ストリーム暗号KCipher-2

2010年3月

KDDI株式会社

背景

- 大容量データの配信
  - 高速暗号の必要性
  - 携帯端末上でも高速に動作可能な暗号の必要性
- ISO標準の改定が開始される

©KDDI Corporation. All Rights Reserved.

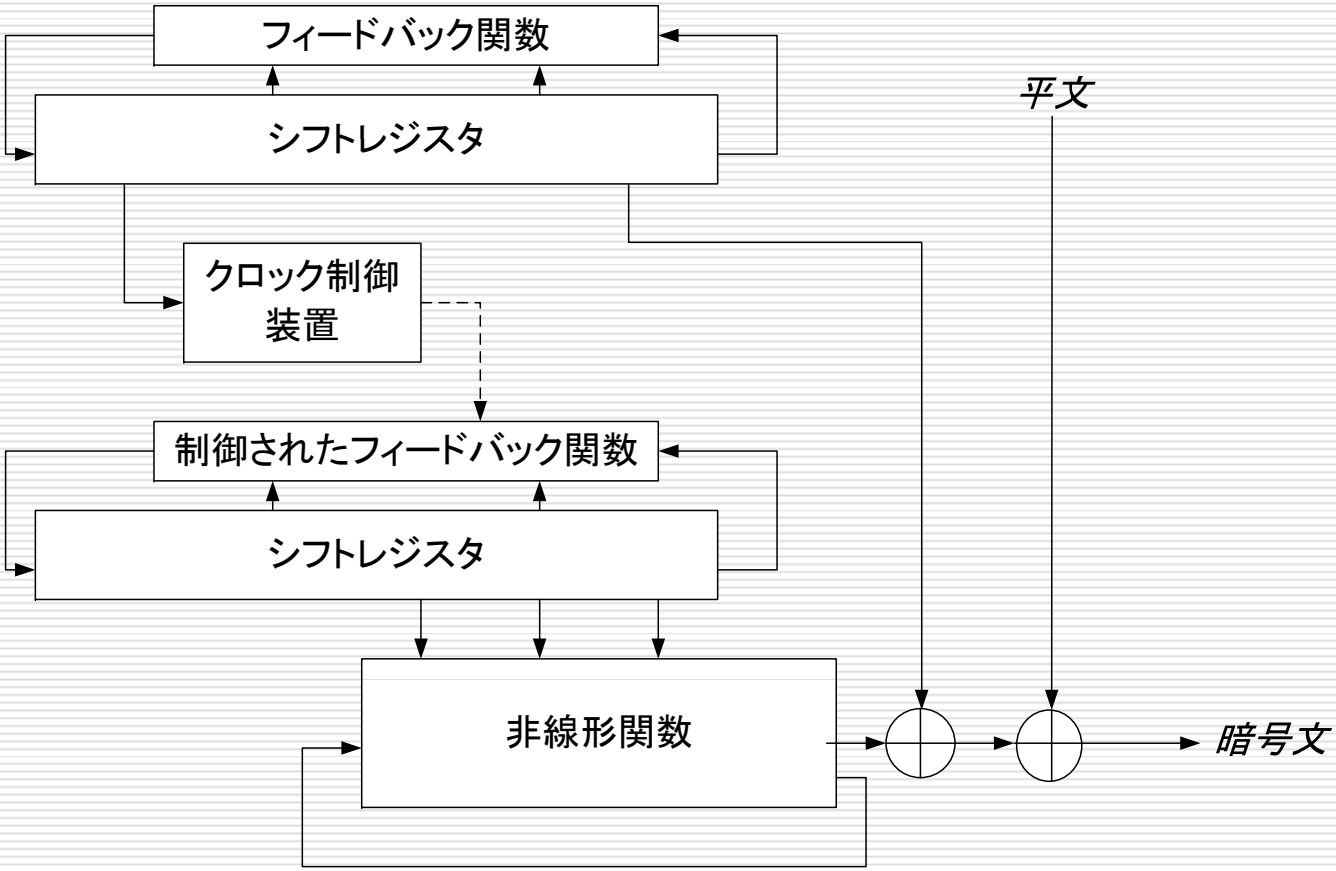
技術仕様について

KCipher-2の設計指針

- 安全性向上に関して
  - 複数のコンポーネントの併用
  - 既存攻撃への対応
- パフォーマンスに関して
  - ワード単位での処理の実現
  - CPU非依存の演算
  - 小さな内部状態
  - 効率的な初期化処理

©KDDI Corporation. All Rights Reserved.

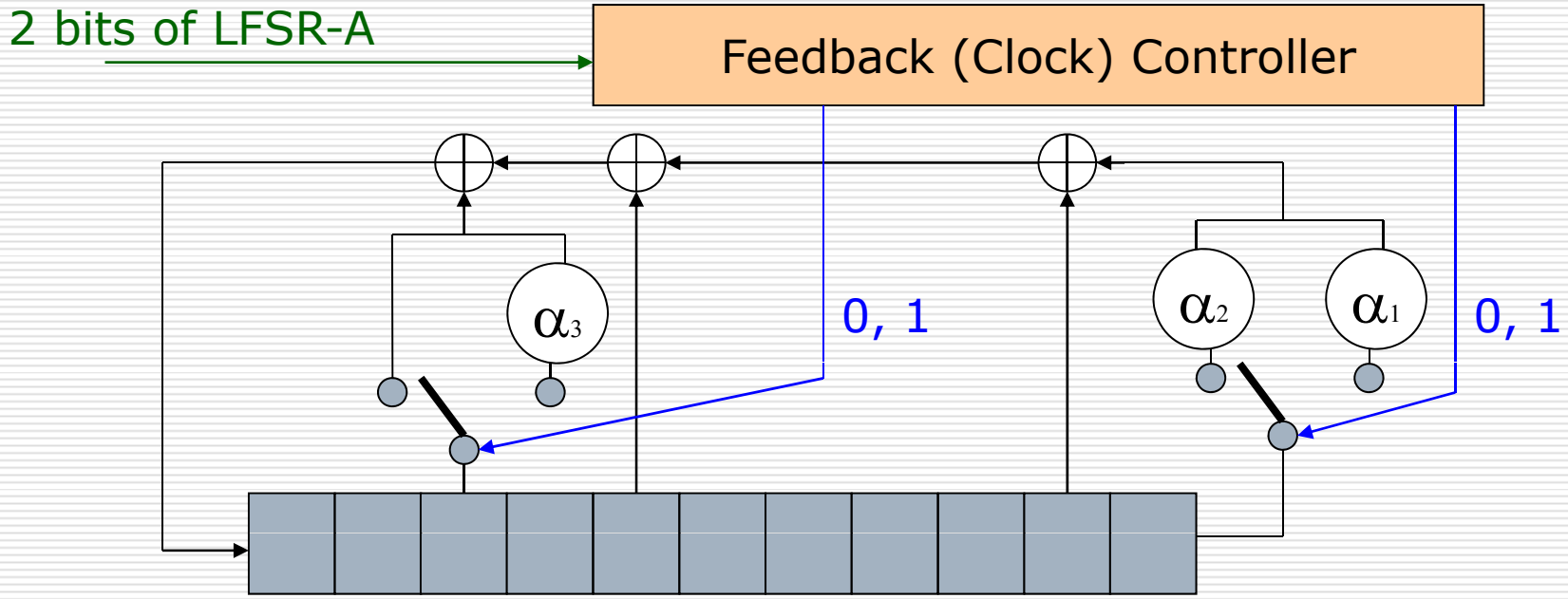
ストリーム暗号KCipher-2



©KDDI Corporation. All Rights Reserved.

Dynamic Feedback Control (DFC)

- LFSR-Bのフィードバック係数を選択する

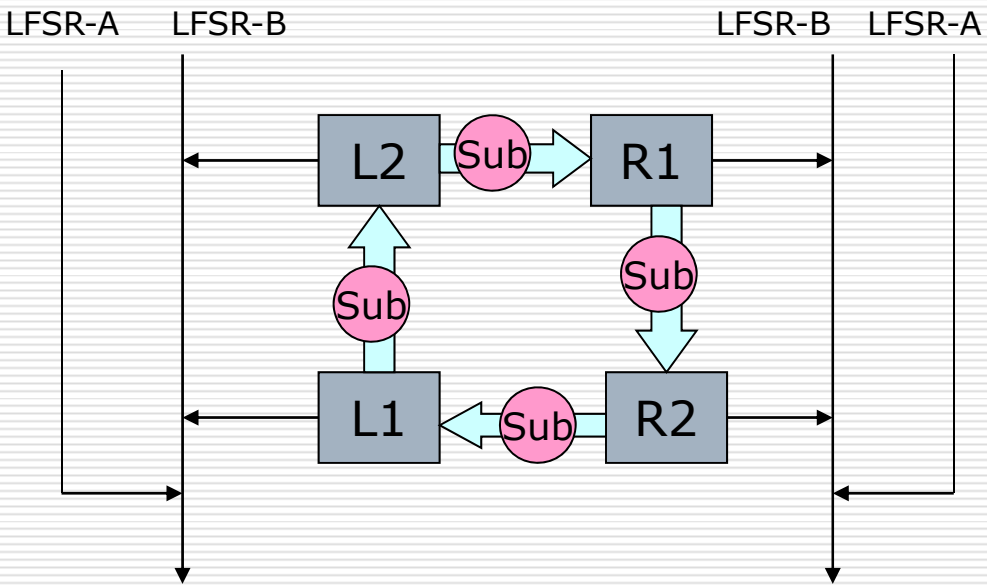


$$f_B(x) = (\alpha_1^{cl1_t} + \alpha_2^{1-cl1_t} - 1)x^{11} + x^{10} + x^5 + \alpha_3^{cl2_t}x^3 + 1 \in GF(2^{32})[x]$$

©KDDI Corporation. All Rights Reserved.

Finite State Machine (FSM)

- 左右対称の構成
  - 2倍の鍵系列を出力
  - セキュリティの向上
    - 左右のレジスタが相互に接続されている



- Substitutionは、SNOW 2.0と同一
- 内部メモリを計算に加えることにより、鍵系列とレジスタとの直接的な関係を隠蔽する
- 2つの異なるLFSRからの出力によって鍵系列を計算することにより、鍵系列を表現する式はより複雑になる

©KDDI Corporation. All Rights Reserved.

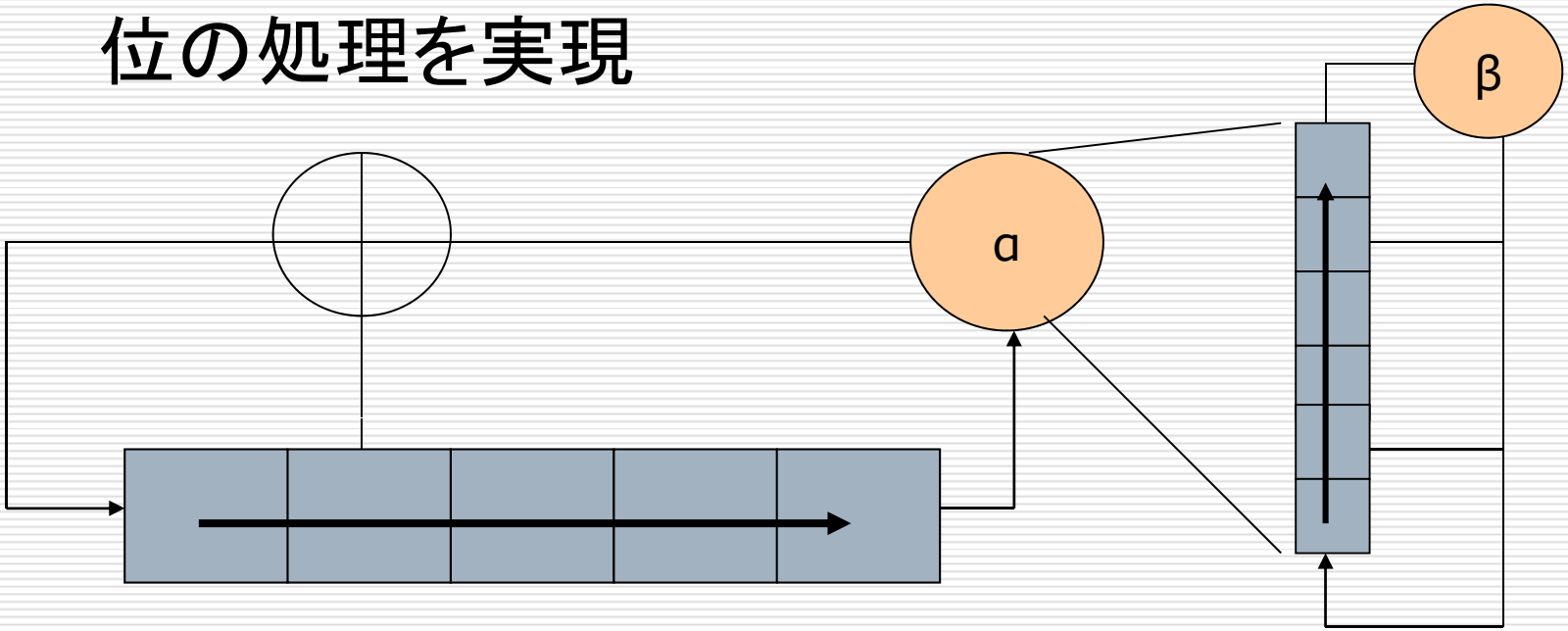
安全性向上に関して

- 非線形関数とクロック制御という2つの要素を組み合わせることにより、安全性を強化
  - 非線形関数
    - 出力系列の代数次数を増加させる。
  - クロック制御
    - 出力系列を確率関数に変化させる。
- 推測決定攻撃、識別攻撃、代数的攻撃などの最新攻撃に対する安全性を確保

©KDDI Corporation. All Rights Reserved.

ワード単位での処理

- LFSRを入れ子構造にすることによりワード単位の処理を実現



GF(2^8) → GF(2^{32}) → GF(2^L)と構成した，GF(2^L)上で原始多項式を使用

©KDDI Corporation. All Rights Reserved.

CPU非依存、省メモリ

- 全体を排他的論理和、算術加算、AND、OR、テーブル参照のみから構成することにより、CPUに依存しない性能を実現
  - 例：Pentium4では、2乗算が低速
- 2つのLFSRは並列的に処理できる
- 内部状態の大きさを最適化し、省メモリを実現
  - LFSR-A: 32bit X 5 レジスタ
  - LFSR-B: 32bit X 11 レジスタ
  - 内部メモリ: 32bit X 4
  - Total: 640 bits

©KDDI Corporation. All Rights Reserved.

効率的な初期化処理

- 24サイクルで初期化を完了
- 13サイクルで初期鍵、初期ベクトルのすべてのビットが内部状態のすべてのビットに拡散

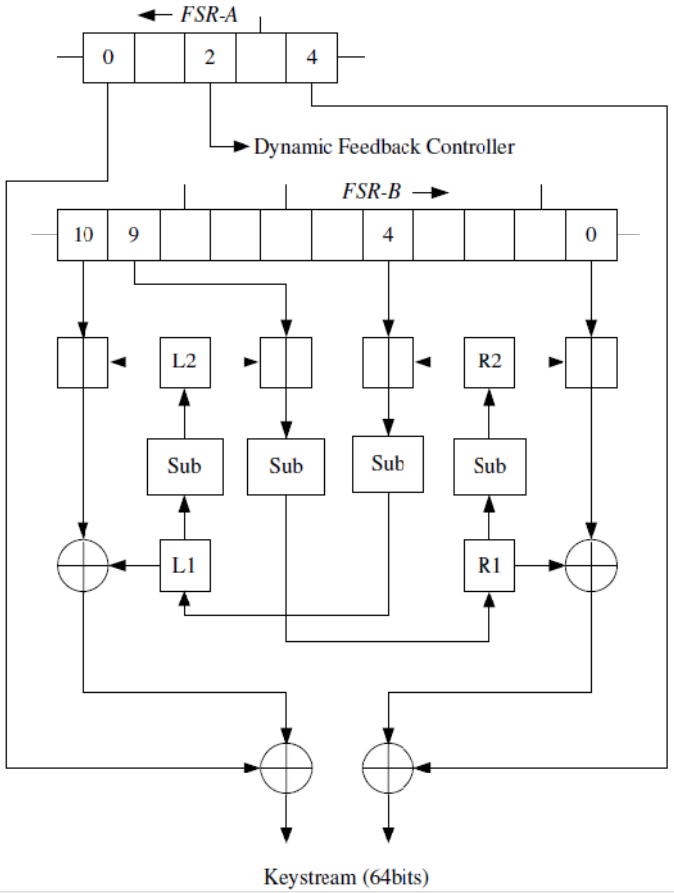
Register	1	3	5	6	13
A_t	*	*	K	K	K, IV
A_{t+1}	*	*	K	K	K, IV
A_{t+2}	*	K	K	K	K, IV
A_{t+3}	*	K	K	K	K, IV
A_{t+4}	*	K	K	K, IV	K, IV
B_t	K	*	K	*	K, IV
B_{t+1}	K	K	*	*	K, IV
B_{t+2}	*	K	*	K	K, IV
B_{t+3}	*	*	K	*	K, IV
B_{t+4}	K	*	*	K	K, IV
B_{t+5}	K	K	K	K	K, IV
B_{t+6}	*	*	K	K	K, IV
B_{t+7}	*	K	K	K, IV	K, IV
B_{t+8}	K	K	K, IV	K, IV	K, IV
B_{t+9}	*	K	K, IV	K, IV	K, IV
B_{t+10}	K	K, IV	K, IV	K, IV	K, IV
$R1_t$	*	K	K, IV	K, IV	K, IV
$R2_t$	*	K	K	K, IV	K, IV
$L1_t$	*	K	K	K	K, IV
$L2_t$	*	K	K	K	K, IV

©KDDI Corporation. All Rights Reserved.

安全性に関する自己評価について

安全性評価

- FSMについては、SNOW2.0を改良した方式とし、安全性を強化
- Distinguishing Attack, Algebraic Attack, GD attack, などに対する安全性を評価
- DFCにより安全性を強化
- 2^{256}以下の計算量の攻撃は見つかっていない
- 外部評価を実施



©KDDI Corporation. All Rights Reserved.

実装性に関する自己評価について

ソフトウェア評価結果

Algorithm	Key. Gen. (Cycle/Byte)	Init. (Cycle/Init.)
K2 (Reference, Pentium 4)	7.50	1308
K2 (Optimal, Pentium 4)	4.97	1162
K2 (Optimal, Pentium III)	5.53	1194
K2 (Optimal, Core 2 Duo)	4.01	860

©KDDI Corporation. All Rights Reserved.

ハードウェア評価結果

Design	Data rate (bits/cycle)	Clock Freq. (MHz)	Throughput (Mbps)	Area (slice)	Throughput/Area (Mbps/slice)	Device
Normal	64	63.9	4090	3067	1.33	Spartan-3
Double-keystream	128	38.0	4864	5295	0.92	Spartan-3
Quad-keystream	256	20.4	5223	9161	0.57	Spartan-3
Normal	64	74.8	4787	2898	1.65	Virtex-II

Target	Data rate (bits/cycle)	Clock Freq. (MHz)	Throughput (Mbps)	Area (slice)	Throughput/Area (Mbps/slice)	Reduction Rate (%)
Spartan-II	64	30.0	1920	2133	0.90	-
Spartan-3	64	39.1	2503	2140	1.17	30.2
Virtex-II	64	48.7	3117	2145	1.45	26.0

©KDDI Corporation. All Rights Reserved.

公開状況、ライセンス等について

公開状況

- 発表期日：2007年7月28日
- 発表者：Shinsaku Kiyomoto　ほか
- 会議名：SECRYPT2007

©KDDI Corporation. All Rights Reserved.

ライセンス

- 事務局や評価者が評価目的で使用する場合は無償とする。
- 電子政府が実用に供する場合は妥当かつ非差別的な条件で提供する。

©KDDI Corporation. All Rights Reserved.

利用実績

- 製品
  - KCipher-2 SDK (KDDI研究所)
- システム等
  - 官公庁系の携帯電話を用いた情報通信システム (2,000ライセンス)
  - 官公庁系のロケーションシステム (5,000ライセンス)
  - Webベースのグループウェア (1,000ライセンス)
  - コンシューマ向けマルチメディアコンテンツ再生ソフトウェア (100万ユーザ)

©KDDI Corporation. All Rights Reserved.