



plaintext



well-formedness



commitment



range proof