Cryptanalysis of the Light-Weight Cipher A2U2

Mohamed Ahmed Abdelraheem¹, Julia Borghoff¹,*
Erik Zenner²,⋆⋆, and Mathieu David³

¹ Technical University of Denmark
{m.a.abdelraheem,j.borghoff}@mat.dtu.dk
² University of Applied Sciences Offenburg, Germany
erik.zenner@hs-offenburg.de
³ Aalborg University, Denmark
md@es.aau.dk

Abstract. In recent years, light-weight cryptography has received a lot of attention. Many primitives suitable for resource-restricted hardware platforms have been proposed. In this paper, we present a cryptanalysis of the new stream cipher A2U2 presented at IEEE RFID 2011 [9] that has a key length of 56 bit. We start by disproving and then repairing an extremely efficient attack presented by Chai et al. [8], showing that A2U2 can be broken in less than a second in the chosen-plaintext case. We then turn our attention to the more challenging known-plaintext case and propose a number of attacks. A guess-and-determine approach combined with algebraic cryptanalysis yields an attack that requires about $2^{49}$ internal guesses. We also show how to determine the 5-bit counter key and how to reconstruct the 56-bit key in about $2^{38}$ steps if the attacker can freely choose the IV. Furthermore, we investigate the possibility of exploiting the knowledge of a “noisy keystream” by solving a Max-PoSSo problem. We conclude that the cipher needs to be repaired and point out a number of simple measures that would prevent the above attacks.

1 Introduction

In recent years, pervasive computing has received a lot of research attention. The idea of integrating ubiquitous processors in a variety of devices and applications requires hardware that is both small and cheap. This poses new challenges for all areas of engineering, and since security and privacy issues are involved in many cases, also for the field of cryptography. The main problem is that the existing cryptographic solutions like the Advanced Encryption Standard (AES) are much too heavy to be usable in tiny pervasive computing devices.

A famous example for such devices are Radio Frequency Identification (RFID) tags. As the name implies, the goal of these tiny devices is to identify themselves to an authorized reader. If not properly protected, both security and privacy

* The author is supported by a grant from the Danish research council for Technology and Production Sciences grant number 10-093667.
** This work was carried out while at the Technical University of Denmark.
problems can be foreseen: An illegal device can pose as a legitimate tag, and an illegal reader can trace the movements of the tag and thus also of its owner. To prevent these kinds of attacks, cryptographic protection is required, but at the same time, the cryptographic primitives involved have to be small and cheap enough not to make the whole system impractical.

For this reason, many light-weight cryptographic solutions (with a special focus on RFID) have been proposed in recent years. Famous recent examples are PRESENT [4], KATAN/KTANTAN [7], PRINTcipher [12], or ARMADILLO [8]. Since these solutions often go the limits of technology and cannot afford the generous security margins built into classical designs, it is not surprising that attacks are frequent [5,13,14,1].

A very recent proposal of this kind is the stream cipher A2U2 that was proposed by David et al. at IEEE RFID 2011 [9] and that was designed for use with light-weight RFID (preferably with printed circuits). Only a few weeks later, an attack was published on IACR Eprint by Chai et al. [8], claiming to break the cipher in a chosen-plaintext attack using extremely little computational resources. However, this attack does not work in practice since it uses an erroneous description of the cipher.

Contents of the paper: In this paper, we start by describing the cipher (Section 2) and by demonstrating why the Chai et al. attack is not working. We then show how to repair it, yielding an attack for the chosen-plaintext case that requires less than a second running time and very little data (Section 3).

We then proceed to discuss the more challenging class of known-plaintext attacks. In Section 4 we describe a guess-and-determine attack that requires guessing $2^{49}$ inner state bits in order to retrieve the starting state.

In addition, we present a chosen-IV attack that makes use of the special key/IV setup of the cipher. A special design feature of A2U2 is that the number of initialization rounds varies and depends on an internal counter. The number of rounds varies from 9 to 126. In Section 5 we propose a differential-style attack which first enables us to find the 5-bit counter key. Moreover, we present an attack that recovers the master key in the case that only 9 initialization rounds are used. The latter attack requires $2^{38}$ computational steps, making it the most efficient known-plaintext attack to date.

In Section 6 we use the fact that there is a strong correlation between the ciphertext xored with a known counter sequence and the sequence which has been used to generate the ciphertext bits. Thus, we know the keystream xored with some error vector. This enables us to describe the problem of recovering the key as a Max-PoSSo problem [2] which means that we solve a polynomial system where a maximal number of the equations shall be satisfied. This can be done using mixed-integer optimization. Using this approach we are able to recover the key in less than $2^{42}$ seconds using a single chosen plaintext.

Finally, in Section 7 we describe urgent changes that should be done to the cipher design in order to avoid the above attacks. We also give some further research directions, both for cryptanalysis and improvement of the cipher.