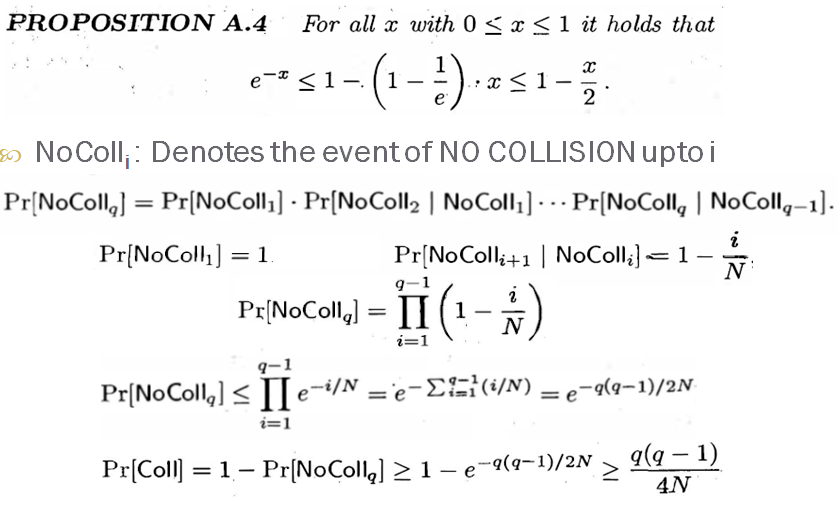
**Collision Resistant Fixed Hash**

Assuming DL is hard to invert, we built fixed length collision resistant hash function.

**Lemma:** Fix a positive integer N, and say elements are chosen uniformly and independently at random from a set of size N. Then the probability that there exist distinct with is at least . i.e.,

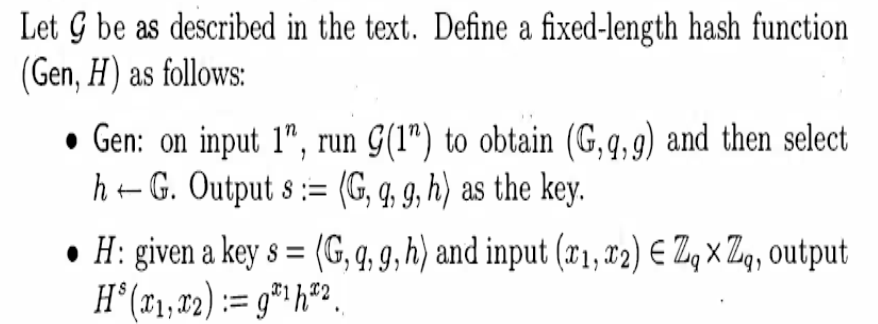
“Smaller the value of q w.r.t N, higher is the collision resistance”

Proof:



Construction of fixed length hash function

Assuming that DL is hard to invert (one-way function).



Proof by contradiction

If discrete logarithm problem is hard relative to G, then the following construction is a fixed-length collision-resistant hash function

For the given value of g, h we found an X, which contradicts the assumption of DL being a one-way function.

Hence, (Gen, H) is a collision resistant hash function.

References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: <https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html>.

[3] Lecture Slides