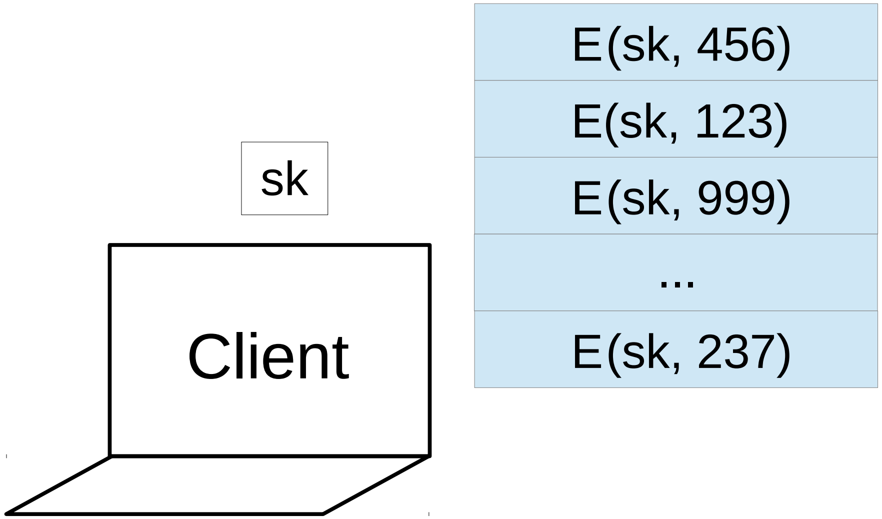
Semantically Secure Order-Revealing Encryption:

Multi-Input Functional Encryption Without Obfuscation

Dan Boneh, Kevin Lewi, Mariana Raykova,
Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption



E(sk, 456)

E(sk, 123)

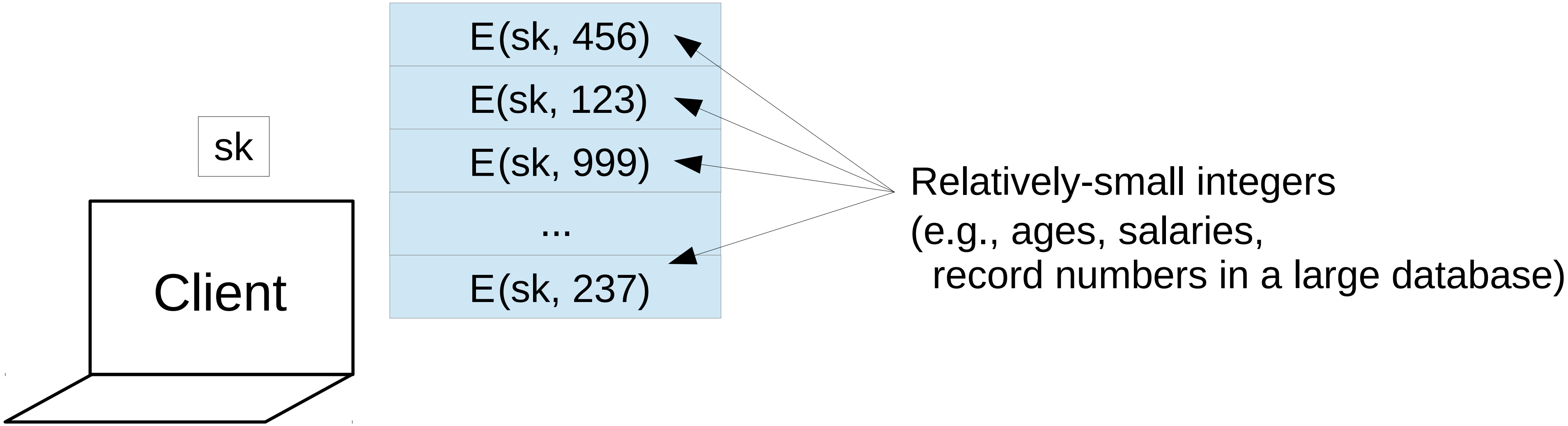
E(sk, 999)

...

E(sk, 237)

Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption



sk

Client

E(sk, 456)

E(sk, 123)

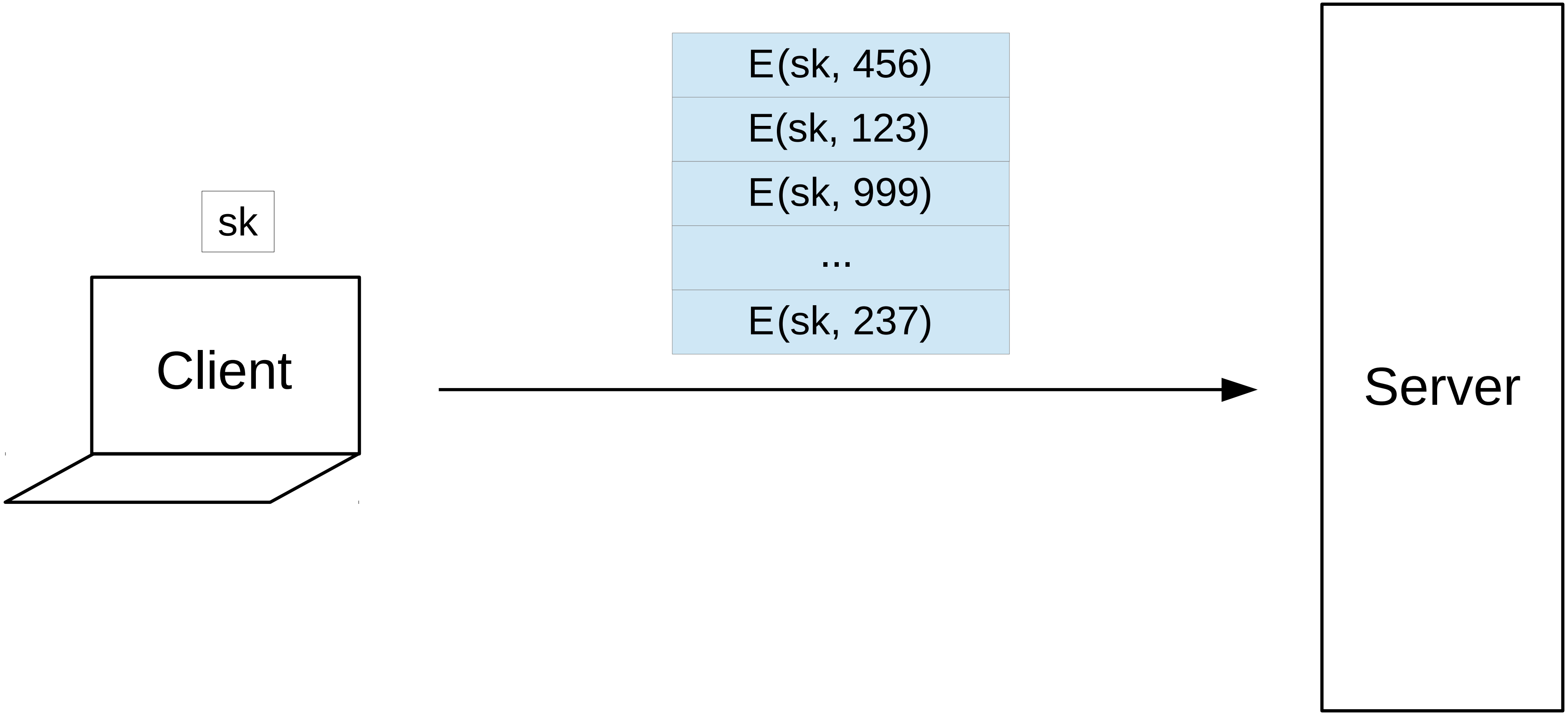
E(sk, 999)

...

E(sk, 237)

Relatively-small integers
(e.g., ages, salaries,
record numbers in a large database)

Order-Revealing Encryption



sk

Client

E(sk, 456)

E(sk, 123)

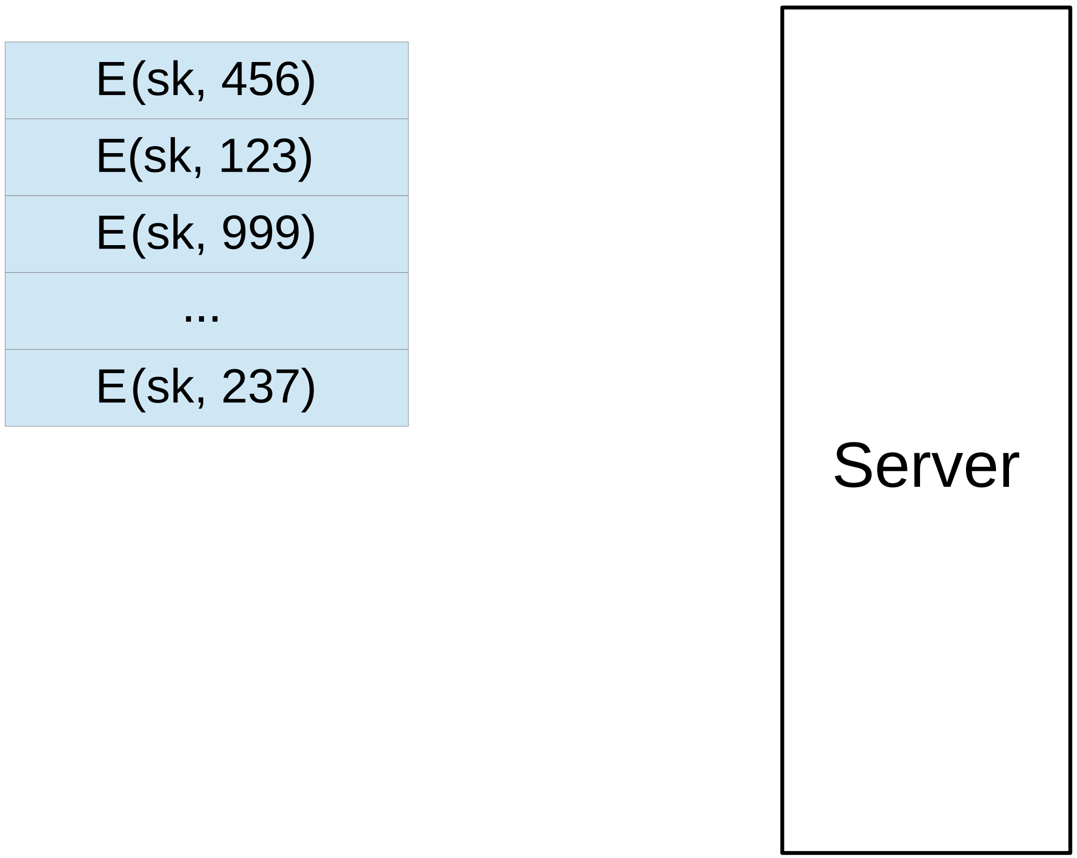
E(sk, 999)

...

E(sk, 237)

Server

Order-Revealing Encryption



E(sk, 456)

E(sk, 123)

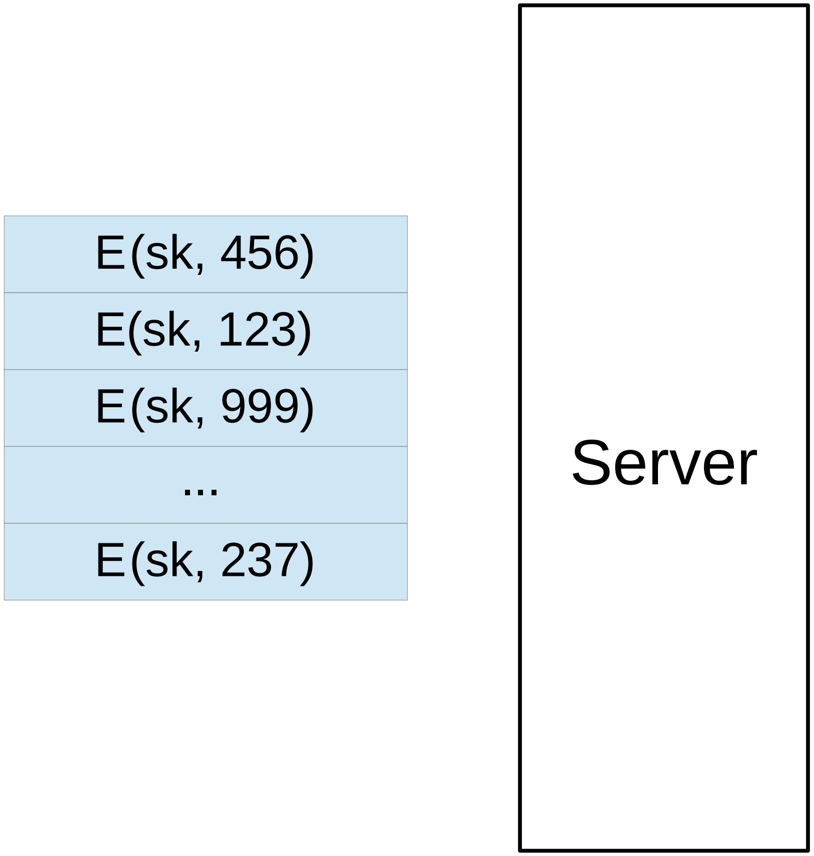
E(sk, 999)

...

E(sk, 237)

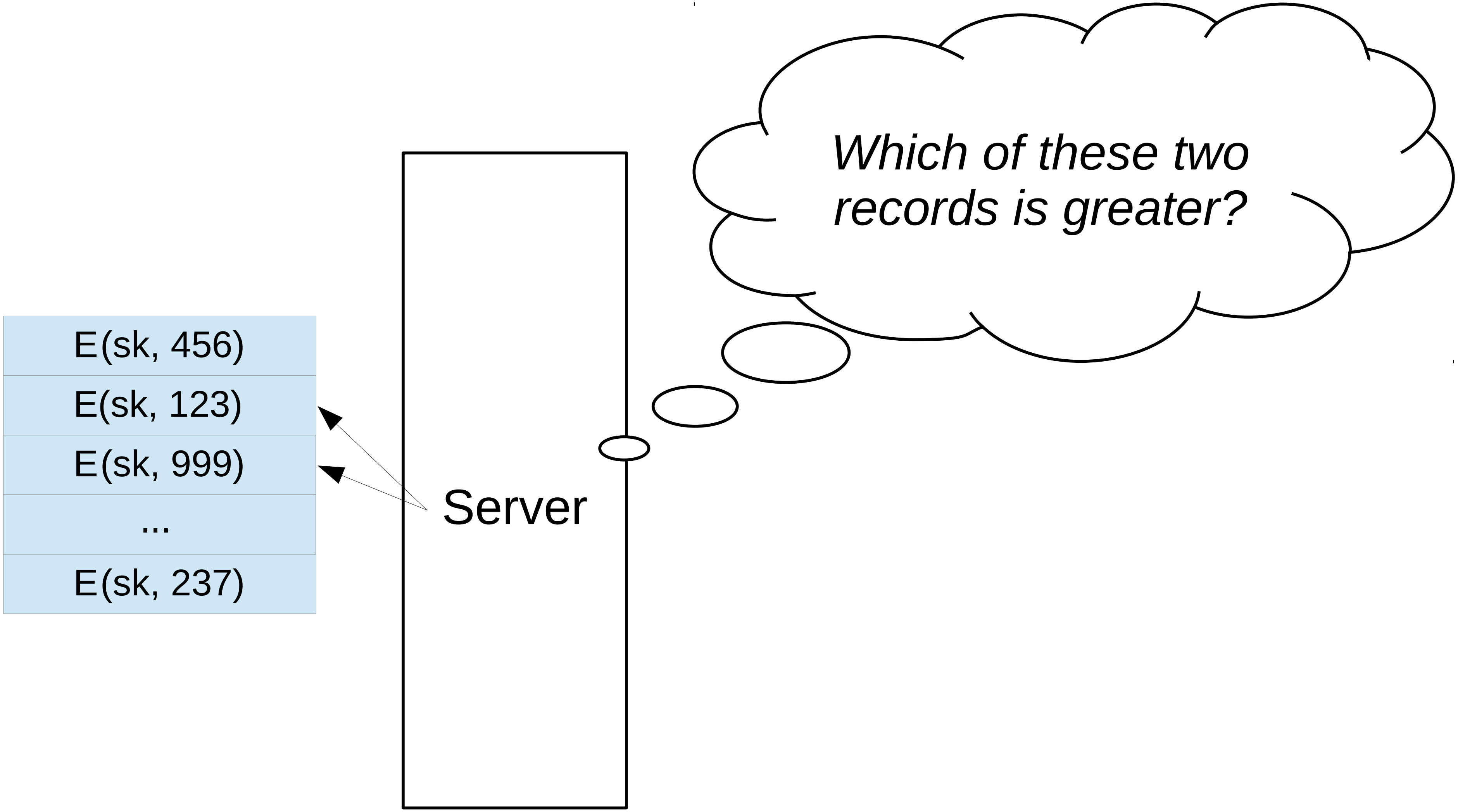
Server

Order-Revealing Encryption



Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption



E(sk, 456)

E(sk, 123)

E(sk, 999)

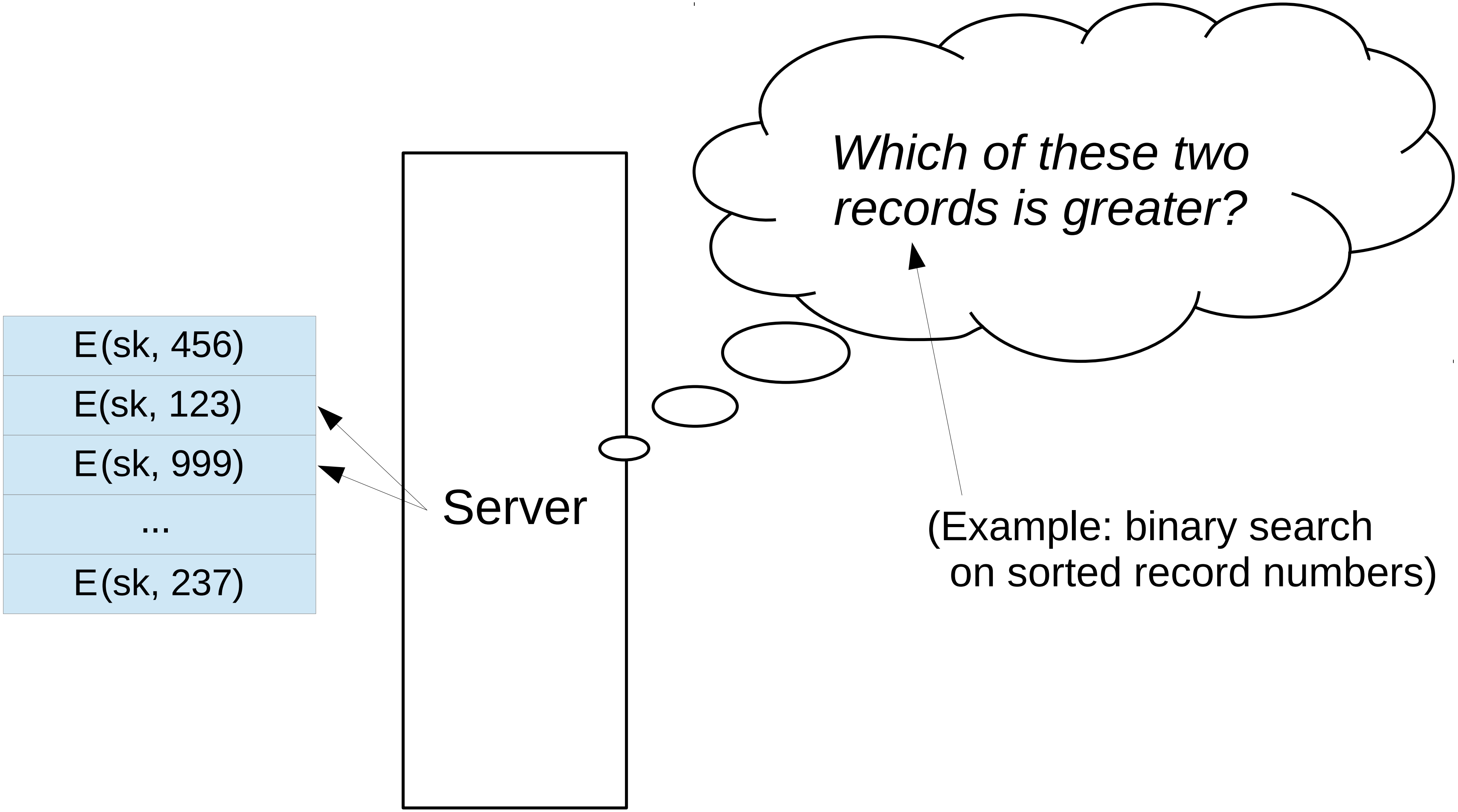
...

E(sk, 237)

Server

Which of these two records is greater?

Order-Revealing Encryption



E(sk, 456)

E(sk, 123)

E(sk, 999)

...

E(sk, 237)

Server

Which of these two records is greater?

(Example: binary search on sorted record numbers)

Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption

Solution 1:

- *Order-Preserving Encryption* [BCLO'04]

$$x < y \implies E(sk, x) < E(sk, y)$$

Order-Revealing Encryption

Solution 1:

- *Order-Preserving Encryption* [BCLO'04]

  $$x < y \implies E(sk, x) < E(sk, y)$$

- BCLO'04: Cannot be CPA-secure (up to ordering) unless ciphertext has exponential size

Order-Revealing Encryption

Solution 1:

- *Order-Preserving Encryption* [BCLO'04]

$$x < y \quad \Longrightarrow \quad E(sk, x) < E(sk, y)$$

- BCLO'04: Cannot be CPA-secure (up to ordering) unless ciphertext has exponential size

Solution 2:

- Multi-Input Functional Encryption [GGJS'14]

Order-Revealing Encryption

Solution 1:

- *Order-Preserving Encryption* [BCLO'04]

  $$x < y \implies E(sk, x) < E(sk, y)$$

- BCLO'04: Cannot be CPA-secure (up to ordering) unless ciphertext has exponential size

Solution 2:

- Multi-Input Functional Encryption [GGJS'14]
- Requires obfuscation of a PRF (e.g., AES)

Order-Revealing Encryption

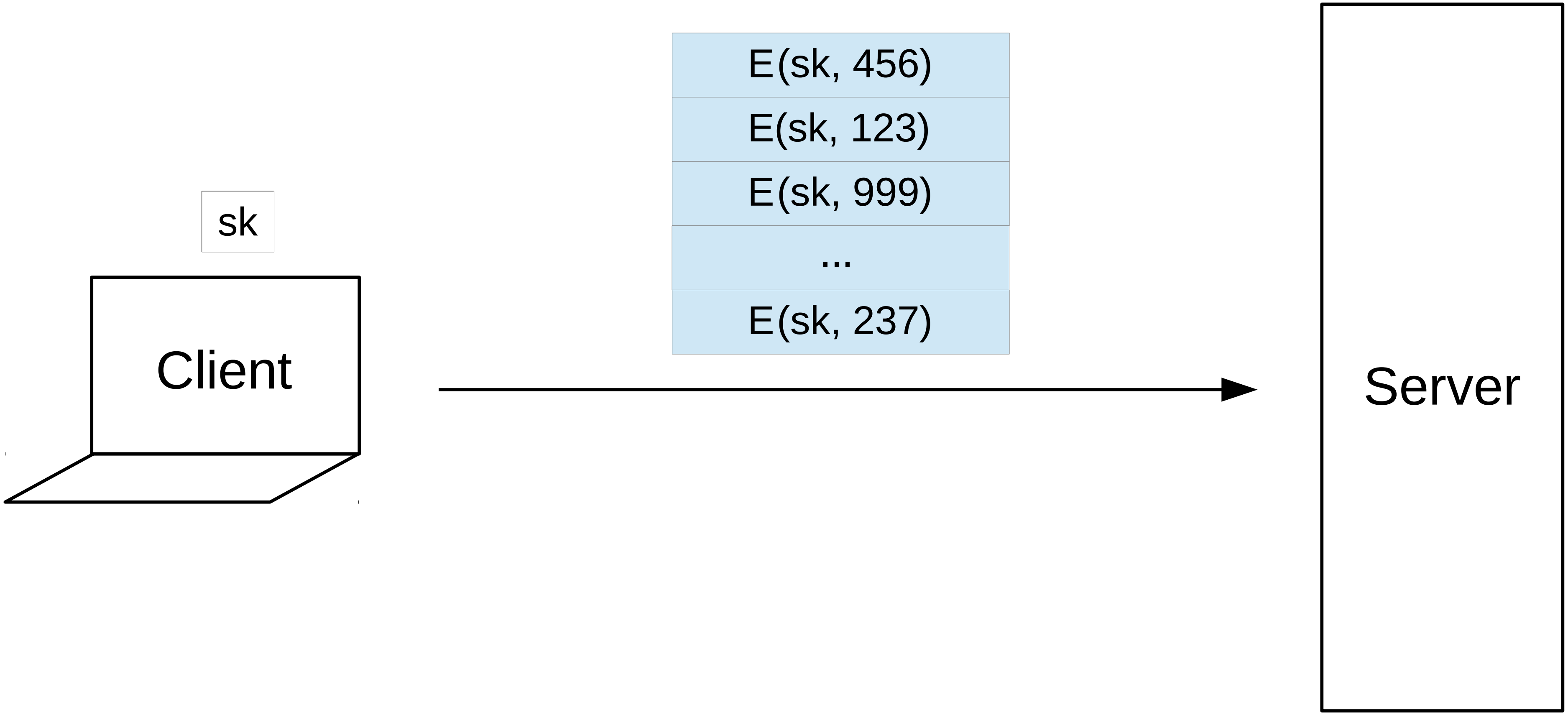
Our results:

- Not order-preserving, but *order-revealing*

Order-Revealing Encryption

Our results:

– Not order-preserving, but *order-revealing*

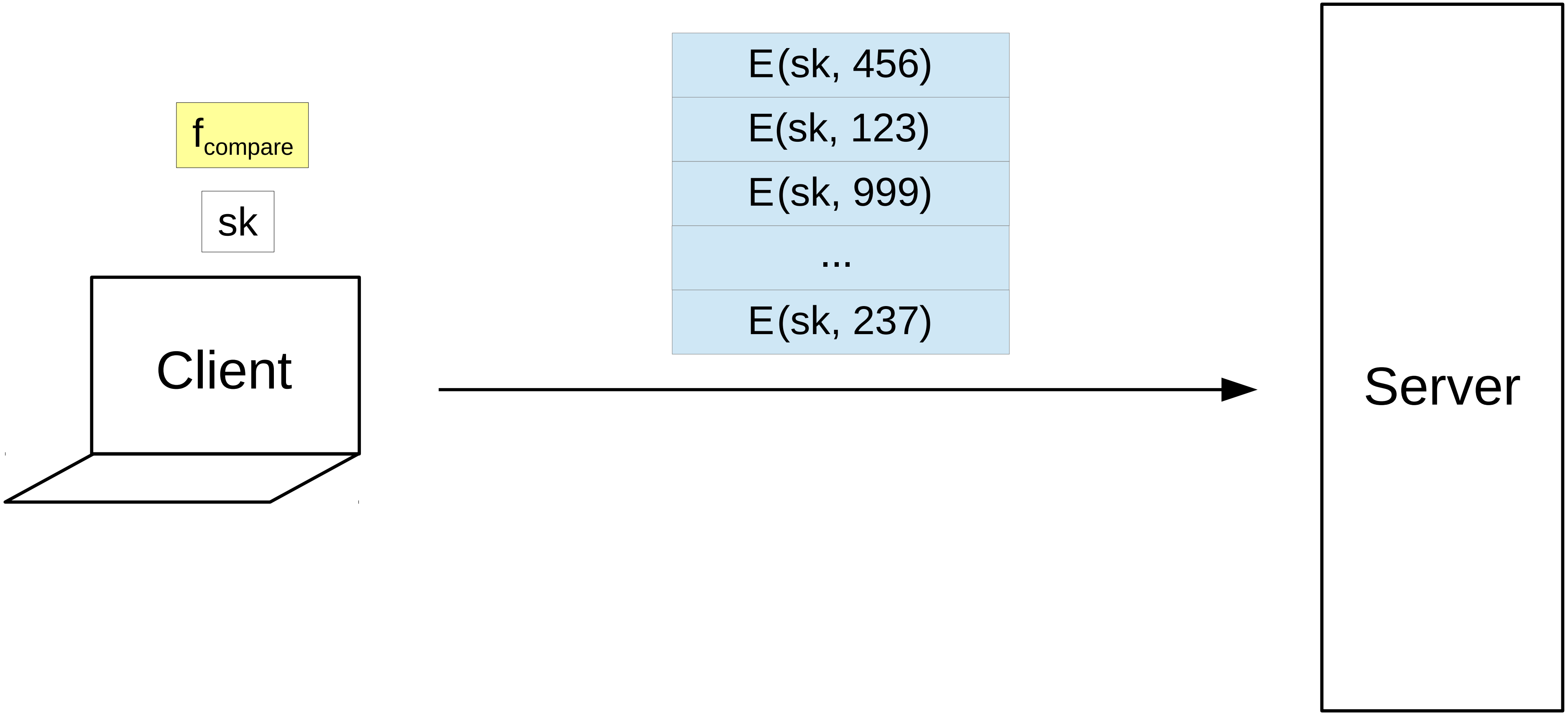


Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption

Our results:

– Not order-preserving, but *order-revealing*

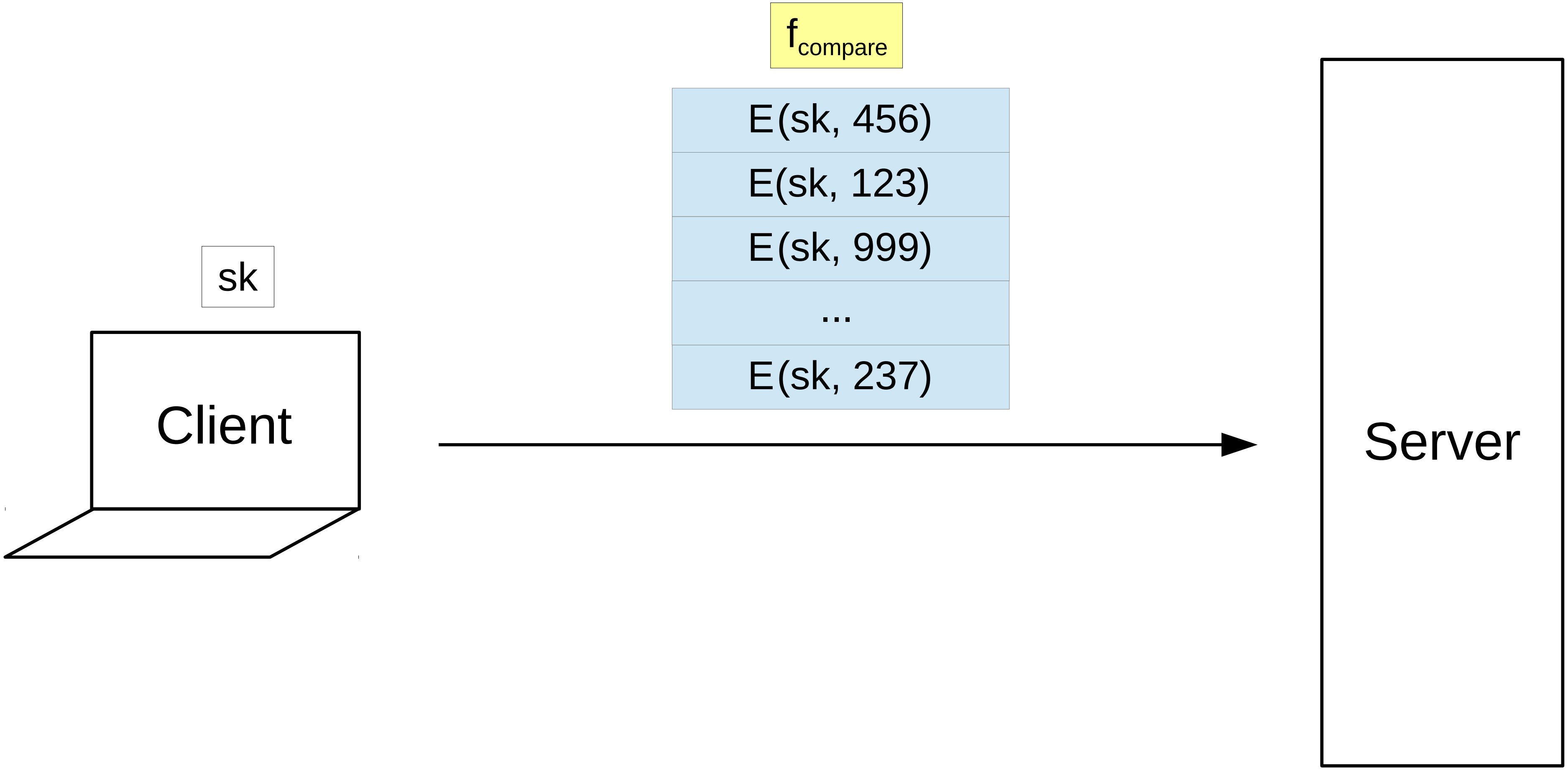


Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption

Our results:

– Not order-preserving, but *order-revealing*



$f_{compare}$

E(sk, 456)

E(sk, 123)

E(sk, 999)

...

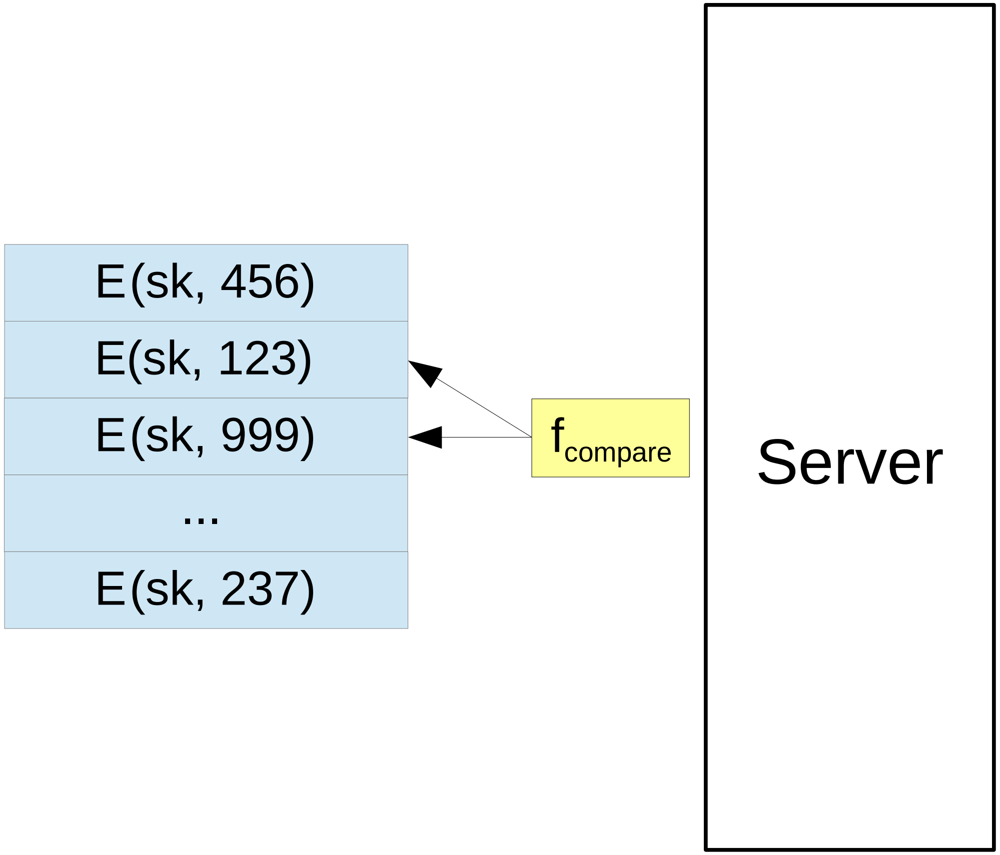
E(sk, 237)

Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption

Our results:

- Not order-preserving, but *order-revealing*



Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation
Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, **Joe Zimmerman**

Order-Revealing Encryption

Our results:

- Not order-preserving, but *order-revealing*

Order-Revealing Encryption

Our results:

- Not order-preserving, but *order-revealing*
- No obfuscation

Order-Revealing Encryption

Our results:

- Not order-preserving, but *order-revealing*
- No obfuscation
  - Inspired by obfuscation techniques

Order-Revealing Encryption

Our results:

- – Not order-preserving, but *order-revealing*
- – No obfuscation
  - – Inspired by obfuscation techniques
- – To compare 16-bit numbers:
  we only need a 17-way multilinear map

Order-Revealing Encryption

Our results:

- Not order-preserving, but *order-revealing*
- No obfuscation
  - Inspired by obfuscation techniques
- To compare 16-bit numbers:
  we only need a 17-way multilinear map
- For k-bit numbers: O(k) ops in (k+1)-linear map

Order-Revealing Encryption

Our results:

– Prove construction in generic map model [BR'13]

Order-Revealing Encryption

Our results:

- Prove construction in generic map model [BR'13]
- Techniques extend to other functionalities; arity > 2

Order-Revealing Encryption

Our results:

- Prove construction in generic map model [BR'13]
- Techniques extend to other functionalities; arity > 2
- Instances of Multi-Input Functional Encryption [GGJS'14] with a single secret key

Order-Revealing Encryption

<u>Our results:</u>

- Prove construction in generic map model [BR'13]
- Techniques extend to other functionalities; arity > 2
- Instances of Multi-Input Functional Encryption [GGJS'14] with a single secret key
- Not fast, but *implementable*!

Order-Revealing Encryption

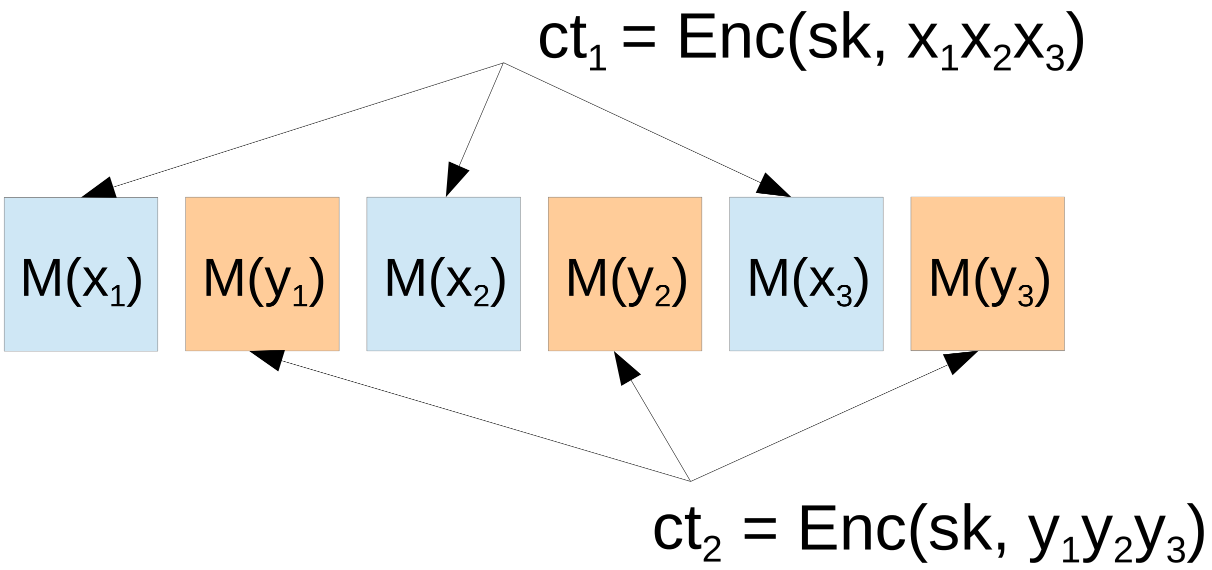
Our results – main techniques:

- Each ciphertext is a sequence of matrices encoded in the exponent of an (asymmetric) multilinear map

Order-Revealing Encryption

Our results – main techniques:

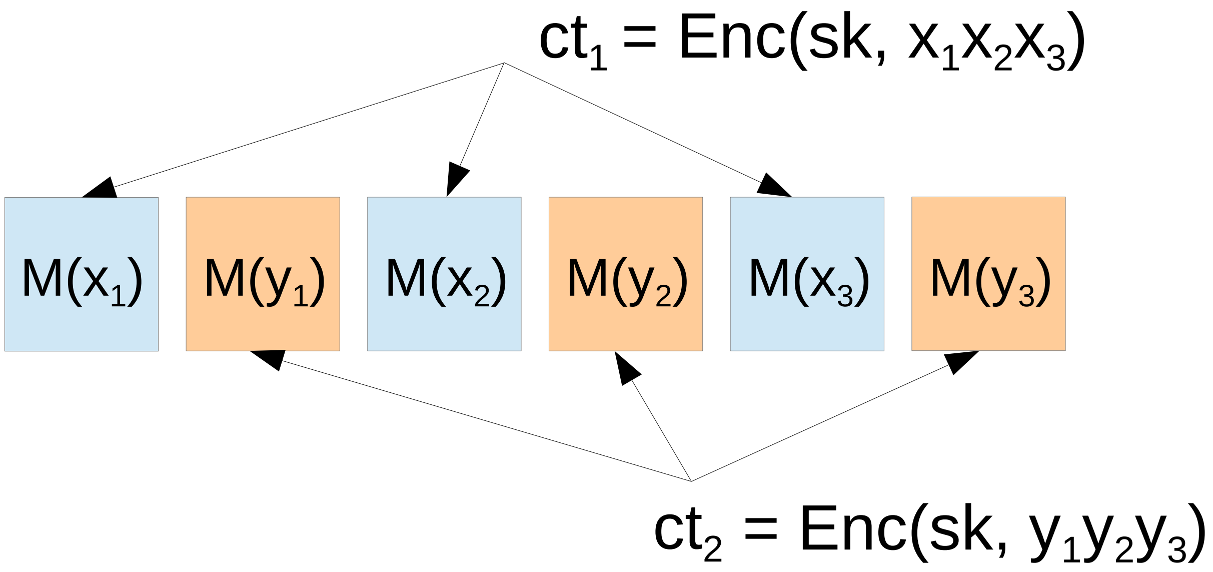
– Each ciphertext is a sequence of matrices encoded in the exponent of an (asymmetric) multilinear map



Order-Revealing Encryption

Our results – main techniques:

- Each ciphertext is a sequence of matrices encoded in the exponent of an (asymmetric) multilinear map



ct_1 = Enc(sk, $x_1x_2x_3$)

$M(x_1)$ $M(y_1)$ $M(x_2)$ $M(y_2)$ $M(x_3)$ $M(y_3)$

ct_2 = Enc(sk, $y_1y_2y_3$)

- To enforce consistency: *exclusive partition families* generalize straddling sets [BGK+'13]

Semantically Secure Order-Revealing Encryption:

Multi-Input Functional Encryption Without Obfuscation

Dan Boneh, Kevin Lewi, Mariana Raykova,
Amit Sahai, Mark Zhandry, **Joe Zimmerman**