WHIRLBOB, the Whirlpool Based Variant of STRIBOB
Lighter, Faster, and Constant Time

Markku–Juhani O. Saarinen\textsuperscript{1(ES)} and Billy Bob Brumley\textsuperscript{2}

\textsuperscript{1} Centre for Secure Information Technologies (CSIT) ECIT, Queen’s University Belfast, Belfast, UK
\texttt{m.saarinen@qub.ac.uk}

\textsuperscript{2} Tampere University of Technology, Tampere, Finland
\texttt{billy.brumley@tut.fi}

Abstract. WHIRLBOB, also known as STRIBOBr2, is an AEAD (Authenticated Encryption with Associated Data) algorithm derived from STRIBOBr1 and the Whirlpool hash algorithm. WHIRLBOB/STRIBOBr2 is a second round candidate in the CAESAR competition. As with STRIBOBr1, the reduced-size Sponge design has a strong provable security link with a standardized hash algorithm. The new design utilizes only the LPS or \( \rho \) component of Whirlpool in flexibly domain-separated BLNK Sponge mode. The number of rounds is increased from 10 to 12 as a countermeasure against Rebound Distinguishing attacks. The \( 8 \times 8 \) - bit S-Box used by Whirlpool and WHIRLBOB is constructed from \( 4 \times 4 \) - bit “MiniBoxes”. We report on fast constant-time Intel SSSE3 and ARM NEON SIMD WHIRLBOB implementations that keep full miniboxes in registers and access them via SIMD shuffles. This is an efficient countermeasure against AES-style cache timing side-channel attacks. Another main advantage of WHIRLBOB over STRIBOBr1 (and most other AEADs) is its greatly reduced implementation footprint on lightweight platforms. On many lower-end microcontrollers the total software footprint of \( \pi + \text{BLNK} = \text{WHIRLBOB} \) AEAD is less than half a kilobyte. We also report an FPGA implementation that requires 4,946 logic units for a single round of WHIRLBOB, which compares favorably to 7,972 required for Keccak / Keyak on the same target platform. The relatively small S-Box gate count also enables efficient 64-bit bitsliced straight-line implementations. We finally present some discussion and analysis on the relationships between WHIRLBOB, Whirlpool, the Russian GOST Streebog hash, and the recent draft Russian Encryption Standard Kuznyechik.

Keywords: WHIRLBOB · STRIBOBr1 · Authenticated encryption · Sponge designs · Timing attacks · Whirlpool · Streebog · CAESAR competition

Much of this research was carried out during tenure of an ERCIM “Alain Bensousan” Fellowship Programme at NTNU, Trondheim.

© Springer International Publishing Switzerland 2015
DOI: 10.1007/978-3-319-26502-5_8
1 Introduction

STRIBOBr2, or WHIRLBOB, is an Authenticated Encryption with Associated Data (AEAD) algorithm and a CAESAR (“Competition for Authenticated Encryption: Security, Applicability, and Robustness”) [21] competition Second Round Candidate [58].

![Fig. 1. A simplified view of a Sponge-based AEAD. Padded Secret Key, Nonce, and Associated Authenticated Data - all represented by $d_u$ words - are first “absorbed” into the state. The $\pi$ permutation is then also used to encrypt data $p_i$ into ciphertext $c_i$ (or vice versa) and finally to “squeeze” out a Message Authentication Code $h_i$.](image)

AEAD algorithms and modes such as GCM [45] provide both confidentiality and integrity protection for messages in a single step, thus eliminating the need for a separate MAC algorithm such as HMAC [46]. This has clear advantages for performance and implementation footprint.

WHIRLBOB uses STRIBOBr1’s BLNK Sponge AEAD mode and parameters without modification. Outside the CAESAR context, BLNK can be also used in a wider set of applications, even to build entire secure lightweight protocol suites [53]. A sponge mode requires only a single cryptographic component; an unkeyed cryptographic permutation $\pi$ (See Figure 1). As with other provable Sponge modes, we assume that $\pi$ is indistinguishable from a random permutation. This work focuses on $\pi$ permutation design and implementation – for BLNK padding details and analysis we refer to [32,54,56,57].

The STRIBOBr1 CAESAR [56] candidate was derived from the Russian GOST hash standard Streebog [26]. In close examination Streebog appears to be modeled after the Whirlpool hash [4], with substantial modifications. However, STRIBOBr1 and WHIRLBOB only differ in the particular numerical selections for tables $C$, $S$, and $L$. These components, $L \circ P \circ S$ or the “LPS permutation” is derived directly from that of Whirlpool for WHIRLBOB. The program code of 64-bit reference implementations is essentially equivalent for both algorithms. Both STRIBOBr1 and WHIRLBOB have 12 rounds.

We show that the particular structure of the Whirlpool components allows WHIRLBOB to have much more efficient SIMD, constant-time, lightweight, and hardware implementations. One of our aims is to allow the same implementation core (such as a special instruction or coprocessor of a SoC [56]) to be also used for unkeyed hashing according to the Whirlpool standard. This is useful in