Sufficiently myopic adversaries are blind

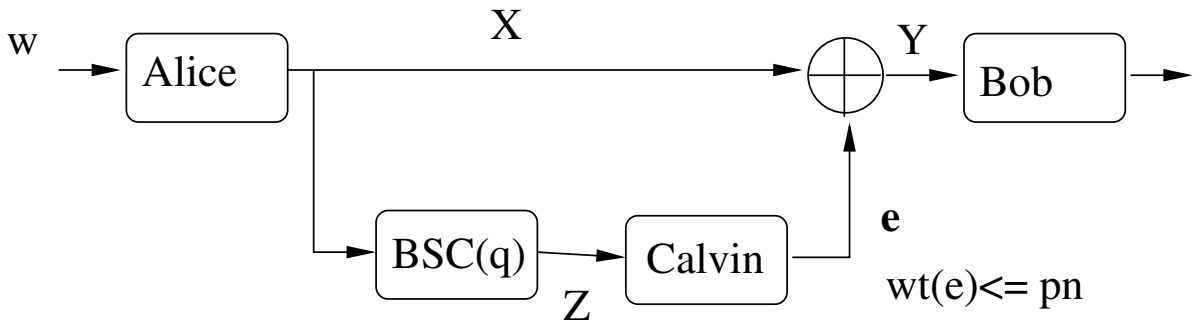
Bikash Kumar Dey

Indian Institute of Technology Bombay

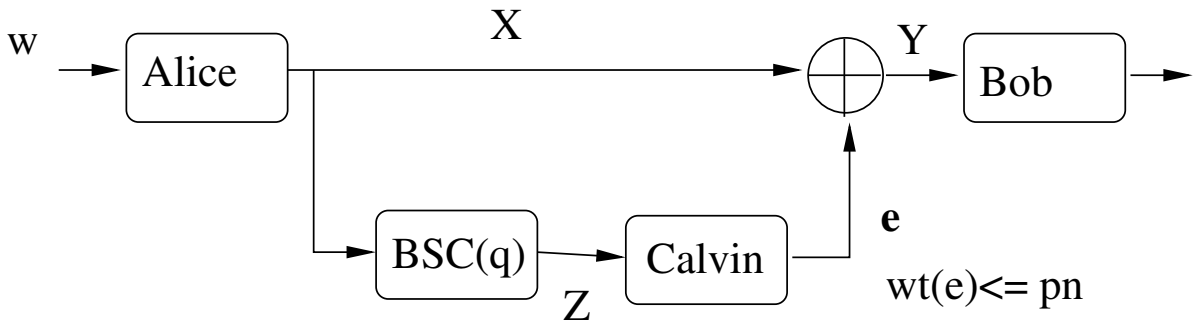
Banff: March 2, 2015

Joint work with
Sidharth Jaggi (CUHK), Michael Langberg (SUNY Buffalo)

Model



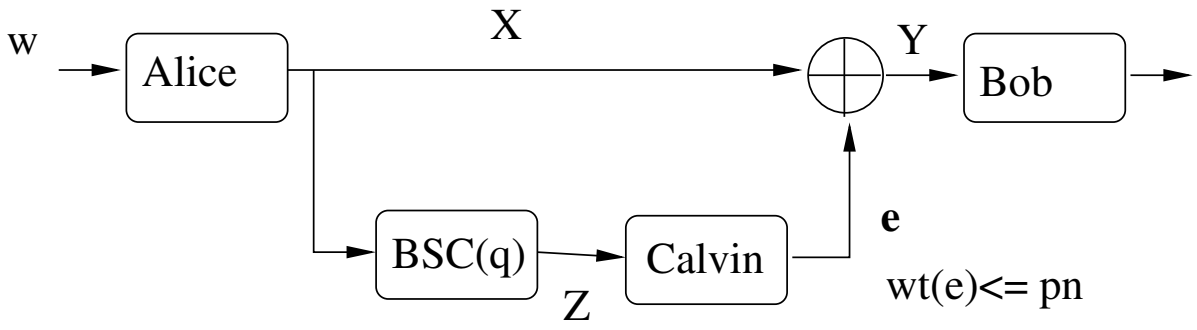
Model



Encoding:

- Random coding (shared randomness): Anand's myopic work
- Deterministic codes - focus of this work
- Performance metric: average error probability

Model



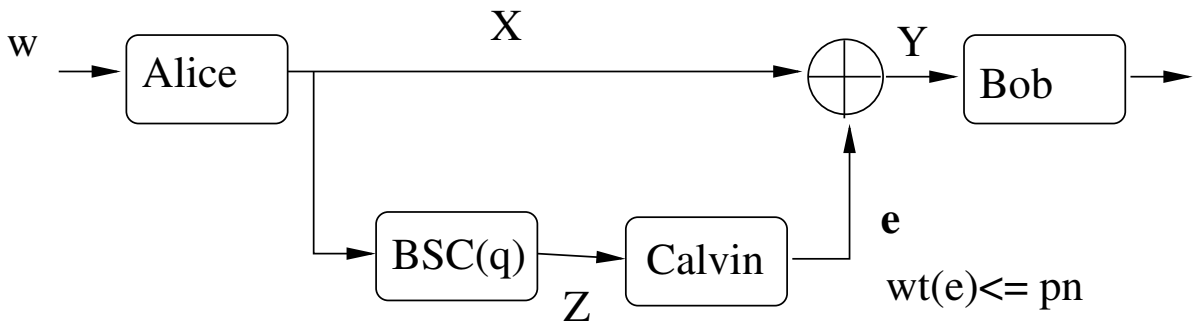
Encoding:

- Random coding (shared randomness): Anand's myopic work
- Deterministic codes - focus of this work
- Performance metric: average error probability

Special cases:

- $q = 1$: Calvin is oblivious ($C = 1 - H(p)$)
- $q = 0$: Calvin is omniscient
- $q < p$: Calvin is omniscient under deterministic coding
- $q > p$: "sufficiently myopic" (our result: $C = 1 - H(p)$)

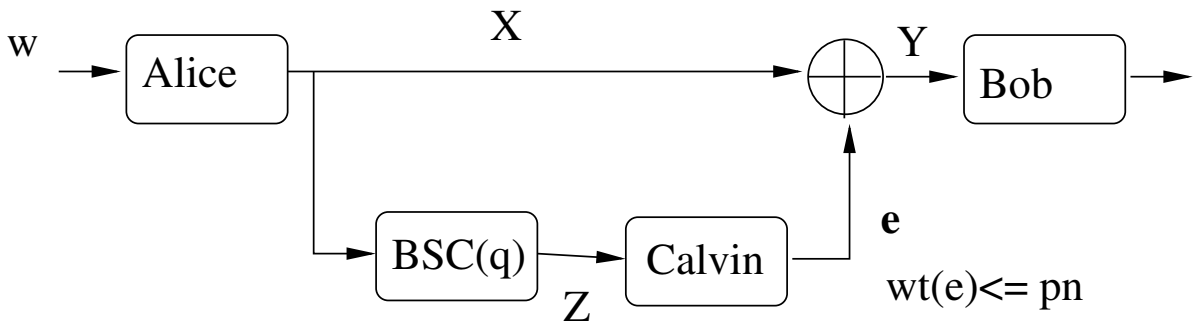
Capacity



When $q > p$,

$$C = 1 - H(p)$$

Capacity



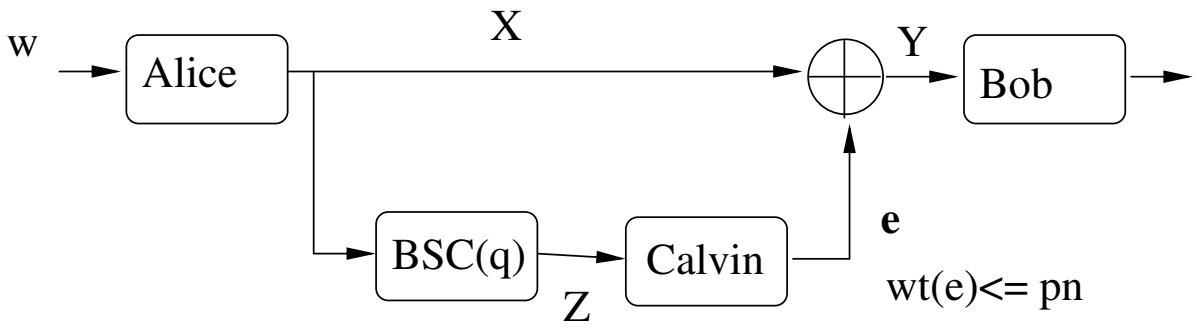
When $q > p$,

$$C = 1 - H(p)$$

Converse: follows from the converse for BSC(p).

- Calvin can simulate BSC($p - \epsilon$) for any ϵ.

Capacity



When $q > p$,

$$C = 1 - H(p)$$

Converse: follows from the converse for BSC(p).

- Calvin can simulate BSC($p - \epsilon$) for any ϵ.

Achievability: using random code construction

- $R = 1 - H(p) - \epsilon$.
- Pick codewords $X(w) : w = 1, 2, \cdots 2^{nR}$ uniformly at random from $\{0, 1\}^n$.
- *Encoding:* $w \mapsto X(w)$
- *Decoding:* Find $\hat{w}$ such that $d(X(\hat{w}), y) \leq pn$. Declare error if $\hat{w}$ is not unique.

A list decoding lemma

List decoding property [Langberg 2008]

Let c be a large enough constant. With high probability ($\geq 1 - 2^{cn^2}$) over the code, for every sphere B of radius np, there are at most $2cn^2$ codewords in it.

A list decoding lemma

List decoding property [Langberg 2008]

Let c be a large enough constant. With high probability ($\geq 1 - 2^{cn^2}$) over the code, for every sphere B of radius np, there are at most $2cn^2$ codewords in it.

Proof outline:

- Consider any sphere and use Chernoff bound.
- Take union bound over the exponentially many spheres.

A list decoding lemma

List decoding property [Langberg 2008]

Let c be a large enough constant. With high probability ($\geq 1 - 2^{cn^2}$) over the code, for every sphere B of radius np, there are at most $2cn^2$ codewords in it.

Proof outline:

- Consider any sphere and use Chernoff bound.
- Take union bound over the exponentially many spheres.

Remark/Extension:

- The result holds if instead of spheres, we take any subset of 'small' volume such that the expected no. of codewords is $\mu < cn^2$. In particular, take μ exponentially small.
- as long as the number of subsets is only exponential.

A list decoding lemma

List decoding property [Langberg 2008]

Let c be a large enough constant. With high probability ($\geq 1 - 2^{cn^2}$) over the code, for every sphere B of radius np, there are at most $2cn^2$ codewords in it.

Proof outline:

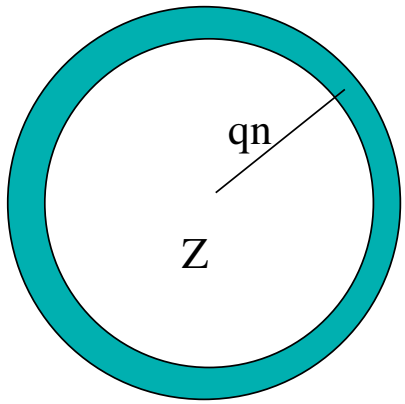
- Consider any sphere and use Chernoff bound.
- Take union bound over the exponentially many spheres.

Remark/Extension:

- The result holds if instead of spheres, we take any subset of 'small' volume such that the expected no. of codewords is $\mu < cn^2$. In particular, take μ exponentially small.
- as long as the number of subsets is only exponential.

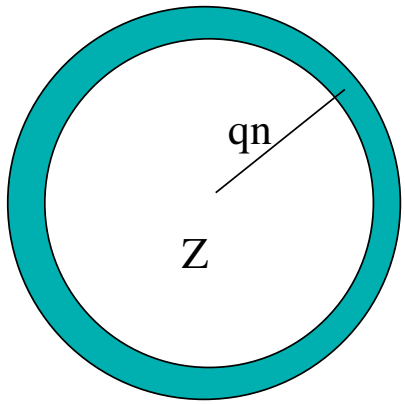
We will assume that the code satisfies this list decoding property.

What is known to Clavin



Definition: $r = d(X(w), Z)$

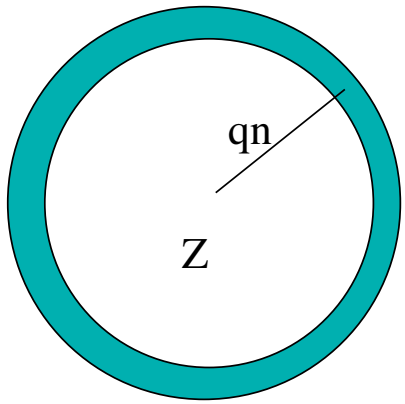
What is known to Clavin



Definition: $r = d(X(w), Z)$
What Calvin knows

- Clavin knows Z.
- Calvin 'knows' that $|r - qn| \leq \delta n$.

What is known to Clavin



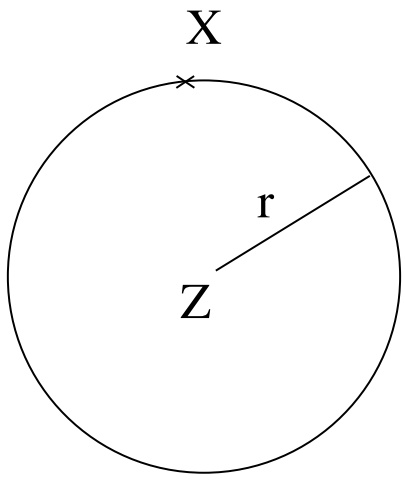
Definition: $r = d(X(w), Z)$
What Calvin knows

- Clavin knows Z.
- Calvin 'knows' that $|r - qn| \leq \delta n$.

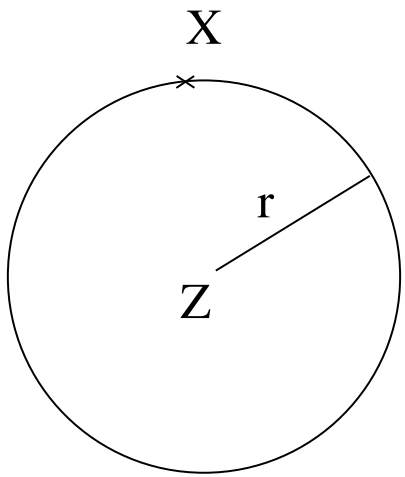
Genie reveals to Calvin

- r

The helpful genie

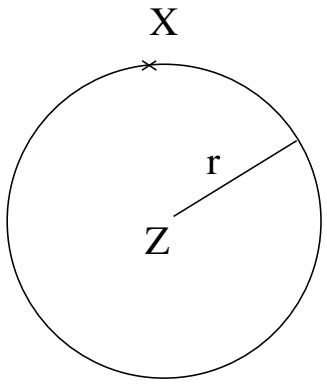


The helpful genie

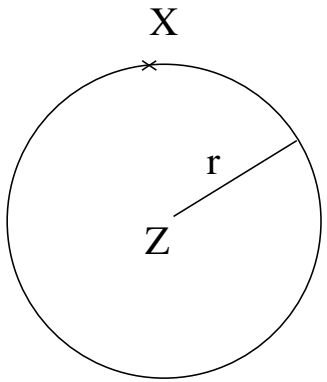


- Volume of this shell $= 2^{nH(r/n)} \in (2^{n(H(q)-\delta_1)}, 2^{n(H(q)+\delta_2)})$ for some $\delta_1 = h_1(\delta), \delta_2 = h_2(\delta)$.
- Expected number of codewords on this shell: $\mu(r) = 2^{n(H(r/n)-H(p)-\epsilon)}$.
- With high probality, for every z, r, $|C \cap Sh(z, r)| \in (\mu(r)/2, 2\mu(r))$.
- The genie partitions these messages (for every z, r) into sets of equal size $2^{n\epsilon/2}$ (except for the last set.) This is done *deterministically*.
- There are exponentially many such sets.
- The **genie reveals the partition** in which the encoded message belongs.

Analysis



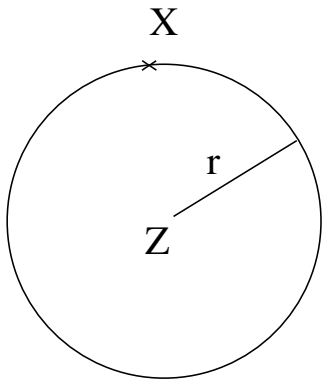
Analysis



We assume

- The code satisfies the list decoding property
- For every $z, r \approx qn$, $|C \cap Sh(z, r)| \in (\mu(r)/2, 2\mu(r))$.

Analysis



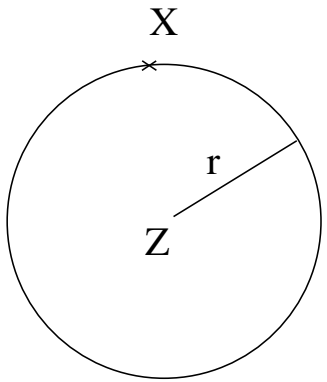
We assume

- The code satisfies the list decoding property
- For every $z, r \approx qn$, $|C \cap Sh(z, r)| \in (\mu(r)/2, 2\mu(r))$.

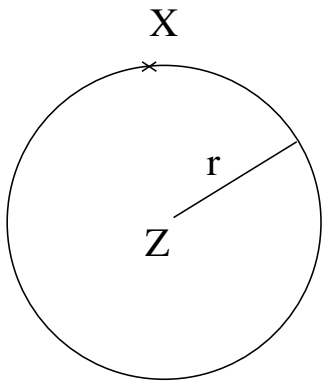
Fix z, r

- Take every possible realization of the messages in $C \cap Sh(z, r)$.
- There are exponentially many partitions of them.
- Take each of them, call the chosen one as S_0.
- All other messages in $C \cap Sh(z, r)$ are in S_1.
- All messages not in $C \cap Sh(z, r)$ are in S_2.

Analysis



Analysis

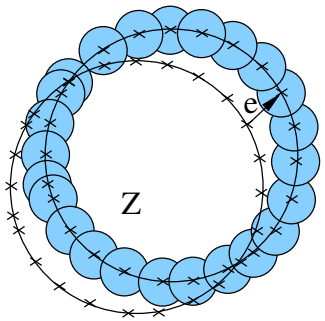


Fix z, r, e.
For every realization of $C \cap Sh(z, r)$, every S_0 in it, we will analyze how many messages in it are confusable by e with another message in S_0, S_1 or S_2.
We will show that, w.h.p.,

- $\leq 4c^2n^4$ messages in S_0 confusable with S_2.
- $\leq 4c^2n^4$ messages in S_0 confusable with S_2.
- $\leq 4c^2n^4 2^{n\epsilon/4}$ messages in S_0 confusable with S_2.

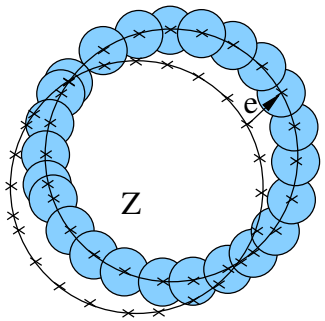
- exponentially small fraction is confusable

Confusion with S_2



- $\{X(w) : w \in S_2\}$ are uniformly distributed in $\{0,1\}^n \setminus Sh(z,r)$ - volume $\geq 2^n - 2^{n(H(q)+\delta_2)} \geq 2^{n-1}$.
- How many $w \in S_0$ are confusable with S_2?

Confusion with S_2

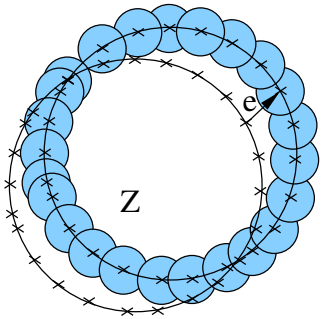


- $\{X(w) : w \in S_2\}$ are uniformly distributed in $\{0,1\}^n \setminus Sh(z,r)$ - volume $\geq 2^n - 2^{n(H(q)+\delta_2)} \geq 2^{n-1}$.
- How many $w \in S_0$ are confusable with S_2?

Count in two steps:

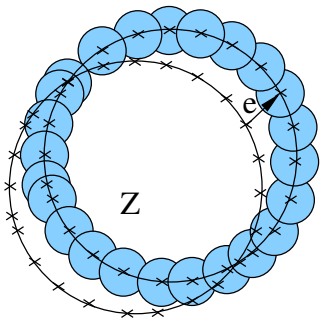
- Number of codewords from S_2 falling in the blob.
  - Blob volume $2^{n(H(p)+\epsilon/2)}$
  - Expected number of codewords in the blob $= 2^{-n\epsilon/2}$
  - List decoding lemma: there are at most cn^2 codewords in the blob with 'very high' probability
- For each $w' \in S_2$, how many codewords in S_0 can it confuse? - at most cn^2 by the list decoding property.
- w.h.p., at most c^2n^4 codewords in S_0 are confusable with S_2.

Confusion with S_1



- $\{X(w) : w \in S_1\}$ are uniformly distributed in $Sh(z, r)$ - volume of $\geq 2^{n(H(q)-\delta_1)} \geq 2^{n-1}$.
- How many $w \in S_0$ are confusable with S_1?

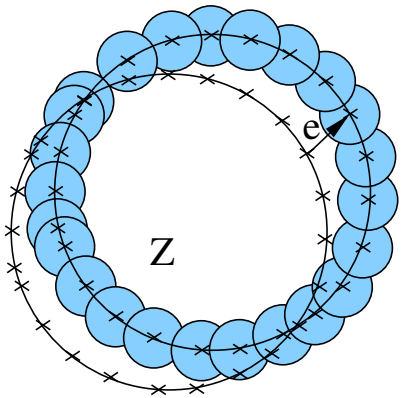
Confusion with S_1

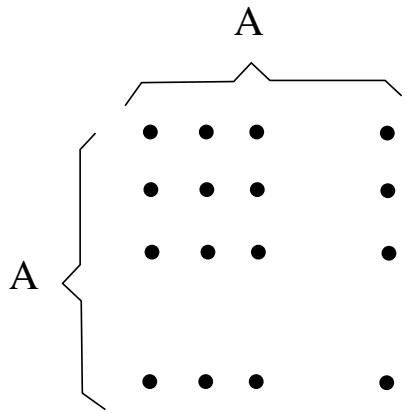


- $\{X(w) : w \in S_1\}$ are uniformly distributed in $Sh(z, r)$ - volume of $\geq 2^{n(H(q)-\delta_1)} \geq 2^{n-1}$.
- How many $w \in S_0$ are confusable with S_1?

Count in two steps as for S_2.

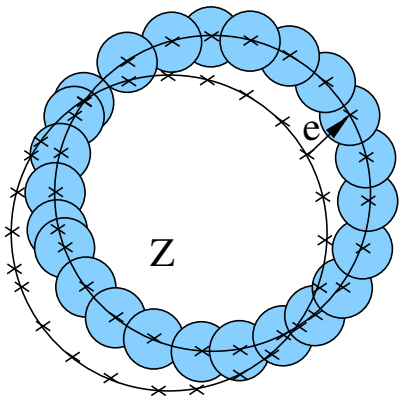
Confusion with S_0

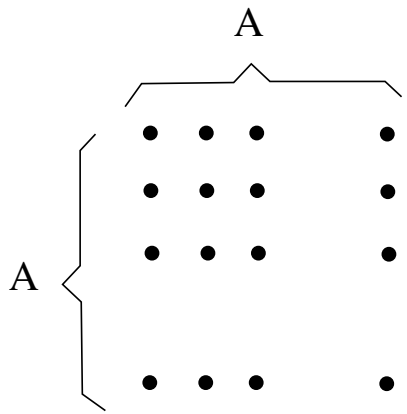




Arrange S_0 in square arrangement as $A \times A$. $|A| = 2^{n\epsilon/2}$.

Confusion with S_0

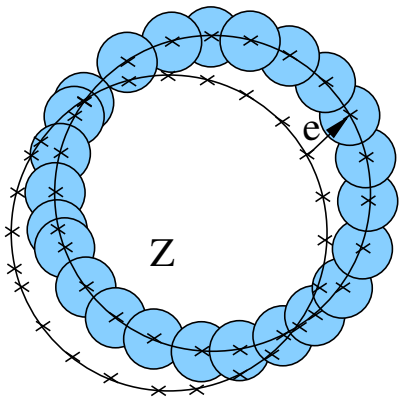


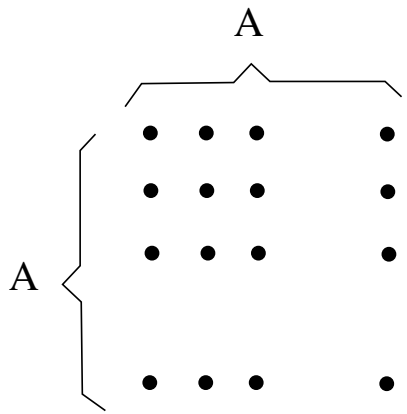


Arrange S_0 in square arrangement as $A \times A$. $|A| = 2^{n\epsilon/2}$.

- How many messages in a row (resp. column) are confusable with some message outside that row (resp. column)?
- at most cn^2 with 'very high' probability.

Confusion with S_0



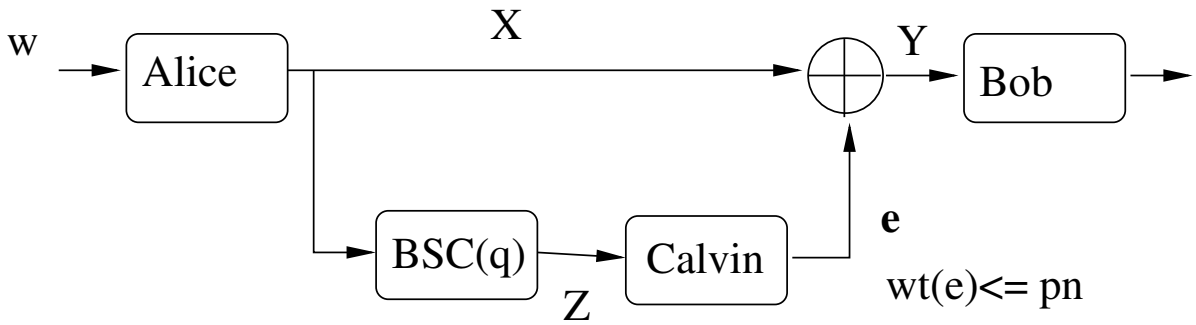


Arrange S_0 in square arrangement as $A \times A$. $|A| = 2^{n\epsilon/2}$.

- How many messages in a row (resp. column) are confusable with some message outside that row (resp. column)?
- at most cn^2 with 'very high' probability.

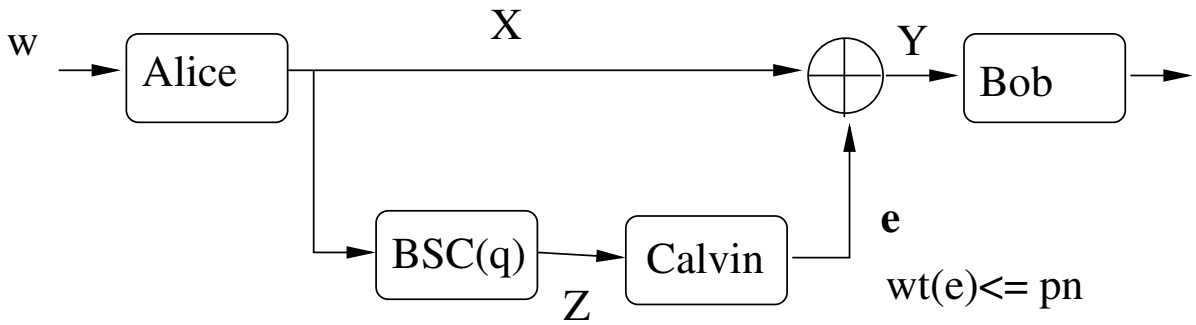
- Define a directed graph of confusability under e.
- In each row (resp. column), there are at most cn^2 nodes with non-zero non-horizontal (resp. non-vertical) out-degree.
- Total number of nodes with non-zero non-horizontal out-degree $\leq cn^2|A|$
- Total number of nodes with non-zero out-degree $\leq 2cn^2|A|$ - exponentially small fraction

Secret message transmission



- $C = H(q) - H(p)$
- Encode message $(H(q) - H(p))$and artificial noise $(1 - H(q))$ using a random code.

Secret message transmission



- $C = H(q) - H(p)$
- Encode message $(H(q) - H(p))$and artificial noise $(1 - H(q))$ using a random code.

Thank You