

PERANCANGAN IMPLEMENTASI SHA-1 PASSWORD CRACKING BERBASIS FPGA:

Studi Kasus Instansi XYZ

TESIS



Oleh:

SITI ZAIM

1111600423

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

JAKARTA

2013

PERANCANGAN IMPLEMENTASI SHA-1 PASSWORD CRACKING BERBASIS FPGA:

Studi Kasus Instansi XYZ

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer



Oleh:

SITI ZAIM

1111600423

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

JAKARTA

2013



LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama Mahasiswa :SITI ZAIM.....
Nomor Induk Mahasiswa :1111600423.....
Program Studi :MAGISTER ILMU KOMPUTER.....
Konsentrasi :REKAYASA KOMPUTASI TERAPAN.....
Fakultas/Program :PASCA SARJANA.....

Menyatakan bahwa Tesis yang berjudul:

.....PERANCANGAN SHA-1 PASSWORD CRACKING BERBASIS FPGA :
.....STUDI KASUS INSTANSI XY2.....
.....

1. merupakan hasil karya tulis ilmiah saya sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta,16 FEBRUARI 2013.....

.....SITI ZAIM.....

Catatan: isian ditulis tangan



LEMBAR PENGESAHAN

Nama Mahasiswa : Siti Zaim
Nomor Induk Mahasiswa : 1111600423
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul : Perancangan SHA-1 Password Cracking
Berbasis FPGA: Studi Kasus Instansi XYZ

Jakarta, 16 Pebruari 2013

Tim Penguji:

Tanda Tangan:

Ketua,

Dr. Ir. Nazori AZ, M.T.

Anggota,

Dr. Moedjiono, M.Sc.

Hadi Syahrial, M.M, M.KOM

Pembimbing Utama,

Dr. Ir. Nazori, AZ, M.T.

Pembimbing Pendamping,

Hadi Syahrial, M.M, M.KOM

Ketua Program Studi

Dr. Ir. Nazori AZ, M.T.

ABSTRAK

Seiring berkembangnya teknologi informasi dan komunikasi yang pesat, saat ini terdapat banyak layanan *software* yang menyediakan sistem otentikasi yang berdasarkan pada kombinasi identitas pengguna (*username*) dan *password*. *Password* tersebut disimpan dalam bentuk *digest* yang dihasilkan dari perhitungan menggunakan skema fungsi hash tertentu, salah satunya SHA-1. Instansi XYZ merupakan instansi pemerintah yang bergerak dalam bidang pengamanan informasi. Instansi XYZ membutuhkan kecepatan komputasi untuk melakukan kriptanalisis termasuk *password cracking* di dalamnya. FPGA merupakan salah satu teknologi komputasi dengan performansi tinggi. Pada penelitian ini dilakukan perancangan implementasi SHA-1 *password cracking* berbasis FPGA. SHA-1 *password cracking* dilakukan dengan menggunakan metode *brute force attack*. Hasil penelitian ini membuktikan bahwa FPGA dapat lebih cepat dari *Personal Computer* (PC) dalam melakukan SHA-1 *password cracking*. Hasil akhir dari penelitian ini berupa rancangan implementasi SHA-1 *password cracking* berbasis FPGA bagi Instansi XYZ. Dengan menggunakan rancangan ini, Instansi XYZ dapat melakukan *password cracking* dengan lebih cepat sehingga informasi dapat lebih cepat disampaikan kepada pimpinan guna pengambilan keputusan dan mendukung pencapaian misi organisasi.

Kata kunci: kriptografi, fungsi hash, *password cracking* , SHA-1, dan FPGA

ABSTRACT

The development of communication and information technologies has increased dramatically. Nowadays, there are many software services that provide authentication system based on user ID (username) and password combination. Passwords are stored in digest, generated using a specific hash function schemes, such as SHA-1. XYZ Agency is a government agency engaged in information security. XYZ Agency requires computing speed to perform cryptanalysis including password cracking. FPGA is one of the high performance in computing platform. This research will be carried out the design implementation of SHA-1 password cracking based on FPGA. The design using brute force attack method to perform SHA-1 password cracking. The result of this research proof that FPGA can perrform SHA-1 password cracking faster than personal computer. The end results of this research is a draft implementation of SHA-1 password cracking based on FPGA for XYZ Agency. By implementing the design, the XYZ agency can perform password cracking faster so that the information can be delivered to the leaders quickly for decision making and support of the organization's mission.

Keywords: cryptography, hash function, password cracking, SHA-1, and FPGA

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Alhamdulillah, segala puji dan syukur senantiasa terpanjatkan kehadirat Allah SWT yang telah berkenan memberikan rahmat dan ridhoNya, sehingga penyusunan tesis berjudul “PERANCANGAN SHA-1 PASSWORD CRACKING BERBASIS FPGA: Studi Kasus Instansi XYZ” dapat selesai tepat waktu. Rasa terima kasih dan penghargaan setulusnya penulis sampaikan kepada:

1. Ayah, Ibu, Kakak dan Adik yang senantiasa memberikan kasih sayang, cinta, semangat dan pengorbanan serta do'a yang tak senantiasa mengalir.
2. Bapak Dr. Ir. Nazori AZ, M.T, Bapak Hadi Syahrial, M.M, M.KOM, Bapak Dr. Moedjiono, M.Sc dan Bapak Assoc. Prof. Dr. Teddy Mantoro atas masukan dan saran yang diberikan dalam penyusunan tesis.
3. Abang, Mbak, dan adik rekans Subdit Nalkripto atas segala bantuan, semangat dan motivasi yang diberikan.
4. Teman, Saudari, Adikku Nitia dan Ica, *thanks for everything*, yakin optimis berbuah manis, *good memories, we make it!*
5. Sacha Moleller, Daniel Siebert, *Steffen Möller*, Jost Bissel, Gerd Pfeiffer, and Tim Pietruck, *thank you so much for sharing knowledge freely, It's amazing!*
6. Mas Coudry, Mbak Ifah, Nahot, dan rekans MKOM UBL 2011.

Tak ada yang sempurna, karena kesempurnaan hanya milikNya. Penulis menyadari tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran untuk penulisan penelitian yang lebih baik. Saran dan kritik dapat dikirimkan ke alamat email bealfathunnisa@gmail.com.

Wassalamu'alaikum Wr.Wb

Jakarta, Pebruari 2013

@lfathunnisa

DAFTAR ISI

ABSTRAK.....	i
KATA PENGANTAR	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL.....	vii
DAFTAR LAMPIRAN.....	viii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	3
1.2.1 Identifikasi Masalah	3
1.2.2 Pembatasan Masalah	3
1.2.3 Rumusan Masalah	4
1.3 Tujuan dan Manfaat Penelitian.....	4
1.3.1 Tujuan Penelitian.....	4
1.3.2 Manfaat Penelitian.....	4
1.4 Tata Urut Penulisan	4
1.5 Daftar Istilah.....	5
BAB II LANDASAN TEORI DAN KERANGKA KONSEP/PEMIKIRAN	6
2.1 Tinjauan Pustaka	6
2.1.1 Kriptografi	6
2.1.2 Fungsi Hash	7
2.1.3 Skema Algoritma MD5	8
2.1.4 Skema Algoritma SHA-1	12
2.1.5 Serangan terhadap Skema Kriptografi.....	17
2.1.6 <i>Password Cracking</i>	19
2.1.7 Perkembangan Teknologi Komputasi	21
2.1.8 Field Programmable Gate Array (FPGA)	23
2.1.9 Pemrograman VHDL	25
2.2 Tinjauan Studi	28
2.3 Tinjauan Obyek Penelitian	31
2.3.1 Objek Penelitian	31
2.3.2 Perangkat keras.....	31
2.3.3 Perangkat lunak	31
2.4 Kerangka Konsep/Pola Pikir Pemecahan Masalah	40
2.5 Hipotesis.....	42
BAB III DESAIN PENELITIAN	43

3.1 Metode Penelitian.....	43
3.2 Metode Pengumpulan Data	43
3.3 Teknik Analisis Data	43
3.4 Langkah-langkah Penelitian	44
3.4.1 Perumusan Masalah.....	44
3.4.2 Studi Kepustakaan	45
3.4.3 Formulasi Hipotesis.....	45
3.4.4 Pengujian dan Analisis	45
3.4.5 Penarikan Kesimpulan.....	46
3.5 Jadwal Penelitian.....	46
BAB IV PERANCANGAN SISTEM DAN ANALISIS.....	48
4.1 Perancangan Sistem.....	48
4.1.1 Permodelan Sistem	49
4.1.2 Identifikasi Komponen <i>datapath</i>	52
4.1.3 Pembuatan <i>Datapath</i>	55
4.1.4 Perancangan Arsitektur Lengkap.....	57
4.1.5 Pembuatan Timing Diagram.....	57
4.1.6 Pembuatan <i>Controller</i> (FSM).....	60
4.1.7 Perancangan Interface.....	62
4.2 Implementasi Sistem	62
4.2.1 <i>Design Entry</i>	63
4.2.2 Design Synthesis.....	72
4.2.3 Implement Design.....	76
4.2.4 <i>Programming</i> Perangkat.....	77
4.2.5 Implementasi pada Perangkat	82
4.3 Pengujian Sistem	83
4.4 Analisis Hasil Implementasi.....	86
4.4.1 Analisis Resource	86
4.4.2 Analisis Performa	87
4.5 Rencana Implementasi	91
4.6 Implikasi Penelitian.....	91
4.6.1 Aspek Sistem	91
4.6.2 Aspek Organisasi.....	91
4.6.3 Aspek Penelitian Lanjutan.....	92
BAB V PENUTUP.....	95
5.1 Kesimpulan.....	95
5.2 Saran.....	95
DAFTAR PUSTAKA	97
LAMPIRAN.....	99

DAFTAR GAMBAR

Gambar	Halaman
II-1 Skema MD5	9
II-2 Pemrosesan pesan MD5	10
II-3 Operasi dasar MD5	11
II-4 Skema SHA-1	13
II-5 Pemrosesan 512 bit SHA-1	14
II-6 Proses Satu Round SHA-1	15
II-7 Blok Diagram FPGA	24
II-8 Struktur Pemrograman VHDL	26
II-9 Tampilan GUI <i>Project Navigator</i>	32
II-10 Pola Pikir	41
III-1 Tahapan Penelitian	44
IV-1 Tahap Perancangan dan Implementasi Modul SHA-1 Cracking	48
IV-2 DFD Level 0 Modul SHA-1 Cracking	50
IV-3 DFD Level 1 Modul SHA-1 Cracking	51
IV-4 DFD Level 2 SHA-1 Core	51
IV-5 DFD Level 3 Round SHA-1	52
IV-6 <i>Datapath</i> Round SHA-1	56
IV-7 <i>Datapath</i> Proses Komparasi	56
IV-8 Arsitektur Lengkap SHA-1 <i>Password Cracking</i>	57
IV-9 <i>Timing Diagram</i> untuk Round SHA-1	58
IV-10 <i>Timing Diagram</i> Proses Komparasi	59
IV-11 <i>Timing Diagram</i> Gabungan Proses Round SHA-1 dan Komparasi	60
IV-12 State Diagram SHA-1 <i>Password Cracking</i>	61
IV-13 Alur Pemrograman VHDL	63
IV-14 Alur SHA-1 <i>Password Cracking</i>	64
IV-15 Skematik Hubungan antar Entitas	65
IV-16 Skematik <i>api_to_core</i>	66
IV-17 Skematik <i>sha1_crypt</i>	67
IV-18 Skematik <i>sha1_core</i>	69
IV-19 Skematik <i>Comparator</i> (<i>sha1compare</i>)	70
IV-20 Skematik <i>core_to_api</i>	71
IV-21 Hasil Simulasi dengan Linux	77
IV-22 Simulasi Modul <i>Sha_core</i>	78
IV-23 Simulasi Modul <i>Sha1compare</i>	79
IV-24 Simulasi Modul Terintegrasi	81
IV-25 Arsitektur DDS	82
IV-26 Konfigurasi Jaringan	83
IV-27 Hasil Test Vector dengan FPGA	84
IV-28 Hasil Test Vector dengan JTR	85
IV-29 Perbandingan Waktu PC dan FPGA	90

DAFTAR TABEL

Tabel	Halaman
II-1	Fungsi <i>gt</i> untuk Setiap Round.....12
II-2	Fungsi <i>ft</i> untuk Setiap Round16
II-3	Perbandingan Waktu dan Biaya28
II-4	Hasil Pengujian Picocomputing29
II-5	Tinjauan Studi29
II-6	Daftar <i>Command Line Interface Options</i> pada JTR.....35
II-7	Algoritma pada JTR.....37
III-1	Rencana Jadwal Penelitian46
IV-1	Deskripsi Port Komponen <i>api_to_core</i>66
IV-2	Deskripsi Port Komponen <i>sha1_crypt</i>68
IV-3	Deskripsi Port Komponen <i>sha1_core</i>69
IV-4	Deskripsi Port Komponen <i>sha1compare</i>70
IV-5	Deskripsi Port Komponen <i>core_to_api</i>71
IV-6	Komponen Macro <i>Sha1_crypt</i>73
IV-7	Penggunaan <i>Resource</i> dan <i>Timing Process</i> <i>sha1_crypt</i>74
IV-8	Komponen Makro Proses Terintegrasi.....75
IV-9	Penggunaan <i>Resource</i> dan <i>Timing Process</i> Proses Terintegrasi76
IV-10	Hasil Tes Vector86
IV-11	Perbandingan Waktu FPGA dan Personal Computer.....89
IV-12	Rencana Implementasi.....92

DAFTAR LAMPIRAN

Lampiran	Halaman
1 Source Code pada FPGA.....	99
2 Hasil Pengujian	108



DAFTAR PUSTAKA

- [Alkalbani 2010] Alkalbani, Abdullah Said, Mantoro, Teddy, Osman, Abu., Comparison between RSA Hardware and Software Implementation for WSNs Security Schemes. *Proceeding 3rd International Conference on ICT4M*, (2010): 84-89.
- [Chu 2008] Chu, Pong P., “*FPGA Prototyping by VHDL Examples: Xilinx Spartan -3 Version*”, New Jersey: John Wiley & Sons, Inc., 2008.
- [FIPS 2012] _____.”*FIPS PUB 180 – 4: Secure Hash Standard (SHS)*”. Gaithersburg: FIPS Publication. 2012.
- [Fischer 2007] Fischer, Thorsten. “Everyday Password Cracking”. *IRM Research White Paper*, IRM PLC, (Desember, 2007): 16 pages.
- [Guneysu 2009] Guneysu, Tim, Erhan.”Cryptography and Cryptanalysis on Reconfigurable Devices.” Ph.D, diss,. Ruhr-University Bochum, 2009.
- [Hanamakumar 2011] Hanamakumar, Veerla, Syamsundar. “Cost-Efficient SHA Hardware Accelerator”. *IJAEST*, vol.no.5, (2011): 37-52.
- [Hulton 2009] Hulton, David, Hur, Mark. “Using FPGA Cluster for Fast Password Recovery”. *A Pico Computing Data Security White Paper*.(November, 2009): 4 pages.
- [Jarvinen 2004] Jarvinen, Kimmo. “Design and Implementation of a SHA-1 Module on FPGAs”. 2004.
- [Kumar 2006] Kumar, asndeeep, Paar, Christof. “Breaking Cipheth with COPACOBANA – A Cost-Optimized Parallel Code Breaker”. *IACR Proceeding*. 2006.
- [Kusbandono 2004] Kusbandono, Arif., “Implementasi Algoritma AES-128 pada Mikrokontroler 8051.” Bachelor Thesis, Institut Teknologi Bandung, Bandung, 2004.
- [Menezes 1996] Menezes, Alfred J., Oorschot, Paul C. , “*Handbook of Applied Cryptography*”, Waterloo: CRC Press, 1996.
- [Simon 2007] Marechal, Simon. “Advances in password cracking” . *J Comput Virol*, vol.4, (2008):73-81.