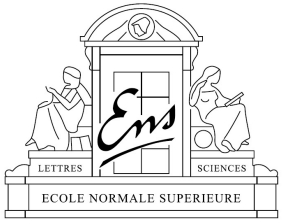
Redundancy-Free Encryption from Rabin and RSA

Gilles Barthe David Pointcheval
Santiago Zanella-Béguelin



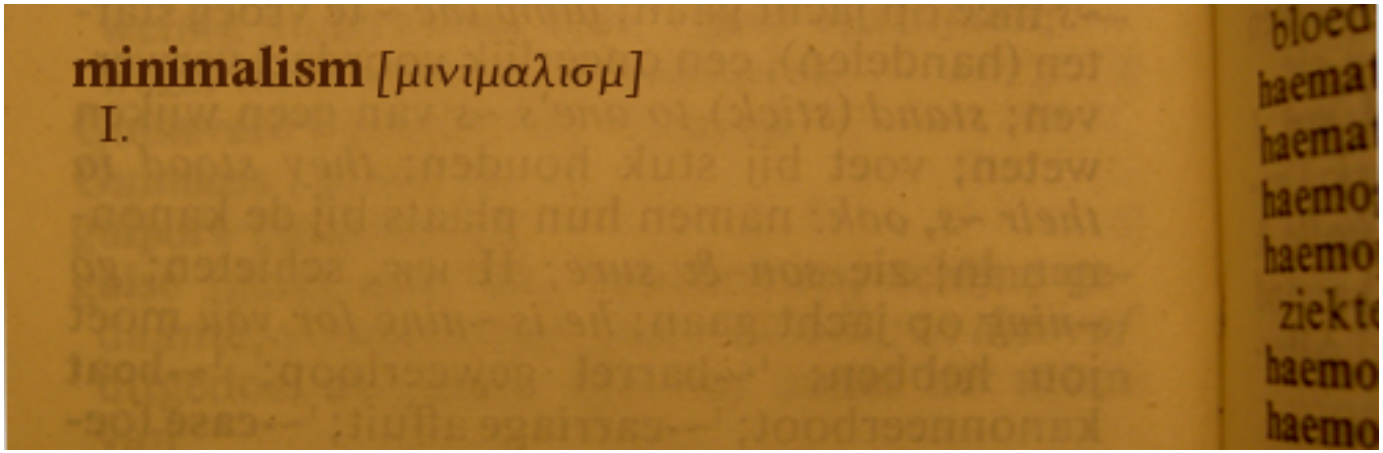
Microsoft®
Research

2012.10.18
ACM CCS

The quest for minimalism in cryptography

Cryptography stripped down to its essential features

- Minimal assumptions sufficient to achieve a cryptographic goal
- Minimal constructions—removing any element results in a totally insecure construction
- Minimality often implies optimality: minimal overhead, efficiency, tight security reductions



Minimalist cryptography

- **Q**: What is the simplest provably secure block cipher?

  A: Single-Key Even-Mansour
  [Dunkellman-Keller-Shamir '12]

$$E_k(m) \stackrel{\text{def}}{=} \mathcal{F}(m \oplus k) \oplus k$$

- **Q**: How many Feistel rounds are enough to build a random permutation from a random function?

  A: At least 7, at most 14
  [Holenstein-Künzler-Tessaro '11]

- **Q**: What is the simplest provably secure padding-based encryption scheme?

  A: In this talk

Minimalist cryptography

- **Q**: What is the simplest provably secure block cipher?

  A: Single-Key Even-Mansour
  [Dunkellman-Keller-Shamir '12]

$$E_k(m) \stackrel{\text{def}}{=} \mathcal{F}(m \oplus k) \oplus k$$

- **Q**: How many Feistel rounds are enough to build a random permutation from a random function?

  A: At least 7, at most 14
  [Holenstein-Künzler-Tessaro '11]

- **Q**: What is the simplest provably secure padding-based encryption scheme?

  A: In this talk

Minimalist cryptography

- **Q**: What is the simplest provably secure block cipher?

  A: Single-Key Even-Mansour
  [Dunkellman-Keller-Shamir '12]

$$E_k(m) \stackrel{\text{def}}{=} \mathcal{F}(m \oplus k) \oplus k$$

- **Q**: How many Feistel rounds are enough to build a random permutation from a random function?

  A: At least 7, at most 14
  [Holenstein-Künzler-Tessaro '11]

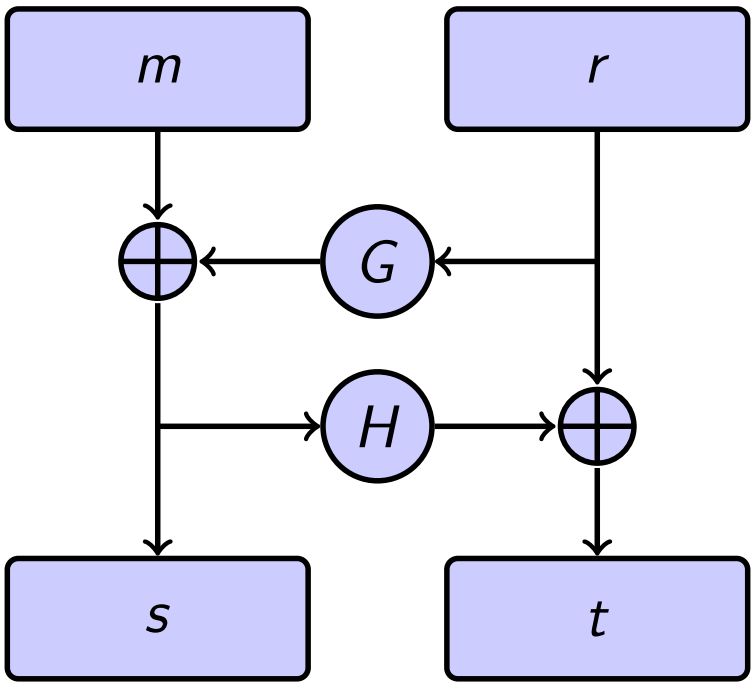
- **Q**: What is the simplest provably secure padding-based encryption scheme?

  A: In this talk

A first attempt: OAEP [Bellare-Rogaway '94]

An *encode-then-encrypt* scheme based on a trapdoor permutation f and hash functions G, H

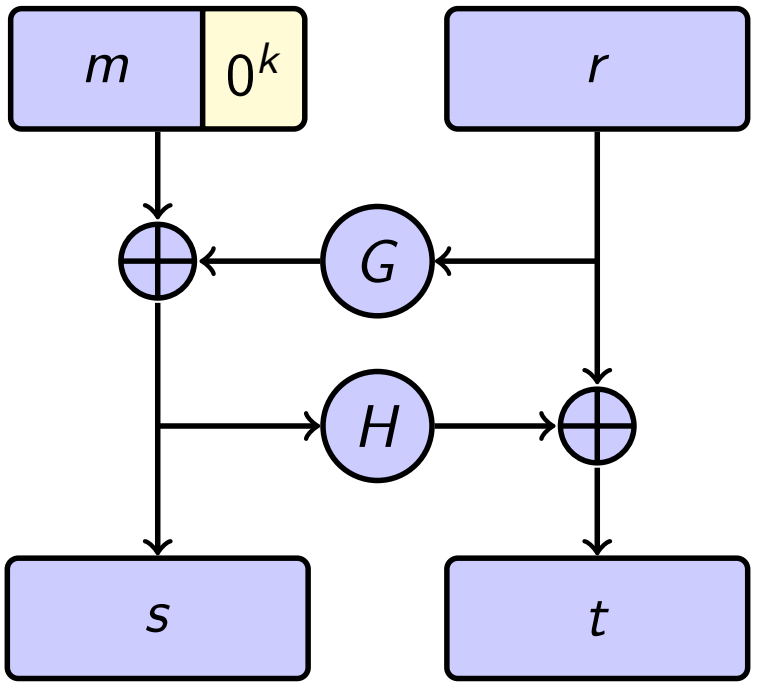
$$\mathcal{E}_{pk}(m; r) \stackrel{\text{def}}{=} f_{pk}\,(\; m \oplus G(r) \;\|\; r \oplus H(m \oplus G(r))\;)$$



A first attempt: OAEP [Bellare-Rogaway '94]

An *encode-then-encrypt* scheme based on a trapdoor permutation f and hash functions G, H

$$\mathcal{E}_{pk}(m; r) \stackrel{\text{def}}{=} f_{pk}\,(\; m \oplus G(r) \;\|\; r \oplus H(m \oplus G(r))\;)$$

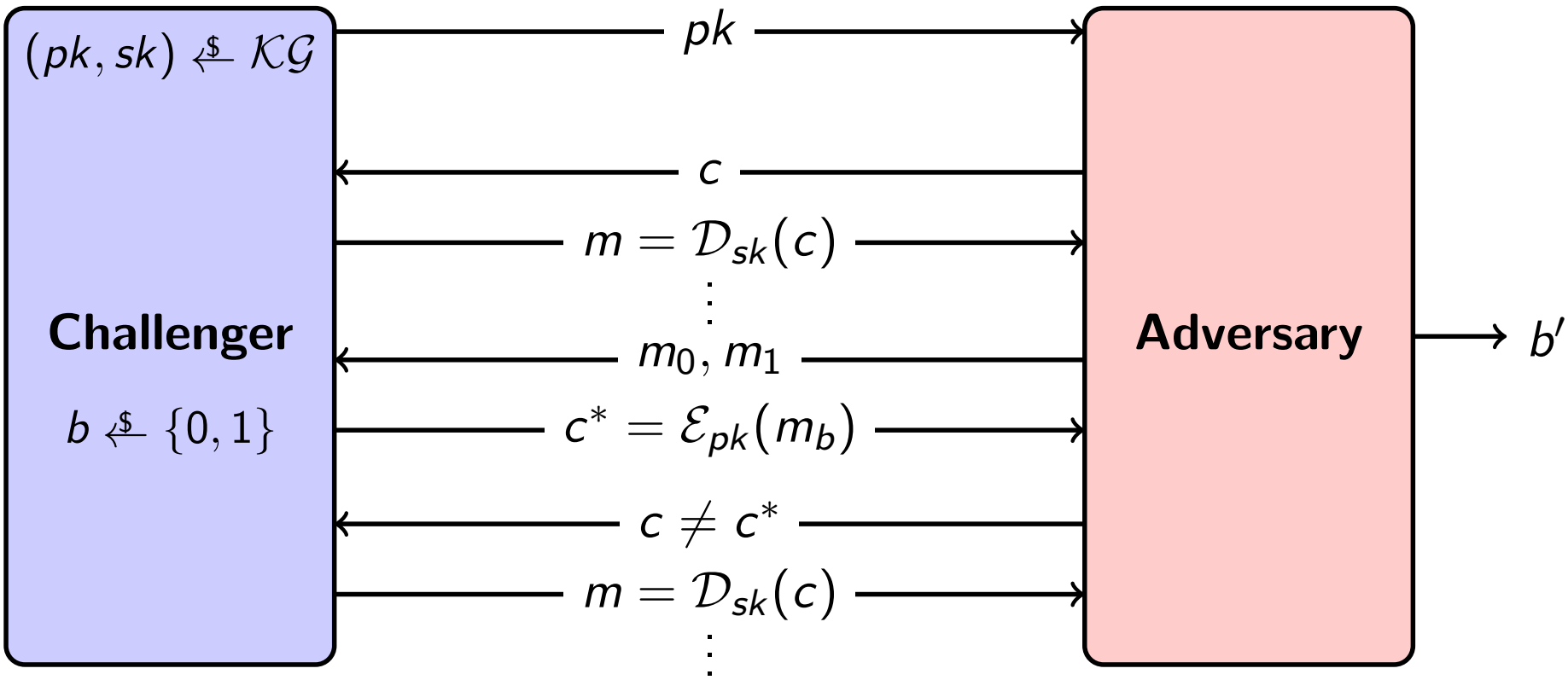


Not that **O**ptimal

Redundancy 0^k needed to get chosen-ciphertext security

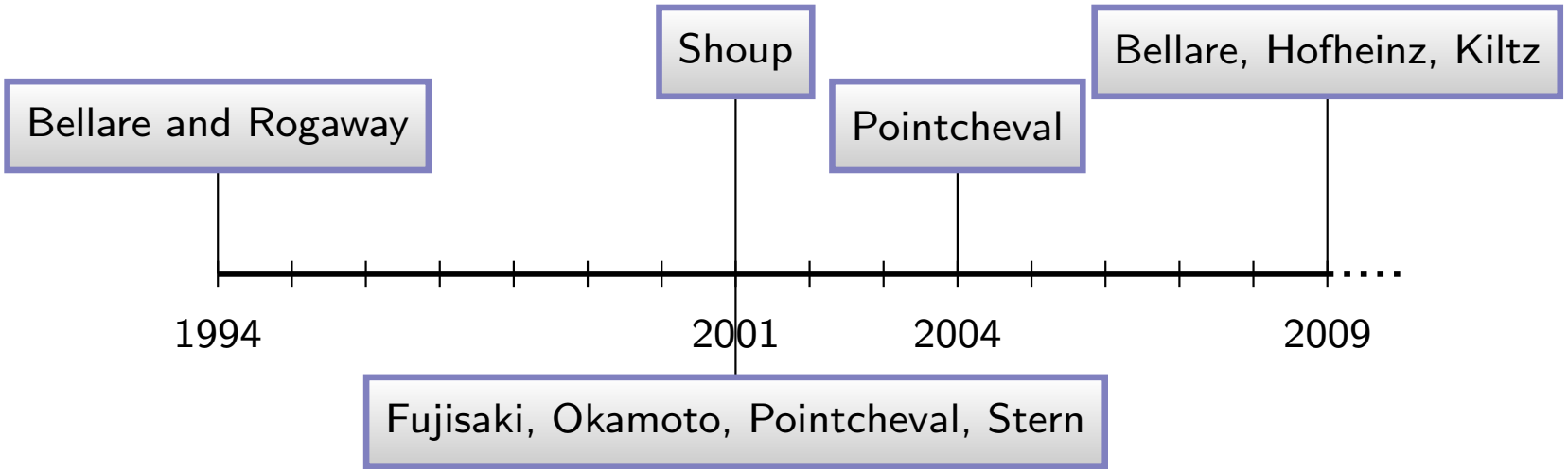
Chosen-ciphertext security

For a public-key encryption scheme $(\mathcal{KG}, \mathcal{E}, \mathcal{D})$, define the experiment CCA:



Advantage of $\mathcal{A}$: $\mathbf{Adv}^{\mathcal{A}}_{\mathrm{CCA}} \stackrel{\mathrm{def}}{=} \left| \Pr[\mathrm{CCA} : b = b'] - \frac{1}{2} \right|$

A timeline of OAEP



1994 Proof of chosen-ciphertext security!

2001 Proof is flawed, but can be patched

- ...weakening the security notion, or
- ...modifying the scheme, or
- ...under stronger assumptions

2004 Filled gaps in 2001 proof

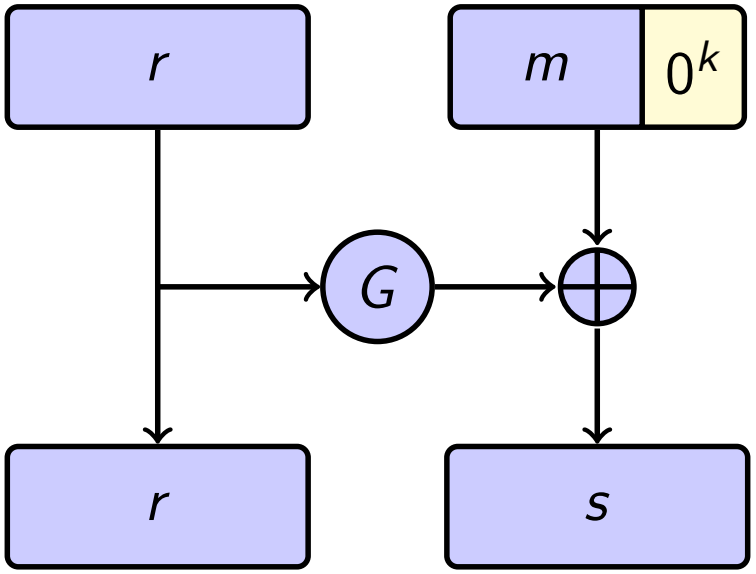
2009 Security definition is ambiguous

2011 Machine-checked proof: filled gaps in 2004 proof

A second attempt: SAEP [Boneh '01]

- Just 1 Feistel round
- CCA-secure when instantiated with Rabin and RSA with $e = 3$

$$\mathcal{E}_{pk}(m; r) \stackrel{\text{def}}{=} f_{pk}\left(\; r \;\; \| \;\; (m \,\|\, 0^k) \oplus G(r) \; \right)$$



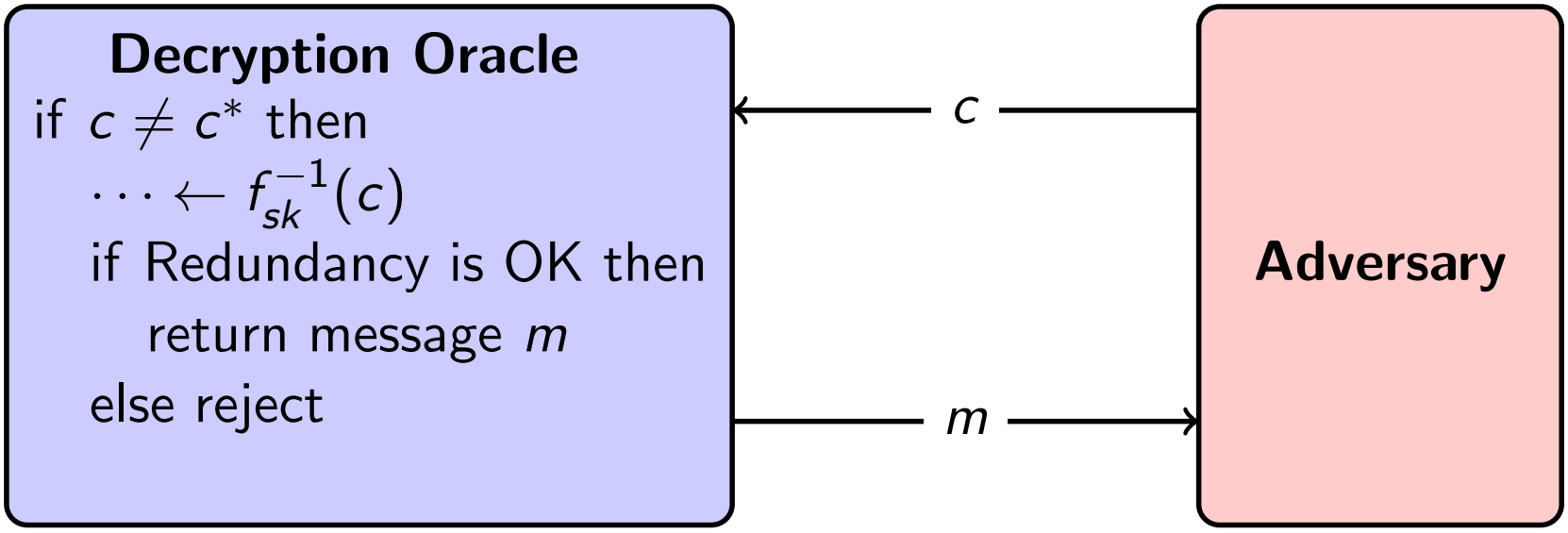
Once more, redundancy 0^k *needed* for chosen-ciphertext security

Security guarantee void as soon as $k \approx \log(q_D)$

Why redundancy is necessary?

- Most proofs of CCA security rely on the implication

$$\text{Plaintext Awareness} \wedge \text{CPA security} \implies \text{CCA security}$$



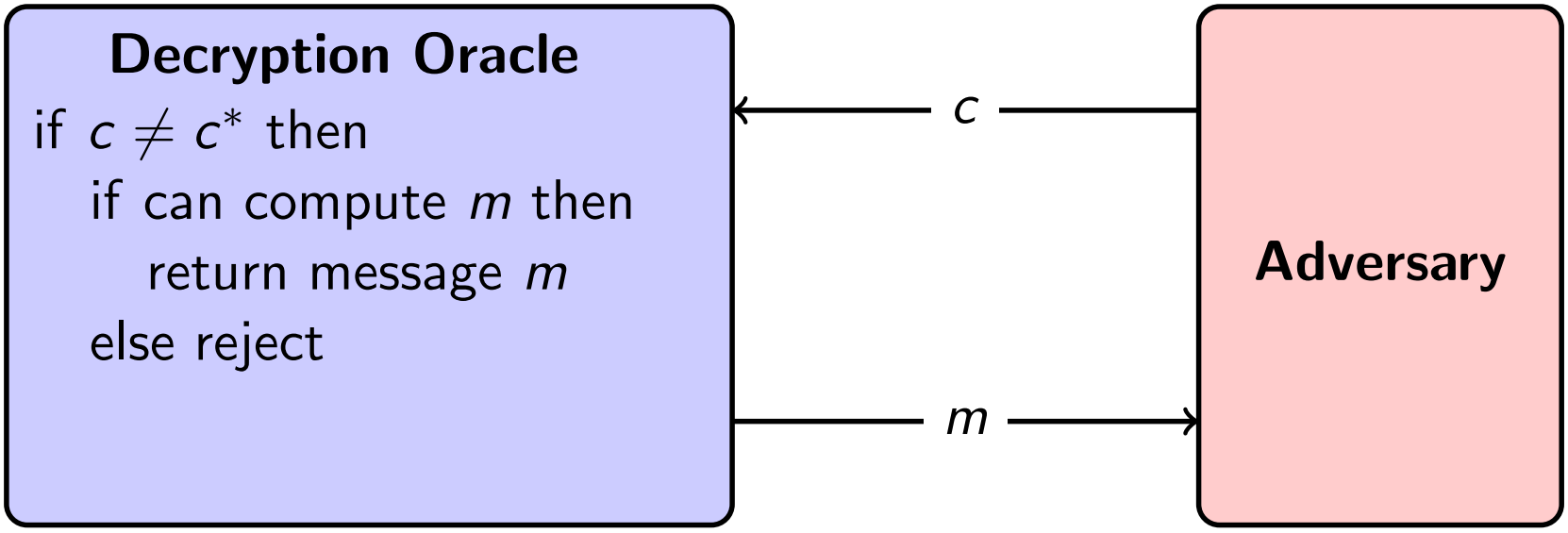
Either m can be computed from previous Adversary's queries
or
the ciphertext is invalid with high probability

If one rejects a valid ciphertext, simulation fails, but f can be inverted with high probability

Why redundancy is necessary?

- Most proofs of CCA security rely on the implication

$$\text{Plaintext Awareness} \wedge \text{CPA security} \implies \text{CCA security}$$



Either m can be computed from previous Adversary's queries
or
the ciphertext is invalid with high probability

If one rejects a valid ciphertext, simulation fails, but f can be inverted with high probability

Is redundancy really necessary?

Q: How much redundancy is needed to get CCA security?

Is redundancy really necessary?

Q: How much redundancy is needed to get CCA security?

0 (**Z**ero)

Every ciphertext is valid, decryption never rejects

Advantages of removing redundancy:

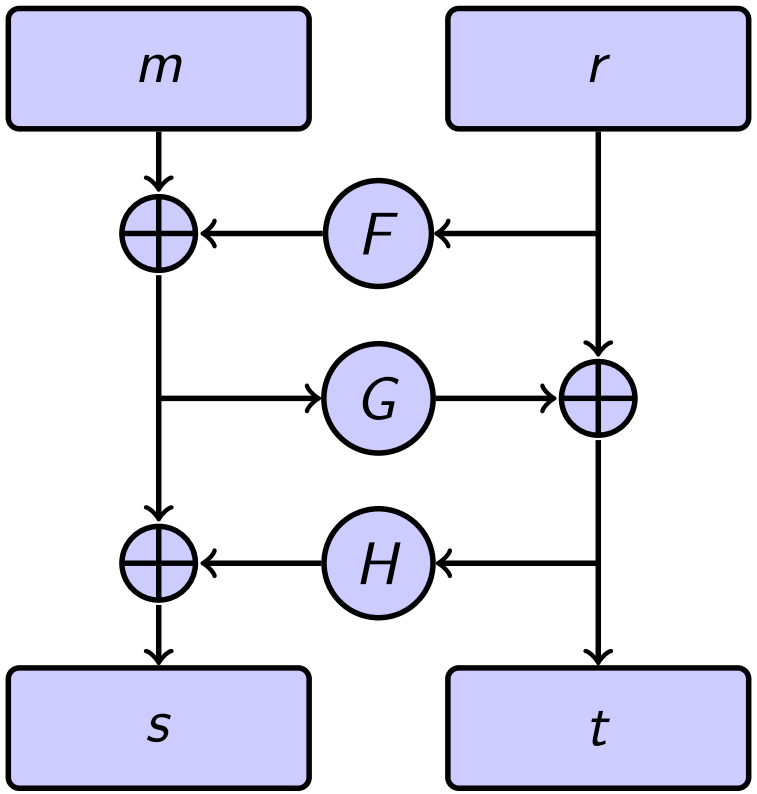
- Simpler implementation
- More bandwidth (less redundancy $\Longrightarrow$ less overhead)
- Absence of padding-oracle attacks
  (no padding errors $\Longrightarrow$ no padding oracle)

  Remember Bleichenbacher's Million Message Attack on PKCS#1 1.5? Is now down to 15,000 messages!
  [Steel-Bardou-Focardi-Kawamoto-Simionato,Kai-Tsay '12]

A secure redundancy-free scheme: OAEP-3R

- [Phan-Pointcheval '03]
- 3-round Feistel
- Loose security reduction $\Longrightarrow$ inefficient, large keys needed

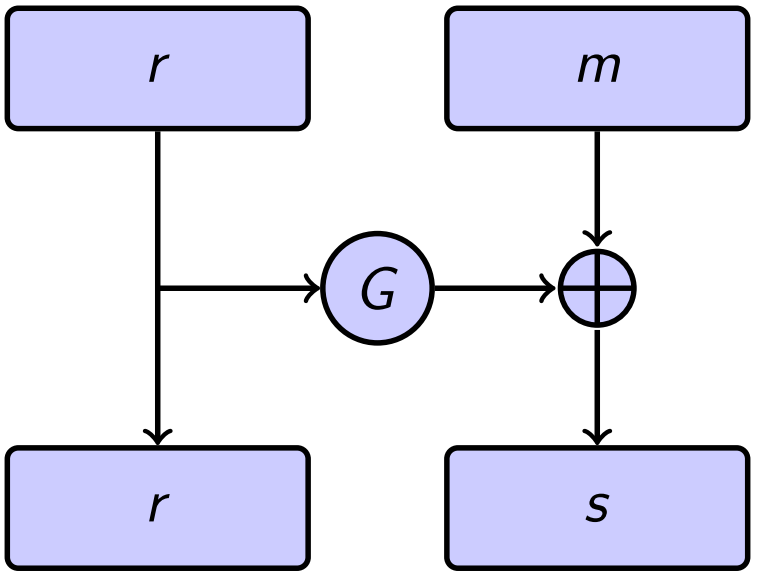
$$\mathcal{E}_{pk}(m;r) \stackrel{\text{def}}{=} f_{pk}\,(\; m \oplus F(r) \oplus H(r \oplus G(m \oplus F(r))) \;\|\; r \oplus G(m \oplus F(r))\;)$$



ZAEP: minimalist redundancy-free secure encryption

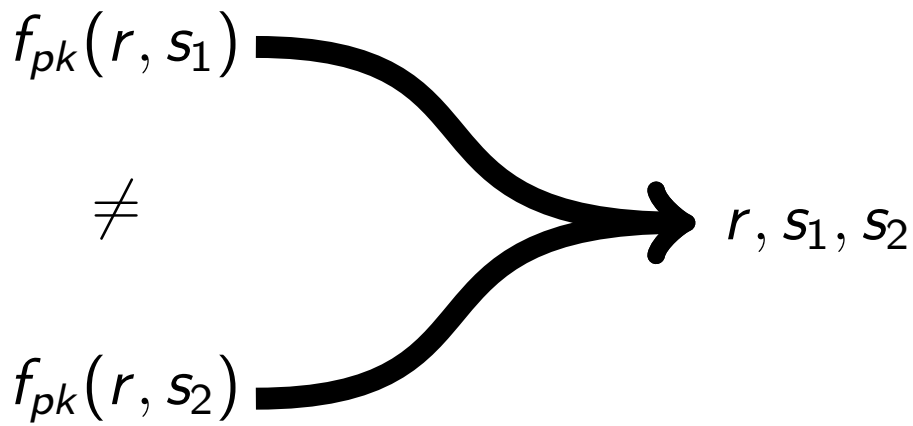
- Idea: take SAEP, but remove 0^k redundancy
- Simplest conceivable padding-based encryption scheme
- Security reduces to inversion of the trapdoor permutation f under minimal additional assumptions
- Tight security reduction $\Longrightarrow$ efficient, practical key sizes

$$\mathcal{E}_{pk}(m; r) \stackrel{\text{def}}{=} f_{pk}\,(\; r \;\|\; m \oplus G(r)\;)$$

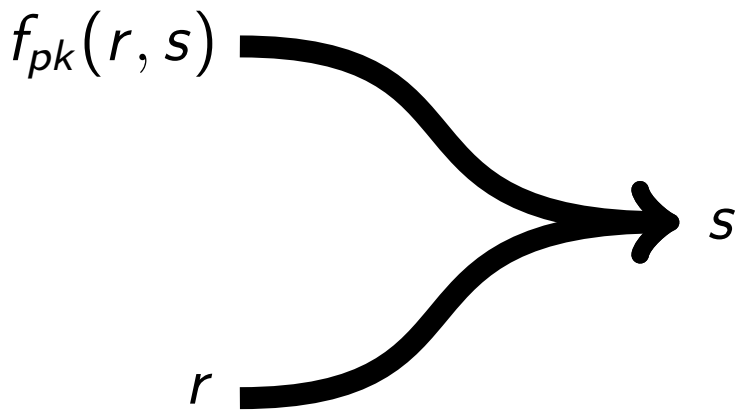


Necessary assumptions

- Common-Input Extractability (CIE)



- Second-Input Extractability (SIE)



Simulation of the decryption oracle

Oracle $G(x)$:
if $x \notin \mathrm{dom}(\boldsymbol{L}_G)$ then
  $c \leftarrow$ find $c \in \mathrm{dom}(\boldsymbol{L}_{\mathcal{D}})$. $\mathsf{sie}_{\boldsymbol{pk}}(c, x) \neq \perp$;
  if $c \neq \perp$ then
    $\boldsymbol{L}_G[x] \leftarrow \boldsymbol{L}_{\mathcal{D}}[c] \oplus \mathsf{sie}_{\boldsymbol{pk}}(c, x)$;
  else
    $\boldsymbol{L}_G[x] \xleftarrow{\$} \{0,1\}^{\ell}$;
return $\boldsymbol{L}_G[x]$

Oracle $\mathcal{D}(c)$:
if $\boldsymbol{q} < q_{\mathcal{D}} \wedge \neg(\boldsymbol{c}^*_{\mathbf{def}} \wedge c = \boldsymbol{c}^*)$ then
  $\boldsymbol{q} \leftarrow \boldsymbol{q} + 1$;
  $r \leftarrow$ find $r \in \mathrm{dom}(\boldsymbol{L}_G)$. $\mathsf{sie}_{\boldsymbol{pk}}(c, r) \neq \perp$;
  if $r \neq \perp$ then return $\boldsymbol{L}_G[r] \oplus \mathsf{sie}_{\boldsymbol{pk}}(c, r)$
  else
    if $c \in \mathrm{dom}(\boldsymbol{L}_{\mathcal{D}})$ then return $\boldsymbol{L}_{\mathcal{D}}[c]$
    else
      $c' \leftarrow$ find $c' \in \mathrm{dom}(\boldsymbol{L}_{\mathcal{D}})$. $\mathsf{cie}_{\boldsymbol{pk}}(c, c') \neq \perp$;
      if $c' \neq \perp$ then
        $(r, s, t) \leftarrow \mathsf{cie}_{\boldsymbol{pk}}(c, c')$;
        return $\boldsymbol{L}_{\mathcal{D}}[c'] \oplus s \oplus t$;
      else
        if $\boldsymbol{c}^*_{\mathbf{def}} \wedge \mathsf{cie}_{\boldsymbol{pk}}(c, \boldsymbol{c}^*) \neq \perp$ then
          $(r, s, t) \leftarrow \mathsf{cie}_{\boldsymbol{pk}}(c, \boldsymbol{c}^*)$;
          $\boldsymbol{L}_G[r] \xleftarrow{\$} \{0,1\}^{\ell}$; return $\boldsymbol{L}_G[r] \oplus s$;
        else
          $\boldsymbol{L}_{\mathcal{D}}[c] \xleftarrow{\$} \{0,1\}^{\ell}$; return $\boldsymbol{L}_{\mathcal{D}}[c]$
else return $\perp$

- Requires programming the random oracle G
- Significantly different from original SAEP (w/redundancy) proof

Security of ZAEP in the Random Oracle Model

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a trapdoor permutation satisfying both SIE and CIE

Theorem (ZAEP is INDCCA secure)

Let $\mathcal{A}$ be an adversary against the CCA security of f-ZAEP that runs within time $t_{\mathcal{A}}$ and makes at most q_G queries to G and $q_{\mathcal{D}}$ decryption queries. Then, there exists an algorithm $\mathcal{B}$ that inverts f with probability ϵ within time $t_{\mathcal{B}}$ such that

$$\begin{aligned} \epsilon &\geq \mathbf{Adv}^{\mathcal{A}}_{\mathrm{CCA}} - \frac{q_{\mathcal{D}}}{2^n} \\ t_{\mathcal{B}} &\leq t_{\mathcal{A}} + 2q_G q_{\mathcal{D}} t_{\mathsf{sie}} + q_{\mathcal{D}}^2 t_{\mathsf{cie}} \end{aligned}$$

In practice, $t_{\mathsf{sie}} \approx t_{\mathsf{cie}} \approx n^3$

Instantiations

Theorem (Coppersmith)

Let $p(X)$ be a monic polynomial of degree d and $N \in \mathbb{N}$. One can find all integer solutions of $p(x) = 0 \mod N$ with $|x| < N^{1/d}$ in time polynomial in $\log(N)$ and d (basically $O(\log(N)^3)$ for small d).

- RSA with small public exponent (e.g. $e = 3$)

$$\text{RSA}[N, e] : \{0,1\}^{n-\ell} \times \{0,1\}^{\ell} \to \{0,1\}^{n}$$
$$\text{RSA}[N, e] : (r, s) \mapsto (r \times 2^{\ell} + s)^{e} \bmod N$$

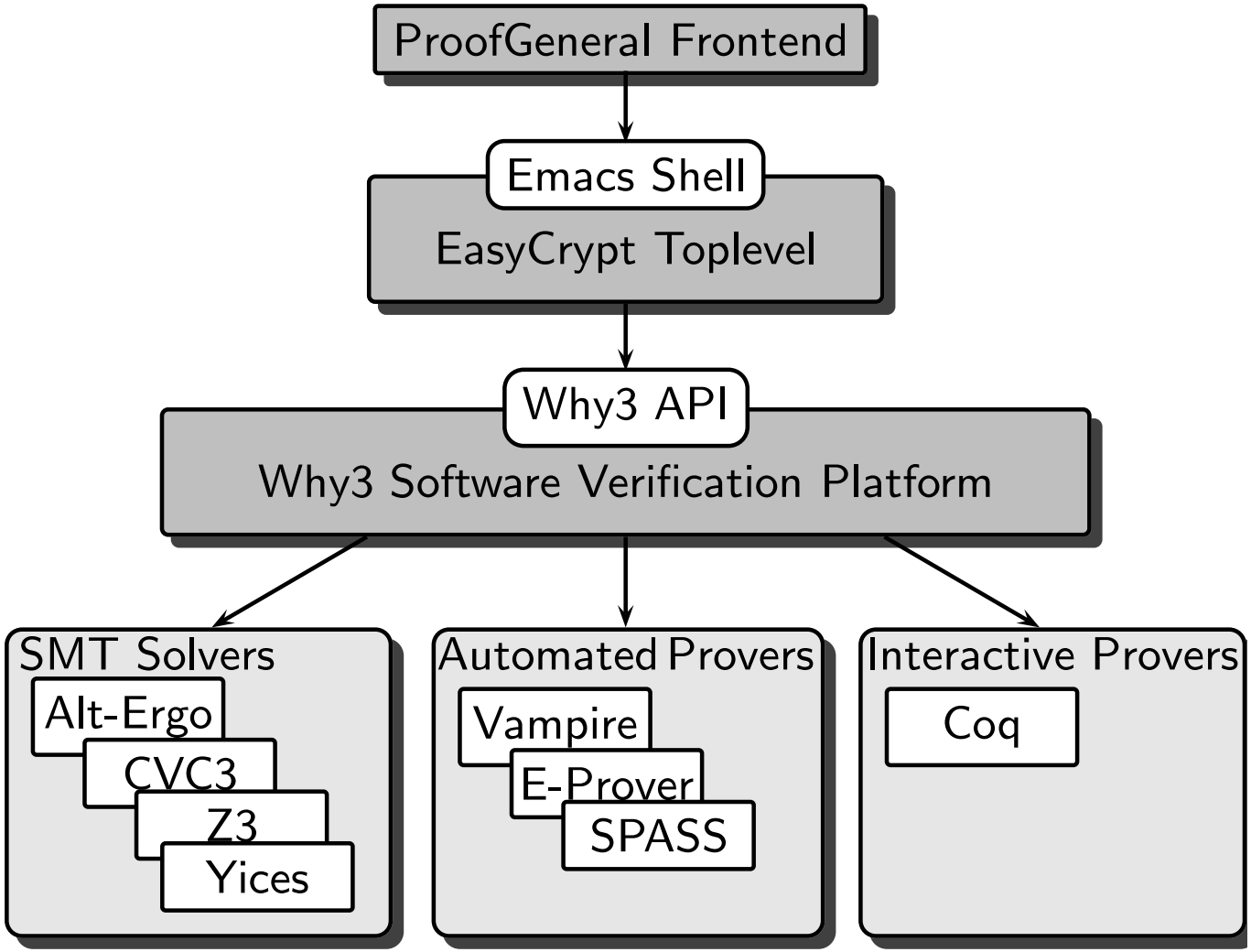
  Satisfies SIE and CIE when $\ell < n/e^2$

- Rabin with Blum integer modulus ($N = pq$; $p, q \equiv 3 \bmod 4$)

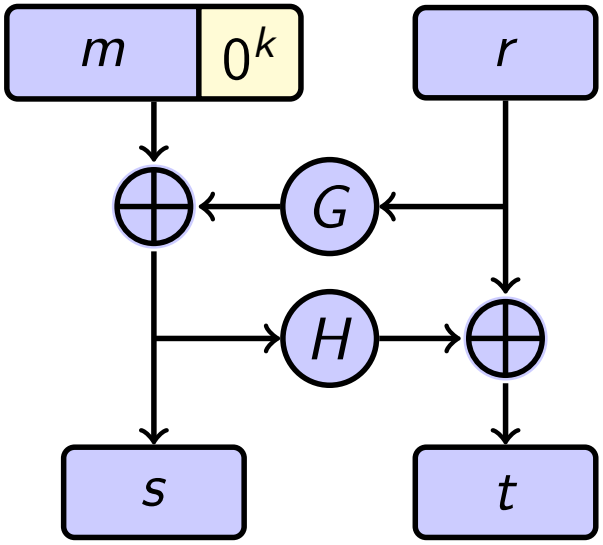
$$\text{Rabin}[N] : \{0,1\}^{n-\ell} \times \{0,1\}^{\ell} \to \{0,1\}^{n}$$
$$\text{Rabin}[N] : (b \| r, s) \mapsto (-1)^{b} \times (r \times 2^{\ell} + s)^{2} \bmod N$$

  Satisfies SIE and CIE when $\ell < n/2$

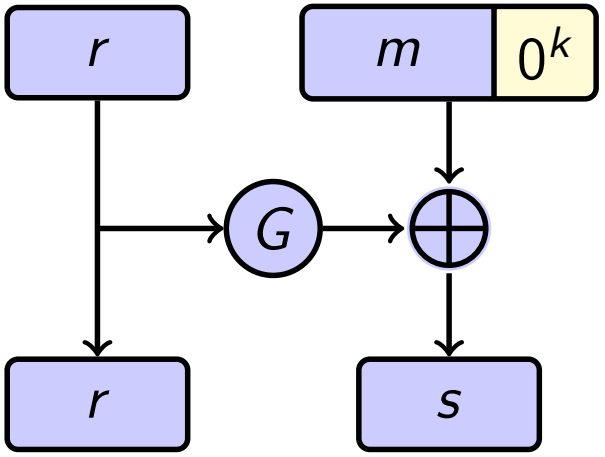
How we prove it: EasyCrypt



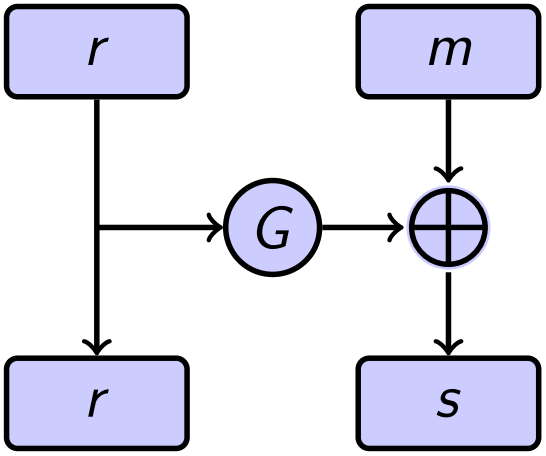
Questions?



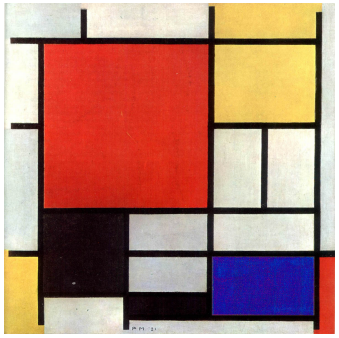
OAEP

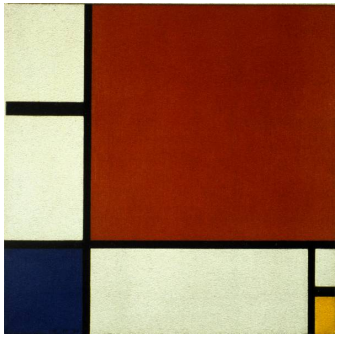


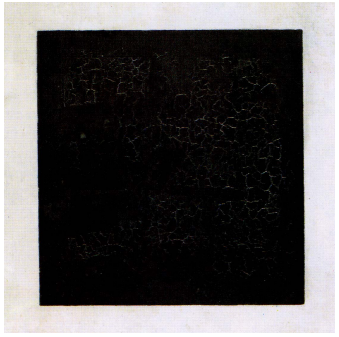
SAEP



ZAEP







`http://easycrypt.gforge.inria.fr`