Fundamental Limits of Secretive Coded Caching

V. Ravindrakumar, P. Panda, N. Karamchandani
V. Prabhakaran

1Department of Electrical Engg.,
IIT Bombay

2School of Technology and Computer Science,
TIFR

ISIT, 2016
- $N$ files of size $F$ bits, $K$ users, each with their own demand

V. Ravindrakumar, P. Panda, N. Karamchan: Fundamental Limits of Secretive Coded Caching
ISIT, 2016 2 / 17
Maddah-Ali and Niesen - General Setup

- $N$ files of size $F$ bits, $K$ users, each with their own demand

- Caching Phase, demands not revealed

- Delivery Phase, demand vector $d$ revealed

- Goal: Smallest rate
- $N$ files of size $F$ bits, $K$ users, each with their own demand

- Caching Phase, demands not revealed
- Delivery Phase, demand vector $\mathbf{d}$ revealed
\(N\) files of size \(F\) bits, \(K\) users, each with their own demand

- Caching Phase, demands not revealed
- Delivery Phase, demand vector \(d\) revealed
- Goal: Smallest rate
Demands
Caches
$M = 1$

$A = (A_1, A_2)$

$B = (B_1, B_2)$

Coded delivery benefits

$R_C = 0.5$ vs $R = 1$ for non-coded
Maddah-Ali and Niesen - Illustration

Demands
Caches

\[ \begin{align*}
A &= (A_1, A_2) \\
B &= (B_1, B_2)
\end{align*} \]

\[ M = 1 \]

Demands
Caches

\[ \begin{align*}
A_1 & \quad B_1 \\
A_2 & \quad B_2
\end{align*} \]

Coded delivery benefits

\[ R_C = 0.5 \text{ vs } R = 1 \text{ for non-coded} \]
Maddah-Ali and Niesen - Illustration

\[ A = (A_1, A_2) \]
\[ B = (B_1, B_2) \]

Demands

Caches

\[ A_2 \oplus B_1 \]

\[ M = 1 \]

Coded delivery benefits

\[ R_C = 0.5 \] vs \[ R = 1 \] for non-coded
\[ A = (A_1, A_2) \]
\[ B = (B_1, B_2) \]

Coded delivery benefits

\[ R_C = .5 \text{ vs } R = 1 \text{ for non-coded} \]
Information Leakage

Demands

\[ A = (A_1, A_2) \]
\[ B = (B_1, B_2) \]

Caches

\[ M = 1 \]

- Potential leakage of data
- Example: Netflix movies
Our Variation

Constraint: For any $\epsilon > 0$,

$$\max_{d \in [N]^K} \max_{k \in [K]} I(W_{[N]/\{d_k\}}; X_d(W, Z), Z_k) < \epsilon$$

Subject to this what’s the minimum delivery rate - $R^*_S(M)$?
A Trivial Example - $N = K = 2$

Demands

Caches

$M = 1$

$W_1$

$W_2$

The scheme gives $R_C(M = 1) = K$ in general.
A Trivial Example - $N = K = 2$

- $T_1$, $T_2$ - Keys
A Trivial Example - $N = K = 2$

- $T_1, T_2$ - Keys
A Trivial Example - $N = K = 2$

- $T_1, T_2$ - Keys
- Gives a rate $R_C(M = 1) = 2$
- The scheme gives $R_C(M = 1) = K$ in general
Secretive Caching

\[ \begin{align*}
W_1 \\
W_2 \\
\end{align*} \]

Demands

Caches

\[ M = 2 \]
Secretive Caching

\[
\begin{align*}
B &= W_1 \oplus T_1 \\
Q &= W_2 \oplus T_2 \\
A &= T_1 \\
P &= T_2
\end{align*}
\]
More Memory - $N = K = 2$

- Secretive Caching

Thus we have

$R_C(M = 2) = 1$

V. Ravindrakumar, P. Panda, N. Karamchan
Fundamental Limits of Secretive Coded Caching
ISIT, 2016
More Memory - $N = K = 2$

- Secretive Caching

Thus we have $R_C(M = 2) = 1$
Notion of Secret Sharing

\[ B = W_1 \oplus T_1 \]
\[ Q = W_2 \oplus T_2 \]
\[ A = T_1 \]
\[ P = T_2 \]

Demands

Caches
\[ M = 2 \]
Notion of Secret Sharing

- (1, 2) secret sharing
- Any 1 share - zero information, 2 together - reconstruction
Notion of Secret Sharing

- \((m, n)\) secret sharing
- Any \(m\) shares - zero information, \(n\) together - reconstruction
Extending to $N = 2$, $K = 3$

- We use a $(2, 3)$ secret sharing scheme

\begin{itemize}
  \item $W_1$ \hspace{1cm} $W_2$
  \item Demands
  \item Caches
  \item $M = 4$
\end{itemize}
Extending to $N = 2$, $K = 3$

- We use a (2, 3) secret sharing scheme

```
Demands
Caches
M = 4

B C
Q S
A C
P S
A B
P Q
```
Extending to $N = 2, \ K = 3$

- We use a (2, 3) secret sharing scheme

\[ A \oplus B \oplus S \]

Demands
Caches
\[ M = 4 \]

\[ \begin{array}{c}
W_1 \\
W_2 \\
A \oplus B \oplus S \\
1 \\
B \ C \\
Q \ S \\
1 \\
A \ C \\
P \ S \\
2 \\
A \ B \\
P \ Q \\
\end{array} \]
Extending to \( N = 2, K = 3 \)

- We use a \((2, 3)\) secret sharing scheme

- Here \( R_C(M = 4) = 1 \)
- For \( N, K > 2 \), \( R_C(M) = 1 \) at \( M = N(K - 1) \)
We've achieved \((M, R_C) = (1, K)\) and \((M, R_C) = (N(K - 1), 1)\).
We've achieved \((M, R_C) = (1, K)\) and \((M, R_C) = (N(K - 1), 1)\).

Intermediate \(M\), i.e. \(1 < M < N(K - 1)\)?
We’ve achieved \((M, R_C) = (1, K)\) and \((M, R_C) = (N(K - 1), 1)\).

Intermediate \(M\), i.e. \(1 < M < N(K - 1)\)?

Memory sharing, can we do better?
We’ve achieved $(M, R_C) = (1, K)$ and $(M, R_C) = (N(K - 1), 1)$

Intermediate $M$, i.e. $1 < M < N(K - 1)$?

Memory sharing, can we do better?

Parameterize $M = Nt/(K - t) + 1$ for some $t \in \{1, ..., K - 2\}$

Use $\binom{K-1}{t-1}, \binom{K}{t}$ secret sharing scheme, $\binom{K}{t+1}$ keys
Generalization Example

- \( N = 2, K = 3 \) at \( t = 1 \) or \( M = 2 \)
- Thus we use \( (\binom{2}{0}, \binom{3}{1}) \) secret sharing scheme, \( \binom{3}{2} \) keys

\[
\begin{array}{c}
W_1 \\
W_2
\end{array}
\]

Demands

Caches

\( M = 2 \)
Generalization Example

- $N = 2$, $K = 3$ at $t = 1$ or $M = 2$
- Thus we use $\binom{2}{0}, \binom{3}{1}$ secret sharing scheme, $\binom{3}{2}$ keys

![Diagram](image-url)
• $N = 2$, $K = 3$ at $t = 1$ or $M = 2$
• Thus we use $\binom{2}{0}, \binom{3}{1}$ secret sharing scheme, $\binom{3}{2}$ keys

We achieve $R_C(2) = \frac{3}{2}$ vs $R_C(2) = \frac{7}{3}$ by memory sharing.
- \( N = 2, \ K = 3 \) at \( t = 1 \) or \( M = 2 \)
- Thus we use \( \left( \binom{2}{0}, \binom{3}{1} \right) \) secret sharing scheme, \( \binom{3}{2} \) keys

\[
T_{1,2} \oplus B \oplus A
\]

Demands
\[
\begin{array}{c}
1 \\
\end{array}
\]

Caches
\[
\begin{array}{c}
A \\
B \\
C \\
\end{array}
\]

Recovered shares
\[
\begin{array}{c}
B \\
A \\
\end{array}
\]

We achieve \( R_C(2) = \frac{3}{2} \) vs \( R_C(2) = \frac{7}{3} \) by memory sharing.
$N = 2, K = 3$ at $t = 1$ or $M = 2$

Thus we use $\binom{2}{0}, \binom{3}{1}$ secret sharing scheme, $\binom{3}{2}$ keys
Generalization Example

- $N = 2$, $K = 3$ at $t = 1$ or $M = 2$
- Thus we use $\left( \binom{2}{0}, \binom{3}{1} \right)$ secret sharing scheme, $\binom{3}{2}$ keys

```
Demands
  1
  1
  2

Caches
  $M = 2$
  $T_{1,2}$
  $T_{1,3}$
  $T_{1,2}$
  $T_{2,3}$
  $T_{1,3}$
  $T_{2,3}$

Recovered shares
  $B$
  $C$
  $A$
  $C$
  $P$
  $Q$
```

We achieve $R_C(2) = \frac{3}{2}$ vs $R_C(2) = \frac{7}{3}$ by memory sharing.
Generalization Example

- $N = 2$, $K = 3$ at $t = 1$ or $M = 2$
- Thus we use $\binom{2}{0}$, $\binom{3}{1}$ secret sharing scheme, $\binom{3}{2}$ keys

We achieve $R_C(2) = 3/2$ vs $R_C(2) = 7/3$ by memory sharing
Theorem 1

For $M = \frac{Nt}{K-t} + 1$ with $t \in \{0, 1, \ldots, K-2\}$

$$R_C(M) \equiv \frac{K(N+M-1)}{N + (K+1)(M-1)}$$

is achievable. Also, at $M = N(K-1)$, $R_C(M) = 1$. 
Theorem 1

For $M = \frac{Nt}{K-t} + 1$ with $t \in \{0, 1, \ldots, K - 2\}$

$$R_C(M) \triangleq \frac{K(N + M - 1)}{N + (K + 1)(M - 1)}$$

is achievable. Also, at $M = N(K - 1)$, $R_C(M) = 1$.

Theorem 2

For $1 \leq M \leq N(K - 1)$,

$$R^*_S(M) \geq \max_{s \in \{1, 2, \ldots, \min\{N/2, K\}\}} \frac{s\lfloor N/s \rfloor - 1 - (s - 1)M}{\lceil N/s \rceil - 1}$$
Theorem 3

For $M \geq M_0$, 

$$1 \leq \frac{R_C(M)}{R_S^*(M)} \leq 16$$

where $M_0 = 1$ for $N \geq K$ and $M_0 \leq 5/2$ for $N < K$

- $N \geq K$ - order-optimality for entire memory range
- $N < K$ - except small memory range
Figure: Comparison for $N = 25$ files and $K = 15$ users
Plot - Cost of Secrecy

Figure: Comparison for $N = 15$ files and $K = 10$ users
Remarks

- Certain small setups - strictly optimal schemes
Remarks

- Certain small setups - strictly optimal schemes
- Additional eavesdropper security implicit
Remarks

- Certain small setups - strictly optimal schemes
- Additional eavesdropper security implicit
- Colluding users - modify secret sharing parameters
Remarks

- Certain small setups - strictly optimal schemes
- Additional eavesdropper security implicit
- Colluding users - modify secret sharing parameters
- Decentralized version - cooking, almost ready, chefs checking for poison
Remarks

- Certain small setups - strictly optimal schemes
- Additional eavesdropper security implicit
- Colluding users - modify secret sharing parameters
- Decentralized version - cooking, almost ready, chefs checking for poison
- Thank you!