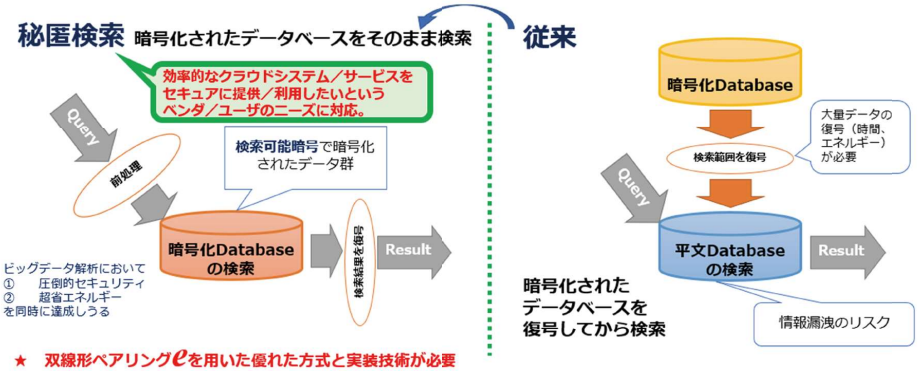
Sensor-to-Cloud Security
–ビッグデータを守る革新的IoTセキュリティ基盤技術の研究開発

委託先 | 横浜国立大学、三菱電機株式会社、東京大学、東北大学、神戸大学、国立研究開発法人産業技術総合研究所、電子商取引安全技術研究組合

主な課題：大規模データを扱うペアリング暗号実装の１０,０００倍の性能向上
主な成果：目標を上回る圧倒的な高速化・省エネ化



★ 双線形ペアリングeを用いた優れた方式と実装技術が必要

楕円曲線群 楕円曲線群 有限体

$$e: G_1 \times G_2 \rightarrow F \qquad \text{双線形性 } e(sA, tB) = e(A, B)^{st}$$

■ 何を目指したか

従来の、復号・再暗号化を要するデータベース検索や、複雑なセキュリティ管理には、膨大な時間と電力がかかる。このため高グレードのセキュリティやプライバシーの達成が難しい。

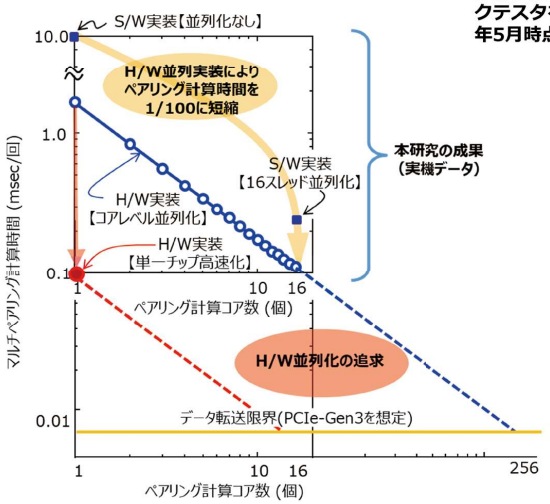
→ これらの解決を図る技術の確立

■ 何を達成したか

ペアリング利用高機能暗号の圧倒的性能向上と適用範囲の拡大

- 楕円曲線上のペアリングに基づく高機能暗号を用い、センサ等のIoT機器からクラウドまでの一貫したセキュリティを実現。
- クラウド上のデータベースでの秘匿検索においては、サーバ上に平文が現れることのないセキュアかつ実用的な秘匿検索システムの構築技術を、分散処理アーキテクチャ/ハードウェア（コアレベル並列化・単一チップ高速化）/ソフトウェア（ミドルウェア・検索アプリ）面から確立した。１０,０００倍という目標を圧倒的に上回る高速化・省エネ化を達成。
- 多数のIoT機器が出力する多数の（メッセージ、署名）ペアに対して、多数の署名を１つに集約し、多数のメッセージと１つの集約署名を検証者に送るという伝送効率の点でメリットのある集約署名技術を、ペアリング利用高機能暗号のもう一つのキラーアプリケーションと位置づけ、開発した。

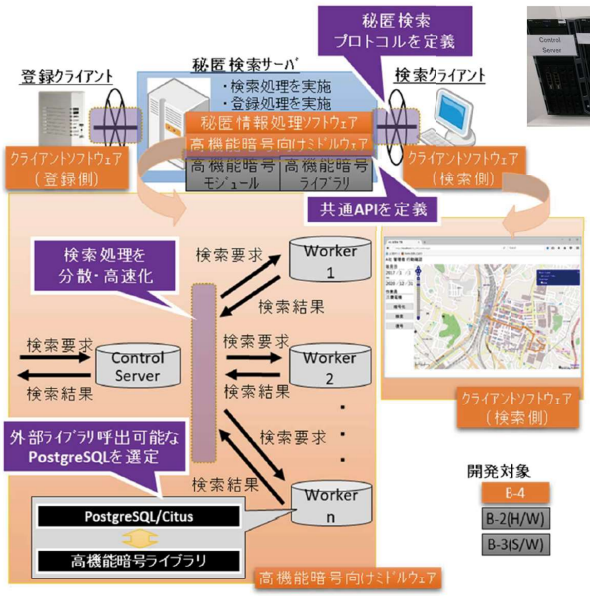
■ 秘匿検索分散処理システムの性能評価



ペアリング計算用試作チップの評価結果を下表に示す。ここでの実現はV2 で表記されたもの。演算制御は全て外部から行う形式。試作チップは6.2mmx 3.1mm 角のチップ上に実現され、2.8M ゲート（２入力NAND 換算）。ロジックテスタを用いた性能評価の結果、最大動作周波数250MHz において33us のペアリング時間を実現。これは2021年5月時点において実測で世界最高速の性能。また、ペアリング演算あたり最小13.7uJ の消費エネルギーを実現。

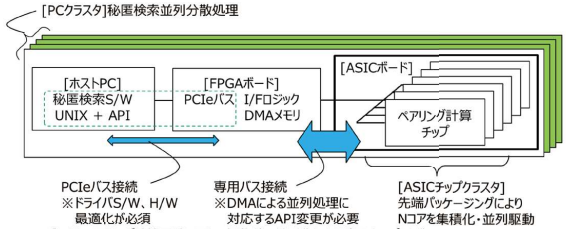
Platform	#Gates [kG]	Area [mm²]	Vdd[V]	Freq [MHz]	1-pair #Clk	1-pair t_{Pair} [us]	1-pair P_{Pair} [mW]	1-pair E_{pair}[uJ]	7-pair (*est / # measure) Vdd	Freq	#Clk	t_{Pair} [us]	P_{Pair} [mW]	E_{pair}[uJ]
Mobile Device[3] Apple A5 32nm	-	-	-	1,000	9,909,000	9,905	-	-			38,139,741	38,140	-	-
HighendPC[4] Corei7-6700K 14nm	-	-	-	4,000	840,000	210	91,000	19,110			3,233,160	808	91,000	12,444,433
HighendFPGA[5] KintexUltra 20nm	14,463slice+460DSP	-	-	170	18,151	107	-	-			69,863	412	-	-
ASIC[6] 130nm	94	-	-	338	5,340,400	15,800	-	-			20,555,200	60,814	-	-
ASIC[7] 65nm	354	2.51	-	800	512,541	640	255	163			1,972,770	2,463	255	627
ASIC[8] 65nm	323	-	-	633	330,053	521	-	-			1,270,374	2,005	-	-
ASIC [2] 65nm	2,793	12.8	1.33	250	8,175	33	2,850	94.0			31,466	127	2,850	361.8
FDSOI: v2			0.75	74.6		110	240	26.5				287	240	102.0
			0.49	9.2		792	17.2	13.7				3,048	17.2	52.7
ASIC 65nm	13,104	21.62	1.4	105	8,000	76.0	1,188	90.3	1.4	66.7	13,784	206.8	1,175	243.0
FDSOI: v5-1 3core			0.75	47.6		168	68.2	11.5	0.75	29.9		461.8	55.4	25.6
			0.32	2.33		3,440	0.95	3.28	0.32	2.13		6,479	1.02	6.62
ASIC 65nm	10,323	21.62	1.4	167	8,000	48.0	1,594	76.5	1.4	115	18,772	163.3	1,601	261.6
FDSOI: v5-2 2core			0.75	50		160	65.0	10.4	0.75	35.7		525.6	61.5	32.3
			0.32	2.56		3,120	0.94	2.93	0.33	2.60		7,227	1.11	8.03
ASIC 12nm	2,300	4.0	1.17	727	8,175	11.3	1,013	11.5			31,466	43.5	1,013	44.3
FinFET			0.8	426		19.4	275	5.34				76.7	275	20.6
			0.68	272		30.3	35.4	1.07				116.6	35.4	4.12

■ 秘匿検索分散処理システムの全体像（↓）とデモンストレータ（↓）



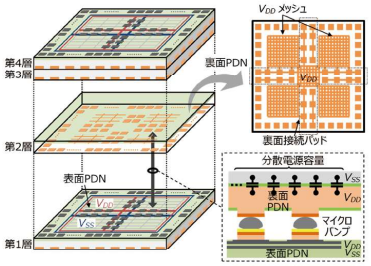
- 秘匿情報処理ソフトウェアを並列化・高速化する秘匿検索分散処理システムのプロトタイプ実証
- マルチスレッドによるミドルウェア並列化と高機能暗号モジュールによるペアリング処理高速化

■ ペアリング計算並列処理モジュール



- ASICボードにペアリング計算回路コアをN個集積、並列化による高スループット化
- PC+PCIe+FPGAによる汎用環境に実装、デモシステム開発の見通しを立て易く
- ①ASICチップ並列接続バスアーキテクチャ、②裏面埋設配線による耐タンパーパッケージング

■ 裏面埋設配線と三次元積層による電源供給網



■ 本資料ではスペース都合で次の研究開発項目についてはその名称を示すにとどめます：

- 高機能暗号方式設計
  追跡可能集約署名方式をはじめとする先進的な高機能暗号方式
- ペアリング利用暗号実装に対するサイドチャネル攻撃耐性評価
- 高機能暗号を用いたゲートウェイ向けソフトウェア
- 高機能暗号実用化戦略

これらは報告書をご参照ください。

事業者からのメッセージ

◆秘匿検索システム研究成果のデモンストレーションを予定しています。ご関心のある方は右記までお問合せください。
◆研究開発の詳細はNEDOのWebページをご参照ください。

連絡先
電子商取引安全技術研究組合
事務局長 服部統幾
TEL:03-5259-8077
E-mail : jimukyoku@ecsec.org

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP16007）の結果得られたものです。