Diplomarbeit

Christian Kirbach

SSL-Beschleunigung mit modernen 3D-Grafikkarten

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783836613101

Christian Kirbach

SSL-Beschleunigung mit modernen 3D-Grafikkarten

Diplom.de

Diplomarbeit

Christian Kirbach

SSL-Beschleunigung mit modernen 3D-Grafikkarten

Diplom.de

Christian Kirbach
SSL-Beschleunigung mit modernen 3D-Grafikkarten

ISBN: 978-3-8366-1310-1
Druck Diplomica® Verlag GmbH, Hamburg, 2008
Zugl. Universität Siegen, Siegen, Deutschland, Diplomarbeit, 2005

Danksagung

Ich widme diese Seite allen Personen, die zur Entstehung dieser Diplomarbeit in unersetzbarer Weise beigetragen haben.

An erster Stelle richtet sich mein Dank an meine Eltern für ihre durchgehende Unterstützung und Befürwortung meines Studiums. Ich danke für die wissenschaftliche Betreuung Univ.-Prof. Dr. Christoph Ruland und Dipl.-Ing. Luigi Lo Iacono vom Lehrstuhl für digitale Kommunikationssysteme der Universität Siegen. Ebenso bedanke ich mich für die freundliche Zusammenarbeit und Unterstützung bei Dipl.-Inf. Nicolas Cuntz vom Lehrstuhl für Computergrafik für die ständige Hilfestellung bei Fragen zur Implementierung und seinen Anregungen zu neuen Lösungsansätzen.
Mein besonderer Dank gilt auch Dipl.-Inf. Dominik Göddeke vom Institut für Angewandte Mathematik und Numerik der Universität Dortmund. Er hat mir freundlicherweise Zugang zu seinem noch unveröffentlichten Tutorial gegeben.

Mein Dank gilt allen Korrekturlesern und -leserinnen: Dipl.-Ing. Andre Schäfer, Katharina Kirbach, Gunnar Spickermann, Hendrik Payer, Stefan Siebel und Dirk Sommer.

Zusammenfassung

Datenaustausch über das Internet gewinnt zunehmend an Bedeutung. Viele Geschäftsbereiche verlassen sich schon heute auf verschlüsselte Kommunikation, wie z.B. Online Banking und Online Shopping. Dabei erfordert insbesondere die Verwendung asymmetrischer kryptographischer Verfahren zur Absicherung der Kommunikation viel Rechenleistung. Aus diesem Grund setzen die Betreiber von Internet-Servern spezielle Hardware-Beschleunigerkarten ein. Sie übernehmen die aufwendigen Berechnungen und entlasten so die CPU der Server. Ein Nachteil dieser Krypto-Hardware sind hohe Anschaffungskosten. Der wachsende Bedarf nach Sicherheit in Informations- und Kommunikationssystemen beflügelt die Suche nach Alternativen, um die enorme Rechenlast zu bewältigen.
Moderne 3D-Grafikkarten sind in den letzten Jahren besonders leistungsstark geworden. Ihr jährliches Leistungswachstum übertrifft sogar das der verbreiteten Mikroprozessoren. Ein großer Verkaufsumsatz hat sie zu günstiger Massenware werden lassen. Zusätzlich macht sie eine steigende Programmierbarkeit sehr flexibel. Die moderne Wissenschaft nutzt Grafikprozessoren schon heute zur Berechnung von Finite Elemente Simulationen und hochauflösenden Computertomographien in Echtzeit. Neue Anwendungsbereiche werden ständig erschlossen.
Im Rahmen dieser Diplomarbeit wird die Möglichkeit analysiert und bewertet, moderne 3D-Grafikkarten für die Berechnungen asymmetrischer kryptographischer Operationen einzusetzen. Insbesondere wird der weit verbreitete RSA-Algorithmus untersucht, welcher auf Exponentiationen von sehr großen Ganzzahlen und Modulo-Operationen basiert. Eine geeignete Grafikbibliothek wie das Plattform übergreifende OpenGL ist erforderlich, um alle Operationen zu steuern. Sie wird eingesetzt, um Daten von und zur Grafikkarte zu transferieren und die erforderlichen Rechenvorgänge des Grafikprozessors anzustoßen. Die programmierbaren Einheiten des Prozessors werden mit Hilfe der Programmiersprache Cg programmiert, ein Derivat der Hochsprache C, das speziell auf die Programmierung von Grafikprozessoren angepasst wurde. Hardware übergreifende Cg-Profile stellen sicher, dass die Programme auf einer Vielzahl von Grafikkarten eingesetzt werden können.
Zum Schluss wird die Geschwindigkeit dieser Implementierung mit der von gängigen RSA-Implementierungen verglichen, die ausschließlich Berechnungen auf der CPU durchführen.

Abstract

Secure internet communications are constantly becoming more important. Lots of businesses rely on encrypted transactions, e.g. online banking and online shopping. In particular asymmetric SSL encryption requires lots of computational power. Dedicated hardware accelerator cards are usually deployed at large server sites. They perform expensive calculations efficiently in favour of the server's CPU. One major drawback of cryptographic hardware is their high price tag. As demand for security increases new possibilities are embraced to handle the workload.
3D graphics cards have become increasingly powerful mainstream products in recent years. Their power growth rate even exceeds general purpose microprocessors. They are in mass production and cheap. Additionally improving programming capabilities have turned them into flexible and versatile devices. Modern science already computes finite element simulations and high-resolution real-time computer tomography on graphics processors. New applications continue to emerge.
This thesis analyses and evaluates the possibility of harnessing the power of modern 3D graphics cards for asymmetric cryptography. In particular the popular RSA algorithm is examined. It involves computing the power of large integer numbers and modulus operations. A suitable graphics library like the cross-platform OpenGL is required for controlling all neccessary operations. It is used to perform data transfers to and from the graphics card and initiate calculations done by GPU programs. These shader programs will be written in the Cg programming language, a derivative of C adjusted for GPU programming. Vendor independent Cg profiles ensure that programs can be compiled for a variety of cross-vendor GPUs.
Finally the performance will be evaluated and compared to state-of-the-art RSA implementations that run on CPUs.

Inhaltsverzeichnis