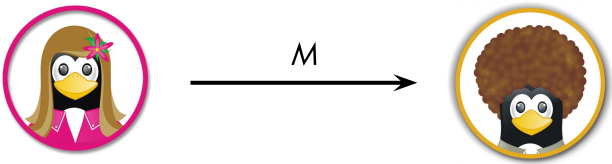
Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5

Pierre-Alain Fouque, Gaëtan Leurent, Phong Nguyen

Laboratoire d'Informatique de l'École Normale Supérieure

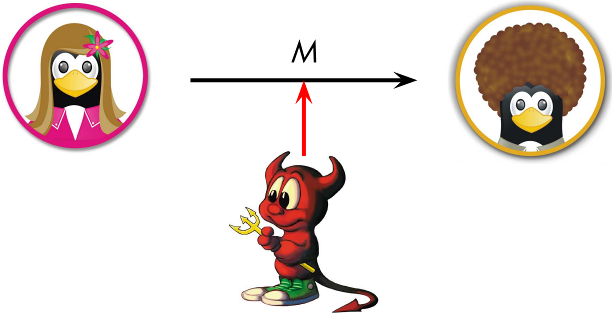
CRYPTO 2007

What is a MAC algorithm?



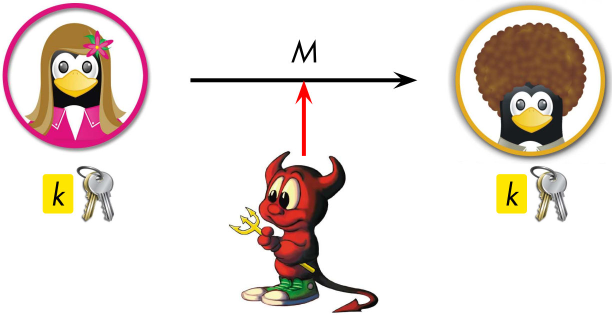
- Alice wants to send a message to Bob
- But Charlie has access to the communication channel
- Alice and Bob share a secret key k...
- ...and use a MAC algorithm.
- Bob rejects the message if $\mathrm{MAC}_k(M) \neq t$

What is a MAC algorithm?



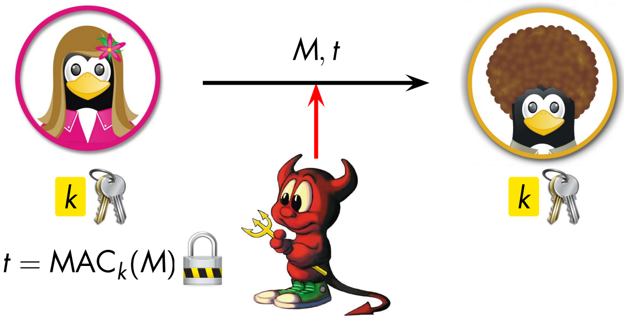
- Alice wants to send a message to Bob
- But Charlie has access to the communication channel
- Alice and Bob share a secret key k...
- ...and use a MAC algorithm.
- Bob rejects the message if $\mathrm{MAC}_k(M) \neq t$

What is a MAC algorithm?



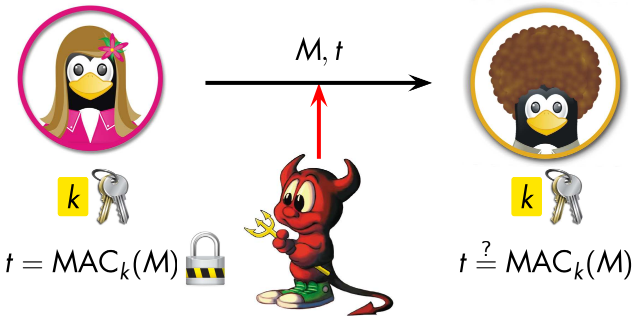
- Alice wants to send a message to Bob
- But Charlie has access to the communication channel
- Alice and Bob share a secret key k...
- ...and use a MAC algorithm.
- Bob rejects the message if $\mathrm{MAC}_k(M) \neq t$

What is a MAC algorithm?



- Alice wants to send a message to Bob
- But Charlie has access to the communication channel
- Alice and Bob share a secret key k...
- ...and use a MAC algorithm.
- Bob rejects the message if $\mathrm{MAC}_k(M) \neq t$

What is a MAC algorithm?



- Alice wants to send a message to Bob
- But Charlie has access to the communication channel
- Alice and Bob share a secret key k...
- ...and use a MAC algorithm.
- Bob rejects the message if $\mathrm{MAC}_k(M) \neq t$

MAC security

A MAC (Message Authentication Code) should provide authentication and integrity protection.

MAC security notions: chosen message attacks

The adversary has access to an oracle $M \mapsto \mathrm{MAC}_k(M)$.
He must compute a new MAC for:

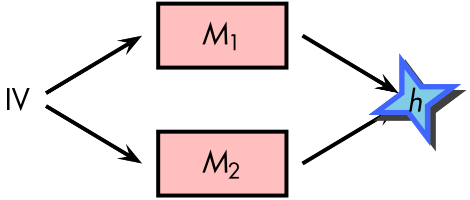
- One message of his choice: existential forgery.
- Any message: universal forgery.

One very popular MAC (ANSI, IETF, ISO, NIST), HMAC is based on a hash function.

Topic of the talk

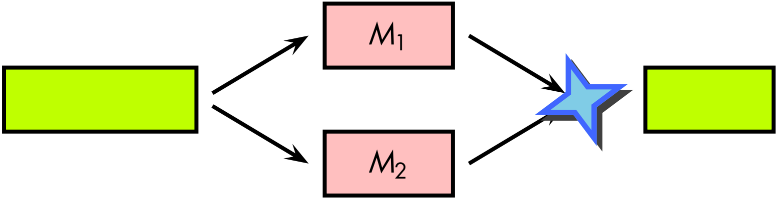
Can we use the attacks on MD4 or MD5 to break HMAC?

Known attacks on MD hash functions



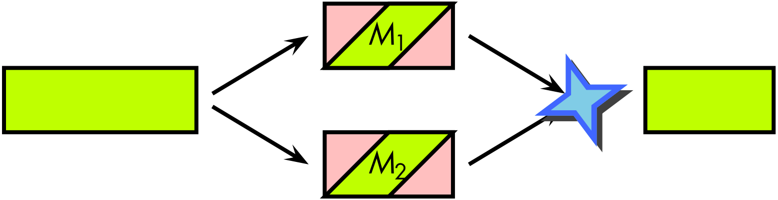
- Collision attacks:
  generate M_1, M_2: $H(M_1) = H(M_2)$
  - MD4 in 2^1, MD5 in 2^{27}, SHA-1 in 2^{63}
  - Colliding blocks look random
  - Limited impact: commitment
- Add a prefix and a suffix, hide the randomness
- Partial freedom in the colliding blocks
- Chosen prefix collisions:
  given P_1, P_2 generate M_1, M_2: $H(P_1||M_1) = H(P_2||M_2)$

Known attacks on MD hash functions



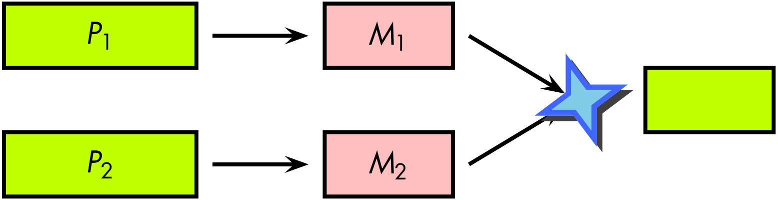
- Collision attacks:
  generate M_1, M_2: $H(M_1) = H(M_2)$
- Add a prefix and a suffix, hide the randomness
  - Include two documents, use the collision as a switch
  - Signature by a third party
  - Fraud is detectable
- Partial freedom in the colliding blocks
- Chosen prefix collisions:
  given P_1, P_2 generate M_1, M_2: $H(P_1||M_1) = H(P_2||M_2)$

Known attacks on MD hash functions



- Collision attacks:
  generate M_1, M_2: $H(M_1) = H(M_2)$
- Add a prefix and a suffix, hide the randomness
- Partial freedom in the colliding blocks
  - Weak challenge-response authentication: APOP
- Chosen prefix collisions:
  given P_1, P_2 generate M_1, M_2: $H(P_1||M_1) = H(P_2||M_2)$

Known attacks on MD hash functions



- Collision attacks:
  generate M_1, M_2: $H(M_1) = H(M_2)$
- Add a prefix and a suffix, hide the randomness
- Partial freedom in the colliding blocks
- Chosen prefix collisions:
  given P_1, P_2 generate M_1, M_2: $H(P_1||M_1) = H(P_2||M_2)$
  - Colliding certificates with *different* names.

MD family status

Current status

Collision-resistance is seriously broken,
but for most constructions, no real attacks are known:

- Key derivation
- Peer authentication
- HMAC
- ...

More in-depth study and improvement of Wang's attack are needed.

Our results on MD4

- We adapted Wang's attack to HMAC/NMAC.
- Universal forgery attack with 2^{88} data and 2^{95} CPU.

MD family status

Current status

Collision-resistance is seriously broken,
but for most constructions, no real attacks are known:

- Key derivation
- Peer authentication
- HMAC
- ...

More in-depth study and improvement of Wang's attack are needed.

Our results on MD4

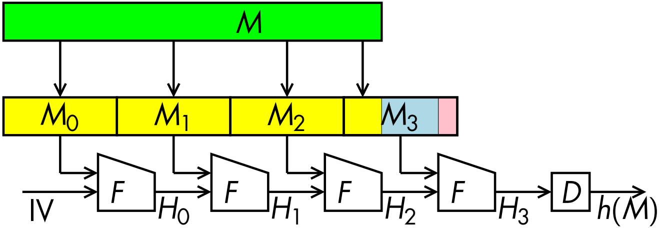
- We adapted Wang's attack to HMAC/NMAC.
- Universal forgery attack with 2^{88} data and 2^{95} CPU.

Outline

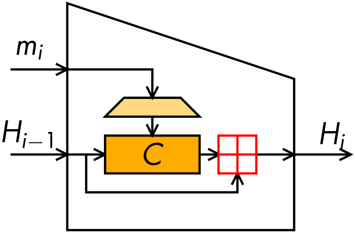
The MD4 hash function

General design

- Merkle-Damgård: $H_i = F(M_i, H_{i-1})$

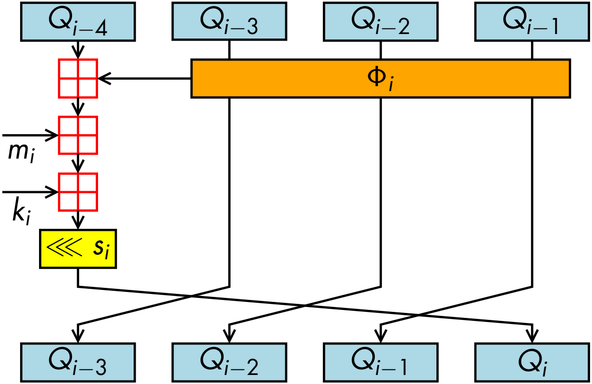


- Davies-Meyer with a Feistel-like cipher.



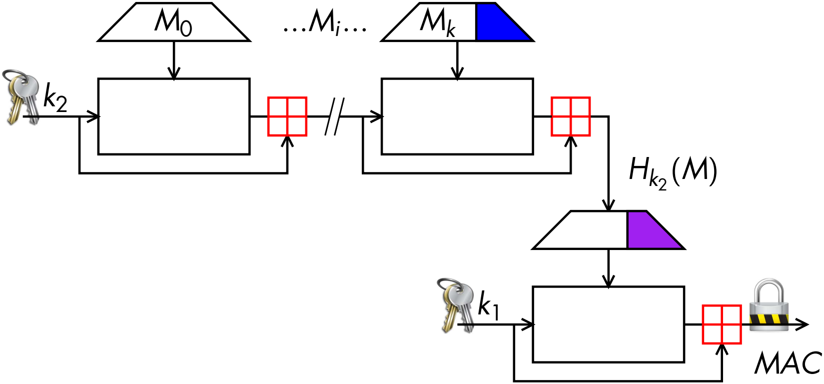
The MD4 compression function

Step update



- $Q_i = (Q_{i-4} \boxplus \Phi_i(Q_{i-1}, Q_{i-2}, Q_{i-3}) \boxplus m_i \boxplus k_i) \lll s_i$
- In: $Q_{-4} \| Q_{-1} \| Q_{-2} \| Q_{-3}$
- Out: $Q_{-4} \boxplus Q_{44} \| Q_{-1} \boxplus Q_{47} \| Q_{-2} \boxplus Q_{46} \| Q_{-3} \boxplus Q_{45}$

NMAC description



- $\mathrm{NMAC}_{k_1,k_2}(M) = H_{k_1}(H_{k_2}(M))$
- Keyed hash function H_k: replace the IV by the key.
- Prevents offline collision search and extension attacks.

HMAC description

- $\mathrm{HMAC}_k(M) = H(\bar{k} \oplus \mathrm{opad} \,||\, H(\bar{k} \oplus \mathrm{ipad} \,||\, M))$
  - opad and ipad are 1-block constants
  - $\bar{k}$ is k padded to one block
- No need to key the hash function.

- $\mathrm{HMAC}_k \approx \mathrm{NMAC}_{H(\bar{k}\oplus\mathrm{opad}),H(\bar{k}\oplus\mathrm{ipad})}$
- HMAC security is equivalent to NMAC security.

HMAC/NMAC security proof

If the compression function F is secure as a PRF then HMAC/NMAC is:

- secure against existential forgery up to $2^{n/2}$
- secure against universal forgery up to 2^n

Outline

MD4 Collisions: Wang's attack

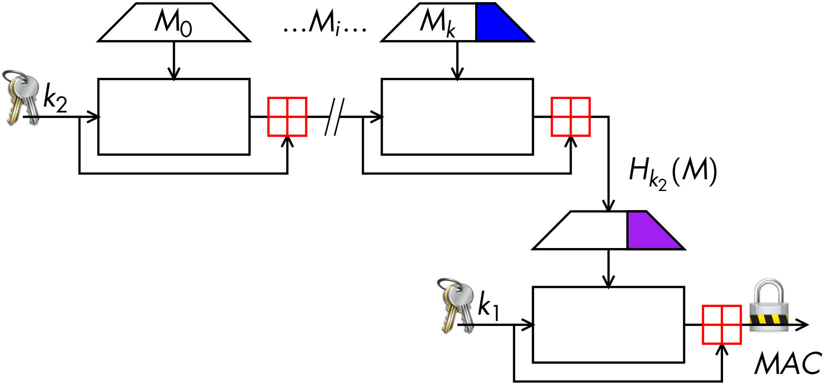
1. Precomputation:
   - Choose a message difference.
   - Compute a differential path.
   - Derive a set of sufficient conditions.
2. Collision search:
   - Find a message that satisfies the set of conditions.

Main result

We know a difference Δ and a set of conditions on the internal state variables Q_i's, such that:

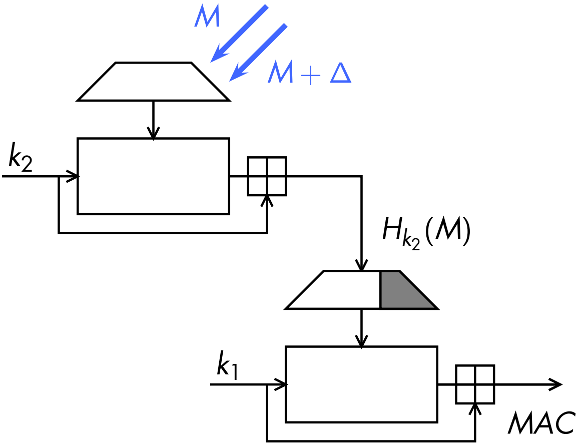
> *If all the conditions are satisfied by the internal state variable in the computation of $H(M)$, then $H(M) = H(M + \Delta)$.*

How to use collisions?



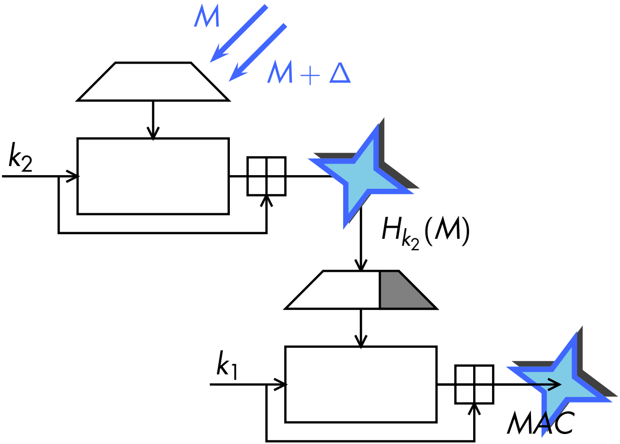
- We can detect hash collisions through NMAC collisions.
- Without the IV, we can't use message modifications.
- Try many pairs $(M, M + \Delta)$, and wait for a collision.
- The collision contains some key information, but we need a way to extract it...

Inner key recovery



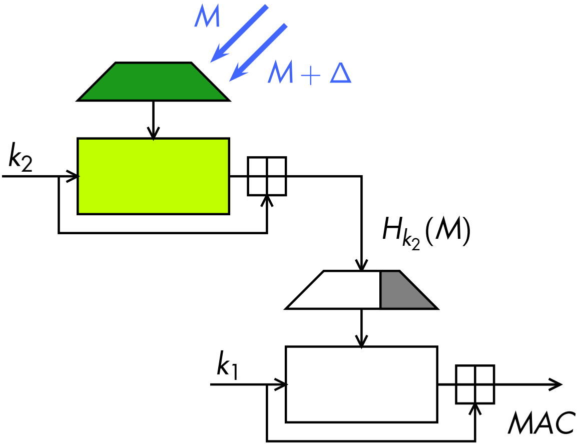
1. Find an inner collision.
2. Use M to modify the inner state.
3. Learn bits of Q_i by observing collisions; compute k_2.

Inner key recovery



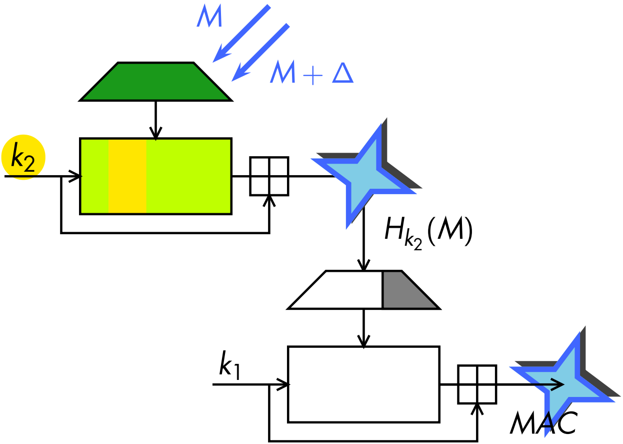
1. Find an inner collision.
2. Use M to modify the inner state.
3. Learn bits of Q_i by observing collisions; compute k_2.

Inner key recovery



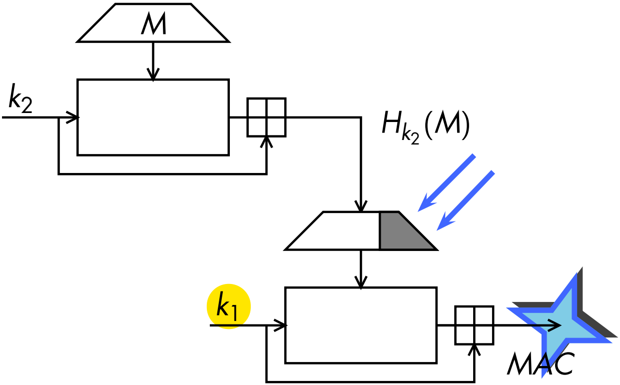
1. Find an inner collision.
2. Use M to modify the inner state.
3. Learn bits of Q_i by observing collisions; compute k_2.

Inner key recovery



1. Find an inner collision.
2. Use M to modify the inner state.
3. Learn bits of Q_i by observing collisions; compute k_2.

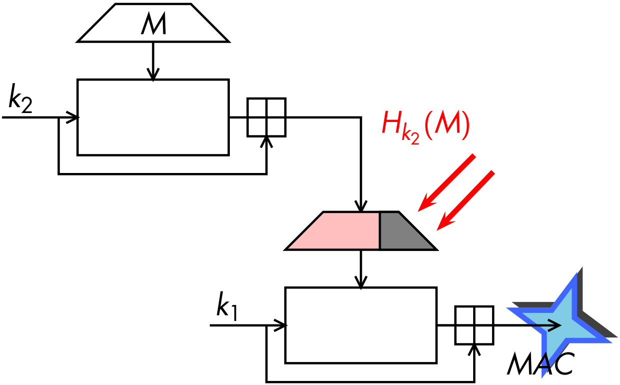
Outer key recovery



Problems

- We can't choose $H_{k_2}(M)$.
- We can only have a difference in the first 128 bits.

Outer key recovery



Problems

- We can't choose $H_{k_2}(M)$.
- We can only have a difference in the first 128 bits.

Contini and Yin's attack (Asiacrypt 2006)

- Recovers the inner key k_2 but not the outer key k_1.
- Best path: $p = 2^{-58}$.
  Complexity 2^{63}.
- Not enough for universal forgery.
  Attacker still need 2^n computations.

Outline

A New IV-recovery Attack

- We want to avoid the need for related messages.
- We look for paths where the existence of collision discloses information about the key.

Advantage

- In Contini-Yin attack, you need to choose a lot of bits in $H_{k_2}(M)$ (related messages).
- We only need to choose the differences in $H_{k_2}(M)$.

Using IV-dependent paths

- Use a differential path with $\delta m_0 \neq 0$.
- The beginning of the path depends on a condition (X) of the IV:
  - $p_X = \Pr_M[H(M) = H(M+\Delta)|X] \gg 2^{-128}$.

step	δm_i	$\partial\Phi_i$	∂Q_i	conditions
0	$\langle \blacktriangle^{[0]} \rangle$		$\langle \blacktriangle^{[3]} \rangle$	
1				$Q^{[3]}_{-1} = Q^{[3]}_{-2}$ (X)

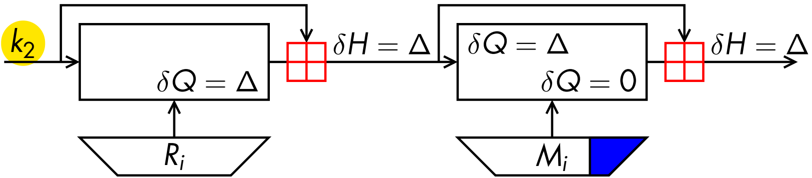
  - $\Pr_M[H(M) = H(M+\Delta)|\neg X] \ll p_X$.

step	δm_i	$\partial\Phi_i$	∂Q_i	conditions
0	$\langle \blacktriangle^{[0]} \rangle$		$\langle \blacktriangle^{[3]} \rangle$	
1		$\langle \blacktriangle^{[3]} \rangle$	$\langle \blacktriangle^{[10]} \rangle$	$Q^{[3]}_{-1} \neq Q^{[3]}_{-2}$ ($\neg$ X)

- We try $2/p_X$ pairs:
  - If we have a collision then (X) is satisfied.
  - Otherwise, (X) is not satisfied.

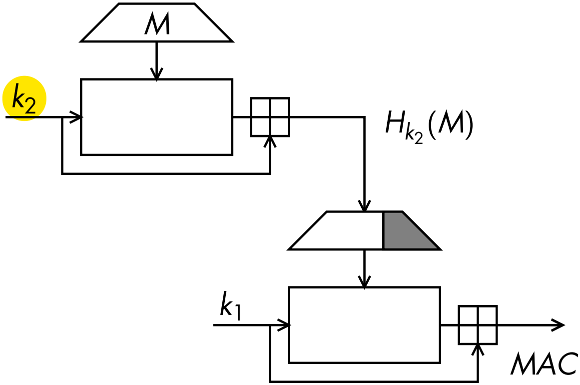
Efficient computation of message pairs

To recover the outer key, we need $2/p_X$ message pairs with $H_{k_2}(M_2) = H_{k_2}(M_1) + \Delta$



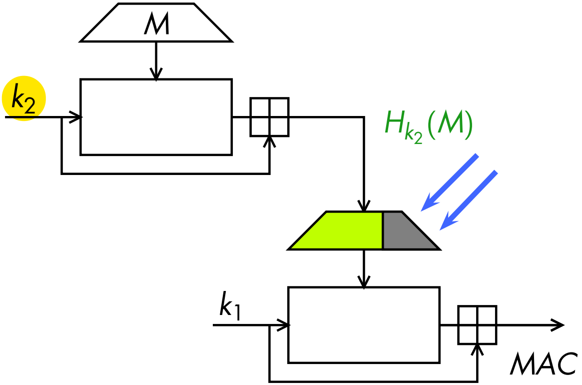
- We start with *one* message pair (R_1, R_2) such that $H_{k_2}(R_2) = H_{k_2}(R_1) + \Delta$ (birthday paradox).
- We compute second blocks (N_1, N_2) such that $H_{k_2}(R_2||N_2) = H_{k_2}(R_1||N_1) + \Delta$
- This is essentially a collision search with the padding inside the block.

New outer key recovery



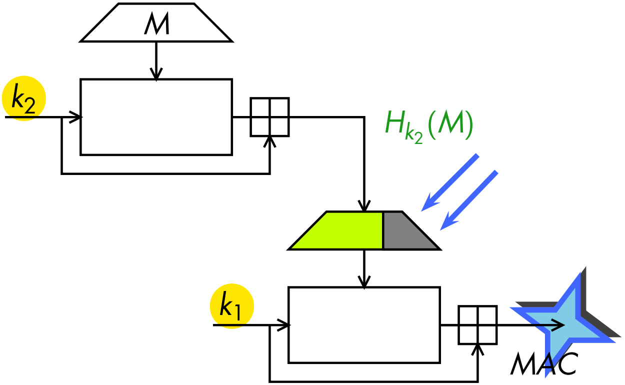
1. Recover k_2.
2. Generate pairs with $H_{k_2}(M_2) = H_{k_2}(M_1) + \Delta$.
3. Learn bits of k_1 by observing collisions.

New outer key recovery



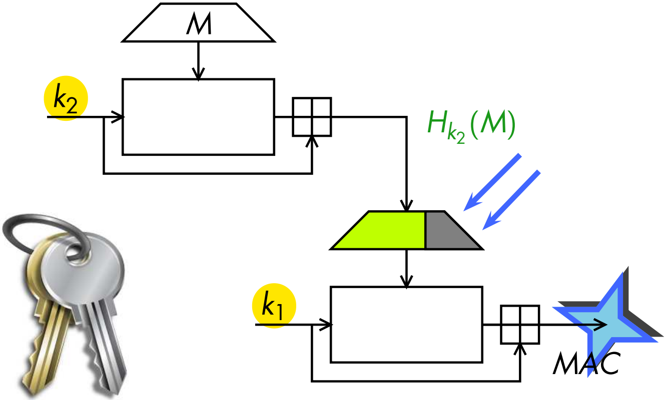
1. Recover k_2.
2. Generate pairs with $H_{k_2}(M_2) = H_{k_2}(M_1) + \Delta$.
3. Learn bits of k_1 by observing collisions.

New outer key recovery



1. Recover k_2.
2. Generate pairs with $H_{k_2}(M_2) = H_{k_2}(M_1) + \Delta$.
3. Learn bits of k_1 by observing collisions.

New outer key recovery



1. Recover k_2.
2. Generate pairs with $H_{k_2}(M_2) = H_{k_2}(M_1) + \Delta$.
3. Learn bits of k_1 by observing collisions.

Differential paths

We need very constrained paths:

- At least one difference in m_0.
- No difference in $m_4 \ldots m_{15}$.
- High probability.
- Many paths (each one gives only one bit of the key).

Differential path algorithm

- We use an algorithm to find a differential path from the message difference Δ.
- We found 22 paths with $p_X \approx 2^{-79}$.
- Attack complexity: 2^{88} data, 2^{105} time.

Differential paths

We need very constrained paths:

- At least one difference in m_0.
- No difference in $m_4 ... m_{15}$.
- High probability.
- Many paths (each one gives only one bit of the key).

Differential path algorithm

- We use an algorithm to find a differential path from the message difference Δ.
- We found 22 paths with $p_X \approx 2^{-79}$.
- Attack complexity: 2^{88} data, 2^{105} time.

Extracting more key bits

When we have a collision for one of the paths,
we can recover some extra information on the key:

step	s_i	δm_i	$\partial\Phi_i$	∂Q_i	conditions
0	3	$\langle\blacktriangle^{[0]}\rangle$		$\langle\blacktriangle^{[3]}\rangle$	
1	7				$Q_{-1}^{[3]} = Q_{-2}^{[3]}$ (X)
2	11				$Q_1^{[3]} = 0$ (Y)
3	19				$Q_2^{[3]} = 1$ (Z)
4	3			$\langle\blacktriangle^{[6]}\rangle$	

Note: (Y) and (Z) are not key bits, they depend on the message.

Use (Y) and (Z) to efficiently reduce the key entropy.

On average we reduce the search space from 2^{105} to 2^{94}.

Conclusion

- Hash collisions can be detected through HMAC/NMAC
- Tailoring Wang's attack: IV-dependent collisions
- Full key recovery

Attack complexity

Attacks		Data	Time	Mem	Remark
Generic	E-Forgery	$2^{n/2}$	-	-	Collision based
	U-Forgery	$2^{n/2}$	2^{n+1}	-	Collision based
		1	$2^{2n/3}$	$2^{2n/3}$	TM tradeoff, 2^n precpu
NMAC-MD4 HMAC-MD4	E-Forgery	2^{58}	-	-	
	Partial-KR	2^{63}	2^{40}	-	
	U-Forgery	2^{88}	2^{95}	-	New result

Conclusion

Possible improvements

- Find better paths.
- Use the method of Contini and Yin for the inner key.
- Use near-collisions for the outer key.

About MD5

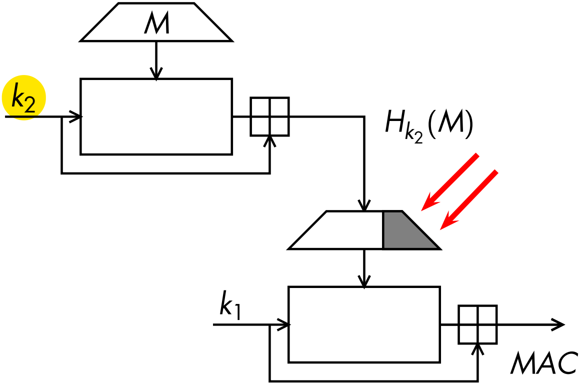
- Our NMAC-MD5 attack is in the related-key model.
- A real attack would require a differential path with less than one block of message...

More NMAC-MD5

Any Questions?

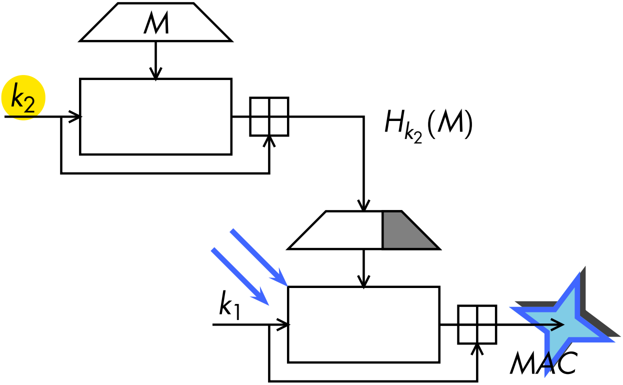
Thank you for your attention.

NMAC-MD5 attack



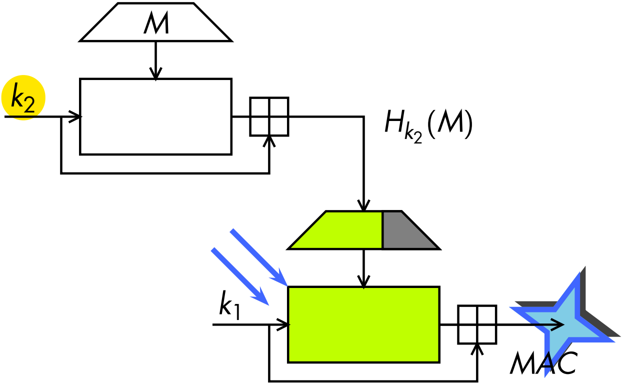
1. We don't have a path with a suitable Δ.
2. We use a path with a difference in the IV
3. Filter $H_{k_2}(M)$ to modify the outer state
4. Learn bits of Q_i by observing collisions; compute k_1.

NMAC-MD5 attack



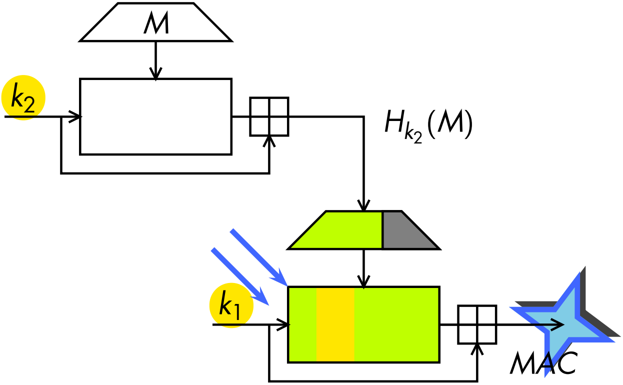
1. We don't have a path with a suitable Δ.
2. We use a path with a difference in the IV
3. Filter $H_{k_2}(M)$ to modify the outer state
4. Learn bits of Q_i by observing collisions; compute k_1.

NMAC-MD5 attack



1. We don't have a path with a suitable Δ.
2. We use a path with a difference in the IV
3. Filter $H_{k_2}(M)$ to modify the outer state
4. Learn bits of Q_i by observing collisions; compute k_1.

NMAC-MD5 attack



1. We don't have a path with a suitable Δ.
2. We use a path with a difference in the IV
3. Filter $H_{k_2}(M)$ to modify the outer state
4. Learn bits of Q_i by observing collisions; compute k_1.

NMAC-MD5 attack

- Small improvement of Contini & Yin's attack.
- Independently found by Rechberger & Rijmen (FC 2007).
- Related key model

Attacks		Data	Time	Mem	Remark
Generic	E-Forgery	$2^{n/2}$	-	-	Collision based
	U-Forgery	$2^{n/2}$	2^{n+1}	-	Collision based
		1	$2^{2n/3}$	$2^{2n/3}$	TM tradeoff, 2^n precpu
NMAC-MD5 *Related keys*	E-Forgery	2^{47}	-	-	
	Partial-KR	2^{47}	2^{45}	-	
	U-Forgery	2^{51}	2^{100}	-	New result

Conclusion

Differential paths

The next slides show some examples of the differential paths used in the NMAC attack.

For more information see:
Automatic search of differential path in MD4,
by Pierre-Alain Fouque, Gaëtan Leurent and Phong Nguyen,
Presented in the ECRYPT hash workshop, 2007,
Cryptology ePrint Archive, Report 2007/206.

Full Key-Recovery attack on HMAC-MD4

G. Leurent

NMAC-MD5

Diff. paths

An IV-dependent path

step	s_i	δm_i	$\partial\Phi_i$	∂Q_i	conditions
0	3	$\langle\blacktriangle^{[0]}\rangle$		$\langle\blacktriangle^{[3]}\rangle$	
1	7				$Q^{[3]}_{-1} = Q^{[3]}_{-2}$
2	11				$Q^{[3]}_{1} = 0$
3	19				$Q^{[3]}_{2} = 1$
4	3			$\langle\blacktriangledown\blacktriangle^{[6,7]}\rangle$	
5	7				$Q^{[6]}_{3} = Q^{[6]}_{2},\ Q^{[7]}_{3} = Q^{[7]}_{2}$
6	11				$Q^{[6]}_{5} = 0,\ Q^{[7]}_{5} = 0$
7	19		$\langle\blacktriangle^{[7]}\rangle$	$\langle\blacktriangle^{[26]}\rangle$	$Q^{[6]}_{6} = 1,\ Q^{[7]}_{6} = 0$
8	3		$\langle\blacktriangledown^{[26]}\rangle$	$\langle\blacktriangle^{[9]},\blacktriangledown^{[29]}\rangle$	$Q^{[26]}_{5} = 1,\ Q^{[26]}_{6} = 0$
9	7				$Q^{[9]}_{7} = Q^{[9]}_{6},\ Q^{[26]}_{8} = 0,\ Q^{[29]}_{7} = Q^{[29]}_{6}$
10	11				$Q^{[9]}_{9} = 0,\ Q^{[26]}_{9} = 1,\ Q^{[29]}_{9} = 0$
11	19			$\langle\blacktriangle^{[13]}\rangle$	$Q^{[9]}_{10} = 1,\ Q^{[29]}_{10} = 1$
12	3			$\langle\blacktriangledown^{[0]},\blacktriangle^{[12]}\rangle$	$Q^{[13]}_{10} = Q^{[13]}_{9}$
13	7				$Q^{[0]}_{11} = Q^{[0]}_{10},\ Q^{[12]}_{11} = Q^{[12]}_{10},\ Q^{[13]}_{12} = 0$
14	11		$\langle\blacktriangledown^{[0]}\rangle$	$\langle\blacktriangle\blacktriangle\blacktriangledown^{[11\ldots13]}\rangle$	$Q^{[0]}_{13} = 1,\ Q^{[12]}_{13} = 0,\ Q^{[13]}_{13} = 1$
15	19		$\langle\blacktriangledown^{[13]}\rangle$		$Q^{[0]}_{14} = 1,\ Q^{[11]}_{13} = Q^{[11]}_{12},\ Q^{[12]}_{13} = 0,\ Q^{[13]}_{13} = 1,\ Q^{[13]}_{12} = 0$
16	3	$\langle\blacktriangle^{[0]}\rangle$	$\langle\blacktriangle\blacktriangledown^{[12,13]}\rangle$		$Q^{[11]}_{15} = Q^{[11]}_{13},\ Q^{[12]}_{15} \neq Q^{[12]}_{13},\ Q^{[13]}_{15} \neq Q^{[13]}_{13}$
17	5				$Q^{[11]}_{16} = Q^{[11]}_{15},\ Q^{[12]}_{16} = Q^{[12]}_{15},\ Q^{[13]}_{16} = Q^{[13]}_{15}$
18	9			$\langle\blacktriangle\blacktriangle\blacktriangle\blacktriangledown^{[20\ldots23]}\rangle$	
19	13				$Q^{[20]}_{17} = Q^{[20]}_{16},\ Q^{[21]}_{17} = Q^{[21]}_{16},\ Q^{[22]}_{17} = Q^{[22]}_{16},\ Q^{[23]}_{17} = Q^{[23]}_{16}$
20	3		$\langle\blacktriangledown^{[23]}\rangle$	$\langle\blacktriangledown^{[26]}\rangle$	$Q^{[20]}_{19} = Q^{[20]}_{17},\ Q^{[21]}_{19} = Q^{[21]}_{17},\ Q^{[22]}_{19} = Q^{[22]}_{17},\ Q^{[23]}_{19} \neq Q^{[23]}_{17}$
21	5				$Q^{[20]}_{20} = Q^{[20]}_{19},\ Q^{[21]}_{20} = Q^{[21]}_{19},\ Q^{[22]}_{20} = Q^{[22]}_{19},\ Q^{[23]}_{20} = Q^{[23]}_{19},\ Q^{[26]}_{19} = Q^{[26]}_{18}$
22	9			$\langle\blacktriangledown^{[29]}\rangle$	$Q^{[26]}_{21} = Q^{[26]}_{19}$
23	13				$Q^{[26]}_{22} = Q^{[26]}_{21},\ Q^{[29]}_{21} = Q^{[29]}_{20}$
24	3			$\langle\blacktriangle\blacktriangledown^{[29,30]}\rangle$	$Q^{[29]}_{23} = Q^{[29]}_{21}$
25	5				$Q^{[30]}_{23} = Q^{[30]}_{22}$
26	9		$\langle\blacktriangle^{[29]}\rangle$		$Q^{[29]}_{25} \neq Q^{[29]}_{23},\ Q^{[30]}_{25} = Q^{[30]}_{23}$
27	13				$Q^{[29]}_{26} = Q^{[29]}_{25},\ Q^{[30]}_{26} = Q^{[30]}_{25}$
28	3			$\langle\blacktriangledown^{[0]}\rangle$	
29	5				$Q^{[0]}_{27} = Q^{[0]}_{26}$
30	9				$Q^{[0]}_{29} = Q^{[0]}_{27}$
31	13				$Q^{[0]}_{30} = Q^{[0]}_{29}$
32	3	$\langle\blacktriangle^{[0]}\rangle$			

A path for the message pair generation

step	s_i	δm_i	$\partial\Phi_i$	∂Q_i	conditions
-4	0			$\langle \blacktriangledown^{[4]} \rangle$	
-3	0				
-2	0				
-1	0				
0	3			$\langle \blacktriangledown^{[7]} \rangle$	
1	7	$\langle \blacktriangle^{[31]} \rangle$		$\langle \blacktriangle^{[6]} \rangle$	$Q_{-1}^{[7]} = Q_{-2}^{[7]}$
2	11	$\langle \blacktriangledown^{[28]}, \blacktriangle^{[31]} \rangle$		$\langle \blacktriangledown^{[7]}, \blacktriangle^{[10]} \rangle$	$Q_0^{[6]} = Q_{-1}^{[6]},\ Q_1^{[7]} = 0$
3	19				$Q_2^{[6]} = 0,\ Q_1^{[7]} = 0,\ Q_1^{[10]} = Q_0^{[10]}$
4	3		$\langle \blacktriangle^{[6]} \rangle$	$\langle \blacktriangle\blacktriangle\blacktriangledown^{[9\ldots11]} \rangle$	$Q_3^{[6]} = 0,\ Q_3^{[7]} = 0,\ Q_3^{[10]} = 0$
5	7			$\langle \blacktriangle^{[13]} \rangle$	$Q_4^{[7]} = 1,\ Q_3^{[9]} = Q_2^{[9]},\ Q_3^{[10]} = 0,\ Q_3^{[11]} = Q_2^{[11]}$
6	11		$\langle \blacktriangle\blacktriangledown^{[10,11]} \rangle$	$\langle \blacktriangledown^{[18]} \rangle$	$Q_5^{[9]} = 0,\ Q_5^{[10]} = 1,\ Q_5^{[11]} = 1,\ Q_4^{[13]} = Q_3^{[13]}$
7	19				$Q_6^{[9]} = 1,\ Q_6^{[10]} = 1,\ Q_6^{[11]} = 1,\ Q_6^{[13]} = 0,\ Q_5^{[18]} = Q_4^{[18]}$
8	3		$\langle \blacktriangle^{[13]} \rangle$	$\langle \blacktriangledown^{[12]}, \blacktriangle^{[16]} \rangle$	$Q_7^{[13]} = 0,\ Q_7^{[18]} = 0$
9	7		$\langle \blacktriangledown^{[12]} \rangle$	$\langle \blacktriangle^{[19]} \rangle$	$Q_7^{[12]} = 1,\ Q_6^{[12]} = 0,\ Q_7^{[16]} = Q_6^{[16]},\ Q_8^{[18]} = 1$
10	11			$\langle \blacktriangledown^{[29]} \rangle$	$Q_9^{[12]} = 0,\ Q_9^{[16]} = 0,\ Q_8^{[19]} = Q_7^{[19]}$
11	19				$Q_{10}^{[12]} = 1,\ Q_{10}^{[16]} = 1,\ Q_{10}^{[19]} = 0,\ Q_9^{[29]} = Q_8^{[29]}$
12	3	$\langle \blacktriangledown^{[16]} \rangle$	$\langle \blacktriangle^{[19]} \rangle$	$\langle \blacktriangle\blacktriangledown^{[15,16]}, \blacktriangle^{[22]} \rangle$	$Q_{11}^{[19]} = 0,\ Q_{11}^{[29]} = 0$
13	7			$\langle \blacktriangledown\blacktriangledown\blacktriangledown\blacktriangle^{[26\ldots29]} \rangle$	$Q_{11}^{[15]} = Q_{10}^{[15]},\ Q_{11}^{[16]} = Q_{10}^{[16]},\ Q_{11}^{[22]} = Q_{10}^{[22]},\ Q_{12}^{[29]} = 1$
14	11		$\langle \blacktriangle^{[29]} \rangle$		$Q_{13}^{[15]} = 0,\ Q_{13}^{[16]} = 0,\ Q_{13}^{[22]} = 0,\ Q_{12}^{[26]} = Q_{11}^{[26]},\ Q_{12}^{[27]} = Q_{11}^{[27]},\ Q_{12}^{[28]} = Q_{11}^{[28]},\ Q_{12}^{[29]} = 1,\ Q_{11}^{[29]} = 0$
15	19		$\langle \blacktriangledown\blacktriangle^{[28,29]} \rangle$	$\langle \blacktriangle^{[15]} \rangle$	$Q_{14}^{[15]} = 1,\ Q_{14}^{[16]} = 1,\ Q_{14}^{[22]} = 1,\ Q_{14}^{[26]} = 0,\ Q_{14}^{[27]} = 0,\ Q_{14}^{[28]} = 1,\ Q_{14}^{[29]} = 1$
16	3		$\langle \blacktriangle^{[15]} \rangle$	$\langle \blacktriangle^{[25]} \rangle$	$Q_{14}^{[15]} \neq Q_{13}^{[15]},\ Q_{15}^{[26]} = Q_{14}^{[26]},\ Q_{15}^{[27]} = Q_{14}^{[27]},\ Q_{15}^{[28]} = Q_{14}^{[28]},\ Q_{15}^{[29]} = Q_{14}^{[29]}$
17	5			$\langle \blacktriangle^{[31]} \rangle$	$Q_{16}^{[15]} = Q_{14}^{[15]},\ Q_{15}^{[25]} = Q_{14}^{[25]}$
18	9				$Q_{17}^{[15]} = Q_{16}^{[15]},\ Q_{17}^{[25]} = Q_{15}^{[25]},\ Q_{16}^{[31]} = Q_{15}^{[31]}$
19	13	$\langle \blacktriangledown^{[16]} \rangle$		$\langle \blacktriangledown^{[28]} \rangle$	$Q_{18}^{[25]} = Q_{17}^{[25]},\ Q_{18}^{[31]} = Q_{16}^{[31]}$
20	3	$\langle \blacktriangle^{[31]} \rangle$	$\langle \blacktriangledown^{[28]}, \blacktriangle^{[31]} \rangle$	$\langle \blacktriangle^{[28]}, \blacktriangledown^{[31]} \rangle$	$Q_{18}^{[28]} \neq Q_{17}^{[28]},\ Q_{19}^{[31]} \neq Q_{18}^{[31]}$
21	5		$\langle \blacktriangledown^{[31]} \rangle$		$Q_{19}^{[31]} \neq Q_{18}^{[31]}$
22	9				$Q_{21}^{[31]} = Q_{19}^{[31]}$
23	13		$\langle \blacktriangle^{[28]} \rangle$		$Q_{22}^{[28]} \neq Q_{21}^{[28]},\ Q_{22}^{[31]} = Q_{21}^{[31]}$
24	3	$\langle \blacktriangledown^{[28]}, \blacktriangle^{[31]} \rangle$			