
Binary Decision Diagrams (BDD) [1] are built on the basis of Shennon decomposition, positive and negative Davio decompositions [2]. These diagrams are widely used for representation and realization of Boolean functions (BF) — «Bit level» — $f(x_1, x_2, ..., x_n)$:

\[
\begin{align*}
S & : f = x \land f_{x=0} \lor x \land f_{x=1} \\
pD & : f = f_{x=0} \oplus x \land (f_{x=0} \oplus f_{x=1}) \\
nD & : f = f_{x=1} \oplus x \land (f_{x=0} \oplus f_{x=1})
\end{align*}
\]

In [2] arithmetic BDD are considered for realization of BF systems — «Word level» — $F(x_1, x_2, ..., x_n)$. The lower circle of BDD based on the arithmetic Shennon decomposition, represents numerical values of the right column of the table of BF system validity; the lower circle of BDD based on the arithmetic positive Davio decomposition consists of coefficients from $\mathbb{Z}$ polynoms received by generalization of a numerical normal form:

\[
\begin{align*}
S_A & : F = (1-x)F_{x=0} + xF_{x=1} \\
pDA & : F = F_{x=0} + x(-F_{x=0} + F_{x=1}) \\
nDA & : F = F_{x=1} + (1-x)(F_{x=0} - F_{x=1})
\end{align*}
\]

In [3] modular forms of arithmetic polynomials are invented. Following [3] arithmetic decomposition BF systems — «Word level» — in the ring $\mathbb{Z}_m$ ($\hat{\oplus}$ — composition in $\mathbb{Z}_m$; $\hat{F} \in \mathbb{Z}_m$) are considered:
In some cases numerical decomposition of BF systems in the ring $\mathbb{Z}_m$, by analogy with modular polynomials from [3], makes it possible to reduce the temporary and/or spatial complexity of BF systems realization by supporting means for the asymmetric cryptoalgorithms (functioning in the ring $\mathbb{Z}_m$) and are applied to support implementers of symmetric cryptoalgorithms and other applications.

REFERENCES