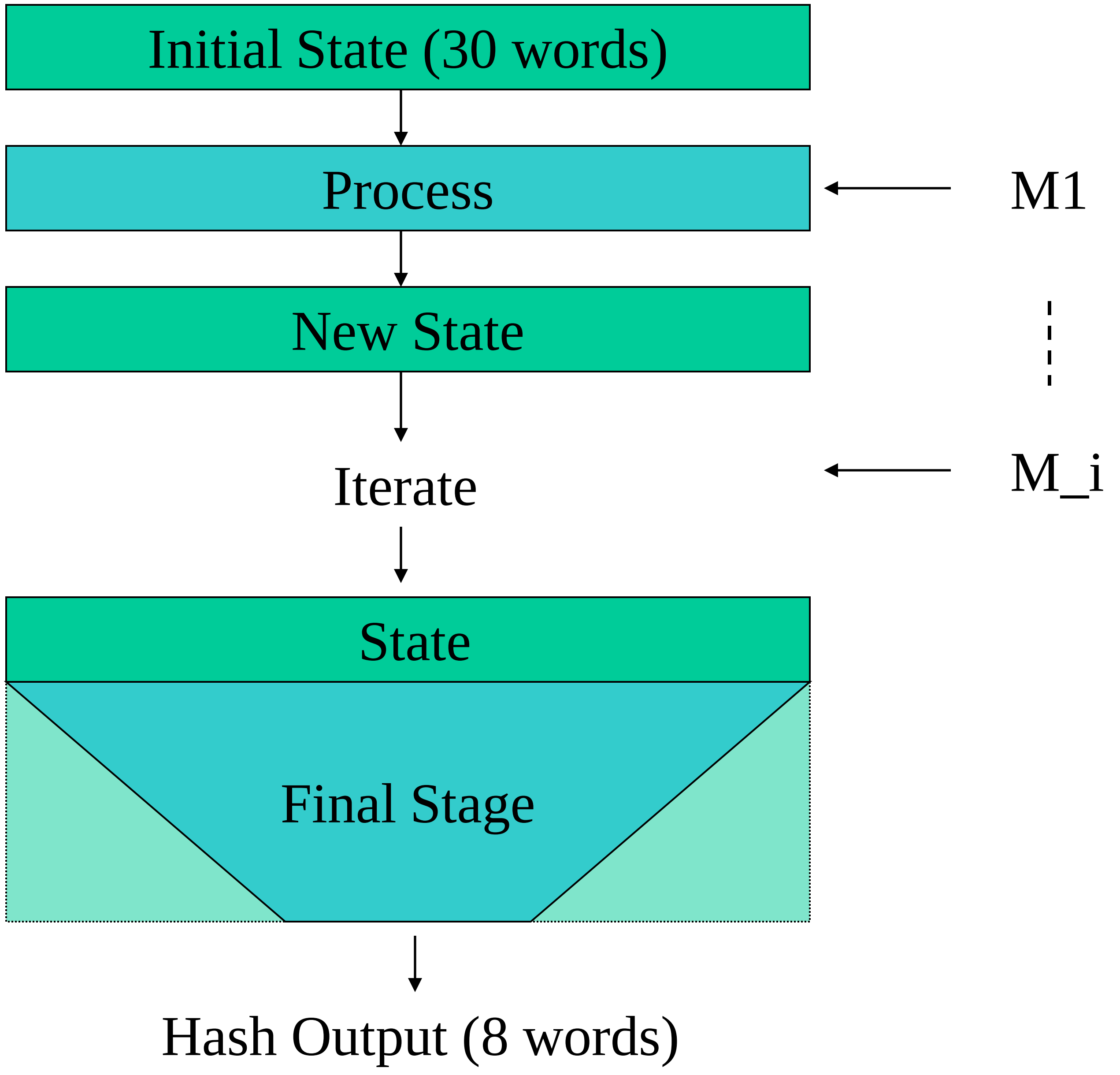
The Hash Function Fugue

Shai Halevi, William E. Hall and Charanjit S. Jutla

IBM T. J. Watson Research Center

Fugue-256


Initial State (30 words)
Process
M1
New State
Iterate
M_i
State
Final Stage
Hash Output (8 words)

Fugue State < SHA-256 State

- Fugue-256 state: 960 Bits
  - All message expansion / feed forward incorporated into this state
- SHA-256 state: 1024 bits
  - 256 bit IV for feed-forward
  - 512 bit message expansion state
  - 256 bit block cipher state

Provable Properties of Fugue

- Provable Properties
  - Those properties which are most vulnerable
  - No ideal primitives assumptions
- Full Fugue is Collision Resistant to differential attacks
- Full Fugue is a Universal Hash Function
- Critical Internal Partial Collision Resistance
- Compression Function for H-MAC:
  - Pseudo-Collision Resistant to differential attacks
  - Universal Hash

State of the Art: Fugue

- Proves collision resistance to differential attacks
  - Collision Resistance : most vulnerable property
    - Need just a pair
    - Non-black box access to hash function
    - Message modifications/ Neutral bits etc.
  - Differential Attacks: most powerful attack
- Bound on both Internal and External Collisions
  - Hence bound on full Fugue
  - Not just a bound on individual differential trails

Internal Collision Theorem

- Proves internal collision requires at least 4 rounds of input
- Assumption: Adversary can only sample random state 4 rounds earlier than collision
  - Similar to one-way property, but not quite
    - Will weaken it next slide
- Adversary allowed to set any differential in state 4 rounds earlier!
- Theorem: Probability that there exists a pair of 4 round inputs so that internal collision $< 2^{-168}$.

Message Modification/Neutral Bits

- Weaker Assumption:
  - Adversary can sample only random state except for ability to do free message modification through 4 SMIX-es.
- Theorem:

  Probability of collision $< 2^{-128}$

Universal Hashing

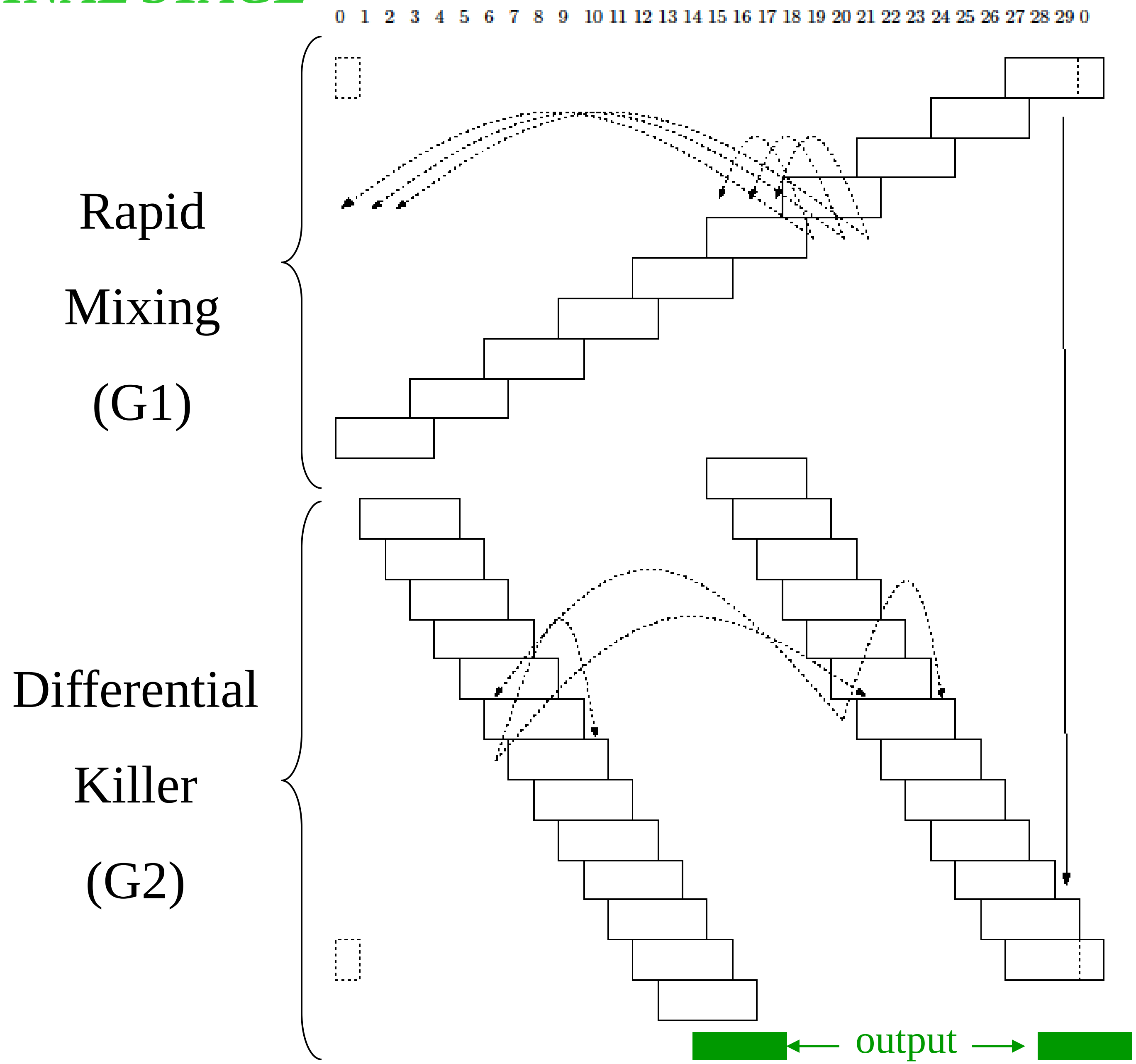
- A minimal necessary security property
  - Not UH => Not CR, Not MAC, Not TCR, …
  - Implies good extractor for Key Derivation
- Theorem:

  Fugue is a 2^{-128}-Universal Hash when keyed through initial 30 word state.
- The only provable Universal hash function, among the 14 SHA-3 candidates

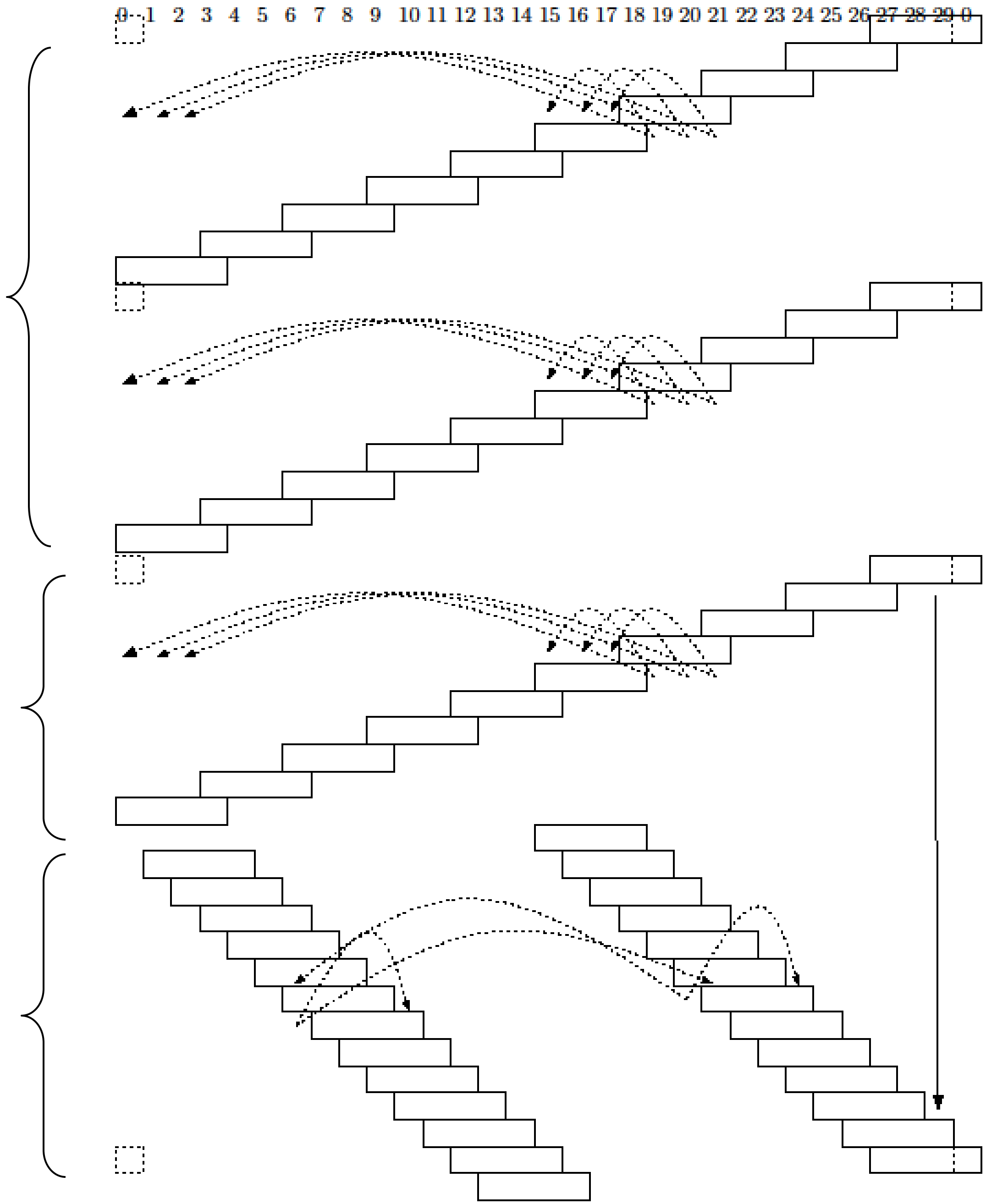
Black Box In-distinguishability

- Similar theorems for partial internal collisions
  - Black Box Model
  - Secret or Known Random Key
- Hence Aumasson-Phan analysis' pre-condition is proven to happen with probability only $< 2^{-142}$.

FINAL STAGE


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 0
Rapid Mixing (G1)
Differential Killer (G2)
output

Input
Rounds



(G1)

(G2)

Software Performance Fugue-256 (Intel Intrinsics in C)

	64 Bit (c/byte)	32 Bit (c/byte)
Core 2 Duo	16.5	17.5
Core i5 (SSE4)	14	
Core i5 w/ AES	13.5	
Speculative (w/ 128-bit Fugue linear-mix instruction)	3 to 4	

Hardware Performance (ASIC)

	Tech.	Gate Count	Throughput
Fugue-256	IBM 90nm	110K	13.9 Gbits/s
Fugue-512	same	121K	7 Gbits/s
SHA-256	same	46K	3 Gbits/s
Fugue-256	180nm (Tillich…)	48K	2.6 Gbits/s
SHA-256	same	19K	1.6 Gbits/s

Conclusion

- Proof-driven design along with right priorities leads to best of both worlds
  - - Exceptional Security
    - no attack even approaches Weak-Fugue-256
    - Weak-Fugue-256 has twice the throughput!
    - Half the final round !
      - Dmitry Khovratovich Structure Attack ~ 2^{300} memory
      - Aumasson-Phan …defends well
      - Meltem Turan …defends well
  - -High Performance

THANK YOU!

Discarded/Additional Slides

Ideal Primitives?

- Andreeva, Mennink & Preneel do a nice survey of security reductions of SHA-3 candidates
  - Good for checking against structural defects
  - But based on Ideal Primitive Assumptions
  - Ideal requirements on components can be un-necessarily strong
    - See e.g. history of SHABAL at SHA-3 zoo
    - likely to be not true
    - lead to sub-optimal speed/security tradeoff design

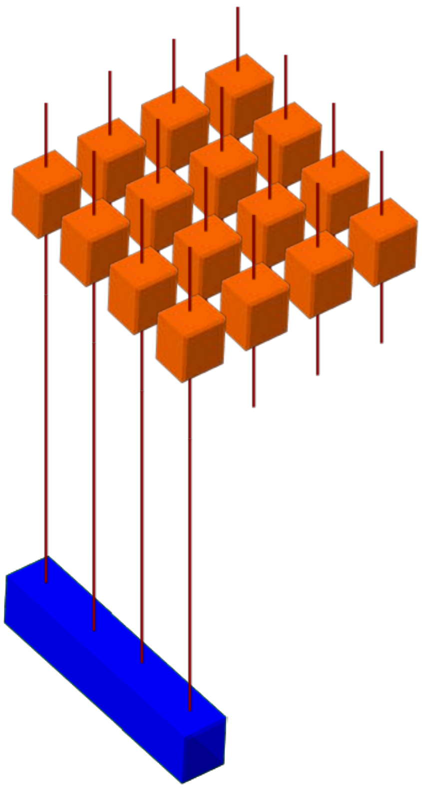
External Collision Provable Bound

- Theorem: For any state difference D $\neq 0$, if the states at the start of G2 are chosen randomly then

  $$\Pr[\text{ Collision in 256 bit output } \mid D\ ] \leq 2^{-129}$$

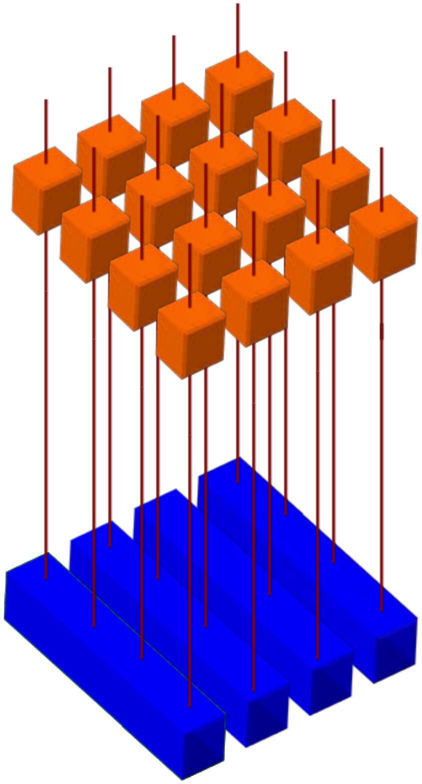
- Recall, assumes independence assumption

AES Round

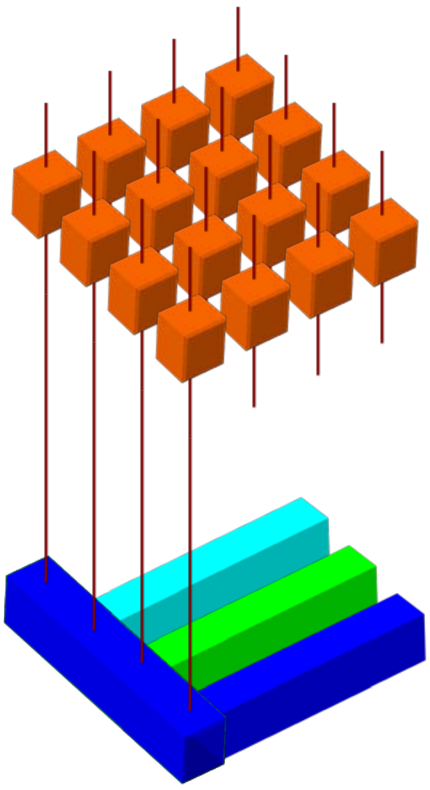


MDS Code over 4 bytes

AES Round



Fugue Elementary Round "SMIX"



Leads to an MDS code over 16 bytes!