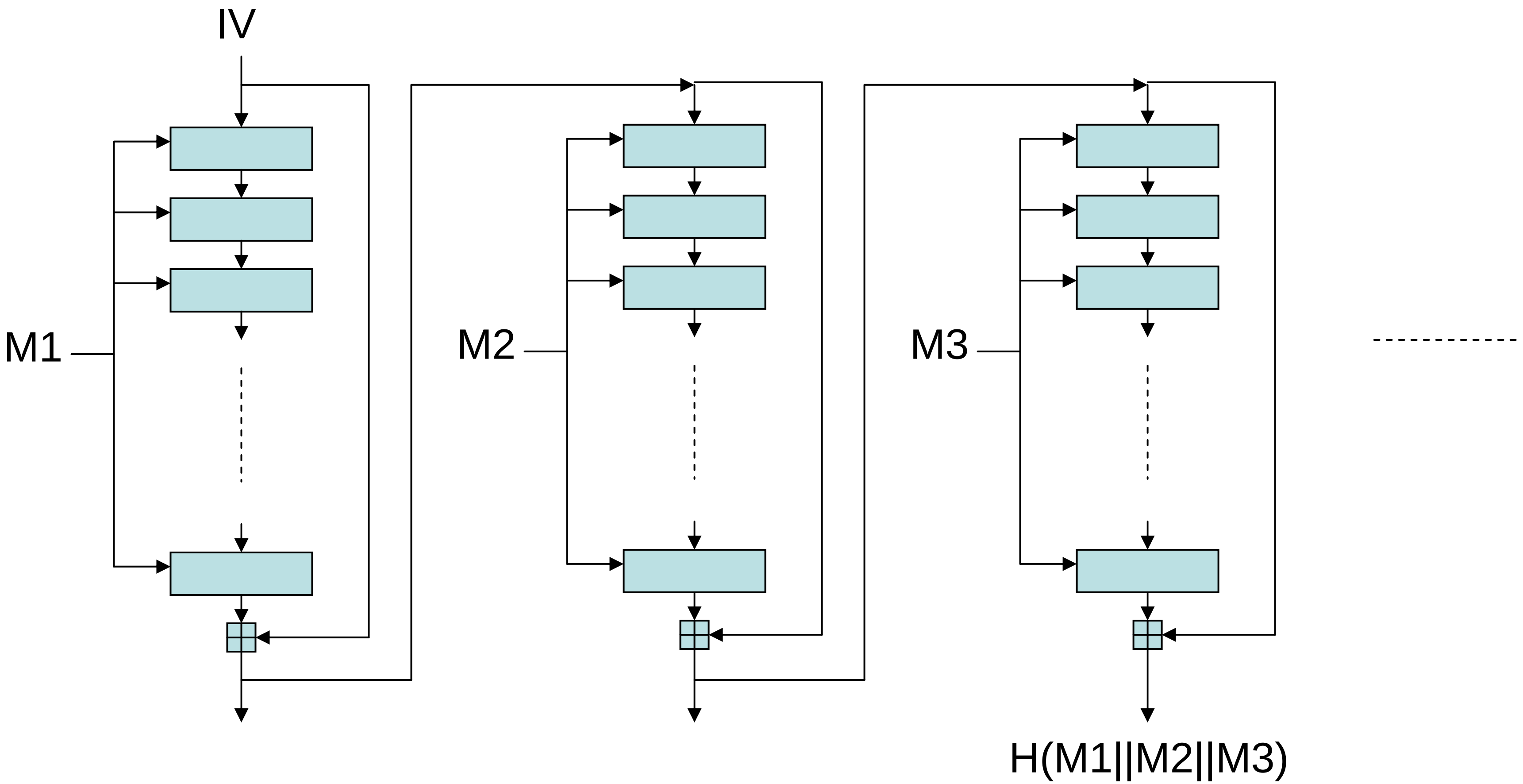
The SHA Family

	Hash Size (bits)	Message Size (bits)	Expected Strength	Best Attack
SHA0	160	512	2^{80}	$\sim 2^{40} - 2^{50}$
SHA1	160	512	2^{80}	$\sim 2^{60}$
SHA2 (SHA256)	256	512	2^{128}	2^{128}
SHA2 (SHA512)	512	1024	2^{256}	2^{256}

Impacts of the SHA1 attacks

- Very widely used (digital signature)
- Finding one collision results in ..?
- NIST's plan to shift to a new function
- How about SHA2?
- When and How to shift

MD-type Hash Function


IV
M1
M2
M3
H(M1||M2||M3)