TECHNOLOGY OFFER

WISSENS/ TRANSFER/ SÜD/

www.wtz-sued.at

Multiplication of Large Operands

The invention is a very efficient multiplication technique for embedded (micro) processors, which process the operands using multiple-precision arithmetic. The technique increases the performance of state-of-the-art multiplication by sophisticated caching of operands. It significantly reduces the number of needed load instructions, which are usually one of the most expensive instructions on modern processors.

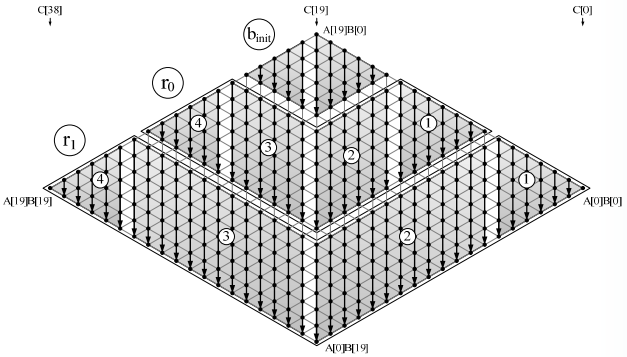
BACKGROUND

Multiplication of large numbers is one of the most fundamental algebraic operations in modern applications. The runtime complexity and efficiency of multiplication determines the overall performance of complex mathematical calculations.

TECHNOLOGY

Operand caching multiplication makes use of the fact that accessing general purpose registers of modern microprocessors is usually faster than accessing (internal or external) memory (RAM). The technology rearranges the processing of partial products during the multiplication such that the needed number of memory-load instructions is reduced to a minimum, which makes the technology faster than existing techniques.

The graphic on the right exemplarily presents a 160-bit multi-precision multiplication on an 8-bit microprocessor (AVR ATmega128). The operands are processed in three rows and are processed from right-to-left.



ADVANTAGES

Operand caching multiplication provides

- improved multiplication performance by about 10 to 23 % compared to related techniques (product scanning, operand scanning, hybrid, …)
- generic (supports different operand sizes and platforms)
- increased speed of applications where multiplication is the main operation

Potential Fields of Application:

Large number multiplication (>160 bits per operand) on microprocessors, e.g.,

- security (e.g., public-key cryptography, digital signatures, …)
- signal processing (acoustics, speech,…)
- image processing (multimedia)

Operand caching multiplication is efficient on embedded systems such as

- smart cards and low-resource devices (RFID, sensor nodes, …)
- RISC-based microprocessors (e.g., AVR ATmega)
- ARM-based systems (smart phones, tablets, PDAs, game consoles, …)
- embedded routers and network devices

Ref.no.: E_427

KEYWORDS:
Long Integer Multiplication
Cryptography
RSA
ECC
Pairing

INVENTORS:
Dr. Michael Hutter
DI Erich Wenger

COOPERATION OPTIONS:

- Licensing
- Technical co-operation
- Ready-to-use assembly optimized source code

DEVELOPMENT STATUS:

- Proof of concept on ARM and AVR ATmega processors
- Ready for deployment

STATUS OF PATENTS:
Granted European patent, validated in Germany

CONTACT:

Dr. Moritz Theisen
Graz University of Technology
Research and Technology House
Mandellstraße 9/II
8010 Graz, Austria
T: +43 316 873 6925
moritz.theisen@tugraz.at
www.tugraz.at

bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft
austria wirtschaftsservice aws

TU Graz Graz University of Technology