情報通信を行なう際の要請

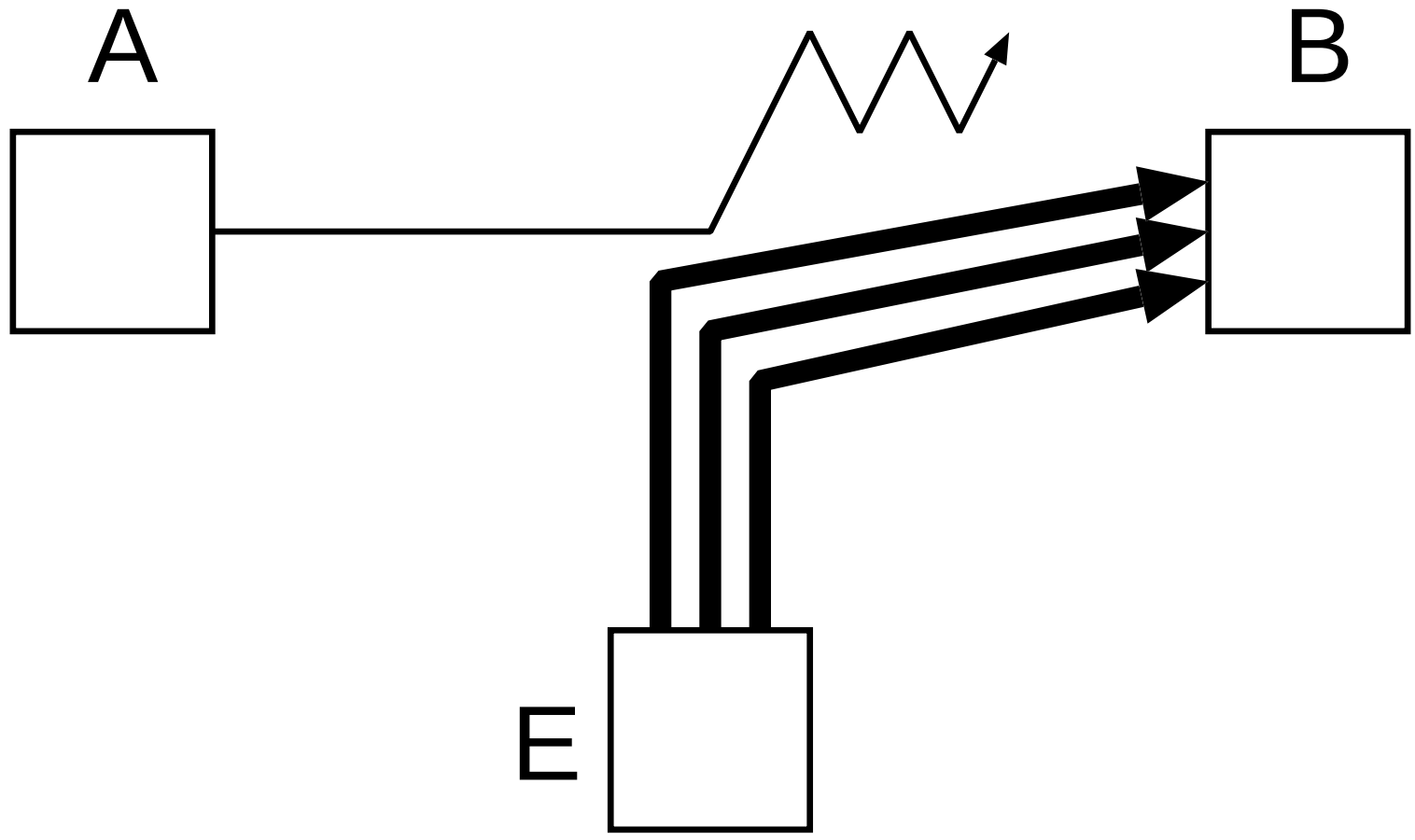
- 効率的に $\longrightarrow$ 情報理論
- 確実に $\longrightarrow$ 符号理論
- 安全に $\longrightarrow$ 暗号理論

安全な情報伝達を阻害するもの

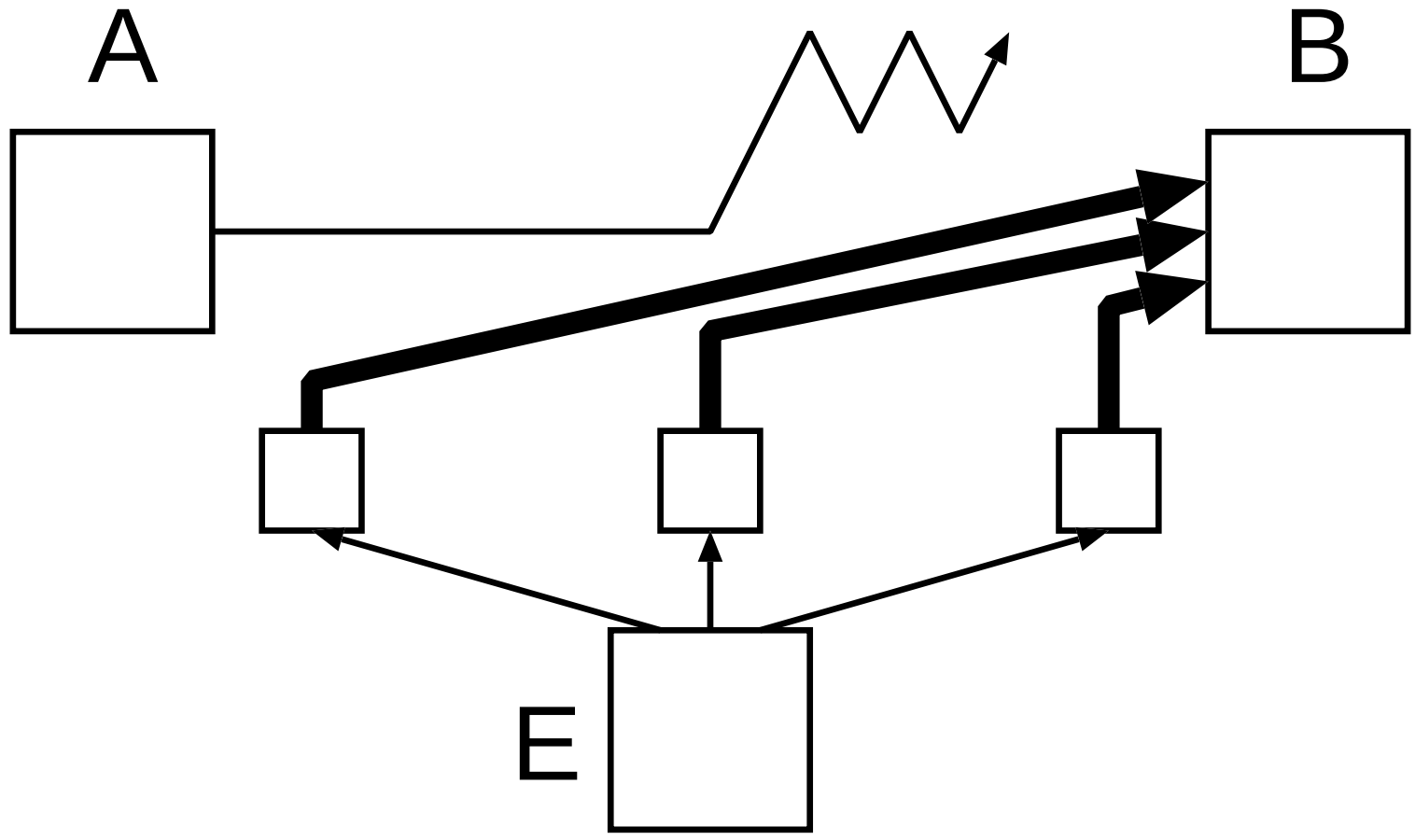
- 妨害 (DoS 攻撃など)
- 盗聴
- 改竄
- なり済まし

など

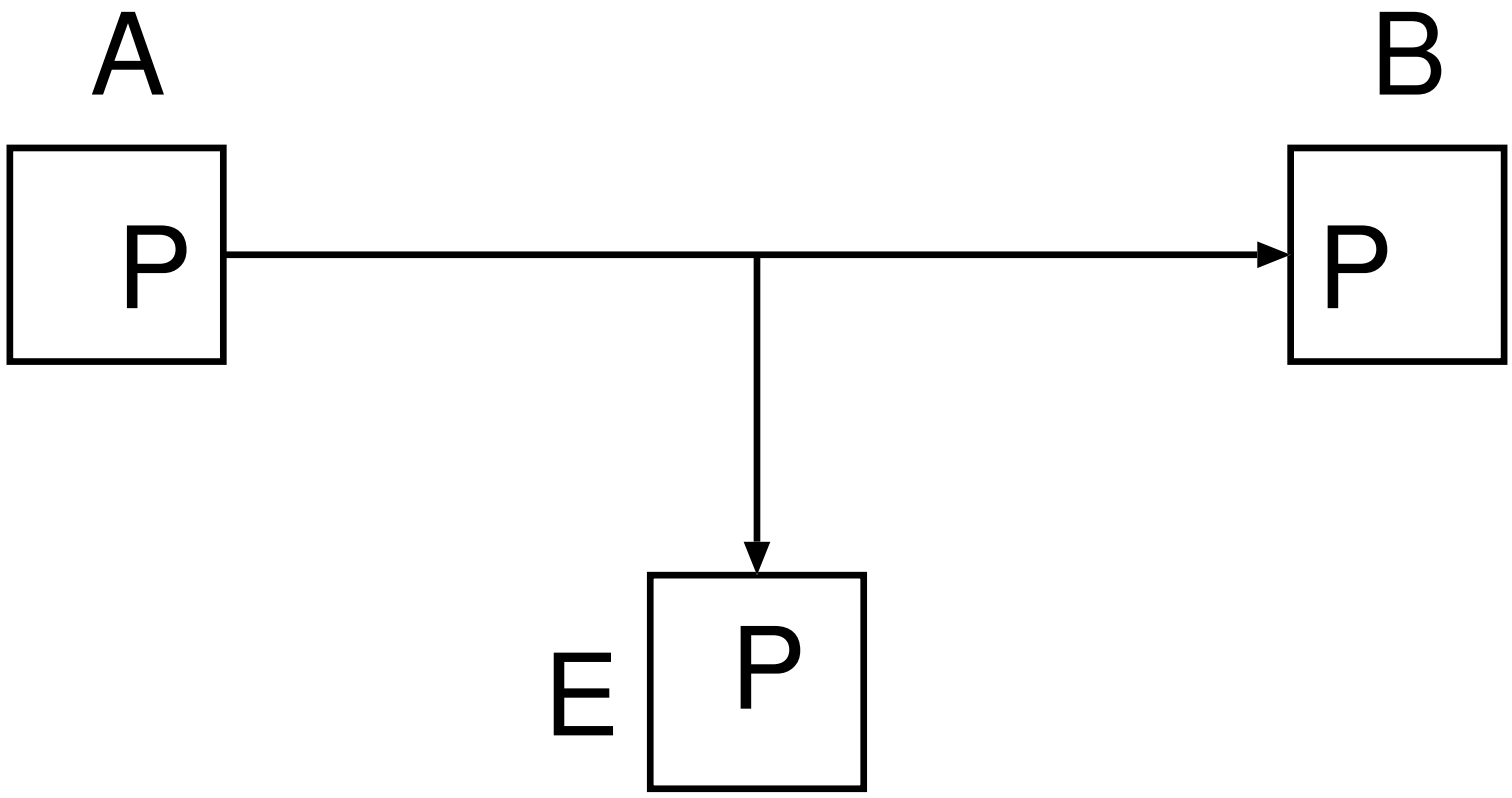
DoS (Denial of Service) 攻撃



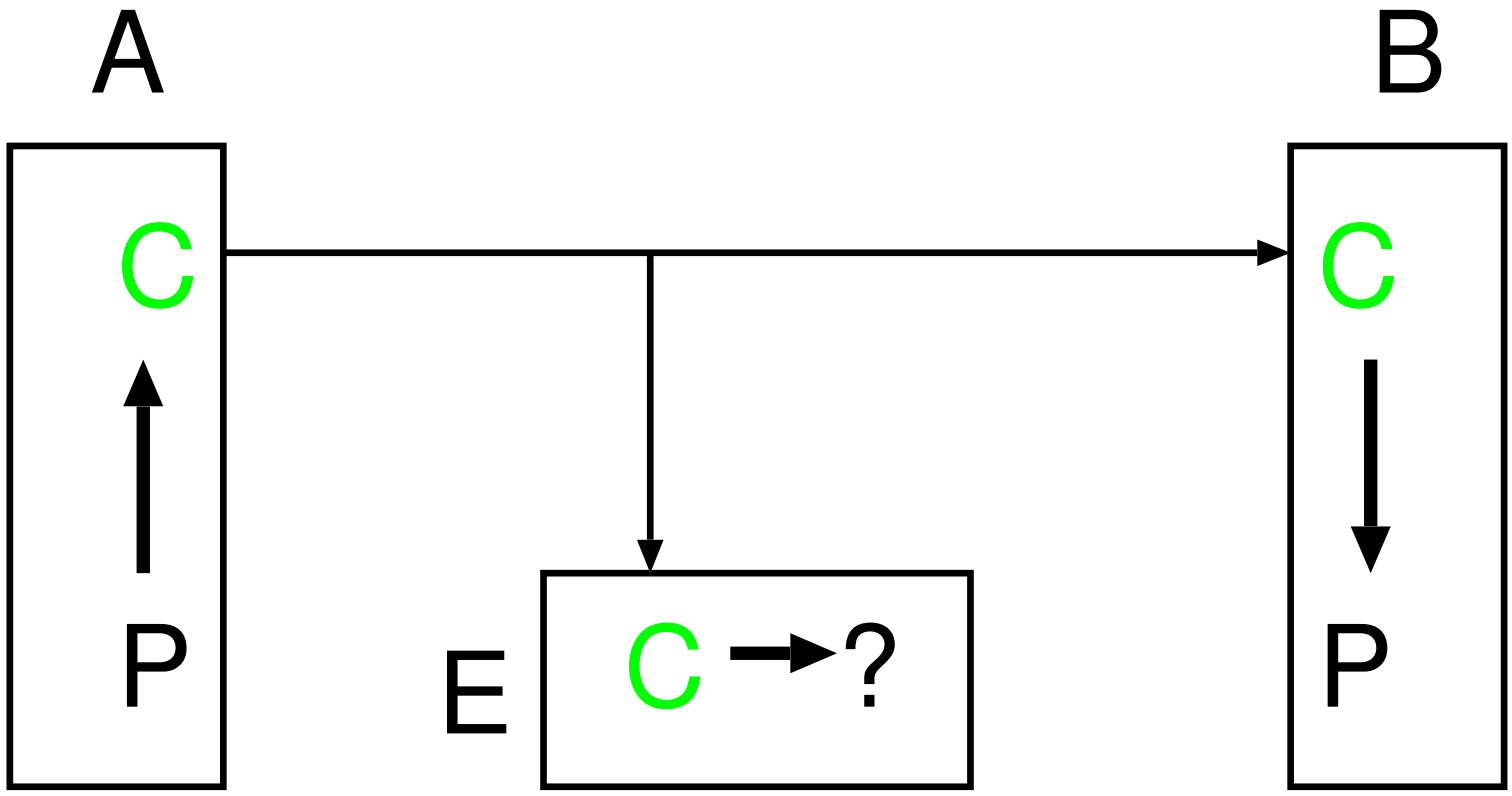
DoS (Denial of Service) 攻撃



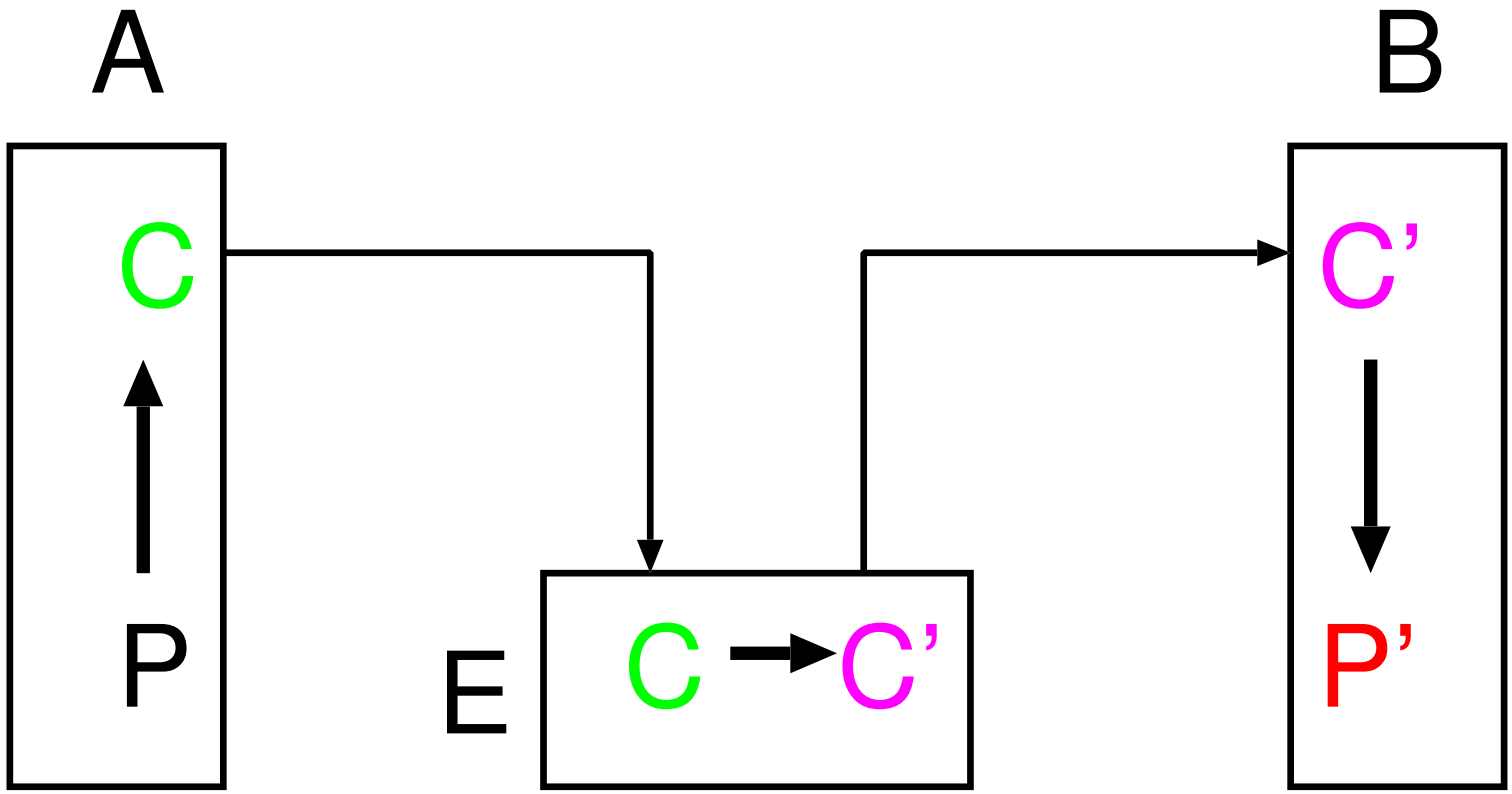
盗聴



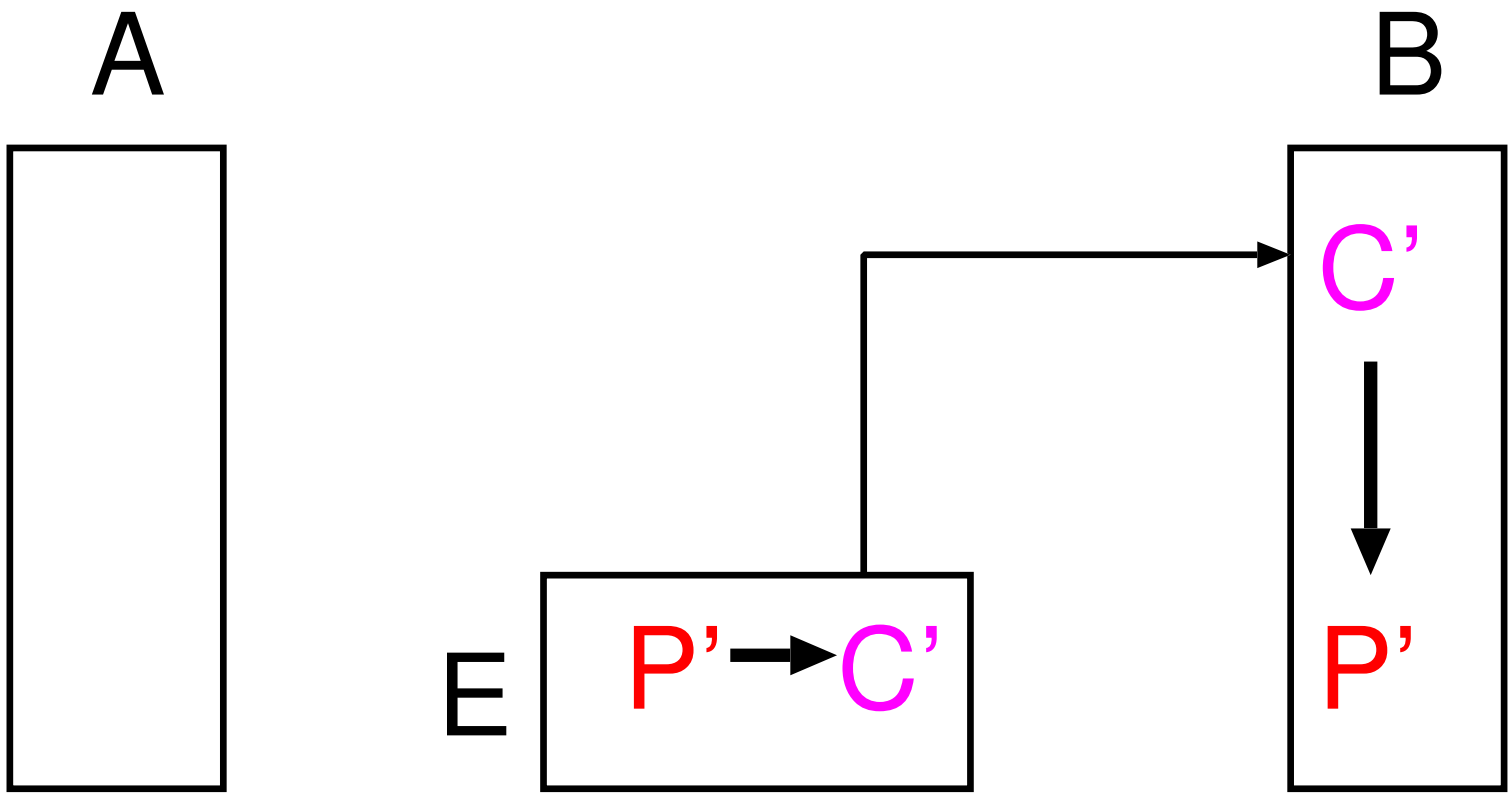
暗号通信で盗聴対策



改竄



なり済まし



暗号通信

公開された情報伝達路 (盗聴可能 と仮定) で、

暗号方式を公開 して通信

- **秘密鍵暗号 (共通鍵暗号)**
- **公開鍵暗号**

秘密鍵 (共通鍵) 暗号

暗号化鍵・復号鍵が同じ

- 換字暗号・Caesar 暗号
- 線型ブロック暗号
- Vernam 暗号
- DES (Data Encryption Standard)
- AES (Advances Encryption Standard)

秘密鍵 (共通鍵) 暗号の特徴

暗号化鍵・復号鍵が同じ

- 一般に原理は簡単で高速
- 事前の鍵共有の必要
- 通信相手毎に別の鍵が必要

公開鍵暗号

暗号化鍵 (公開鍵)・復号鍵 (秘密鍵) が別

- **事前の鍵共有の必要無し**

  $\longrightarrow$

  見ず知らずの人からも送ってもらえる

- **署名機能がある**

  $\longrightarrow$ **改竄・なり済まし の対策**

  $\longrightarrow$ **否認防止 の機能も持つ**

公開鍵暗号

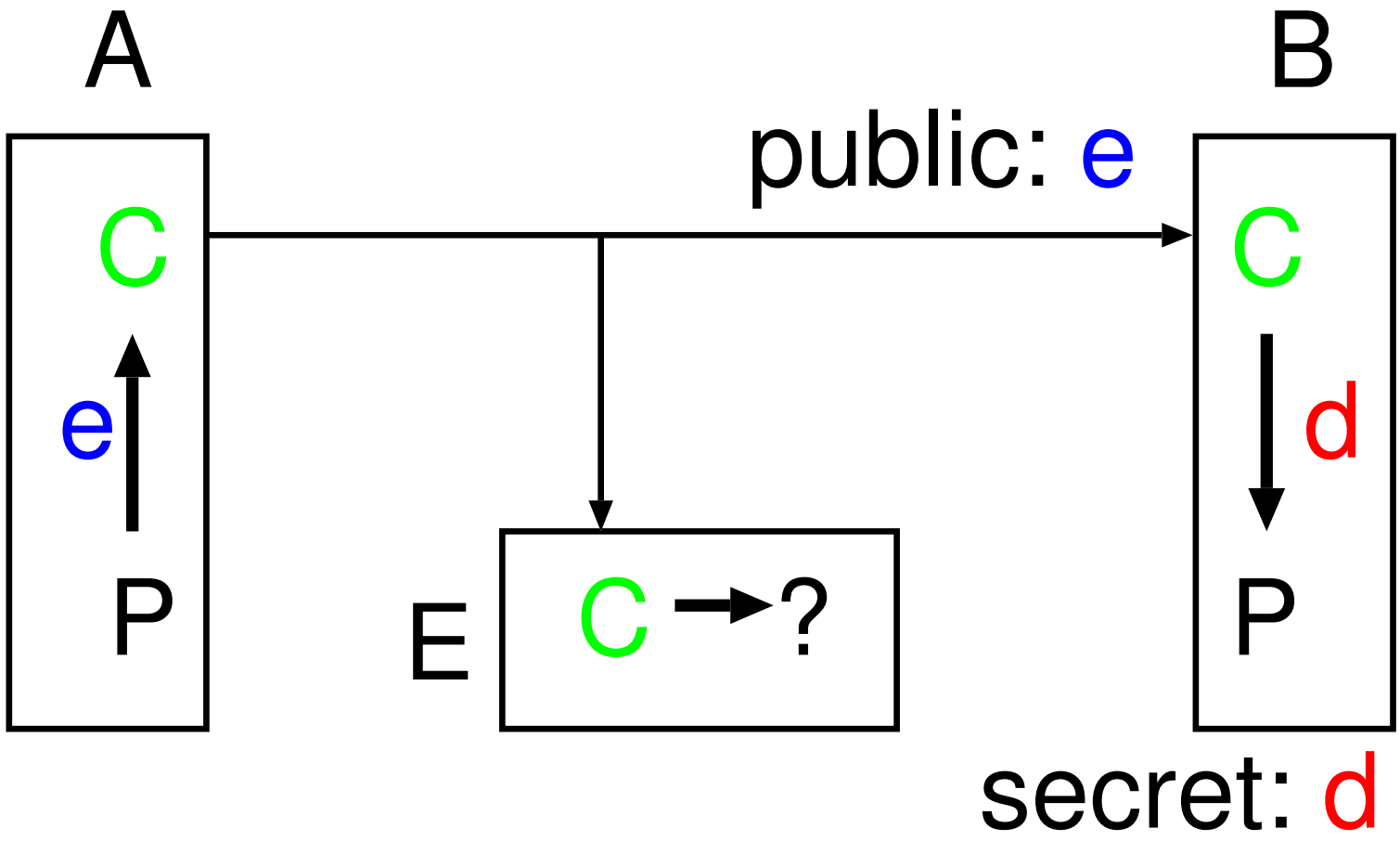
一般には、
**　暗号化・復号が共通鍵暗号に比べて低速**

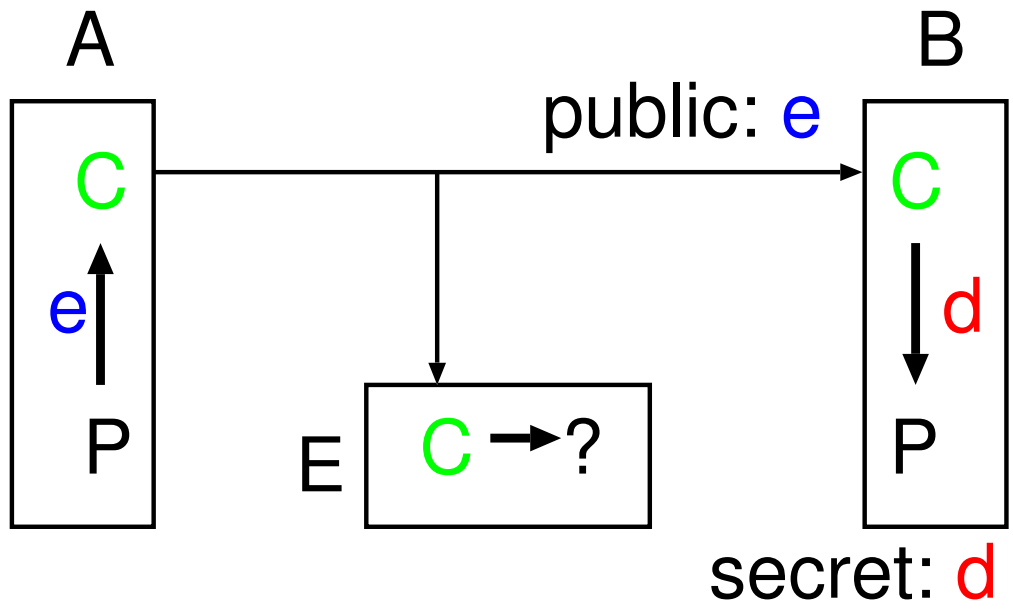
そこで、

- **始めに公開鍵暗号方式で鍵を送付・共有**
- **その鍵を用いて秘密鍵暗号方式で通信**

というように、組合わせて用いることが多い。

公開鍵暗号による暗号通信



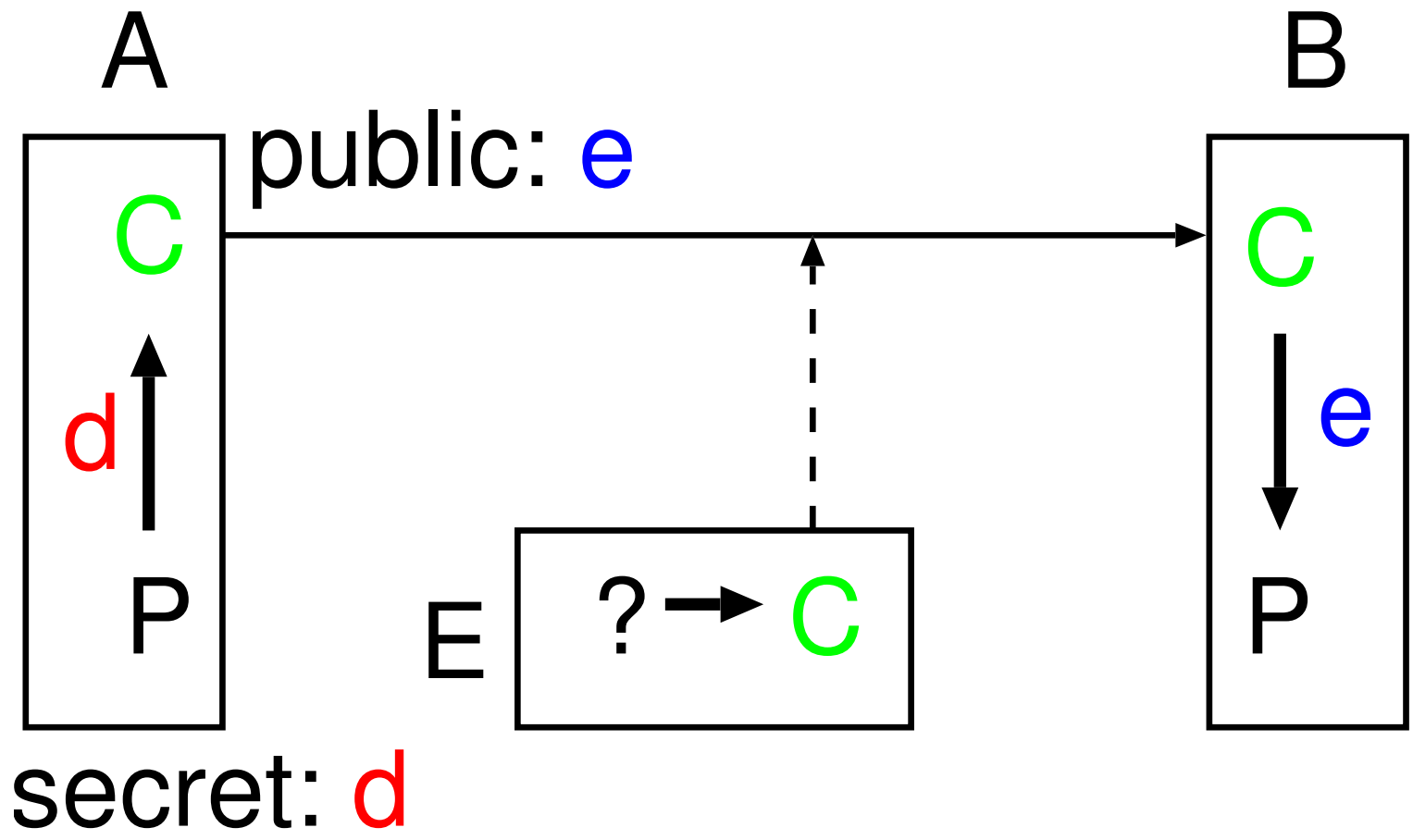


しかし、これだと誰でも暗号化できるので、

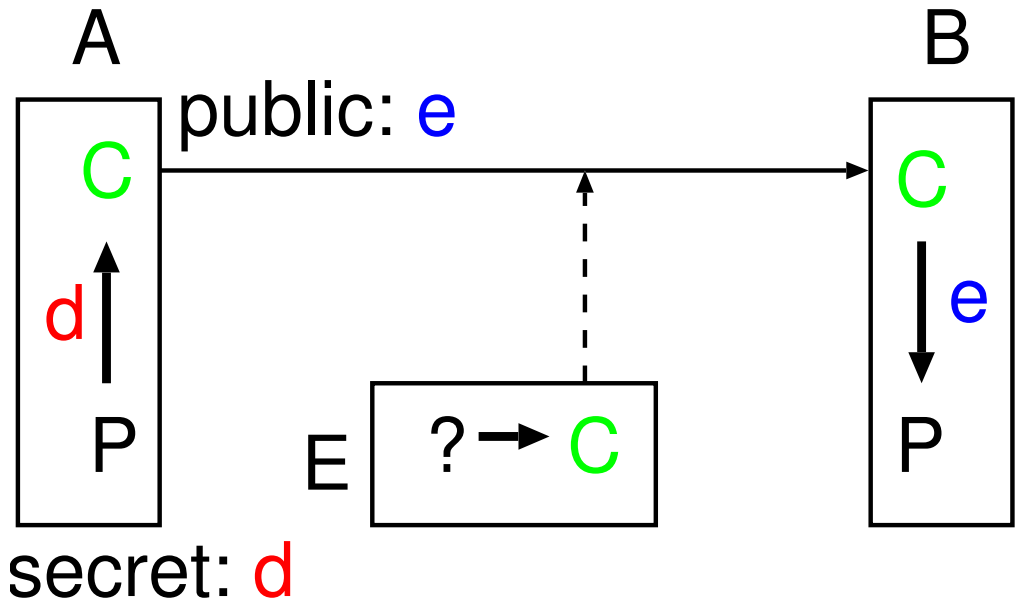
A 氏が送った保証がない。

⟶ 署名の必要性

公開鍵暗号を用いた署名



公開鍵暗号を用いた署名



盗聴者 E 氏は

平文 P は判らないが、暗号文 C は盗聴可能

$\longrightarrow$ いつも同じ署名は使えない

公開鍵暗号を用いた署名

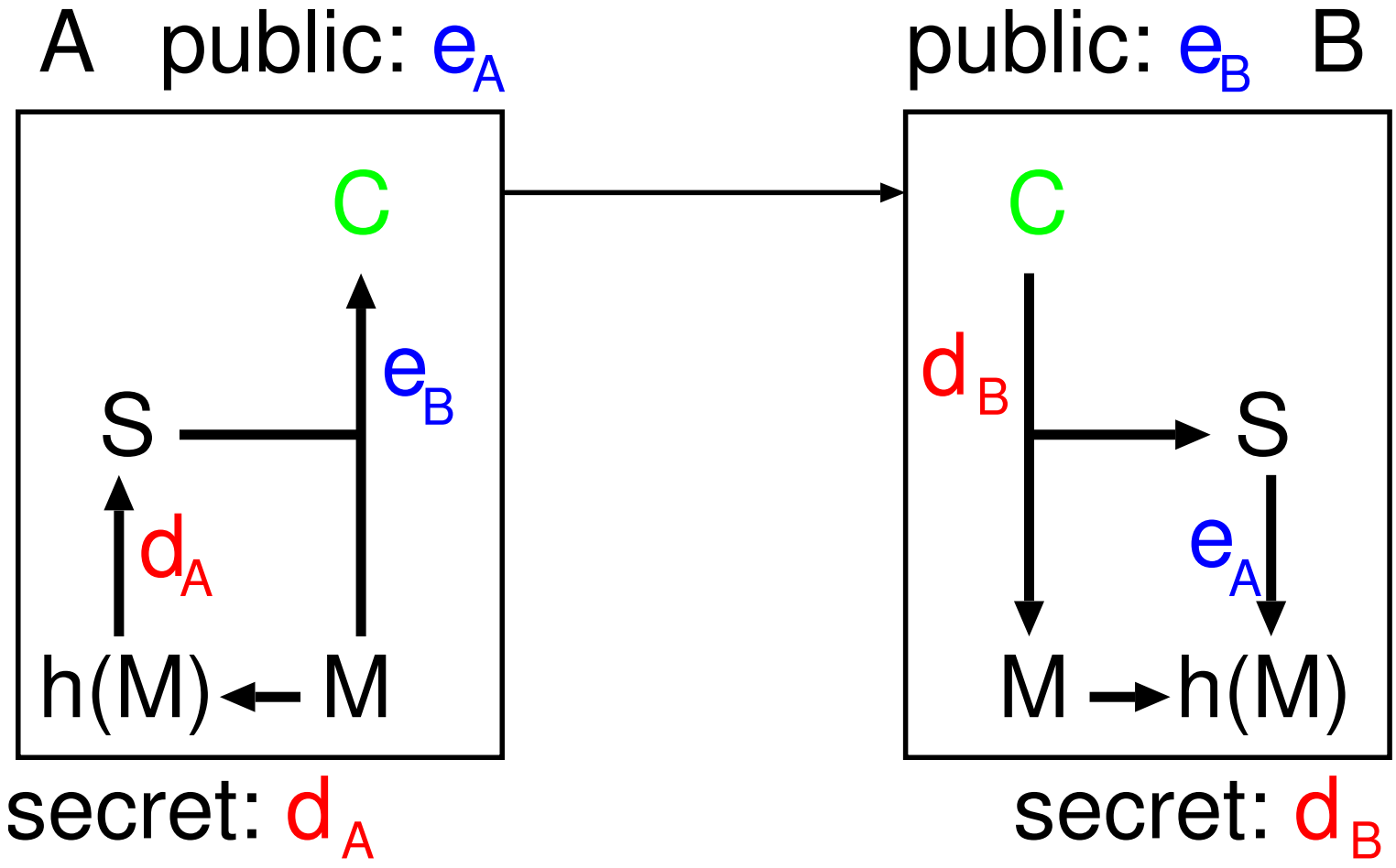
実際には、メッセージ本文 M に対して、

M から決まる短い値 (ハッシュ値) $h(M)$ を

送信者 A 氏の秘密鍵で暗号化した文字列 S を本文 M に添付して、

受信者 B 氏の公開鍵で一緒に暗号化して送る。

公開鍵暗号を用いた署名



公開鍵暗号の特徴

- 暗号化は誰でも出来る
- 復号は秘密鍵を知らないと出来ない
  (もの凄く時間が掛かる)

そんな都合の良い仕組みが本当にあるのか ?

$\longrightarrow$ ある!! (多分大丈夫)

計算困難な問題 を利用
(素因数分解・離散対数問題)

代表的な公開鍵暗号方式

- **RSA 暗号 (Rivest-Shamir-Adleman)**
- **Diffie-Hellman 鍵共有**
- **ElGamal 暗号**