ON SECRET SHARING, RANDOMNESS, AND RANDOM-LESS REDUCTIONS

Divesh Aggarwal Eldon Chung Maciej Obremski Joao Ribeiro

UNIFORM RANDOMNESS

Lots of applications

- BPP algorithms
- Cryptographic constructions
- Distributed and Network Protocols
- Etc

UNIFORM RANDOMNESS

Lots of applications

- BPP algorithms
- Cryptographic constructions
- Distributed and Network Protocols
- Etc

But can we generate uniform randomness?

IDEAL WORLD

$Pr[X_i = 0] = Pr[X_i = 1] = ½$

$Pr[X = x] = 1/2^n$

MINIMAL REALISTIC ASSUMPTION

The random number generator outputs X, such that

- "Hard" to guess X
- Equivalently, for all x, $\Pr[X=x] \leq 1/2^k$
- $H_\infty(X) \geq k$

MINIMAL REALISTIC ASSUMPTION

The random number generator outputs X, such that

- "Hard" to guess X
- Equivalently, for all x, $\Pr[X=x] \leq 1/2^k$
- $H_\infty(X) \geq k$

How can we use such a source for crypto applications?

EXTRACTING UNIFORM RANDOMNESS

EXTRACTING UNIFORM RANDOMNESS

Unfortunately, no deterministic extractor extracts from all such sources

EXTRACTING UNIFORM RANDOMNESS

Unfortunately, no deterministic extractor extracts from all such sources

Can we still build crypto primitives from min-entropy sources?

BUILDING CRYPTO PRIMITIVES FROM WEAK SOURCES

[DOPS04] showed that the following crypto tasks are impossible from block sources (e.g. Santha Vazirani) source.

- Encryption
- Secret Sharing
- Zero knowledge
- Secure two party computation
- Bit commitment

TO SUMMARIZE..

Uniform

TO SUMMARIZE..

Uniform

Extractable

TO SUMMARIZE..

Uniform

Extractable

Crypto primitives can be built!

TO SUMMARIZE..

Uniform

Extractable

Block source

Crypto primitives can be built!

TO SUMMARIZE..

Uniform

Extractable

Block source

Min-entropy source

Crypto primitives can be built!

TO SUMMARIZE..

Uniform	Extractable

Crypto primitives can be built!

Block source	Min-entropy source

Many crypto primitives impossible

TO SUMMARIZE..

Uniform	Extractable

Block source	Min-entropy source

Crypto primitives can be built!

Many crypto primitives impossible

Question: What crypto primitives can be built from some weak source that is not extractable?

TO SUMMARIZE..

Are there sources in the middle good for crypto?

Crypto primitives can be built!

Many crypto primitives impossible

Question: What crypto primitives can be built from some weak source that is not extractable?

ENCRYPTION $\Longrightarrow$ EXTRACTION [BD07]

- Let K be some key sampled from the source used for encryption.

ENCRYPTION $\Longrightarrow$ EXTRACTION [BD07]

- Let K be some key sampled from the source used for encryption.
- They extract uniform randomness from $Enc(K, \mathbf{0})$

ENCRYPTION $\Longrightarrow$ EXTRACTION [BD07]

- Let K be some key sampled from the source used for encryption.
- They extract uniform randomness from $Enc(K, \mathbf{0})$
- Notice $Enc(K, \mathbf{0}) \approx Enc(K, U)$, where U is a uniform message

ENCRYPTION $\Longrightarrow$ EXTRACTION [BD07]

- Let K be some key sampled from the source used for encryption.
- They extract uniform randomness from $Enc(K, \mathbf{0})$
- Notice $Enc(K, \mathbf{0}) \approx Enc(K, U)$, where U is a uniform message
- $Enc(K, U)$ is a convex combination of $Enc(k, U)$, where key k is any fixed key in the key space.

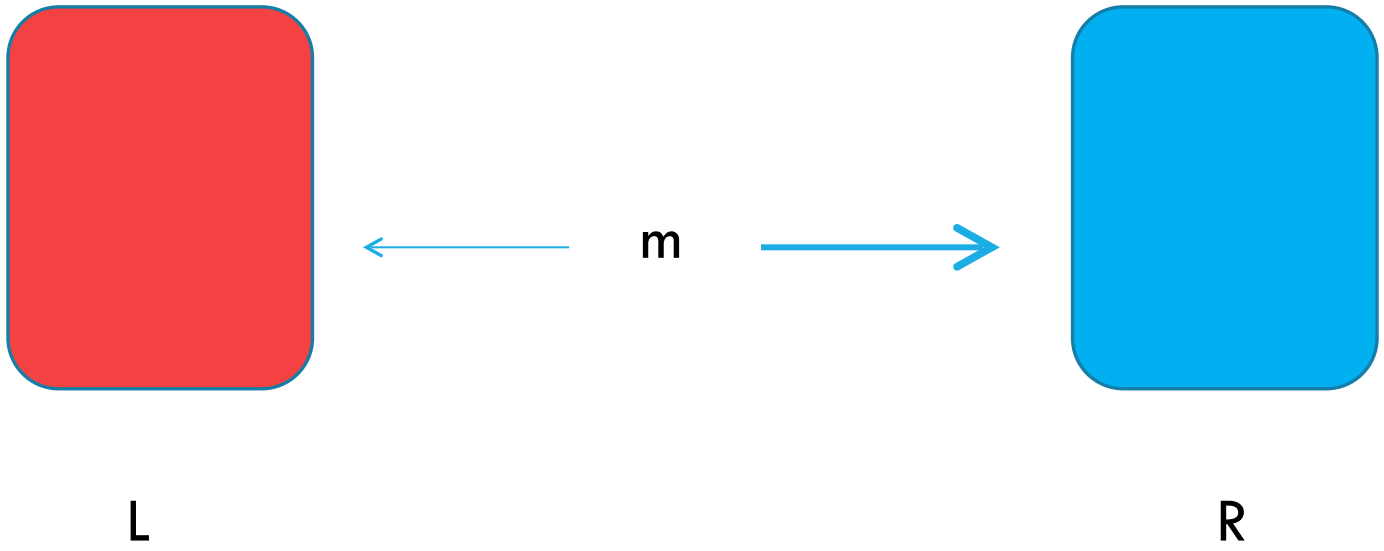
ENCRYPTION $\Longrightarrow$ EXTRACTION [BD07]

- Let K be some key sampled from the source used for encryption.
- They extract uniform randomness from $Enc(K, \mathbf{0})$
- Notice $Enc(K, \mathbf{0}) \approx Enc(K, U)$, where U is a uniform message
- $Enc(K, U)$ is a convex combination of $Enc(k, U)$, where key k is any fixed key in the key space.
- Correct decryption implies that $Enc(k, U)$ is a flat distribution over $2m$ ciphertexts.

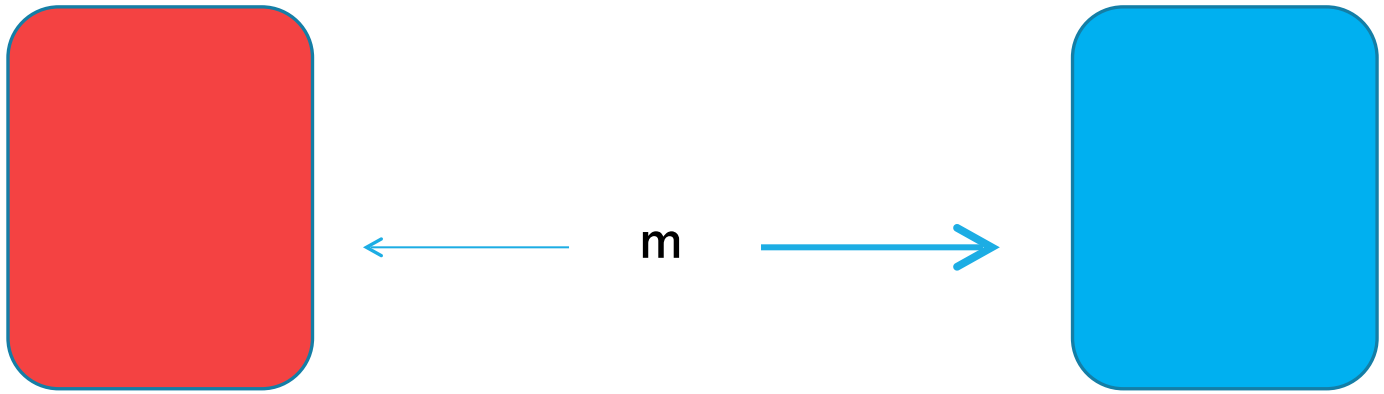
ENCRYPTION $\Longrightarrow$ EXTRACTION [BD07]

- Let K be some key sampled from the source used for encryption.
- They extract uniform randomness from $Enc(K, \mathbf{0})$
- Notice $Enc(K, \mathbf{0}) \approx Enc(K, U)$, where U is a uniform message
- $Enc(K, U)$ is a convex combination of $Enc(k, U)$, where key k is any fixed key in the key space.
- Correct decryption implies that $Enc(k, U)$ is a flat distribution over $2m$ ciphertexts.
- Extraction possible from a "not too large" number of flat distributions

2-OUT-OF-2 SECRET SHARING

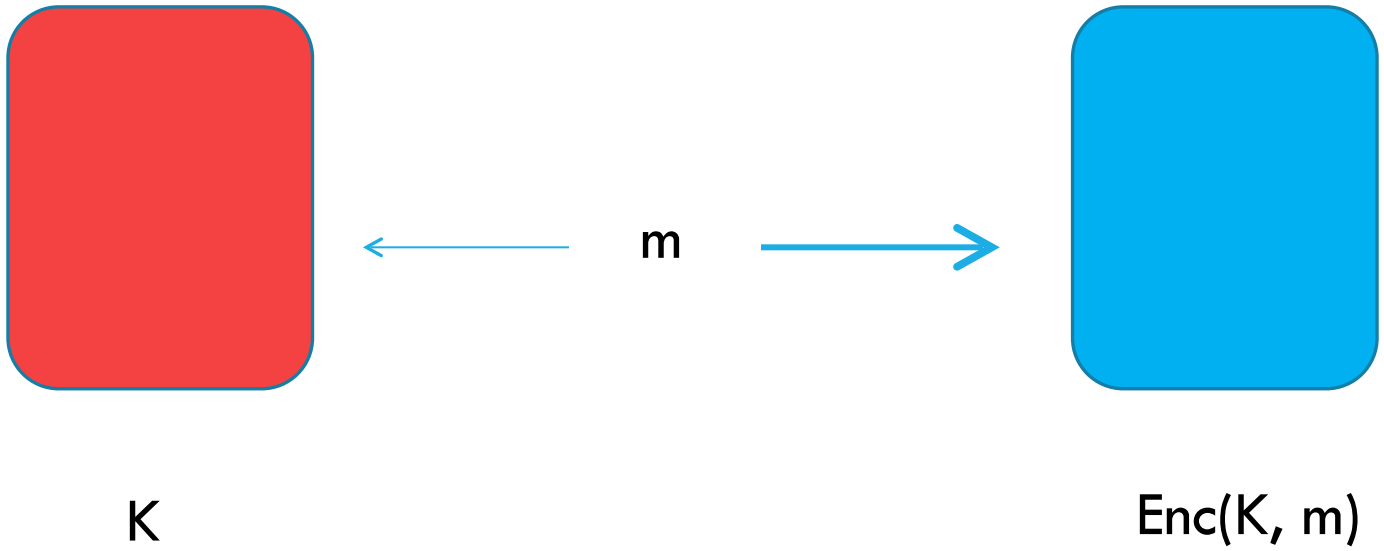


2-OUT-OF-2 SECRET SHARING

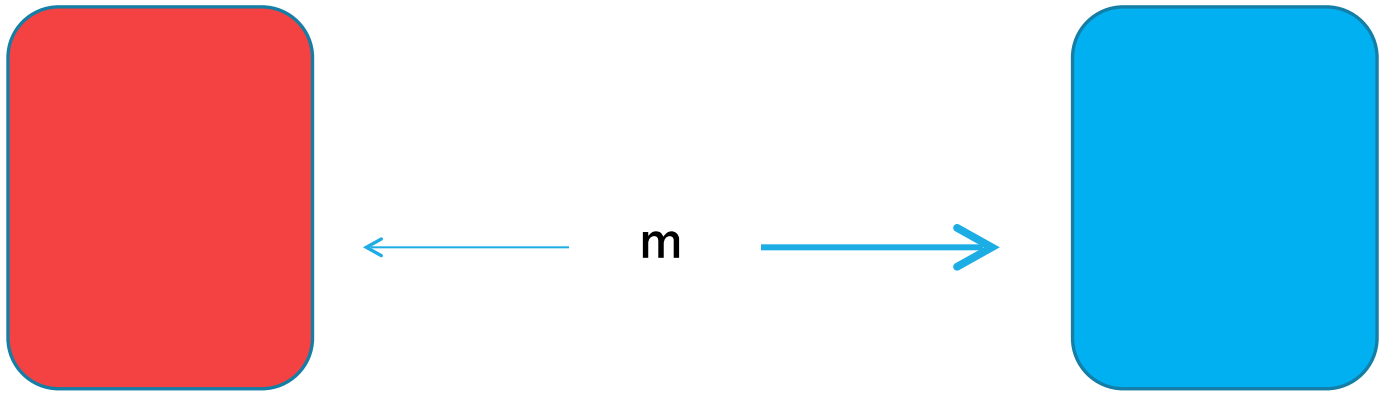


One of L, R does not reveal any information about m. Together, they can reconstruct m.

ENCRYPTION IS ALSO 2-OUT-OF-2 SECRET SHARING

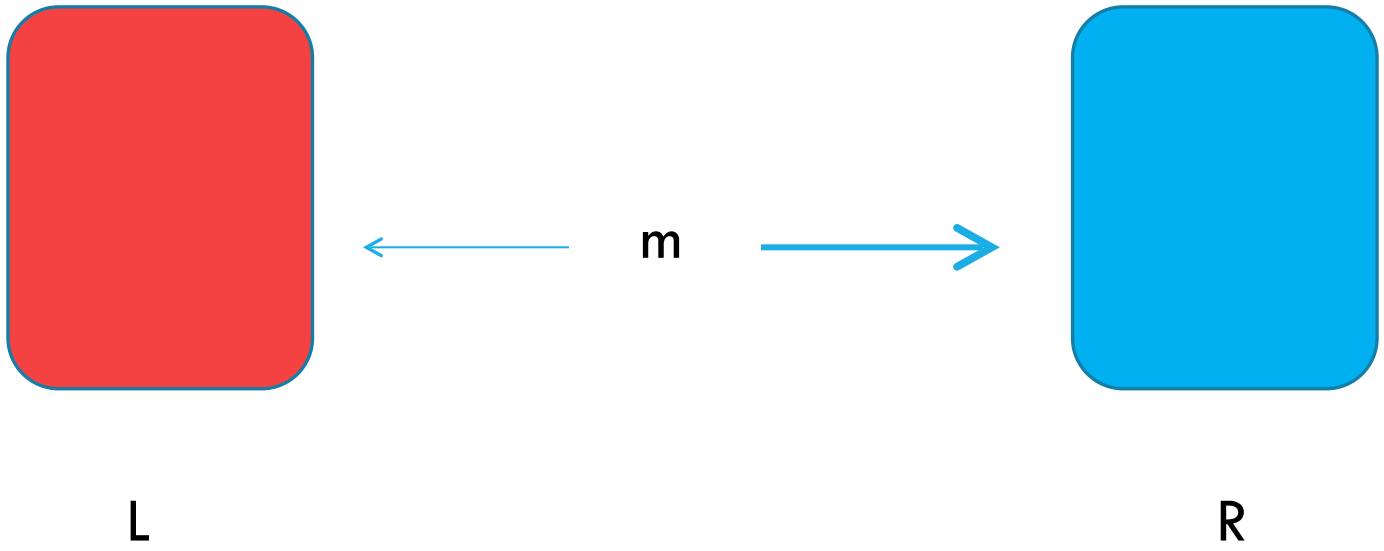


ENCRYPTION IS ALSO 2-OUT-OF-2 SECRET SHARING

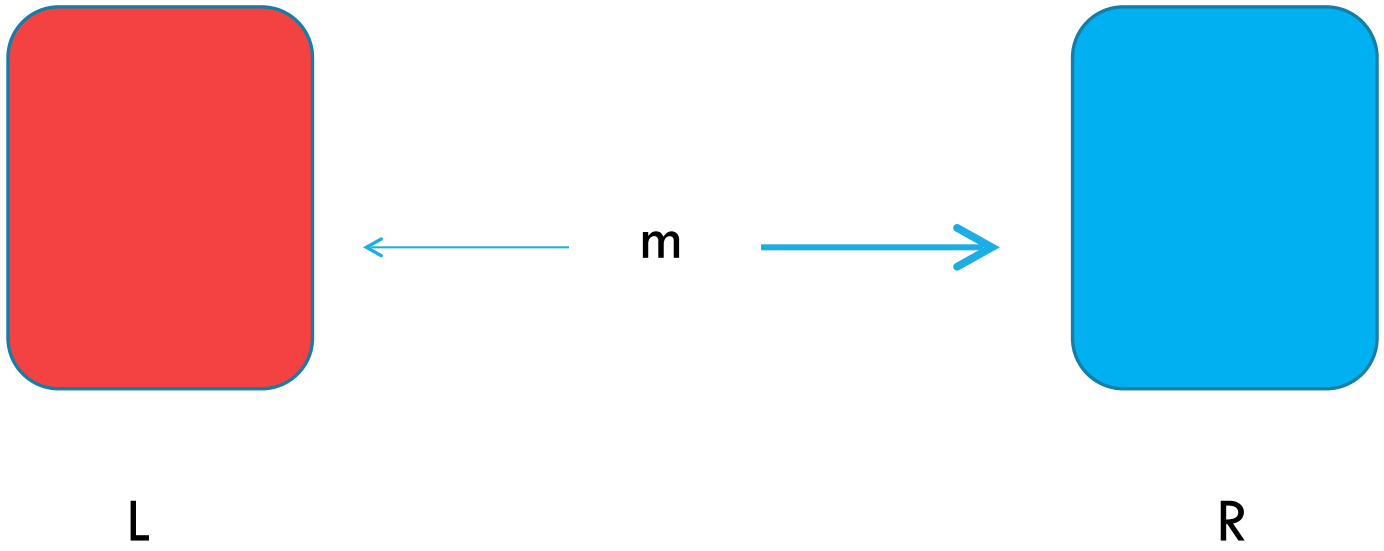


Cannot learn anything about m from any one of K, or Enc(K,m). Together, they determine m.

DOES 2-2 SECRET SHARING IMPLY EXTRACTION

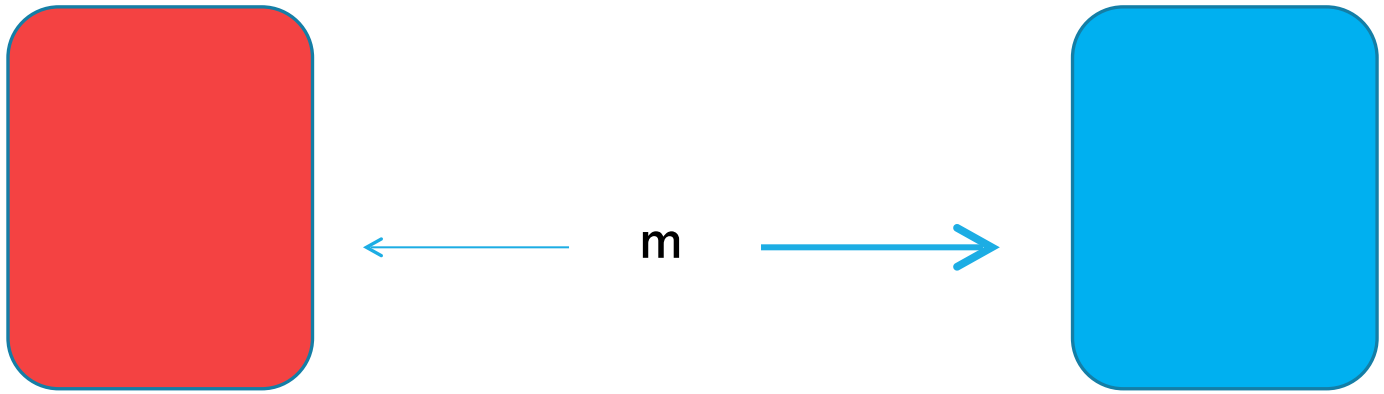


DOES 2-2 SECRET SHARING IMPLY EXTRACTION



Question: Does 2-out-of-2 secret sharing imply extraction? (Asked by [BD07])

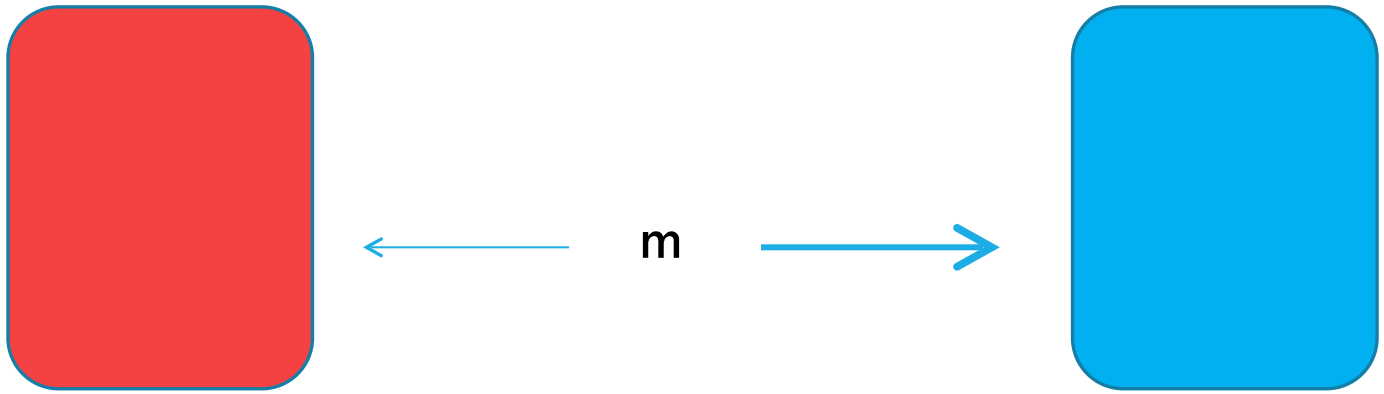
DOES 2-2 SECRET SHARING IMPLY EXTRACTION



Question: Does 2-out-of-2 secret sharing imply extraction? (Asked by [BD07])

How hard can this question be? [Me2012]

DOES 2-2 SECRET SHARING IMPLY EXTRACTION



Question: Does 2-out-of-2 secret sharing imply extraction? (Asked by [BD07])

How hard can this question be? [Me2012]

Quite Hard!! [Me2022]

EXPLAINING THE DIFFICULTY

- Suppose we use the same idea as encryption!

EXPLAINING THE DIFFICULTY

- Suppose we use the same idea as encryption!
- Suppose (similar to encryption) we try to extract from LeftShare(K, $\mathbf{0}$)

EXPLAINING THE DIFFICULTY

- Suppose we use the same idea as encryption!
- Suppose (similar to encryption) we try to extract from LeftShare(K, $\mathbf{0}$)
- We have that LeftShare(K, $\mathbf{0}$] $\approx$ LeftShare(K, U), where U is a uniform message

EXPLAINING THE DIFFICULTY

- Suppose we use the same idea as encryption!
- Suppose (similar to encryption) we try to extract from LeftShare(K, $\mathbf{0}$)
- We have that LeftShare(K, $\mathbf{0}$] $\approx$ LeftShare(K, U), where U is a uniform message
- LeftShare(K, U) is a convex combination of LeftShare(k, U), where key k is any fixed key in the key space.

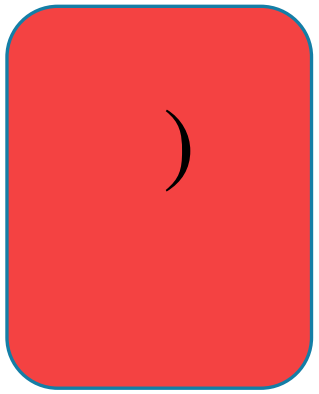
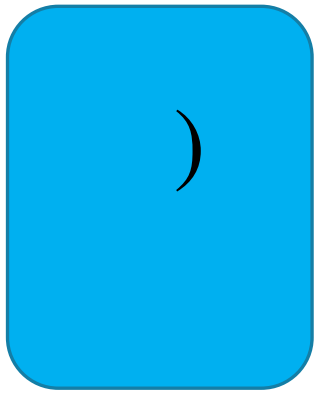
EXPLAINING THE DIFFICULTY

- Suppose we use the same idea as encryption!
- Suppose (similar to encryption) we try to extract from LeftShare(K, $\mathbf{0}$)
- We have that LeftShare(K, $\mathbf{0}$] $\approx$ LeftShare(K, U), where U is a uniform message
- LeftShare(K, U) is a convex combination of LeftShare(k, U), where key k is any fixed key in the key space.
- Unfortunately, LeftShare(k, U) might not have any entropy.

WE CONSIDER THIS QUESTION FOR LEAKAGE RESILIENT SECRET SHARING

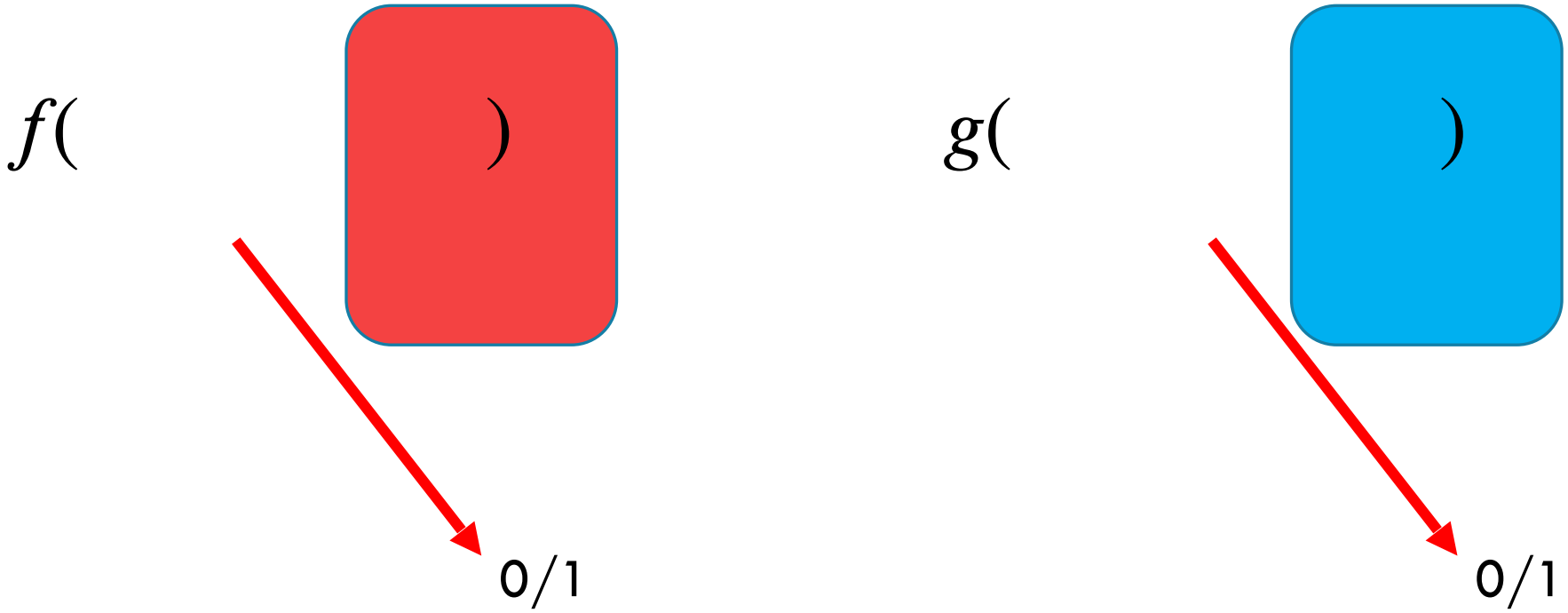
LEAKAGES:

Think about a model where information from two parts may be obtained, but separately.

$f($  $)$ $g($  $)$

LEAKAGES:

Think about a model where information from two parts may be obtained, but separately.



OUR RESULT: LRSS $\Longrightarrow$ EXTRACTION

- By XOR lemma, we can assume $f,\ g$ leak t bits, (error blows up by $2t$.)

OUR RESULT: LRSS $\Longrightarrow$ EXTRACTION

- By XOR lemma, we can assume $f,\ g$ leak t bits, (error blows up by $2t$.)
- We will extract uniform randomness from $f(K,\ \mathbf{0}),\ g(K, \mathbf{0})$

OUR RESULT: LRSS $\Longrightarrow$ EXTRACTION

- By XOR lemma, we can assume $f,\ g$ leak t bits, (error blows up by $2t$.)
- We will extract uniform randomness from $f(K,\ \mathbf{0}),\ g(K, \mathbf{0})$
- Notice $f(K,\ \mathbf{0}),\ g(K, \mathbf{0}) \approx f(K,\ U),\ g(K, U),$ where U is a uniform message

OUR RESULT: LRSS $\Longrightarrow$ EXTRACTION

- By XOR lemma, we can assume $f,\ g$ leak t bits, (error blows up by $2t$.)
- We will extract uniform randomness from $f(K,\ \mathbf{0}),\ g(K, \mathbf{0})$
- Notice $f(K,\ \mathbf{0}),\ g(K, \mathbf{0}) \approx f(K,\ U),\ g(K, U),$ where U is a uniform message
- $f(K,\ U),\ g(K, U)$ is a convex combination of $f(k,\ U),\ g(k,\ U)$ where key k is any fixed key in the key space.

OUR RESULT: LRSS $\Longrightarrow$ EXTRACTION

- By XOR lemma, we can assume $f,\ g$ leak t bits, (error blows up by $2t$.)
- We will extract uniform randomness from $f(K,\ \mathbf{0}),\ g(K, \mathbf{0})$
- Notice $f(K,\ \mathbf{0}),\ g(K, \mathbf{0}) \approx f(K,\ U),\ g(K, U),$ where U is a uniform message
- $f(K,\ U),\ g(K, U)$ is a convex combination of $f(k,\ U),\ g(k,\ U)$ where key k is any fixed key in the key space.
- We can choose $f,\ g,$ such that $f(k,\ U),\ g(k,\ U)$ have high min-entropy (non-trivial step)

OUR RESULT: LRSS $\Longrightarrow$ EXTRACTION

- By XOR lemma, we can assume $f,\ g$ leak t bits, (error blows up by $2t$.)
- We will extract uniform randomness from $f(K,\ \mathbf{0}),\ g(K, \mathbf{0})$
- Notice $f(K,\ \mathbf{0}),\ g(K, \mathbf{0}) \approx f(K,\ U),\ g(K, U),$ where U is a uniform message
- $f(K,\ U),\ g(K, U)$ is a convex combination of $f(k,\ U),\ g(k,\ U)$ where key k is any fixed key in the key space.
- We can choose $f,\ g,$ such that $f(k,\ U),\ g(k,\ U)$ have high min-entropy (non-trivial step)
- Extraction possible from a "not too large" number of min-entropy distributions

IMPLICATIONS FOR NON-MALLEABLE CODES

- A Non-malleable code in the split-state model have been studied extensively in the last decade.

IMPLICATIONS FOR NON-MALLEABLE CODES

- A Non-malleable code in the split-state model have been studied extensively in the last decade.

- An NMC is also a leakage-resilient secret sharing scheme.

IMPLICATIONS FOR NON-MALLEABLE CODES

- A Non-malleable code in the split-state model have been studied extensively in the last decade.
- An NMC is also a leakage-resilient secret sharing scheme.
- Non-malleable codes in the split-state model imply extraction

IMPLICATIONS FOR NON-MALLEABLE CODES

- A Non-malleable code in the split-state model have been studied extensively in the last decade.
- An NMC is also a leakage-resilient secret sharing scheme.
- Non-malleable codes in the split-state model imply extraction
- Contrast to the fact that AMD codes can be constructed from an entropy source.

PART 2: RANDOM-LESS REDUCTIONS

- Reducing crypto primitive A to B without additional randomness
    - Given a construction for A, we give a construction for B.

- If B requires an extractable source, we have that A also requires an extractable source.

PART 2: RANDOM-LESS REDUCTIONS

- Reducing crypto primitive A to B without additional randomness
    - Given a construction for A, we give a construction for B.

- If B requires an extractable source, we have that A also requires an extractable source.

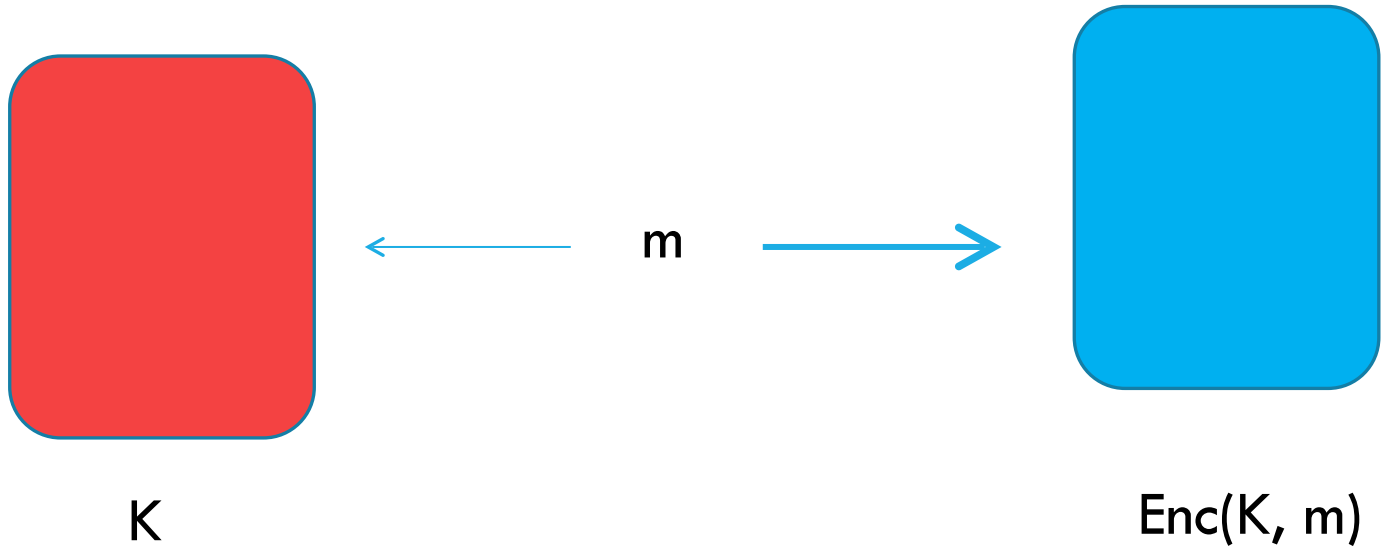
Example: Encryption
reduces to 2-out-of-2
secret sharing!

PART 2: RANDOM-LESS REDUCTIONS

- Reducing crypto primitive A to B without additional randomness
    - Given a construction for A, we give a construction for B.

- If B requires an extractable source, we have that A also requires an extractable source.

Example: Encryption reduces to 2-out-of-2 secret sharing!



PART 2: RANDOM-LESS REDUCTIONS

- Question: For what $n,\ t,\ n',\ t'$ can (n, t) secret sharing be converted to (n', t') secret sharing without additional randomness

PART 2: RANDOM-LESS REDUCTIONS

- Question: For what $n,\ t,\ n',\ t'$ can (n, t) secret sharing be converted to (n', t') secret sharing without additional randomness

- We show many different reductions for different choices of $n,\ t,\ n',\ t'$.

PART 2: RANDOM-LESS REDUCTIONS

- Question: For what $n,\ t,\ n',\ t'$ can (n, t) secret sharing be converted to (n', t') secret sharing without additional randomness

- We show many different reductions for different choices of $n,\ t,\ n',\ t'$.

    - A simple example is $n' = t' = 2$. The reduction will give $t - 1$ different shares to one party, and any one other share to the second

PART 2: RANDOM-LESS REDUCTIONS

- Question: For what $n,\ t,\ n',\ t'$ can (n, t) secret sharing be converted to (n', t') secret sharing without additional randomness

- We show many different reductions for different choices of $n,\ t,\ n',\ t'$.

    - A simple example is $n' = t' = 2$. The reduction will give $t - 1$ different shares to one party, and any one other share to the second

Motivates distribution designs: Distribute n shares into n' sets such that any t sets contain t' shares, and less than t sets contain less than t' shares.

DISTRIBUTION DESIGNS

- We find distribution designs for several different choices of $n,\ t,\ n',\ t'$
- In some cases, these designs are tight and cannot be improved.

CONCLUSIONS

- If 2-out-of-2 secret sharing implies extraction, then
    - t-out-of-n threshold secret sharing implies extraction for any $t,\ n$
    - So, extracting from 2-out-of-2 SS might be harder.

CONCLUSIONS

- If 2-out-of-2 secret sharing implies extraction, then
    - t-out-of-n threshold secret sharing implies extraction for any $t,\ n$
    - So, extracting from 2-out-of-2 SS might be harder.

Hopefully, our work motivates our main open question: Can we extract randomness from a t out of n secret sharing scheme for any t, n ?

THANK YOU!

Questions?