# What is Leaked is Invisible to the Eye

## Strong Forward Privacy for Dynamic Searchable Encryption


**Yohei Watanabe** [1] Kazuma Ohara [2,3]

Mitsugu Iwamoto [3] Kazuo Ohta [3]

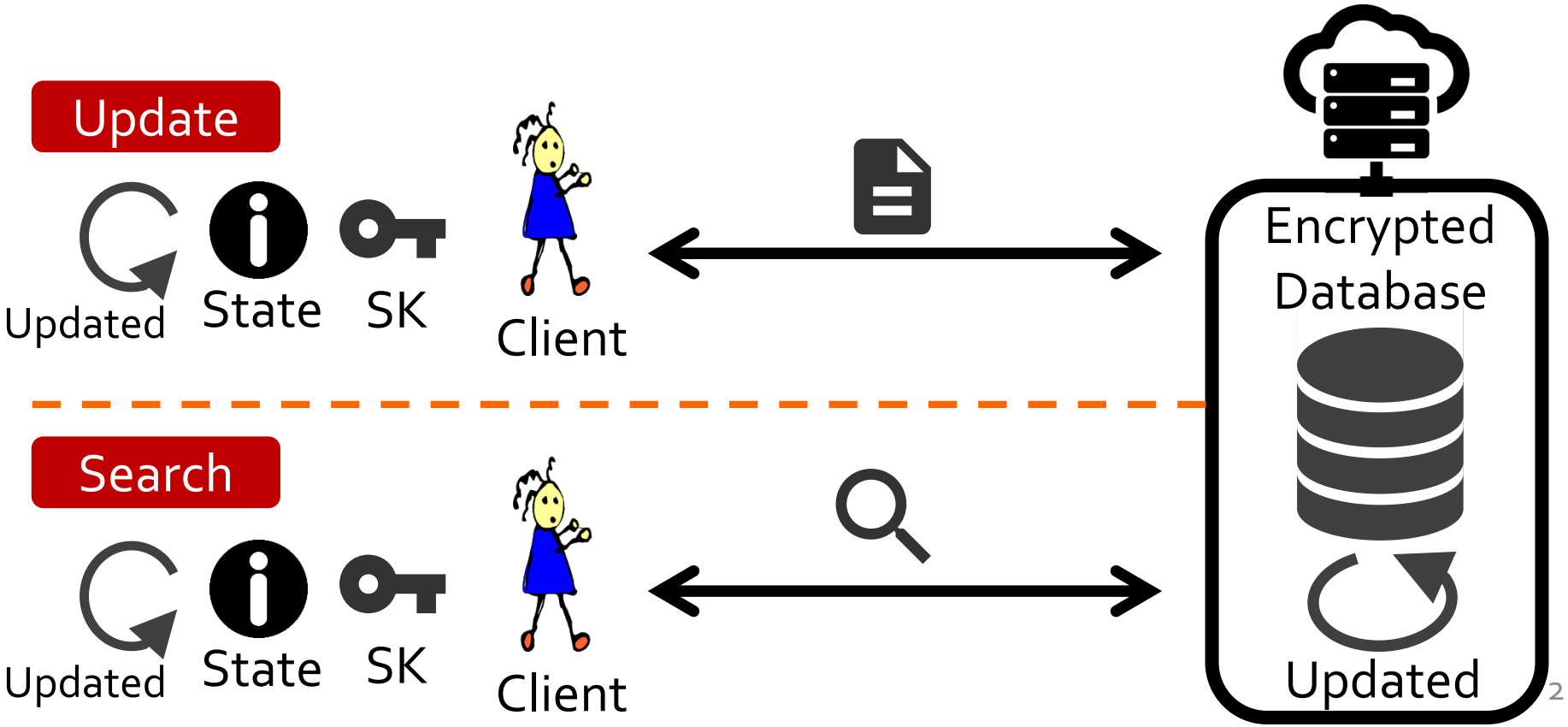
1: NICT, Japan

2: NEC, Japan

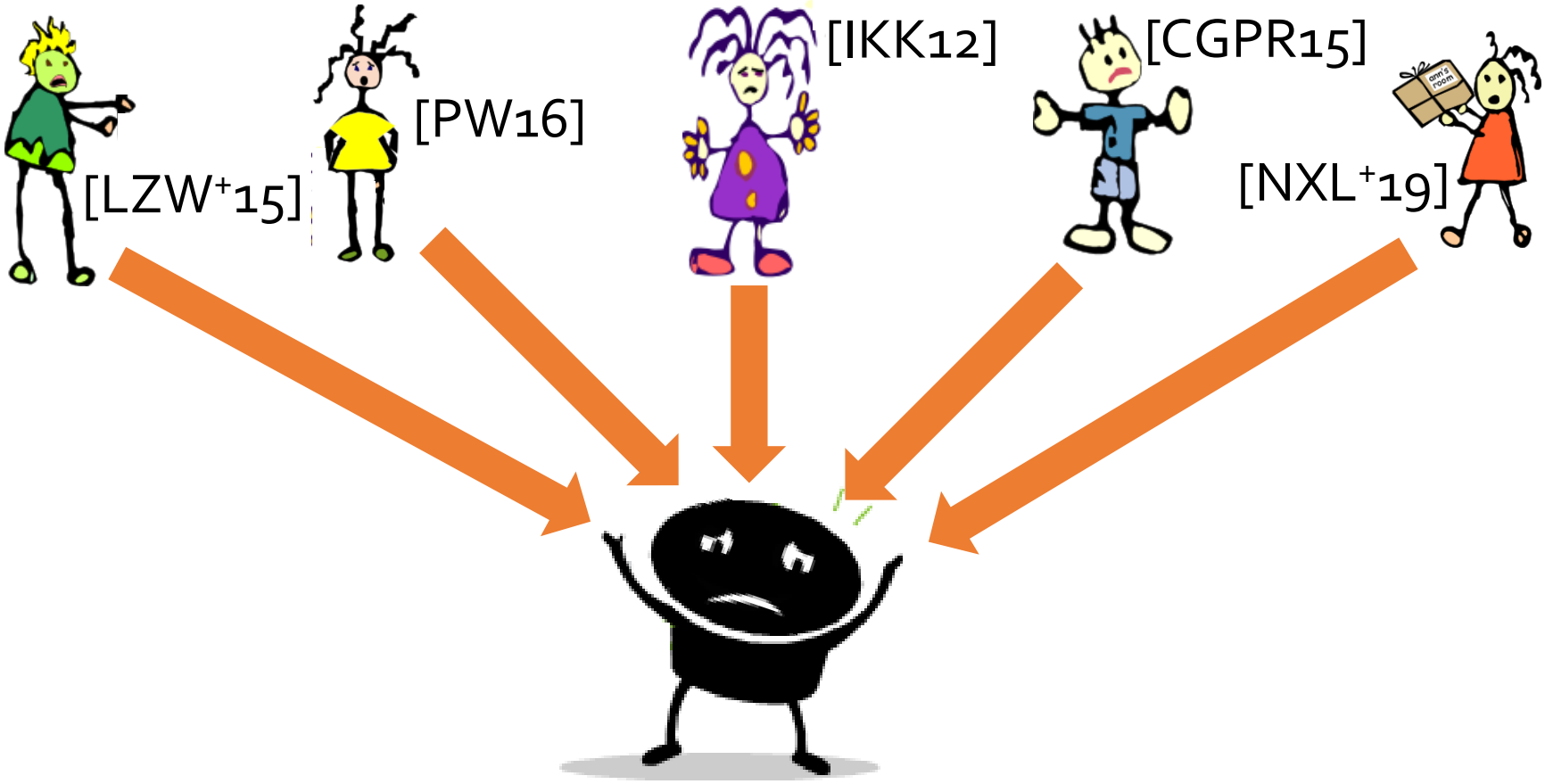
3: The University of Electro-Communications (UEC), Japan

# Dynamic Searchable Symmetric Encryption
[KPR, CCS'12]

- Allows dynamic addition/deletion of document files
- Provides efficient searches encrypted data
- Reveals "inconsequential" information during each operation



# Attacks Using Leakage during Search



# Attacks Using Leakage during Search


Dynamic SSE

# Attacks Using Leakage during Search

[LZW+15]

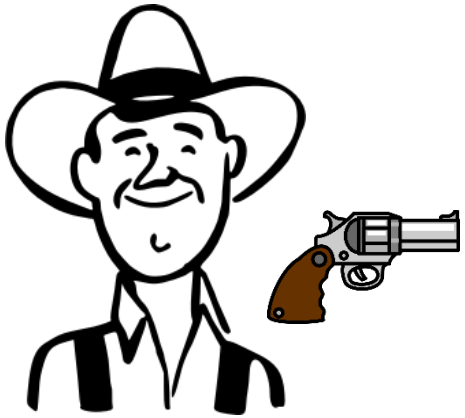
[PW16]

[IKK12]

[CGPR15]


[NXL+19]

Unrealistic Assumptions



File Injection Attack
[ZKP16]

Dynamic SSE

# Attacks Using Leakage during Search

[LZW+15]

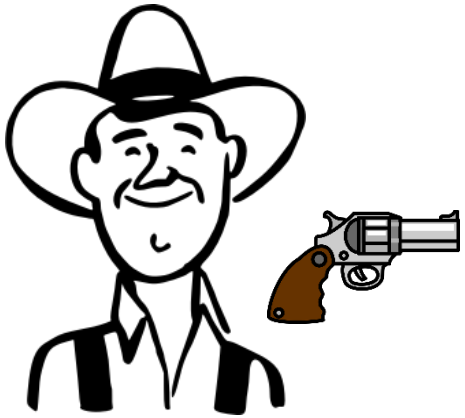
[PW16]

[IKK12]

[CGPR15]


[NXL+19]

Unrealistic Assumptions



File Injection Attack
[ZKP16]

Dynamic SSE

# Attacks Using Leakage during Search

[LZW+15]

[PW16]

[IKK12]

[CGPR15]

[NXL+19]

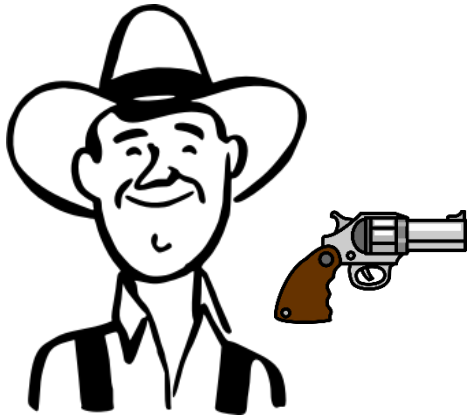
Unrealistic Assumptions

File Injection Attack
[ZKP16]

Dynamic SSE

# Attacks Using Leakage during Search


Unrealistic Assumptions



File Injection Attack
[ZKP16]

Dynamic SSE

# Attacks Using Leakage during Search

[LZW+15]

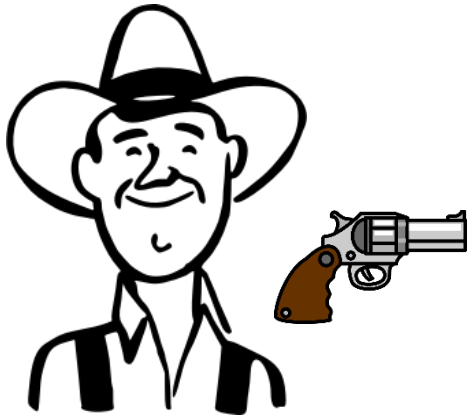
[PW16]

[IKK12]

[CGPR15]


[NXL+19]

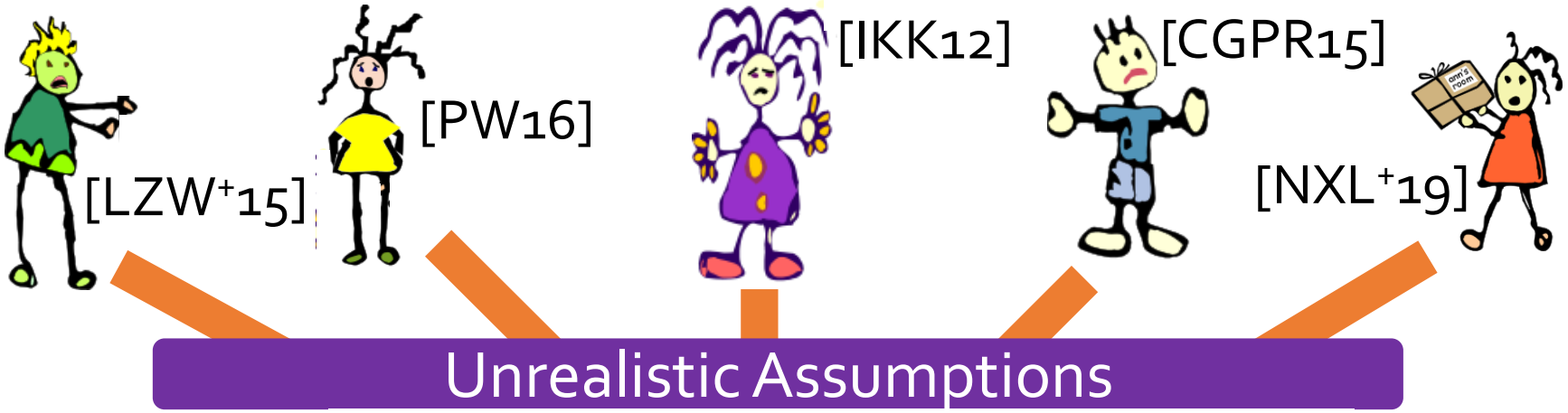
Unrealistic Assumptions

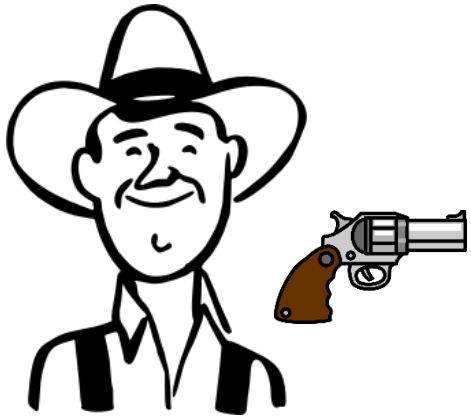


File Injection Attack
[ZKP16]

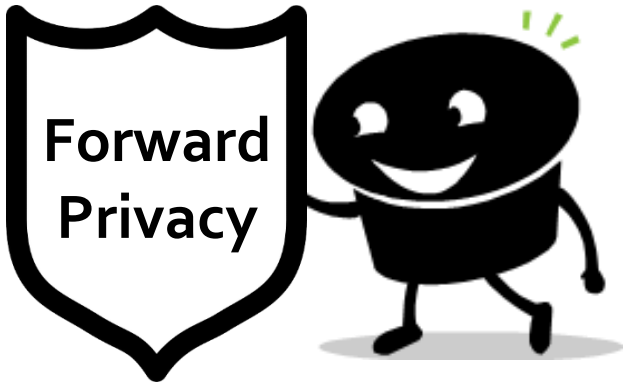
Dynamic SSE

# Attacks Using Leakage during Search



File Injection Attack
[ZKP16]

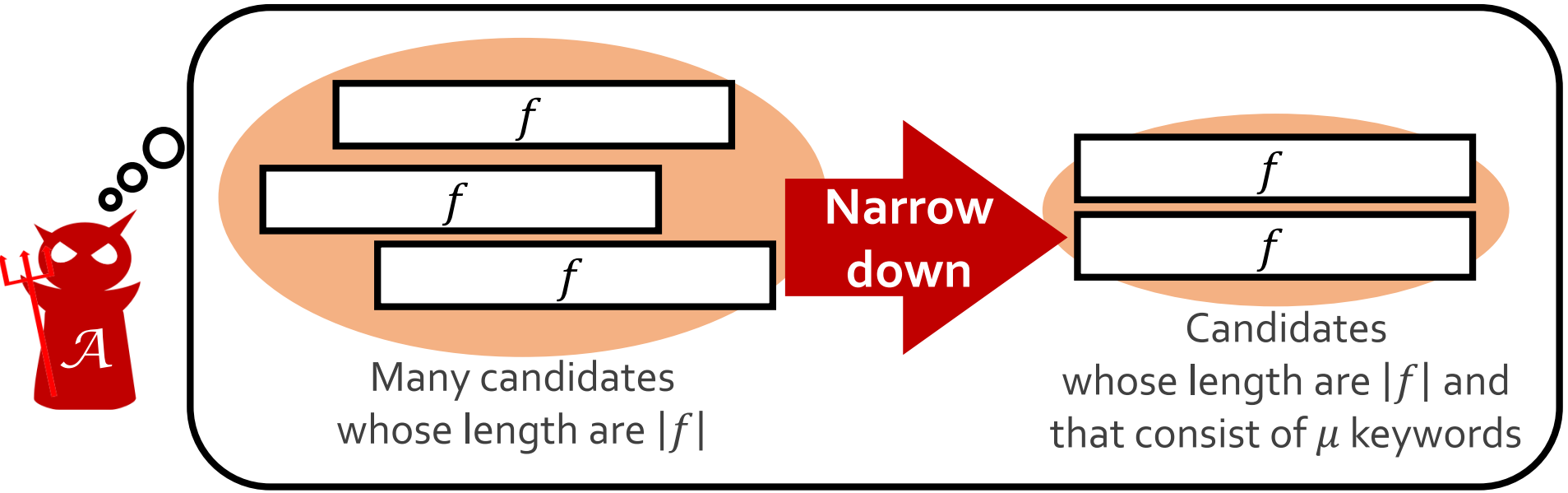



Dynamic SSE

# Our Focus: How about Leakage during Update?

- All existing dynamic SSE schemes (even with FP) leak
  - Identifier of file $f$
  - File length $|f|$
  - **The number of distinct keywords $\mu$ in $f$**

during add operations

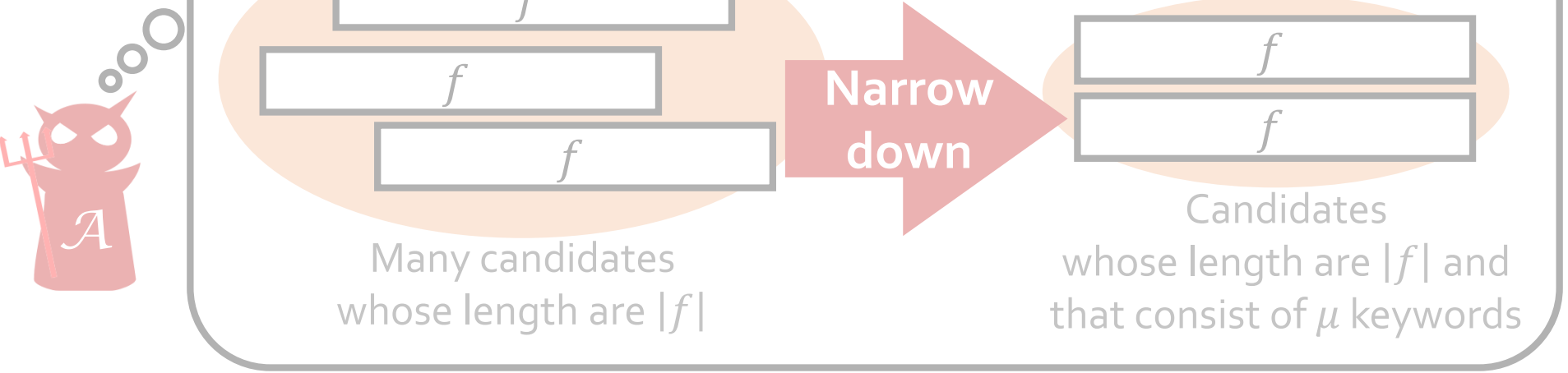


# Our Focus: How about Leakage during Update?

- All existing dynamic SSE schemes (even with FP) leak
  - Identifier of file $f$
  - File length $|f|$
  - **The number of distinct keywords $\mu$ in $f$**

during add operati

**Question: Is this leakage insignificant in practice?**



# Motivating Example: STR Analysis (by FBI)

- Suppose dynamic SSE over DNA database
- We focus on *short tandem repeat* (STR)
  - Repeating DNA sequences used for:
    - Parent DNA Test
    - Identification of missing persons and suspects
  - The number of STRs varies according to an individual
- FBI employs STR analysis in Combined DNA Index System

Small number of distinct keywords

➡ Same sequences or patterns in DNA ?

# Our Work: Strong Forward Privacy

- Dynamic SSE satisfies **strong forward privacy** if it leaks
  - Identifier of file $f$
  - File length $|f|$
  - ~~**The number of distinct keywords $\mu$ in $f$**~~

  during add operations
- Propose **two strongly forward-private constructions**:
  1. **Achieves no state info.** but search is less efficient
     - Based on Curtmola et al.'s scheme [CGKO, CCS'06]
  2. **Provides efficient search and update**
     - Based on Etemad et al.'s scheme [EKPE, PoPETs'18]

# Strong Forward Privacy Seems to Be Needed

[LZW+15]

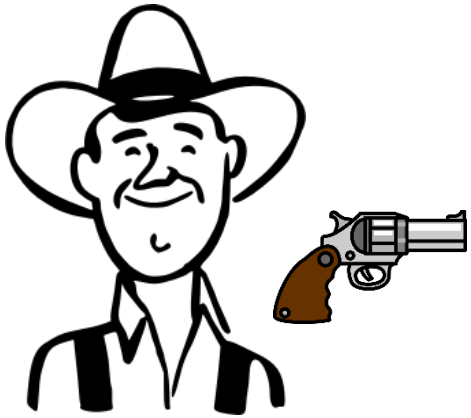
[PW16]

[IKK12]

[CGPR15]

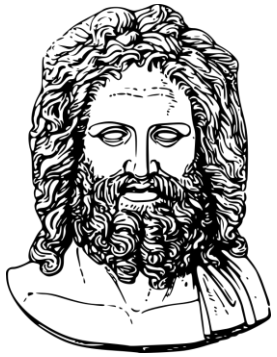

[NXL+19]

Unrealistic Assumptions



File Injection Attack
[ZKP16]


Dynamic SSE



New Threat

**Thank you! ☺**