PPT

A pseudorandom Poly Time. (Real Hdp.)

Also known as the Hard - Core - Bit - Gen ?

NP Hard Problem

G is a cyclic group.

$\{y\}$ is a generator.

$x \in G, \exists \; y$

$y^3 = x$

$y = \log_y x$

$\{1, y, \ldots, y\}$

$y^2 = \{1, y, y^2\}$

$\{1, y, \ldots, y^{q-1}\}$

$\{1, y^2, y^4, y^6, y^8, y^{10}, y^{12}, y^{14}, y^{16}, y^{18}, y^{20}, y^{22}, y^{24}, y^{26}, y^{28}, y^{30}, y^{32}, y^{34}, y^{36}, y^{38}, y^{40}, y^{42}, y^{44}, y^{46}, y^{48}, y^{50}, y^{52}, y^{54}, y^{56}, y^{58}, y^{60}, y^{62}, y^{64}, y^{66}, y^{68}, y^{70}, y^{72}, y^{74}, y^{76}, y^{78}, y^{80}, y^{82}, y^{84}, y^{86}, y^{88},