A Collision for 70-step SHA-1 in a Minute

Christophe De Cannière and Florian Mendel
and Christian Rechberger

FSE 2007 Rump Session, 2007/03/27

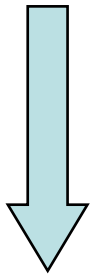
Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Actual Collisions for Reduced SHA-1

- CRYPTO 2005: Wang, Yin and Yu
  58-step Collision with about 2^{33} compression function calls

- ASIACRYPT 2006: De Cannière and Rechberger
  64-step Collision with about 2^{35} compression function calls



?

Full 80-step Collision

A Collision for 70-step SHA-1

$\sim 2^{40}$ CF $\sim 2^{43}$ CF

i	Message 1 (m_0), first block				Message 1 (m_1), second block			
1–4	3BB33AAE	85AECBBB	57A88417	8137CB9C	ABDDBEE2	42A20AC7	A915E04D	5063B027
5–8	4DE99220	5B6F12C7	726BD948	E3F6E9B8	4DDF989A	E0020CF7	7FFDC0F4	EFEFE0A7
9–12	23607799	239B2F1D	AAC76B94	E8009A1E	0FFBC2F0	C8DE16BF	81BBE675	254429CB
13–16	C24DE871	5B7C30D8	000359F5	90F9ED31	5F37A2C6	CD1963D3	FFCA1CB9	9642CB56
i	Message 2 (m_0^*), first block				Message 2 (m_1^*), second block			
1–4	ABB33ADE	35AECBE8	67A8841F	8137CBDF	3BDDBE92	F2A20A94	9915E045	5063B064
5–8	9DE99252	EB6F12D7	826BD92A	23F6E9FA	9DDF98E8	50020CE7	8FFDC096	2FEFE0E5
9–12	236077A9	C39B2F5F	8AC76BF4	08009A5F	0FFBC2C0	28DE16FD	A1BBE615	C544298A
13–16	E24DE821	9B7C3099	E0035987	30F9ED32	7F37A296	0D196392	1FCA1CCB	3642CB55
i	XOR-difference are the same for both blocks							
1–4	90000070	B0000053	30000008	00000043	90000070	B0000053	30000008	00000043
5–8	D0000072	B0000010	F0000062	C0000042	D0000072	B0000010	F0000062	C0000042
9–12	00000030	E0000042	20000060	E0000041	00000030	E0000042	20000060	E0000041
13–16	20000050	C0000041	E0000072	A0000003	20000050	C0000041	E0000072	A0000003
i	The colliding hash values							
1–5	151866D5	F7940D84	28E73685	C4D97E18	97DA712B			

Speed up to <1 second

- The method used for this example is heavily based on

  De Cannière and Rechberger: “Finding SHA-1 Characteristics: General Results and Applications”, Asiacrypt 2006.

- NEW: The “Programerang – Method”, based on

  Goldstine and von Neumann, “Planning and Coding of Problems for an Electronic Computing Instrument,” The Institute for Advanced Study, Princeton, NJ, 1947.

Speed up to <1 second

```
void main(void)
{
  printf("1st message:\n");
  printf("3BB33AAE 85AECBBB 57A88417 8137CB9C 4DE99220 5B6F12C7 726BD948 E3F6E9B8 ");
  printf("23607799 239B2F1D AAC76B94 E8009A1E C24DE871 5B7C30D8 000359F5 90F9ED31\n");

  printf("ABDDBEE2 42A20AC7 A915E04D 5063B027 4DDF989A E0020CF7 7FFDC0F4 EFEFE0A7 ");
  printf("0FFBC2F0 C8DE16BF 81BBE675 254429CB 5F37A2C6 CD1963D3 FFCA1CB9 9642CB56\n");

  printf("2nd message:\n);
  printf("ABB33ADE 35AECBE8 67A8841F 8137CBDF 9DE99252 EB6F12D7 826BD92A 23F6E9FA ");
  printf("236077A9 C39B2F5F 8AC76BF4 08009A5F E24DE821 9B7C3099 E0035987 30F9ED32\n");

  printf("3BDDBE92 F2A20A94 9915E045 5063B064 9DDF98E8 50020CE7 8FFDC096 2FEFE0E5 ");
  printf("0FFBC2C0 28DE16FD A1BBE615 C544298A 7F37A296 0D196392 1FCA1CCB 3642CB55\n");

}
```

Utilizes a new type of precomputation:

The “Compilerang-Technique”

A Collision for 70-step SHA-1 in a Minute

Christophe De Cannière and Florian Mendel
and Christian Rechberger

Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Disclaimer: not all slides are meant to be taken serious