# Tail bounds and applications in Cryptography

Giorgos Panagiotakos

Introduction to Modern Cryptography
Course Organizer: Prof. Aggelos Kiayias

October 26, 2016

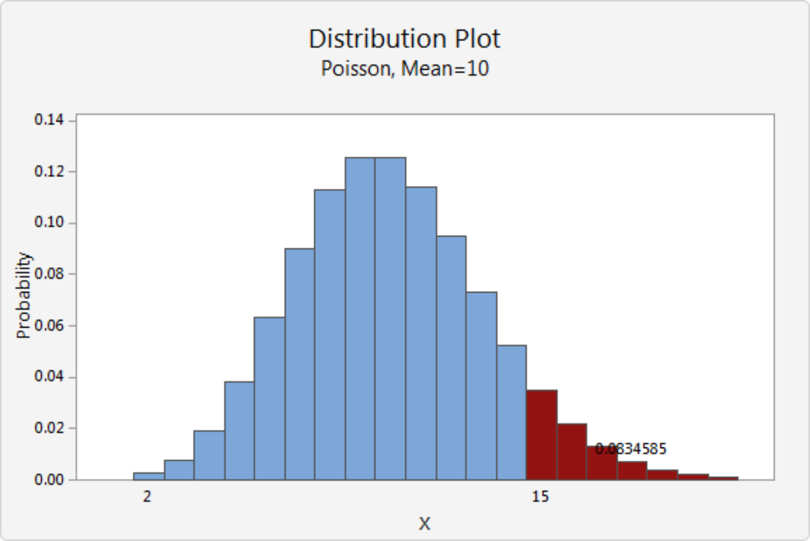



Figure: http://support.minitab.com/en-us/minitab-express/1/distribution_plot_poisson_shade_right_tail.xml_Graph_cmd1o1.png

# Discrete probability space

For some random experiment we define:

**Definition (Discrete probability space)**

$\hat{\Omega} = (\Omega, \{p_\omega\}_{\omega \in \Omega})$ is a probability space where

- $\Omega$ is the set of outcomes
- $p_\omega \geq 0, \ \forall \omega \in \Omega$
- $\sum_{\omega \in \Omega} p_\omega = 1$

# Discrete probability space

For some random experiment we define:

Definition (Discrete probability space)

$\hat{\Omega} = (\Omega, \{p_\omega\}_{\omega \in \Omega})$ is a probability space where

- $\Omega$ is the set of outcomes
- $p_\omega \geq 0, \; \forall \omega \in \Omega$
- $\sum_{\omega \in \Omega} p_\omega = 1$

Bernoulli trial

# Discrete probability space

For some random experiment we define:

## Definition (Discrete probability space)

$\hat{\Omega} = (\Omega, \{p_\omega\}_{\omega \in \Omega})$ is a probability space where

- $\Omega$ is the set of outcomes
- $p_\omega \geq 0, \ \forall \omega \in \Omega$
- $\sum_{\omega \in \Omega} p_\omega = 1$

## Bernoulli trial

- $\Omega = \{success, fail\}$
- $p_{success} = p$
- $p_{fail} = 1 - p$

# Events

## Definition (Event)

- An event $E$ is a subset of $\Omega$.
- $Pr[E] = \sum_{\omega \in E} p_\omega$

# Events

## Definition (Event)

- An event $E$ is a subset of $\Omega$.
- $Pr[E] = \sum_{\omega \in E} p_\omega$

## Example

# Events

## Definition (Event)

- An event $E$ is a subset of $\Omega$.
- $Pr[E] = \sum_{\omega \in E} p_\omega$

## Example

- $Pr[\{\}] = 0$
- $Pr[\{success\}] = p$
- $Pr[\{fail\}] = 1 - p$
- $Pr[\{success, fail\}] = p + (1 - p) = 1$

# Random Variable

### Definition (Random variable)

A random variable in $\hat{\Omega}$ is a function $X : \Omega \to \mathbb{R}$.

### Definition (Expectation)

The expectation of $X$ is $E[X] = \sum_{\omega \in \Omega} X(\omega) \cdot p_\omega$

# Random Variable

## Definition (Random variable)

A random variable in $\hat{\Omega}$ is a function $X : \Omega \rightarrow \mathbb{R}$.

## Definition (Expectation)

The expectation of $X$ is $E[X] = \sum_{\omega \in \Omega} X(\omega) \cdot p_\omega$

## Bernoulli random variable

# Random Variable

**Definition (Random variable)**

A random variable in $\hat{\Omega}$ is a function $X : \Omega \to \mathbb{R}$.

**Definition (Expectation)**

The expectation of $X$ is $E[X] = \sum_{\omega \in \Omega} X(\omega) \cdot p_\omega$

**Bernoulli random variable**

- $X(success) = 1$
- $X(fail) = 0$
- $E[X] = 0 \cdot (1 - p) + 1 \cdot p = p$

# Random Variable

## Linearity of Expectation

For any two random variables $X, Y$ it holds that

$$E[X+Y] = E[X] + E[Y]$$

# Random Variable

## Linearity of Expectation

For any two random variables $X, Y$ it holds that

$$E[X + Y] = E[X] + E[Y]$$

## Example

# Random Variable

## Linearity of Expectation

For any two random variables $X, Y$ it holds that

$$E[X + Y] = E[X] + E[Y]$$

## Example

- $X_1, \dots, X_n$ are Bernoulli random variables.
- $E[X_i] = p$
- $E[\sum_{i=1}^{n} X_i] = \sum_{i=1}^{n} E[X_i] = np$

# Binomial random variable

## Definition (Binomial r.v.)

$B(n, p)$ is the r.v. of the number of successes in $n$ independent Bernoulli trials with probability of success $p$.

# Binomial random variable

## Definition (Binomial r.v.)

$B(n, p)$ is the r.v. of the number of successes in $n$ independent Bernoulli trials with probability of success $p$.

## Binomial random variable

- $X_1, \ldots, X_n$ are independent Bernoulli random variables.
- $X = \sum_{i=1}^{n} X_i$ is $B(n, p)$
- $E[X] = np$
- $Pr[X = k] = \binom{n}{k} p^k (1-p)^{n-k}$

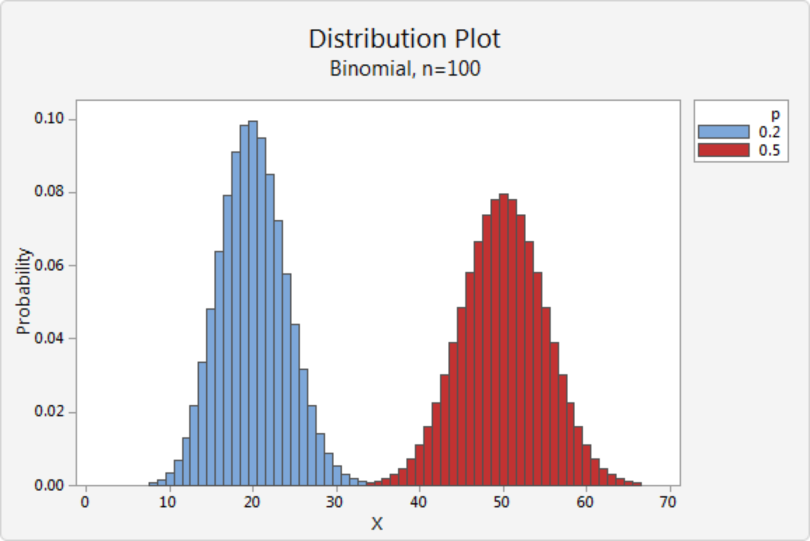
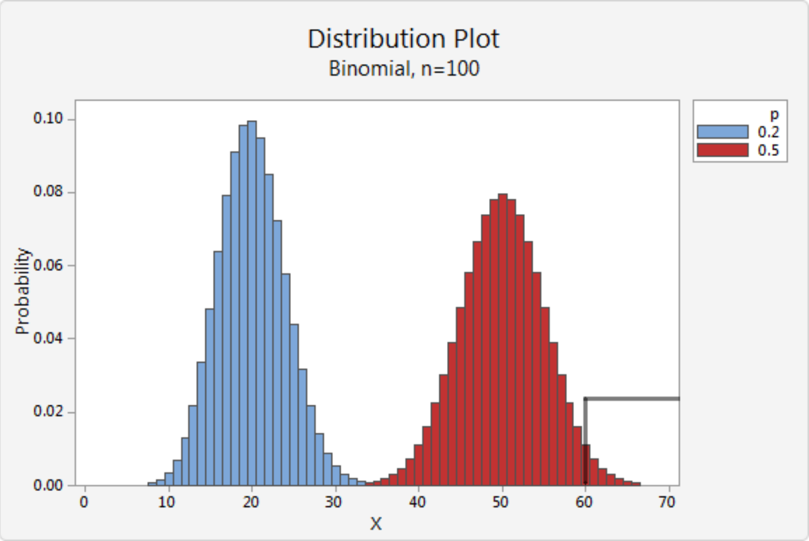



Figure: http://support.minitab.com/en-us/minitab-express/1/distribution_plot_binary_vary_parameters.xml_Graph_cmd1o1.png

# Tail bounds



Distribution Plot
Binomial, n=100
Probability
0.10
0.08
0.06
0.04
0.02
0.00
0
10
20
30
40
50
60
70
X
p
0.2
0.5

# Markov's inequality

## Markov's inequality

For any r.v. $X$ that takes only non-negative values, for any $t > 0$:

$$Pr[X \geq t] \leq \frac{E[X]}{t}$$

# Markov's inequality

## Markov's inequality

For any r.v. $X$ that takes only non-negative values, for any $t > 0$:

$$Pr[X \geq t] \leq \frac{E[X]}{t}$$

## Example

# Markov's inequality

## Markov's inequality

For any r.v. $X$ that takes only non-negative values, for any $t > 0$:

$$Pr[X \geq t] \leq \frac{E[X]}{t}$$

## Example

- $X \sim B(n, p)$
- $Pr[X \geq \frac{6E[X]}{5}] = Pr[X \geq \frac{6np}{5}] \leq \frac{E[X]}{\frac{6}{5}E[X]} = 5/6$

# Chernoff's bound

Let $X_1, \ldots, X_n$ be independent random variables taking values in $\{0, 1\}$ and $Pr[X_i = 1] = p_i$. Then for any $\delta \in (0, 1)$ and $\mu = \sum_{i=1}^{n} p_i$ it holds that:

$$Pr[\sum_{i=1}^{n} X_i \leq (1-\delta)\mu] \leq e^{-\mu\delta^2/2}$$

*and*

$$Pr[\sum_{i=1}^{n} X_i \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}$$

# Chernoff's bound

Let $X_1, \ldots, X_n$ be independent random variables taking values in $\{0,1\}$ and $Pr[X_i = 1] = p_i$. Then for any $\delta \in (0,1)$ and $\mu = \sum_{i=1}^n p_i$ it holds that:

$$Pr[\sum_{i=1}^{n} X_i \leq (1-\delta)\mu] \leq e^{-\mu\delta^2/2}$$

*and*

$$Pr[\sum_{i=1}^{n} X_i \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}$$

## Example

# Chernoff's bound

Let $X_1, \ldots, X_n$ be independent random variables taking values in $\{0, 1\}$ and $Pr[X_i = 1] = p_i$. Then for any $\delta \in (0, 1)$ and $\mu = \sum_{i=1}^{n} p_i$ it holds that:

$$Pr[\sum_{i=1}^{n} X_i \leq (1-\delta)\mu] \leq e^{-\mu\delta^2/2}$$

*and*

$$Pr[\sum_{i=1}^{n} X_i \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}$$

## Example

- $X \sim B(n, p)$
- $Pr[X \geq \frac{6E[X]}{5}] = Pr[X \geq (1 + 1/5)\mu] \leq e^{-np/75}$

# Markov vs. Chernoff's bound

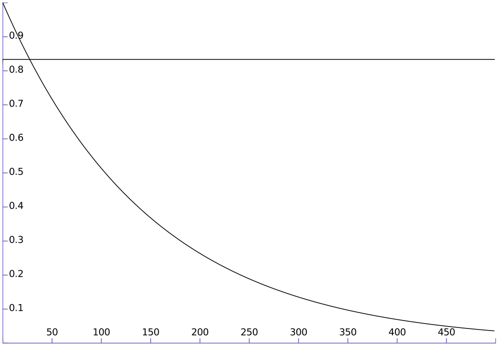



Figure: $5/6$ vs. $e^{-n0.5/75}$

# Markov vs. Chernoff's bound

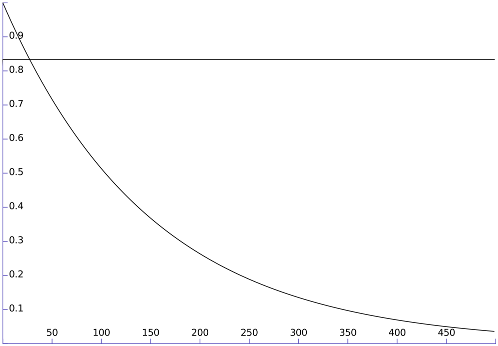



Figure: $5/6$ vs. $e^{-n0.5/75}$

- Chernoff's bound goes **exponentially** fast to 0.
- Markov's bound does not take in account neither the independence nor the number of the random variables.
- **Caveat**: For Chernoff's bound independence and boundedness of the summands is needed.

# Application: Bitcoin

# Cryptocurrency

*A cryptocurrency is a medium of exchange using cryptography to secure the transactions and to control the creation of new units.*

## Main properties

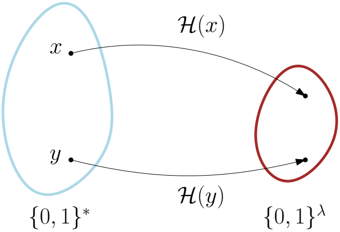
- Trust Distribution
- Verifiability
- Pseudonimity/Anonymity/Traceability

# Bitcoin

*Currently most popular cryptocurrency.*

- Introduced by Nakamoto in 2008.
- 1 BTC = \$650 (\$290 last time I used this slide)
- Hash rate: 1.6 Exa Hashes/sec (0.35 last time)
- Distributed public ledger of transactions open to anyone
- Proof of Work vs. Sybil Attacks
- Pseudonymous

# Hash functions




- $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$
- Easy to compute
- Collision resistant: hard to find two inputs that are mapped to the same output

# Hash functions

## Collision Resistance

A family of hash functions $\mathcal{F} = \{\mathcal{H}_i : D_i \rightarrow R_i\}_{i \in \mathcal{I}}$ is collision resistant if:

- $\exists$ PPT algorithm *Gen* such that $\forall \lambda \in \mathbb{N} : Gen(1^\lambda) \in \mathcal{I}$
- $|R_i| < |D_i|$
- $\forall x, i \in \mathcal{I}$, $\mathcal{H}_i(x)$ can be calculated in $PT$.
- $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\mu$, such that $\forall \lambda \in \mathbb{N}$:

$$Pr[i \leftarrow Gen(1^\lambda); (x, y) \leftarrow \mathcal{A}(1^\lambda, \mathcal{H}_i) : \mathcal{H}_i(x) = \mathcal{H}_i(y)] \leq \mu(\lambda)$$

# Hash functions

## Collision Resistance

A family of hash functions $\mathcal{F} = \{\mathcal{H}_i : D_i \rightarrow R_i\}_{i \in \mathcal{I}}$ is collision resistant if:

- $\exists$ PPT algorithm *Gen* such that $\forall \lambda \in \mathbb{N} : Gen(1^\lambda) \in \mathcal{I}$
- $|R_i| < |D_i|$
- $\forall x, i \in \mathcal{I}$, $\mathcal{H}_i(x)$ can be calculated in $PT$.
- $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\mu$, such that $\forall \lambda \in \mathbb{N}$:

$$Pr[i \leftarrow Gen(1^\lambda); (x, y) \leftarrow \mathcal{A}(1^\lambda, \mathcal{H}_i) : \mathcal{H}_i(x) = \mathcal{H}_i(y)] \leq \mu(\lambda)$$

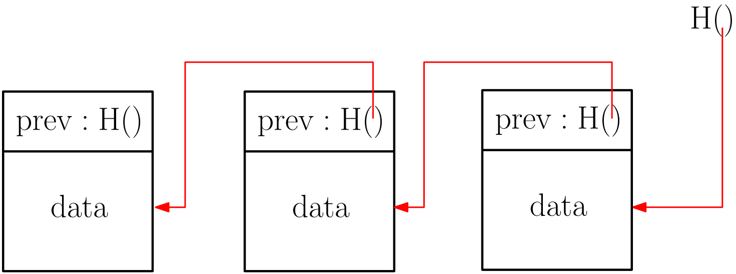
**Birthday Paradox**: $1.2 \cdot 2^{\lambda/2}$ random queries, $Pr[collision] > 1/2$

# Blockchain

*A chain of blocks that contain transactions.*

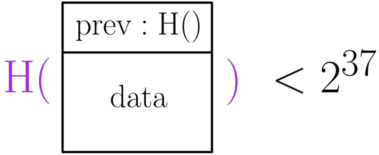
## Properties

- All participants maintain possibly different blockchains.
- Order of blocks defines order of transactions.
- Blocks are connected through hashes (sha256).
- Every block is a POW.



# Proof of Work[Dwork and Naor]

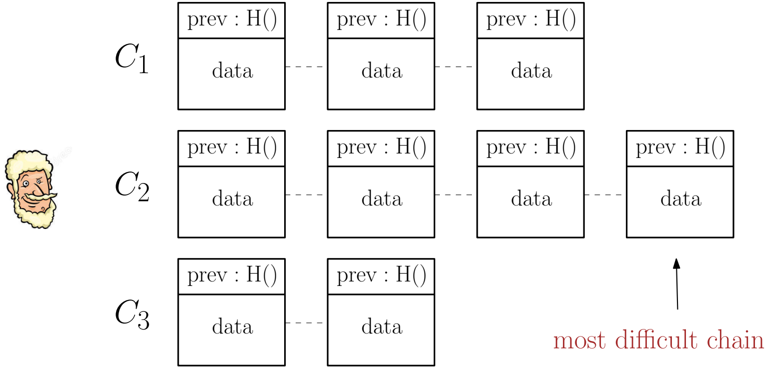
*A proof that an amount of computational work has been done.*




- Block is valid only if the hash of the block is small.
- $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{256}$
- Difficulty is adjusted every 2016 blocks, so that one block is generated every 10 minutes.
- Miners are rewarded for the blocks they mine.

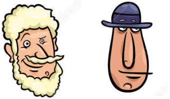
# Chain selection

*Each player chooses the most difficult chain from the ones he have heard.*

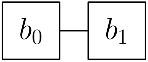


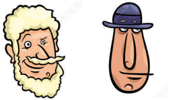
# Example

$b_0$

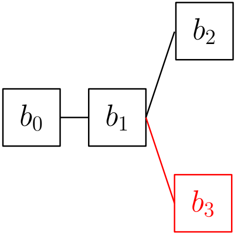


# Example

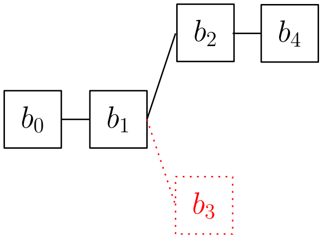


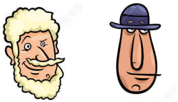



# Example




# Example



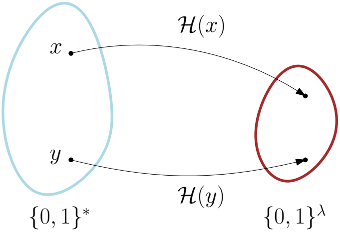



In order to prove security we first need a model.

# Model[Garay, Kiayias, Leonardos 2015]

- Synchronous network : Protocol takes place in successive rounds.
- Unknown but fixed #parties: $n$
- Parties have access to an unreliable anonymous broadcast functionality.
- Every message sent, is received in the following round.
- No one can tell who sent the message with certainty.
- Each miners can do $q$ hashes per round

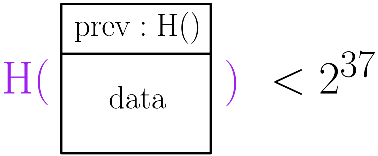
# Hash functions




- $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$
- Easy to compute
- Collision resistant: hard to find two inputs that are mapped to the same output

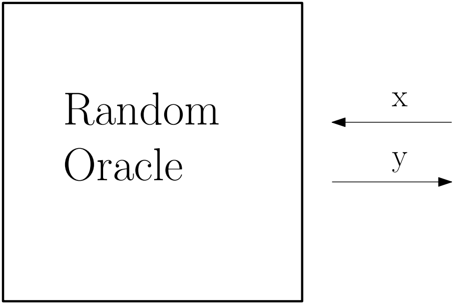
# Proof of Work[Dwork and Naor]

*A proof that an amount of computational work has been done.*



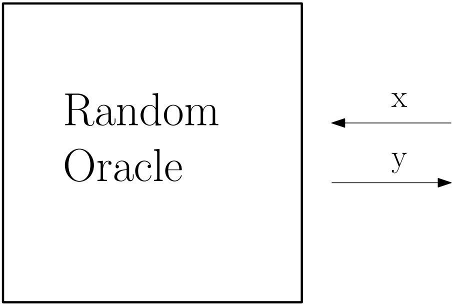

- Block is valid only if the hash of the block is small.
- $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^{256}$
- Difficulty is adjusted every 2016 blocks, so that one block is generated every 10 minutes.
- Miners are rewarded for the blocks they mine.

# Random Oracle




- If $x \notin History$ then $y \xleftarrow{R} \{0,1\}^\lambda$ and add $(x, y)$ to $History$.
- Otherwise, find $(x, y) \in History$

# Random Oracle




- If $x \notin History$ then $y \xleftarrow{R} \{0,1\}^\lambda$ and add $(x, y)$ to $History$.
- Otherwise, find $(x, y) \in History$

$$Pr[\mathcal{H}(x) < D] = D/2^\lambda$$

# Random Oracle

- It was introduced by Bellare and Rogaway in 1993.
- Random oracle is a standard technique used mainly to model hash functions.
- It leads to efficient constructions with provable security.
- There will be also discussion regarding this technique in subsequent lectures.

# Chains

## Definition

A valid *block* is a triple: $\langle s, x, r \rangle$ satisfying $\mathcal{H}(r, G(s, x)) < D$

## Definition

A valid *chain* is a sequence of valid blocks, such that any two consecutive blocks $\langle s_1, x_1, r_1 \rangle$, $\langle s_2, x_2, r_2 \rangle$ satisfy $s_2 = \mathcal{H}(r_1, G(s_1, x_1))$.

# Chains

**Definition**

A valid *block* is a triple: $\langle s, x, r \rangle$ satisfying $\mathcal{H}(r, G(s,x)) < D$

**Definition**

A valid *chain* is a sequence of valid blocks, such that any two consecutive blocks $\langle s_1, x_1, r_1 \rangle$, $\langle s_2, x_2, r_2 \rangle$ satisfy $s_2 = \mathcal{H}(r_1, G(s_1, x_1))$.

- probability of finding a valid block with one query is $p = \frac{D}{2^\lambda}$

# Adversary

- The adversary can corrupt up to $t$ parties.
- At every round he can do $qt$ queries to the oracle.
- He is rushing: sees all messages and then decides what to send.
- Can spoof the source of the messages.
- Can do partial broadcast.

# A first lemma

## Definition

A round is *uniquely successful* if exactly one honest party finds a valid block.

- Let r.v. $X_i$ be 1 if round $i$ is a uniquely successful round and 0 otherwise.
- Let r.v. $Z_{i,j}$ be 1 if the adversary finds a valid block in his $j$-th query at round $i$.
- Let $\gamma = Pr[X_i = 1]$ and $\beta = qtp$.
- Assuming $\gamma \geq (1+\delta)\beta$, show that for any $s$:

$$Pr[\sum_{i=1}^{s} X_i < (1+\delta/2)\sum_{i=1}^{s}\sum_{j=1}^{qt} Z_{i,j}] < negl(s)$$

# Proof

W.l.o.g. assume all queries to the random oracle are different.

- $X = \sum_{i=1}^{s} X_i$ is $B(s, \gamma)$
- $Z = \sum_{i=1}^{s} \sum_{j=1}^{qt} Z_{i,j}$ is $B(sqt, p)$
- Apply Chernoff bound to both!

# Proof

W.l.o.g. assume all queries to the random oracle are different.

- $X = \sum_{i=1}^{s} X_i$ is $B(s, \gamma)$
- $Z = \sum_{i=1}^{s} \sum_{j=1}^{qt} Z_{i,j}$ is $B(sqt, p)$
- Apply Chernoff bound to both!

## Reminder

For independent Bernoulli variables $Y_i$, any $\delta \in (0,1)$ and $\mu = \sum_{i=1}^{n} Pr[Y_i = 1]$:

$$Pr[\sum_{i=1}^{n} Y_i \leq (1-\delta)\mu] \leq e^{-\mu\delta^2/2}$$

*and*

$$Pr[\sum_{i=1}^{n} Y_i \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}$$

# Proof

In our case, for $\delta \in (0, 1)$:

$$Pr[X \leq (1 - \delta/8)\gamma s] \leq e^{-\gamma s \delta^2/128} \leq negl(s)$$
$$and$$
$$Pr[Z \geq (1 + \delta/9)\beta s] \leq e^{-\beta s \delta^2/243} \leq negl(s)$$

# Proof

In our case, for $\delta \in (0,1)$:

$$Pr[X \leq (1-\delta/8)\gamma s] \leq e^{-\gamma s \delta^2/128} \leq negl(s)$$

*and*

$$Pr[Z \geq (1+\delta/9)\beta s] \leq e^{-\beta s \delta^2/243} \leq negl(s)$$

## Union bound

By the union bound, none of the above events happens with probability at least $1 - negl(s)$. Thus in this case:

$X >$ $\qquad > (1+\delta/2)Z$

# Proof

In our case, for $\delta \in (0,1)$:

$$Pr[X \leq (1-\delta/8)\gamma s] \leq e^{-\gamma s \delta^2/128} \leq negl(s)$$
$$and$$
$$Pr[Z \geq (1+\delta/9)\beta s] \leq e^{-\beta s \delta^2/243} \leq negl(s)$$

## Union bound

By the union bound, none of the above events happens with probability at least $1 - negl(s)$. Thus in this case:

$X > (1-\delta/8)\gamma s$ $\qquad$ $(1+\delta/2)(1+\delta/9)\beta s > (1+\delta/2)Z$

# Proof

In our case, for $\delta \in (0, 1)$:

$$Pr[X \leq (1 - \delta/8)\gamma s] \leq e^{-\gamma s \delta^2/128} \leq negl(s)$$

$$and$$

$$Pr[Z \geq (1 + \delta/9)\beta s] \leq e^{-\beta s \delta^2/243} \leq negl(s)$$

## Union bound

By the union bound, none of the above events happens with probability at least $1 - negl(s)$. Thus in this case:

$$X > (1-\delta/8)\gamma s \geq (1-\delta/8)(1+\delta)\beta s \quad (1+\delta/2)(1+\delta/9)\beta s > (1+\delta/2)Z$$

# Proof

In our case, for $\delta \in (0,1)$:

$$Pr[X \leq (1-\delta/8)\gamma s] \leq e^{-\gamma s \delta^2/128} \leq negl(s)$$
$$and$$
$$Pr[Z \geq (1+\delta/9)\beta s] \leq e^{-\beta s \delta^2/243} \leq negl(s)$$

## Union bound

By the union bound, none of the above events happens with probability at least $1 - negl(s)$. Thus in this case:

$$X > (1-\delta/8)\gamma s \geq (1-\delta/8)(1+\delta)\beta s \geq (1+\delta/2)(1+\delta/9)\beta s > (1+\delta/2)Z$$