Cofactorization on GPUs

Andrea Miele\textsuperscript{1}, Joppe W. Bos\textsuperscript{2}, Thorsten Kleinjung\textsuperscript{1}, Arjen K. Lenstra\textsuperscript{1}
\textsuperscript{1}LACAL, EPFL, Lausanne, Switzerland
\textsuperscript{2}NXP Semiconductors

NUMBER FIELD SIEVE
Asymptotically fastest known factoring algorithm.
Key to assessing security of RSA cryptosystem.
RSA 768-bit modulus factored with NFS in 2010.

Idea: to factor an odd composite $n$, find:
$x, y$ such that $x^n \equiv y^2 \pmod{n}$ and $x \neq \pm y \pmod{n}$

Two main phases:
\begin{itemize}
  \item RELATION COLLECTION (90\% OF TOTAL TIME)
  \item LINEAR ALGEBRA STEP (10\% OF TOTAL TIME)
\end{itemize}

NFS RELATIONS
Two positive integer smoothness bounds: $B_1$, $B_2$
Irreducible $f(X), f(X)$ of degree 1 and $d$ small ($d=5, 6$)

Relation: $(a, b)$ with $a,b$ coprime integers ($b>0$):
\begin{itemize}
  \item $bf(a/b)$ is $B_1$-smooth except (at most) 4 large primes
  \item $b^2f(a/b)$ is $B_2$-smooth except (at most) 4 large primes
\end{itemize}

COLLECT RELATIONS (TASK PARALLELISM!)
SIEVING: find pairs $(a, b)$: $bf(a/b)$ ($b^2f(a/b)$) is product of a $B_1$-smooth ($B_2$-smooth) part and "small" cofactor

POST SIEVING (NORMALLY 12-17\% OF THE TOTAL TIME):
1. Compute $bf(a/b)$ and $b^2f(a/b)$ (200-400 bits)
2. Find small factors pair-by-pair (or re-sieve, bad on GPU)
3. Factor cofactors pair-by-pair (COFACTORIZATION)

FASTER NFS WITH GPUs?
SIEVING: memory hungry, done on CPUs
PREVIOUSLY: offload ECM to GPUs or FPGAs
IDEA: offload ALL POST-SIEVING (COFACTORIZATION) to GPUs

POST SIEVING ON GPUs: OUTLOOK
Input: Set of good candidate pairs $(a, b)$ output by sieve
Output: The relations contained in the input set

Two Kernels run sequentially (one or more pairs per thread):
1. Rational side: check $bf(a/b)$ for smoothness (discard bad)
2. Algebraic side: check $b^2f(a/b)$ for smoothness (output rels)

Sequential Radix 2\textsuperscript{3} Montgomery arith (coalesced GM access)
PTX optimized code (MAD, loop unrolling, 32M as "scratchpad")

CONCLUSION AND FUTURE WORK
\begin{itemize}
  \item Modern GPUs can accelerate NFS factoring
  \item Using GPUs can lead to lower factoring cost
  \item Optimize for Kepler GPUs
  \item Get figures for RSA 1024-bit
\end{itemize}