暗号技術検討会
量子コンピュータ時代に向けた
暗号の在り方検討タスクフォース（第２回）

令 和 元 年 ９ 月 ６ 日
１０：００～１２：００
経 済 産 業 省 別 館 １１階
１１１１各省庁共用会議室

議 事 次 第

１　開会

２　議題

（１）前回議事概要の確認について

（２）耐量子計算機暗号の扱いについて

（３）軽量暗号の動向について

（４）軽量暗号等の扱いについて

（５）その他

３　閉会

配付資料一覧

資料１　第１回会合議事概要（案）

資料２　耐量子計算機暗号の扱いについて

資料３　岩田先生提出資料

資料４　軽量暗号等の扱いについて

資料1

量子コンピュータ時代に向けた暗号の在り方検討タスクフォース（第１回）
議事概要（案）

1. 日時

令和元年６月 24 日（月）18:00～20:00

2. 場所

経済産業省別館 11 階　1111 各省庁共用会議室

3. 出席者（敬称略）

構成員：松本勉、宇根正志、國廣昇、高木剛、松井充、松本泰、満塩尚史

オブザーバ：徳永竜一、久山純也、岡田崇志、衛門愛子、小高久義、寺田麻倫、中村美穂、青山豊克、荒木美敬、土本雄介、筧文貴、西城泰裕、野口信、三島崇、中村佳憲、岡野孝子、松田隆宏

事務局：（総務省）泉宏哉、赤阪晋介、豊重巨之
（経済産業省）三角育生、稲垣良一
（国立研究開発法人情報通信研究機構（NICT））盛合志帆
（独立行政法人情報処理推進機構（IPA））神田雅透

4. 議事

（１）　タスクフォースの設置について
（２）　量子コンピュータの動向について
（３）　耐量子計算機暗号の動向について

5. 配付資料

資料１	「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」開催要綱（案）
資料２	量子コンピュータ時代に向けた暗号の在り方検討タスクフォースの設置について
資料３	國廣構成員提出資料
資料４	高木構成員提出資料

6. 議事概要

6.1. 開会

タスクフォース事務局から開会の宣言があり、総務省の泉審議官から開会の挨拶が行われた。また、事務局から資料１に基づき開催要綱（案）の説明があり、原案のとお

り承認された。さらに、座長の選出が行われ、松本勉構成員が座長に選出された。

6.2. 議事

（１） タスクフォースの設置について

資料２に沿って、暗号技術検討会事務局より説明が行われた。

（２） 量子コンピュータの動向について

資料３に沿って、國廣構成員より説明が行われた。

（３） 耐量子計算機暗号の動向について

資料４に沿って、高木構成員より説明が行われた。

（４） 意見交換

事務局からの説明及びヒアリング対象者からのプレゼンテーションの後、意見交換が行われた。主な意見等は次のとおり。

松本勉座長：資料４の 21 ページのグラフはどのように見れば良いか。

高木構成員：縦軸が LWE 問題（ノイズ付き多元連立一次方程式）のノイズ、横軸が LWE 問題の次元を表す。左下の赤いセルが実際に解かれた問題、赤いセルの中の丸の色がその問題を解いたアルゴリズムを表す。例えば、灰色のところは 2016 年に BKZ 2.0 algorithm で解かれており、黄色いところは Progressive-BKZ algorithm で解かれている。アルゴリズムが改良されると解読記録が伸び、グラフの右上に近づいていく。グラフの右上には、128 ビット量子安全性を表す曲線が三本引かれており、いつ頃に 128 ビット量子安全性が解けるかという予想図をこのグラフをもとに作成することができる。

宇根構成員：高木構成員の説明の中で、NIST が 2048 ビット RSA を 2030 年頃にやめるという話があったが、2031 年以降は耐量子計算機暗号に移行するのか、RSA の鍵長を伸ばす方向なのか、NIST はどのような意向か。

高木構成員：2030 年以降の動向は、鍵の長さを伸ばしたものが何ビットセキュリティに相当するかに左右されるだろう。

宇根構成員：いつ頃量子コンピュータが実用化されるかという話を議論するにはまだ知見が少ないということであるが、ベンチマークとしてどのような情報が明らかになれば暗号方式の移行のタイミングが見通せるようになるか。あるいは、過去のコンベンショナルな暗号の移行の際には、どのような情報が役に立ち、いつ頃に移行の時期を見通せるようになったか。

國廣構成員：量子コンピュータの性能に関しては、何量子ビットか、ノイズがどの程度あるか、何回演算ができるかという三点が重要な指標。量子ビットが 2000 から 4000 程度ないと計算自体ができない。ノイズが非常に大きくても、2000 から 4000 ぐらいの量子ビットを持つような量子コンピュータができ始めれば状況は変わる。様々な報道等においても、ノイズの多さは表面上に出てこず、何量子ビットのものがでたとか、何量子ビットのものを商用的に使い始めたという話はよく出てくるため、量子ビットがどの程度かという指標をウォッチすべき。

松井構成員：量子コンピュータはいつできるかわからない一方で、準備しておく必要もあるというのが本当のところではあるが、一般の方々に受け入れてもらえるようにその旨を伝えるのは難しい。ジャーナリスティックには量子コンピュータの登場によって暗号が危ないと騒がれがちだが、いつできるかわからないということと、準備をしておく必要があるということを、どのように社会の中でコンセンサスを得ていくかということを議論するのも、本タスクフォースの目的の一つ。

今の暗号は使い続けた上で、量子コンピュータに対しても準備をしておくという言葉の使い方をすべき。量子コンピュータによって世の中がどう変わっていくのかという議論があった上で、その先に暗号の危殆化という課題もあるという視点が必要。

松本泰構成員：2005 年の MD5 の危殆化のときも、現在に似たような状況だった。SHA-1 も危殆化のおそれがあるということで、SHA-3 が作られたが現在全く使われていない。PQC がそのようになる可能性もある。

資料２に「大規模システムの改修・更改には 10 年以上要する」と記載されているが、本質的に議論する必要があるのは、システムのライフサイクルではなくデータのライフサイクル。50 年間保存すべき暗号化データであれば、50 年間安全な暗号アルゴリズムや署名アルゴリズムが必要。実際はデータとシステムには相互依存関係があり、移行には非常に時間がかかる。暗号の移行を考える際、世の中の暗号化や署名がされたデータについて、どの程度の保存期間が必要かという議論を最初にすべき。2030 年にすぐに切りかわるものでは決してない。例えば、PKI のルート認証局は 20 年程度の有効期間、産業用の IoT 機器については 30 年の有効期間が望まれている。

実際にインプリメントされている楕円曲線暗号は 256 ビットや 384 ビットであるため、危殆化については RSA の 3072 ビットや楕円曲線暗号の 256 ビットを基準として考えるべき。

また、PQC の実装に関しては、軽量暗号と同様、アプリケーションオリ

エンテッドになり、応用によって実際のアルゴリズムを切りかえる可能性が高い。

満塩構成員：量子コンピュータのリソースには非連続性があり、いきなり飛躍的に伸びることがあると理解している。

また、現実的に量子コンピュータがいつ出てくるのかは全く見えていない。

國廣構成員：量子コンピュータを開発するに当たり、どのようなデバイスを使うべきか誰もわかっていないが、デバイスごとに量子ビット数や計算時間等の得意不得意があり、現在は様々な方向性で量子コンピュータを作っている状況。

例えば2048量子ビットを持つが何も計算できないというものや、大量に計算はできるが２量子ビットしかないといった、とがった特徴を持つものができた後で、両方の長所を併せ持つものができてくるのではないかと考えるが、それがいつ頃になるかはわからない。

松本勉座長：量子コンピュータの能力がどのように伸びていくかということについて、我々の知見を高めるためにはどうすれば良いかという議論が必要。

資料３の13ページは、量子誤りがないときに必要な量子ビット数についての見積もりだが、量子誤りがある場合には全く機能しないか。

國廣構成員：量子誤りがあると全く機能しない。ほんの少しの誤りがあっただけでも、10 の 11 乗回計算を繰り返してしまうため、ノイズだらけになってしまい、そもそも動かない。

松本勉座長：量子誤り訂正は、もともとの誤りが小さければ直せるか。

國廣構成員：しきい値以下の誤りであるならば、原理的には直せる。

松本勉座長：コヒーレンシーが保たれる時間というのがあって、壊れる前に計算が終わっていないと意味がないということか。

國廣構成員：然り。状態が壊れる前に計算をやり切るためには１回当たりの計算が数マイクロセカンド以内に終わらないといけない。誤り訂正をしない限りにおいては状態が崩れてしまって素因数分解はできない。どういう形でノイズが乗るかというのは状況によって変わり、量子の状態は完全に保たれているものの演算をする際に誤りが発生するというケースや、量子の状態が徐々に消えていってしまうケースなど、様々な崩れ方がある。崩れ方によって対処の難度が変わってくるので、誤りがどういう誤りなのかを把握する必要がある。

松本勉座長：ミリセカンドも行かないくらいの短い間に一気に計算する必要があるのが現状であり、将来的にもどうなるか不明。普通のスーパーコンピュータで何年もかけて計算しているのと比べると、何年も計算し続けられるも

のはできないのではないか。

量子コンピュータは難しい技術ではあるが、NISQ（ノイジー・インターメディエイト・スケール・クオンタム）であれば、使えるアプリケーションがあると期待されているか。

國廣構成員：量子化学の計算や金融関係では使えるのではないかと言われている。

松本勉座長：IBM やグーグル、インテルが現在開発している量子コンピュータを無理やり素因数分解をするようにプログラムすると、何ビットまでアタックできるか。

國廣構成員：ノイズの出方に統一性が無いために対処が難しく、かつノイズが大きいので、素因数分解できるところまで到達していないと聞いている。

國廣構成員：資料４の５ページ目に引用されている『Interface』2019 年３月号に掲載されているように、量子コンピュータの規模が直線的に伸びていくと予測している人もいる。実際に実現できているか否かという観点からは、例えば、2018 年に IBM が 50 ビットを実現させている。また、Rigetti は 2019 年に 128 ビットのものをつくると宣言している。近い将来について宣言しているところには、ある程度の確信を持って開発を進めているのだろう。ビット数だけではなく誤りも込みで考えなければ実際の性能は分からないため、ビット数だけを見るのは危険だが、どのようなノイズが乗るかという点までを含めた発表はされないため、将来を予測するのは難しい。

松本勉座長：『Interface』のグラフの「数千ビットの素因数分解（誤り訂正なし）」という線と「数千ビットの素因数分解（誤り訂正あり）」はそれぞれ何を意味するか。

國廣構成員：前者は、誤りのないコンピュータが仮にあった場合、10 の３乗から４乗の量子ビット数が必要であること、後者は、誤り訂正をした上で素因数分解しようとすると 10 の６乗必要だということを表している。

松本勉座長：高木構成員から説明のあった格子暗号等の耐量子計算機暗号は、ラージスケール・クオンタムに対して、現時点では耐えられるということか、今の量子コンピュータの原理であれば将来的にも耐えられるということか。

高木構成員：資料４の 21 ページのグラフの右上に３本の点線があるが、これは実際に解読するときのアルゴリズムの差異を表すもの。一番悪いと赤い点線のところで解けてしまう可能性がある。１目盛りが５倍から 10 倍ぐらい違うため、鍵長がかなり影響を及ぼす状況であり、このモデルに応じて、次元やノイズを上げないといけない。アカデミックの分野でも、ノイズのない大規模な量子コンピュータに対してどの程度安全かという標準的なモデルがまだ策定されていない。

松本勉座長：Shor のアルゴリズムや、その発展形のものを使ってアタックできるものではないか。

高木構成員：然り。Shor のアルゴリズムのような指数時間の多項式時間へのスピードアップは、素因数分解と離散対数問題とそれに関係する問題に対するものであり、NIST が検討しているような耐量子計算機暗号に対しては当てはまらないのではないかと議論されている。

松本勉座長：耐量子計算機暗号として格子暗号や誤り訂正符号ベースのもの、多変数多項式ベースのもの、同種写像ベースのもの等を使おうとすると、RSA 暗号や楕円曲線暗号と比べるとデータサイズが大きくなってしまう。仮に RSA 暗号や楕円曲線暗号と PQC の併用が難しいとした時に、例えば格子暗号を高機能暗号として活用するといったように、アプリケーション面からの開拓も必要。

また、松本泰構成員から、PKI や産業用 IoT 機器等に用いる公開鍵証明書や長期的な署名に対しては、現状でも 2048 ビットでは危険で、4096 ビット以上が求められるという指摘があった。そのような長い鍵長が求められる分野に対して、耐量子計算機暗号の積極的な使用を推奨することはできないか。

松井構成員：例えば格子暗号には、ポストクオンタムだけではなく、完全準同型暗号としての価値もある。公開鍵の歴史はどれだけアプリケーションが広がってきたかという歴史でもあり、アプリケーションが広がらない暗号は使われなくなっていく。

暗号で高機能なことができることが一番重要で、さらにクオンタムレジスタントでもあるから使い道があるというロジックが健全。現在は格子暗号等、様々な原理の暗号を研究している段階ではあるが、実際にどの暗号が使用されて残っていくかという視点も必要。

また、署名の鍵長に関しては、1 つの暗号アルゴリズムだけではなく、署名を重ねていくテクニックなど、様々な組合せを考えていく必要がある。

松本泰構成員：暗号の移行という観点からは、PQC が使えるかという暗号アルゴリズムだけの問題ではなく、移行するアーキテクチャーやその標準化についての議論も必要。

産業系 IoT 機器に関しては、数多くの IoT のセキュリティに関するガイドラインにおいて、ルート証明書のトラストの鍵はハードウェアや耐タンパー性のデバイスに入れることが推奨されていることもあって、多くの機器で暗号アルゴリズムはハードウェアに実装される方向になっており、PQC を実装するのは難しくなっている。スマートフォン等のスマー

トデバイスには暗号技術がしっかりと実装されており、その技術がこれから IoT 機器に流入していくが、スマートフォンよりもずっと長いライフサイクルを要求されており、暗号技術の実装には課題が多い。

宇根構成員：PQC を高機能暗号として活用するという方向性については賛同。最近では、金融分野において、暗号資産やキャッシュレス決済等に暗号を積極的に使っていくという動きがある。特に暗号資産は長期的に安全なものを実装していくことが前提となる。格子暗号等、NIST が現在選定を進めている暗号の中には、高機能暗号として使っていくことができるものもあり、そのような方式の暗号が選定されていくのではないか。

長い鍵が必要な場合については、クリプトアジリティやセキュリティアジリティをキーワードに、移行が必要になったときにより効率的かつタイムリーに移行していくためにはどうすればよいかを検討しているところ。システム交換のタイミングで、新しい暗号方式やデータ保護の機構に移しやすい設計を入れていくことが必要であり、鍵長を伸ばすというよりも、どうやってマイグレーションを効率的に行えるシステムにしていくのかという視点が重要。

高木構成員：一般的には、楕円曲線暗号は RSA 暗号に比べて鍵長が短いため、RSA 暗号より先に危殆化するといわれているが、実態を伺いたい。

國廣構成員：楕円離散対数問題に関しては、RSA 暗号も楕円曲線暗号も大きくは評価が変わらない。一方で、素因数分解に関しては、鍵長が短い楕円曲線暗号の方が早く危殆化するのは間違いない。

松本勉座長：楕円曲線暗号であっても、2048 ビットといったように、RSA 暗号と同じ鍵長であれば楕円曲線暗号の方が強いのではないか。

國廣構成員：然り。

満塩構成員：量子コンピュータを実装するデバイスとして様々なパターンがあるということであったが、実装はかなりの高額になるだろうから、装置全体の評価に際してはコストとの比較もパラメータ化したほうが良い。

また、世間では、量子ゲート型コンピュータではなく量子アニーリング型コンピュータで暗号を解くと誤解されているように、量子ゲート型コンピュータ、量子アニーリング型コンピュータ、量子通信、量子暗号の関係に混乱が見られるので、CRYPTREC として正確なところをレポートしてもよいのではないか。

高木構成員：NIST のセカンドラウンドには 26 方式通っているが、大学と企業と混成で通しているケースが非常に多い。特にセカンドラウンドでは、安全性はもちろんのこと、ソフトウェアだけではなくてハードウェアの性能も評価することになっている。

NIST が標準化する方式が決定した際、その方式は安全性の評価だけでなく、実装データも一通り揃っていることになる。提案に参加しているのはアメリカの大手 IT 企業が多いため、その企業がその方式をプロモートし始めると、日本が置いていかれかねないという危機感を抱いている。

松本勉座長：本日の議論では、新しい暗号を使っていく際、新しいアプリケーションに活用できるといった明るい面があったり、移行の仕組みをうまく作ったりしないと、なかなか移行しにくいのではないかという意見があった。

また、量子コンピュータで現在の素因数分解がどのぐらい危機にさらされているかという点について、直感的な理解が進んだ。

事務局（IPA）：資料４の 11 ページに関して、NIST SP 800-131A の Revision 2 では、2031 年以降は 128 ビット安全性の暗号を使用すべきと記載されている。128 ビット安全性の暗号が何かというのは、NIST SP 800-57 の Revision 4 に、RSA であれば 3072 ビット、楕円曲線暗号であれば 256 ビットと定義されている。さらにそれ以上の安全性を持つ暗号については、RSA であれば 7068 ビットや 15360 ビット、楕円曲線暗号だと 384 ビットや 512 ビットについて記載されている。

6.3. 閉会

経済産業省の三角審議官から閉会の挨拶が行われた。

また、事務局から次回は９月頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

以上

CRYPTREC
Cryptography Research and Evaluation Committees

資料2

耐量子計算機暗号の扱いについて

令和元年９月６日
CRYPTREC事務局

前回までの議論

■ 量子コンピュータ・耐量子計算機暗号の動向について。

- 耐量子計算機暗号の研究動向調査報告書（2019年3月）
  「RSA暗号に対する量子コンピュータを使用した場合の実際的な脅威が差し迫っているとは現時点では断言できない。」

- 2019年6月第一回TFにおける構成員ご発言
  「量子コンピュータはいつできるかわからない一方で、準備しておく必要もあるというというのが本当のところではある」
  「現実的に量子コンピュータがいつ出てくるのかは全く見えていない。」
  「ビット数だけではなく誤りも込みで考えなければ実際の性能は分からないため、ビット数だけを見るのは危険だが、どのようなノイズが乗るかという点までを含めた発表はされないため、将来を予測するのは難しい。」

論点

■ CRYPTREC暗号リストにおける耐量子計算機暗号の取扱いについて。

- 現時点において、量子コンピュータの性能がどう向上していくか十分な知見がない。諸外国においても、耐量子計算機暗号の標準化について議論が始まってはいるが結論は出ていない。
- 他方、CRYPTREC暗号リストは、安全性及び実装性能ともに優れた暗号技術を推奨するべく取りまとめたものであり、量子コンピュータがどのようなものになるかわからない以上、耐量子計算機暗号の性能について正しい評価を行うことは現時点においては困難である。
- 耐量子計算機暗号については、今般の改定においては、CRYPTREC暗号リストに含めるのではなく、ガイドライン等の別の文書として扱うこととしてはどうか。

  ※当該文書については、暗号リストと併せてリスト群として提示してはどうか。

論点

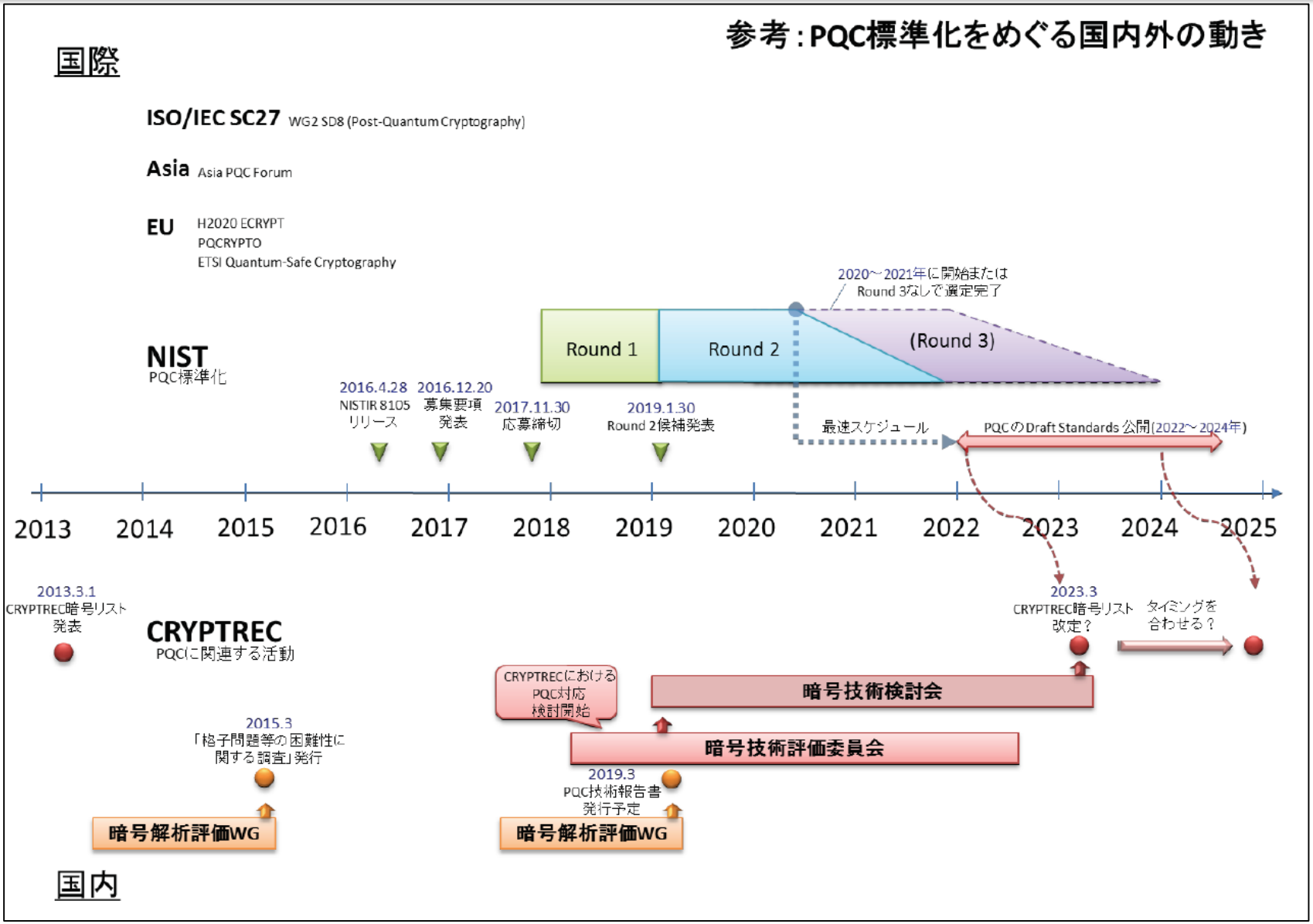
■ 我が国としての耐量子計算機暗号の在り方を踏まえた検討について。

- 米国（NIST）の耐量子計算機暗号の標準化は2022～2024年とされ、日本(NICT等)発の暗号方式はRound2に含まれていない。

- これから先、NISTが選定する暗号方式を中心にした議論が想定される中で、我が国における耐量子計算機暗号の開発・標準化はどのような方向を目指すのか。

- 今後、CRYPTREC暗号リストにおける耐量子計算機暗号の取扱いは、その方向性や開発・標準化スケジュールを踏まえて検討を行うべきではないか。

参考


参考：PQC標準化をめぐる国内外の動き
国際
ISO/IEC SC27 WG2 SD8 (Post-Quantum Cryptography)
Asia Asia PQC Forum
EU H2020 ECRYPT
PQCRYPTO
ETSI Quantum-Safe Cryptography
NIST
PQC標準化
2020～2021年に開始または
Round 3なしで選定完了
Round 1
Round 2
(Round 3)
2016.4.28
NISTIR 8105
リリース
2016.12.20
募集要項
発表
2017.11.30
応募締切
2019.1.30
Round 2候補発表
最速スケジュール
PQCのDraft Standards 公開(2022～2024年)
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2013.3.1
CRYPTREC暗号リスト
発表
CRYPTREC
PQCに関連する活動
2023.3
CRYPTREC暗号リスト
改定？
タイミングを
合わせる？
CRYPTRECにおける
PQC対応
検討開始
暗号技術検討会
暗号技術評価委員会
2015.3
「格子問題等の困難性に
関する調査」発行
2019.3
PQC技術報告書
発行予定
暗号解析評価WG
暗号解析評価WG
国内

資料3

軽量暗号の現状と動向

名古屋大学
岩田　哲

2019年9月6日

アジェンダ

- 軽量暗号
- 現状と動向
  - CRYPTREC
  - CAESAR
  - NIST
  - ISO/IEC
- まとめ

軽量暗号

- 小型デバイス向け暗号
  - RFIDタグ、センサノード、スマートカード、車載機器、医療機器等
  - PC向け、サーバ向け暗号技術が適さない環境
- 主な性能指標
  - 回路規模
  - 消費電力量
  - レイテンシ
  - メモリサイズ

軽量暗号の利用

- RFIDタグ：物流管理
- センサー：農業、防災
- 家電、スマートテレビ
- 医療分野
- 産業用システム
- 自動車
- 等々、利用分野は広がっている

軽量暗号の開発

- ブロック暗号
  - Present, Simon, Speck, Simeck, TWINE, Midori, Piccolo, LED, CLEFIA等
- ストリーム暗号
  - ChaCha20, Enocoro, Grain, MICKEY, Trivium等
- ハッシュ関数
  - Keccak, PHOTON, QUARK, SPONGENT等, NIST LWC応募方式
- メッセージ認証コード
  - SipHash, LightMAC等
- 認証暗号
  - ACORN, Ascon等, NIST LWC応募方式

Present概要

- CHES 2007
- Bogdanov, Knudsen, Leander, Paar, Poschmann, Robshaw, Seurin, Vikkelsoe
- 4ビットSboxとビット置換のみの線形層の繰り返し構造
  - ブロック長64ビット、31ラウンド、鍵長80, 128ビット
  - 設計者の推奨は80ビット鍵

CRYPTRECの取り組み

- CRYPTREC暗号技術ガイドライン
  - CRYPTREC軽量暗号ワーキンググループ、2017年3月
  - 目次
    - 軽量暗号とその活用法
    - 軽量暗号の性能比較（ブロック暗号、認証暗号）
      - ハードウェア実装
      - ソフトウェア実装
    - 代表的な軽量暗号
      - ブロック暗号、ストリーム暗号、ハッシュ関数、メッセージ認証コード、認証暗号

CRYPTREC暗号技術ガイドライン留意点

- 軽量暗号で達成可能な安全性
  - 従来技術よりも低い傾向
    - 64ビットブロック暗号
    - 2^{32}ブロック=32ギガバイト
  - 電子政府推奨暗号でもリスクなしの運用は困難であり、軽量暗号でも利用に応じたリスクを考慮する運用が必要

CAESAR

- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- 認証暗号のコンペティション、学術コミュニティ主導
- タイムライン
  - 2014年3月　応募締め切り　57方式
  - 2015年7月　第二ラウンド候補　30方式
  - 2016年8月　第三ラウンド候補　17方式
  - 2018年3月　ファイナリスト　8方式
  - 2019年2月　ポートフォリオ　6方式

CAESARポートフォリオ

- Use Case 1（Lightweight applications）
  - Ascon
  - ACORN
- Use Case 2（High-performance applications）
  - AEGIS-128
  - OCB
- Use Case 3（Defense in depth）
  - Deoxys-II
  - COLM

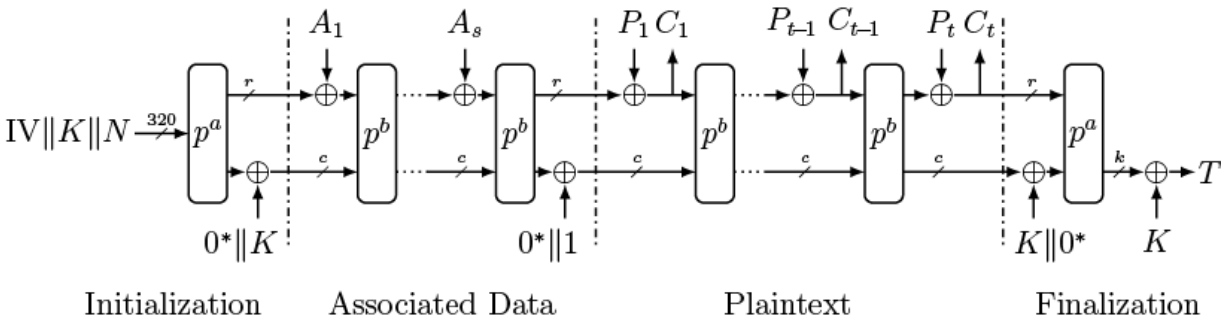
CAESAR Use Case 1

- Use Case 1: Lightweight applications (resource constrained environments)
  - critical: fits into small hardware area and/or small code for 8-bit CPUs
  - desirable: natural ability to protect against side-channel attacks
  - desirable: hardware performance, especially energy/bit
  - desirable: speed on 8-bit CPUs
  - message sizes: usually short (can be under 16 bytes), sometimes longer

Bernstein, CAESAR use cases, CAESAR mailing list, July 17, 2016より引用

CAESAR Use Case 1ポートフォリオ

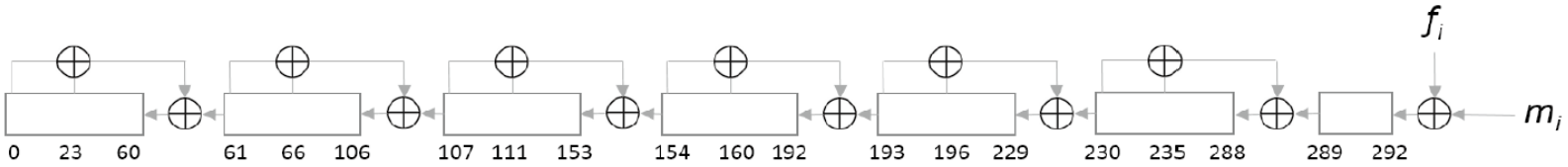
- Ascon
  - Dobraunig, Eichlseder, Mendel, Schläffer



Ascon v1.2 Submission to the CAESAR Competition, Dobraunig, Eichlseder, Mendel, Schläffer, https://competitions.cr.yp.to/round3/asconv12.pdf より転載

CAESAR Use Case 1ポートフォリオ

- ACORN
  - Hongjun Wu



ACORN: A Lightweight Authenticated Cipher (v3), Hongjun Wu
https://competitions.cr.yp.to/round3/acornv3.pdf, Fig. 1.1より転載

NIST軽量暗号標準化プロジェクト

- 軽量暗号の標準化プロジェクト
- 認証暗号とハッシュ関数
  - ハッシュ関数はオプション
- タイムライン
  - 2から4年のプロジェクト
  - 2019年2月　応募締め切り　57方式
    - 第一ラウンド候補56方式
  - 2019年8月　第二ラウンド候補　32方式
    - 第二ランドはおおよそ1年間の予定

NIST軽量暗号標準化プロジェクト応募要項

- Minimum Acceptability Requirements
- AEAD
  - Nonceの利用
  - 鍵長は最低128ビット
  - 攻撃に必要な計算量は2^{112}以上（古典計算機、単一鍵設定）
  - Primary memberは鍵長が128ビット以上、nonce長96ビット以上、タグ長64ビット以上、入力（平文、associated data）サイズの制限（一つの鍵で処理できるデータ量）は2^{50}-1バイトを下回ってはならない

NIST軽量暗号標準化プロジェクト応募要項

- Minimum Acceptability Requirements
- ハッシュ関数
  - 攻撃（Collision, (Second-)Preimage）に必要な計算量は2^{112}以上（古典計算機）、ハッシュ長は256ビット以上
  - Primary memberは入力サイズの制限が2^{50}-1バイトを下回ってはならず、出力長は256ビット以上でなければならない

NIST軽量暗号標準化プロジェクト応募要項

- Design Requirements
  - 現在のNIST標準よりも“should perform significantly better in constrained environments (hardware and embedded software platforms)”
  - 短い入力に対する計算効率（8バイトなど）
  - ハードウェア、組み込みソフトウェアでの小型実装性能（ROM/RAM）
  - low energy/low power/low latency実装への柔軟な対応
  - マイクロコントローラ実装での効率
  - 効率的な事前計算（鍵の処理など）
  - timing attack/SPA/DPA/SEMA/DEMAを含むサイドチャネル攻撃に対する耐性

NIST軽量暗号標準化プロジェクト応募要項

- 入力サイズ、安全性（サイドチャネル攻撃を含む）、実装性能に対する非常に高い要求
  - 2^{50}-1バイト=1ペタ-1バイト
  - 関連鍵攻撃
  - multi-user/multi-key setting

NIST軽量暗号標準化プロジェクト第二ラウンド候補方式

ACE	ASCON	COMET	DryGASCON
Elephant	ESTATE	ForkAE	GIFT-COFB
Gimli	Grain-128AEAD	HYENA	ISAP
KNOT	LOTUS-AEAD & LOCUS-AEAD	mixFeed	ORANGE
Oribatida	PHOTON-Beetle	Pyjamask	Romulus
SAEAES	Saturnin	SKINNY-AEAD/-HASH	SPARKLE (SCHWAEMM and ESCH)
SPIX	SpoC	Spook	Subterranean 2.0
SUNDAE-GIFT	TinyJambu	WAGE	Xoodyak

[lwc-forum] NIST Lightweight Cryptography Project - Second-round candidates (2018年8月31日、メーリングリスト)より引用

ISO/IECにおける状況

- ISO/IEC 29192
  - 軽量暗号
  - Present, CLEFIA, Enocoro, Trivium, PHOTON, SPONGENT
- ISO/IEC 29167
  - RFID用技術
  - Grain v1/-128A

まとめ

- 軽量暗号に関する現状と動向
  - CRYPTRECの取り組み
  - CAESAR
  - NIST標準化プロジェクト
  - ISO/IEC

- NIST LWC
  - 時期：2021年から2023年ころの予定
  - 認証暗号とハッシュ関数のみ
    - ブロック暗号、ストリーム暗号、暗号化モード、MAC
  - 応募要項は高いレベルの安全性を要求
- 非常にアクティブな研究分野で、継続的な注視が必要

CRYPTREC
Cryptography Research and Evaluation Committees

資料4

軽量暗号等の扱いについて

令和元年９月６日
CRYPTREC事務局

論点

■ CRYPTREC暗号リストにおける軽量暗号の取扱いについて。

- 軽量暗号は、IoT機器等のリソースの限られたデバイスにも実装可能な暗号として、性能と安全性のトレードオフ等により様々な指標で最適化された方式が存在する。
- 一方、CRYPTREC暗号リストは、安全性及び実装性能ともに優れた暗号技術を推奨するべく取りまとめたものであり、安全性を一部トレードオフした軽量暗号は上述の趣旨にそぐわないのではないか。

→　軽量暗号については、CRYPTREC暗号リストに含めるのではなく、ガイドライン等の別の文書として扱うことが適当ではないか。
　他方、今後IoT機器の政府調達も増えていくことが予想されるところ、2017年3月に発行したCRYPTREC 暗号技術ガイドライン(軽量暗号)について、今後必要に応じて更新等を行い、積極的に活用してはどうか。

論点

■ CRYPTREC暗号リストにおける高機能暗号の取扱いについて。

- 高機能暗号は、CRYPTREC暗号リストに記載されている従来の暗号アルゴリズムでは実現ができなかった付加機能を提供することができる。
- ただし、暗号の利用目的や用途に応じて必要となる暗号強度／付加機能が異なることから、高機能暗号を利用する際には、暗号の安全性だけでなく、当該暗号アルゴリズムがどのような付加機能を提供するのかまでをセットで考慮する必要がある。これは、CRYPTREC暗号リストの技術分類の考え方と合致しないのではないか。

→　高機能暗号については、CRYPTREC暗号リストに含めるのではなく、ガイドライン等の別の文書として扱うことが適当ではないか。
　また、ガイドラインを作るのであれば、軽量暗号と同様、積極的に活用してはどうか。