Báo cáo ngày 7/1/2025

5. Nhược điểm của PBC:

Bảo mật thấp: PBC chỉ cung cấp mức bảo mật 80-bit, không đáp ứng được yêu cầu bảo mật cao của các ứng dụng hiện đại.

Lỗi thời: Thư viện PBC đã lâu không được cập nhật, do đó không hỗ trợ các thuật toán và kỹ thuật mới nhất.

Dễ bị tấn công: Do sử dụng các đường cong elliptic và tham số đã cũ, PBC có thể dễ bị tấn công hơn so với các thư viện mới