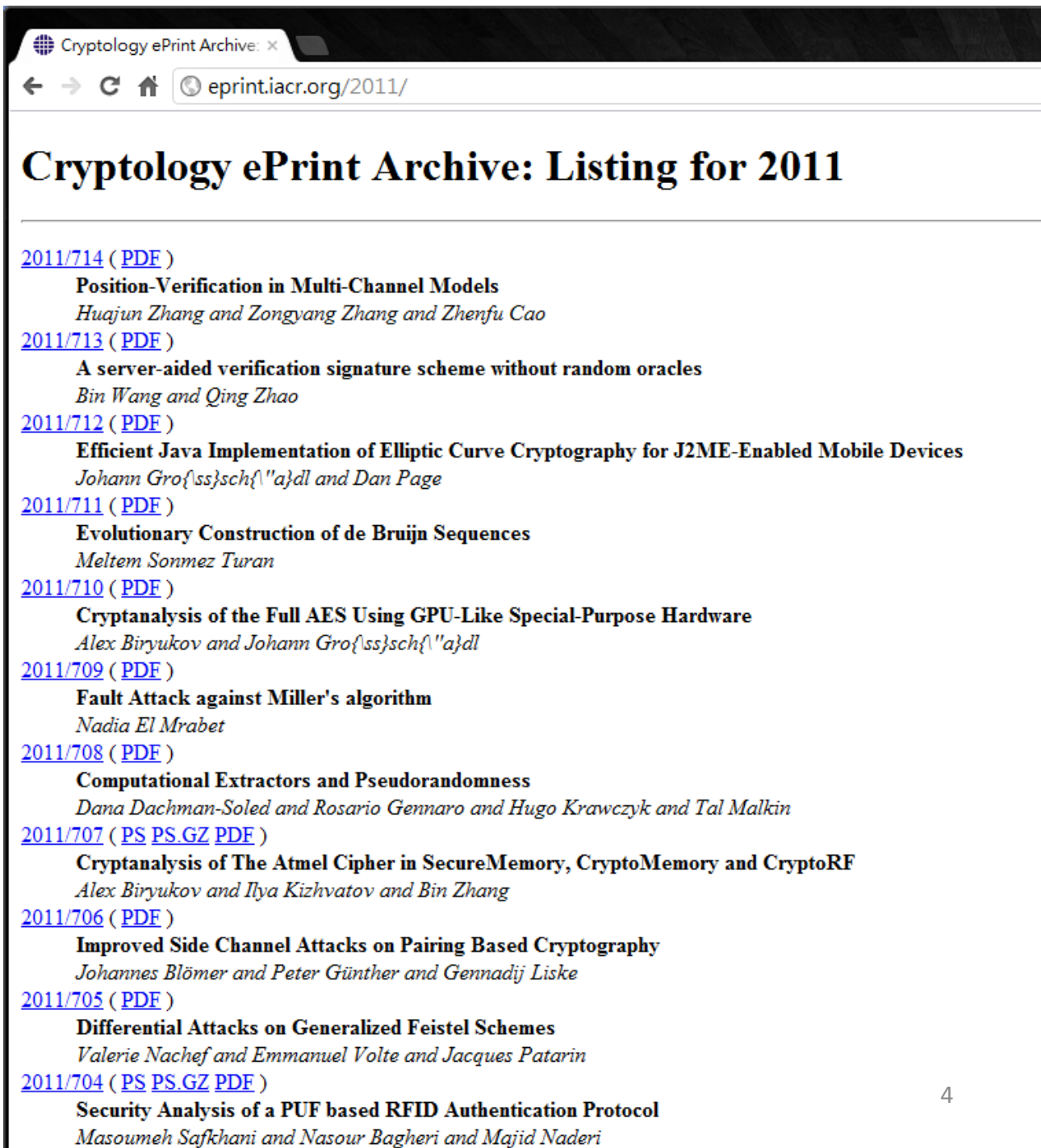
Searchable Encryption

kw : keyword



Server gains no knowledge about kw or the file content stored on the Cloud Storage

Data Example



Cryptology ePrint Archive: x
← → ↻ 🏠 eprint.iacr.org/2011/

Cryptology ePrint Archive: Listing for 2011

[2011/714 \(PDF \)](#)
Position-Verification in Multi-Channel Models
Huajun Zhang and Zongyang Zhang and Zhenfu Cao

[2011/713 \(PDF \)](#)
A server-aided verification signature scheme without random oracles
Bin Wang and Qing Zhao

[2011/712 \(PDF \)](#)
Efficient Java Implementation of Elliptic Curve Cryptography for J2ME-Enabled Mobile Devices
Johann Gro{\ss}schl and Dan Page

[2011/711 \(PDF \)](#)
Evolutionary Construction of de Bruijn Sequences
Meltem Sonmez Turan

[2011/710 \(PDF \)](#)
Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware
Alex Biryukov and Johann Gro{\ss}schl

[2011/709 \(PDF \)](#)
Fault Attack against Miller's algorithm
Nadia El Mrabet

[2011/708 \(PDF \)](#)
Computational Extractors and Pseudorandomness
Dana Dachman-Soled and Rosario Gennaro and Hugo Krawczyk and Tal Malkin

[2011/707 \(PS PS.GZ PDF \)](#)
Cryptanalysis of The Atmel Cipher in SecureMemory, CryptoMemory and CryptoRF
Alex Biryukov and Ilya Kizhvatov and Bin Zhang

[2011/706 \(PDF \)](#)
Improved Side Channel Attacks on Pairing Based Cryptography
Johannes Blömer and Peter Günther and Gennadij Liske

[2011/705 \(PDF \)](#)
Differential Attacks on Generalized Feistel Schemes
Valerie Nachev and Emmanuel Volte and Jacques Patarin

[2011/704 \(PS PS.GZ PDF \)](#)
Security Analysis of a PUF based RFID Authentication Protocol
Masoumeh Safkhani and Nasour Bagheri and Majid Naderi

Data Example

Cryptology ePrint Archive: x
eprint.iacr.org/2011/311

Cryptology ePrint Archive: Report 2011/311

Targeted Malleability: Homomorphic Encryption for Restricted Computations

Dan Boneh and Gil Segev and Brent Waters

Abstract: We put forward the notion of targeted malleability: given a homomorphic encryption scheme, in various computations one can perform on encrypted data. We introduce a precise framework, generalizing the foundation of Naor (SICOMP '00), ensuring that the malleability of a scheme is targeted only at a specific set of "allowable" functions.

In this setting we are mainly interested in the efficiency of such schemes as a function of the number of repeated homomorphic operations. If the number of ciphertexts grows linearly with the number of such operations is straightforward, obtaining more realistic (or merely) efficiency guarantees.

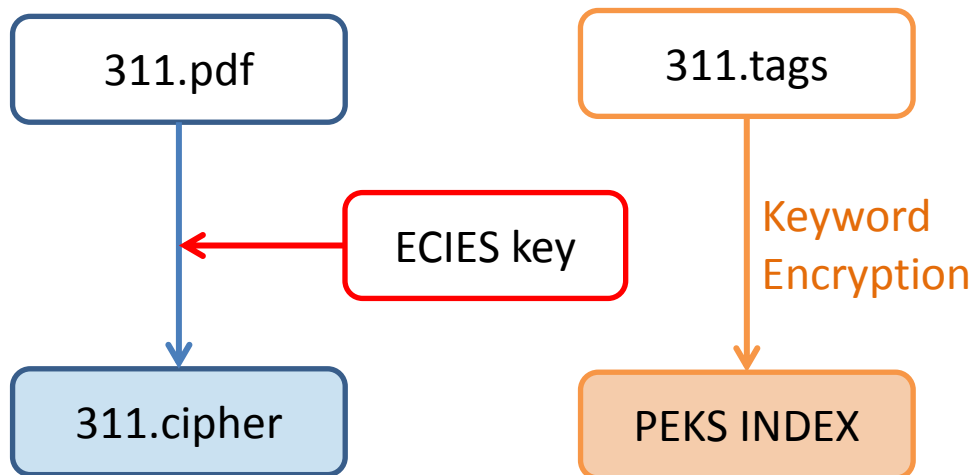
We present two constructions that transform any homomorphic encryption scheme into one that offers targeted malleability and on succinct non-interactive arguments, which are currently known to exist in the standard model based on various assumptions. These constructions offer somewhat different efficiency guarantees, each of which may be preferable depending on the use case.

Category: Foundations / **Keywords:** foundations / Homomorphic encryption, non-malleable encryption

```
1 id: 311
2 title: Targeted Malleability: Homomorphic Encryption for Restricted Computations
3 author: Dan Boneh
4 author: Gil Segev
5 author: Brent Waters
6 keyword: foundations
7 keyword: Homomorphic encryption
8 keyword: non-malleable encryption
9
```

Keyword Lists (311.tags)

Public Key Encryption with Keyword Search (PEKS) (1/3)



311.pdf

Targeted Malleability:
Homomorphic Encryption for Restricted Computations

Dan Boneh* Gil Segev[†] Brent Waters[‡]

Abstract

We put forward the notion of *targeted malleability*: given a homomorphic encryption scheme, in various scenarios we would like to restrict the homomorphic computations one can perform on encrypted data. We introduce a precise framework, generalizing the foundational notion of *non-malleability* introduced by Dolev, Dwork, and Naor (SICOMP '00), ensuring that the malleability of a scheme is targeted only at a specific set of “allowable” functions.

In this setting we are mainly interested in the efficiency of such schemes as a function of the number of repeated homomorphic operations. Whereas constructing a scheme whose ciphertext grows linearly with the number of such operations is straightforward, obtaining more realistic (or merely non-trivial) length guarantees is significantly more challenging.

We present two constructions that transform any homomorphic encryption scheme into one that offers targeted malleability. Our constructions rely on standard cryptographic tools and on succinct non-interactive arguments, which are currently known to exist in the standard model based on variants of the knowledge-of-exponent assumption. The two constructions offer somewhat different efficiency guarantees, each of which may be preferable depending on the underlying building blocks.

Keywords: Homomorphic encryption, Non-malleable encryption.

*Stanford University. Supported by NSF, DARPA, and AFOSR.

[†]Microsoft Research, Mountain View, CA 94043, USA.

[‡]University of Texas at Austin. Supported by NSF CNS-0716199, CNS-0915361, and CNS-0952692, DARPA PROCEED, Air Force Office of Scientific Research (AFO SR) MURI, DHS Grant 2006-CS-001-000001-02, and the Sloan Foundation.

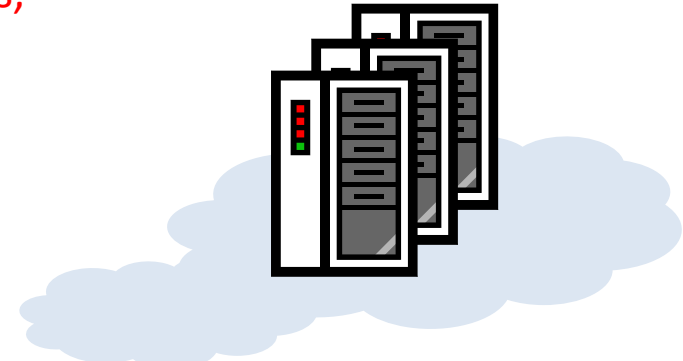
Search Keyword

Search kw:

- Trapdoor(author: Brent Waters, Alice's private key)



Alice



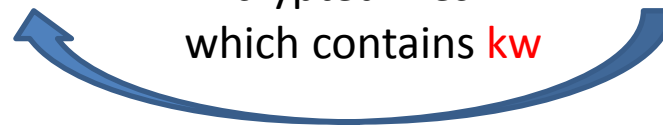
Test:

for each file
tests PEKS in

PEKS INDEX

Reply:

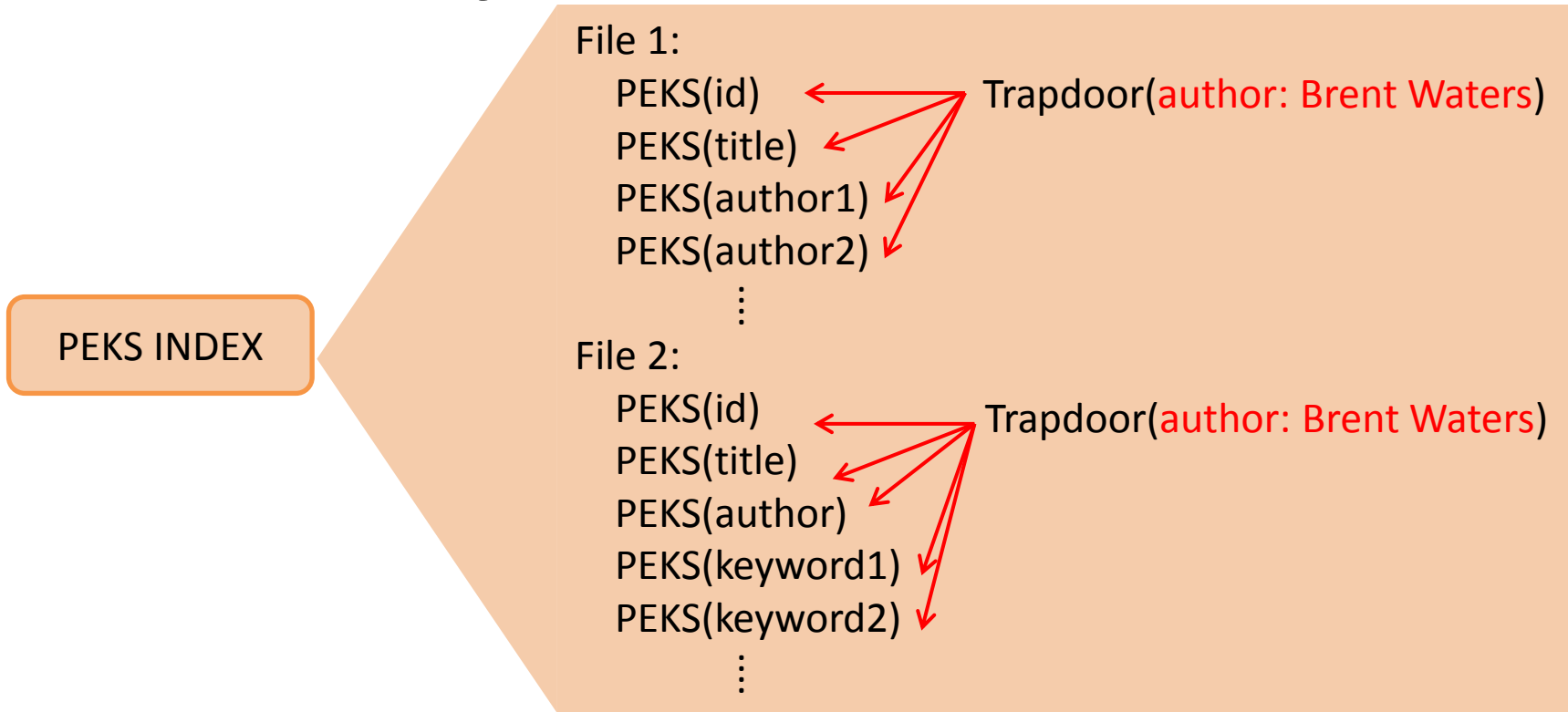
- Encrypted files which contains kw



311.aes128

311.rsa

Search Keyword



$$PEKS = (g^r, H_2(t)), \quad t = e(H_1(KW), h^r), \quad h = g^\alpha$$

$$Trapdoor = H_1(KW)^\alpha$$

Server tests each PEKS whether $H_2(e(H_1(KW)^\alpha, g^r)) = H_2(t)$

Implementation

- PBC Library by [Ben Lynn](#)
- Tate Pairing
- supersingular curve: $y^2 = x^3 + x$ over F_q
 - embedding degree $k = 2$
 - q is a prime and $q \equiv 3 \pmod{4}$
 - q is 1536-bit long
 - group order r is 256-bit long

- Key Length:

NIST Recommendations (2011)							NIST	
Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Elliptique Group	Curve	Hash (A)	Hash (B)
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512

Forthcoming Research

To enhance search capability

Query Type

Equality query: $(x_i = a)$ for any $a \in T$

Comparison query: $(x_i \geq a)$ for any $a \in T$

Subset query: $(x_i \in A)$ for any $A \subseteq T$

Equality conjunction: $(x_1 = a_1) \wedge \dots \wedge (x_w = a_w)$

Comparison conjunction: $(x_1 \geq a_1) \wedge \dots \wedge (x_w \geq a_w)$

Subset conjunction: $(x_1 \in A_1) \wedge \dots \wedge (x_w \in A_w)$

Demo PEKS library

MainWindow

Seachable Encryption demo - PEKS

Command

KeyGen

Encrypt data file :

Encrypt All kw file :

Search keyword :

Decrypt file :

Search Result

Name	Size	Type	D
49.pdf.aes128	400 KB	aes128 File	3/
49.pdf.rsa	256 bytes	rsa File	3/
96.pdf.aes128	369 KB	aes128 File	3/
96.pdf.rsa	256 bytes	rsa File	3/
311.pdf.aes128	283 KB	aes128 File	3/
311.pdf.rsa	256 bytes	rsa File	3/
352.pdf.aes128	441 KB	aes128 File	3/
352.pdf.rsa	256 bytes	rsa File	3/
369.pdf.aes128	1.1 MB	aes128 File	3/
369.pdf.rsa	256 bytes	rsa File	3/
479.pdf.aes128	400 KB	aes128 File	3/
479.pdf.rsa	256 bytes	rsa File	3/
581.pdf.aes128	338 KB	aes128 File	3/
581.pdf.rsa	256 bytes	rsa File	3/
INDEX	103 bytes	File	3/

Name	Size	Type
[-] eprint_tags		Folder
[-] eprint2011		Folder
[-] peks_encrypted		Folder
[-] peks_keys		Folder
[-] rsa_keys		Folder
[-] search_result		Folder
demoPEKS	75 KB	File
demoPEKS.py	12 KB	py File
demoPEKS.pyc	8 KB	pyc File
demoPEKS.ui	9 KB	ui File
Makefile	442 bytes	File
start.py	7 KB	py File

```
1 311.pdf.aes128
2 352.pdf.aes128
3 369.pdf.aes128
4 479.pdf.aes128
5 49.pdf.aes128
6 581.pdf.aes128
7 96.pdf.aes128
8
```

11

- Questions?

- Thank you