

Search

[HOME](#) | [ABOUT US](#) | [SUBSCRIBE TO DDJ](#)

ARTICLES

SOURCE CODE

DEVSEARCHER

TECHNICAST

BOOK REVIEWS

OP-EDS

WORLD PROCESSOR RESOURCES

RESOURCES

PROGRAMMER'S WALL

SOFTWARE

CAREERS

MAILING LISTS

DR. DOBBS'S STORE

CUSTOMER SERVICE

August 12, 1999

## The CHES Cryptography Conference

By Dan Bailey

*Dan is in the Cryptography and Information Security Group of the Electrical Engineering Department of Worcester Polytechnic Institute. He can be reached at [bailey@wpi.edu](mailto:bailey@wpi.edu)*

More than 150 scientists and industry experts from over 37 countries will come to Worcester Polytechnic Institute for the first annual Workshop on Cryptographic Hardware and Embedded Systems (CHES), to be held August 12-13, 1999. The CHES conference proceedings will appear in Springer-Verlag's *Lecture Notes in Computer Science* series, edited by Cetin Koc of Oregon State University and Christof Paar of WPI.

In contrast to previous workshops and conferences in the area of cryptography, CHES adopts a practical approach. "Cryptography," says workshop co-organizer Christof Paar, "is rapidly moving from a somewhat esoteric niche area into an important discipline with applications in virtually all future information technology products, such as personal computers, wireless phones, and set-top boxes." This need to provide a forum for practical systems and design issues led to CHES' inception.

In line with this focus on practical systems, many of the workshop's 29 talks will address issues of efficient implementation and attacks on practical systems. Particularly interesting efficient implementations of DES in an ASIC and public-key algorithms on a DSP will be presented, along with attacks on RSA and smartcards.

Sandia National Labs made a splash recently with its announcement of a new world record in fast DES implementation. Despite its age of more than twenty years, this block cipher is considered the workhorse of cryptography: It has been implemented in more systems and on more platforms than any other. Furthermore, with new "triple" modes of operation newly defined in ANSI X9.52, DES continues to be a popular algorithm, especially for high-speed networking. Ever-increasing network speeds offered by ATM and other technologies present a problem: Previous fast DES implementations have a throughput far below the 10Gbps required for a SONET OC-192c stream. With OC-192c as the goal, Sandia's engineers implemented the 16 rounds of DES in a fully pipelined fashion with hardware devoted to each round. Sandia's pipelined approach yields the fastest reported DES implementation: At 105 MHz, the 0.6 micron CMOS device yields 6.7 Gbps, and simulations indicate 9.28 Gbps is possible with the current design.

A team from Fujitsu reports an implementation on the Texas Instruments TMS3206201 digital signal processor (DSP) of three popular public-key algorithms. Their effort includes RSA (perhaps the most widely used public-key algorithm), DSA, a U.S. government standard for digital signatures, and ECDSA, a U.S. government standard for digital signatures using elliptic curves. The 200 MHz TI DSP is highly optimized for the arithmetic calculations required for high-end signal processing applications. In contrast to general-purpose microprocessors such as the Intel Pentium, for example, a DSP is designed to handle a multiply-and-accumulate (MAC) operation in a single cycle. In fact, the TI DSP used by the Fujitsu engineers can handle six additions and two multiplications in a single cycle at 200 MHz. The team uses these architectural advantages along with a new variant of Montgomery multiplication to produce stellar results. For 1024-bit RSA decryption, they



achieve a time of 11.7 msec, an improvement by a factor of four over previously reported results on a 200 MHz Pentium. For 512-bit DSA verification, they achieve a time of 5.14 msec, and 160-bit ECDSA yields a time of 3.97 msec. Of course, no matter how fast a system is, it is useless if it falls easily to attacks.

Several interesting attacks on real-world systems will be presented at CHES. These fall into two general categories. Some, like Adi Shamir's Twinkle device, attack a particular algorithm. Others, like power analysis, attack devices that execute a particular algorithm. Both types of attack must be considered when designing real-world systems.

Adi Shamir's Twinkle design is perhaps the most-anticipated paper to be presented at CHES. A few weeks ago, the cryptographic community was abuzz with rumors of a new factoring attack by Shamir, one of the co-inventors of the RSA algorithm. This public-key technique relies on the difficulty of the integer factorization problem. That is, given  $n=pq$  for  $p, q$  of roughly equal size, find  $p$  and  $q$ . To address this problem, mathematicians have developed algorithms such as the Quadratic Sieve and the Number Field Sieve (NFS). These algorithms consist of two stages: a sieving procedure that is typically run on a large number of workstations and a linear algebra step typically run on a supercomputer. General-purpose workstations are a poor platform for sieving, however. Specifically, a fast workstation implementation stores modular squares in array elements and loops over the primes smaller than some bound. For 512-bit composite integers, this approach requires roughly 100 MB of RAM and 5-10 seconds per sieve iteration. Twinkle, on the other hand, does the same job in 0.01 seconds, a speed-up of 500-1000 times over a general-purpose workstation.

To achieve this level of performance increase, Twinkle relies on optoelectronics. Instead of looping over the primes, Twinkle assigns them to LEDs with intensities proportional to the bit length of the prime. Thus by measuring the light intensity emitted, one can calculate the sum of the bit lengths of the smooth prime divisors for the modular square in question. It can then be easily determined if the modular square factors completely or if there are other larger factors. By finding the bit length in this way, we avoid the need to scan 100 MB of RAM. In addition, the use of optoelectronics allows the device to be built in quantity for an estimated cost of \$5,000 when clocked at 10 GHz. If this development can be realized in a real device, 512-bit RSA moduli can be easily factored. Due to the U.S. government's restrictions on the export of strong cryptography, 512-bit RSA is the de facto standard for exportable web browsers and servers. This development has serious implications for those deploying real-world systems based on RSA: 512-bit keys are not adequate.

From efficient implementation to attacks on real-world systems, the CHES workshop promises to provide a forum for innovative results in the practical areas of cryptography, bridging the gap between the cryptography research community and the application areas.

Advertisement



Copyright © 1999 *Dr. Dobb's Journal*  
*Dr. Dobb's Journal's* [Privacy Policy](#)  
Comments: [webmaster@www.ddj.com](mailto:webmaster@www.ddj.com)