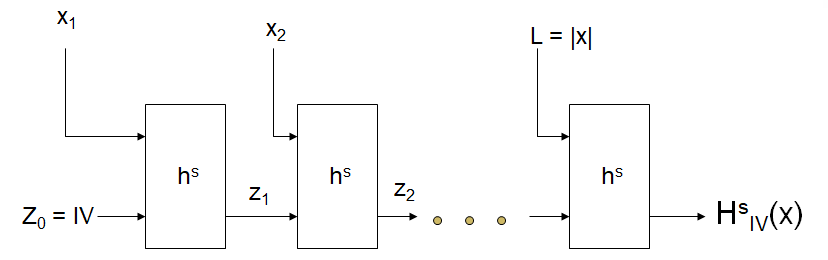
**Construction of variable length hash function from fixed length hash function**

**Merkle Damgard Transform**

Theorem:

If (Gen, h) is a fixed length collision resistant hash function, then (Gen, H) is a collision resistant hash function



Let (Gen, h) be a fixed-length collision-resistant hash function for inputs of length and output length . Construct a variable-length hash function (Gen, H) as flows:

* Gen: remains unchanged
* H: on input a key s and a string of length in what follows:
  1. Set (i.e., the number of blocks in x). Pad x with zeroes so its length is a multiple of . Parse the padded result as the sequence of – bit blocks . Set where L is encoded using exactly bits.
  2. Set .
  3. For , compute
  4. Output .

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