Order-Preserving Encryption Revisited

Improved Security Analysis and Alternative Solutions

Alexandra Boldyreva
Georgia Tech

Nathan Chenette
Georgia Tech

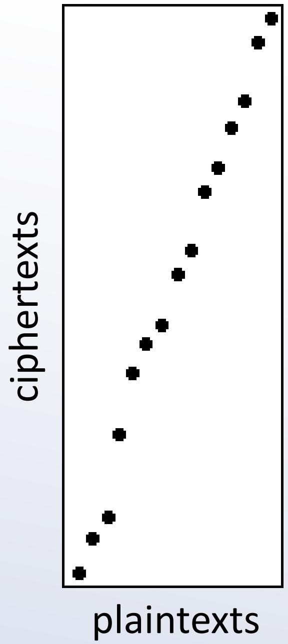
Adam O'Neill
UT Austin

Background and Motivation

Order-Preserving Encryption (OPE)

A symmetric encryption scheme is order-preserving if encryption is deterministic and strictly increasing

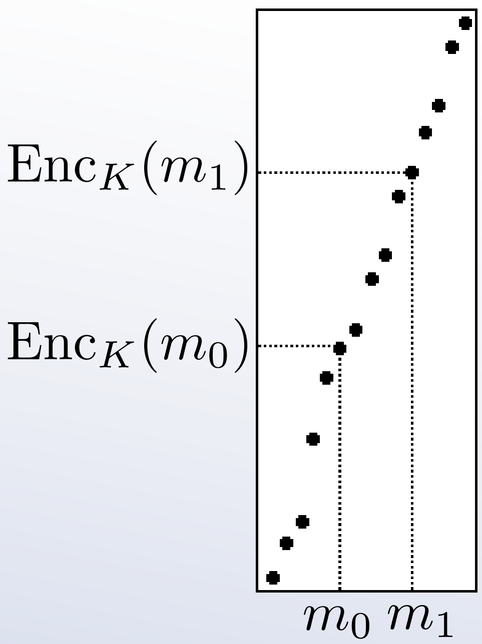
Example OPE function $\mathrm{Enc}_K(\cdot)$ for $K \xleftarrow{\$} \mathrm{KeyGen}$:



Order-Preserving Encryption (OPE)

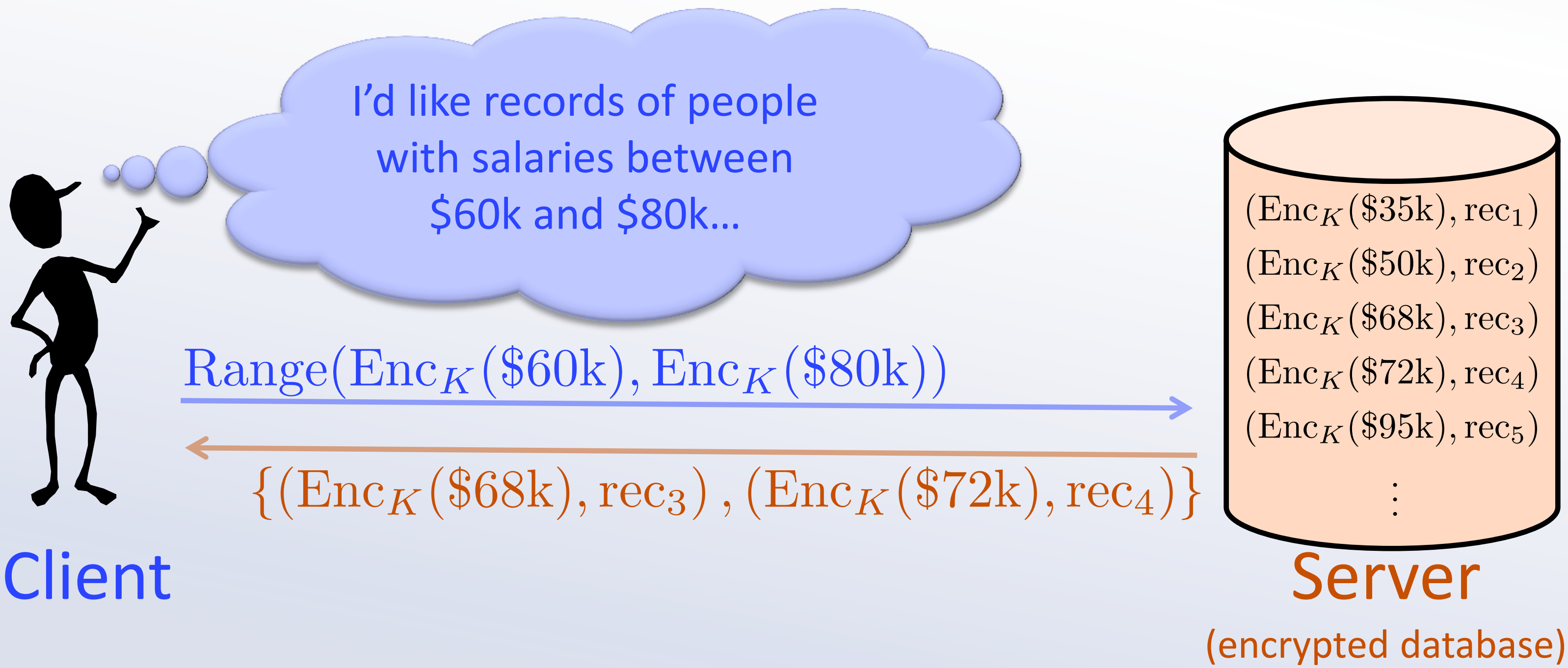
A symmetric encryption scheme is order-preserving if encryption is deterministic and strictly increasing

Example OPE function $\mathrm{Enc}_K(\cdot)$ for $K \xleftarrow{\$} \mathrm{KeyGen}$:



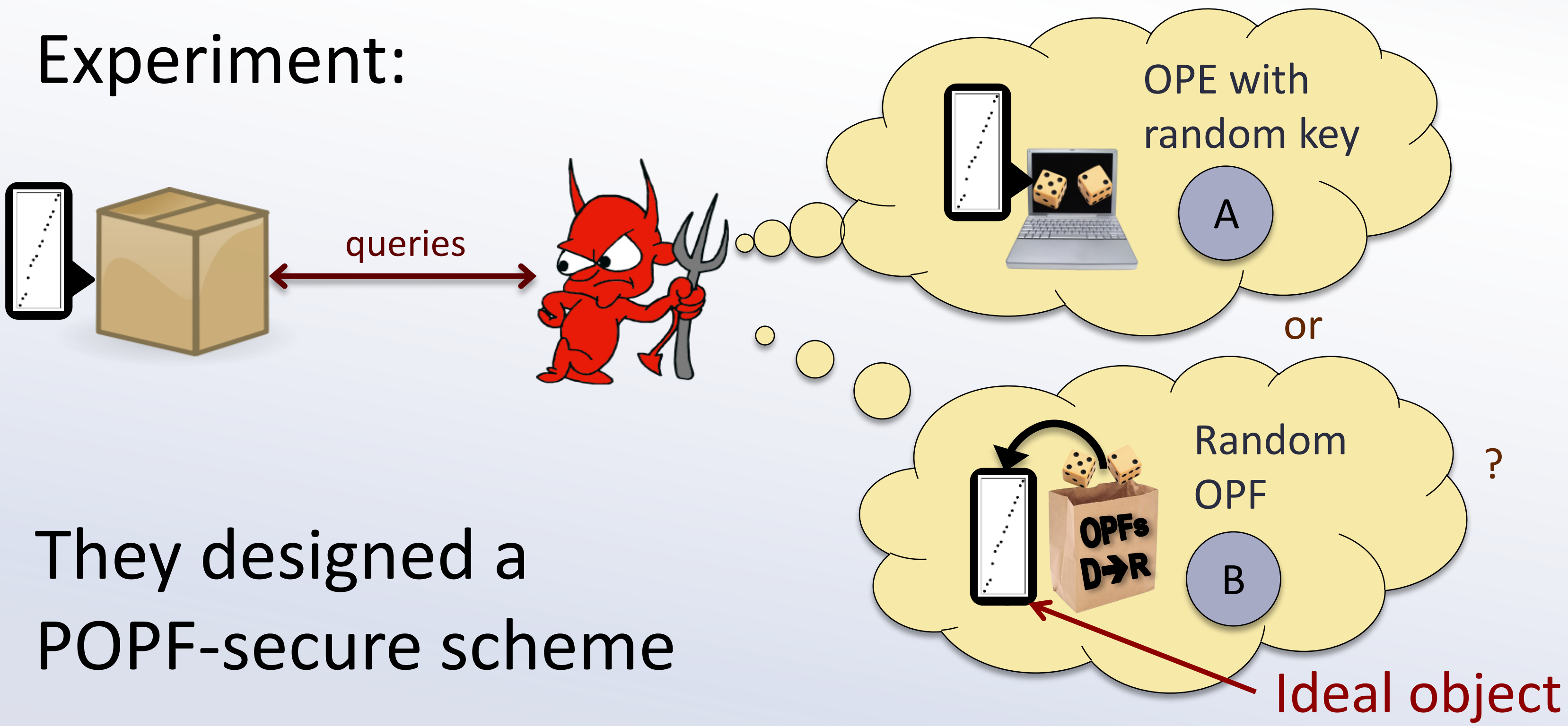
OPE application: Range Queries on Encrypted Data

[AKSX04] suggested OPE as a protocol to support efficient range queries for outsourced databases



Cryptographic Study of OPE

- [BCLO09] defined a secure OPE to be a pseudorandom order-preserving function (POPF)
- Experiment:



- They designed a POPF-secure scheme

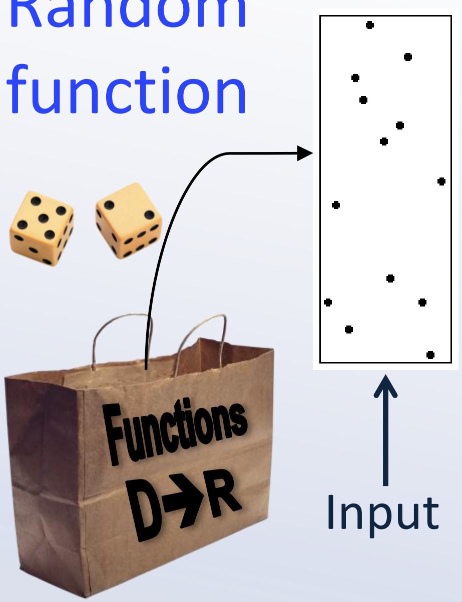
Security Guarantees of Ideal Object?

- Practitioners want to implement the OPE scheme right away as it has been proven POPF-secure and is in any case better than no encryption
- But, as emphasized by [BCLO09], we must first establish security guarantees of the ideal object, a random OPF
  - What information is necessarily leaked?
  - What information is secure?
- To elaborate…

Security Guarantees of Ideal Object?

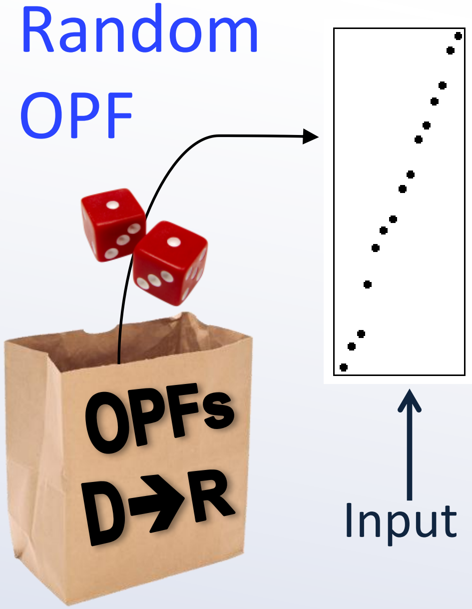
- The security properties of a random OPF are unclear
  - Compare to the case of PRF/random function

Random function



GUARANTEE:
Output leaks
only equality

Random OPF



Output leaks…
- order
- approx. location
- approx. distance
- more?

Our Contributions

Our Contributions

- We suggest several notions of one-wayness to analyze OPE security
- We analyze the one-wayness of a random OPF (and thus by extension the POPF-secure scheme of [BLCO09])
- We introduce two generalizations/modifications of the OPE primitive that support range queries in (only) particular circumstances with improved one-wayness
  - Modular order-preserving encryption (modular range queries)
  - Committed order-preserving encryption (static database)

One-wayness Notions of Security

New Security Notions

- Central concern: what do ROPF ciphertexts reveal/hide about…
  - location of plaintexts?
  - distance between plaintexts?
- We propose several varieties of one-wayness

(r, z)-Window One-wayness

- r = window size
- z = challenge set size

$$m_1, \ldots, m_z \xleftarrow{\$} \mathrm{MsgSp}$$
$$K \xleftarrow{\$} \mathrm{KeyGen}$$

$$\xrightarrow{\mathrm{Enc}_K(m_1), \ldots, \mathrm{Enc}_K(m_z)}$$

$$\xleftarrow{(m_L, m_L + r)}$$

Adversary

Adversary's advantage is the probability of the event that

$$\exists i : m_i \in [m_L, m_L + r)$$

(r, z)-Window Distance One-wayness

- r = distance window size
- z = challenge set size

$$m_1, \ldots, m_z \xleftarrow{\$} \mathrm{MsgSp}$$
$$K \xleftarrow{\$} \mathrm{KeyGen}$$

Adversary

$$\xrightarrow{\mathrm{Enc}_K(m_1), \ldots, \mathrm{Enc}_K(m_z)}$$

$$\xleftarrow{(d_L, d_L + r)}$$

Adversary's advantage is the probability of the event that

$$\exists i \neq j : d(m_i, m_j) \in [d_L, d_L + r)$$

One-wayness of a Random OPF

ROPF One-wayness Results: Overview

	Small Window $r = 1$	Large window $r \approx \frac{z}{\sqrt{M}}$
Window One-wayness	"Secure" (upper bound on any adversary's advantage)	"Insecure" (lower bound on constructed adversary's advantage)
Distance Window One-wayness	"Secure" (upper bound on any adversary's advantage)	"Insecure" (lower bound on constructed adversary's advantage)

Size of message space

ROPF: "Secure" under small-window one-wayness

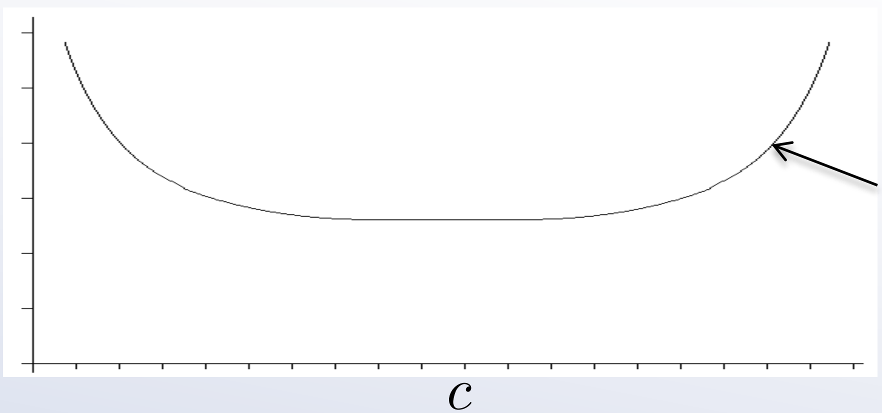
- We prove an upper bound on $(1, z)$-WOW advantage against ROPF
- Theorem: If $N \geq 2M$ for $\begin{cases} M & \text{= Size of message space} \\ N & \text{= Size of ciphertext space} \end{cases}$,

$$\mathbf{Adv}^{1,z\text{-wow}}_{\mathsf{ROPF}_{[M],[N]}}(A) < \frac{9z}{\sqrt{M - z + 1}}$$

- Interpretation:
  - Any adversary's probability of inverting one of z encryptions of random plaintexts is bounded by (approx) a constant times $z/\sqrt{M}$
  - For reasonable z, this is small.

Proof strategy

- Reduce to problem of bounding $(1,1)$-WOW-advantage
- Each ciphertext c has a most likely plaintext (m.l.p.) m_c given that encryption is a random OPF
  - Given c, adversary's best option is to output m_c



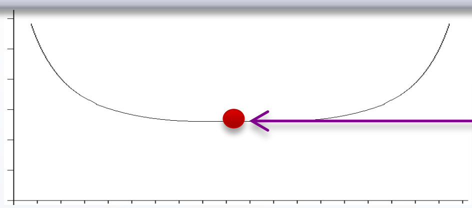
m.l.p. probabilities

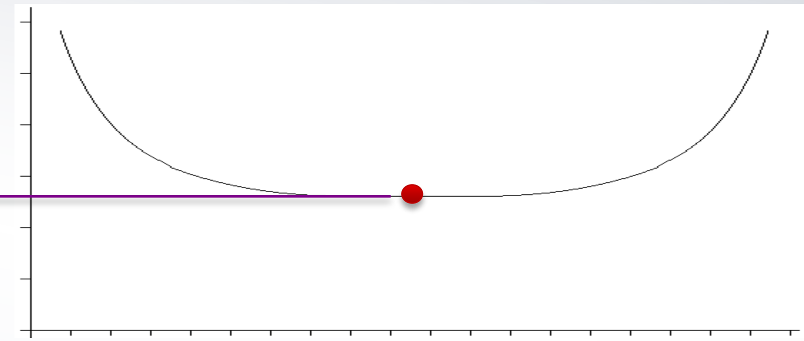
$$\Pr\left[f(c) = m_c \mid f \xleftarrow{\$} \mathrm{OPF}_{[M],[N]}\right]$$

  - Upper bound on advantage: the average m.l.p. probability
  - = (area under curve) / (#ciphertexts)

Proof outline

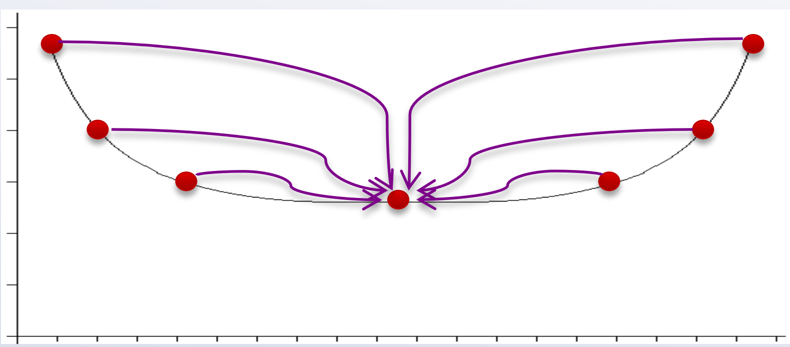
Let $P(c, M, N) =$
$\Pr\left[f(m) = m_c \mid f \xleftarrow{\$} \mathrm{OPF}_{[M],[N]} \right]$



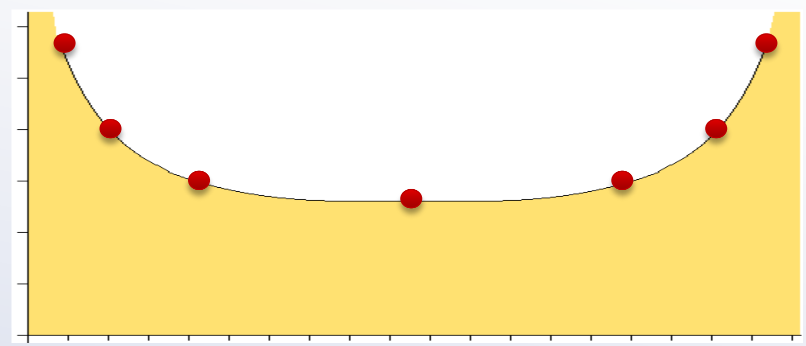


1 Start with $P(N'/2, M', N')$
for M', N' small and fixed

2 For general M, N, write $P(N/2, M, N)$
as a function of $P(N'/2, M', N')$



3 For $\frac{1}{N} < k < \frac{N-1}{N}$, write $P(kN, M, N)$
as a function of $P(N/2, M, N)$



4 Integrate this function over the
ciphertext range and divide by N
to find the approx. avg. m.l.p. prob.

ROPF: "Insecure" under large-window one-wayness

- We prove a lower bound on an adversary's (r, z)-WOW advantage against ROPF

$\begin{cases} M & = \text{Size of message space} \\ N & = \text{Size of ciphertext space} \end{cases}$

- Theorem: For any b there exists an adversary A such that for $r \approx b\sqrt{M}$,

$$\boxed{\mathbf{Adv}^{r,z\text{-wow}}_{\mathsf{ROPF}_{[M],[N]}}(A) \geq 1 - 2e^{-b^2/2}}$$

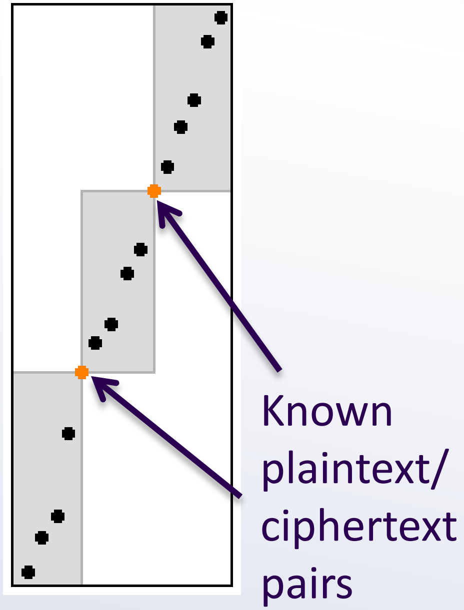
- Interpretation:
  - Given z encryptions of random plaintexts, adversary A can (with high probability) invert one of them to within a size $b\sqrt{M}$ window, where b is a medium-sized constant (say, 8)

ROPF distance window one-wayness

- Analogous to the WOW case, we show:
  - Upper bound on $(1, z)$-DWOW advantage of any adversary
  - Lower bound on an adversary's (r, z)-DWOW advantage for $r \approx b\sqrt{M}$
- Interpretation:
  - Guessing the exact distance between encryptions of two random plaintexts is hard.
  - Guessing the approximate distance is easy.

Further security considerations for ROPF

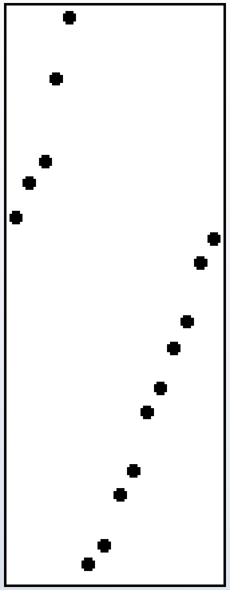
- If some plaintext/ciphertext pairs are known, the adversary's view (and our analysis) applies to the subspaces between these points
- Choosing ciphertext space size N: $N \geq 7M$ should be sufficient for analysis to hold
- Assumption alert!
  - Our analysis is limited to uniformly random challenge messages
  - Open problem to extend otherwise



Alternatives to Order-preserving Encryption

Modular OPE

- Generalization of OPE in which "modular order" is preserved, supports modular range queries
- The OPE scheme of [BCLO09] can be extended to an MOPE scheme by prepending a random (secret) shift
  - Now optimally (r, z)-WOW secure
  - (r, z)-DWOW security is equivalent to that of the OPE scheme
  - Knowledge of a single plaintext/ciphertext pair essentially reduces the MOPE to an OPE

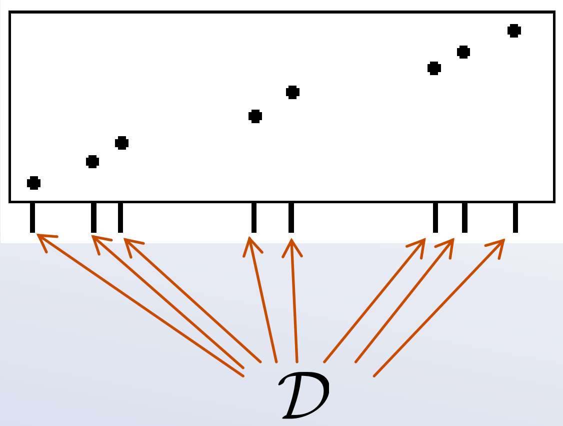


Committed OPE

- Past results [AKSZ04] have implemented schemes for range queries on predetermined static databases
  - Key generation takes database as input, all ciphertexts revealed
  - OP version of secure searchable index schemes ([CGKO06], etc.)
- We straightforwardly construct an optimally-secure OPE tagging scheme using monotone minimal perfect hash functions (MMPHFs) [BBPV09]

$\mathcal{D}$ = message space (static database)

$\mathrm{KeyGen}(\mathcal{D})$:
Outputs a key corresponding to the MMPHF sending the ith element of $\mathcal{D}$ to i



Conclusion

Conclusion

- We made significant progress in addressing the [BCLO09] open question of analyzing the security of a random OPF
  - Introduced new security models using one-wayness notions
  - Analyzed ROPF under those models
- We introduced two variations of OPE that could be useful in some settings
- Taken with certain precautions, we hope our results will help practitioners determine whether the security vs. functionality tradeoff of OPE is acceptable for their applications

Thanks!