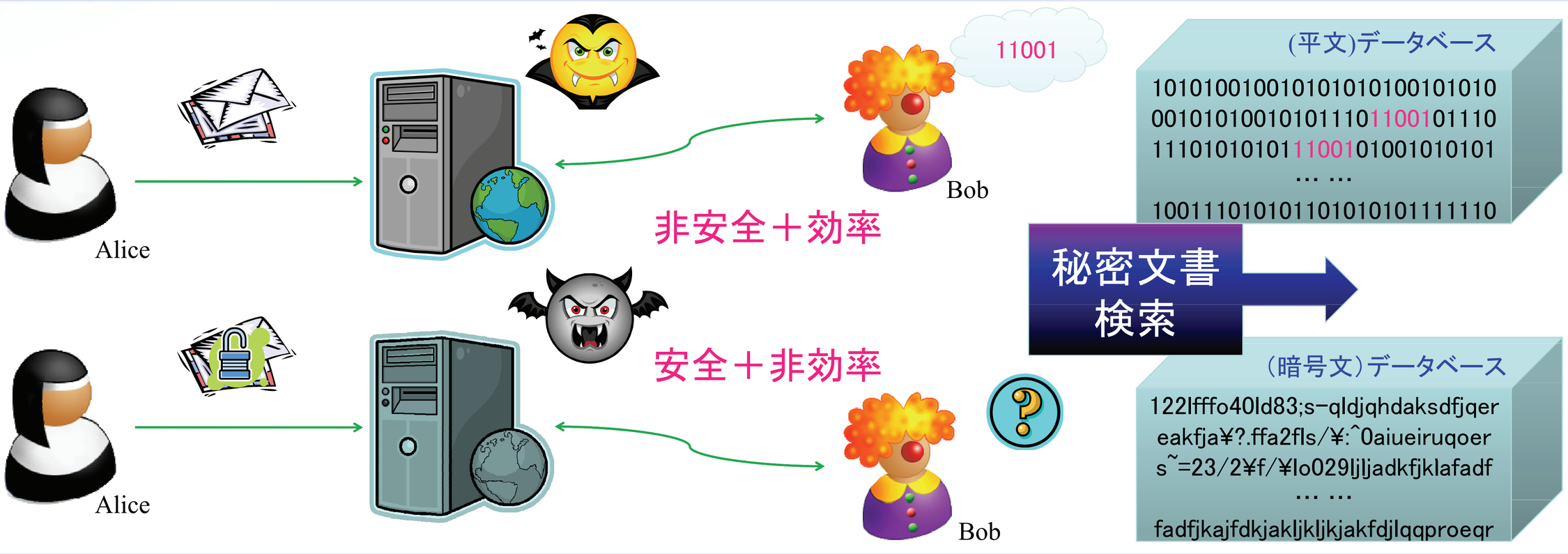
情報セキュリティ研究センター
Research Center for Information Security
サイ　ヨウ（Cui Yang）

効率的な検索可能ハイブリッド暗号方式

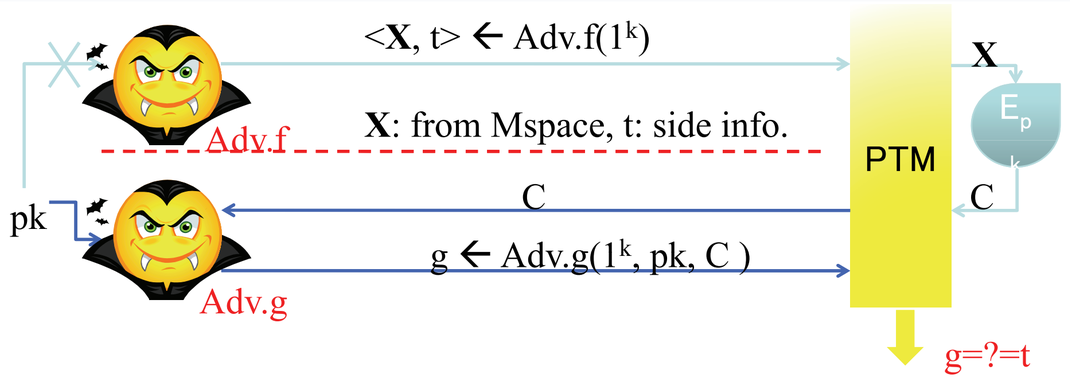
研究概要：顧客管理やきめ細かなサービスを提供する上で、大規模データベースの管理は必要不可欠となっている。一方、個人情報の漏えい防止やプライバシー保護の観点から、データの暗号化も必要となっているが、データの暗号化はデータベースの高度な機能をそぎ落とすという問題点がある。本研究では、データ保護と効率的な検索機能の両立を可能とするハイブリッド暗号方式の研究を行う。



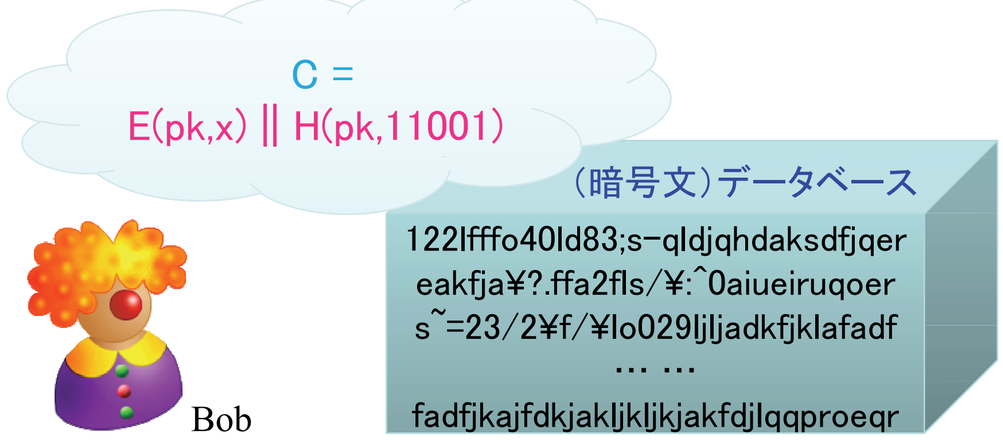
Q. なぜ暗号化されたデータを検索するのが難しい？
A. 暗号化アルゴリズムはランダムに暗号文を出力するため、Bobが暗号文を予測できない。
→ では、ランダムでなく、確定論的な暗号 (Deterministic Encryption)を使用すれば、どうでしょう？
CRYPTO　2007で、Bellareらが提案した。

Q. 安全性定義は妥当か？
A. 暗号の強秘匿性定義とよく似っている。
平文空間のMin Entropyが十分であれば、
暗号文のプライバシーが保証される。

定義 →



確定論的な暗号を用いて、安全＋効率検索ができる



本研究の貢献：CRYPTO 2007論文では、LPのハイブリッド暗号が構成できなかったが、我々の提案によって、初めてLPのハイブリッド暗号を提案した。

Q. なぜハイブリッド暗号？
A. 長いメッセージによく使用される。
Q. なぜLength-Preserving（LP）?
A. 通信オーバーヘッドが最少、効率がいい

Deterministic Encryption　　Deterministic Encryption
LP $E_{pk}(X_1)$ || $H(pk||X_1)$ ⇨ EaH, ¬LP
e.g. RSA-DOAEP

Deterministic Encryption　SKE　Deterministic ハイブリッド暗号
LP $E_{pk}(X_1)$ || LP $E_{sk=H(pk||X_1)}(X_2)$ ⇨ LP

National Institute of
Advanced Industrial Science
and Technology
AIST

Research Center for
Information Security

効率的な検索可能ハイブリッド暗号方式

セキュリティ基盤技術研究チーム
サイ　ヨウ　(Cui Yang)

研究の背景

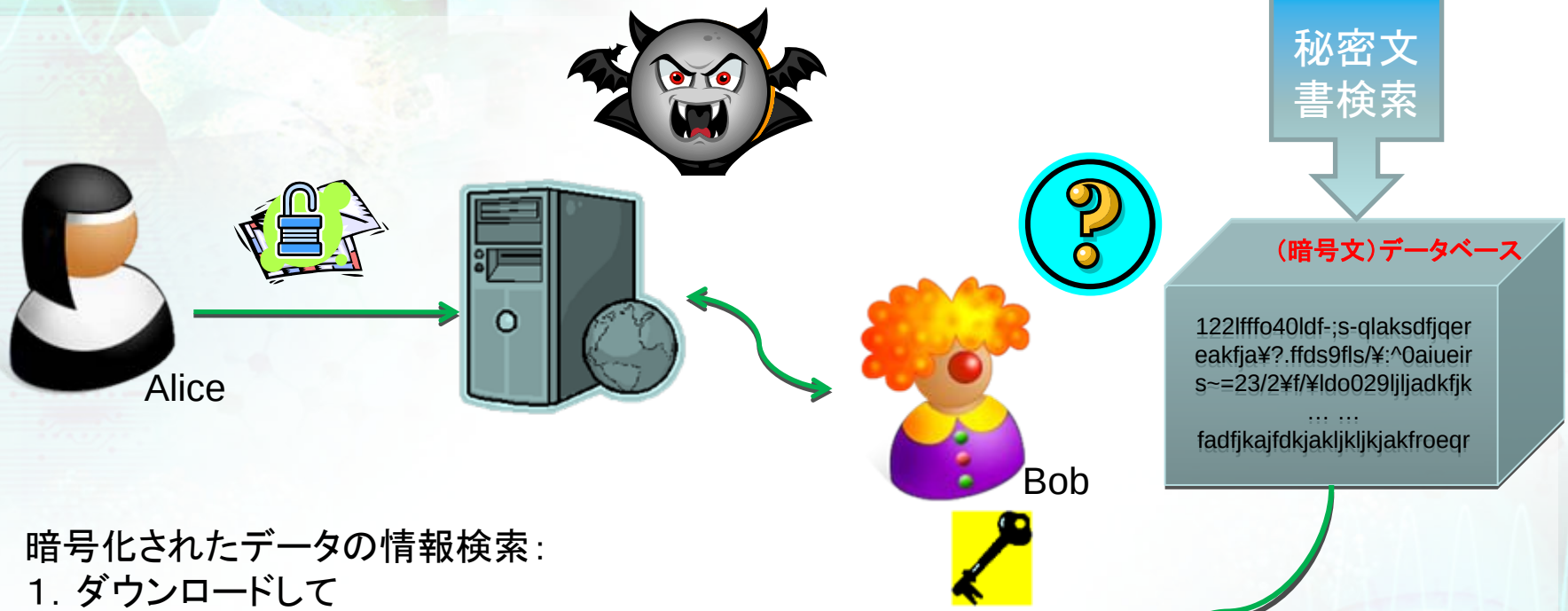
Webメールやアウトソーシングサービスなどの普及に伴い、データベースの管理者が不十分な管理を行ったり、データを悪用したり等の問題が生じる。
例：2004年、OOBBの顧客情報漏洩事件では、被害総額OO億円を超えた。

“広告や関連情報を表示する際に、電子メールの内容を人間がチェックすることはありません。” … …

CM リンク:
- •学校
- •セミナー
- •… …

情報検索：
非安全＋効率

既存の問題点



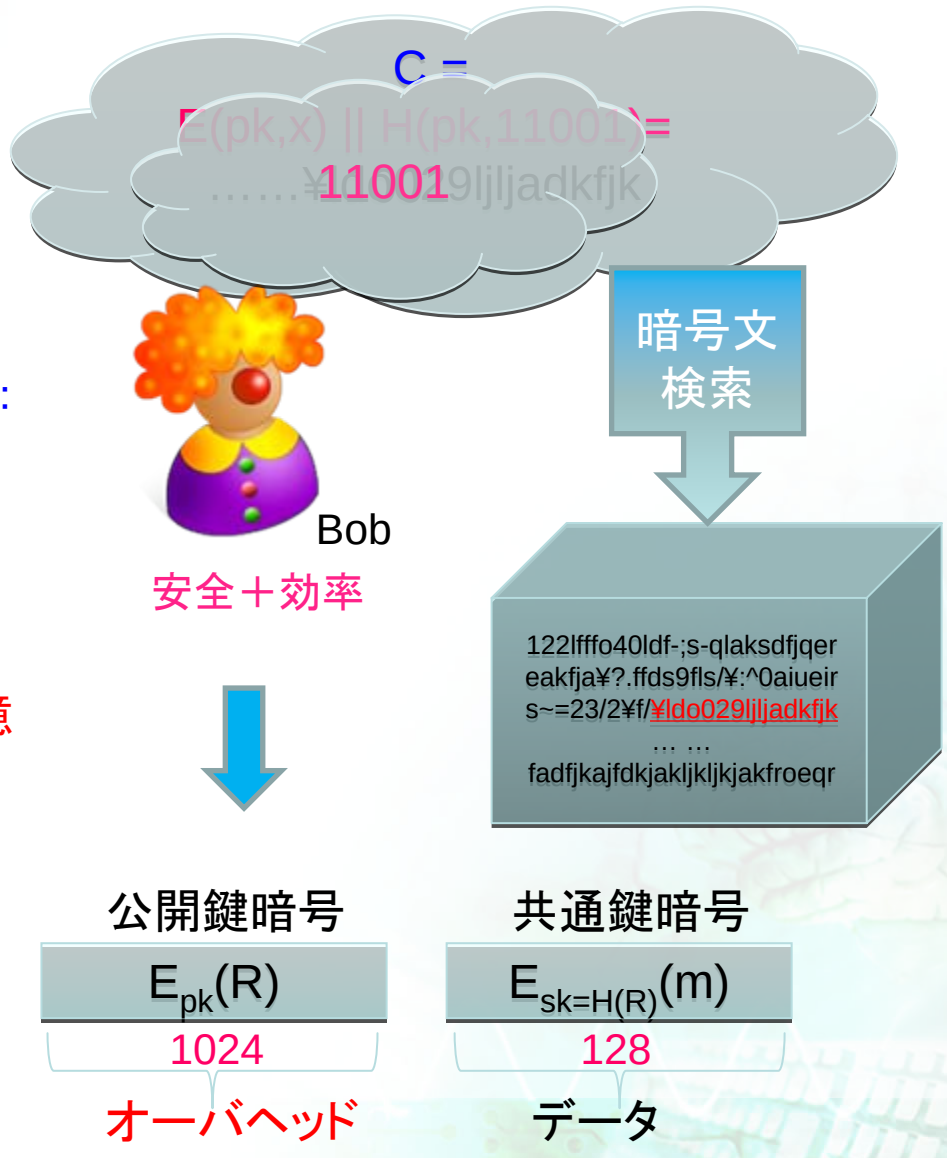
暗号化されたデータの情報検索:
1. ダウンロードして
2. すべて復号して、調べる

暗号化されたデータの情報検索(最近):
PEKS (Public-key Enc. w/t. Keyword Search)
1. 事前に用意した index だけが検索できる
2. index に対応する token をサーバに投げて
3. サーバがすべての index をはかる

本研究のモチベーションと関連研究

“Deterministic Encryption （DE)”
国際会議Crypto 2007, Bellareらの提案:

1. 初めての安全、かつ効率的に検索できる公開鍵暗号方式を提案した。
2. 一般的に使用されるハイブリッド暗号（HE)として構成した場合、大きい記憶容量が必要になる。



National Institute of Advanced Industrial Science and Technology AIST

提案方式：ハイブリッド暗号-最適の結果

Research Center for Information Security

DE　　ハッシュ関数

LP $E_{pk}(X1)$ || $H(pk||X1)$ ⇒ ¬LP EaH

e.g. RSA-DOAEP　　オーバヘッド

DE　　共通鍵暗号

LP $E_{pk}(R)$ || LP $E_{sk=H(R)}(X2)$ ⇒ ¬LP HE

オーバヘッド

DE　　共通鍵暗号

LP $E_{pk}(X1)$ || LP $E_{sk=H(pk||X1)}(X2)$ ⇒ LP HE

通信コストの比較	DE [BBN'07] (EaH)	DE [BBN'07] (HE)	**Ours**
メッセージ オーバヘッド	128 bits	1024 bits	0