1079-94-167 **Claude Carlet**, LAGA, Universities of Paris 8 and Paris 13;, CNRS, UMR 7539, University of Paris 8, Department of Mathematics, Paris, France, **Philippe Gaborit**, XLIM-DMI, Universite de Limoges, Limoges, France, **Jon-Lark Kim*** (jl.kim@louisville.edu), 328 Natural Sciences Building, Department of Mathematics, Louisville, KY 40292, and **Patrick Sole**, CNRS/LTCI, UMR 5141, Telecom ParisTech, Paris, France. *A new class of codes for Boolean masking of cryptographic computations.*

We introduce a new class of rate one half binary codes: **complementary information set codes.** A binary linear code of length $2n$ and dimension n is called a complementary information set code (CIS code for short) if it has two disjoint information sets. This class of codes contains self-dual codes as a subclass. It is connected to graph correlation immune Boolean functions of use in the security of hardware implementations of cryptographic primitives. Such codes permit to improve the cost of masking cryptographic algorithms against side channel attacks. In this paper we investigate this new class of codes: we give optimal or best known CIS codes of length < 132. We derive general constructions based on cyclic codes and on double circulant codes. We derive a Varshamov-Gilbert bound for long CIS codes, and show that they can all be classified in small lengths ≤ 12 by the building up construction. (Received January 11, 2012)