Projects based on the FK-method

1. Introduction

High-speed algorithm for arithmetic operation in the finite fields is the one of fundamental techniques which affects on the whole IT industry from IC card chip to internet protocol design.

Because of just this importance, almost of research works on the speed enhancements of the finite field operations has been steadily supported by governments, organizations and enterprises such as Intel.

This document gives the outline of new method that significantly speeds up the finite field multiplication and describes what is possible when using this new method to practics.

2. Fractal-structured Karatsuba method (FK method) for the finite field multiplication.

Karatsuba method is known as the fastest algorithm for polynomial multiplication reaching near to theoretical limit in computational estimation.[2]

But unfortunately, it is only theoretical.[1, p.434]

In practices, this method is recognized to be almost useless, because a large amount of push-pop work on stack memory is required for putting Karatsuba method into computer algorithm.

The FK method we construct is designed just to eliminate such an overhead by using special type of stack cell structure and of its logic between cells.

In this cell structure which we said fractal type, the FK method converts multiplication in $GF(2^k)$ into very simple cell operation not requiring recursive iteration for recombination.

So FK method is over 20 times faster than Han's method introduced in [5].1998 and about 7 times faster than the Montgomery method specially introduced for DLP operation in [3]. 1998(used in[4].2001).

When using FK method, usual P4-1.8GHz desktop can perform two millions of multiplications in $GF(2^{191})$ or one million in $GF(2^{431})$ for every second.

It means one can generate more than twenty thousand of the elliptic curve crypto-key in $GF(2^{191})$ for every second.

Such a high speed of FK method makes it possible to remove main bottlenecks in the many real-time cryptosystems both of hardware and software.

Below we describe one project efficiently exploiting such a benefit of FK method.

3. New type of real-time security system for duplex speech communications.

Speech communication such as telephone, handphone needs a large amount of packets to be real-time transported.

Real-time requirement makes it impossible for any cryptosystem to enable global backward-randomizing in this packet sequence because every packet must leave from device in given delay time limit.

It results in a large possibility of backdoor attacks using stochastics theory of Markov process, without breaking public key security system.

The longer communication time is, the greater the possibility of goaling in such an attacks is, because more sample packets are collected and analysed for stochastics.

To cut off this danger principally, a new type of cryptosystem we design, uses only physical random sequence without using any stream- or block-sequence for randomizing packet sequence.

Another most important property of this cryptosystem is that the longer communication time is, the larger crypto-safety of system grows as in snow-avalanche.

Our system protocols have such a mechanism that any parallel computation is impossible to be applied for breaking this “avalanche”.

We say this mechanism Free Avalanche Crypto-system (FAC)

The bottleneck in realizing FAC system is real-time generation of public keys needed to exchange physical random sequence between communication sides

FK-algorithm offers just high speed, enabling to remove this bottleneck by any usual risc MPU.

For example, following FAC device for speech communication can be easily composed.

- Default cryptosystem: Elliptic in $GF(2^{191})$
- Key-generating speed: More than 20 per second
- Speech bandwidth: 3 KHz
- Trans- bandwidth : 2 Kbps duplex

- Compression chip: Ambe series
- Mpu chip: SH or ARM series

1 minute after starting talk with this FAC device, the strength of security grows over 20*60=1200 times higher than the default value of starting moment, estimating by quantity of attack computation against this dynamic public key security system.

4. Making Compiler for the FK algorithm on various machine platforms.

FK algorithm consists of assembly codes realizing very intricate interactions of fractal- structured cells, which is impossible to write manually by hand.

Any C- compiler is also not efficient to produce these assembly codes, because of peculiar, irregular structure of stack cells.

So, for good coding of FK algorithm it is necessary to use new compiler professionally optimized for it.

Making this compiler sensitively depends on every structures of machine such as registers, caches, pipelines, memory speeds and so on.

At present, we developed such a compiler only for X86 CPU and use on only desktop machine to make various software implementations.

But, it will be more valuable if such a compiler is migrated to other industrial devices such as MPUs, DSPs and CPLDs for targeting concrete aims.[6][7]

In this direction, we hope more global cooperative development works with any organization interested in our research.

References

[1] R. Crandall, C. Pomerance, “Prime Numbers”; A Computational Perspective, Springer(2000)

[2] I.F.Blake, G.Seroussi, N.P.Smart, “Elliptic Curves in Cryptography”, Cambridge University Press(1999)

[3] C.K.Koc, T.Acar, “Montgomery Multiplication in $GF(2^k)$”, Design, Codes and Cryptography, 14, 57-69(1998)

[4] M. Aydos, T. Yanic, C.K. Koc, “High-Speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor”, IEE Proc. Commun., vol.148, no.5, 273-279(2001)

[5] Y.Han, P.C.Leong, P.C.Tan, J.zhang, “Fast Algorithms for Elliptic Curve Cryptosystems over Binary Finite Field, Asiacrypt’98, pp.75-84

[6] C.H.Kim, S.Oh, J.Lim, “A New Hardware Architecture for Operations in $GF(2^n)$”, IEEE Trans. Computers, vol.51, no.1, 90-91(2002)

[7] A.HalbutoGullari, C.K.Koc, “Parallel Multiplication in $GF(2^k)$, Using Polynomial Residue Arithmetic”, Designs, Codes and Cryptography, 20, 155-173(2000)

[8] A. Reyhani-Masoleh and M. A. Hasan, “Fast Normal Basis Multiplication Using General Purpose Processors”, IEEE Trans. Computers, 52, 11, 1379-1390(2003)

[9] D. Hankerson, J. Lopez and A. Menezes, “Software Implementation of Elliptic Curve Cryptography over Binary Fields”, CHES2000, 1-24

[10] A. Reyhani-Masoleh and M. A. Hasan, “Efficient Multiplication Beyond Optimal Normal Bases”, IEEE Trans. Computers, 52, 4, 428-439(2003)