Response to "Slid Pairs in Salsa20 and Trivium"

Daniel J. Bernstein *

Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045
snuffle6@box.cr.yp.to

The paper "Slid Pairs in Salsa20 and Trivium" by Priemuth-Schmid and Biryukov states various "attacks" on Salsa20 and Trivium. The paper claims that "Salsa20 does not have 256-bit security," that its "attacks" demonstrate a "certificational weakness" in Salsa20, that "it is crucial for the security of Salsa20 that nonces are chosen at random," that the "attacks" can be "exploited in certain scenarios," etc.

These claims are entirely without merit. The "attacks" on Salsa20 are vastly more expensive than the standard brute-force attacks discussed in the original Salsa20 documentation. (I haven't looked at the "attacks" on Trivium.)

Specifically, the best "attack" in the paper receives ciphertexts from 2^{191} users and finds a 256-bit key after time 2^{192} on a machine of size roughly 2^{192}. This is described as an "improved" version of a trivial birthday attack that needs ciphertexts from 2^{192} users. See Table 3 in the paper.

For comparison, standard cipher-independent brute-force attacks receive a very small amount of ciphertext and find a 256-bit key after time 2^{128} on a machine of size roughly 2^{128}. More sophisticated, but still standard, cipher-independent brute-force attacks receive ciphertexts from (for example) 2^{64} users and find a 256-bit key after time 2^{96} on a machine of size roughly 2^{96}. (See, e.g., my 2005 paper "Understanding brute force.")

Standard brute-force attack	New "attack"
2^{64} inputs	2^{191} inputs
time 2^{96} to break one input	time 2^{192} to break one input
machine cost 2^{96}	machine cost 2^{192}

The fundamental reason that the new "attack" is so expensive, compared to standard attacks, is that the "attack" starts from a hypothesized key-pair relation $R(k_0, k_1)$ that is satisfied with probability only about $1/2^{256}$. Redefining $R(k_0, k_1)$ as the relation "$k_0 = \alpha$" (and ignoring k_1), for a constant α, would achieve the same $1/2^{256}$ success probability, not just against Salsa20 but against any 256-bit cipher. The authors could use the same superficial "analysis" to claim that AES, with a 256-bit key, provides much less than 256-bit security.

---

* Permanent ID of this document: 18ebd5dbaba4900d5e686070cec146ed. Date of this document: 2008.09.25. This work was supported by the National Science Foundation under grant ITR–0716498.