なまけもの暗号

安永 憲司

金沢大学

第6回公開鍵暗号の安全な構成とその応用ワークショップ

2013.3.19

なまけもの

「木から降りたくない」

なまけもの

「何もしたくない」

安全性

全体の安全性　＝　最も弱い部分の安全性

世の中全体の安全性　＝　  　による安全性

安全性への影響

- 自身への影響は仕方ない

- 他者への影響が問題

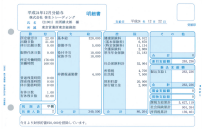
ケーススタディ：給与明細の電子配布

- K 沢大学では給与明細配布を電子化

- 内容を秘匿するため公開鍵暗号を利用

ケーススタディ：給与明細の電子配布

暗号化担当係


明細１　明細２　明細３　・・・

pk_1　pk_2　pk_3　・・・

安全な暗号化のためには
いい乱数を使うこと

情報セキュリティの専門家

M 保教授

pk_1　pk_2　pk_3　・・・

職員１　職員２　職員３　・・・

いい乱数？

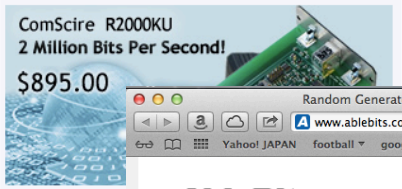
Comscire, World's Best True Random Number Generato

comscire.com

Yahoo! JAPAN football google research dictionary travel others

World's Best True Random Number Generators

True Random Number Generators (TRNGs) are at the heart of all modern computer applications requiring the highest levels of data security and complete confidence in the fairness of random selections or drawings. Hardware random generators use a physical source of randomness that is fundamentally unpredictable. ComScire sells the world's highest-quality, most reliable TRNGs based on our patented and exhaustively-tested technology proven for over 17 years. Our worldwide customers include national and state lotteries, online gaming companies, gaming systems manufacturers, and military and civilian security agencies.



True Random N
for Critical Gam
• Windows 32 /
• USB 2.0 Full-S
GUARANTEED t

Buy Now

True Rand

www.protego.se

Yahoo! JAPAN football google research dictionary travel others

ENCRYPTION Embedded Systems
TRNG Technology

Company Shop Products What's New Site Map Contact Protego

True Random Number Generators

New Product Announcement

SG100 EVO-USB

USB Connectivity with proven security

Today Protego is proudly announcing it's newest product offering, **SG100 EVO-USB**. Based on a great demand from our customers we have taken the proven SG100

量子物理型の真性乱数発生器・ IDQ-QUANTIS-USB _アルゴ

www.argocorp.com/compo/IDQ/IDQ_USB.html

Yahoo! JAPAN football google research dictionary travel others

量子物理型・真性乱数発生器USB
AR-QUANTIS-USB

●仕様 ●価格 ●ドキュメント&資料

ツイート 5 いいね！ 0 B! 1

今のコンピューターから得られる乱数は真の意味での一様な乱数ではありません。IDQ-Quantisは、真性乱数を生成するため量子物理を使用し、量子が本質的にランダムであるという原則に基づく真の乱数を提供します。

AR-QUANTIS-USBは、素量光学プロセスを利用する物理的な乱数発生器ボードです。光子(光粒子)は、半透明の鏡にひとつずつ送られて検出され、排反事象(反射/透過)は「0」-「1」ビット値に関連づけられます。AR-Quantis-USBは、ランダムビットストリームの" Failure" & "Disabling" を確実に検出するために連続的にモニターされます。USBインタフェイスを採用し4Mbit/秒の高速ランダムストリームを提供します。GUIとAPIも支援されコンピューター/サーバーに接続して使用することができます。

Random Generator for Excel 2013-2003 – generate random numbers, passwords, strings, dates.

www.ablebits.com/excel-random-generator/index.php

Yahoo! JAPAN football google research dictionary travel others

AbleBits HOME PRODUCTS DOWNLOADS PURCHASE SUPPORT

Random Generator for Microsoft Excel

Generate random numbers, passwords or strings in Excel 2010, 2013 - 2003

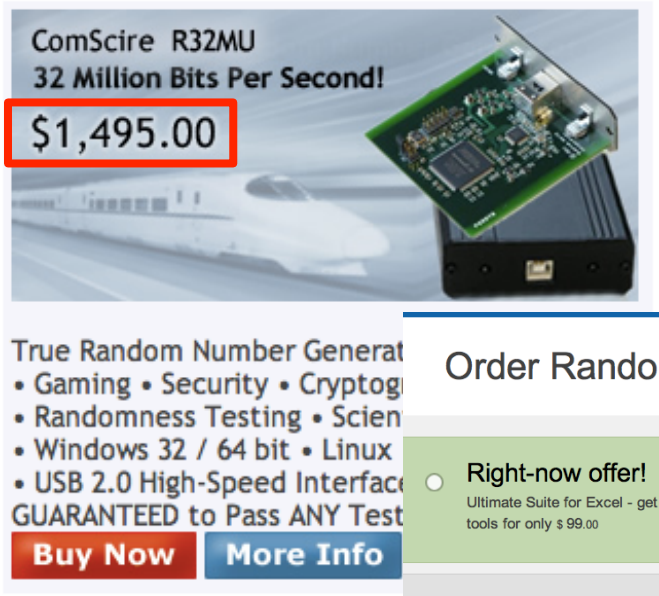
With **Random Number Generator** for Excel you can easily fill a range of cells with any random data. In just a couple of clicks you can:

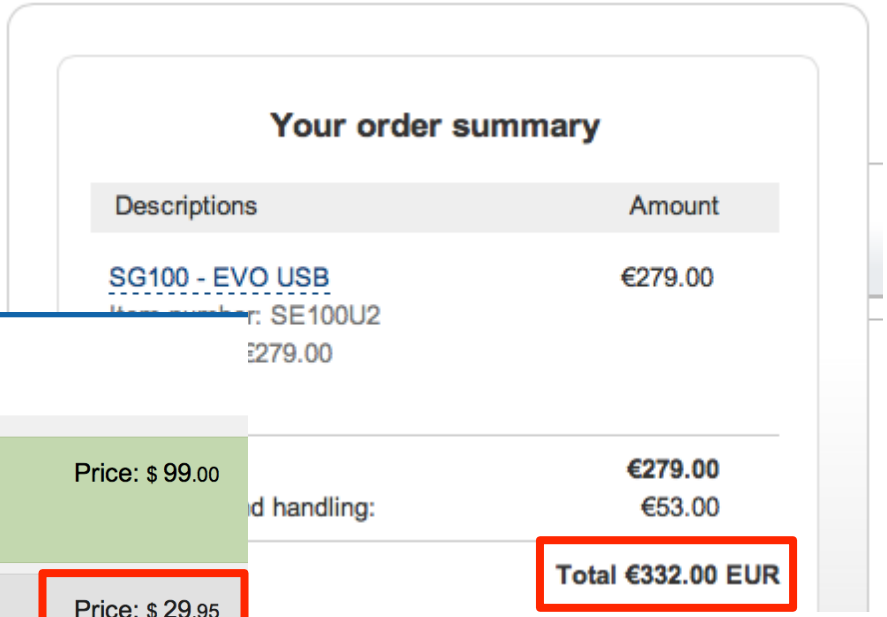
- Generate unique random numbers, integers, dates, booleans, reals
- Generate random passwords of a given length with different charsets (e.g. A - Z, 0 – 9) or special symbols
- Take a random sample of your data set
- sheets with names taken from the cell contents

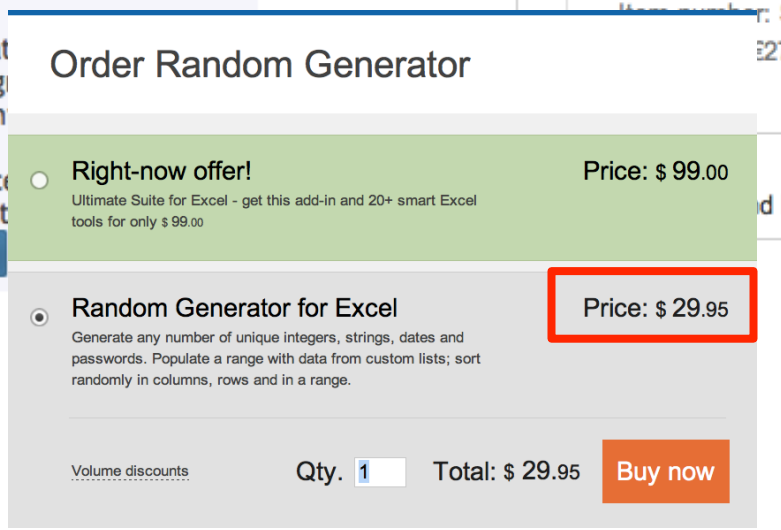
20+ Excel tools in one pack
Save 60% off

Take your Excel productivity to a new level

いい乱数は高価







価格

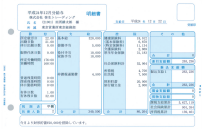
商品コード（型番）	内容	価格（税別）
AR-QUANTIS-USB-4M	量子物理型・真性乱数発生器 USB I/F ソフトウェア付	￥169,000.-

ケーススタディ：給与明細の電子配布

暗号化担当係

予算あんま残ってないんだよなぁ


明細１


明細２


明細３

・・・

pk_1　pk_2　pk_3　・・・

職員１

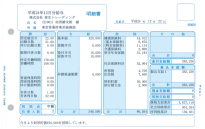
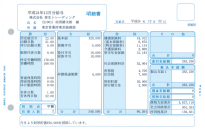
職員２

職員３

・・・

ケーススタディ：給与明細の電子配布

暗号化担当係

明細１　明細２　明細３　・・・

pk_1　pk_2　pk_3　・・・

ちょっと待てよ。
給与明細はオレの個人情報じゃない。

別に安全に送らなくても
いいじゃん！

職員の望む安全性は
達成されなかった！

乱数部分を 0･･･0
にして暗号化

c_1　c_2　c_3　・・・

職員１　職員２　職員３　・・・

教訓

公開鍵暗号では、
なまけものの行動が他者の安全性を脅かす

本研究

なまけものが実行しても安全な公開鍵暗号

研究成果

- 「なまけもの」という概念を導入

- なまけもの公開鍵暗号
  - 安全性の定式化
  - 不可能性
  - 安全な方式の提案

なまけもの

(1) ある状況では安全性に興味がなくなる

(2) 正直者のような行動をとるが、
なるべくコストのかかる行動はしたくない

- 正直者のような行動：
  プロトコルに従っている可能性がある行動
  - 例．乱数部分を固定系列に変更
- コストのかかる行動：
  何がコストかは、なまけものの性質に依存
  - 例．乱数生成（計算がコスト）
    ラウンド数増加（時間がコスト）

なまけもの公開鍵暗号

- 送信者 S と受信者 R がなまけもの
- なまけものは

  (1) 秘匿したいメッセージ集合 M_S, M_R をもち

  (2) 乱数生成をコストと考える

  - 乱数として以下を選択可能
    1. 高コストの真性乱数（Good randomness）
    2. コストゼロの固定系列（Bad randomness）

目標：$m \in M_S \cup M_R$ に対する秘匿通信

安全性の定式化

- 送信者、受信者、敵による三者間ゲームを定義

- なまけものの利得関数を定義

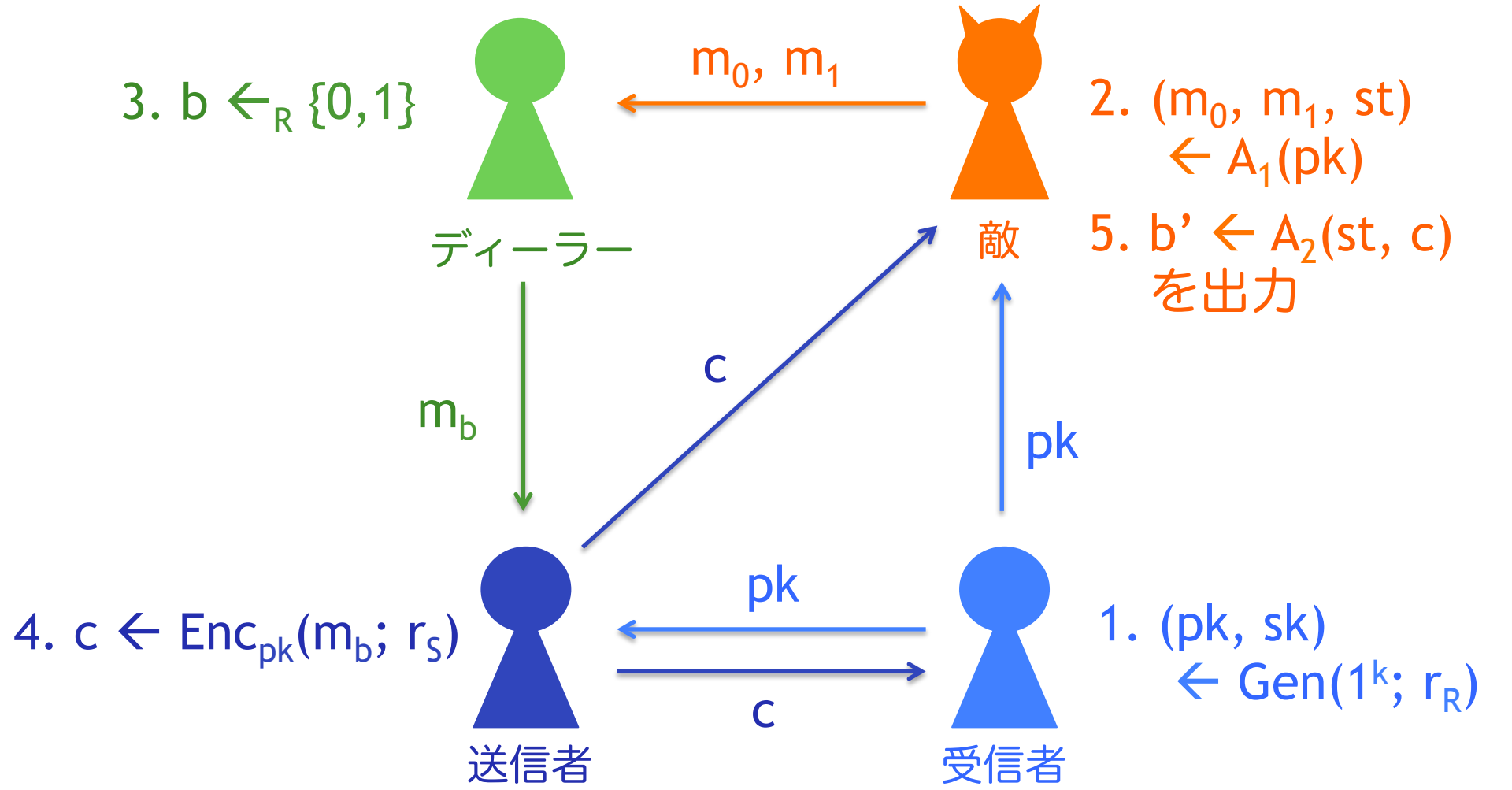
暗号方式が安全

⇔

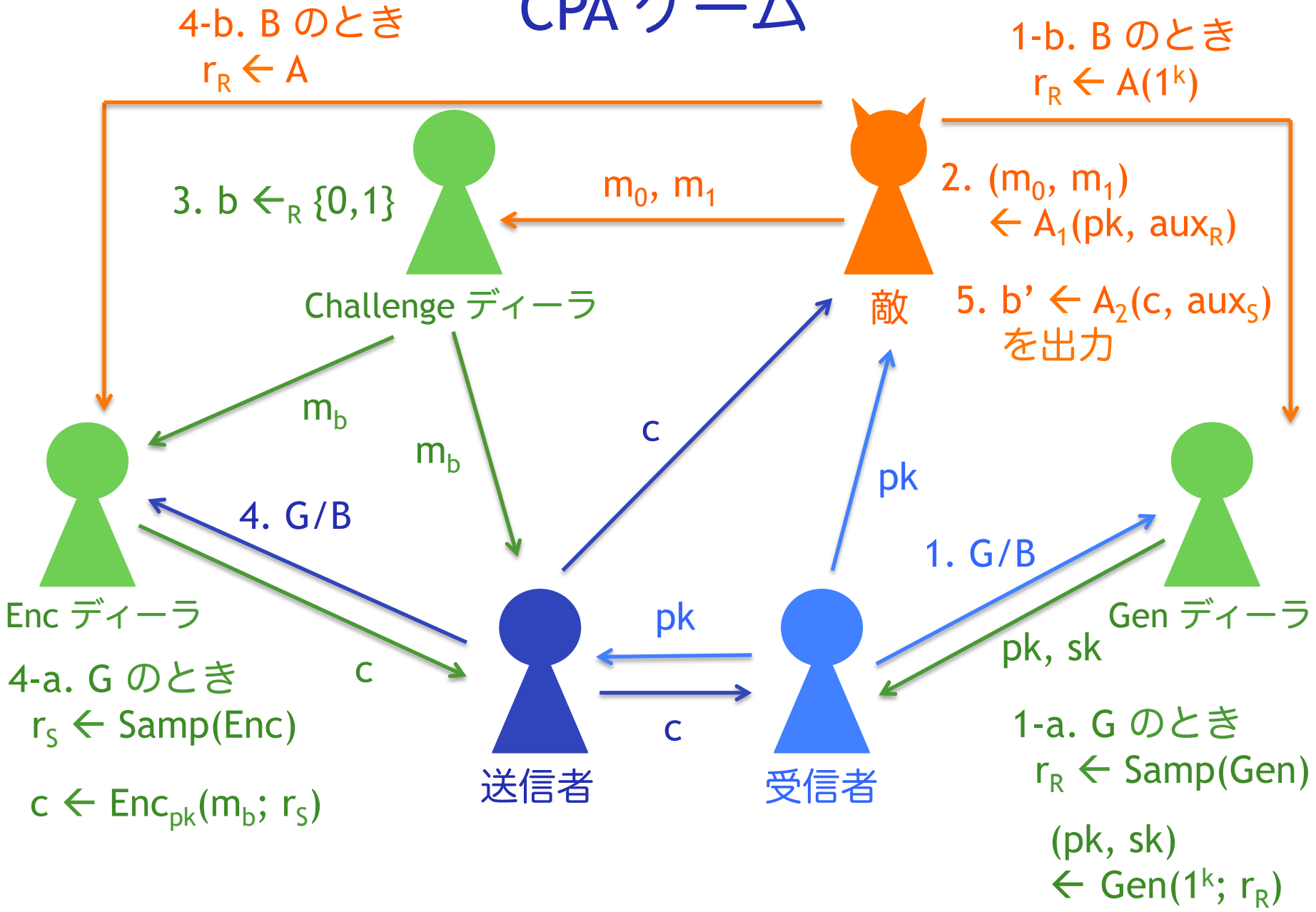
(1) なまけものにとって
その方式に従うことが合理的

(2) 従っていれば秘匿通信を実現

通常の CPA ゲーム


3. b ←R {0,1}
m0, m1
2. (m0, m1, st) ← A1(pk)
ディーラー
敵
5. b' ← A2(st, c) を出力
mb
c
pk
4. c ← Encpk(mb; rS)
pk
c
1. (pk, sk) ← Gen(1k; rR)
送信者
受信者

CPA ゲーム


4-b. B のとき
$r_R \leftarrow A$
1-b. B のとき
$r_R \leftarrow A(1^k)$
3. $b \leftarrow_R \{0,1\}$
m_0, m_1
2. $(m_0, m_1) \leftarrow A_1(pk, aux_R)$
Challenge ディーラ
敵
5. $b' \leftarrow A_2(c, aux_S)$ を出力
m_b
m_b
c
pk
4. G/B
1. G/B
Enc ディーラ
Gen ディーラ
pk
c
pk, sk
4-a. G のとき
$r_S \leftarrow Samp(Enc)$
$c \leftarrow Enc_{pk}(m_b; r_S)$
c
送信者
受信者
1-a. G のとき
$r_R \leftarrow Samp(Gen)$
$(pk, sk) \leftarrow Gen(1^k; r_R)$

CPA ゲームについて

- 実際は、一般化して定義
  - 送信者も Gen を実行
  - Enc は対話も可

- ゲームの出力は
  $Out = (Win, Val_S, Val_R, Num_S, Num_R)$
  - $Win \in \{0,1\}$,　$Win = 1 \Leftrightarrow b = b'$
  - $Val_w \in \{0,1\}$,　$Val_w = 1 \Leftrightarrow m \in M_w$
  - Num_w : $w \in \{S, R\}$ が Good を選択した回数

利得関数

- 出力 Out = (Win, Val_S, Val_R, Num_S, Num_R) のとき

$$u_w(Out) = (-\alpha_w) \cdot Win \cdot Val_w + (-\beta_w) \cdot Num_w$$

  - $\alpha_w, \beta_w > 0$ はある固定実数値
  - $\alpha_w / 2 > q_w \cdot \beta_w$ と仮定（ q_w : Num_w の最大値 ）
    - Good のコストで $\alpha_w / 2$ の利得（安全性）を得る価値あり

- 戦略の組 (σ_S, σ_R) に従ったときの利得

$$U_w(\sigma_S, \sigma_R) = \min E[u_w(Out)]$$

  - min はすべての敵, メッセージ空間 M_S, M_R でとる

なまけもの公開鍵暗号の安全性

- 公開鍵暗号方式 Π、戦略の組 (σ_S, σ_R) に対し、$(\Pi, \sigma_S, \sigma_R)$ が （狭義）Nash 均衡付き安全

1. (σ_S, σ_R) が (狭義) Nash 均衡
2. (σ_S, σ_R) に従ったとき、
   任意の敵、メッセージ空間 M_S, M_R に対して

$$\Pr[\ \mathrm{Win} \cdot (\mathrm{Val}_S + \mathrm{Val}_R) \neq 0\ ] \leq 1/2 + \mathrm{negl}(k)$$

ゲームの解概念

相手が従っているとき、
自分も従えば利得が最大化

- (σ_S, σ_R) が Nash 均衡：
  - 任意の $w \in \{S, R\}$, σ_w' に対して、

$$U_w(\sigma_S^*, \sigma_R^*) \leq U_w(\sigma_S, \sigma_R) + negl(k)$$

ただし、$(\sigma_S^*, \sigma_R^*) = (\sigma_S', \sigma_R)$ if $w = S$
(σ_S, σ_R') otherwise

相手が従っているとき、
従わないと利得が下がる

- (σ_S, σ_R) が 狭義 Nash 均衡：
  1. (σ_S, σ_R) が Nash 均衡
  2. 任意の $w \in \{S, R\}$, $\sigma_w' \neq \sigma_w$ に対して、

$$U_w(\sigma_S^*, \sigma_R^*) \leq U_w(\sigma_S, \sigma_R) - 1/k^c$$

ただし、c は定数

最初の考察（不可能性）

命題１．送信者が秘密鍵をもたない
→ Nash 均衡付き安全でない

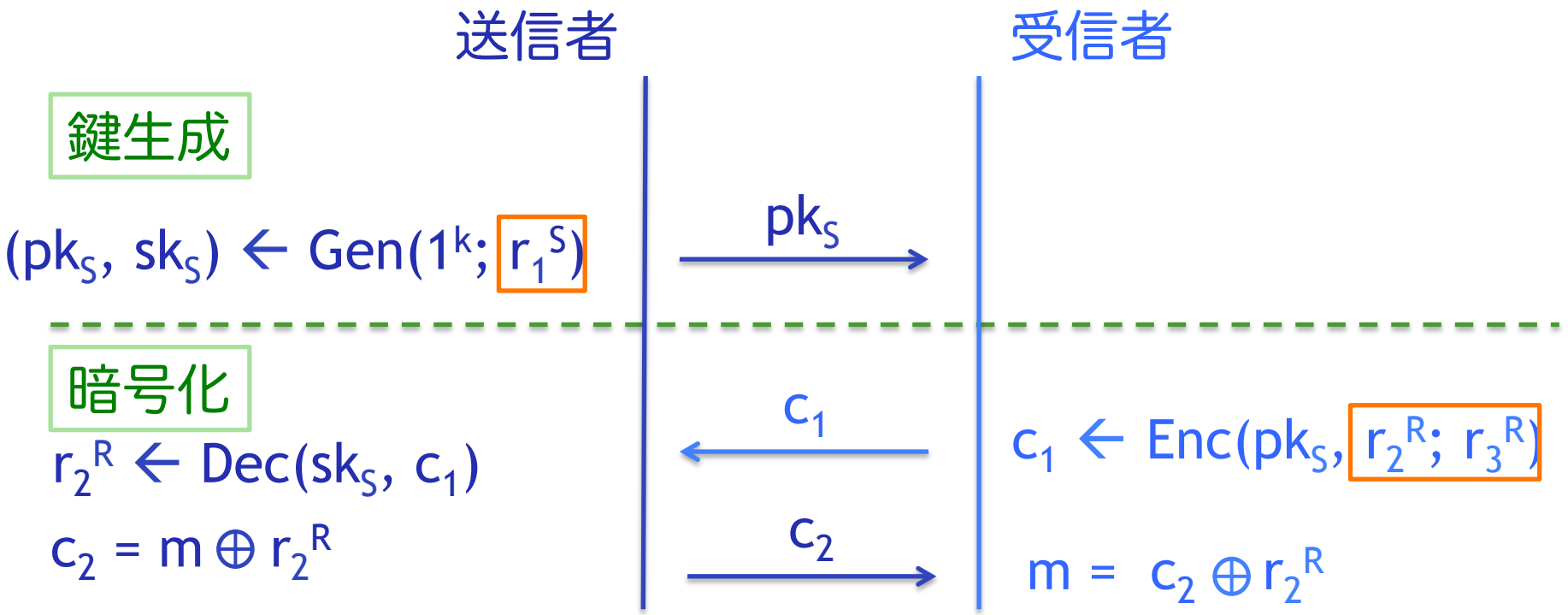
- 証明：$m_b \in M_R \setminus M_S$ のとき、送信者は Bad を選択
  → 敵は送信者の入力について
  m_b 以外すべて知っているので勝てる

命題 2. Enc が 1ラウンド
→ Nash 均衡付き安全でない

- 証明：$m_0 = (m, m)$, $m_1 = (m, m')$, $m \neq m'$,
  $m, m' \in M_R \setminus M_S$ を考える
  → 送信者は Bad を選択
  → 敵は同じ乱数で暗号化しておけば勝てる

安全な公開鍵暗号（基本的な設定）

- 2ラウンド暗号方式 Π_{two}：
  - アイディア：暗号化の乱数を受信者が生成
    受信者は、乱数をちゃんと生成するしかない



2ラウンド暗号化方式 Π_{two}

- 戦略 (σ_S, σ_R):
  - σ_S：常に Good, σ_R：常に Good

定理 1. $(\Pi_{two}, \sigma_S, \sigma_R)$ は狭義 Nash 均衡付き安全

- Π_{two} の問題点：受信者が、$m \notin M_R$ であることを知っていると、安全でなくなる
  - メッセージの重要性を知っているという状況

受信者に付加情報がある場合

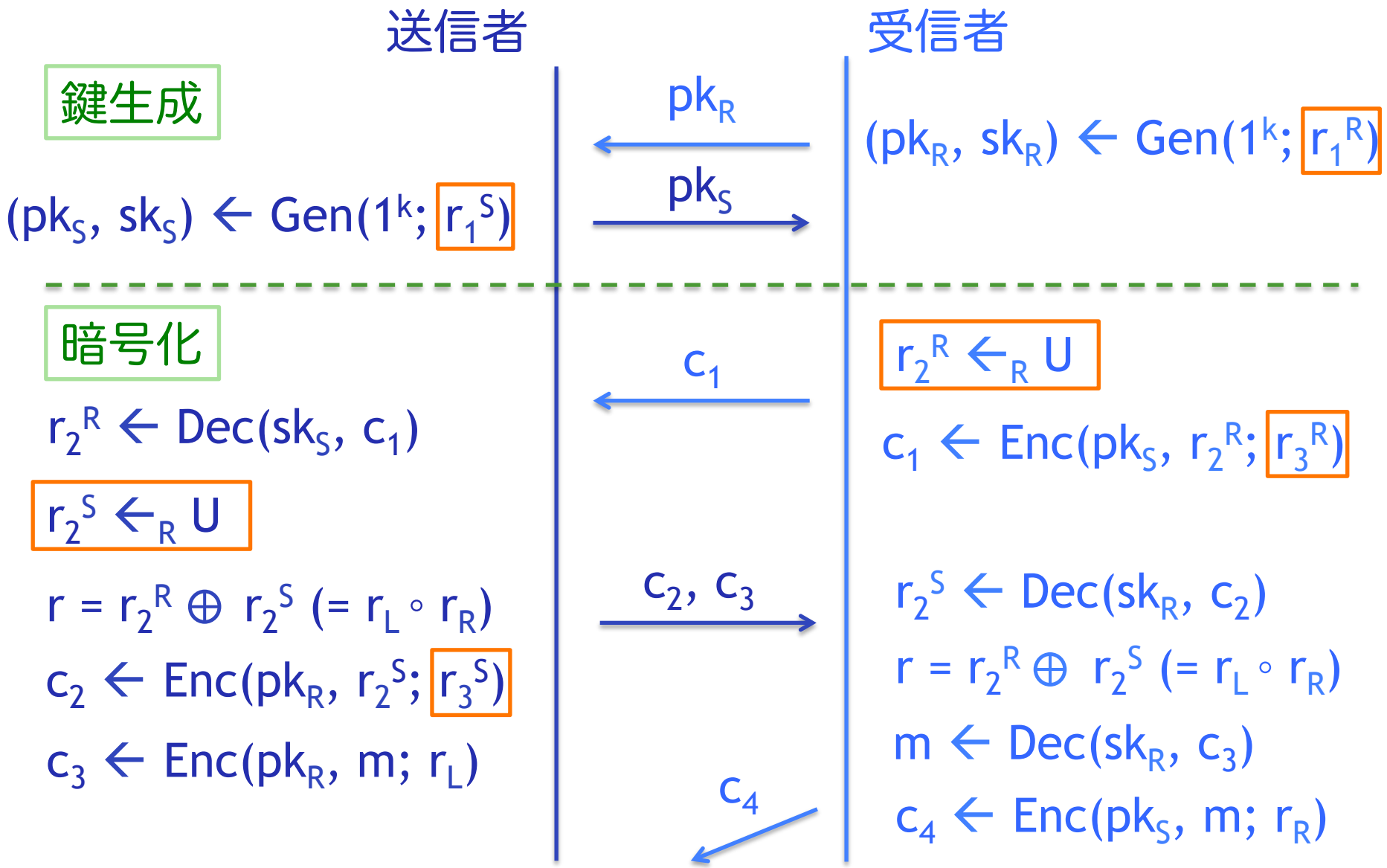
- ゲームを修正：受信者に Val_R を与えるか否かを敵が決める

- 3ラウンド暗号方式 Π_{three}

  アイディア：

  - 暗号化フェーズで鍵共有
    - どちらかが Good を使えば共有鍵も Good
  - 共有鍵を暗号化の乱数とする

3ラウンド暗号方式 Π_{three}



3ラウンド暗号方式 Π_{three}

- 戦略 (σ_S, σ_R):
  - σ_S : Gen は常に Good;
    Enc は $m \in M_S$ のとき Good, それ以外 Bad
  - σ_R : Gen は常に Good;
    Enc は、付加情報なし or $Val_R = 1$ なら Good,
    それ以外は Bad

定理 2. $(\Pi_{three}, \sigma_S, \sigma_R)$ は狭義 Nash 均衡付き安全

定理 2 の証明（1/2）

鍵生成（送信者）	鍵生成（受信者）	暗号化（送信者）	暗号化（受信者）	秘匿性
Good	Good	Good	-	✓
Good	Good	-	Good	✓
Bad	-	-	-	x
-	Bad	-	-	x

- 鍵生成がともに Good のとき
  $r = r_2^R \oplus r_2^S$ であり、どちらかが Good ならば r は Good
- 鍵生成で送信者が Bad
  → $m \in M_S \setminus M_R$ のとき、c_4 から m がわかる
- 鍵生成で受信者が Bad
  → $m \in M_R \setminus M_S$ のとき、c_3 から m がわかる

定理 2 の証明（2/2）

- 受信者が σ_R に従うと仮定
  - 送信者が σ_S に従わないとき

    (1) Gen で Bad → 秘匿でなくなり利得減

    (2) Enc で $m \in M_S$ のとき Bad

    → 秘匿でなくなり利得減

- 送信者が σ_S に従うと仮定
  - 受信者が σ_R に従わないとき

    (1) Gen で Bad → 秘匿でなくなり利得減

    (2) Enc で付加情報なし or $Val_R = 1$ のとき Bad

    → 秘匿でなくなり利得減

Π_{three} の問題点

- 送受信者ともに $m \in M_S \cap M_R$ と知っているとき
  どちらが Good を選ぶのか決まらない

送信者と受信者に付加情報がある場合

- ゲームを修正：送信者に Val_R を与えるか、
  受信者に Val_S や Val_R を与えるかを敵が決める

命題 3.
上記のゲームに対して、
異なる戦略ペア (σ_S, σ_R), (ρ_S, ρ_R) が存在し
ともに Π_{three} を狭義 Nash 均衡付き安全にする

(σ_S, σ_R)：送信者が Enc で Good
(ρ_S, ρ_R)：受信者が Enc で Good

命題 3 について

- 送受信者それぞれが、自身に高利得な方の戦略を選ぶと秘匿性が破られる

  → 両者によって最悪の結果

- 最悪な結果を避ける方法
  - 受信者は $m \in M_S \cap M_R$ と知ったとき、乱数部分をオールゼロにする
  - 送信者は、受信者の乱数をチェックし、オールゼロのときは Good を選択

非対話型の暗号方式

- 不可能性を避けることが必要

方式 1. 行動に対して仮定を追加した方式

方式 2. セットアップフェーズで対話を行う方式

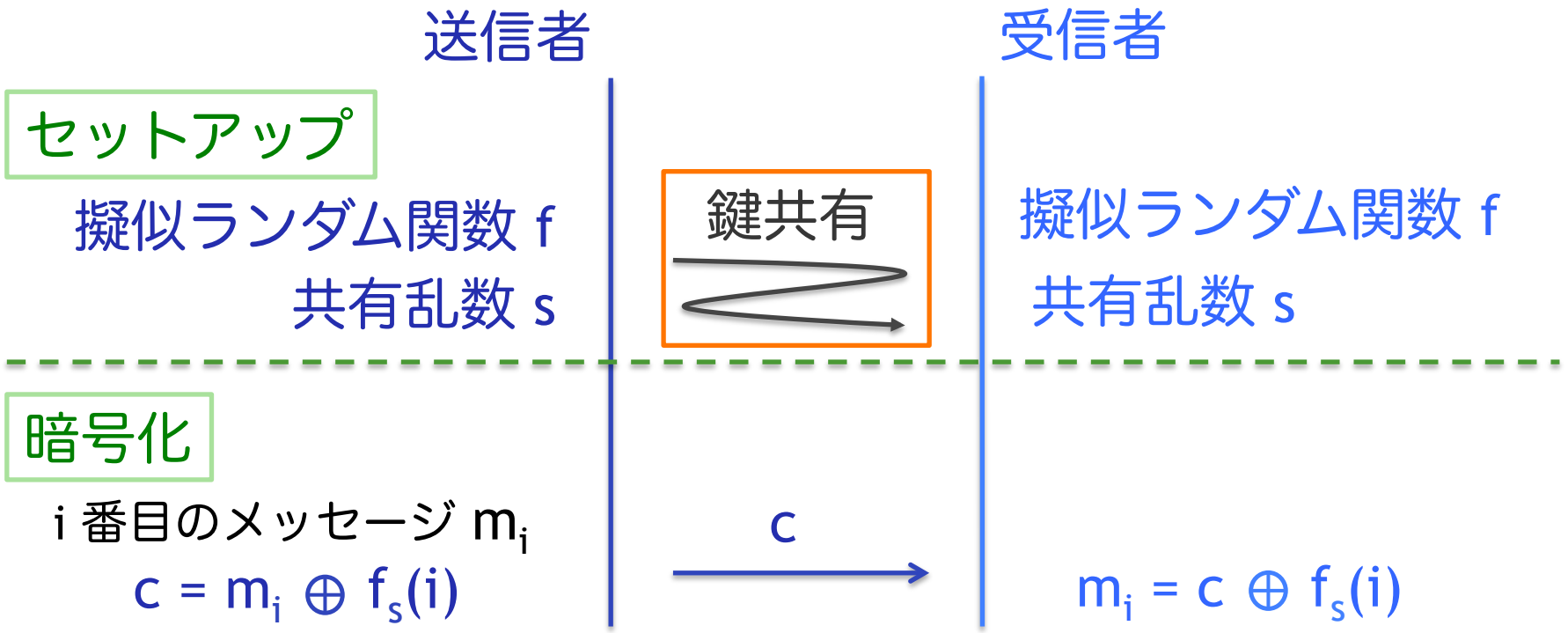
方式 1. 行動に対して仮定を追加した方式

追加仮定：秘密情報を敵に知られたくない

- Signcryption 方式において
  暗号文とその乱数から署名鍵を計算可能 → 安全
  - 送信者は署名鍵（秘密鍵）を
    知られたくないので Good を使う

方式 2.セットアップフェーズで対話を行う方式（送受信者間でカウンタを共有）

- 方式のアイディア
  - セットアップフェーズで乱数 s を共有
  - 暗号化での乱数として s を利用



まとめ

公開鍵暗号では、
なまけものの行動が他者の安全性を脅かす

- 研究成果
  - なまけものに対する安全性の定式化
  - 不可能性
  - 安全な方式の提案
- 今後の研究
  - Good/Bad だけでなく、より一般的な乱数情報源
  - 他の暗号プロトコルにおけるなまけものの影響

ゲーム理論
を利用

おしまい