230701242349723619910125112477682271151121011931642481

207206182177100(206228761702151732301789 9)20624312575240 1

Cryptanalysis on Graphic Cards or other Highly Parallel Architectures

11210125479: 64235227115112101(2342188864112101, 1171131261801992042271151121

112101115185: `100-2628-E-001-004-MY3`

245230193173: 2012 126 8 235 1 233220 2013 126 7 235 31 233

248105216254: 235178248105

66122232161: 71126225105189125100223

1121016824972: 16810293

24523024799: 164161227115124234842361992271152 10

248105233193: 16421619323410112652353123 3

254243: 20991227811242481058021522 9

16422975110

9818711210116421820410523017323017899871811257524018 7, 11179218204186772481676 4, 16710193191119239247178239198 7RSA18624018724211111716718617871, 9321198758819920111911211957821620818124923622511310875881991861257524018767225113108758819918612575240187792182048mann12410421022620118 CASED11925422278227115164223(93243Darmstadt236222106199)22711520625379124163124206191 6(163206113108)18611316378105721257079722182047879248207941701112112221820468110186117642102502072061732309199842341057291116240187104220113116206672182042401877220910422011368117202232123213, 24116710120425211025118 F4/F5 116226107243214, 18711622610798179170116115178186104214223206104247185115213105727023621923710618687210, 19578189185219209110233SAGE67

218204981042201137588199186171110240187226113712091042201841701842321232138718622711512012, 22679116105105162678020121820421717964199228761861787167

246228114: 207206182177100, 173230198, 12575240187, 2251131087588199

Abstract

In this project we conducted cryptanalytic studies on parallel architectures. This is our specialty. We also made attacks on discrete logarithms and RSA earlier and made a name in the crypto community. This is a continuation of the study extending to the cryptanalysis of post-quantum public-key cryptography, which is a common research interest for us and for our long-term research partners, the CASED (Center for Advanced Security rEsearch, Darmstadt) team at TU Darmstadt headed by Academician Johannes Buchmann (of the National Academy of Sciences of Germany).

Post-Quantum Cryptography studies public-key cryptographic schemes which will not be dealt a fatal blow when large quantum computers appear. However, no one knows whether any of these can be made practically safe under conventional attacks. We seek to address this question.

In our major result we showed that multivariate cryptography can be assisted by highly parallel structures. We build a highly parallel XL solver which can be better than the best F4 and F5 algorithms previously considered champions. The program scales well to many cores or machines with high speed interconnect, and will be donated to open source project SAGE.

Our recent works were selected to CHES 2012, which is one of the biggest and most important conferences in cryptography, and something to be proud of. We have also some more minor results.

Keywords:GPU, parallelization, cryptanalysis, post-quantum cryptography

Contents

101165

1 11620980216186

218204248193886418623524 1: Darmstadt 186Johannes Buchmann 208194204241237239176119234286199124186124104677618620616477218204642116611923218611210111376701192342342361 24(DFG) 186102214, 25379218204111831798121422 7, 196711842112082152432142272532182048070641022406 7, 218204721702151732301869199, 22711523922511310875881991862401871861982482 15, 93116239211242243184(Lattice)80104220184(Multivariate)18622511310875881991862401876 7

2 17871(Results)

PQCrypto (2251131087588199) means implementing cryptography that will survive the invention of quantum computers. We achieve breakthroughs in getting faster cryptanalysis and a better understanding of provably secure complexity offered for cryptosystems based on these systems.

XL algorithm to solve systems.:

Solving a system of multivariate quadratic equations (MQ) is a hard problem whose complexity estimates are relevant to many cryptographic scenarios. In some cases it is required in the best known attack; sometimes it is a generic attack (such as for the multivariate PKCs), and some of the time it determines a provable level of security (such as for the QUAD stream ciphers).

Under some reasonable assumptions, the best way to solve generic MQ systems is the XL algorithm implemented with a sparse matrix solver such as Wiedemann. Knowing how fast one can implement this attack gives us a good idea of how future cryptosystems related to MQ can be broken, similar to how implementations of General Number Field Sieve that factors smaller RSA numbers gives us more insight into the security of actual RSA-based cryptosystems.

This paper describes such an implementation of XL with Block Wiedemann. We are able to solve in 2.5 days, on a 48-core, 64GB RAM computer (cost: US$6000), a system with 30 variables and 60 equations over GF(16) (a computation of about 2^{57} GF(16)-multiplications). We do not expect F_4/F_5 to accomplish this due to its much higher space usage. We are also able to solve in 1.3 days, on a single Amazon EC2 `cc2.8xlarge` instance, a system with 23 variables and 32 equations of GF(16). This directly translates to an estimate of the *cost* to break the HFE Challenge 2 at US$< 2^{43}. The software can be easily adapted to other small fields including GF(2). More importantly, it scales nicely for small clusters, NUMA machines, and a combination of both to test systems which are only 1.5 orders of magnitude away in bit-complexity from the Block Wiedemann used for RSA-768.

The Comparison of XL vs F_4/F_5 vs Brute Force

We address the much needed comparison of XL vs vs F_4/F_5 vs Brute Force and show that XL is better asymptotically in most cryptologically interesting situation than F_4/F_5 by showing that the difference in the XL degree and the F_4/F_5 degree of operation is often at most 1 asymptotically. This paper is in

preparation.

Brute-force attack using FPGAs vs GPUs

We show that the CHES 2010 result can be extended to energy efficient FPGAs such that it can have much much better energy performance, even parts-cost-performance than GPUs, which we do in this (submitted) paper. We have to do a lot of engineering to get around obstacles posed by the Xilinx hardware and software tools. We are able to improve the energy to performance ratio by a factor of more than 10.

3 112101168712192518010523 0

218204187211787923418116365224247110872341811867588199186204106227811 24(937980126201172202
252236186234852041041862342182278112 4CHES
2012, 228118849365722342312102506 5XL
116226107792512442392436423518676831 19(overde-
termined) 170184232123213186198248215186204206116226107,
16125070107234721 86F_4/F_5 116226107186163172672182042192371861617865195661852191181808 5
19267
112711611792541991631611721676665787921820418822472194234181186164215180209122151631 7
10524067

4 List of Attachments

254243176981871121012452301862152 29,

- T. Chou, C.-M. Cheng, R. Niederhagen, and B.-Y. Yang, Solving Quadratic Equations with XL on Parallel Architectures, to appear at CHES 2012 (14th workshop on Cryptographic Hardware and Embedded Systems, September 9-12, Leuven, Belgium) LNCS 7428, pp. 356-373.

- M.-S. Chen, C.-M. Cheng, B.-Y. Yang, RAIDq: A software-friendly, multiple-parity RAID, USENIX HotStorage 2013 (USENIX Federated Workshops, June 27-28, San Jose, CA, USA), to appear.

- S. Tanaka, T. Chou, B.-Y. Yang, C.-M. Cheng, K. Sakurai: Efficient Parallel Evaluation of Multivariate Quadratic Polynomials on GPUs, WISA 2012 (13th Workshop on Information Security Applications, August 16-18, Jeju Island, Korea), LNCS 7690, pp. 28-42.

- D. J. Bernstein, N. Duif, T. Lange, *P. Schwabe, and B.-Y. Yang, High-speed high-security signatures, Journal of Cryptographic Engineering 2:2(2012), pp. 77-89. This is a full version of the paper at CHES 2011 (13th Workshop on Cryptographic Hardware and Embedded Systems, September 28 - October 1, Nara, Japan), LNCS 6917, pp. 124-142.