Finding SHA-1 Characteristics - General Results and Applications

Christophe De Cannière and
Christian Rechberger

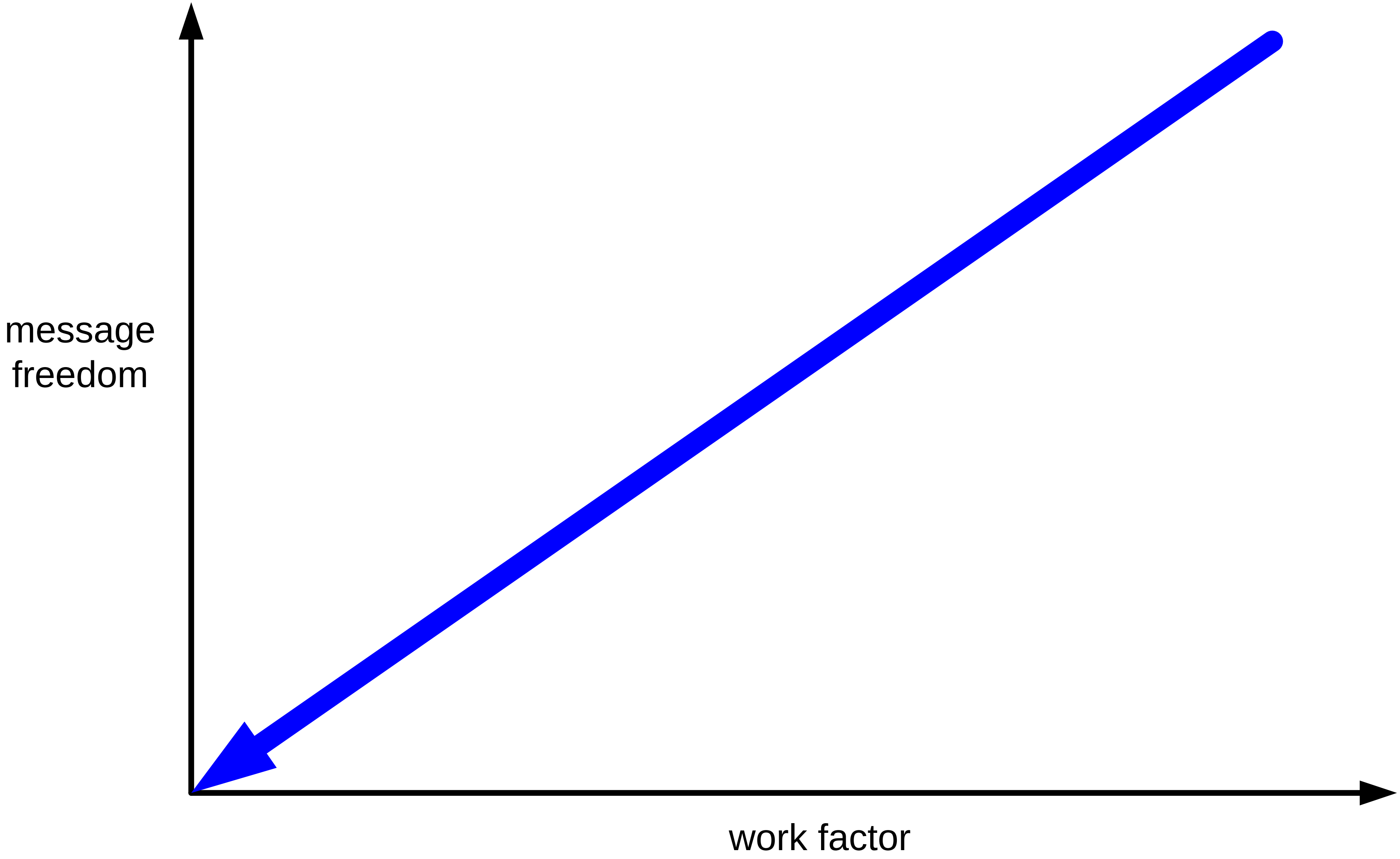
NIST Hash Function Workshop 2006

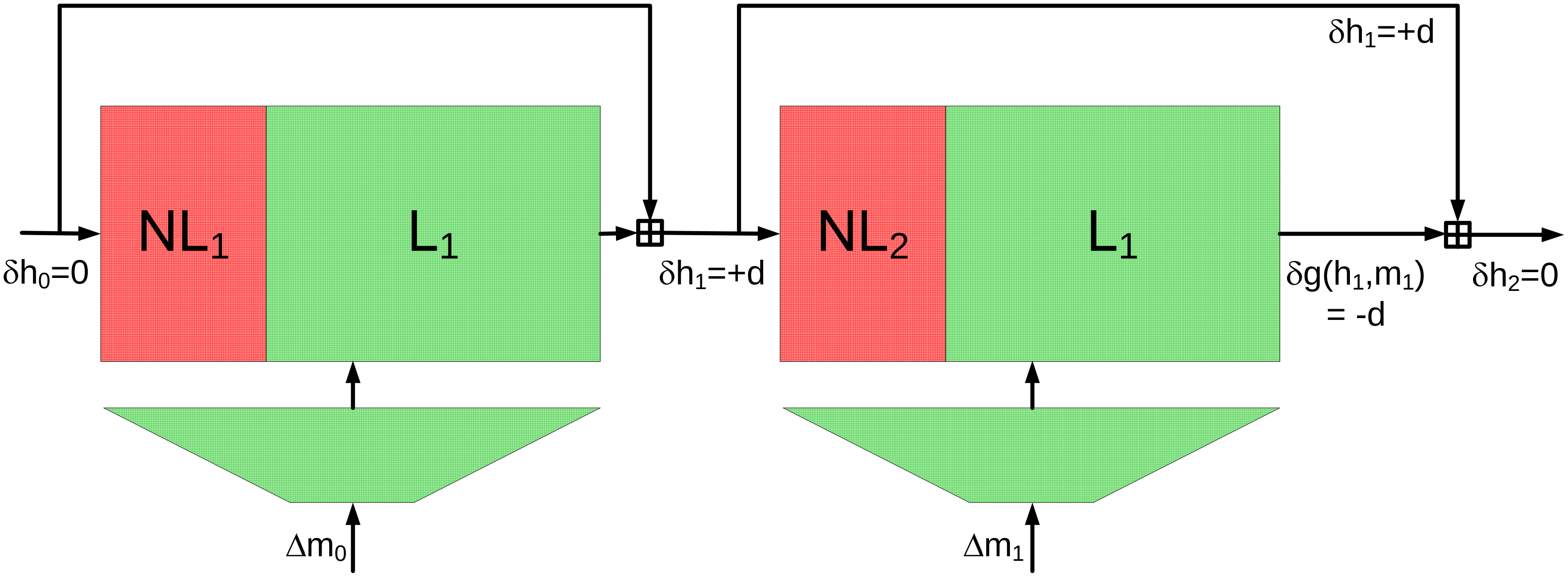
Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

To appear at ASIACRYPT 2006

Finding Collisions as a Continuing Optimization Process

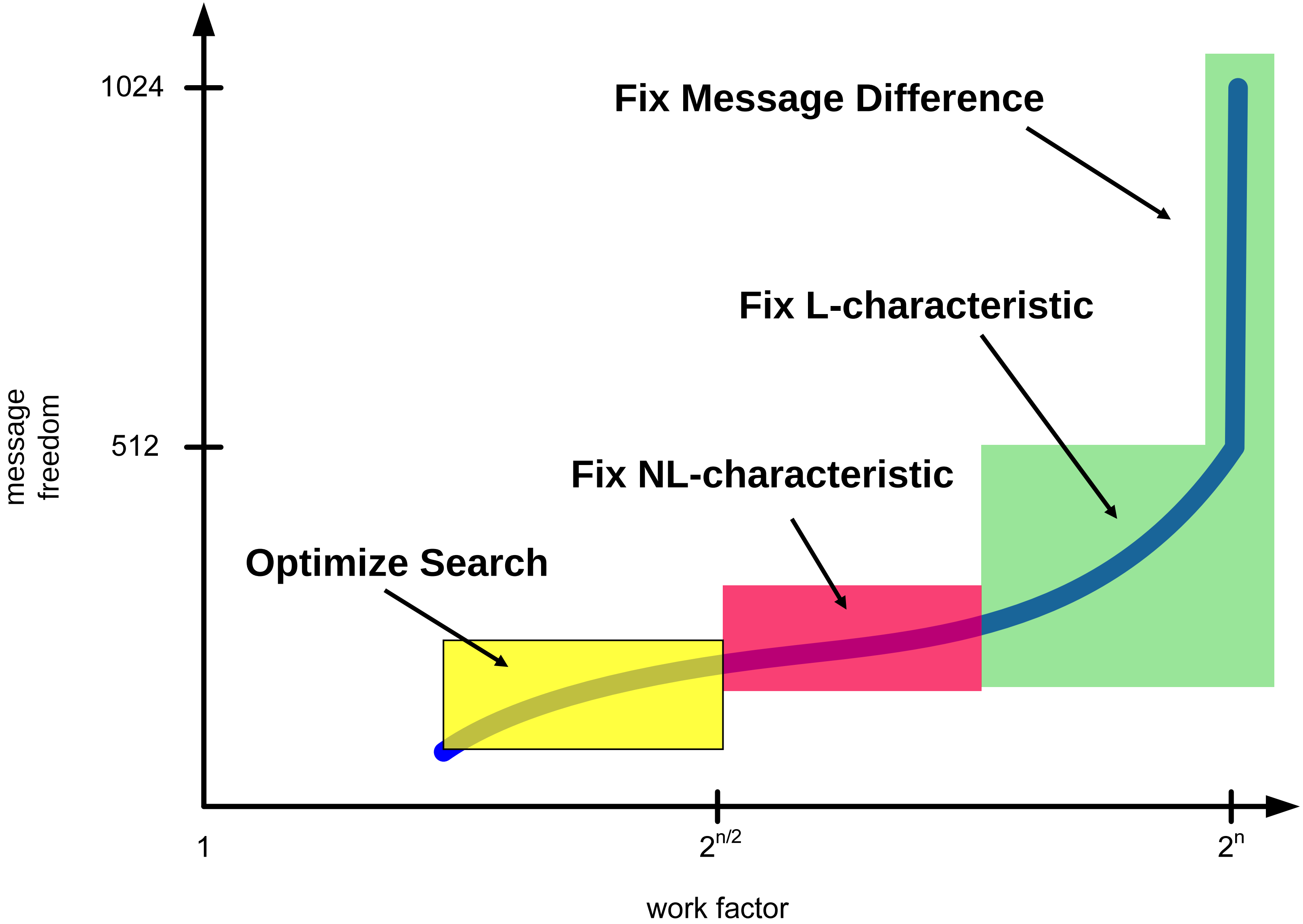




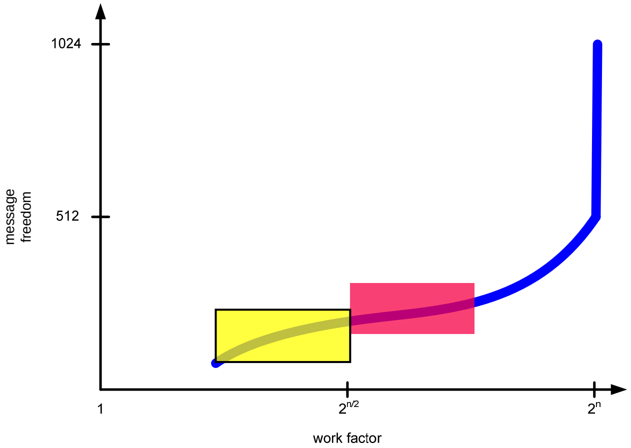
- Two key techniques of Wang et al.:
  - Manually find suitable complex characteristic NL_1 and NL_2
  - Advanced message modification to improve work factor

- Methods are rather ad hoc (manual)
- Optimization?

New View – Roughly Illustrated



Principles

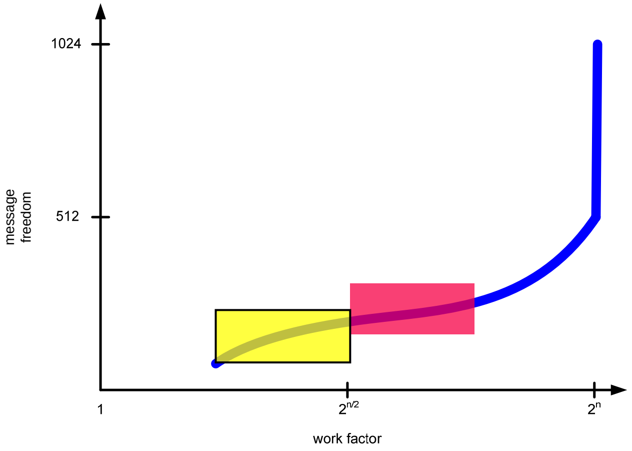


- Generalized conditions

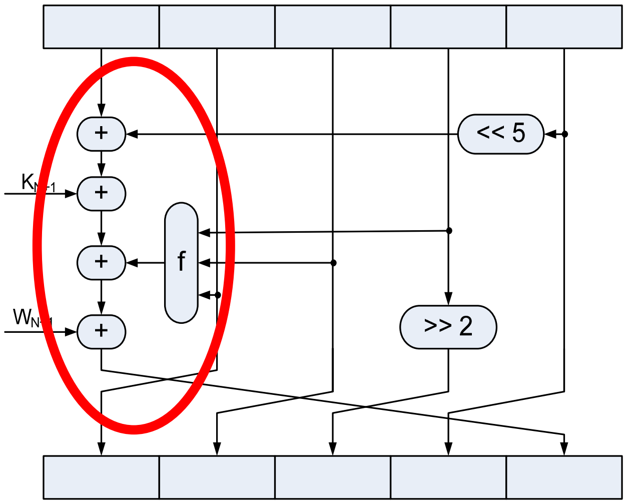
m	m*
0	0
0	1
1	0
1	1

Type	Possibilities
XOR	2
Signed-bit	4-6
Generalized:	**16**

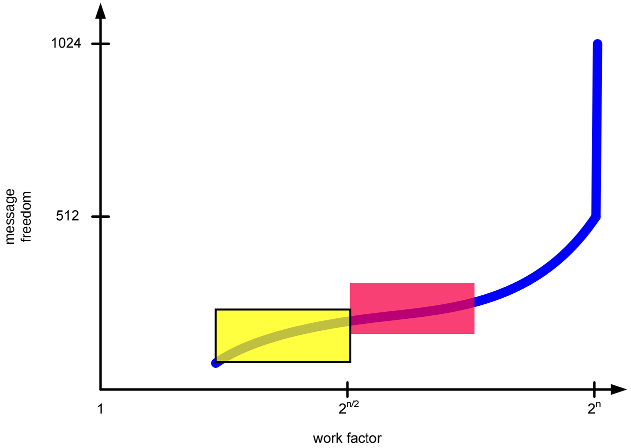
Principles



- Generalized conditions
- Use “bit-sliced design” to efficiently
  - Propagate conditions *within one* step transformation
  - Propagate conditions *among all* step transformations

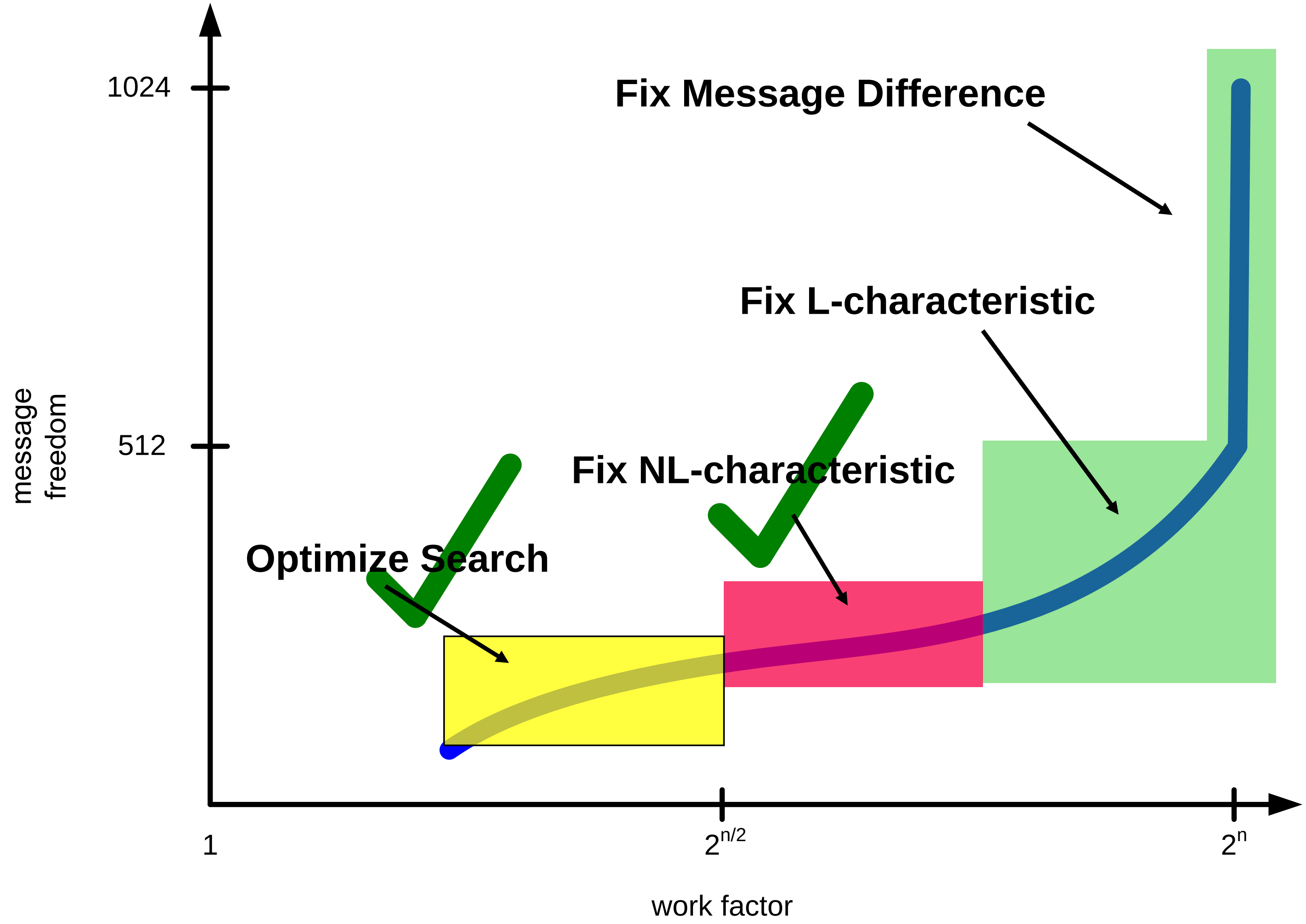


Principles

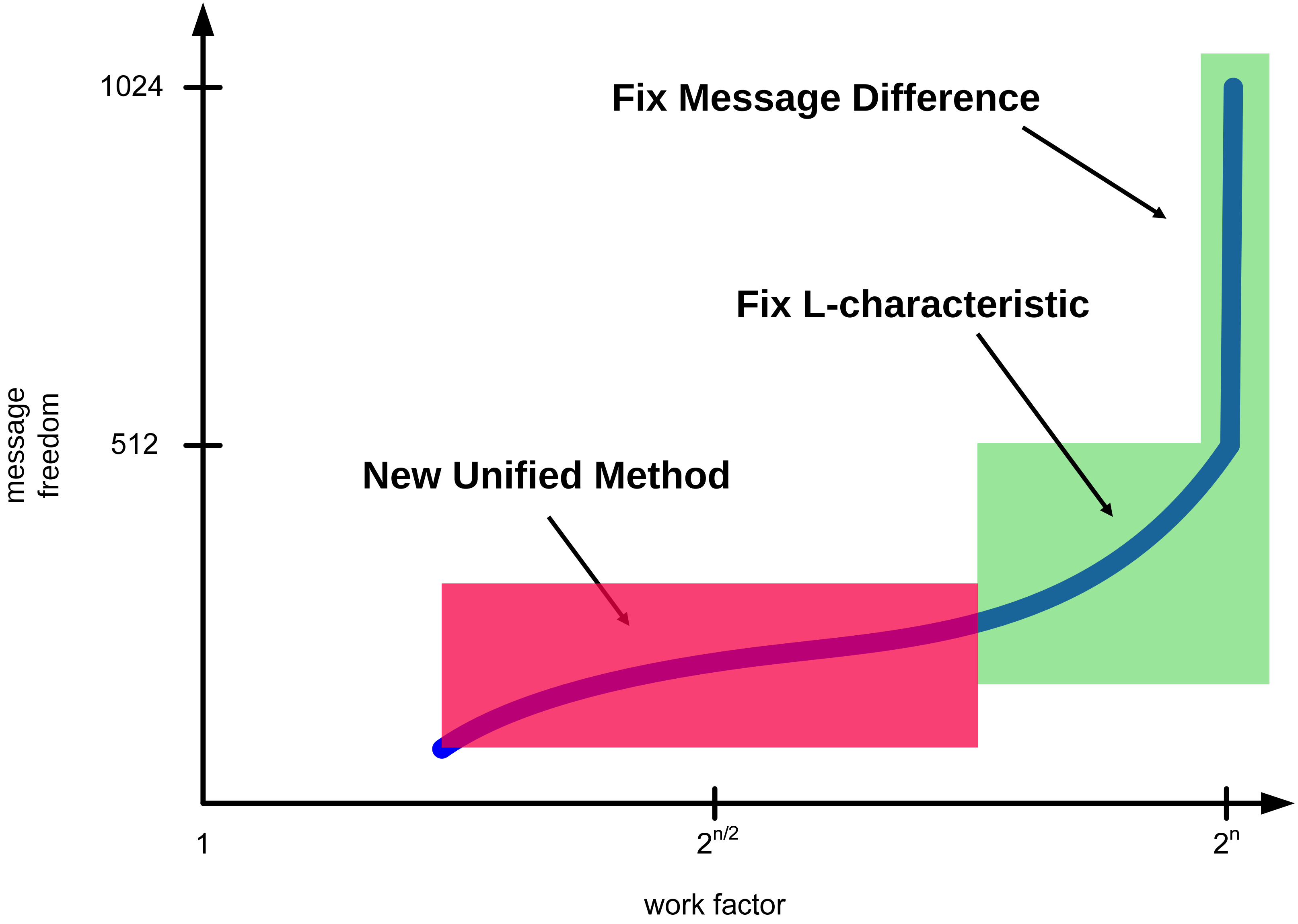


- Generalized conditions
- Use “bit-sliced design” to efficiently
  - Propagate conditions *within one* step transformation
  - Propagate conditions *among all* step transformations
- Precise estimate of work factor
  - Model: simple depth-first exhaustive search
  - #nodes in search tree
- **Continuously add more conditions to improve work factor**

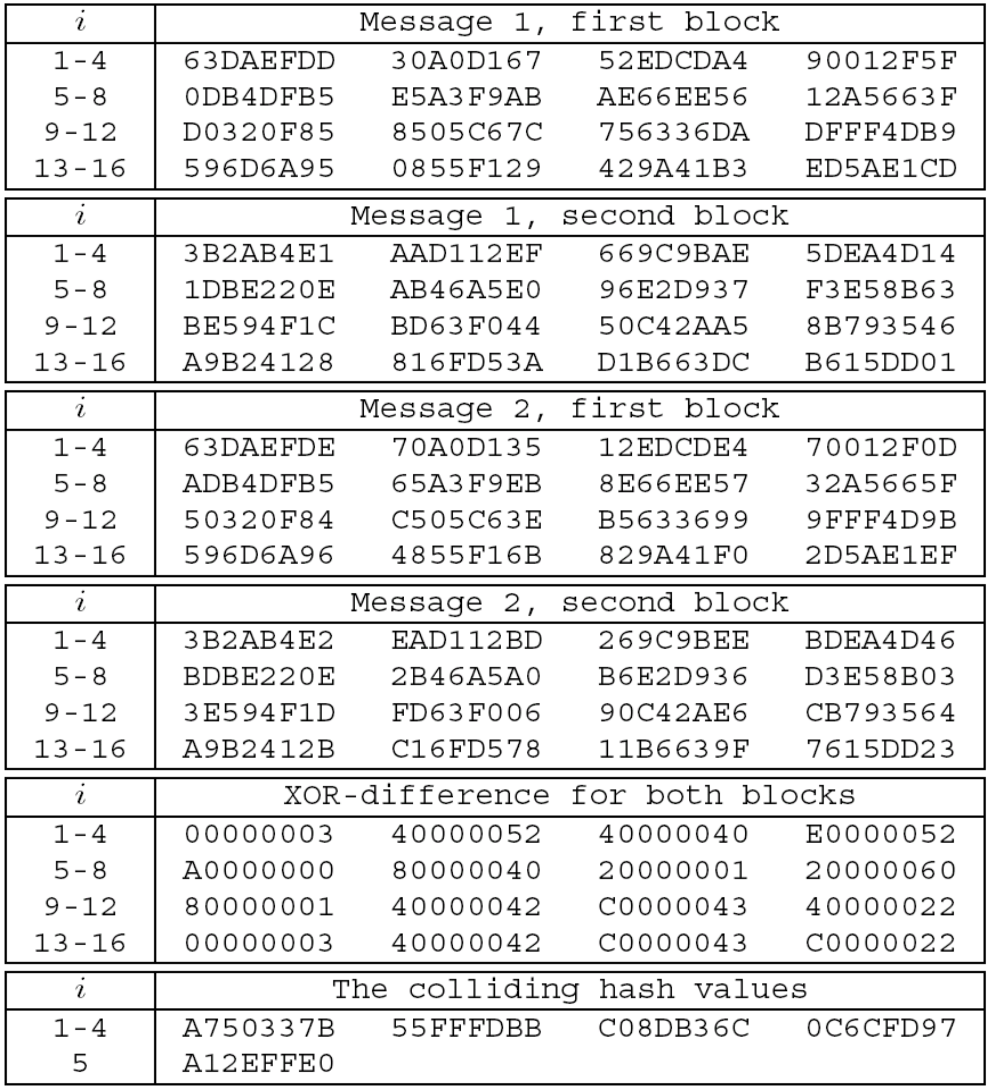
New View – Roughly Illustrated



New View – Roughly Illustrated



Example: 64-step SHA-1 Collision



i	Message 1, first block			
1-4	63DAEFDD	30A0D167	52EDCDA4	90012F5F
5-8	0DB4DFB5	E5A3F9AB	AE66EE56	12A5663F
9-12	D0320F85	8505C67C	756336DA	DFFF4DB9
13-16	596D6A95	0855F129	429A41B3	ED5AE1CD

i	Message 1, second block			
1-4	3B2AB4E1	AAD112EF	669C9BAE	5DEA4D14
5-8	1DBE220E	AB46A5E0	96E2D937	F3E58B63
9-12	BE594F1C	BD63F044	50C42AA5	8B793546
13-16	A9B24128	816FD53A	D1B663DC	B615DD01

i	Message 2, first block			
1-4	63DAEFDE	70A0D135	12EDCDE4	70012F0D
5-8	ADB4DFB5	65A3F9EB	8E66EE57	32A5665F
9-12	50320F84	C505C63E	B5633699	9FFF4D9B
13-16	596D6A96	4855F16B	829A41F0	2D5AE1EF

i	Message 2, second block			
1-4	3B2AB4E2	EAD112BD	269C9BEE	BDEA4D46
5-8	BDBE220E	2B46A5A0	B6E2D936	D3E58B03
9-12	3E594F1D	FD63F006	90C42AE6	CB793564
13-16	A9B2412B	C16FD578	11B6639F	7615DD23

i	XOR-difference for both blocks			
1-4	00000003	40000052	40000040	E0000052
5-8	A0000000	80000040	20000001	20000060
9-12	80000001	40000042	C0000043	40000022
13-16	00000003	40000042	C0000043	C0000022

i	The colliding hash values			
1-4	A750337B	55FFFDBB	C08DB36C	0C6CFD97
5	A12EFFE0			

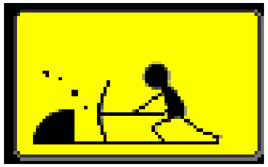
- 64-step 2-block colliding pair of messages
- Work factor was equivalent to 2^{35} SHA-1 computations
(1 day on a single PC)

Summary – What's new?

Automatically finding complex characteristics for SHA-1 ✓

Precise calculation of work factor and available degrees of freedom for collision search ✓

New and slim final search procedure



Future Work / Work in Progress

- Updated 80-step estimate
- Apply to other hash functions like RIPEMD-160, SHA-2 members
- Allow arbitrary different messages before colliding block
- Speedup for herding attacks

Finding SHA-1 Characteristics

Christophe De Cannière and
Christian Rechberger

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

***Faculty of Computer Science
Graz University of Technology***

http://www.iaik.tugraz.at/research/krypto