Leakage-Flexible CCA-secure PKE:

Simple Construction and Free of Pairing

Baodong Qin **Shengli Liu**

Shanghai Jiao Tong University

PKC 2014

March 26, 2014

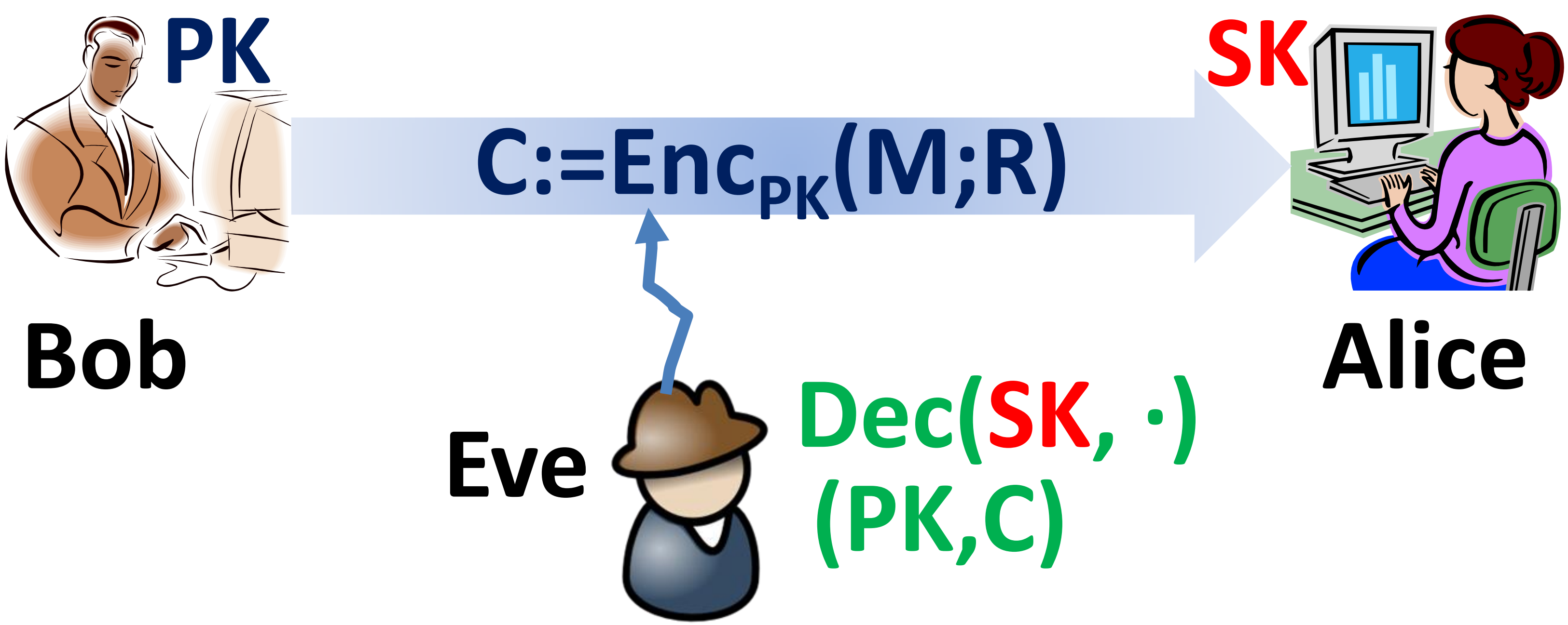
Contents

- Models of Key Leakage
- Previous Constructions and Limitations
- Refined subgroup indistinguishability (RSI) assumption
- Leakage-resilient CCA-secure PKE under the RSI assumptions
- Conclusion

1. Models of Key Leakage

Traditional Security Models

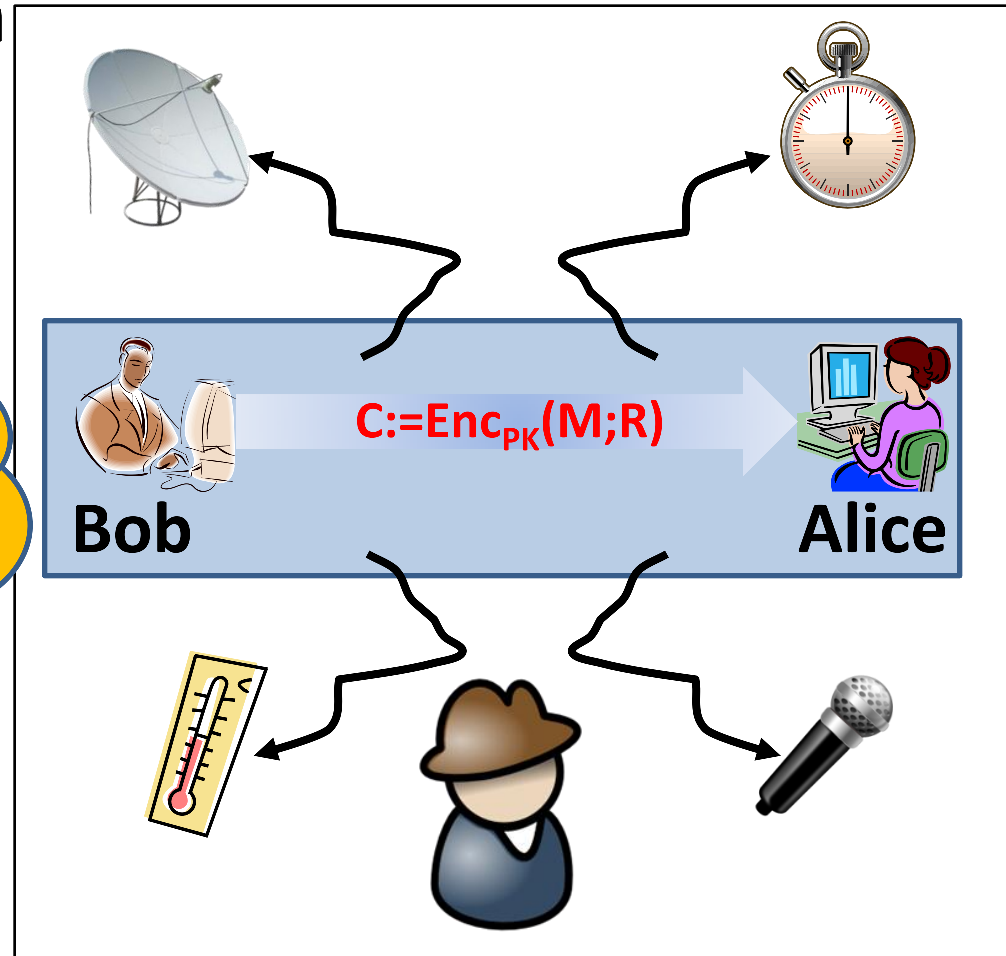
- e.g. public-key setting
  - ✓(SK, R) are private, (PK, C) are public
  - ✓Semantic security[GM84]
  - ✓Chosen-ciphertext security[NY90,RS91]



Real-Life Environments

- Leaking information
  - Electromagnetic radiation
  - Tim...
  - **Memory attack** [HSHCPCFAF08]

Side-channel attacks



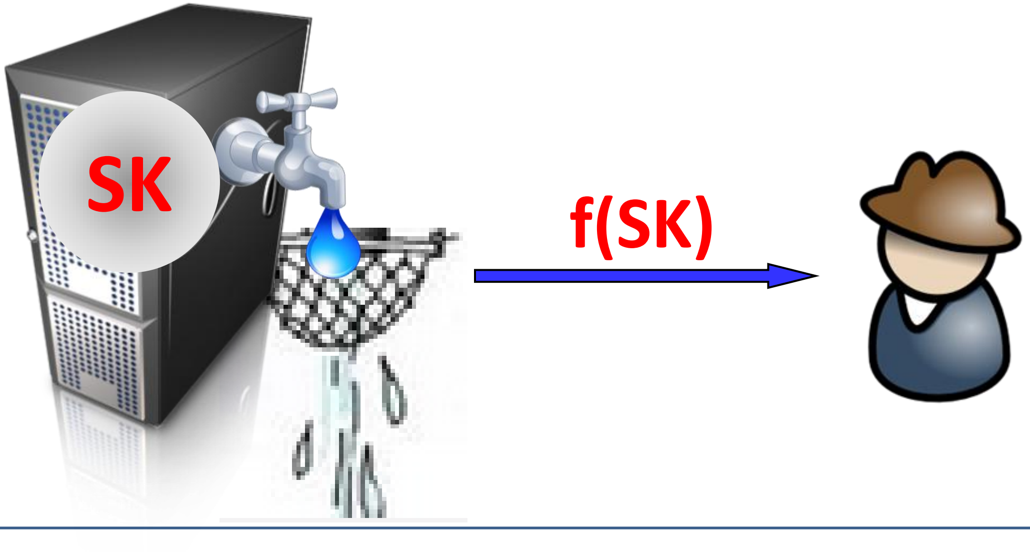
Real-Life Environments

- Leaked information: sounds, power…

✓ Not all information is useful, but some

  ✓ may reveals secret key

✓ How to model key leaks?

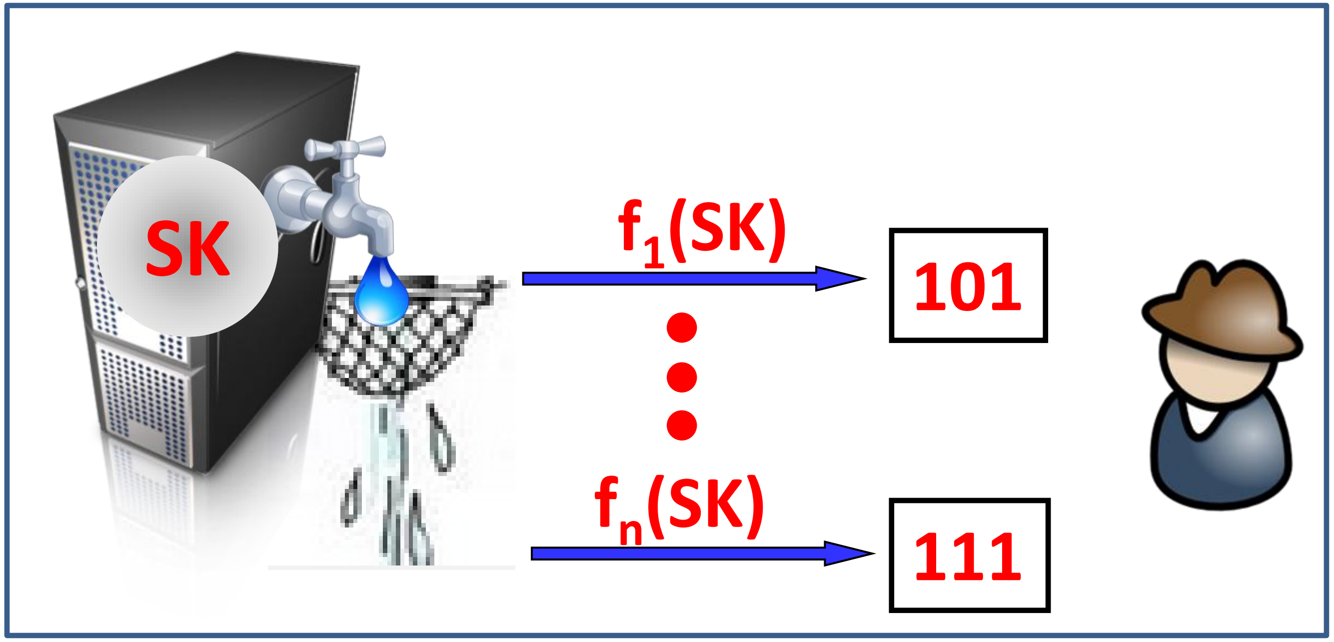


Key Leakage Models

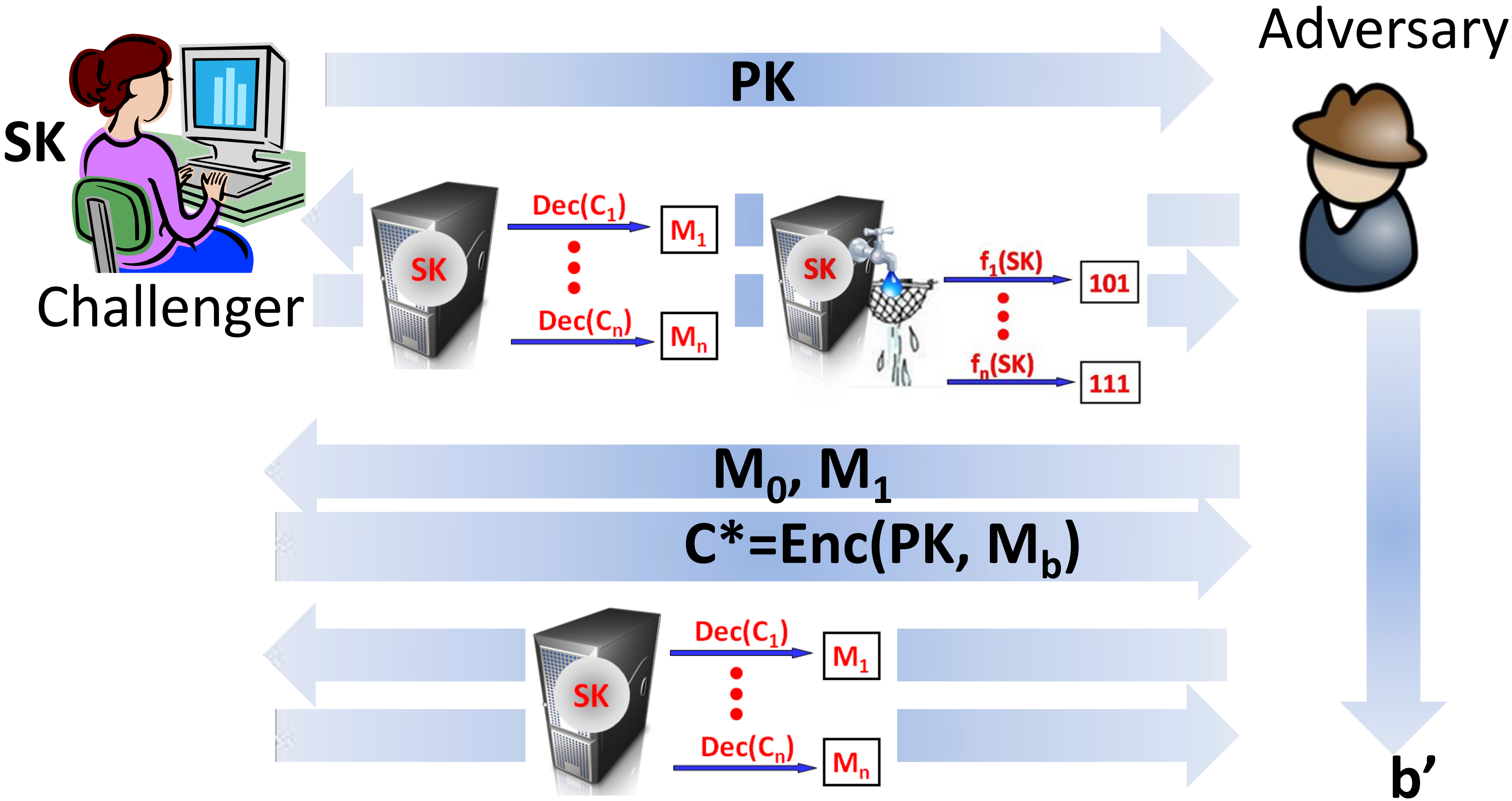
- Only computation leaks information, e.g., [MicaliR04]
- Bounded leakage model, e.g., [AkaviaGV09,NaorS09]
- Continual leakage model, e.g., [BrakerskiKKV10, DodisHLW10]
- Auxiliary input model, e.g. [DodisKL09]
- Continual auxiliary input model, e.g. [YuenCZY12]
- ……

Bounded-Leakage Model

- $\sum |\mathbf{f_i}| \leq \lambda$ (bound)
- Leakage-rate: $\lambda/|SK|$
  - ✓ Leakage flexible if $\lambda/|SK|=1-o(1)$



Leakage-resilient CCA PKE



Advantage:=|Pr[b=b']-1/2|

2. Previous Constructs and Limitations

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

Previous Constructions

- Against pas... k...

Leakage-flexible CCA PKE

[DHLW10,GHV12]

Practical, but complicated construction, involve pairing

[... ...,...]

✓**Good** security, **good** efficiency, **lower** leakage rate

✓**Good** security, **good** efficiency, **higher** leakage rate

✓**Good** security, **bad** efficiency, **flexible** leakage

Good security, **good** efficiency, **flexible** leakage ??

Our Contributions

- General instantiation of [QL13] LR-CCA , applying universal hash proof system[CS02] and one-time lossy filter [QL13]
  - **Refined subgroup indistinguishability (RSI)** assumption, Including DCR, QR…
- **Improved leakage-rate:** From 1/2-o(1) to 1-o(1)
  - 1/2-o(1) (DDH, DCR) from [QL13], improved to
  - **leakage-flexible CCA-secure PKE**
    - **Practical, Simple construction, Without pairing**
    - **Under a special RSI assumption**

3. RSI Assumption

RSI Assumption

- Group description: (G, T, g, h), such that
  - $G=G_1 x G_2$
  - G_1 and G_2 are cyclic groups; g and h are generators.

    r_1:=ord(g), r_2:=ord(h)
  - $gcd(r_1,r_2)=1$ (==> G is also a cyclic group)
  - Elements in G are efficiently checkable.
  - An upper bound $T \geq r_1 \times r_2$.

$$\{x \leftarrow Z_T\} \approx_s \{x \leftarrow Z_{r1 \times r2}\}$$

RSI Assumption

$$\{w: w \leftarrow G_1\} \approx_c \{w: w \leftarrow G\}$$

$$\Downarrow$$

$$\{w: w \leftarrow G_1\} \approx_c \{w: w \leftarrow G \backslash G_1\}$$

$$g^x \approx_c g^x \cdot h$$

x is uniform over {1,…, T}

Example: a special RSI assumption (G, T, g, h)

- $P=2pq+1$

  P, p, q primes

- Group: Quadratic residues

  $G=QR_P=G_p x G_q$

  $T=pq$,

  $x \in QR_P$, $g=x^q$, $h=x^p$

- Assumption: $G_p \approx_c QR_P$

G. Nieto, et.al [NBD2005]

4. From RSI to PKE

From RSI (G, T, g, h) to Hash Proof System

- Subset membership problem

  Valid vs Invalid $\boxed{G_1 \approx_c G \backslash G_1}$

- Projective hash $\{H_{sk}: G \rightarrow G\}$, $sk \leftarrow Z_T$:

  $$\boxed{pk = g^{sk}, \quad H_{sk}(c) = c^{sk} \quad (c \in G)}$$

- If $c = g^r \in G_1$ with witness r, then

  $$\boxed{H_{sk}(c) = (pk)^r = g^{sk \cdot r} = g^{r \cdot sk} = c^{sk}}$$

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

From RSI to Hash Proof System

- **ε -universal HPS**:
  for $c \in G \backslash G_1$, the guess probability of value $H_{sk}(c)$ conditioned on pk, is at most **ε**.
- Suppose $e \geq 2$ is the smallest prime factor of r_1. Then **HPS is 1/e universal**
- Reduce the guess probability to $\mathbf{1/e^n}$ by

  n-fold parallelization.

$H_{sk1}(c)=c^{sk1}$ $H_{sk2}(c)=c^{sk2}$ … $H_{skn}(c)=c^{skn}$

$H_{sk1}(c)=pk_1^r$ $H_{sk2}(c)=pk_2^r$ … $H_{skn}(c)=pk_n^r$

From RSI to One-Time Lossy Filter

- (Dom, ℓ)-One-time lossy filter: (FGen, FEval, FTag)
  - FGen(1^κ) → (ek, td); ek also determines a tag space $\mathcal{T}$, $\mathcal{T}_{inj} \subset \mathcal{T}, \mathcal{T}_{lossy} \subset \mathcal{T}, \mathcal{T}_{inj} \cap \mathcal{T}_{lossy} = \emptyset$
  - FEval(ek, t, x) computes $f_{ek,t}(x)$.

    If $t=(t_a, t_c) \in \mathcal{T}_{inj}$, $f_{ek,t}(x)$ is injective.

    If $t=(t_a, t_c) \in \mathcal{T}_{lossy}$, $f_{ek,t}(x)$ has at most 2^ℓ values.
  - FTag(td, t_a) → t_c, such that $t=(t_a, t_c)$ is a lossy tag.

Indistinguishability:

$\{ (ek, (t_a, t_c)) \}_{\text{random } tc} \approx_c \{ (ek, (t_a, t_c')) \}_{tc' = FTag(td, ta)}$

Evasiveness

Given a lossy tag (t_a, t_c'), it is hard to get a new non-injective one.

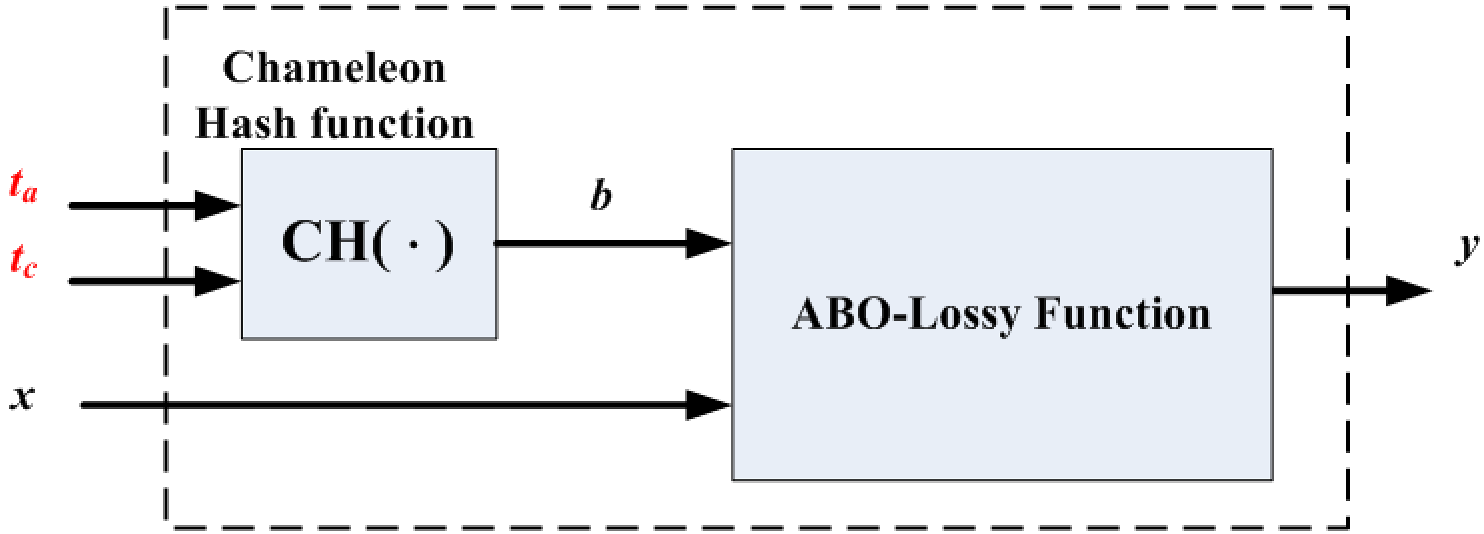
From RSI to One-Time Lossy Filter

- Construction idea
- All-but-one lossy function + chameleon hash function
- All-but-one lossy function: all tags are injective except one lossy t*

$$t^*=CH.Eval(t_a; t_c)$$

From RSI to One-Time Lossy Filter

- Constructing ABO-Lossy Function from RSI
- Constructing OT-LF from Chameleon Hash and ABO-Lossy Function



General Construction of One-Time Lossy Filter

From RSI to One-Time Lossy Filter

- ABO-lossy function from RSI assumption
- A simple example: (G, T, g, h)

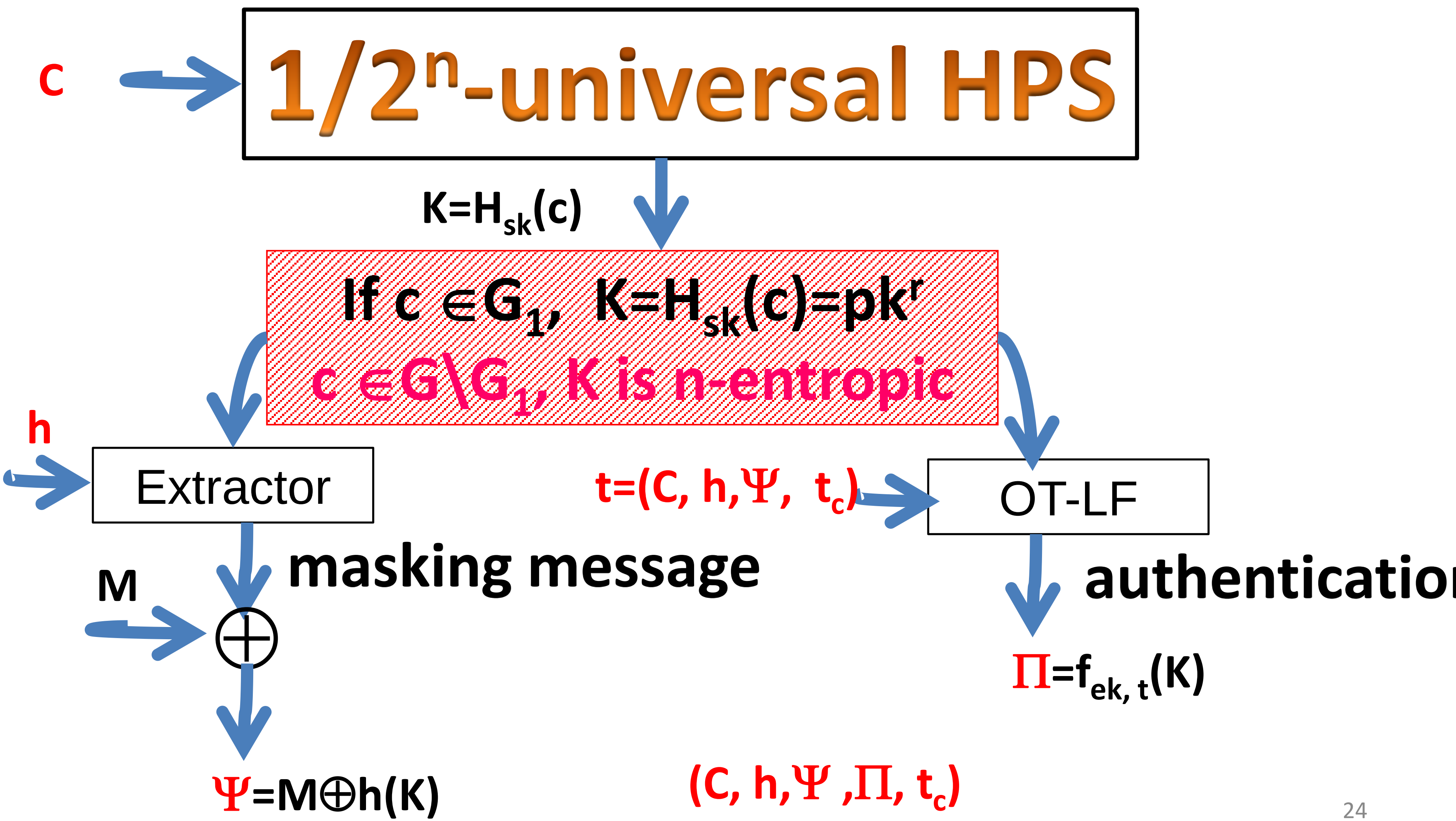
$$ek=g^s \bullet h^{-b^*}$$

- $F_{abo}(ek, b, x)=(g^s \bullet h^{-b^*} \bullet h^b)^x=(g^s \bullet h^{b-b^*})^x$

$$x \in Z_T$$

- If $b=b^*$, then $F_{abo}(ek, b,x)=g^{sx} \in G_1$, hence $|F_{abo}(b^*,x)| \le r_1$.
- If $b \neq b^*$, then $(g^s h^{b-b^*})^x$ is injective, since $g^s h^{b-b^*}$ is a generator of G.

Final Step: PKE = HPS + OT-LF



Parameters

- $P=2pq+1$, $G=QR_P=G_p x G_q$, $T=pq$
- HPS is 1/q-univeral

$$|p|=512,\ |q|>512$$

$$|SK|=\log pq=512+\log q$$
$$\lambda=\log q - m - \log p - \omega\log(\kappa)$$
$$=\log q - 80-512-160=\log q - 752$$

For sufficiently large q, leakage-rate:

$$\lambda/|SK| \rightarrow 1-o(1)$$

Comparison

Table 1: Parameters of leakage-flexible CCA-secure PKE schemes

Scheme	Group Type	Assumption	Group Size # bits	Ciphertext Size # $\mathbb{G}$	Pairing
DHLW10	Prime	SXDH	160	$\lceil (2/\alpha)(2+1/2) \rceil + 16$	Yes
DHLW10	Prime	DLIN	160	$\lceil (3/\alpha)(3+1/2) \rceil + 35$	Yes
GHV12	Prime	DLIN	160	$2\lceil 4/\alpha \rceil + 6$	Yes
This paper	Composite	RSI	$\lceil 1264/\alpha \rceil$	2	**No**

$\alpha \in [0,1)$ is the leakage-rate.

SHANGHAI JIAO TONG UNIVERSITY

Conclusion

- A general assumption: RSI
- Improve leakage rate 1/2-o(1) from [QL13] (DDH,DCR) to 1-o(1) under a special RSI assumption.
- The first pairing-free leakage-flexible CCA-secure PKE

Thank you!