IoTのセキュリティ？ カオスでしょ！

平成28年5月24日（火曜日）@JST

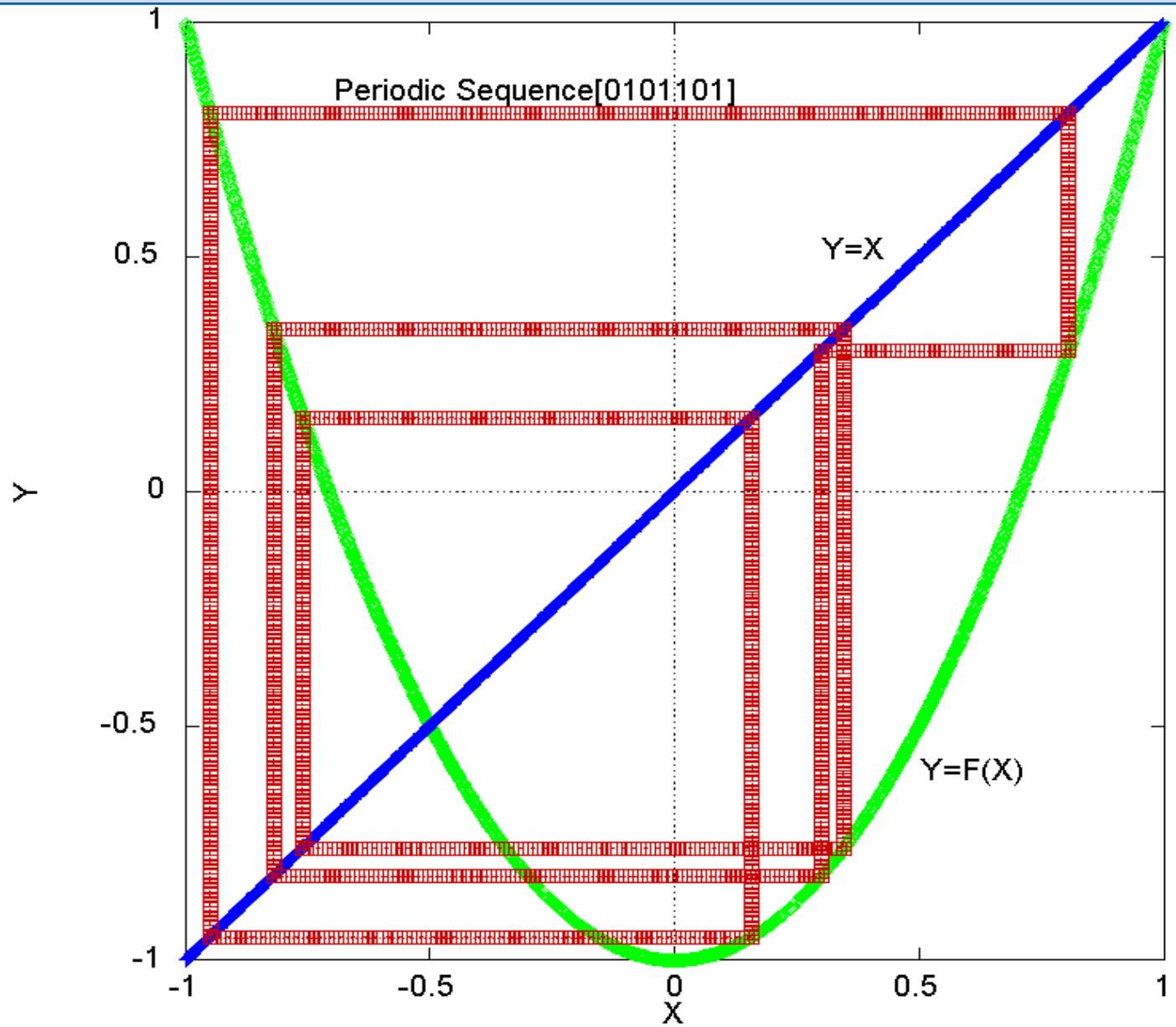
京都大学大学院 情報学研究科
数理工学専攻

教授　梅野 健
http://chaosken.amp.i.kyoto-u.ac.jp/

世界で初めて物理現象として観測されたカオス
(誕生の地：京大, 1961年11月 上田睨亮（名誉教授)が大学院生の時)

世界で初めてカオス符号（チェビシェフ多項式 $Y=2X^2-1$）が2値最適なGold符号よりスペクトル拡散用拡散符号として優れていることを示す.

Ref., K. Umeno and K-I. Kitayama, Electroncis Letters (1999)



新技術(超高速・超軽量カオス暗号)開発の歴史

1998年4月　KUが郵政省入省(郵政省カオス秘話通信PJ参画)

1999年3月. 最初のオリジナルの特許出願→2000年2月登録
(暗号テーブルを用いないカオス写像の並列化暗号)
特許3030341号(現在も維持. VSC-Vector Stream Cipher)

2002年　最初の製品化-世界初暗号化データベース「eCipherGate」

2003年　世界初リアルタイムHDTV暗号化(CRL報道発表)

2003年　新技術(カオス暗号・通信技術)による起業化
株式会社カオスウェア(NICT・JST技術の活用)創業・設立

2004年　VSC暗号仕様公開@カオスウェア(万人が評価可能に)

2004年　VSC-SDK開発→スタジオアリス全店舗に採用(2005年)

2012年4月　KUが京都大学に移籍。できなかったことを中心に教授開始

2016年1月　世界初・安全性証明可能暗号VSC2.0の論文公開

2016年3月　世界最高速(40-100Gbps達成可能)暗号発明. 特許出願

本技術に関する知的財産権

- 発明の名称 :乱数発生装置、乱数発生及びコンピュータプログラム
- 出願番号 :特願2016-041564
- 出願人 :国立大学法人京都大学
- 出願日 :2016年3月3日
- 発明者 :岩崎淳、梅野健

基礎暗号技術への投資

投資期間　　＝10年必要

投資額　　＝10億円必要

上場時時価総額　＝1000億円以上
[米国RSA社参照]

置き換え実装コスト＝限りなくゼロに近い

結論ー＞本特許ライセンス料数億円投資は安い!

IoT時代の到来

Internet of Things

ありとあらゆるものが
インターネットに接続される
(2020年までに、IoTデバイス数が530億台)

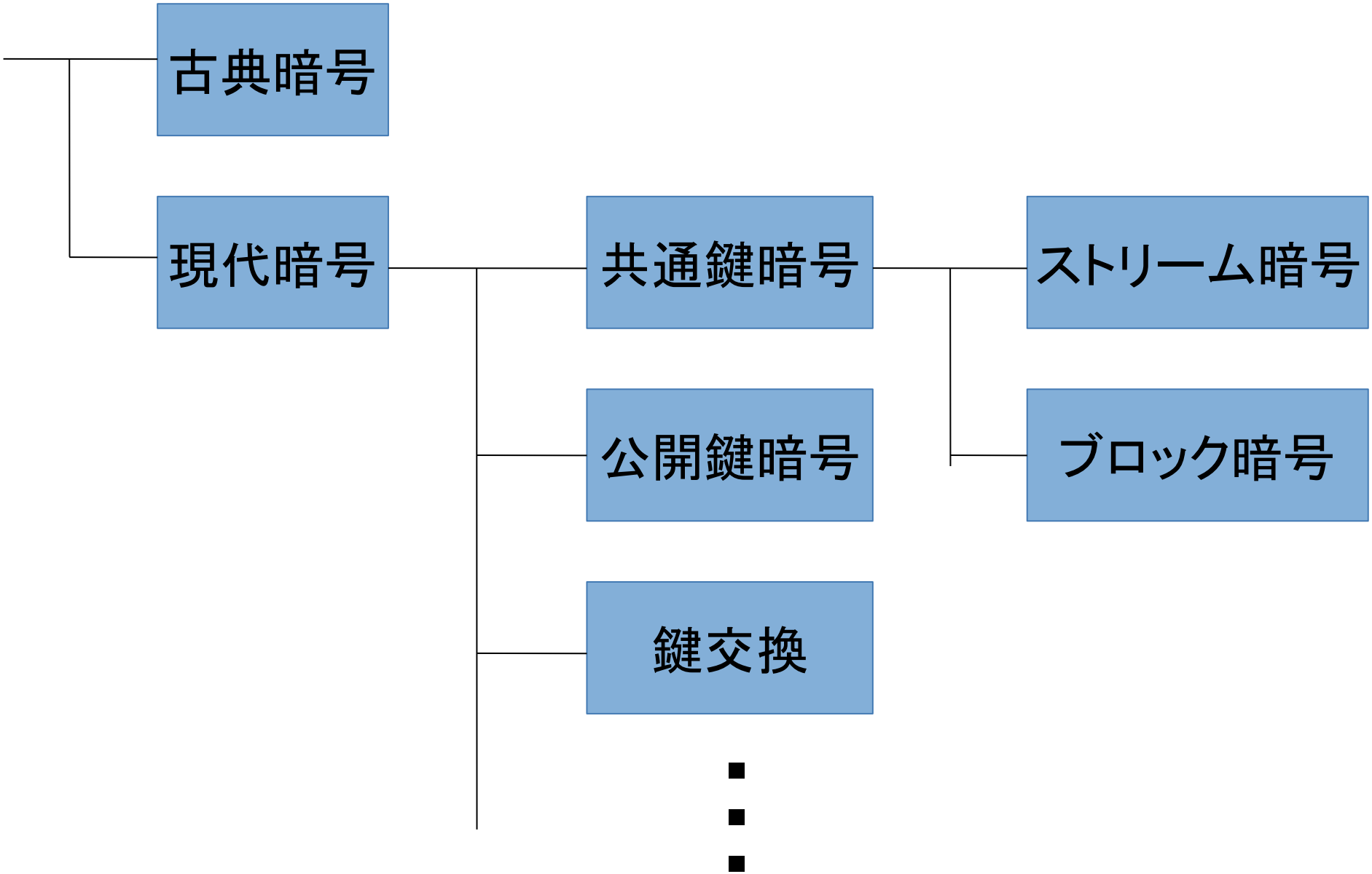
- よりセンシティブな情報がより多くインターネットに接続される
- 情報セキュリティが守られないと、深刻な事態になる

情報セキュリティを支える暗号技術には、

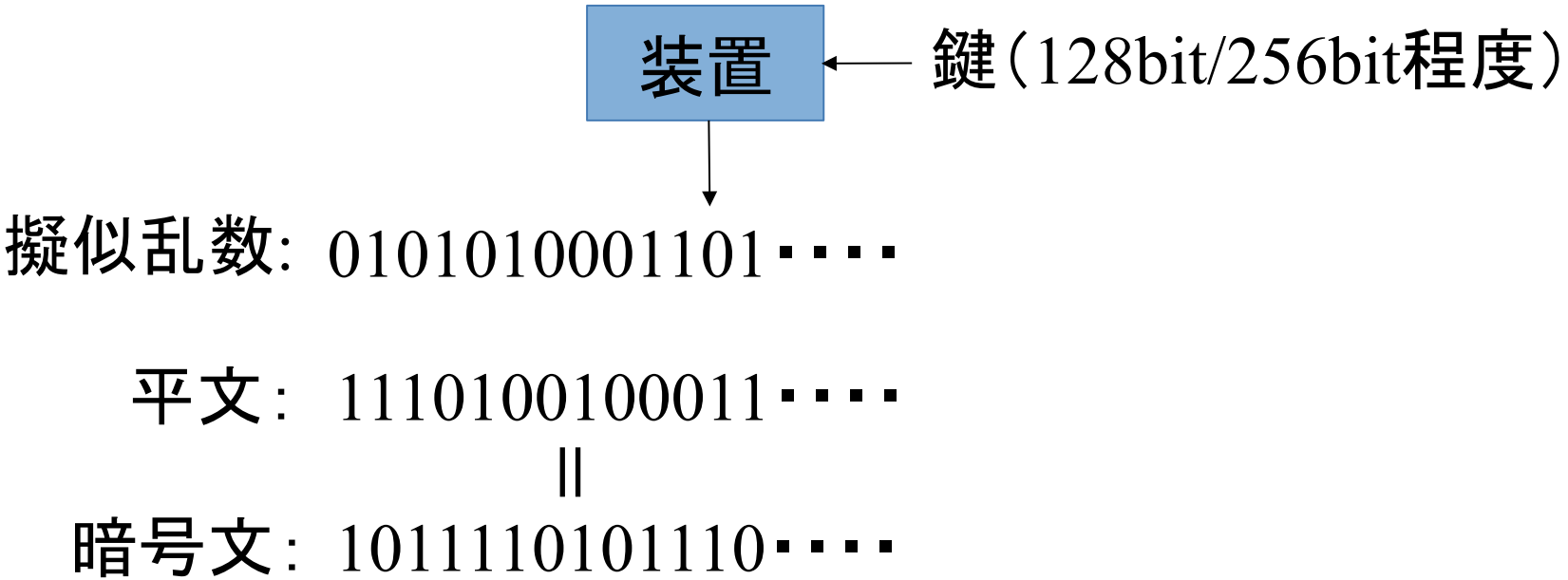
高速、軽量、安全

が求められる

暗号



ストリーム暗号



- 一般にブロック暗号より軽量・高速
- 擬似乱数に高い乱数性（ランダムさ）が求められる
- 擬似乱数生成器としても使える

従来のストリーム暗号

- 従来のストリーム暗号では，メインのパーツは
  ガロア体上の演算

- 既に多くの暗号で使用され、研究されつくしている

→ 大幅な速度向上は難しい

暗号そのものの設計に先立って、新しいパーツが必要

→ カオス写像を使う(メモリ不要)

注目するパーツ　一筆書き多項式

2冪剰余環 ＝

この範囲を超えたら mod 2^w　（ 2^w で割った余り）をとる

多項式を使って、2冪剰余環を移動していくことを考える

例えば

１ → ７ → ４ → ３ → ・・・

軌道ができる

⋮

軌道の周期が　＝ 一本の軌道が2冪剰余環を巡る

→ は一筆書き多項式

一筆書き多項式

$\mathrm{mod}\ 2^W$ は高速に計算できる

一筆書き多項式は高速に計算できる

ストリーム暗号に使いたい！

一筆書き多項式自体は、昔から一部の乱数生成器で使われてきた

しかし、乱数性が良くない（単純な規則性がある）

ストリーム暗号としては使い物にならない

新技術

一筆書き多項式を1つでは単純すぎる

↓

複数の一筆書き多項式を組み合わせれば良い

一筆書き多項式の良い点は、軌道の周期が長いこと。
これを崩したくはない。

なので、

一筆書き多項式を、周期を保ったまま、複数組み合わせる方法を開発

新技術の詳細

$F_i(X) = \sum_{j=0}^{N} a_{i,j} X^j$ は，N 次以下の一筆書き多項式であるとする．

$$x_1(t+1) = \sum_{j=0}^{N} \left\{ a_{1,j} + \sum_{k=1}^{K} \sum_{l=1}^{L} C_{i,j,k,l} x_k(t)^l \right\} x_1(t)^j \mod 2^w$$

$$x_2(t+1) = \sum_{j=0}^{N} \left\{ a_{2,j} + \sum_{k=1}^{K} \sum_{l=1}^{L} C_{i,j,k,l} x_k(t)^l \right\} x_2(t)^j \mod 2^w$$

$$\vdots$$

$$x_K(t+1) = \sum_{j=0}^{N} \left\{ a_{K,j} + \sum_{k=1}^{K} \sum_{l=1}^{L} C_{i,j,k,l} x_k(t)^l \right\} x_K(t)^j \mod 2^w$$

- $j = 0$ 以外の任意の (i, j, k, l) に対して，$C_{i,j,k,l} \equiv 0 \mod 4$
- 任意の (i, k, l) に対して，$C_{i,0,k,l} \equiv 0 \mod 2$
- 任意の i に対して，$\sum_{k=1}^{K} \sum_{l=1}^{L} C_{i,0,k,l} \equiv 0 \mod 4$
- 任意の i に対して，$\sum_{k=1}^{K} \sum_{l:3\text{ 以上の奇数}} C_{i,0,k,l} \equiv 0 \mod 4$

新技術の性能評価①

速度評価

プロセッサ： Intel Core i5

暗号化速度： 2.19 cycle/Byte

1Byteを暗号化するのにかかるクロック数

値が小さいほうが速い

現時点で世界最高速のストリーム暗号と考えられる
K2-Cipherの 2.88 cycle/Byte より速い

新技術の性能評価②

乱数性評価

NIST SP 800-22 : 乱数性を評価する一つのツール

188項目のテストで構成

これを、100回行った

合格したテスト項目数	回数
188	71
187	22
186	6
185	1

理想的なプロポーション

※NIST SP 800-22は、必ずしも合格する項目数が多いほうが良いわけではない

→ 乱数性に問題はみられない

新技術の特徴

- 高速
- 軽量(たった64Byte!)
- 省電力

容量の大きなデータでも
瞬時に暗号化できる

センサー等、小さな
デバイスにも搭載できる

想定される用途

暗号化ならどんなところでも使えるが、特に

- 大容量の暗号化
  - 4K、8K(28Gbps-40Gbps)をリアルタイム暗号化
  - 医療画像などセンシティブな情報
  - データセンター
- プロセッサや電源の制限が厳しいデバイスでの暗号化
  - スマートフォン、ウェアラブル端末
  - センサーデバイス

企業への期待

- 現在未解決の40Gbps以上の暗号化については、本技術導入により克服できると考えている。
- 通信・放送・データセンター・ロボット・自動運転の技術を持つ、企業との共同研究を希望。
- また、8K, 5Gを開発中の企業、自動運転等必須のハードウェアセキュリティ分野への展開を考えている企業には、本技術の導入が有効と思われる。
- H29.9頃の特許前までに公開各分野の有力な企業に絞って先行ライセンシングしたい。
- 今後のフロー例: 共同研究(1年間)→特許実施契約

産学連携の経歴

- 2000年-2002年　ジャパン・インフォメーションテクノロジー社とデータベース暗号化技術「eCipherGate」共同開発
  第15回中小企業新技術新製品賞(2003)
- 2000年-2003年　JSTプレベンチャー事業に採択
- 2003年　株式会社カオスウェア設立
- 2003年　第5回 LSI IPアワード IP賞　受賞
  [世界初カオス暗号チップ]
- 2005年-2009年　JST委託開発事業に採択(カオスウェア)
- 2009年　JST委託開発事業成功認定
  [5GHz帯カオスCDMA通信用チップ]

本技術に関する知的財産権

- 発明の名称：乱数発生装置、乱数発生及びコンピュータプログラム
- 出願番号　：特願2016-041564
- 出願人　　：国立大学法人京都大学
- 出願日　　：2016年3月3日
- 発明者　　：岩崎淳、梅野健

お問い合わせ先

京都大学産学連携担当
関西TLO株式会社
ライセンシング・アソシエイト
担当: 藤ヶ崎諒平

ＴＥＬ 075-753-9150
e-mail fujigasaki@kansai-tlo.co.jp