**Hash Design Problem**

Hash functions are used for:
- message digests
- key derivation functions
- message authentication codes
- random oracles
- signatures, encryption, …

Recently, many attacks on existing hash functions found
• New methodologies needed!!!

Our work encompasses new design criteria and novel implementations of hash functions which resist above deficiencies.

**Known Approaches**
- Study one property at a time
- Theory: analyze new, ad hoc construction for each property
- Practice: use existing (often insecure) constructions and “hope for the best”

**New Approaches**
- Multi-property preservation with one design – both theory and practice
- New design criteria
  - Indifferentiability from random oracle
- New, provably secure constructions

**Indifferentiability from Random Oracle**

Constructing ideal primitive $G$ using $F$:

$G = \text{desired ideal primitive (VIL: random oracle)}$

$F = \text{available ideal primitive (compression function or block cipher)}$

$E = \text{construction of } G \text{ using } F$

$\mathcal{S} = \text{Simulator of } F \text{ using } G$

$D = \text{Distinguisher (to be fixed by } \mathcal{S})$

Composition Theorem

Any protocol $P$ secure in $\mathcal{S}$ model is also secure in $F$ model when $E$ is used to implement $G$ (using $F$)

**New Mode of Operation for Block Ciphers**

**Enciphered CBC**

- Multi-property preserving mode
  - (only) twice slower than CBC
  - fixed keys, no re-keying
- Preserves pseudorandomness and unforgeability:
  - hedge against block cipher security
  - first constant-rate domain extension of length-preserving MACs
- Yields random oracle (and, thus, collision-resistant hash function) in the ideal cipher model

**Common design methodology: build variable-input length (VIL) hash from a fixed-input length (FIL) primitive:**

- FIL compression function $f$. Variants of cascade construction are used:

  $\begin{align*}
  & f(x, y) = E_s(y) \oplus y \\
  & \text{New Haven, Connecticut}
  \end{align*}$

$\text{Block cipher } E. \text{ Build compression function via Davies-Meyer transform:}$

$\text{Provably Indifferentiable Constructions}$

**Prefix-free:**

**Chopping output:**

$\text{NMAC (fresh } g):$  

$\text{HAMAC:}$

$\text{All constructions can be implemented via "black-box calls" to SHA (or any cascade)}$

$\text{All constructions work in the ideal cipher model with the Davies-Meyer construction:}$

$\text{Indifferentiability from Random Oracle}$

$\text{New, provably secure constructions}$