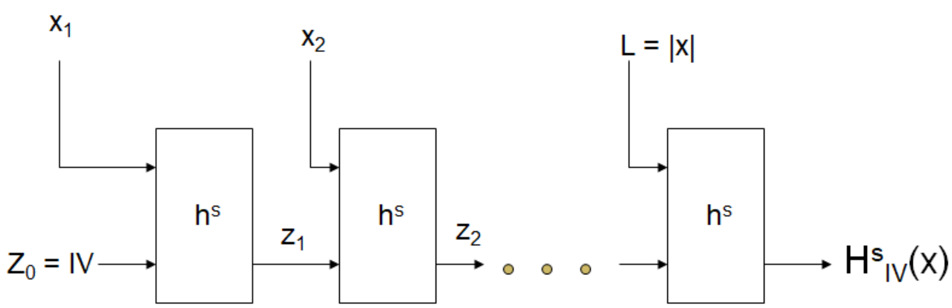
2021201041
Nvss Maneesh Gupta

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 $2l(n)$ and output length $l(n)$. Construct a variable-length hash function (Gen, H) as flows:

- Gen: remains unchanged
- H: on input a key s and a string $x \epsilon \{0.1\}^*$ of length $L < 2^{l(n)}, do\ the\ following\ (set\ l = l(n)$ in what follows:
  1. Set $B := \left\lceil \frac{L}{l} \right\rceil$ (i.e., the number of blocks in x). Pad x with zeroes so its length is a multiple of l. Parse the padded result as the sequence of l – bit blocks $x_1, x_2, \dots, x_B$. Set $x_{B+1} := L$, where L is encoded using exactly l bits.
  2. Set $z_0 := 0^l$.
  3. For $i = 1, \dots, B + 1$, compute $z_i := h^s(z_{i-1}||x_i)$.
  4. Output z_{B+1}.

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