IPA 暗号フォーラム 2006 (2006/10/5, 経団連会館)

ハッシュ関数の今後について

Future of Secure Hash Function

廣瀬勝一

Shoichi Hirose

福井大学工学研究科

Univ. of Fukui

2006 年 10 月 5 日

Future from Academic or Technical Point of View

- Collisions will be found for SHA-1 in the near future
- NIST recommends use of SHA-2 family (SHA-224/256/384/512)
- NIST plans a competition for Advanced Hash Standard, which will start around 2008 (tentative)

How to design hash functions which will replace SHA-2 family?

Applications and Required Properties

Without secret key

- **MDC** Collision Resistance (**無衝突性**)
- **Random Oracle** Correlation Immunity (**入出力の非相関性**)

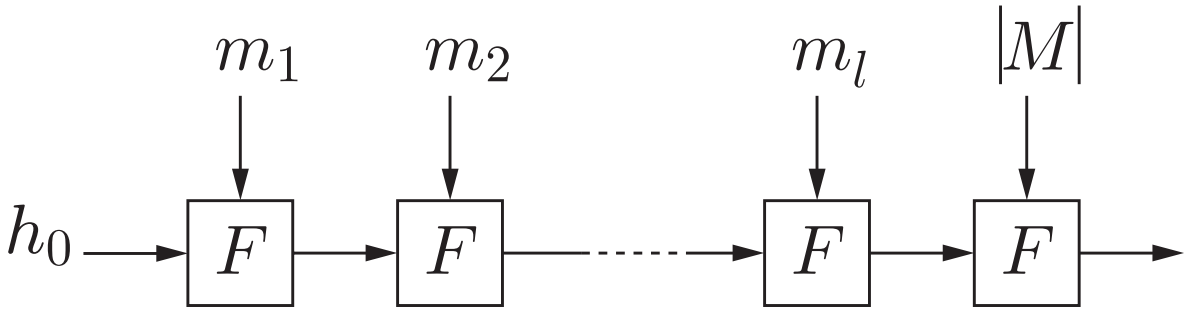
With secret key

- **MAC** Unforgeability (**偽造困難性**)
- **PRF, PRG** Pseudorandomness (**擬似ランダム性**)

Hash Function Construction

Compression Function + Domain Extension

- Single compression function
- One universal scheme or several schemes for domain extension
  - Merkle-Damgård
    - ∗ does not make random oracles
    - ∗ suffers from multi-collision attack
  - One for MDC and RO, and another for MAC



Compression Function Construction

Design like a block cipher seems better against Wang's differential attack

- Conservative as a research problem?
- We still do not know how to construct really secure one

Collision resistance is meaningful only for function families

- Design as an element of a function family