ArcticCrypt 2016
Reflection Report

Tetiana Yarygina

Abstract

This report reflects on the presentations given during ArcticCrypt 2016 with an emphasis on the topics of my personal interest. Attendance of the even was funded by COINS Research School.

1 Featured papers

Although many noteworthy papers were presented at ArcticCrypt 2016, the following papers are of particularly interest to me:

- *Missing a trick: Karatsuba variations* by Mike Scott.
  The paper rediscovers a forgotten "arbitrary degree" variant of Karatsuba multiplication algorithm (ADK). The paper establishes a specific break-even point where Karatsuba variants should be considered ahead of the classic schoolboy method for long multiplication.
- *Backtracking-Assisted Multiplication* by Houda Ferradi et.al.
  The paper presents a new algorithm for multiplication by a constant. The method uses backtracking to find a multiplication friendly encoding (an alternative representation) of the constant operand a. The algorithm aims to express some a_i as a linear combination of other a_js with small coefficients. It is then easy to reconstruct the whole multiplication $b \times a$ from the values of the $b \times a_j$ only. The more linear combinations are found, the less multiplications will be performed.
- *CacheBleed: A Timing Attack on OpenSSL Constant Time RSA* by Yuval Yarom et.al.
  The paper presents CacheBleed, the first timing attack to recover low address bits from secret-dependent memory accesses. The attack targets the modular exponentiation operation (i.e. during RSA decryption) as implemented in OpenSSL version 1.0.2f as well as its several forks such as LibreSSL and BoringSSL. The attack exploits cache-bank conflicts present in Intel Sandy Bridge Processor family. It is assumed that the victim and the attacker run concurrently on two hyperthreads of the same processor core. Thus, the victim and the attacker share the L1 data cache.

The paper demonstrates that it is possible to identify the exponentiation operations using cache-bank conflicts. Furthermore, the paper shows that is also possible to identify the individual multiplication operations performed during the modular exponentiation operation. For 4096-bit RSA the presented attack can fully recover the private key after observing 16,000 decryptions. The proposed countermeasures for the CacheBleed attack are disabling hyperthreading, constant-time implementations, and modifying memory accesses.

- *KISS: A Bit Too Simple* by Greg Rose
  The paper analyses security properties of KISS ("Keep it Simple Stupid") pseudo-random number generator originally proposed in 1993. Although the authors of KISS has never claimed cryptographic security for the KISS generator, others have made the intellectual leap and claimed that it is of cryptographic quality. The paper presents a number of standard attacks against KISS, where the best attack requires about 70 words of generated output and a few hours of computation to recover the initial state. The paper concludes that the KISS generator should not be used in any context where cryptographic security is important because its period (maximum, expected, and minimum) is not as long as originally claimed.

2 The ArcticCrypt Excursion

One day was dedicated to an exciting boat trip where all the workshop participants were invited. The ship was sailing slowly towards north east and the Nordenskild glacier. The featured destination was Pyramiden, an abandoned Russian mining settlement where everything is still intact. At the northernmost point of the route, our ship was approximately 1300 km away from the geographical North Pole. During the trip we also passed Brucebyen, Skansebukta, Svenskehuset at Kapp Thordsen, and the bird mountain at Diabas. The guide on board enlightened us about fascinating nature, history, hunters, and fauna of the arctic region.