量子コンピュータ時代の

暗号技術とインターネット技術

量子コンピュータ時代の暗号技術とインターネット技術を「ポスト量子ビット」と参照します：これについての記事を連載します。今回はその第一回目、ポスト量子ビットの輪郭記事です。

量子コンピュータによって公開鍵暗号の「うそ」がバレる日が近づいています。「うそ」も短い時間ならいいんですが、長い時間の「うそ」はバレる、たとえば、電子署名は全滅です、ビットコインなど暗号通貨も全滅です。ブロックチェーンは長い時間に耐えるからこそ、それは「信用」ですが、その「信用」が余命 10 年と「医者」に言われたら、どうでしょう？

NIST vs METEORA

ポスト量子ビットには二つのイニシャテイブが有る。一つは、短い時間なら「うそ」をついてもいいという訳だから、公開鍵を何とか改良しようという発想です。改良すると言っても、相手は量子計算ですから、「うそ」の時間と計算エラーとはトレードオフの関係です、また、性能ともトレードオフの関係です、この対策を行うハメになっている。この対策のための対策を「プロトコル互換」と言います。プロトコル互換は「馬車を改良する」の意味です：馬車を改良したら馬車になる、決して「汽車」には成らない、ですね。馬車の改良イニシャテイブがアメリカは国家機関 NIST です。もう一つのイニシャテイブは METEORA SYSTEM です、馬車の改良イニシャテイブではないから「プロトコル非互換」と言います。こちらが「汽車」です。下の図は 2018 年から 2028 年までを見た様子です。

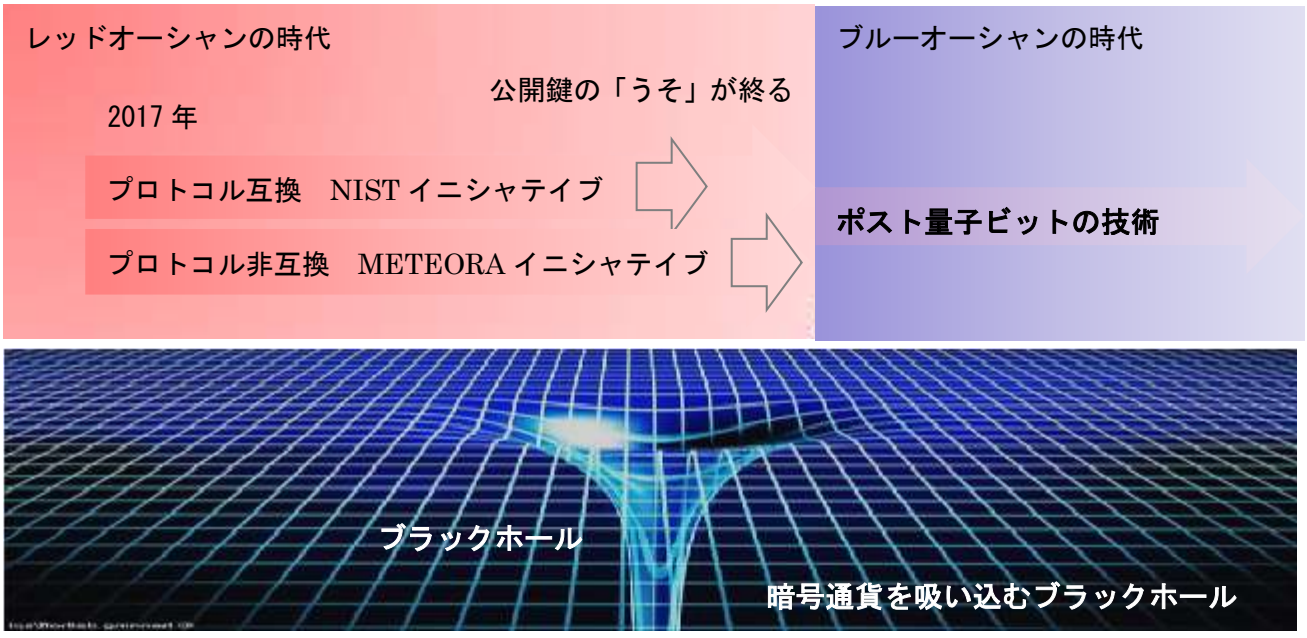

図１：今はレッドオーシャン、間もなくブルーオーシャンに変わる。

プロトコル非互換

プロトコル非互換の技術は量子計算に対しても「長いうそ」をつくことが出来ます。その数理と手段を「衝突証言 a collision attest」と言います。陽子と陽子を衝突させる衝突実験をスイスの CERN でやっています、約 1 兆回の実験をやれば、ヒッグス粒子を一つ検出するという話です：この衝突実験を量子計算の内部に閉じ込めることが出来るでしょうか？ナンセンスですね。**秘密を探る作業は重労働（高コスト）になります、**それが衝突実験の意味です。

同じく「衝突証言 a collision attest」も重労働（長時間）になります：**秘密鍵のアクセス権を持たない者が秘密鍵を復元しようとすると、その不正行為は重労働（長時間）になる**、そういう仕組みが「衝突証言 a collision attest」です。たとえば、1 兆回の 1 兆回の 1 兆回の又 1 兆回…というような重労働になってしまう。「衝突証言」は量子計算の外部世界の実験です。この実験で秘密鍵を復元することは出来るが、その確率は=$1/2^{256}$、ヒッグス粒子の出現確率よりも遥かに小さい。ですから衝突実験は重労働（長時間）です。それで**プロトコル非互換の方は「長いうそ」をつくこと出来ます**。これがポスト量子ビットの基盤です。追々本連載で紹介します。

ご存じのように、ブロックチェーンをブロックチェーンにしているのは Proof of Work の計算です：これは不正行為には重労働（高コスト）を課す話です。「衝突証言」の方も不正行為に重労働（長時間）を課す話です。ですから「衝突証言」に基づく”ブロックチェーン”を設計できる。それはどんな”ブロックチェーン”になるでしょうか？

目に見えないもの、「信用」を創る

プロトコル非互換の「長いうそ」は、目には見えない「信用」を創ることが出来ます。ブロックチェーンは素晴らしい発明です。なぜなら、目に見えるコンピュータプログラムが目に見えない「信用」を創り出したからです。目に見えるもので目に見えない「価値」を創り出した、それが素晴らしい、画期的な理由です。しかし、**公開鍵はもう「長いウソ」をつくことが出来ないから**、ブロックチェーンは素晴らしいが、その「信用」は終わりです。ブロックチェーンの「信用」がもたらした暗号通貨も終わり：今はただのチューリップでしょう。**今後、「信用」は、すなわち、マネーはプロトコル非互換の技術で創るしか手が有りません**：ブロックチェーンに代わる技術を仮に「ブロックトレーン」と言いましょう。ブロックチェーンを改良したらブロックチェーン 2.0…3.0…となり、ブロックトレーン（汽車）には成りません。ここでブロックチェーンの信用とブロックトレーンの信用を比較します：表 1 の通りです。

目に見えないもの、「信用」	ブロックチェーン Block chain	ブロックトレーン Block train
流通性[注1]（系列に限らない決済）	○	○
連続譲渡性[注1]（人から人へ流通）	○	○
汎用性[注1]（用途を限らない）	○	○

記録の非可逆性	◯	◯
即時完了性（ブロック追加の）	↗ 不可能（マイニング）	◯ 二つで一つの署名法[注2]
ブロックの非可逆性（撤回・差し替え、改ざんが不可能）	◯ Proof-of-Work ✓不正行為には重労働を課す	◯ 衝突証言 a collision attest[注3] ✓不正行為には重労働を課す
記録の匿名性	◐ ✓取引記録は公開される。 ✓参加者を識別する名前： ビットコインアドレス	◐ ✓取引記録は公開される。 ✓参加者を識別する名前： **公開パスワード**[注4]
暗号通貨の請求・支払コード	◯ ビットコインアドレス	◯ **公開パスワード**[注4]
マネーローンダリング	↗ 可能	◯ 不可能（端末間プロトコル）
不正送金、取引所の横領	↗ 可能（ロジカルに可能）	◯ 困難（署名データは二つ有る）
貨幣の需要に応える能力、貨幣の暴騰を管理する能力、貨幣の発行主体に誰でも成れる！	↗ ダメ！	◯ OK ✓暗号通貨を立ち上げた者がマネーの発行と管理を行う。

表１：暗号通貨の対比

表１を一瞥すれば、ブロックトレーンはブロックチェーンの弱みを克服したように見えます：即時完了性（ブロック追加の）、ブロックの非可逆性（撤回・差し替え、改ざんが不可能）、マネーローンダリング、取引所の不正送金、取引所の横領、貨幣の需要に応える能力、貨幣の暴騰を管理する能力など全ての項目においてブロックトレーンは勝ると見えます。優位を可能にしている技術がいくつか目に入る：即時完了性における「二つで一つの署名法」[注2]、ブロックの非可逆性における「衝突証言 a collision attest」[注3]、それと暗号通貨の請求・支払い時に必要な「公開パスワード」[注4]です。これら注 2・注 3・注 4 の実装アルゴリズムは、共通の数学的な基盤から派生していて、根っ子は同じです。なお、注１：仮想通貨 Page116 東洋経済から引用。

この共通の数学的な基盤が何かについて本連載で採り上げます：ここで、数学的な基盤の軸は知識分割と衝突証言の二つから成ること、取引所の不正送金や横領が難しくなる理由などを開示する予定（知識分割に依り秘密鍵に相当するデータが見えなくなる）。アルゴリズムについては下記の「集合発明家」に限り開示します。

集合発明家 (a collective inventor)

関連特許（後述）は二つ有る。そこの実施例とアルゴリズムはポスト量子ビットを視野に入れたものではないが、その数学的な基盤はポスト量子ビットにとって不可欠な基盤です。近い将来、新たな実施例とアルゴリズムを伴い、特許申請の時は来るでしょう。が、当社で申請する考えはなく「集合発明家」(a collective inventor)に申請の特典を与えることを考えています。

集合発明家とは METEORA SYSTEM の事業継承をするエンジニアと企業の自発的な集団です。METEORA SYSTEM 株式会社は上記関連特許のライセンス事業に特化する一方、集合発明家が発明者の DNA を継承しブルーオーシャンに船出します、起業する訳です。恐らく、第二の IBM になるでしょう。

発明は開発とは違います、改良とも違います。開発と改良は最初から出発駅と終着駅が与えられていますが、発明はそうではない、専門家が想定し得ないものです。人のワクワク感が拍車をかけるものです。ですから、一人一人は発明の経験が無くても、発明家の DNA を受け入れれば発明の磁場が生まれ、その磁場が発明家になる…。エンジニアさん、企業さん、何か惹かれるものを感じたら、ご一報を下されば、と思います。

関連特許

[特許証]

特許第 6025160 号

発明の名称　二つで一つのパスワード

特許権者　渡邊栄治

メテオーラ・システム株式会社

出願番号　特願 2016-544660

登録日　平成 28 年 10 月 21 日（October 21.2016）

PCT の文書

検索エンジンへ WIPO➔PATENTSCOPE database ➔国際公開番号　WO 2016/009570

特許第 6025160 号の検索

https://www.j-platpat.inpit.go.jp➔特許公報（B）➔6025160 入力

[掴み]

この特許に派生するアプリケーションの一つが「2015 年 非対称パスワード」です。サービス側からパスワード p が漏えいする事件が有りました。パスワード p はユーザの記憶 q とは異なるという「うそ」は直ぐバレるので、

p=q

です。それで、パスワード p が漏えいすれば、ユーザの記憶 q も漏えいする訳です。ここに大事な論点があります、パスワードは本質的に p=q ですから、「**パスワード自体に安全保障の備えが無**

い」という点です。もし、パスワードが

$p \neq q$

というパスワードでしたら、どうなるでしょうか？パスワード p が漏えいしてもユーザの記憶 q は漏えいしない！何と単純な論理でしょう。単純ではあるが、「**パスワード自体に安全保障の備えが有る**」ことに注目します。実装形態もスマートフォンになるのでユーザの利便性も申し分ない。これを非対称パスワードと名付けました。世の中が大歓迎すると思っていました。しかし、そうは成らなかった：注目する方は多かったが、IT 業界のみなさんは「間に合ってます」というものでした、「現状が一番好きだ」と言っています。

皆さんが言うイノベーションというのは現状維持のための一手らしい、何であれ現状が大好き！ここから発明家はこんなことを学んだ：私の発明品は**現状が足元から崩れる時に**「どうですか？」と提案するものだと。現状が足元から崩れる時とは他でもない、公開鍵の「うそ」がバレる日のことです。もはや「長いうそ」はつけないことを賢明な方々は理解しているでしょうから、こうやって準備を開始しました。

その一つが「公開パスワード」です。非対称パスワードの $p \neq q$ は「長いうそ」です、バレないのです。量子計算が「短いうそ」にしようとガンバッテも、衝突証言という重労働を避けることが出来ません。で、非対称パスワード p を公開パスワードとして利用します。ブロックチェーンに適用する場合は、これがビットコインアドレスに代わります。皆さんは、その時、ブラウザの https に代わる通信路を探すでしょう。鍵交換の技術を探すでしょう。公開パスワードはそれにも役立ちます、特許第 5314240 号「通信路システム」の初期値の設定に役立ちます。

[特許証]

特許第 5314240 号

発明の名称　通信路システム

特許権者　渡邊栄治

出願番号　2006-308164

出願番号　特願 2006-308164

登録日　平成 25 年 7 月 12 日（July 12.2013）

特許第 5314240 号の検索

https://www.j-platpat.inpit.go.jp➜特許公報（B）➜5314240 入力

[掴み]

公開鍵の「うそ」がバレる日、これが鍵交換の主役に躍り出ます。乱数で乱数を暗号化した時には通信線上から鍵の情報が漏えいしない：これを発明者は「乱数 by 乱数」と呼んでいます。これを通信路の初期値の更新に使います。この計算プロセス＝「３way handshake」は非可逆です。ブロックチェーンも非可逆が肝です。**非可逆性はポスト量子ビットの基本的な属性です**。公開鍵のプロトコル互換からは出て来ない属性です。このポスト量子ビットはインターネットに何をもたらすか…ひとことで言え！と迫られたら、何と応えようか？インターネットのアプリケーション層は非可逆になる。これが答えだろうと思います。このインターネットにサイバーテロはいったい何をするのか？非可逆層に向かってサイバーテロは可能か？

第一回 END

渡辺栄治