タイムリリース暗号を利用したデジタルコンテンツのための事前配信システムの提案

白勢研究室

2116050 吉田 努

2016/7/28

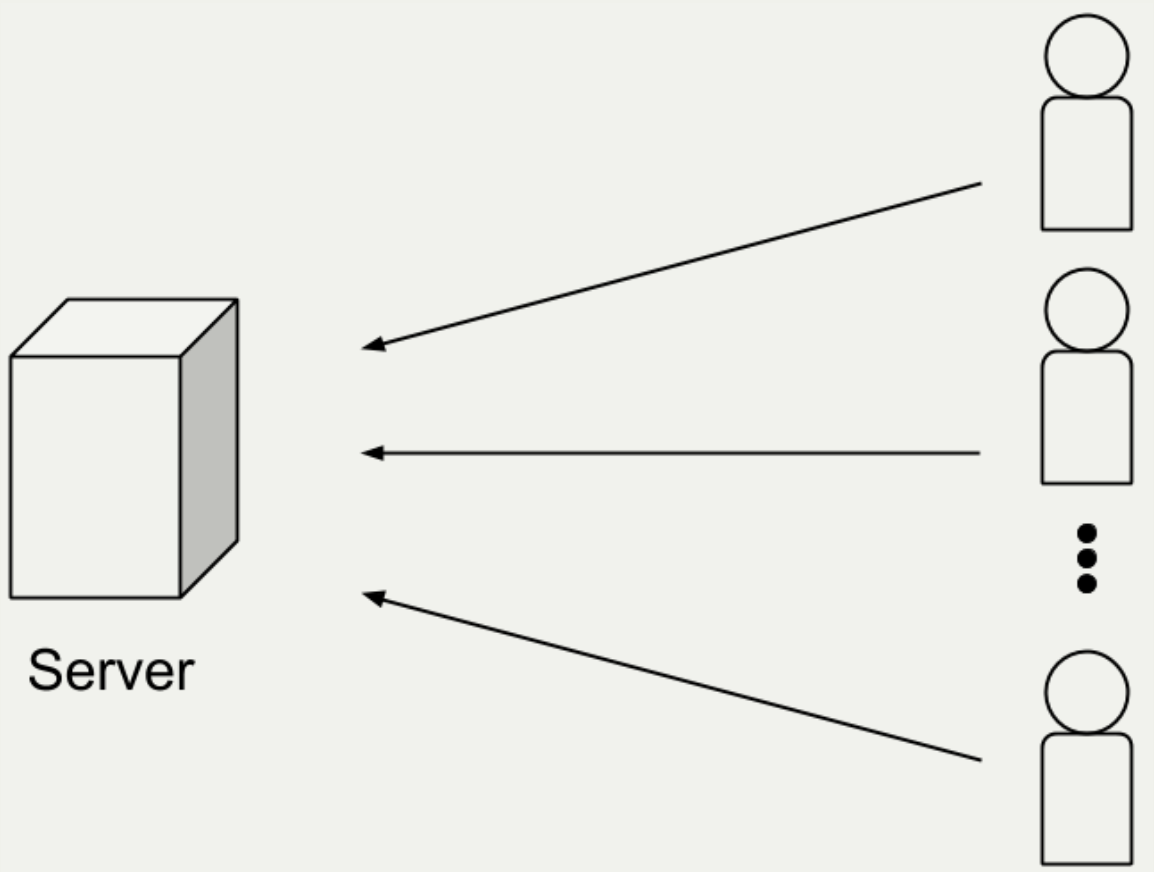
目次

- 背景
- 目的
- 関連研究
- 研究手段
- 研究経過
- まとめ
- 参考文献

背景(1/2)

- デジタルコンテンツ
  - 電子書籍
  - ゲーム
  - 映像
  - 音楽

背景(2/2)



- コンテンツリリース時
  - サーバの負荷増
  - ユーザの負担増

タイムリリース暗号によって解決できるのでは

タイムリリース暗号

- タイムリリース暗号とは
  - 時間指定(未来)で暗号文を復号することができる暗号
- 実用化されていない暗号の一つ

目的

- タイムリリース暗号でデジタルコンテンツを暗号化
- デジタルコンテンツの事前配信
  - コンテンツリリース時のサーバの負担を減少させる
  - ユーザの負担を削減

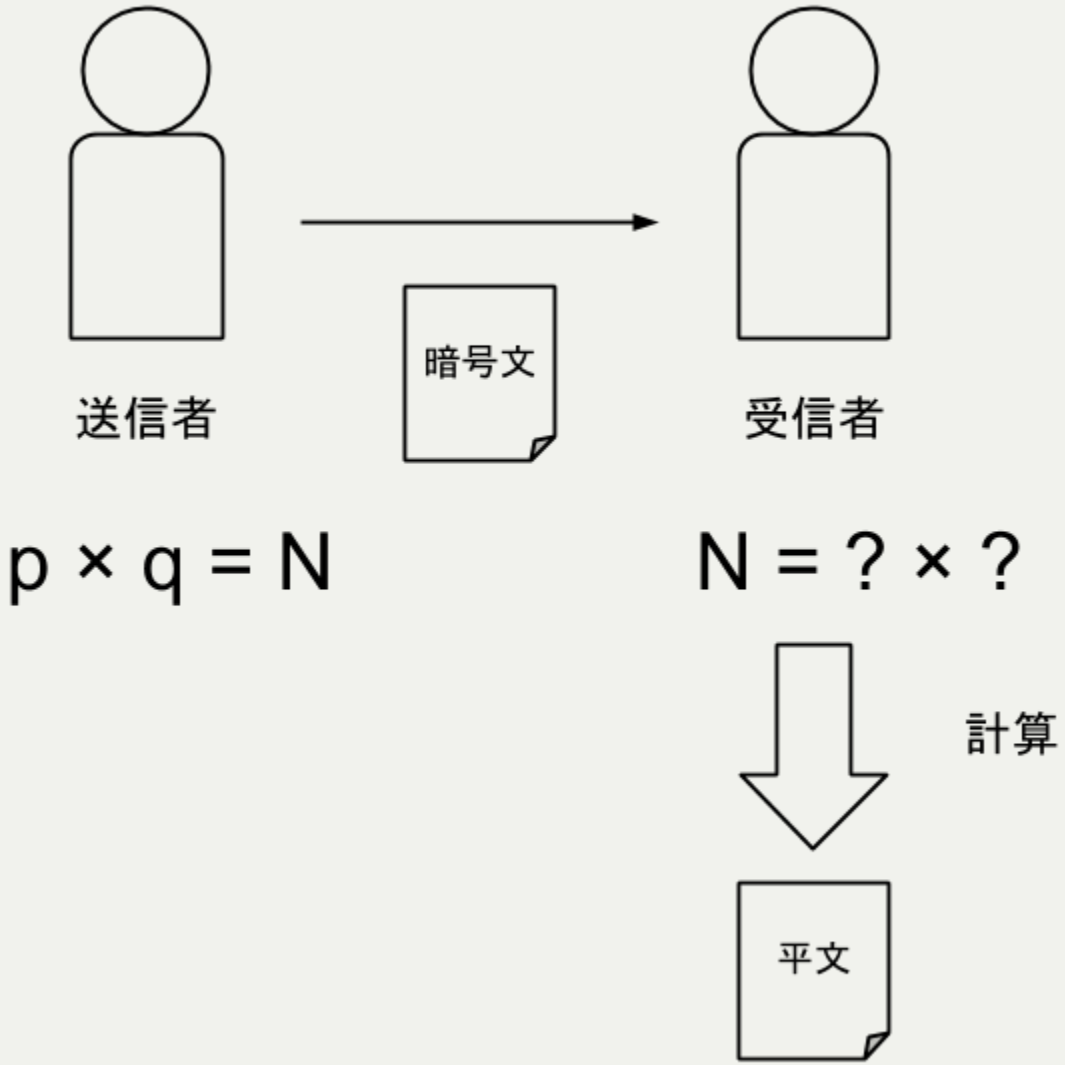
関連研究

- タイムリリース暗号
  - time-lock pazzle
  - trusted server
  - pairing

Time-lock Pazzle

- 数学的に計算時間がかかる問題を送信
  - 素因数分解など
- 受信者は計算することで復号可能
- 非現実的なシステム
  - 正確な復号時刻
  - 計算資源

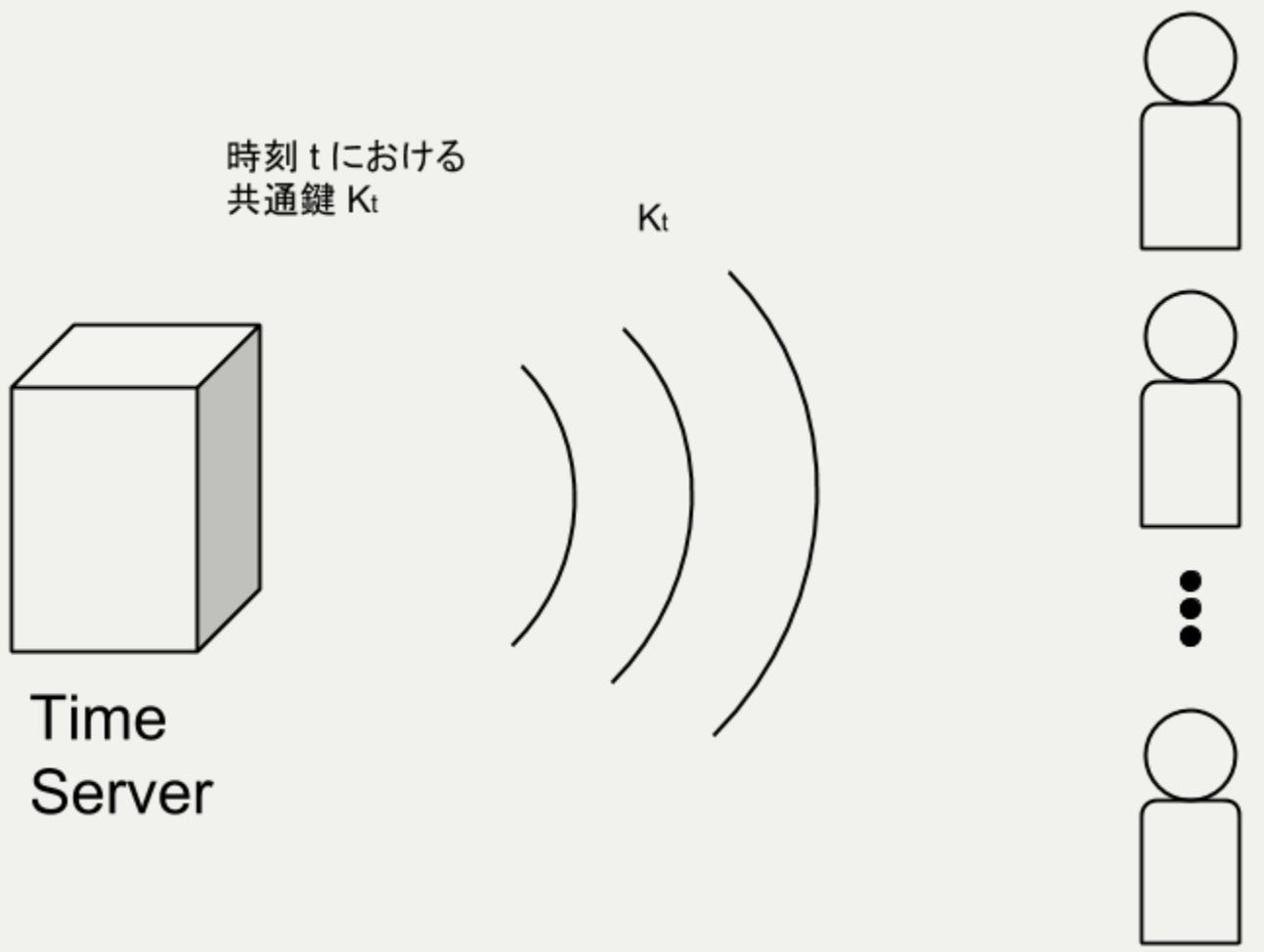
Time-lock Pazzle



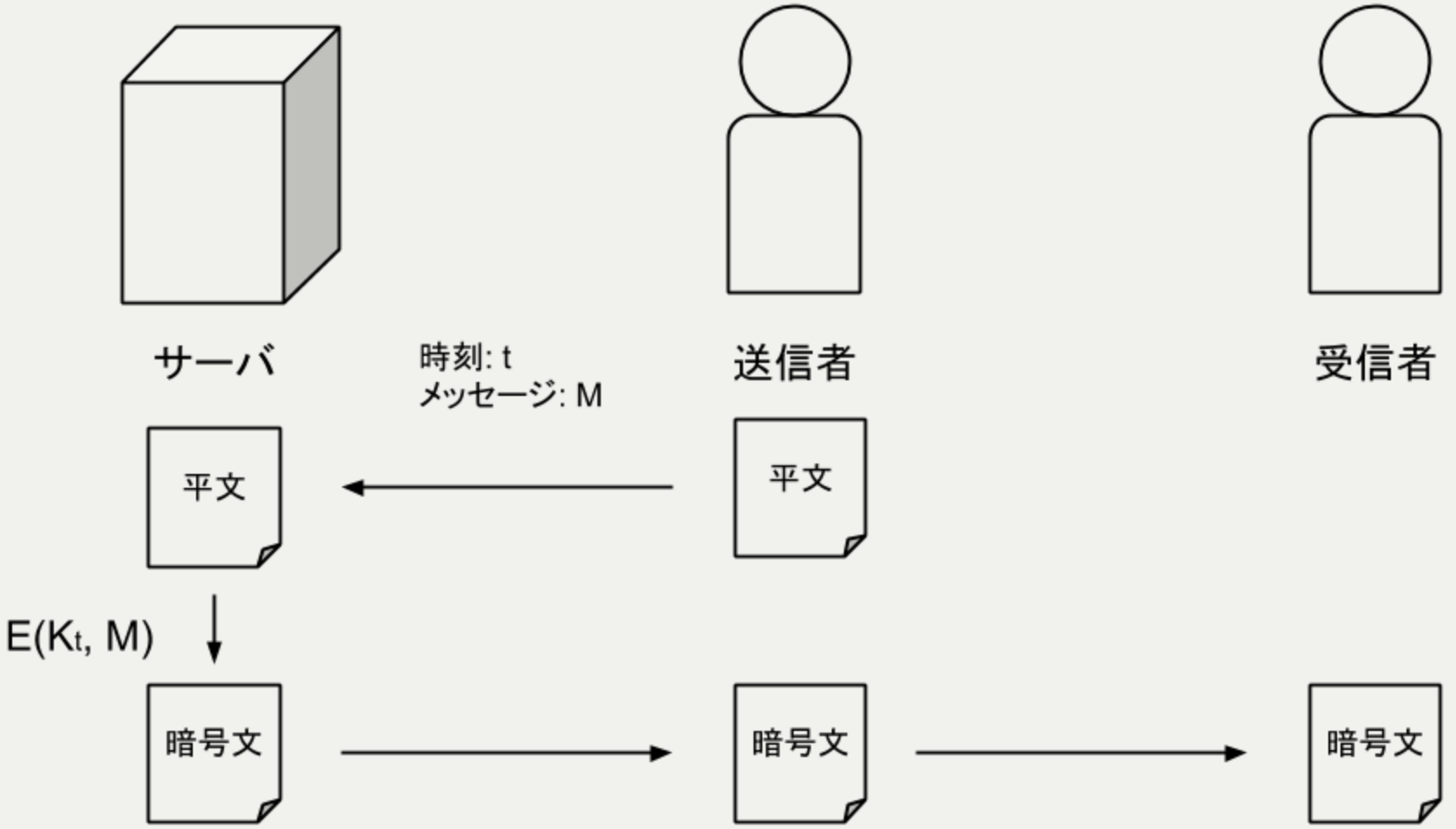
Trusted Server

- 公開鍵と共通鍵のペアを利用
- サーバを介してメッセージを暗号化
- タイムサーバ
  - 共通鍵暗号の鍵を定期的に送信

Trusted Server



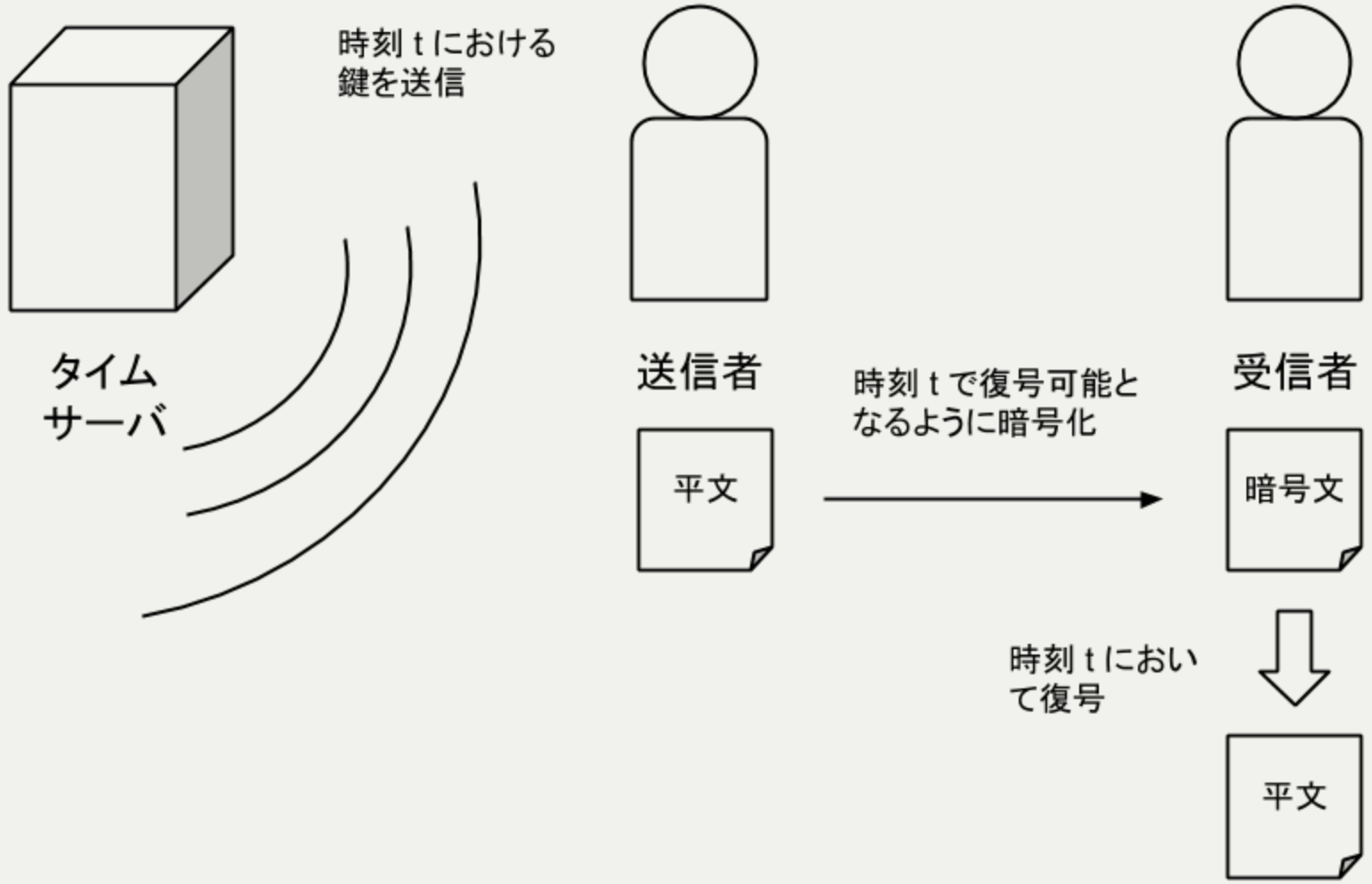
Trusted Server



Pairing

- 楕円曲線上で定義される双線形写像
  - 楕円曲線上の2点から有限体の元へ写す
- 送信者とタイムサーバとの間でやりとりを一度行う
- スケーラビリティと匿名性と言う点で優れている

Pairing


時刻 t における
鍵を送信
タイム
サーバ
送信者
受信者
時刻 t で復号可能と
なるように暗号化
平文
暗号文
時刻 t におい
て復号
平文

研究手段

- ペアリングを用いたタイムリリース暗号
- セキュリティパラメータの決定
- タイムサーバ/クライアントの構築
- Pairingライブラリ
  - Tepla
  - PBC

研究経過

- Pairingの学習
- タイムリリース暗号の学習
- TeplaやPBCの習得

まとめ

- デジタルコンテンツの普及
- デジタルコンテンツの事前配信の需要があるのでは
  - サーバの負荷軽減
  - ユーザの負担を解消
- pairingを利用したタイムリリース暗号

参考文献

- Chan, AC-F., and Ian F. Blake. "Scalable, server-passive, user-anonymous timed release cryptography." 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05). IEEE, 2005.
- 光成 滋生, "クラウドを支えるこれからの暗号技術." 秀和システム, 2015