DYNAMIC SEARCHABLE SYMMETRIC ENCRYPTION

Arpan Kapoor

October 20, 2015

National Institute of Technology, Calicut

OUTLINE

1. Introduction
2. Definitions
3. The SSE-1 scheme
4. Making SSE-1 dynamic
5. Example
6. Conclusion

INTRODUCTION

- SSE allows client to encrypt data such that it can still be searched.
- Application: Cloud storage.

DEFINITIONS

Symmetric Key Encryption

- Same key for encryption and decryption.

  $c = E_K(m) \qquad\qquad m = D_K(c)$

Homomorphic Encryption

- Permit computations on encrypted data.
- Obtaining $E_K(f(x))$ from $E(x)$.

Psuedorandom Function

- Polynomial time function whose output is indistinguishable from a random function.

$$F\colon \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^m$$

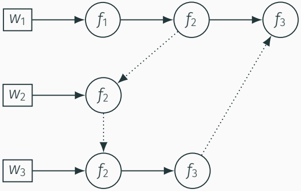
- Given F, K, $x_1, \dots, x_a$ and $F_K(x_1), \dots, F_K(x_a)$, $F_K(x_{a+1})$ can't be predicted for any x_{a+1}.

SSE-1 SCHEME

MAKING SSE-1 SCHEME

EXAMPLE

Index



Search Table T_s

$F_{K_1}(w_1) \rightarrow 4$

$F_{K_1}(w_2) \rightarrow 0$

$F_{K_1}(w_3) \rightarrow 5$

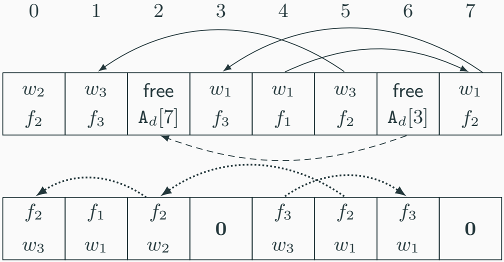
free → 6

Deletion Table T_d

$F_{K_1}(f_1) \rightarrow 1$

$F_{K_1}(f_2) \rightarrow 5$

$F_{K_1}(f_3) \rightarrow 4$



0	1	2	3	4	5	6	7
w_2 f_2	w_3 f_3	free $\mathtt{A}_d[7]$	w_1 f_3	w_1 f_1	w_3 f_2	free $\mathtt{A}_d[3]$	w_1 f_2

Search Array $\mathtt{A}_s$

f_2 w_3	f_1 w_1	f_2 w_2	**0**	f_3 w_3	f_2 w_1	f_3 w_1	**0**

Deletion Array $\mathtt{A}_d$

Questions?

REFERENCES I

[1] C. Bösch, P. Hartel, W. Jonker, and A. Peter.
A survey of provably secure searchable encryption.
ACM Computing Surveys (CSUR), 47(2):18, 2014.

[2] S. Kamara, C. Papamanthou, and T. Roeder.
Dynamic searchable symmetric encryption.
In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 965–976. ACM, 2012.