The Merkle-Damgård Construction

ECE 4156/6156 Advanced Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading

- Intro to Modern Cryptography by Katz and Lindell, Chapter 5

History

- In the 1980s Ivan Bjerre Damgård was a researcher at the Mathematical Institute in Aarhus U., Denmark
- At the same time Ralph Merkle worked at Xerox PARC
  - Merkle is credited with (co-)inventing public key cryptography, often referred to as Diffie-Hellman-Merkle PKC
  - Merkle and Damgård knew each other and both corresponded
- Both independently published their work in Crypto 1989

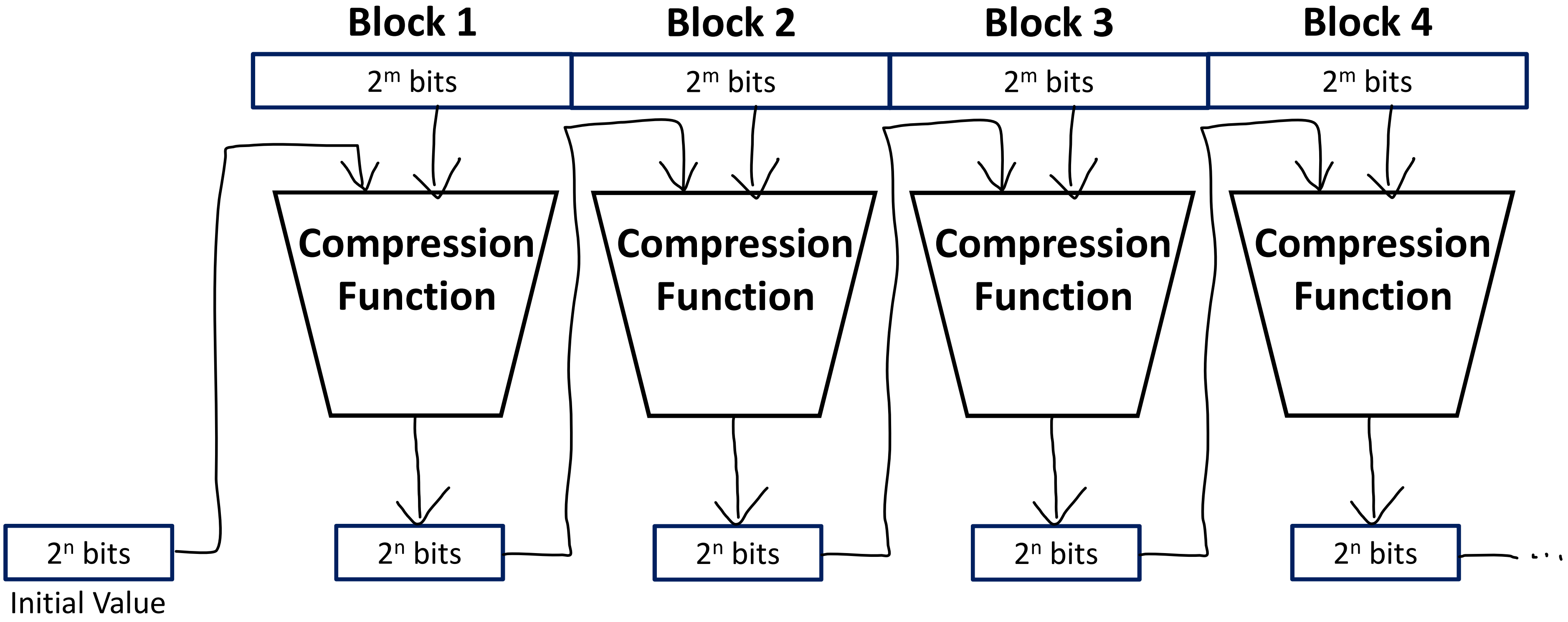
Goals

- Construction of a one-way hash function built upon fixed-length hash functions
- Provably hard to crack
  - If the fixed-length hash function has a tiny probably of discovery of a collision, so does the hash function able to receive arbitrary length inputs
  - The arbitrary length hash function is built out of repetition of the fixed length hash function

Message Padding

- For simplicity and due to lack of time, we will skip the details regarding how to properly pad messages and maintain the Merkle-Damgård construction properties

Merkle-Damgård Construction, m ≥ n



What Does the Merkle-Damgård Construction Prove?

- Collision Resistance (CR) of the compression function $\Rightarrow$ CR of the overall function
  - If the <2^m,2^n> to 2^n compression function is CR
    - So is the overall function over any number of blocks

Proof Outline

- We will not cover the proof here
  - You can learn it in a mathematics or computer science theory class
- Outline
  - Suppose there exists a collision with non-trivial probability in the overall function
    - A non-trivial probability for *n* bits would be, for example, a probability p where $p > 2^{-n}$
  - Then we can prove that there exists a collision with non-trivial probability in the compression function
  - Early proofs used, for example, DES as a building block for the compression function
    - The properties of DES (no one has cracked DES other than with brute-force attacks) were used to show CR

All Modern Hash Functions

- Use the Merkle-Damgård Construction