K I K

Kasseler Informatik-Kolloquium

UNIKASSEL VERSITÄT

Informatik

Im Kasseler Informatik-Kolloquium (KIK) präsentieren Forscherinnen und Forscher aktuelle Ergebnisse zu Grundlagen und Anwendungen der Informatik bzw. verwandten Gebieten.

Das KIK findet an der **Universität Kassel, in der Wilhelmshöher Allee 73** statt.

Kontakt: Prof. Dr. Bernhard Sick
FG Intelligente Eingebettete Systeme
Tel.: 0561/804-6020, bsick@uni-kassel.de

Di., 03. September 2019, 16.00 Uhr
im Hörsaal 0315

Dr. Abdelkrim Kamel Oudjida
(Advanced Technologies Development Center, Algiers)

"Radix-2^w Arithmetic for Scalar Multiplication in Elliptic Curve Cryptography (ECC)"

Abstract:

Scalar multiplication K×P, where K is a nonnegative constant and P is a point on the elliptic curve, requires two distinct operations: addition (ADD) and doubling (DBL). To reduce the number of ADD operations, a recoding of K with fewer nonzero digits is necessary. Based on Radix-2^w arithmetic, a new w-bit windowing algorithm is presented to speed up the scalar multiplication with low memory consumption. Contrary to existing methods, to minimize the number of ADDs the window size (w) is determined by an exact analytic formula depending on the bit-length (l) of the scalar K. The number of required precomputations is minimal regarding the value of w. The proposed algorithm recodes the binary string K and evaluates the multiplication on-the-fly from right-to-left and left-to-right, likewise. In comparison to the non-adjacent form (NAF), Radix-2^w algorithm reduces ADDs by 35% in average for NIST recommended GF(2^l) finite fields. When considering the maximum number of ADDs (upper bound), a saving of 56% in average is achieved over NAF. Furthermore, Radix-2^w method is very easy to be used and highly reconfigurable, allowing speed- memory trade-off to satisfy different crypto-system constraints. Most importantly, the method is resilient to side-channel attacks based on power, timing, and statistical analysis.