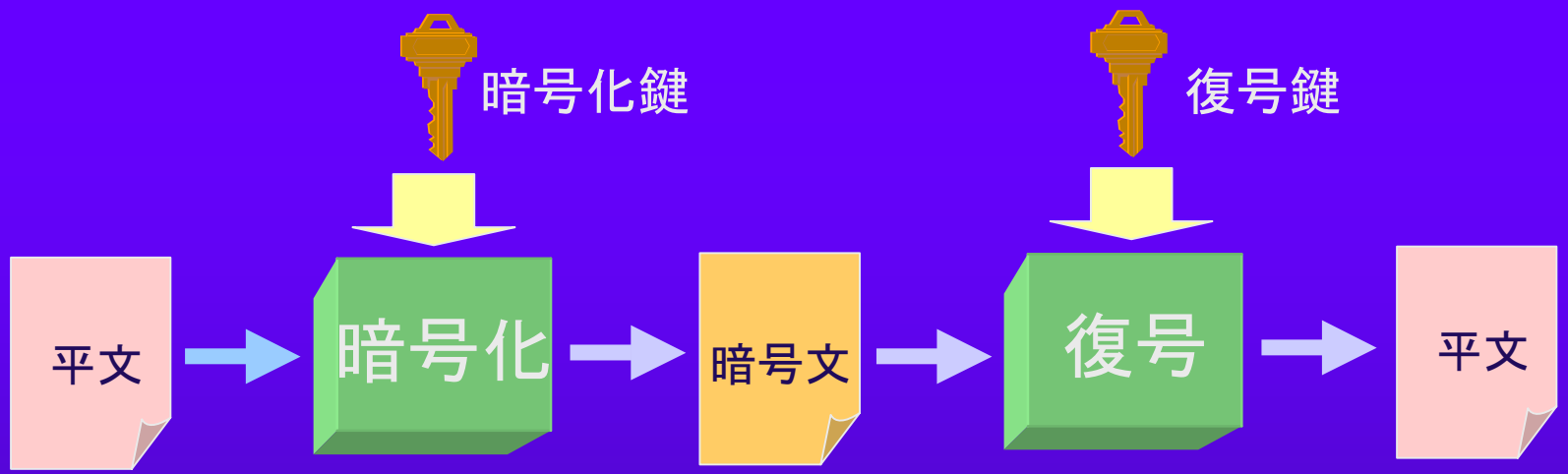
NTTと三菱電機が共同で次世代暗号アルゴリズム「Camellia」を開発

－ 高度な安全性と世界最高レベルの効率性を両立させた共通鍵ブロック暗号 －

２０００年　３月　１０日

日本電信電話株式会社
三菱電機株式会社

共通鍵暗号と公開鍵暗号



共通鍵暗号	暗号化鍵＝復号化鍵	秘匿通信のための暗号化に使用
公開鍵暗号	暗号化鍵≠復号化鍵	共通鍵暗号用鍵の配送及び電子署名/認証に使用

共通鍵暗号の現状

- ブロック暗号が主流
- 現在　・・・・64ビットブロック暗号

（例）DES（旧米国標準）、FEAL(NTT)、MISTY（三菱電機）

- 次世代・・・・128ビットブロック暗号

次世代共通鍵暗号の例

- 次期米国標準暗号AESの最終5候補
  MARS（米）、RC6（米）、Rijndael（ベルギー）、Serpent（英、イスラエル、ノルウェー）、Twofish（米）

共通鍵暗号分野における両社の技術と次世代暗号

- NTT　高速ソフトウェア実装に適した暗号設計技術
- 三菱電機　小型/高速ハードウェア実装に適した暗号設計技術
- 両社　暗号安全性評価技術（世界トップレベルの研究者）

両社の技術を結集

新しい次世代共通鍵暗号「Camellia」を共同で研究開発

次世代共通鍵暗号Camelliaの特徴

- 安全性　現在最強の解読法である差分解読法や線形解読法を用いても、解読が事実上不可能であることを確認
- 効率/実用性　マルチプラットフォームにおいて世界最高レベルの効率/実用性
  - ソフトウェア実装（32ビットCPU、8ビットCPU）
    - AESの5候補暗号と比べても同等もしくはそれ以上高速
    - 高度に最適化されたDESに比べて2倍以上高速
  - ハードウェア実装（専用チップ）
    - AESの5候補暗号と比べて、いずれよりも格段に小型化/高速化が可能
    - 世界最小レベルの小型化：10KG程度

CamelliaをISO標準への提案 (ISO/JTC1/SC27)

- ISOでは、暗号を標準化対象外としてきた（1990年頃より）
- 今年より暗号を標準化の対象とするように見直し
  - 3月9日　対象とすることに関する投票（結果は4月に明らかに）
  - 3月15日　暗号方式の提案締め切り（日本国内委員会では、3月10日締め切り）
  - 4月　ロンドン会議（手続き/今後のスケジュール等を検討）
  - 2001年/2002年　標準方式の決定（複数方式？）
- NTT−三菱電機はCamelliaをISOに提案

Camellia ― 技術のポイント

- 広がる暗号応用
  ―マルチプラットフォーム暗号への期待―

  – 32/64-bit CPU　例：電子認証システム
    - 豊富なメモリと強力な命令で高速暗号化を実現

  – 8-bit CPU　例：ICカード応用（電子マネー）
    - 限られたメモリ量と命令セットで実装する必要

  – ハードウエア　例：携帯電話,暗号ﾌﾟﾛｾｯｻ等
    - 小型・低消費電力設計が必須条件

Camellia ― 技術のポイント

- マルチプラットフォーム暗号に
  適したアルゴリズム構成要素とは？

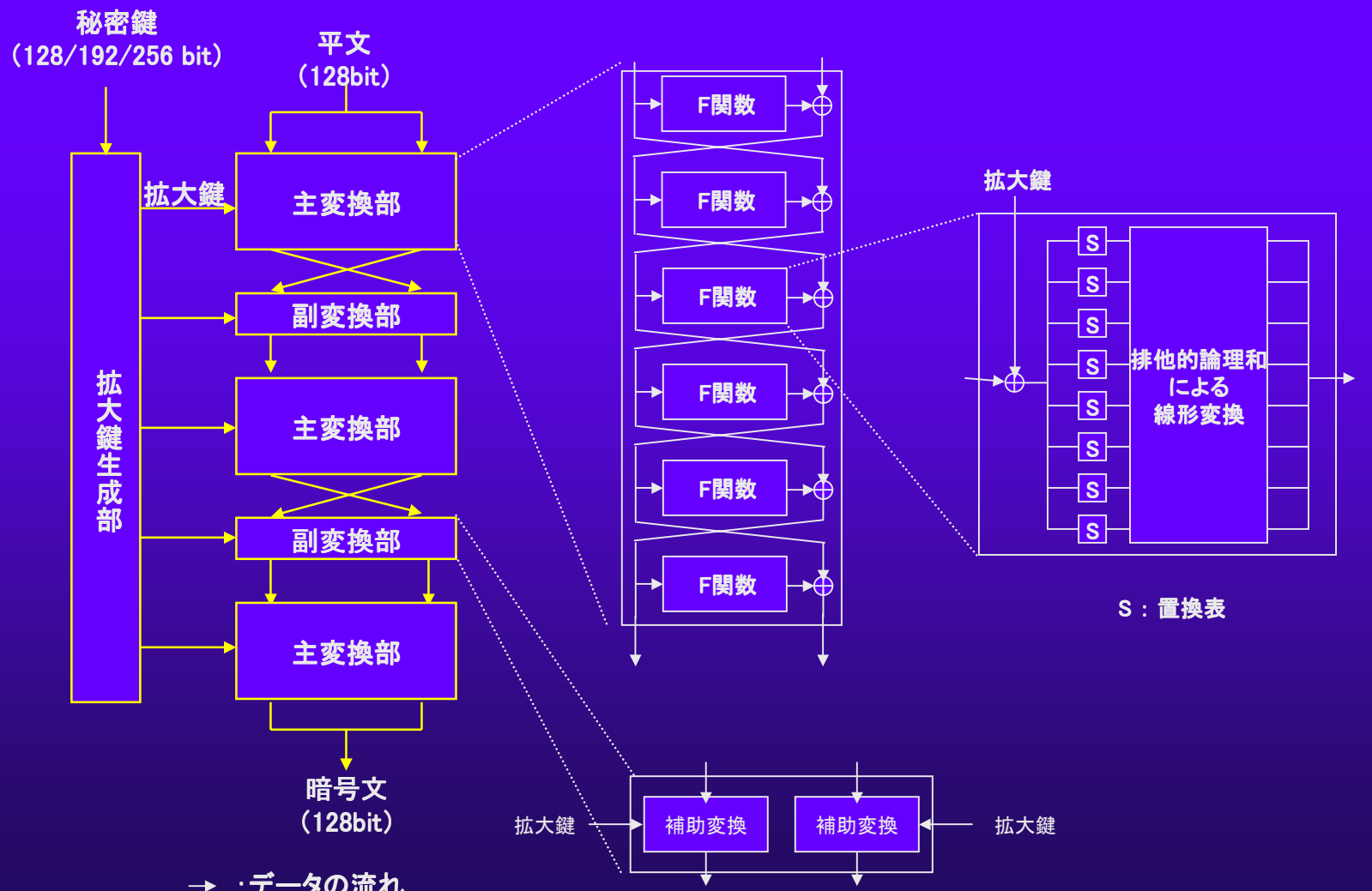
	32/64-bit CPU	8-bit CPU	ﾊｰﾄﾞｳｴｱ
論理演算（AND,OR,..）	高速	高速	小型高速
算術演算（ADD,MUL,..）	高速	命令依存	大型低速
ﾃｰﾌﾞﾙ参照（乱数表等）	高速	低速	設計依存
メモリ量	制約少ない	RAM ｻｲｽﾞに厳しい制約	消費電力に大きく影響

Camellia ― 技術のポイント

- 明確な設計原理にもとづく暗号
  ― Camellia の設計方針1 ―

  - **8 ビットを主な処理単位とする全体構造**
    - あらゆるプロセッサのソフトウエアで高速性を実現
  - **論理演算とﾃｰﾌﾞﾙ参照の組み合わせで実現**
    - ソフトウエアとハードウエアの性能を両立
  - **論理ｹﾞｰﾄ数が少なくしかも安全なﾃｰﾌﾞﾙ設計**
    - ハードウエアでの小型、低消費電力化を実現

Camellia の暗号化プロセス



Camellia ― 技術のポイント

- 明確な設計原理にもとづく暗号
  ― Camellia の設計方針2 ―

  - **構造の異なる2種の関数の組み合わせで実現**
    - 既存の解読法への対処と将来の解読法に対する防御
  - **主変換部だけで十分な安全性を確保**
    - 差分解読法や線形解読法等に対する確実な対処
  - **副変換部でさらに安全性を強化**
    - 速度やサイズに対するインパクトが最小になるよう設計
    - 暗号化と復号を（拡大鍵の順序以外）同じ回路で実現可能

Camellia ― 技術のポイント

- Camellia の性能
  ―インプリメンテーションの一例―

  - Pentium III Processor
    - 約300cycles/block
      （800MHz の場合340Mbps：電話5000回線に相当）
    - 高度に最適化された DES の2倍以上高速
  - Hardware
    - 21cycles/block　約10KGates
    - 128 ビットブロック暗号としては世界最小クラス

NTTと三菱電機が共同で次世代暗号アルゴリズム「Camellia」を開発

－ 高度な安全性と世界最高レベルの効率性を両立させた共通鍵ブロック暗号 －

２０００年　３月　１０日

日本電信電話株式会社
三菱電機株式会社