

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

NGUYỄN HỮU HOÀNG

**NGHIÊN CỨU
ĐỘ AN TOÀN CỦA HÀM BẮM MD5**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2013

Số hóa bởi Trung tâm Học liệu

<http://lrc.tnu.edu.vn/>

Số hóa bởi Trung tâm Học liệu

<http://lrc.tnu.edu.vn/>

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

NGUYỄN HỮU HOÀNG

**NGHIÊN CỨU
ĐỘ AN TOÀN CỦA HÀM BẮM MD5**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. Hồ Văn Canh

Thái Nguyên - 2013

MỤC LỤC

MỞ ĐẦU	1
CHƯƠNG 1 LÝ THUYẾT VỀ HÀM BẮM	2
1.1. Định nghĩa hàm băm.....	2
1.2. Các tính chất của hàm băm.....	3
1.3. Xung đột băm	3
1.4. Ứng dụng	4
1.5. Một số hàm băm phổ biến	4
1.5.1. Hàm băm MD4.....	6
1.5.2. Hàm băm SHA-1.....	6
1.5.3. Hàm băm SHA-256.....	8
1.5.4. Hàm băm SHA-384, SHA-512.....	10
CHƯƠNG 2 HÀM BẮM MD5	15
2.1. Giới thiệu	15
2.2. Khái niệm.....	15
2.3. Ứng dụng	16
2.4. Thuật giải	16
2.5. Sự khác nhau MD4 và MD5.....	24
CHƯƠNG 3 ĐÁNH GIÁ ĐỘ AN TOÀN MD5 DỰA TRÊN THỬ NGHIỆM TẤN CÔNG	25
3.1. Tấn công hàm băm.....	25
3.2. Các phương pháp tấn công hàm băm phổ biến	25
3.2.1. Tấn công dựa trên lý thuyết ngày sinh	25
3.2.2. Tấn công mở rộng chiều dài trên MD5 (Length-Extension Attack).....	27
3.2.3. Tấn công thuật toán	29
3.2.4. Tấn công theo nguyên lý vét cạn.....	36

3.3. Đánh giá độ an toàn MD5 dựa trên việc sử dụng các bộ xử lý đồ họa GPU để tính toán khôi phục mật khẩu	36
3.3.1. Những ưu điểm của GPU so với CPU	37
3.3.2. Sử dụng Cluster GPU tính toán khôi phục mật khẩu MD5	39
3.3.3. Kết luận về độ an toàn MD5	48
KẾT LUẬN.....	52
TÀI LIỆU THAM KHẢO.....	53

LỜI CẢM ƠN

Đầu tiên, tôi xin gửi lời cảm ơn chân thành và sắc nhất tới Tiến sỹ Hồ Văn Canh, thầy đã tận tình chỉ bảo và giúp đỡ tôi trong suốt quá trình làm luận văn. Bên cạnh những kiến thức tôi còn học hỏi được ở thầy tinh thần làm việc khoa học và nghiêm túc.

Tôi xin chân thành cảm ơn tới Khoa CNTT Trường Đại học Công nghệ thông tin và Truyền thông, các thầy cô đã giúp đỡ và tận tình truyền đạt các kiến thức cho tôi trong suốt quá trình học tập và nghiên cứu. Tôi xin cảm ơn ban chủ nhiệm khoa và các cán bộ đã tạo điều kiện tốt nhất cho chúng tôi trong quá trình học tập và hoàn thành luận văn của mình.

Tôi xin bày tỏ lòng biết ơn tới gia đình, bạn bè, đồng nghiệp và những người thân đã động viên khích lệ tinh thần và giúp đỡ tôi hoàn thành luận văn này.

LỜI CAM ĐOAN

Tôi xin cam đoan, toàn bộ nội dung liên quan tới đề tài được trình bày trong luận văn là bản thân tôi tự tìm hiểu và nghiên cứu, dưới sự hướng dẫn của Thầy giáo TS. Hồ Văn Canh.

Các tài liệu, số liệu tham khảo được trích dẫn đầy đủ nguồn gốc. Tôi xin chịu trách nhiệm trước pháp luật lời cam đoan của mình.

Học viên thực hiện

Nguyễn Hữu Hoàng

THUẬT NGỮ VIẾT TẮT

Số thứ tự	Thuật Ngữ	Tên Đầy Đủ
1	MAC	Message Authentication Code
2	HMAC	Keyed-Hash Message Authentication Code
3	opad	Outer pad
4	ipad	Inner pad
5	SHA	Secure Hash Algorithm
6	MD	Merkle-Damgård
7	TLS	Transport Layer Security
8	CA	Certification Authority
9	IPSec	Internet Protocol Security
10	GPU	Graphic Proccessing Unit
11	SM	Streaming Multiprocessor

Ý NGHĨA CÁC KÝ HIỆU

Số thứ tự	Ký hiệu	Ý nghĩa
1	$\oplus$	Phép toán XOR
2	$\lll$	Phép dịch bit vòng
3	$\parallel$	Phép ghép chuỗi
4	$\vee$	Phép OR
5	$\wedge$	Phép AND
6	$\neg$	Phép phủ định
7	$+$	Phép cộng module 2^{32}
8	$\text{ROTR}^n(x)$	Dịch xoay vòng x sang bên phải n bit
9	$\text{SHR}^n(x)$	Dịch bit của số x sang bên phải n bit

DANH MỤC HÌNH VẼ

<i>Hình 1.2. Cấu trúc lặp của hàm băm MD.....</i>	<i>5</i>
<i>Hình 2.1. Thuật toán mô tả MD5/SHA-1</i>	<i>19</i>
<i>Hình 3.1. Cấu trúc lặp Merkle-Damgård (sao chép từ Wikipedia).....</i>	<i>28</i>
<i>Hình 3. 2. Tấn công mở rộng chiều dài</i>	<i>28</i>
<i>Hình 3. 3. Biểu đồ so sánh sự phát triển của GPU và CPU</i>	<i>38</i>
<i>Hình 3.4. So sánh số nhân của GPU và CPU.....</i>	<i>38</i>
<i>Hình 3.5. Mô tả chiến lược kiểm tra mật khẩu song song</i>	<i>40</i>
<i>Hình 3. 6. Chia mật khẩu vào các nhóm.....</i>	<i>41</i>
<i>Hình 3.7. Tạo giá trị băm cho mật khẩu</i>	<i>49</i>
<i>Hình 3.8. Add giá trị băm của mật khẩu vào phần mềm</i>	<i>50</i>
<i>Hình 3.9. Quá trình tạo và kiểm tra mật khẩu</i>	<i>50</i>
<i>Hình 3.10. Tìm kiếm mật khẩu thành công</i>	<i>51</i>