Equations over the finite field $\mathbb{F}_{2^n}$

Sihem Mesnager
(joint work with K.H. Kim)

University of Paris VIII (department of mathematics) and
university of Paris XIII (LAGA)

Let N_a be the number of solutions to the equation $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ where $\gcd(k, n) = 1$. In 2004, by Bluher it was known that possible values of N_a are only 0, 1 and 3. In 2008, Helleseth and Kholosha have got criteria for $N_a = 1$ and an explicit expression of the unique solution when $\gcd(k, n) = 1$. In 2014, Bracken, Tan and Tan presented a criterion for $N_a = 0$ when n is even and $\gcd(k, n) = 1$. In this talk, we review some equations over $\mathbb{F}_{2^n}$ and present the solution of the equation $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n, k) = 1$. We explicitly calculate all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(x)$. New criterion for which a, N_a is equal to 0, 1 or 3 is a by-product of our result.