Pengembangan Fungsi Hash Kriptografis Baru Berbasis Konstruksi Spons untuk Internet of Things (IoT) = The Development of Novel Sponge-based Cryptographic-Hash-Functions for Internet of Things (IoT)

Susila Windarta, author

Abstrak

Penelitian ini berhasil mengembangkan dua permutasi baru, yaitu Modified-SATURNIN yang dihasilkan dari modifikasi permutasi pertama pada komponen supers-box, dan permutasi WSR berbasis block cipher SIMON-like. Kedua permutasi ini memiliki ketahanan yang baik terhadap kriptanalisis diferensial dan linier. Tiga fungsi hash ringan baru, yaitu ALIT-Hash, TJUILIK-Hash, dan WSR-Hash, diusulkan dalam penelitian ini. ALIT-Hash berbasis algoritma block cipher SATURNIN dan mode operasi Beetle. TJUILIK-Hash adalah fungsi hash berbasis Modified-SATURNIN dengan mode operasi Beetle. WSR-Hash menggunakan permutasi WSR dengan mode spons. Ketiga fungsi hash ini memiliki ketahanan yang baik terhadap serangan preimage, second preimage, dan collision. Hasil analisis keamanan menunjukkan bahwa fungsi hash yang diusulkan memiliki tingkat keamanan yang baik dalam hal kriptanalisis diferensial dan linear. Tingkat keamanan diferensial dari TJUILIK-Hash lebih baik daripada ALITHash karena perubahan pada s-box. Dalam uji kinerja, pada perangkat keras Arduino Mega2560 Rev. 3, ALIT-Hash dan TJUILIK-Hash menunjukkan kecepatan eksekusi yang sama untuk semua ukuran byte yang diuji, yaitu sebesar 0,1879-0,188 detik. Namun, keduanya masih kalah cepat dibandingkan dengan beberapa algoritma lain. WSR-Hash memiliki waktu eksekusi sebesar 0,2005 detik untuk data berukuran 1024 byte, 0,0304 detik untuk data berukuran 128 byte, dan 0,0091 detik untuk data berukuran 16 byte. Rerata waktu eksekusi dari ketiga ukuran data adalah 0,0800 detik. Pada perangkat lunak komputer personal 64-bit, ALIT-Hash dan TJUILIK-Hash menunjukkan performa yang cukup baik, meskipun memiliki waktu eksekusi yang lebih lambat. ALIT-Hash memiliki waktu eksekusi rerata 1,814 mikrodetik, sedangkan TJUILIK-Hash memiliki waktu eksekusi rerata 36,007 mikrodetik. WSR-Hash memiliki rerata waktu eksekusi 112,428 mikrodetik untuk 1024 byte, 128 byte, dan 16 byte. Rerata throughput WSR-Hash sebesar 20,243 bit/mikrodetik. Dalam simulasi pada Contiki-NG dan simulator Cooja, ALIT-Hash dan TJUILIK-Hash menunjukkan kinerja yang baik dibandingkan dengan beberapa fungsi hash yang dibandingkan. WSR-Hash juga memperlihatkan performa yang kompetitif dengan throughput sebesar 1.891,34 bit/detik, konsumsi energi sebesar 10,90 mJ, dan ukuran ROM dan RAM yang lebih kecil. Selain itu, ketiga fungsi hash yang diusulkan berhasil lulus pengujian keacakan kriptografis dengan p-value lebih besar dari 0,01. Uji keacakan NIST STS menunjukkan bahwa TJUILIK-Hash berhasil lulus semua pengujian, sedangkan ALIT-Hash hanya gagal dalam subuji overlapping template. WSRHash lulus 15 uji NIST STS. Oleh karena itu, penerapan fungsi hash yang diusulkan ini perlu dipertimbangkan untuk efektivitas biaya dan tingkat keamanannya yang tinggi, yang sangat penting untuk perangkat IoT dengan sumber daya terbatas.

.....This study successfully developed two new permutations: Modified-SATURNIN, which is a modification of the first permutation of the super s-box component, and WSR, which is based on the block cipher SIMON-like. Both permutations exhibit strong resistance against differential and linear cryptanalysis. This study proposes three new lightweight hash functions: ALIT-Hash, TJUILIK-Hash, and WSR-Hash.

The Alit-Hash algorithm is derived from the block cipher Saturnin and utilizes the Beetle mode of operation. The hash function TJUILIK-Hash is derived from the Modified-SATURNIN algorithm and utilizes the Beetle operation mode. The WSR-Hash algorithm employs the WSR permutation in sponge mode. These three hash functions exhibit strong resistance against preimage, second preimage, and collision attacks. The security analysis indicates that the proposed hash function demonstrates a satisfactory level of security against differential and linear cryptanalysis techniques. The differential security level of TJUILIK-Hash surpasses that of ALIT-Hash due to modifications made to the s-box. Performance tests were conducted on the Arduino Mega2560 Rev. hardware. Both ALIT-Hash and TJUILIK-Hash exhibit consistent execution speeds across all tested byte sizes, averaging 0.1879-0.188 seconds. However, both algorithms are slower compared to specific other algorithms. The execution time of WSR-Hash is 0.2005 seconds for 1024 bytes, 0.0304 seconds for 128 bytes, and 0.0091 seconds for 16 data. The mean execution time for the three different data sizes is 0.0800 seconds. The ALIT-Hash and TJUILIK-Hash algorithms perform satisfactorily on 64-bit personal computer software, although their execution times are relatively slower. The average execution time of ALIT-Hash is 1.814 microseconds, whereas TJUILIK-Hash has an average execution time of 36.007 microseconds. The average execution time of WSR-Hash for 1024 bytes, 128 bytes, and 16 bytes is 112.428 microseconds. The mean throughput of WSR-Hash is 20.243bits/microseconds. In the simulation conducted on Contiki-NG and the Cooja simulator, the performance of ALIT-Hash and TJUILIK-Hash was superior to that of certain other hash functions. The WSR-Hash algorithm demonstrates competitive performance in terms of throughput (1,891.34 bits/sec), energy consumption (10.90 mJ), and smaller ROM and RAM sizes. Furthermore, the three hash functions under consideration have successfully passed the cryptographic randomness test, exhibiting a p-value exceeding 0.01. The NIST STS randomness test indicated that TJUILIK-Hash demonstrated successful performance across all tests, whereas ALIT-Hash only failed in the overlapping template subtest. The WSR-Hash algorithm successfully passed all 15 NIST STS tests. Hence, adopting these suggested hash functions is recommended due to their cost-effectiveness and robust security features, which are vital for IoT devices with limited resources.