3-2　QKD を用いた情報理論的安全なパスワード認証分散ストレージ

藤原幹生　早稲田篤志　野島　良　盛合志帆　尾形わかは　佐々木雅英

分散ストレージは長期にデータを安全に保存する場合に必須である。分散ストレージは秘密のデータを有するデータオーナーのサーバ、複数のストレージサーバ及びそれらを結ぶ通信リンクで構成されている。分散ストレージでは“秘密分散”と呼ばれ、データを“シェア”と呼ばれるデータに分割し、ストレージサーバに保存する手法が広く用いられている。データを復元するためにはデータオーナーは複数のシェアを集める必要がある。シャミアの (k,n) 閾値秘密分散法ではデータを n 個のシェアに分割し、データ復元には k 個以上のシェアを収集する必要がある。仮にシェアの情報が k-1 個盗聴者に漏洩し、盗聴者が無限の計算能力を持っていたとしても一切データの秘匿性は脅かされることはなく、情報理論的安全性が保たれる。このスキームでは伝送と認証については安全に行われることが前提となっているが、実際のシステムでは伝送・認証をも情報理論的安全性を保つ必要がある。我々は認証時には 1 つのパスワードだけで情報理論的に安全に実施でき、データ伝送には情報理論的安全な鍵生成が可能な量子鍵配送 (quantum key distribution: QKD) のネットワークを用い、情報理論的安全な認証・伝送・保存・復元をユーザフレンドリーなシステムの実証に成功した。

1　まえがき

ゲノムデータなど、世代を超え 100 年単位の秘匿性を必要とする情報が製薬や医療などで利用されており、その通信時の秘匿性を担保するために暗号技術開発の確立が急務となっている。その一方で我々が日頃使用している素因数分解や離散対数の計算困難さを基本とした暗号方式では、量子コンピュータ [1] が完成した暁に危殆化するとの懸念があることに加え、年々増強される計算機能力のため、30 年後も安全であると担保できていないのが現状である。他の暗号方式では、耐量子計算機暗号の最有力な方式として格子暗号 [2][3] 等が提案されているが、それらの性能評価は 2020-2022 年に NIST (米国の国立標準技術研究所：National Institute of Standards and Technology) で行われる予定 [4] であり、現在我々が既に直面している安全性への回答は数年以上待たなければならない状況である。加えて、暗号方式の変化は暗号化に必要な公開密鍵の鍵長の変化が伴う可能性が高く、現在の通信プロトコルのまま使用できない恐れがある。つまり通信機器の OSI モデルの各層での通信プロトコルの改変は、通信装置の大幅な更新を必要とする場合があり得る。それに対し、現在の通信システムに専用線を用いたシステムを付加することにより、将来の情報漏洩の脅威からの解放を実現できる方法として、二者間での情報理論的に安全に乱数を共有できる量子鍵配送 [5][6] と Vernam’s one-time pad 暗号の組合せが挙げられる。本方式では将来の盗聴の脅威から完全に解放される。量子鍵配送は 2000 年当初より敷設ファイバでの伝送実験 [6] が開始され、現在では GHz のクロックを有する高速量子鍵配送装置 [7][8] が開発されている。また、世界各国で量子鍵配送のネットワーク運用も進んでいる [9]–[11]。量子鍵配送は、伝送時の安全性は担保できるが、データの保存に関してはソリューションを与えていない。一方、現代暗号の分野では情報理論的に安全なデータ保存方法としてシャミアの閾値秘密分散法 [12] が知られていたが、この方式ではシェアと呼ばれる秘密データの復元に必要なデータの伝送の安全性に対しては“想定”するのみであった。言い換えると量子鍵配送と秘密分散の融合はお互いの欠点を補いあう極めて合理的な発展である。

NICT と東京工業大学は量子鍵配送と秘密分散の融合の上にユーザフレンドリーかつヒューマンエラーが起きにくいシステムとして、1 つのパスワードで情報理論的に安全に認証のできるプロトコルも開発し、2016 年には世界で初めて認証・伝送・保存・復元を情報理論的に安全に行うシステムのデモに成功した [13]。本稿ではそのプロトコルとシステムについて解説する。

2　情報理論的安全な単一パスワード秘密分散プロトコル

2.1　シャミアの (k,n) 閾値分散法

本節では我々のスキームの基本であるシャミアの

(k,n) 閾値分散法 [12] を説明する。(k,n) 閾値秘密分散法では、最初に、秘密データ S (整数) のデータオーナーが S から n 個のシェアと呼ばれる値を生成する。次に、データオーナーは、シェアサーバ (1 ～ n) に各シェアを秘密裏に渡す。データオーナーは、この後、秘密データを消去する。秘密データの復元には、k 台シェアサーバが協力して k 個のシェアを収集し、所定の計算をすることにより、秘密データ S を復元できる。このとき k を閾値と定義する。数式での記述は、以下のようになる。

分散：定数項を秘密データ S とするランダムな k-1 次多項式

$$f(x)=a_{k-1}x^{k-1}+....+a_1x+a_0 \qquad (1)$$

を生成する。ここで、$a_{k-1},....a_1,a_0$ はランダムな整数であり、a_0 が秘密データ S である。

シェア保有者の識別子を i としたとき、シェア保有者にはシェアとして $(i,f(i))$ を配布する。

復元時、k 台のシェアサーバが $(i,f(i))$ を持ち寄ることにより、$a_0=S$ を求める。

秘密データ S の復元は、下記の式に従って行う。復元に協力する k 人のシェアサーバの識別子を $\{i_1,...i_k\}$ とする。このとき、各シェアサーバの保有するシェアについて、

$$\begin{aligned} f(i_1)&=a_{k-1}i_1^{k-1}+....+a_1i_1+a_0 \\ &\vdots \\ f(i_k)&=a_{k-1}i_k^{k-1}+....+a_1i_k+a_0 \end{aligned} \qquad (2)$$

が成り立つ。ここで、$(i_1,f(i_1)),\cdots,(i_k,f(i_k))$ が与えられれば、未知変数を $a_{k-1},....a_1,a_0$ の k 個とする k 変数 1 次方程式が k 個与えられる。したがって、この連立方程式より、すべての未知変数を求めることが可能であり、秘密データ S を復元できる。

実際に秘密情報を復元する際には、ラグランジュ補間が利用される。

図 1 には、閾値分散法 (3,4) の例を示している。2 次方程式中の 3 つの変数を確定するために、3 組以上の $(i,f(i))$ があれば、秘密データ S を復元できる。

2.2　パスワード秘密分散プロトコル

シェアの状態から秘密データの情報が漏洩することはないという特徴のほかに、シェアはシェア同士で足し算、掛け算が可能であるという特徴を有している。例えばデータ $D^{(1)}$ と $D^{(2)}$ の和のシェアは $f_{D^{(1)}}(a_i)+f_{D^{(2)}}(a_i)$ となる。同様に $D^{(1)}\times D^{(2)}$ のシェアは $f_{D^{(1)}}(a_i)\times f_{D^{(2)}}(a_i)$ となる。ここで留意点としては、シェアの足し算の際には閾値が変化しないことに対し、$f_{D^{(1)}}(x)\times f_{D^{(2)}}(x)$

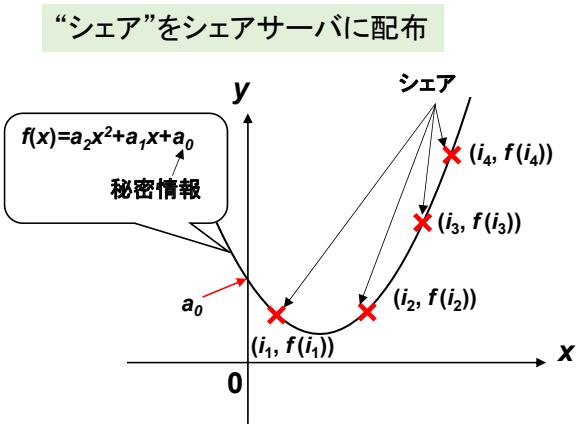


図 1　シャミアの閾値分散法 (3,4) の例

の多項式の次元は $2k-2$ となり、データの復元には $2k-1$ 個のシェアが必要となる。我々が実装したパスワード分散はこの性質を大いに利用し、情報理論的安全な認証を 1 つのパスワードで可能なスキームとなっている。スキームは 3 段階に大別される。最初に秘密データとパスワードのシェアを伝送するレジストレーションフェーズ、データ復元時の秘匿性を担保するためのシェアの計算を行うサーバ間通信・計算フェーズ、最後にデータ復元フェーズとなる。以下に閾値 (3,4) の例を挙げて詳細を記述する。

(1) レジストレーションフェーズ (registration phase)

(1 − 1) 計算機での演算に適したメルセンヌ素数 $q=2^m-1$ を用い、秘密データを $(m-1)$ ビット単位の l 個のブロック $D=D_l|D_{l-1}|\cdots|D_1$ に分割する。さらにパスワード P を用いてメッセージ認証コード (MAC) を $MAC=D_lP^l+D_{l-1}P^{l-1}+\cdots+D_1P$ と計算し、データに D_{l+1} として連接する。以下の方法で作成する。

(1 − 2) 其々のデータブロックに対して 1 ～ 4 のシェアサーバに伝送するシェア $f_{D_i}(1)$，$f_{D_i}(2)$，$f_{D_i}(3)$，$f_{D_i}(4)$ ($i=1,\ldots,l+1$) を作成する。その際多項式の次元は 2 である。さらにパスワード P に対しても 1 次元の多項式を用いてシェア $f_P(1)$，$f_P(2)$，$f_P(3)$，$f_P(4)$ を作成する。

(1 − 3) シェアをシェアサーバに QKD リンクからの鍵を用いた OTP 暗号化し伝送する。以下、サーバ間の通信は全て QKD + OTP での暗号化を用いる。

(1 − 4) 各シェアサーバはシェアを格納する。

(2) サーバ間通信・計算フェーズ (pre-computation phase)

(2 − 1) 其々のサーバ (j-th) で乱数 R_j を生成し、その乱数のシェア $f_{Rj}(1),f_{Rj}(2),f_{Rj}(3),f_{Rj}(4)$ を 1 次の多項式で生成する。さらにデータ“0”のシェア

$f_{0j}(1), f_{0j}(2), f_{0j}(3), f_{0j}(4)$ を 2 次の多項式を用いて生成する。それら乱数と “0” のシェアをシェアサーバに伝送する。

(3) データ復元フェーズ（reconstruction phase）

ここでデータオーナーはパスワードを思い出し、それを P' とする。

(3 − 1) データオーナーは 4 つあるシェアサーバの中から 3 つを選択する。例としてサーバ 1 ～ 3 (L= {1, 2, 3}) を選択したとする。

(3 − 2) データオーナーはパスワード P' に対しシェア $f_{P'}(1)$ ， $f_{P'}(2)$ ， $f_{P'}(3)$ を 1 次の多項式を用いて生成する。

(3 − 3) 各シェアサーバに $f_{P'}(j)$ を送る。

(3 − 4) データオーナーのサーバでは、データ復元に用いるシェアサーバの数が 3 以外であれば、その要求は不適切と判断し停止する。3 であれば各シェアサーバは $l+1$ 個のデータブロックに対して $= f_{R1}(j) + f_{R2}(j) + f_{R3}(j)$, $Z = f_{01}(j) + f_{02}(j) + f_{03}(j)$ を計算し、

$$F_{ji} = \left(f_P(j) - f_{P'}(j)\right)R + Z + f_{D_i}(j) \qquad (3)$$

(F_{ji} （ $i = 1, \ldots, l+1$ ）) をデータオーナーのサーバに送る。

(3 − 5) データオーナーはラグランジュ補間法で $F_i(j) = F_{ji}$ を求め、$F_i(0)$ のデータブロックを求める。

(3 − 6) データオーナーは $F_1(0), \ldots, F_l(0)$ から MAC を計算し、その結果が $F_{l+1}(0)$ と一致していれば秘密データの復元に成功したと判断する。そうでない場合は何らかの詐称がされたと判断し、先の組合せとは異なるシェアサーバの組合せで秘密データ復元を試みる。

上記の手順において、仮に $P' \neq P$ であったならば、秘密データは f_{Rj} と f_{0j} によりマスクされ、一切の情報が漏れることはない。このように、伝送・保存・認証・復元が情報理論的に実現できる。図 2 にプロトコルの概要を示す。

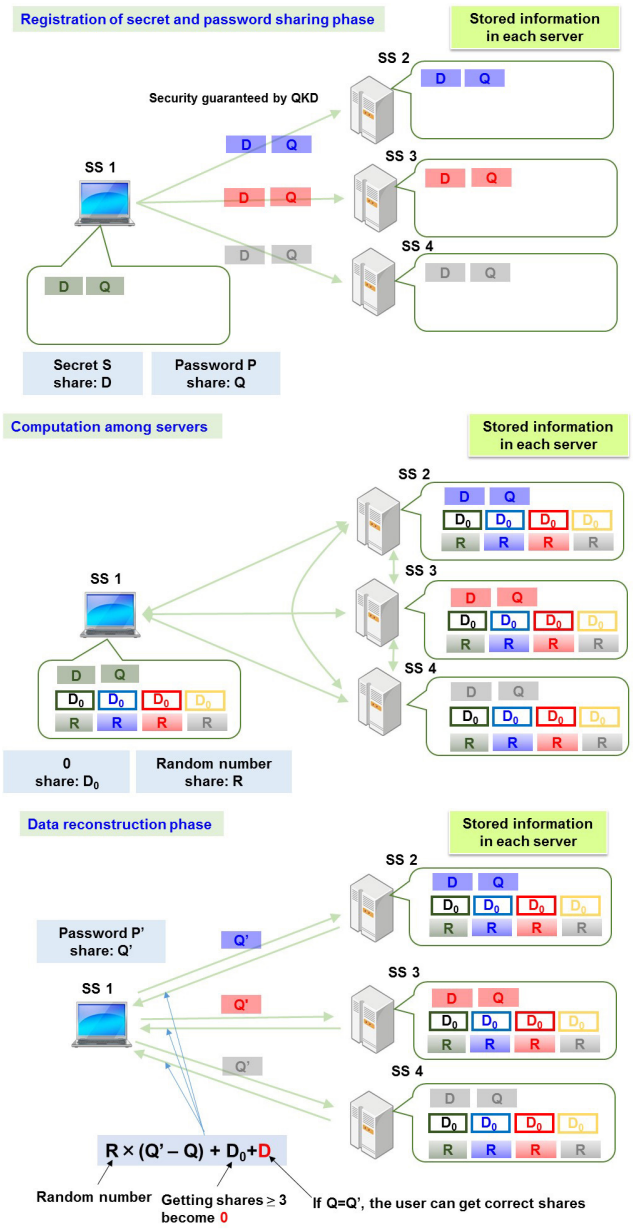


図 2　パスワード秘密分散プロトコル概略

3　QKD ネットワーク上での実証

我々のスキームを実現するのには QKD リンク及びそれらをネットワーク化した通信ネットワークが必須である。NICT では 2010 年より JGN [14] 等の協力を頂きながら NICT 本部（小金井）を中心とする Tokyo QKD Network [14] を運用してきた。我が国の QKD 装置の性能は世界最高性能を有するが、それでも信号の通信媒体が光子一つひとつであるため、伝送路の損失の影響を受けやすく、伝送距離・速度はファイバ 50 km で 1 Mbps 程度である [7][8]。QKD のサービス範囲を広げるため、複数の QKD リンクを連結し、連結部分（ノードと定義）では鍵情報を通常のビットストリームとして保存している。このノードは厳格に安全性が保たれ、外部からこのビット情報を盗むことができないと仮定しているため “信頼できるノード (trusted node)” と定義している。鍵配送の伸長が必要な場合は、ノードに蓄積されている異なる QKD リンクの鍵を、排他的論理和を施しながらリレーすることにより実現している。このような QKD ネットワークを運用するには厳格な鍵管理を可能とするネットワークアーキテクチャが必要である。NICT では 2010 年から、QKD ネットワークアーキテクチャの開発 [11][15] と QKD の鍵を利用した通信アプリケーション [16] の開発を進めている。我々の提案するネット

ワークアーキテクチャは OSI モデルを参考に 3 層構造から構成されている。量子レイヤと呼ぶ層には各 QKD リンクが該当する。鍵管理レイヤでは各 QKD 装置で生成された鍵を決められたフォーマットに変換し、QKD リンク同士のリレーを可能とし、様々なアプリケーションに安全な鍵を提供する。鍵管理レイヤの上にはアプリケーションレイヤが定義されており、情報理論的に安全な鍵を用いた様々な通信アプリケーションが開発されている。量子レイヤと鍵管理レイヤを合わせて QKD プラットフォームと定義している（図 3）。以下に鍵管理レイヤを構成の詳細を述べる。

各“信頼できるノード”には 1 つの鍵管理エージェント（key management agent: KMA）が設置され、各 QKD リンクからの鍵の収集と管理を行っている。KMA 同士は認証付き公開通信路で結ばれており、鍵リレーを行う。鍵リレー時には鍵が生成された際に付加される鍵 ID などの情報も伝送される。

QKD プラットフォームには 1 台の鍵管理サーバ（key management server: KMS）が設定され、信頼できるノード内に設置される。KMS は各 QKD リンクのエラーレート、鍵生成レート、蓄積鍵量などの情報を KMA より収集する。鍵残量・鍵生成レートから鍵リレーのルート決定、さらに鍵残量の減少やインシデント発生時のルート変更の指示を行う。さらには KMA に蓄積された鍵のライフサイクルを監視し、生成されてからの期間が一定以上経過した鍵は消去するよう KMA に指示を出す。

QKD プラットフォームからアプリケーションレイヤに鍵を渡すインターフェースとして鍵供給エージェント（key supply agent: KSA）が各ノードに 1 台設置されている。KSA はアプリケーションに応じた鍵フォーマットで鍵を供給し、同時に鍵 ID、アプリケーションの種類及び日付を記録し、それらの情報を KMS に伝達する。

QKD プラットフォームの概念で最も重要である点の 1 つに QKD プラットフォームとアプリケーションレイヤとの責任分界点が、この境界に設定されている点が挙げられる。アプリケーションレイヤと QKD プラットフォームとの情報のやり取り内容は極めて限定的であり、アプリケーション層からは QKD プラットフォームから受ける鍵以外の情報は一切アクセスできない。また、QKD プラットフォームからも、どの様なコンテンツがアプリケーションで扱われるかなどの情報には一切アクセスできない。それぞれの機器への

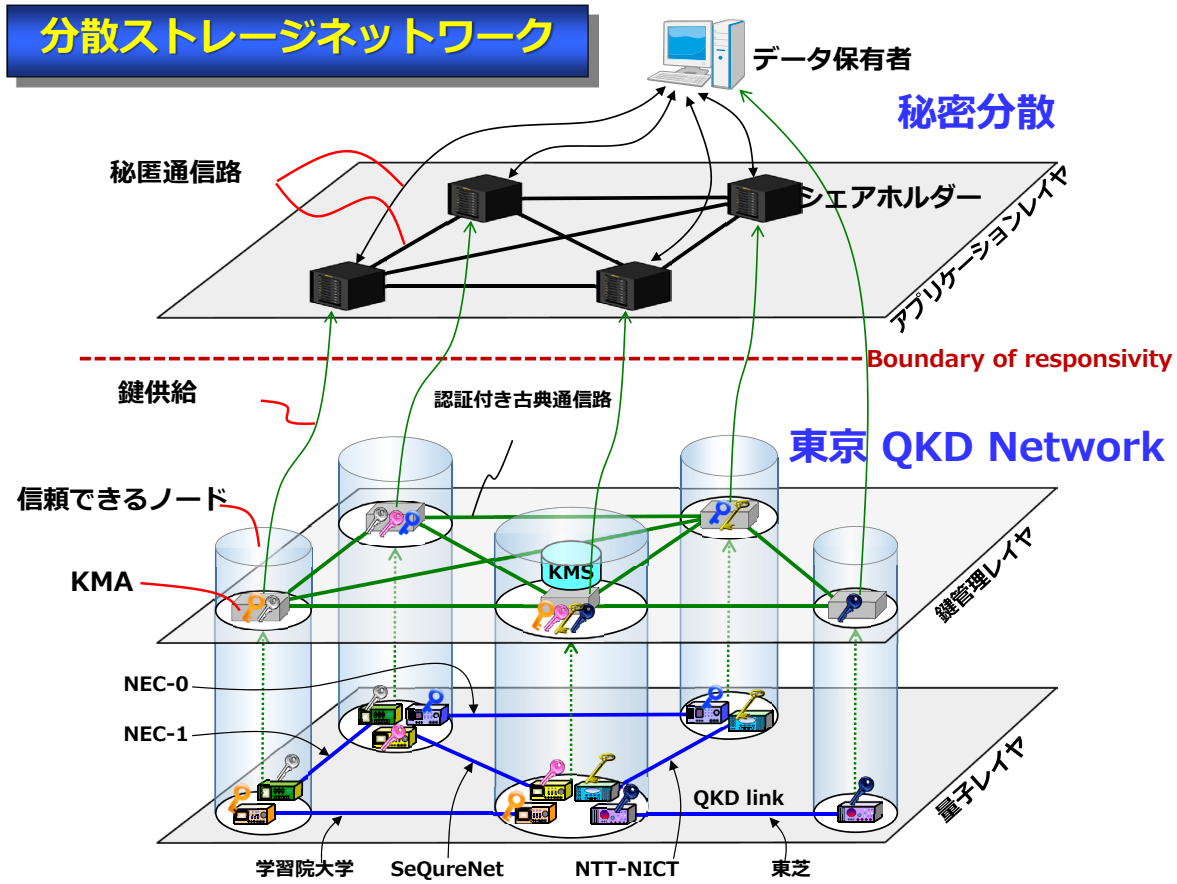


図 3　Tokyo QKD Network 上に形成した QKD プラットフォームと分散ストレージネットワークイメージ

表 1　Tokyo QKD Network の QKD リンクプロトコル及び伝送距離・損失

	Protocol	Transmission	
		Length（km）	Loss（dB）
NEC-0	BB84 with decoy	50（Spooled fiber NICT premise）	10
NEC-1	BB84 with decoy	22（field installed 95 % areal line）	13
Toshiba	BB84 with decoy	45（field installed 50 % areal line）	14.5
NTT-NICT	DPS-QKD	90（field installed 50 % areal line）	28.6
Gakushuin	CV-QKD	2（NICT premise）	2
SeQureNet	CV-QKD	2（NICT premise）	2

アクセス時の権限分離を厳密に設定することにより、ネットワークセキュリティ上の基本的安全性対策が施されている。

Tokyo QKD Network を形成している QKD リンクは NEC [7]、東芝 [8]、学習院大学 [17]、NTT-NICT [18]、SeQureNet [19] が担当している。NTT-NICT のリンクは小金井 – 大手町を結ぶ JGN [14] のダークファイバを利用している。各装置の詳細は他章に譲り、表 1 に各 QKD リンクのプロトコルと伝送距離・伝送損失をまとめる。

我々はこの分散ストレージ上で、認証･伝送･保存･復元を情報理論的に安全に実施可能なシステムを構築した。図 4 には秘密分散実行時の 3 フェーズ（registration pre-computation reconstruction）のプロセス時間　(a) データサイズ 46 kbyte の場合のメルセンヌ素数のインデックスサイズ依存性 (b) メルセンヌ素数 $2^{44497}-1$ を用いたい場合のファイルサイズ依存性を示す。

図 4 で得られている結果は計算機には通常の PC を使用しており、実際のストレージシステムで用いられている高性能サーバを用いれば当然その処理速度は飛躍的に改善される。一方で現行のシステムの処理速度を決めている最大要因は QKD プラットフォームから得た鍵を用いた OTP 暗号化の際に必須である鍵同期、言い換えるとサーバ内での鍵のソーティング処理が挙げられる。今後のソフトウェアの改良により、より高速処理が可能と予想される。現行のシステムでもメール伝送にも通常利用されている 10 Mbyte のデータをレジストレーションから復元まで 2 分程度で処理が完了できることを実証し、世界で初めて認証・伝送・保存・復元を情報理論的安全なシステム上でのデモンストレーションに成功した。

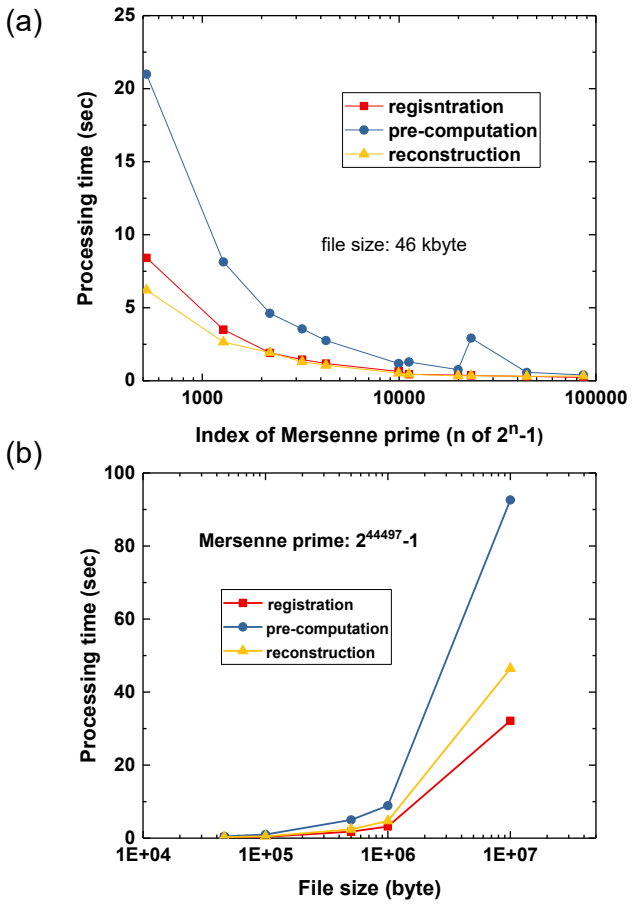


図 4　秘密分散実行時の 3 フェーズ (registration pre-computation reconstruction) のプロセス時間　(a) データサイズ 46 kbyte の場合のプロセス時間のメルセンヌ素数のインデックスサイズ依存性 (b) メルセンヌ素数 $2^{44497}-1$ を用いたい場合のプロセス時間のファイルサイズ依存性

4　まとめ

我々は認証時には 1 つのパスワードだけで情報理論的に安全に実施でき、データ伝送には情報理論的安全な鍵生成が可能な QKD のネットワークを用い情報理論的安全な認証・伝送・保存・復元をユーザフレンドリーなシステムの実証に成功した。今後、サーバに保存されているシェアを定期的に更新し、長期のデータストレージの際にも、長期保存による情報漏洩を防止する機能を付加することにより、超長期に安全なデータの秘匿保存を可能とするシステムを構築する。

今後、新たに様々な暗号・ネットワークシステムが

運用されることになっても、情報理論的安全性を担保できない物であれば、それには必ず盗聴・解読の危険が伴う。今回我々が開発したシステムは原理的に解読不可能なシステムであり、近未来に予想される攻撃に対しても極めて頑健なシステムであると言える。将来新たな暗号解読に対する脅威が発生しても、安全なシステムとしてのソリューションとしてNICTが即座に我が国の国民に提供できる。我々はこの技術を将来の脅威に備え、絶えず高度化し続ける必要があると考える。

また、本システムでは秘密分散の特徴である秘密計算を利用している。この秘密計算を利用することにより、データに記載されているプライバシーを堅牢に守りながら、統計データを計算するなど今後クラウドサービスにも適用が期待できる。このような高機能化を推し進めることにより、情報通信の安心安全を提供するというNICTの本分を全うしていく決意である。

謝辞

本研究開発の一部は総合科学技術・イノベーション会議により制度設計された革新的研究開発推進プログラム（ImPACT）の支援を受けて実施された。ImPACT「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現　量子セキュアネットワーク」参画機関の方々との有意義な意見交等ご支援いただいたことに感謝いたします。

【参考文献】

1 P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” Proceeding of the 35 th Annual Symposimu on Fundations of Computer Science, pp.12–134 (IEEE Computer Society Press, Los Alamitos, 1994).
2 J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A Ring based Public Key Cryptosystem,” ANTS- III Proceedings of the Third International Symposium on Algorithmic Number Theory, pp.267–288 (ANTS-III, London, 1998).
3 O. Goldreich, S. Goldwasser, and S. Halevi, “Public- Key Cryptosystems from Lattice Reduction Problems,” Proceeding of CRYPTO 1997 pp.112–131 (Springer, Heidelberg, 1997).
4 http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf
5 C. H. Bennett and G. Brassard, “Quantum cryptography: public-key distribution and coin tossing,” in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, New York, 1984), pp.175–179
6 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74 (1), pp.145–195 (2002)
7 K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, “Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days,” Opt. Express 21 (25), pp.31395–31401 (2013).
8 J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, “Stability of high bit rate quantum key distribution on installed fiber,” Opt. Express. 20(15), pp.16339–16347 (2012).
9 D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, “Long-term performance of the SwissQuantum quantum key distribution network in a field environment,” New J. Phys. 13 (12), 123001, 1-18 (2011).
10 M. Peev, C. Pacher, R. Alleaume, C. Barreiro, W. Boxleitner, J. Bouda, R.Tualle-Brouri, E. Diamanti, M. Dianati, T. Debuisschert, J. F. Dynes, S.Fasel, S. Fossier, M. Fuerst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentchel, H. Hübel, G. Humer, T. Länger, M.Legre, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, E. Querasser, G. Ribordy, A. Poppe, L. Salvail, S. Robyr, M. Suda, A. W. Sharpe, A. J. Shields, D. Stucki, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in Vienna,” New J. Phys. 11(7), 075001/1-37 (2009).
11 M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the Tokyo QKD Network,” Opt. Express, 19(11), pp.10387–10409 (2011).
12 A. Shamir, “How to share a secret,” Communications of the ACM, 22, pp.612–613 (1979).
13 M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki, “Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing,” Sci. Reports, 6, 28988-1-8 (2016).
14 http://www.jgn.nict.go.jp/
15 M. Sasaki, M. Fujiwara, R-B. Jin, M. Takeoka, T. S. Han, H. Endo, K. Yoshino, T. Ochi, S. Asami, and A. Tajima, “Quantum Photonic Network: Concept, Basic Tools, and Future Issues,” J. Selected Topics in Quant. Elec., 21, 6400313 (2015).
16 M. Fujiwara, T. Domeki, S. Moriai, and M. Sasaki, “Highly secure network switches with quantum key distribution systems,” Int. J. Network security 17, pp.34–39 (2015).
17 T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, “Quantum cryptography using pulsed homodyne detection,” Phys. Rev. A68, 042331 (2003).
18 K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, “Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area,” IEEE J. Lightwave tech. 32, pp.141–151 (2014).
19 http://www.sequrenet.com/datasheets/datasheet_cygnus.pdf

藤原幹生　（ふじわら　みきお）
未来ICT研究所
量子ICT先端開発センター
研究マネージャー
博士（理学）
量子鍵配送、光子検出技術、極低温エレクトロニクス

早稲田篤志　（わせだ　あつし）

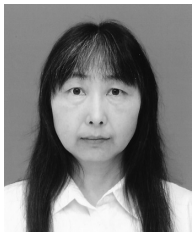
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
情報セキュリティ

野島　良　（のじま　りょう）

サイバーセキュリティ研究所
セキュリティ基盤研究室
研究マネージャー
博士（工学）
暗号理論、暗号プロトコル、情報セキュリティ
プライバシー、セキュリティ

盛合志帆　（もりあい　しほ）

サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士（工学）
暗号技術、セキュリティ評価、プライバシー
保護技術



尾形わかは　（おがた　わかは）

東京工業大学工学院
教授
博士（工学）
暗号理論、公開鍵暗号、署名、暗号プロトコル

佐々木雅英　（ささき　まさひで）

未来 ICT 研究所
主管研究員
理学博士
量子通信、量子暗号