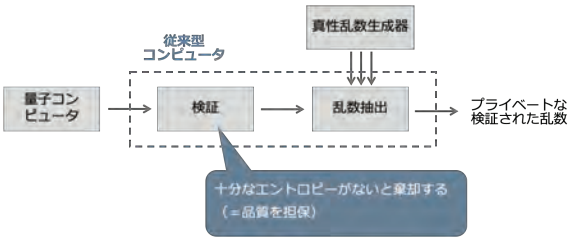
子もつれ」は物理的な手法で計測することが可能である点だ。これを応用することで、従来では不可能であった生成中の乱数の品質確認が実現できる（**図 3**）。逆に言えば、ここまで踏みこむことで初めて量子乱数生成を利用する明確な理由が生じるのではないかと考えている。暗号分野の研究者は現在、この「デバイス独立性」について活発な議論を行っている最中である。

【図 3】 デバイスに極力依存せずに乱数を生成する手法



SMS認証の課題

フィッシング詐欺などが課題のSMS認証 電話発信型の着信認証で問題を解決

ケーブルテレビのマイページなど、あらゆるサービスでセキュリティとして導入されている SMS 認証だが、利便性やフィッシング詐欺への悪用などさまざまな課題から電話発信型の新しい認証方式に変化しつつある。SMS 認証の課題と解決策を 3 点から解説する。

松村颯太
株式会社オスティアリーズ
Marketing Manager

1 ユーザ離脱

SMS 認証はショートメールで数桁の数字などのコードを受信して、サービス画面に正しい認証コードを入力すると認証が完了するが、ユーザが SMS を受信できない、SMS の受信が遅いなどの理由で認証ができず、ユーザ離脱につながるケースが発生している。

2 フィッシング詐欺への悪用

昨今、偽サイトにユーザを誘導し個人情報を盗み取るフィッシング詐欺が増加している。その偽サイトへ誘導するためのチャネルとして SMS が悪用されており、ユーザは本物と偽 SMS の見分けがつかず、SMS の開封率、認証成功率の低下につながっている。

【図】SMS 認証と着信認証の比較

3 不正目的の複数アカウント作成

キャンペーンへの重複応募、初回登録特典の複数回利用などの不正目的の複数アカウント作成防止のため、認証が導入されているケースがあるが、SMS 認証に使用するデータ通信用電話番号（SIM）は購入時に本人確認が必要なく大量購入可能なものもあるため、SNS などで SMS 認証代行が行われ逮捕者が出るなど、社会問題となっている。

上記のような SMS 認証の課題を解決するため、昨今では電話発信型の着信認証サービスが拡がりを見せている。電話発信型のためユーザが SMS でコードを受信する必要がなく、老若男女問わず簡単にワンコールで認証可能であり、フィッシング詐欺のチャネルとして悪用されることもない。また、電話発信（音声通話）を行う電話番号は購入時に本人確認が必須のため、大量保持が難しく不正目的の複数アカウント作成防止にも効果が高いところも特徴だ。

ケーブルテレビのユーザは高齢者の割合が高い。使い慣れている電話を使い、フィッシング詐欺のチャネルになることもない電話発信型の着信認証は、ケーブルテレビ事業者に適した認証方式である。