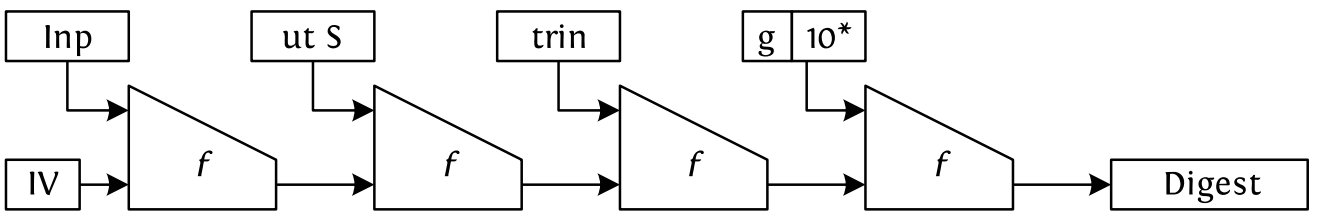
The iterating mode

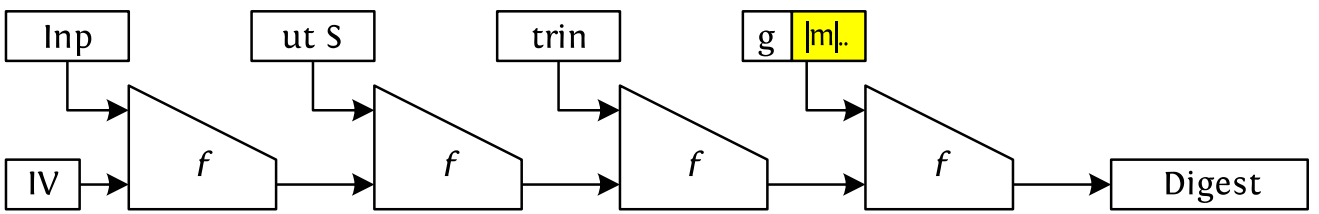
Basic Merkle-Damgård: very simple and elegant



Yes, but can we have collision-resistance preservation?

The iterating mode

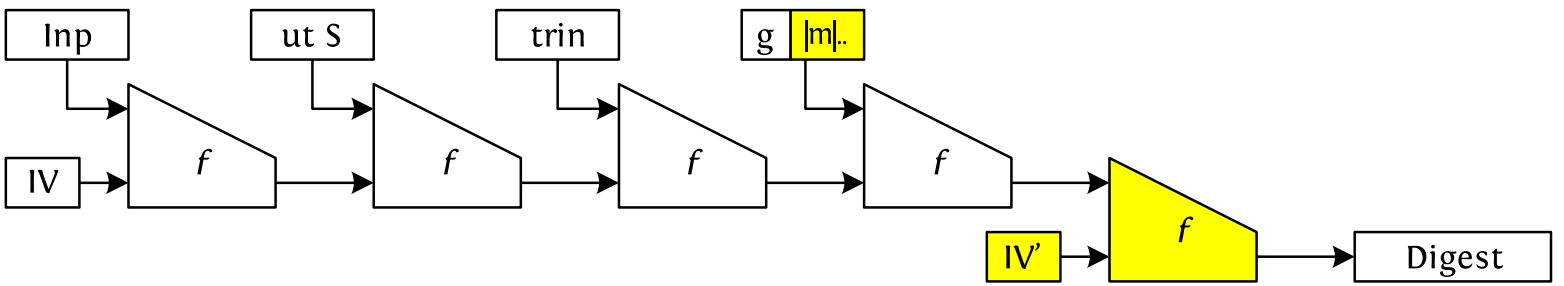
Merkle-Damgård with *strengthening*



Yes, but what about length extension attacks and the like?

The iterating mode

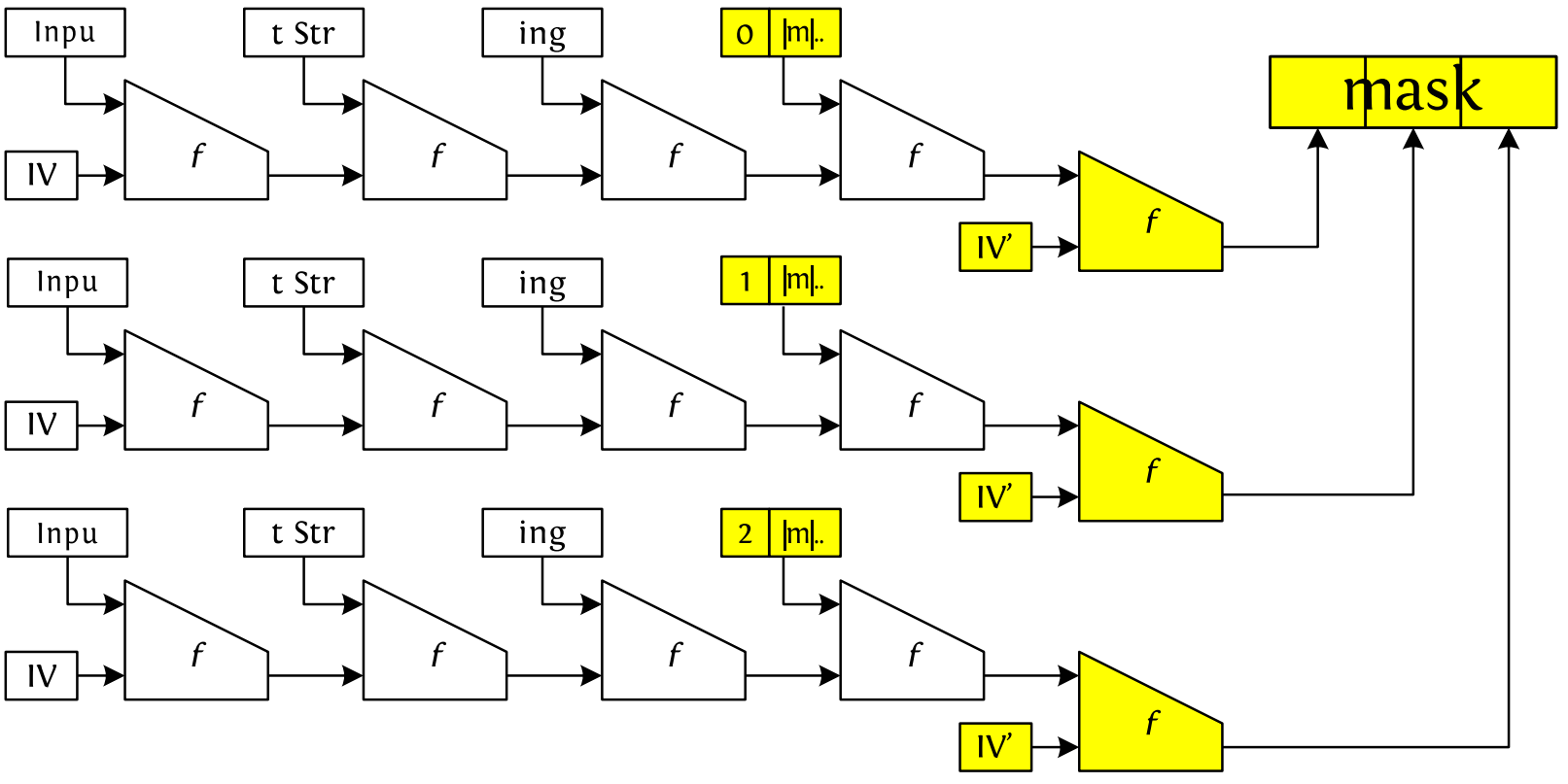
Enveloped Merkle-Damgård



Yes, but we need long output for full-domain hashing (OAEP, RSA-PSS, KEM, etc)?

The iterating mode

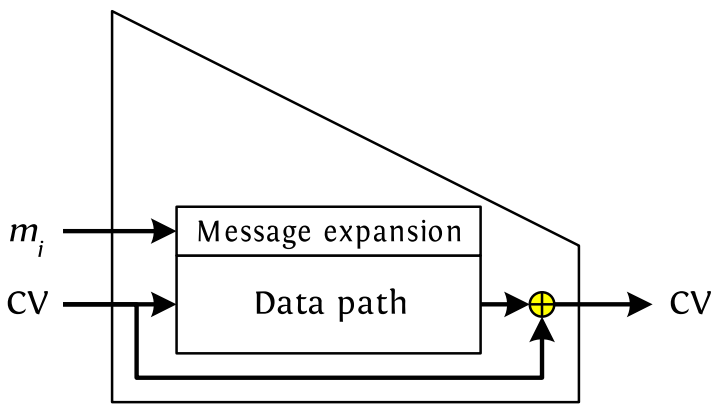
Mask generating function construction



This does what we need!

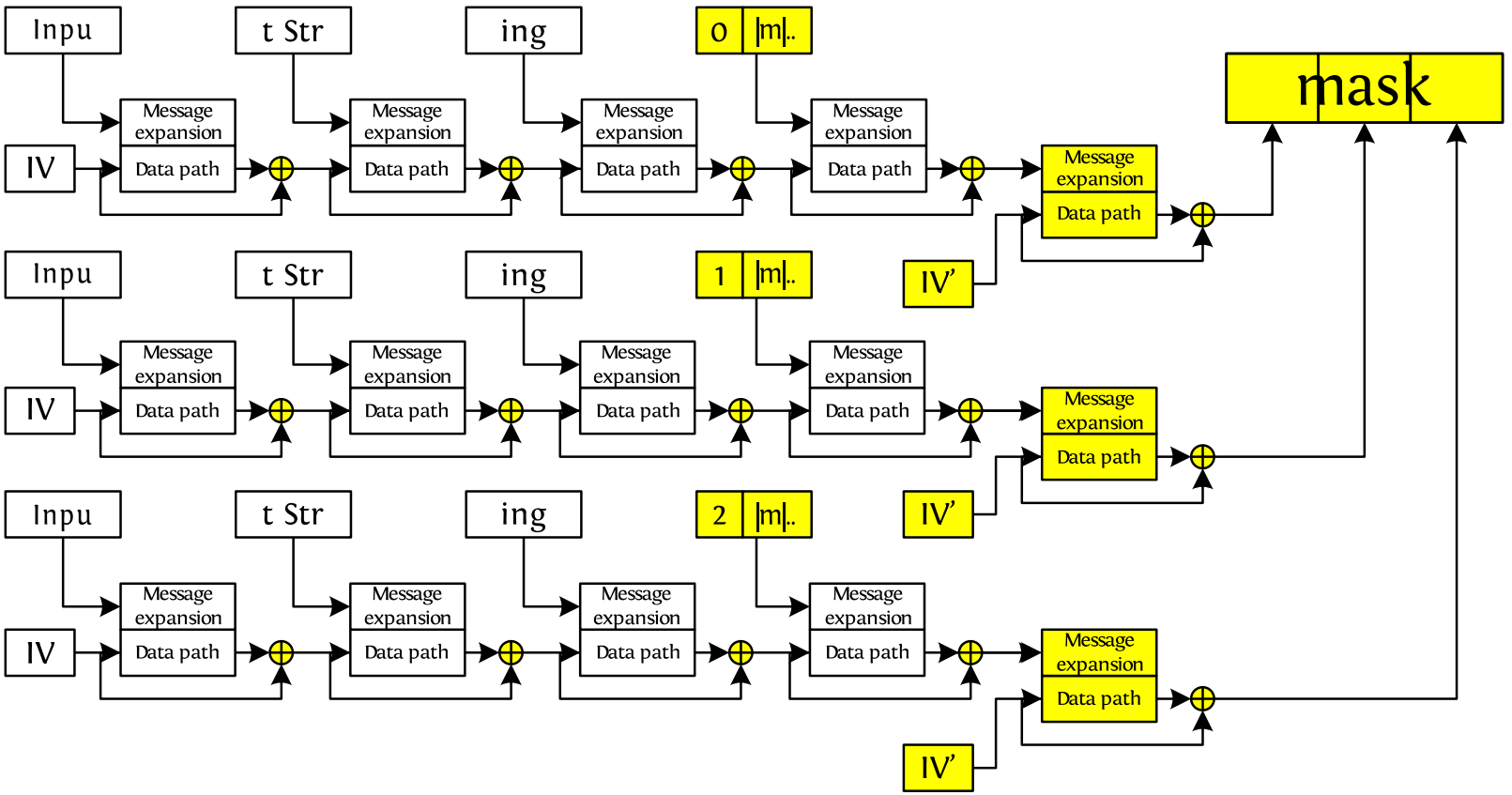
The compression function

Block cipher in Davies-Meyer mode



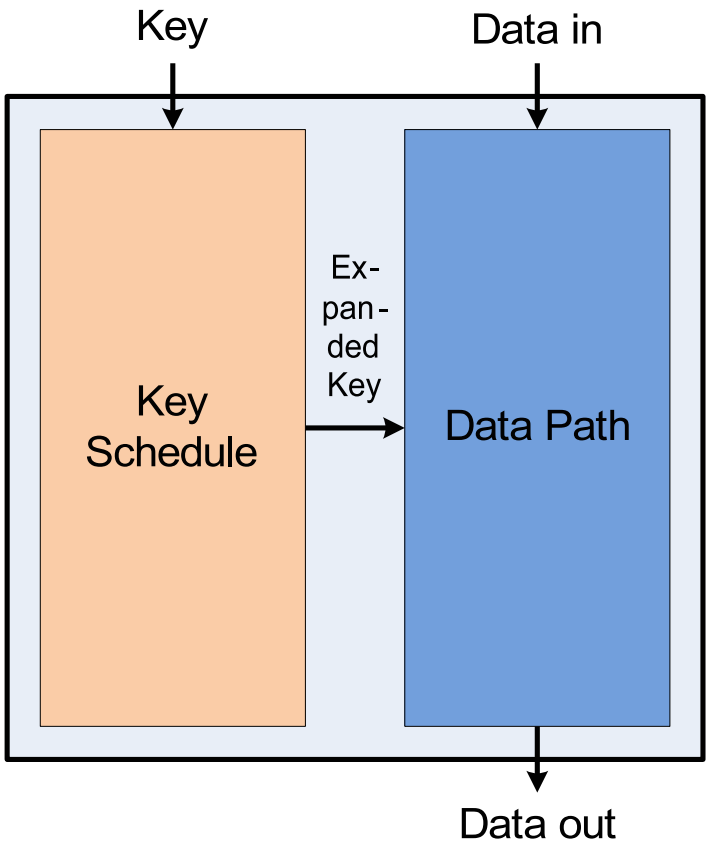
That's it!

The final solution

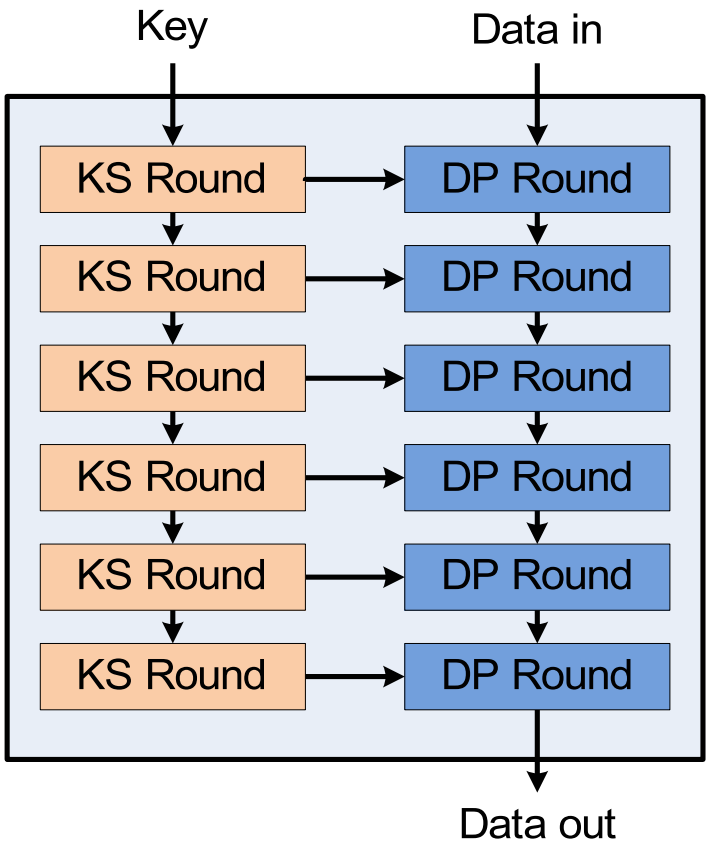


Now we just have to build a suitable block cipher ...

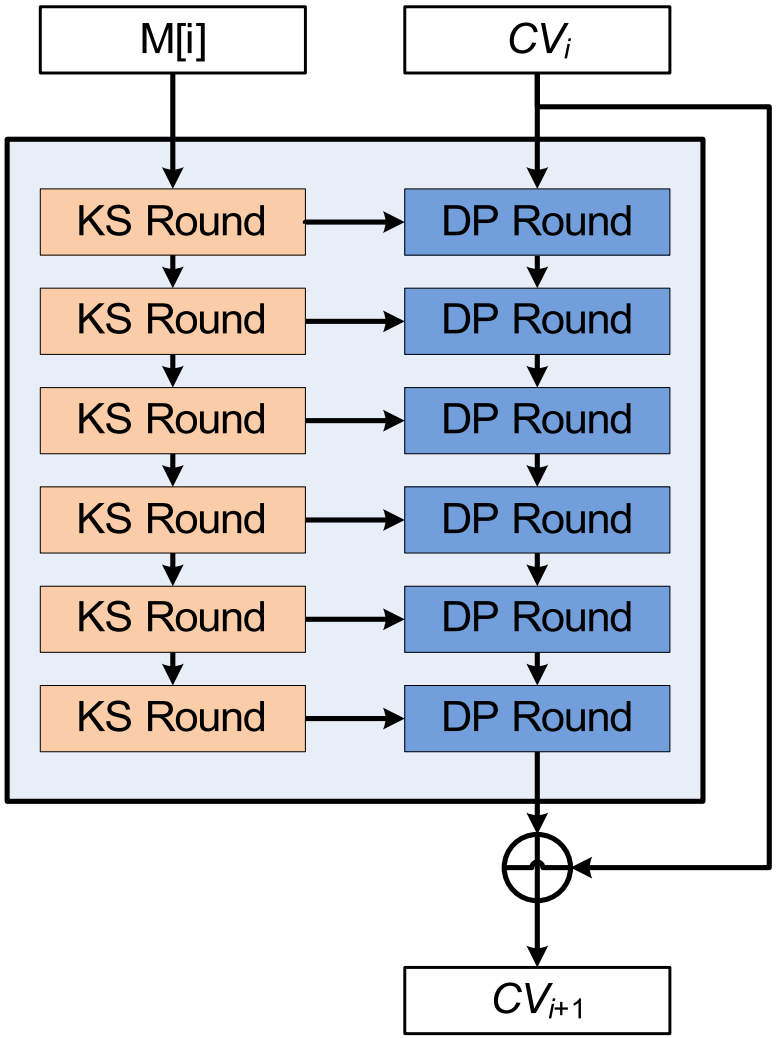
Block cipher operation



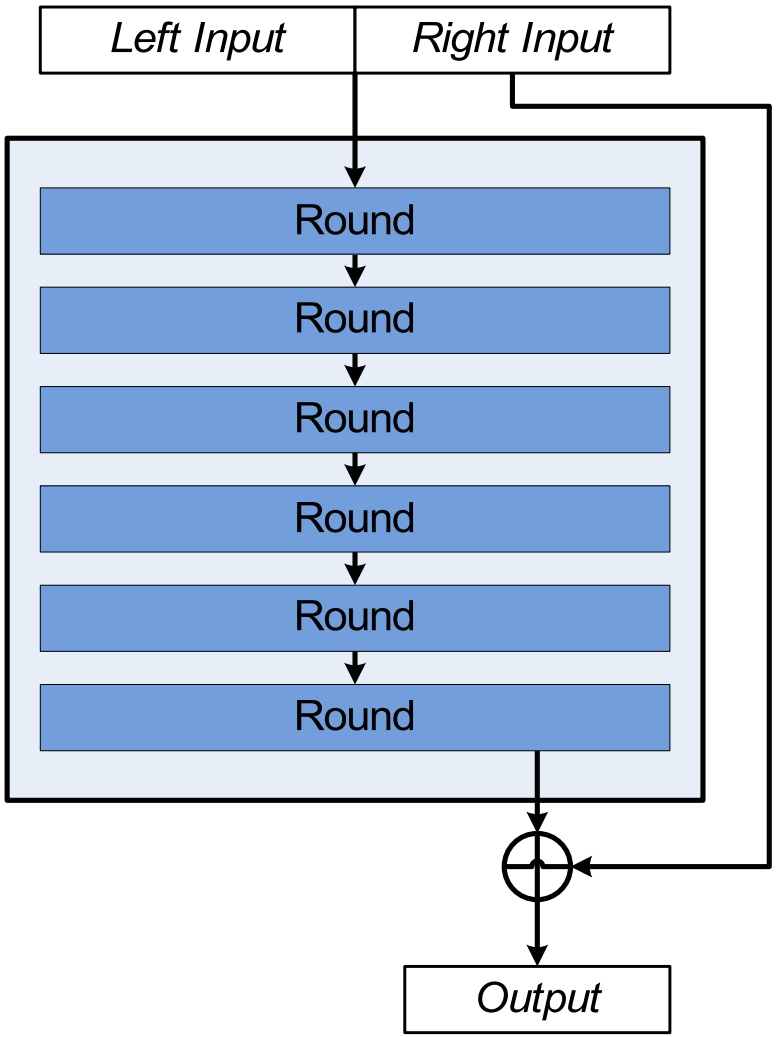
Block cipher internals



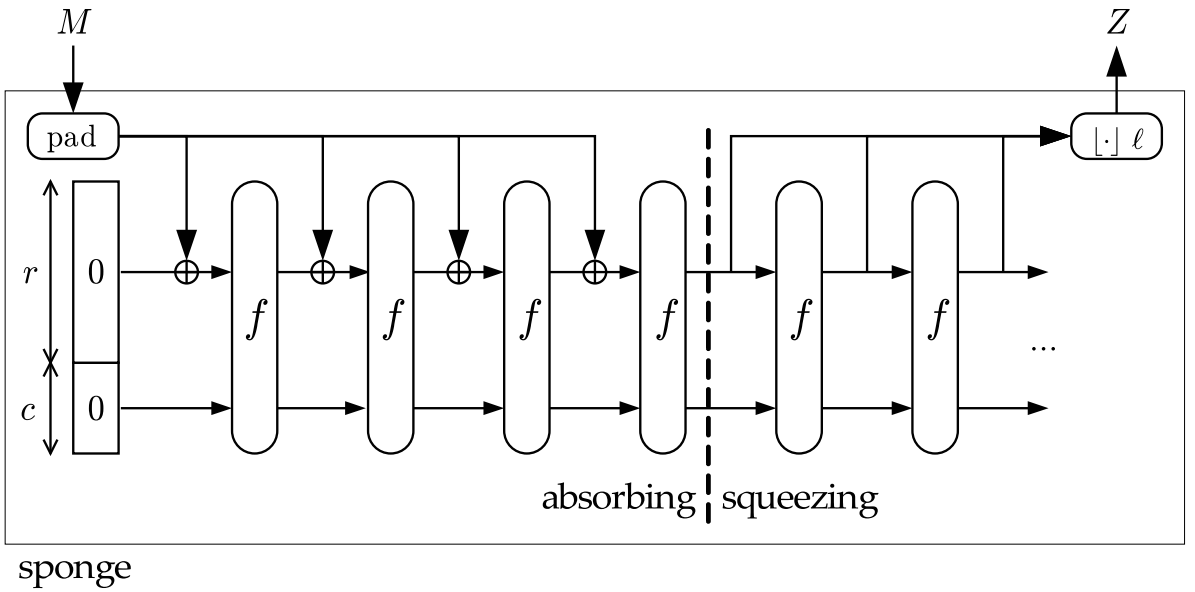
Hashing use case: Davies-Meyer compression function



Simplifying the view: iterated permutation



The result: the sponge construction



- f: a b-bit permutation with $b = r + c$
  - efficiency: processes r bits per call to f
  - security: provably resists generic attacks up to $2^{c/2}$
- Flexibility in trading rate r for capacity c or vice versa

Generic security of the sponge construction

Theorem (Indifferentiability of the sponge construction)

The sponge construction calling a random permutation, $\mathcal{S}'[\mathcal{F}]$, is (t_D, t_S, N, ϵ)-indifferentiable from a random oracle, for any t_D, $t_S = O(N^2)$, $N < 2^c$ and for any ϵ with $\epsilon > f_{\mathsf{P}}(N) \approx \frac{N}{2^{c+1}}$.

[Keccak team, Eurocrypt 2008]

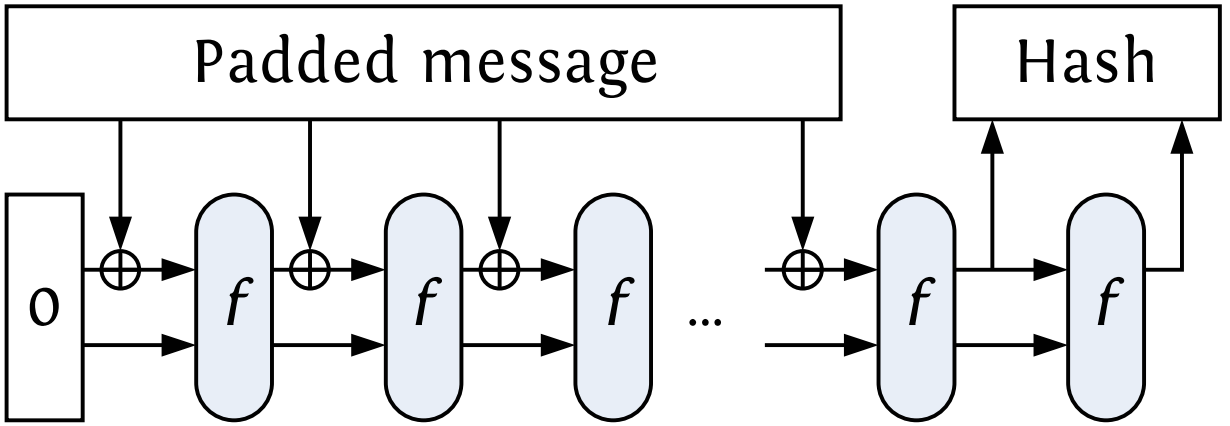
Informally, a random sponge is like a random oracle when $N < 2^{c/2}$.

- Collision-, preimage-resistance, etc., up to security strength $c/2$
- The bound assumes f is a random permutation
  - It covers generic attacks
  - ...but not attacks that exploit specific properties of f

Keccak

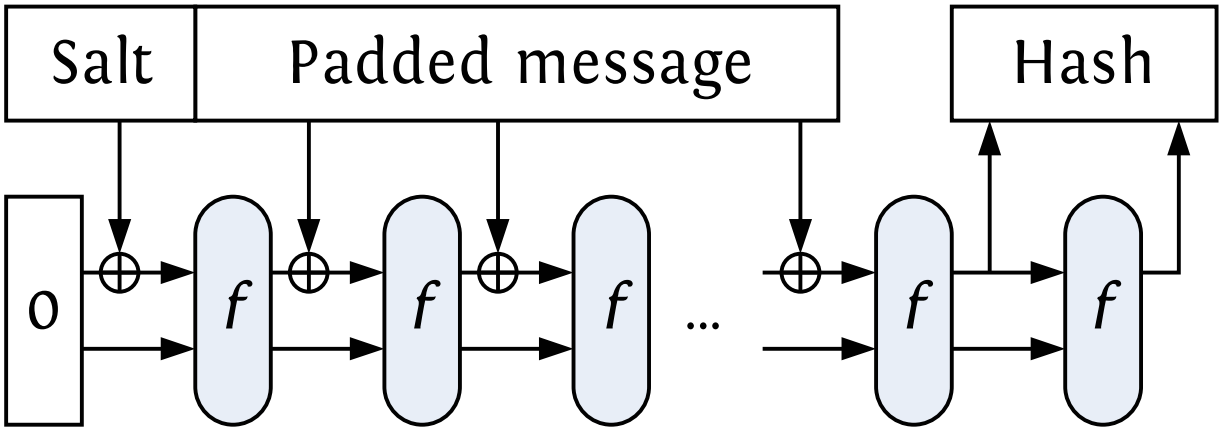
- Instantiation of a *sponge function*
- the permutation Keccak-f
  - 7 permutations: $b \in \{25, 50, 100, 200, 400, 800, 1600\}$
- Security-speed trade-offs using the same permutation, e.g.,
  - SHA-3 instance: $r = 1088$ and $c = 512$
    - permutation width: 1600
    - security strength 256: post-quantum sufficient
  - Lightweight instance: $r = 40$ and $c = 160$
    - permutation width: 200
    - security strength 80: same as SHA-1

Regular hashing



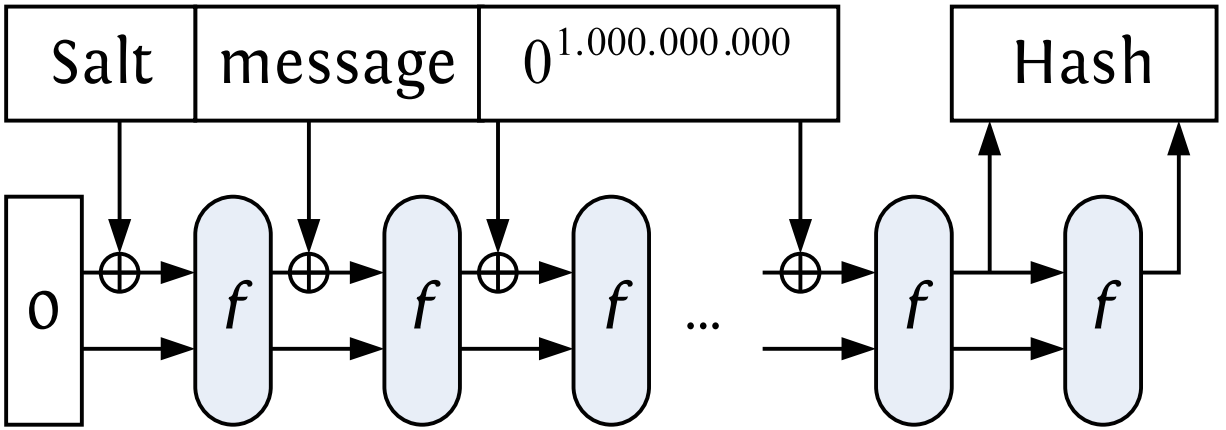
- Electronic signatures
- Data integrity (*shaXsum* ...)
- Data identifier (*Git, online anti-virus, peer-2-peer* ...)

Salted hashing



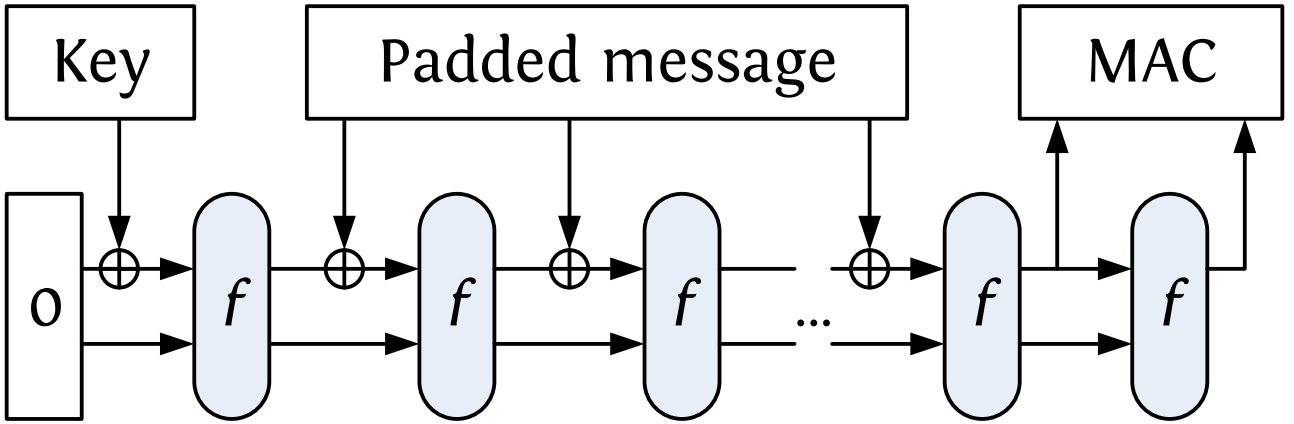
- Randomized hashing (RSASSA-PSS)
- Password storage and verification (*Kerberos*, /etc/shadow)

Salted hashing



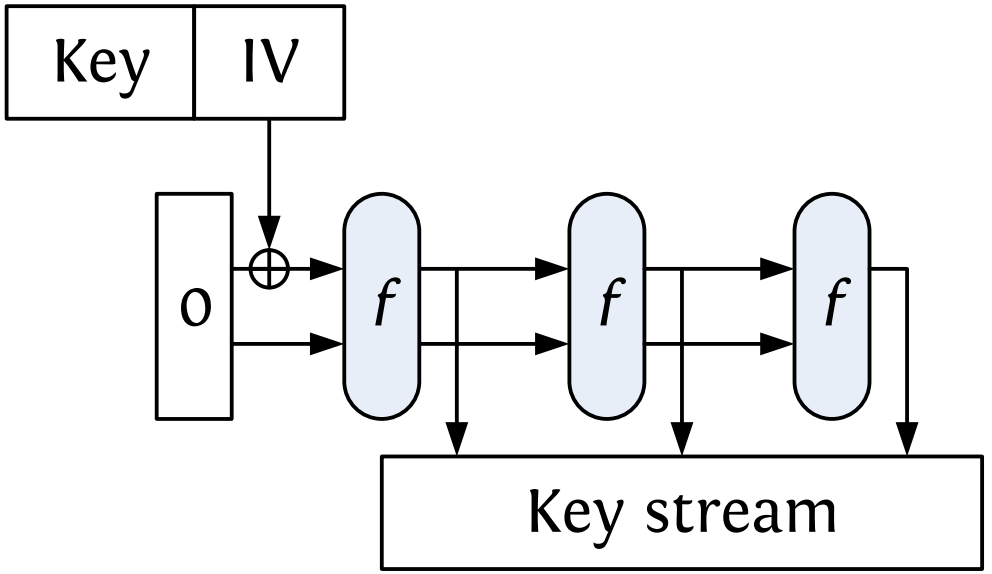
- Randomized hashing (RSASSA-PSS)
- Password storage and verification (*Kerberos*, /etc/shadow)
  - ...Can be as slow as you like it!

Message authentication codes



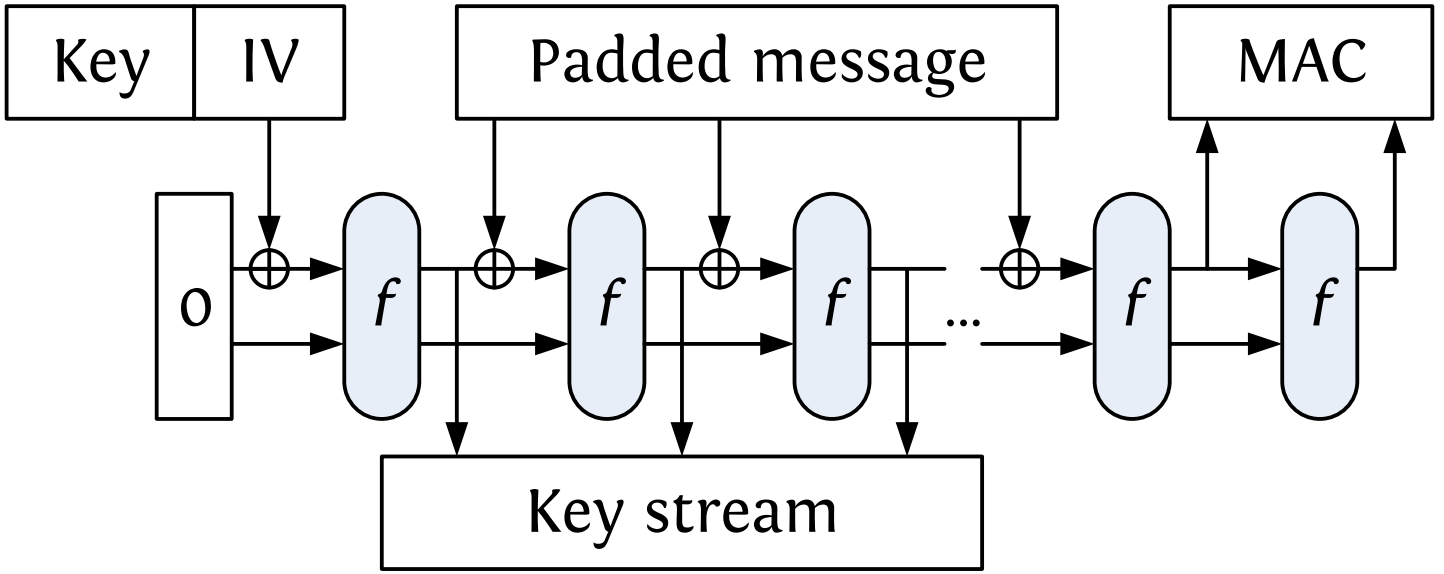
- As a message authentication code
- Simpler than HMAC [FIPS 198]
  - Required for SHA-1, SHA-2 due to length extension property
  - No longer needed for sponge

Stream encryption



- As a stream cipher
  - Long output stream per IV: similar to OFB mode
  - Short output stream per IV: similar to counter mode

Single pass authenticated encryption



- Authentication and encryption in a single pass!
- Secure messaging (*SSL/TLS, SSH, IPSEC* ...)