PUBLIC-KEY ENCRYPTION

Brief recap of RSA:

$$N = p \cdot q$$

-) "Textbook" version. $pk = (N, e)$; $sk = (N, d)$

$$e \cdot d \equiv 1 \mod (p-1)(q-1)$$

$m \in \mathbb{Z}_N^*$ $\quad c = m^e \mod N$ NOT

$m = c^d \mod N$ CPA SECURE

-) PKCS #1.5. Pad the message with random $r \in \{0,1\}^\ell$

$$c = (\hat{m})^e \mod N \; ; \quad \hat{m} = r \| m$$

CPA - security? Only known for $l = |m| - 1$

and anyway not provably secure assuming FACTORING

but under RSA assumption.

$$(\text{RSA} \Rightarrow \text{FACTORING}) \; ; \; (\text{FACTORING} \overset{?}{\Rightarrow} \text{RSA})$$

-) CCA security?? Bleichenbacher showed

a CCA attack that allows to recover plaintext

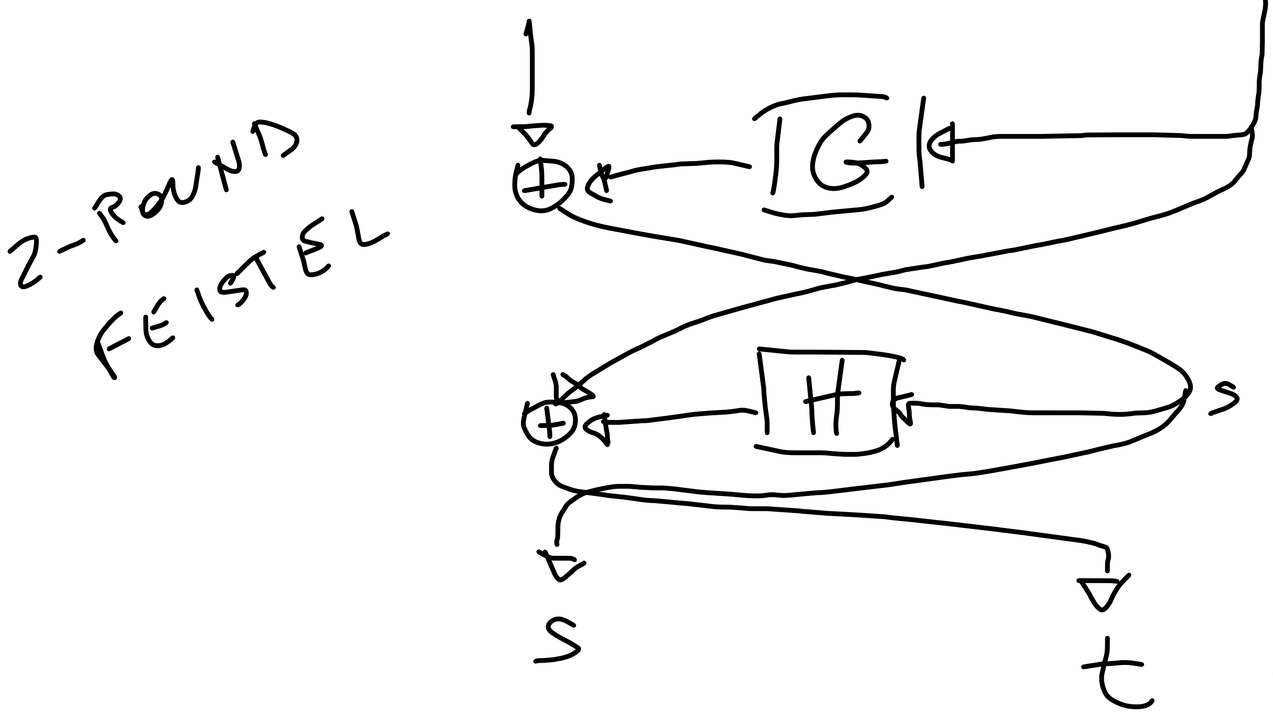
using very limited "decryption queries".

PKCS # 2.0.

ℓ-bit msg

$m' = m \| 0^{\lambda_1}$

$r \in \{0,1\}^{\lambda_0}$ RANDOM



$s = m' \oplus G(r) \in \{0,1\}^{\ell+\lambda_1}$

$t = r \oplus H(s) \in \{0,1\}^{\lambda_0}$

$c = (s \| t)^e \bmod n$

Provable security?

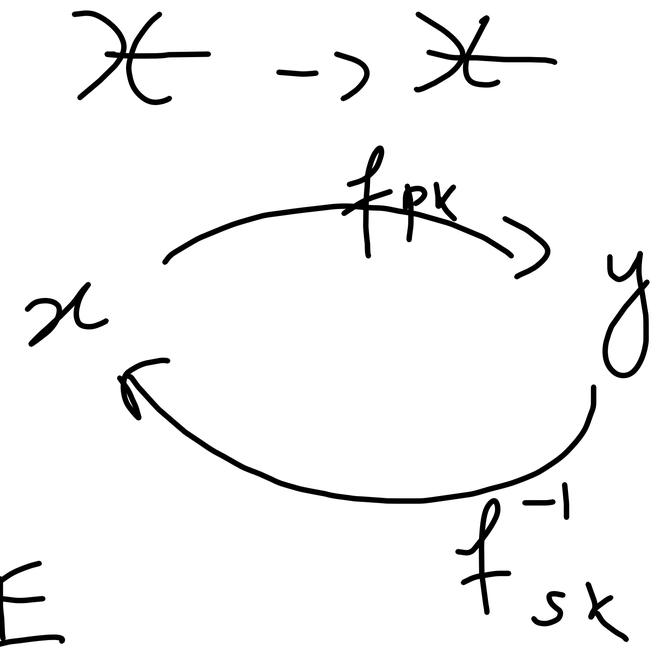
- RSA assumption
- G, H random oracles (IDEAL HASH FUNC.)

DEF (TDP). $\Pi = (Kgen, f, f^{-1})$

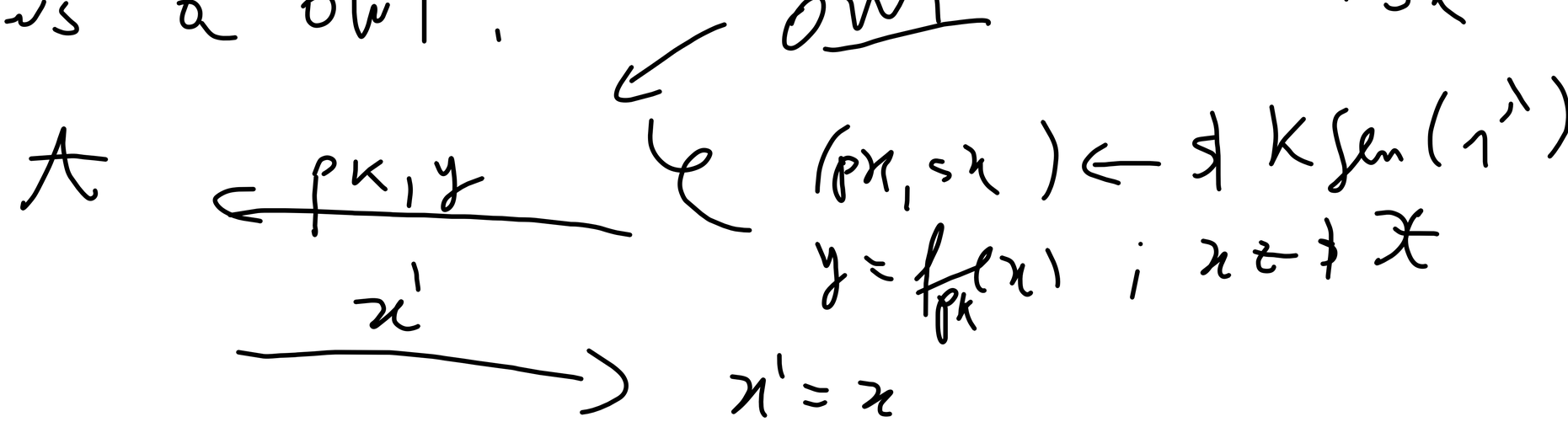
s.t. $(pk, sk) \leftarrow\$ Kgen(1^\lambda)$

$f_{pk}(x) = y$ i $f_{pk} : \mathcal{X} \to \mathcal{X}$

$f^{-1}_{sk}(y) = x$



cual f_{pk} es a OWP:



OBS. The RSA $\Pi = (KGen, f, f^{-1})$ s.t.

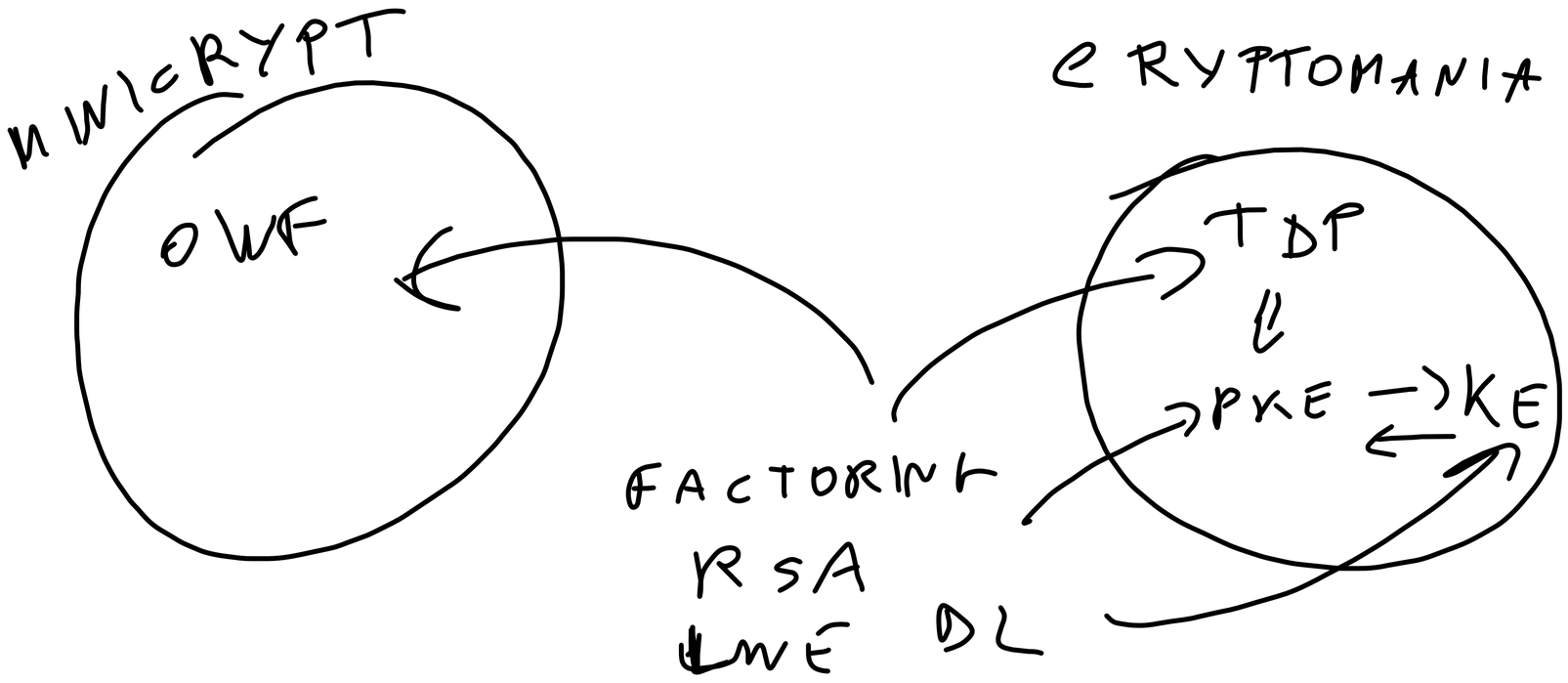
$$pk = (n, e) \qquad sk = (n, d$$

$$e \cdot d \equiv 1 \bmod \varphi(n)$$

$$f_{pk}(x) = x^e \bmod n = y$$

$$f^{-1}_{sk}(y) = y^d \bmod n. = x$$

This is a TDP under RSA assumption.



TDP ⇒ CPA PKE.

$(Kgen, f, f^{-1}) \Rightarrow (pk, sk) \leftarrow Kgen(1^\lambda)$

$Enc(pk, m) = \left(f_{pk}(r),\ h_{pk}(r) \oplus m\right)\ ;\ r \leftarrow \{0,1\}^n$

$Dec(sk, (c_1, c_2)) = h\left(f^{-1}_{sk}(c_1)\right) \oplus c_2 = m$

HARD-CORE BIT of f

Ex. Show that CPA secure PKE for $M = \{0,1\}$ implies CPA-secure PKE for $M = \{0,1\}^t$ for $t = \text{poly}(\lambda)$.

DDH $\Rightarrow$ PKE (CPA). Elgamal PKE. ('84)

-) $\underline{\text{Kgen}(1^\lambda)}$: params $= (\mathbb{G}, g, q) \leftarrow\!\$\ \text{GroupGen}(1^\lambda)$

$x \leftarrow\!\$\ \mathbb{Z}_q$; $pk = (\text{params}, h)$ $h = g^x$ (x-times)

$sk = x$

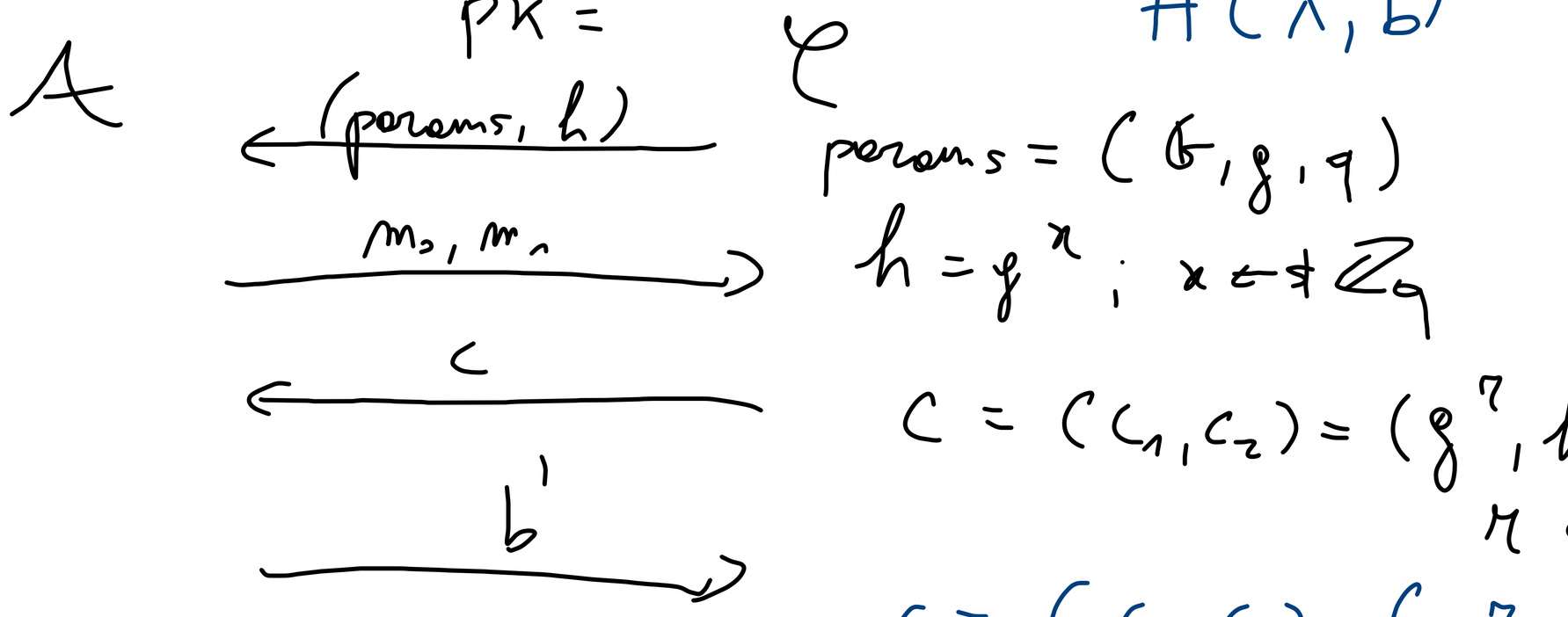
-) $\underline{\text{Enc}(pk, m)}$: $c = (c_1, c_2) = (g^r, h^r \cdot m)$; $r \leftarrow\!\$\ \mathbb{Z}_q$

($r \xleftarrow{\in} \mathbb{G}$, g^r)

-) $\underline{\text{Dec}(sk, (c_1, c_2))}$: $\dfrac{c_2}{c_1^x} = \dfrac{h^r \cdot m}{(g^r)^x} = \dfrac{h^r \cdot m}{(g^x)^r} = m$ ✓

THM ElGamal is CPA secure under DDH.

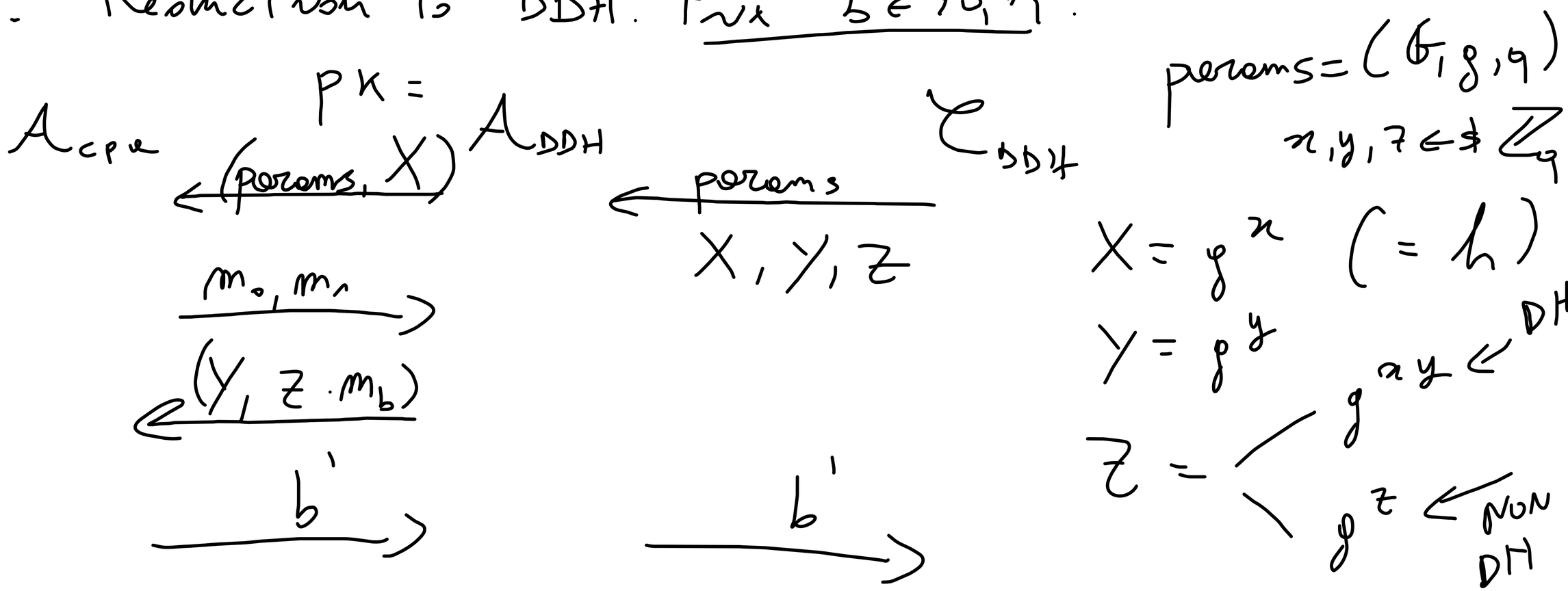
Proof. Start with original $GAME^{cpa}_{\Pi,A}(\lambda,b) \equiv G(\lambda,b)$



Want: $G(\lambda,0) \approx_c G(\lambda,1)$

LEMMA. $G(\lambda, b) \approx_c H(\lambda, b)$, $\forall\, b \in \{0,1\}$.

Proof. Reduction to DDH. For $b \in \{0,1\}$:



Thus: $\Pr[b' = 1 : G(\lambda, b)] = \Pr[b' = 1 : (X, Y, Z) \text{ are DH}]$

$\Pr[b' = 1 : H(\lambda, b)] = \Pr[b' = 1 : (X, Y, Z) \text{ are NON-DH}]$

LEMMA $H(\lambda,0) \equiv H(\lambda,1)$.

Proof. In $H(\lambda,b)$ we have $(c_1, c_2) = (g^x, g^z \cdot m_b)$

$p x = g^x$.

Then g^z is UNIFORM and indep. of everything

and thus $g^z \cdot m_b$ is uniform. So c does not depend on b.

$\square$

$\Rightarrow G(\lambda,0) \approx_c H(\lambda,0) \equiv H(\lambda,1) \approx_c G(\lambda,1)$

$\Rightarrow G(\lambda,0) \approx_c G(\lambda,1)$

Ex. Elgamal NOT CCA-secure. It's malleable.

$$(c_1, c_2) = (g^r, h^r \cdot m)$$

$$\left(c_1 \cdot g^{r'}, c_2 \cdot h^{r'}\right) = \left(\underbrace{g^{r+r'}}, \underbrace{h^{r+r'} \cdot m}\right)$$

RE-RAND.

PARTIAL HOMOMORPHIC:

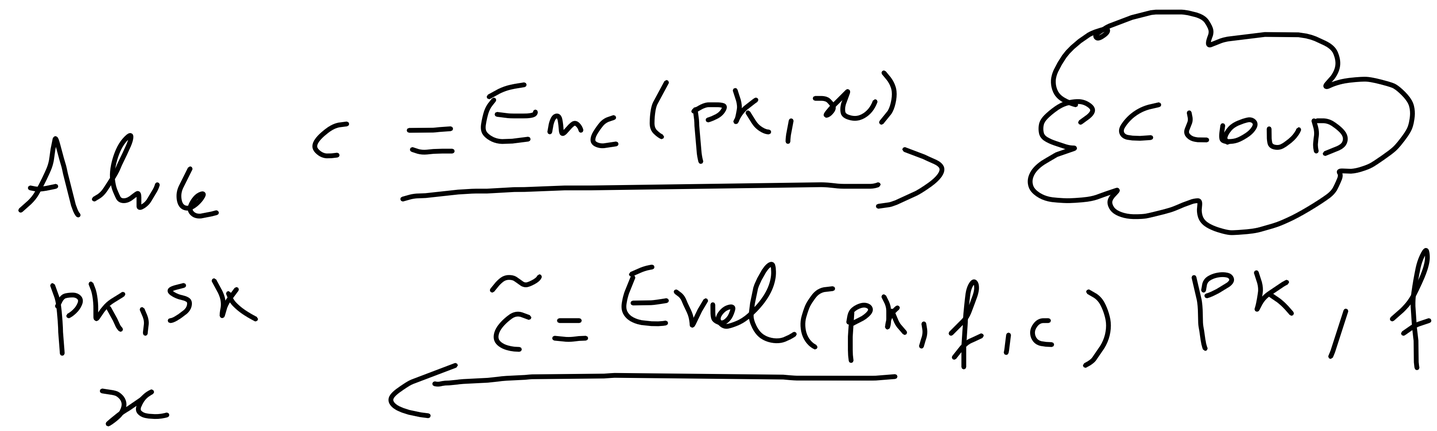
$$(c_1, c_2) = (g^r, h^r \cdot m)$$

$$(c_1', c_2') = (g^{r'}, h^{r'} \cdot m')$$

$$\left(c_1 \cdot c_1', c_2 \cdot c_2'\right) = \left(g^{r+r'}, h^{r+r'} \cdot (m \cdot m')\right)$$

Enc of $m \cdot m'$

In some applications, actually a FEATURE:



FHE ... FULLY HOMOMORPHIC

$Dec(sk, \tilde{c}) = f(x)$, $\forall f, \forall x$

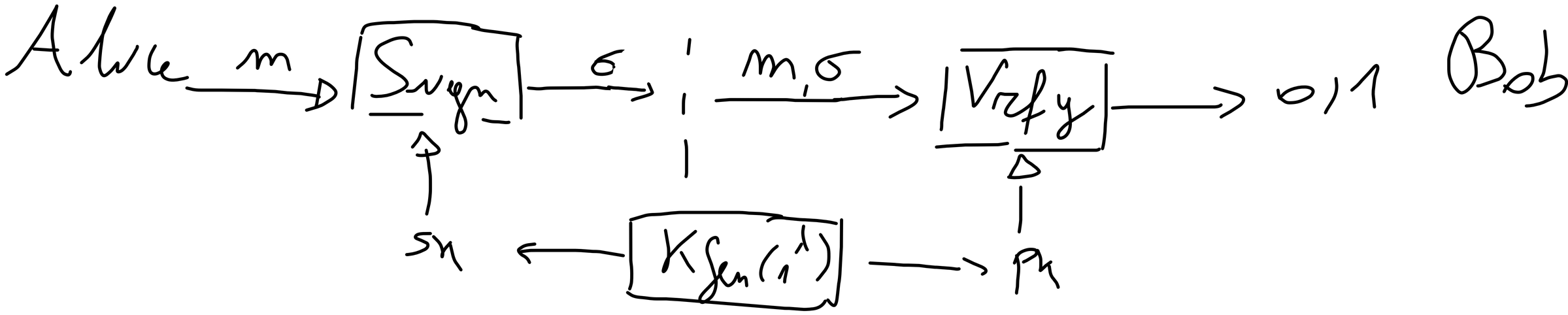
← (CPA)

Does FHE exist? Asked by Rivest around '78.

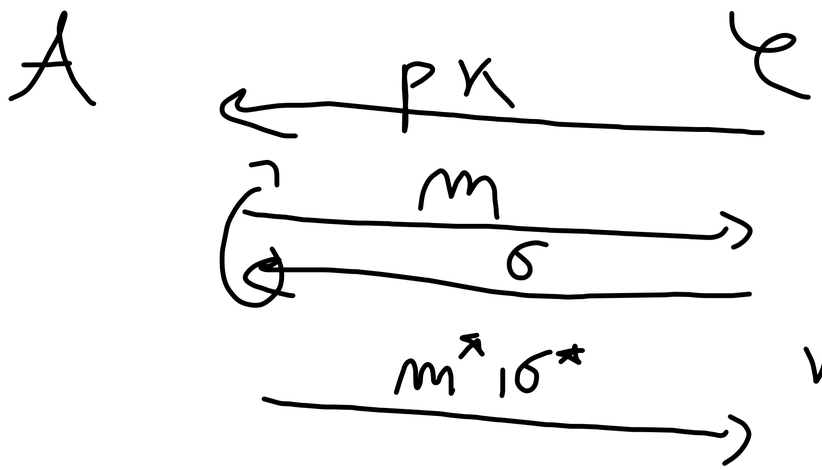
2012: Gentry gave first construction.

Today: LWE

DIGITAL SIGNATURES



DEF (UF-CMA) Π is UFCMA.

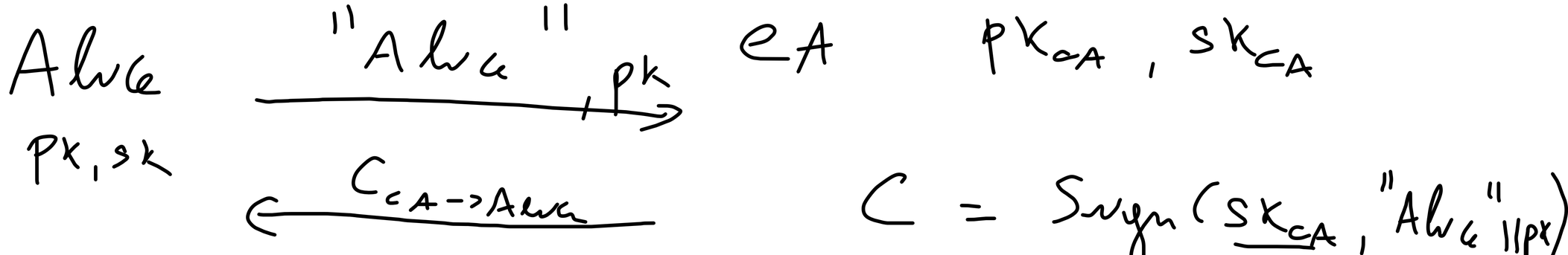


$(pk, sk) \leftarrow\!\$\ Kgen(1^\lambda)$

$\sigma = Sign(sk, m)$

win: $m^* \notin \{m\}$; $Vrfy(pk, (m^*, \sigma^*)) = 1$

Main application: Authentication of pks! (PKI)



UF-CMA: RSA, DL, FACTORING

(OWF)