Tightly CCA-Secure Encryption without Pairings

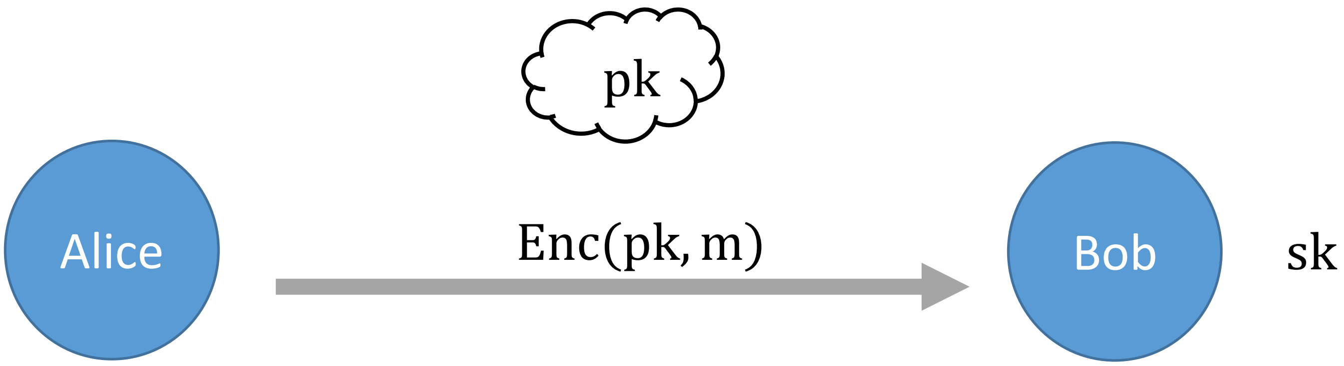
Romain Gay, ENS

Dennis Hofheinz, KIT

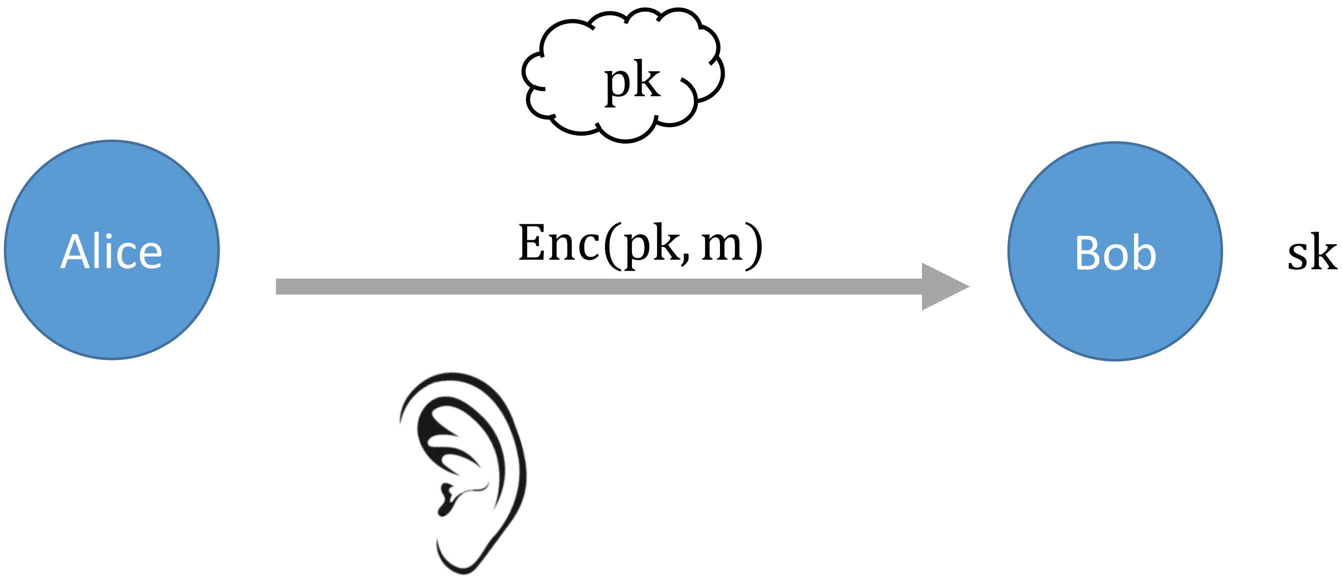
Eike Kiltz, RUB

Hoeteck Wee, ENS

Security of encryption



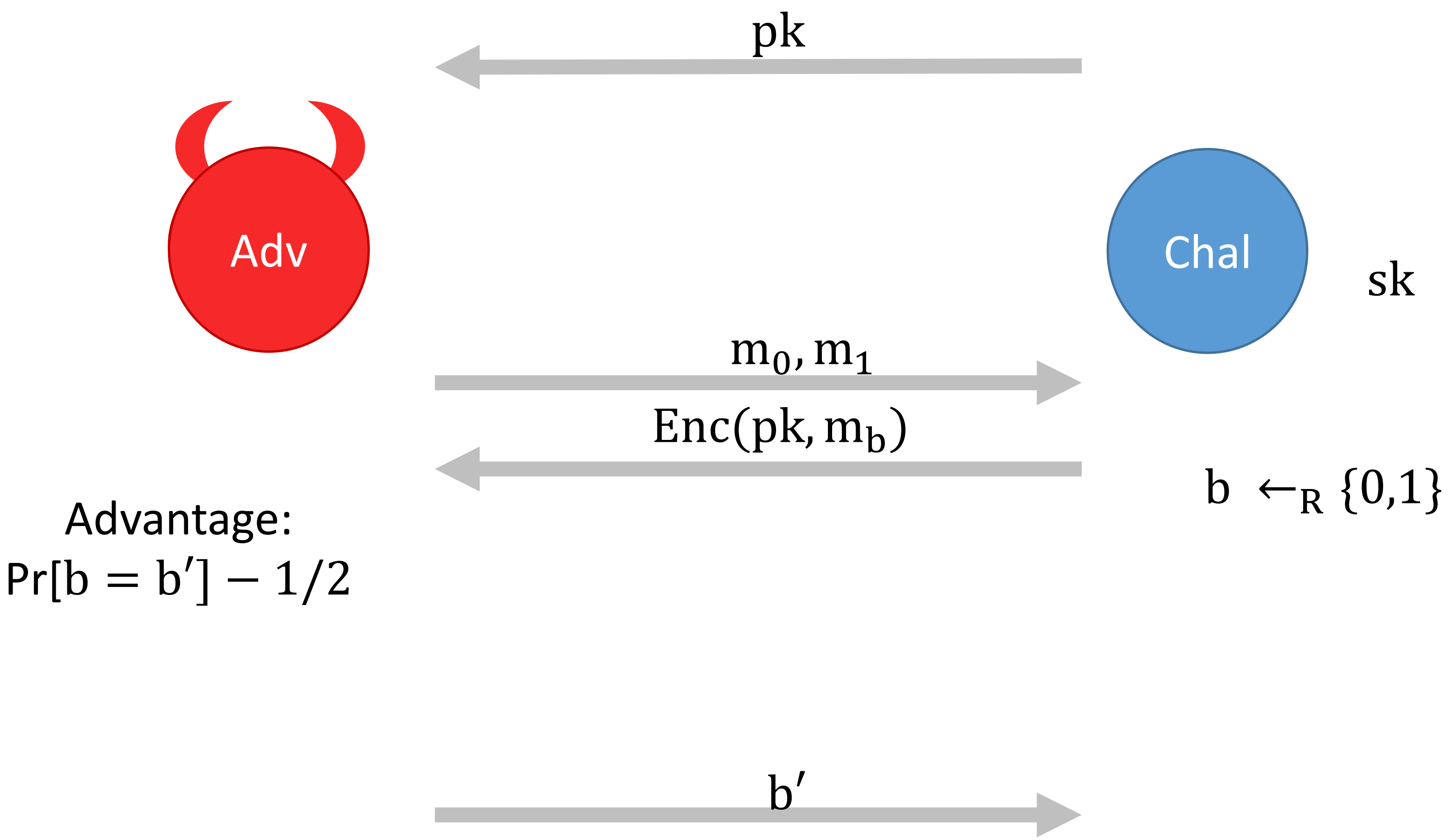
Security of encryption



→ no information on m

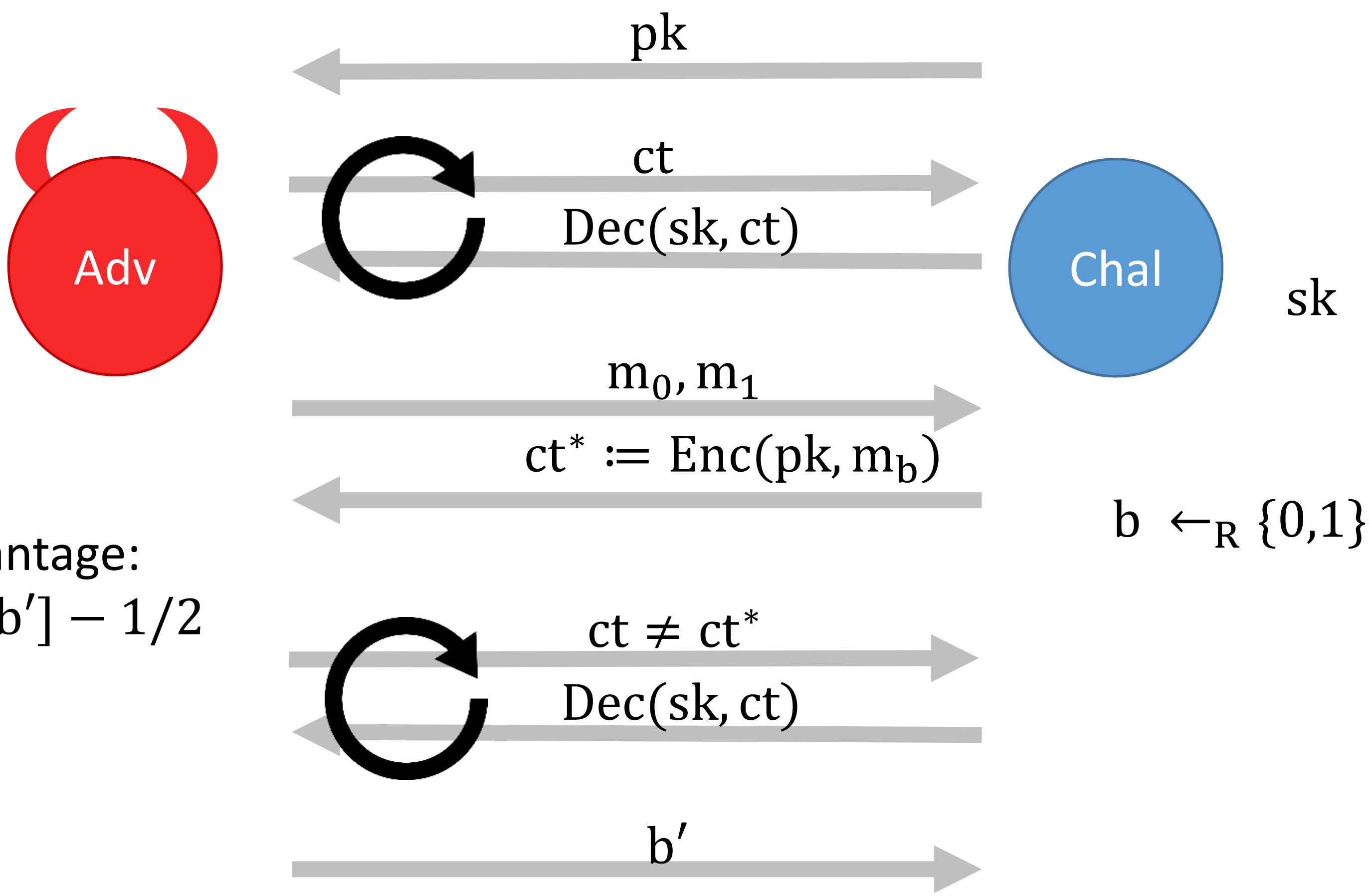
Chosen-Plaintext Attack (CPA)

[Goldwasser, Micali 84]



Chosen-Ciphertext Attack (CCA)

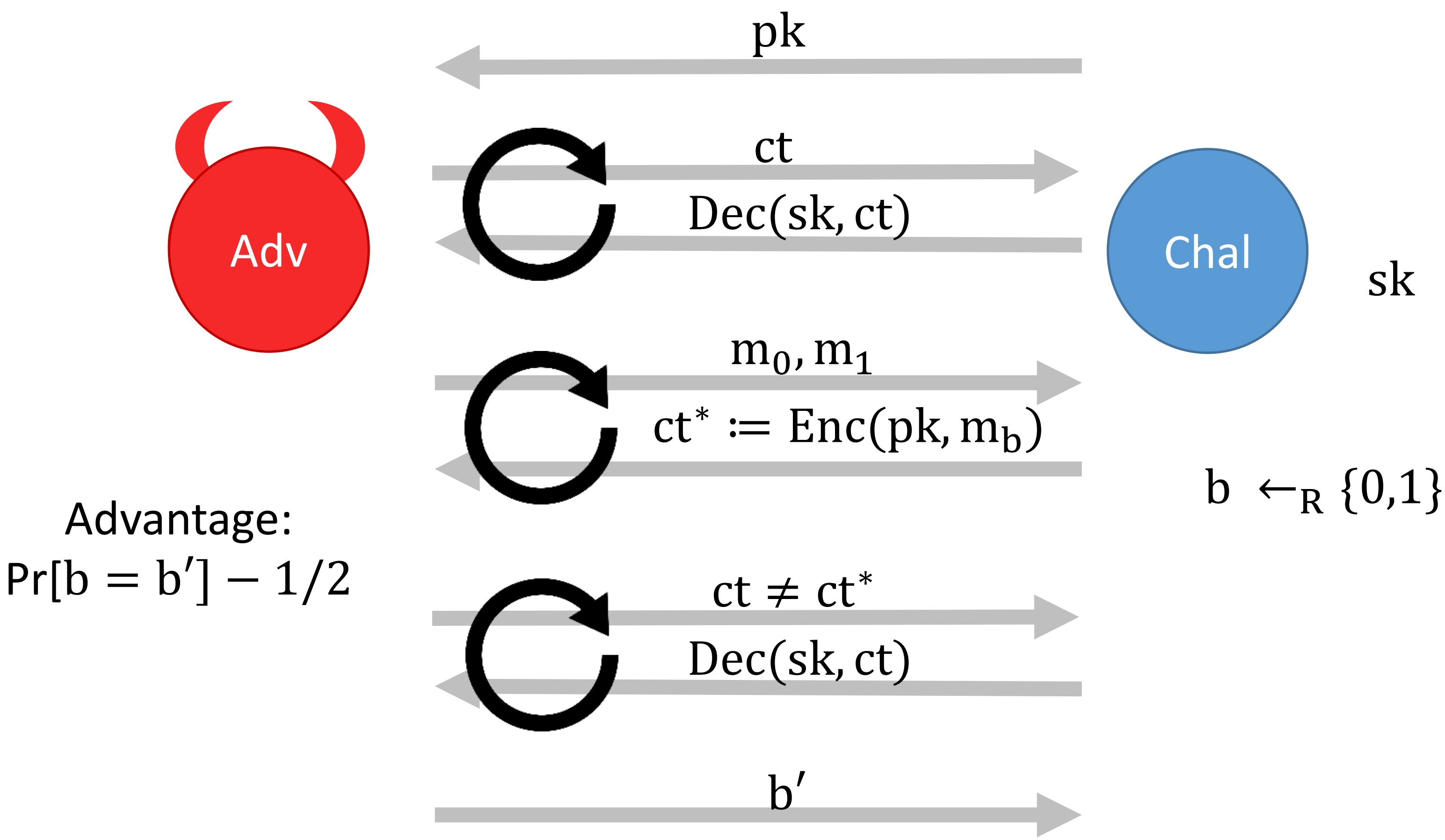
[Rackoff, Simon 91]



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

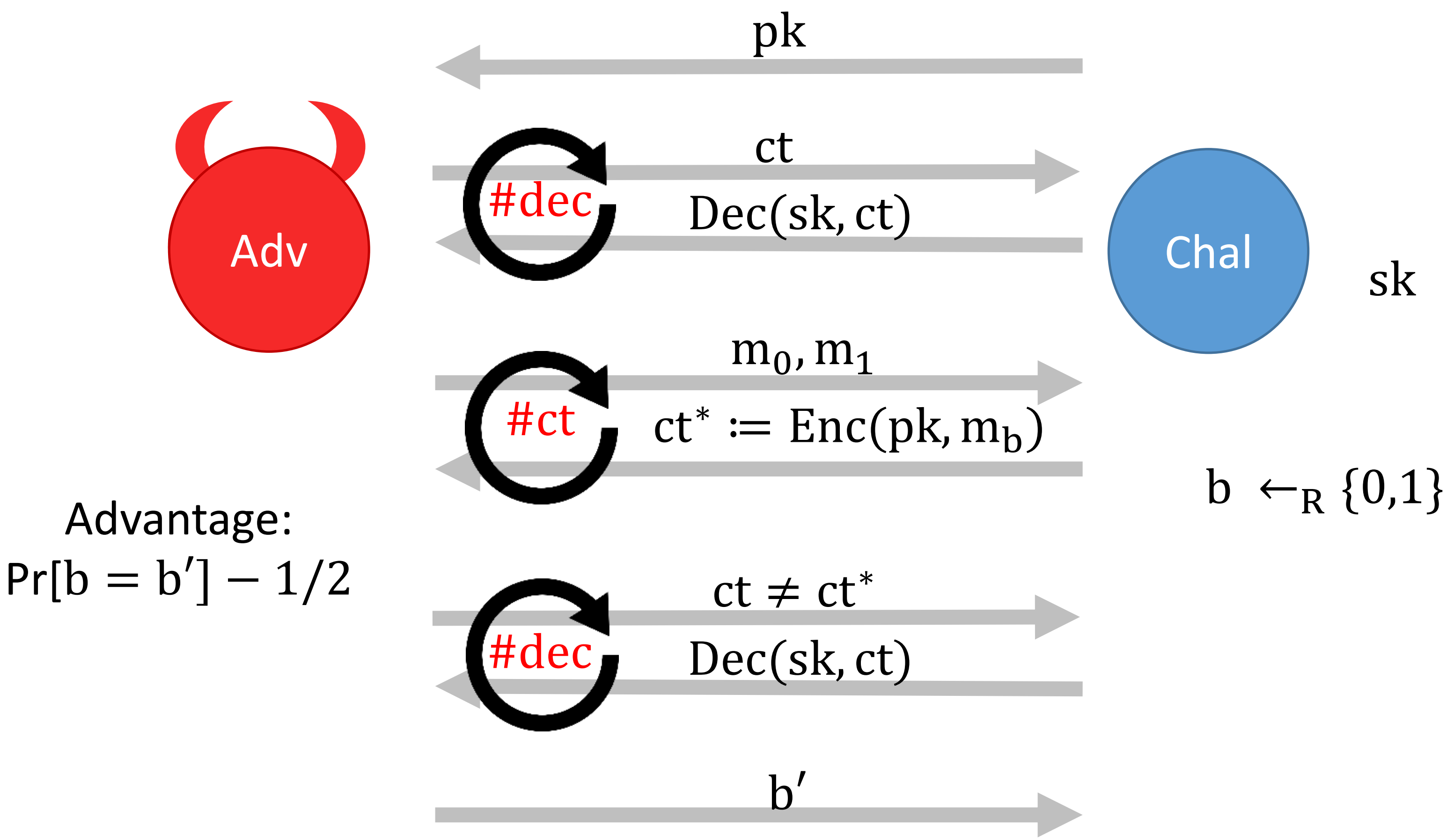
Chosen-Ciphertext Attack (CCA)

[Rackoff, Simon 91]

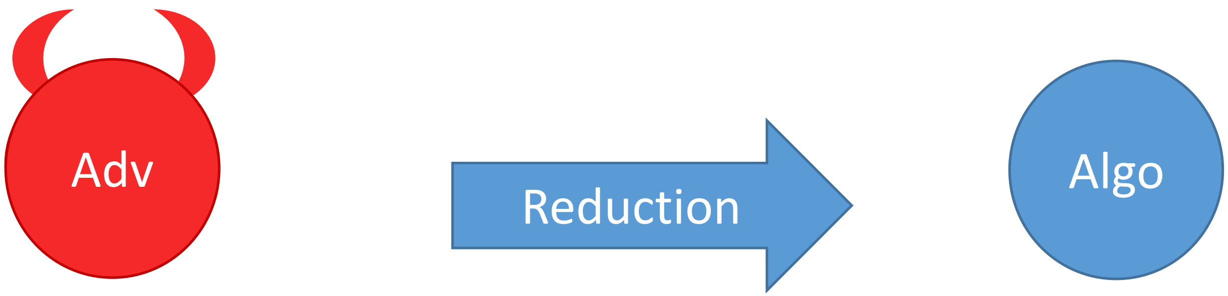


Chosen-Ciphertext Attack (CCA)

[Rackoff, Simon 91]



Tight security



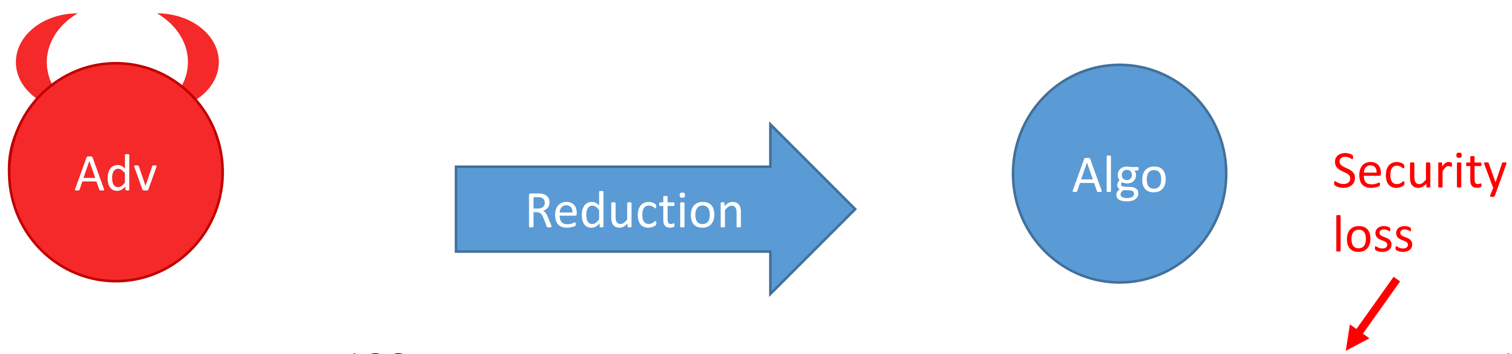
Security loss

Advantage = ε

Advantage = ε/L to break DDH

Non-tight: $\mathrm{L} = \Omega(\#\mathrm{ct})$

Tight security



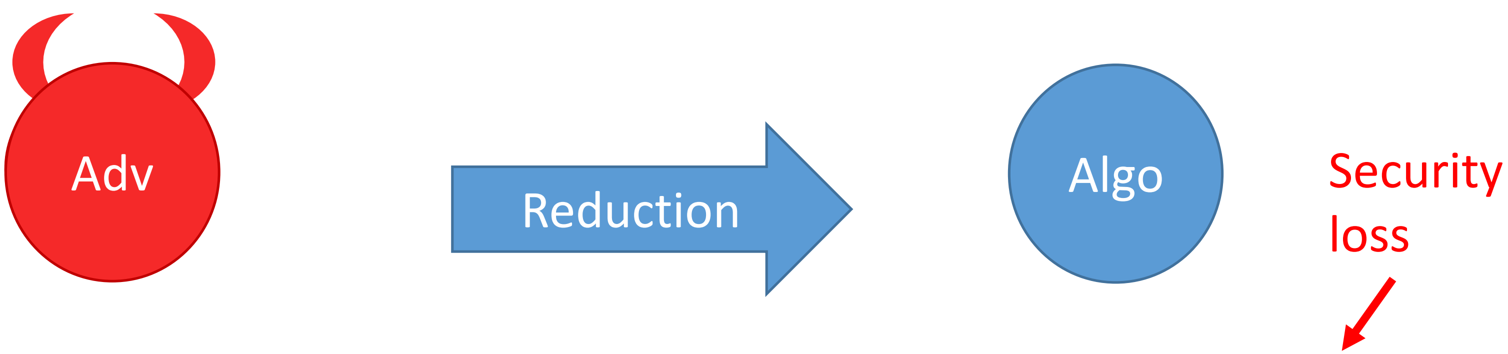
Advantage = $\varepsilon < 2^{-128}$

Advantage = $\varepsilon / L < 2^{-158}$ to break DDH

Non-tight: $L = \#ct = 2^{30}$

Tight security

[Bellare, Boldyreva, Micali 00; Coron 00; Hofheinz, Jager 12]



Advantage = ε

Advantage = ε/L
to break DDH

Tight: $L = \text{"small"}$
e.g. $L = O(\lambda)$

Prior works: CCA-secure encryption

Scheme	|ct|-|m|	Loss L	Assumption
CS 98	3	$\Omega(\#\mathrm{ct})$	DDH
KD 04	2		

Prior works: CCA-secure encryption

Scheme	|ct|-|m|	Loss L	Assumption
CS 98	3	$\Omega(\#ct)$	DDH
KD 04	2		
HJ 12	$O(\lambda)$	$O(1)$	DLIN
LPJY 15	47	$O(\lambda)$	
AHY 15	12		
GCDCT 15	10		SXDH

no pairing

pairings

Prior works: CCA-secure encryption

Scheme	|ct|-|m|	Loss L	Assumption
CS 98	3	$\Omega(\#ct)$	DDH
KD 04	2		
HJ 12	$O(\lambda)$	$O(1)$	DLIN
LPJY 15	47	$O(\lambda)$	
AHY 15	12		
GCDCT 15	10		SXDH

no pairing (CS 98, KD 04)

pairings (HJ 12, LPJY 15, AHY 15, GCDCT 15)

Does tightness require pairings?

Prior works: CCA-secure encryption

Scheme	|ct|-|m|	Loss L	Assumption	
CS 98	3	$\Omega(\#ct)$	DDH	no pairing
KD 04	2			
HJ 12	$O(\lambda)$	$O(1)$	DLIN	pairings
LPJY 15	47	$O(\lambda)$		
AHY 15	12			
GCDCT 15	10		SXDH	
This work	3	$O(\lambda)$	DDH	no pairing

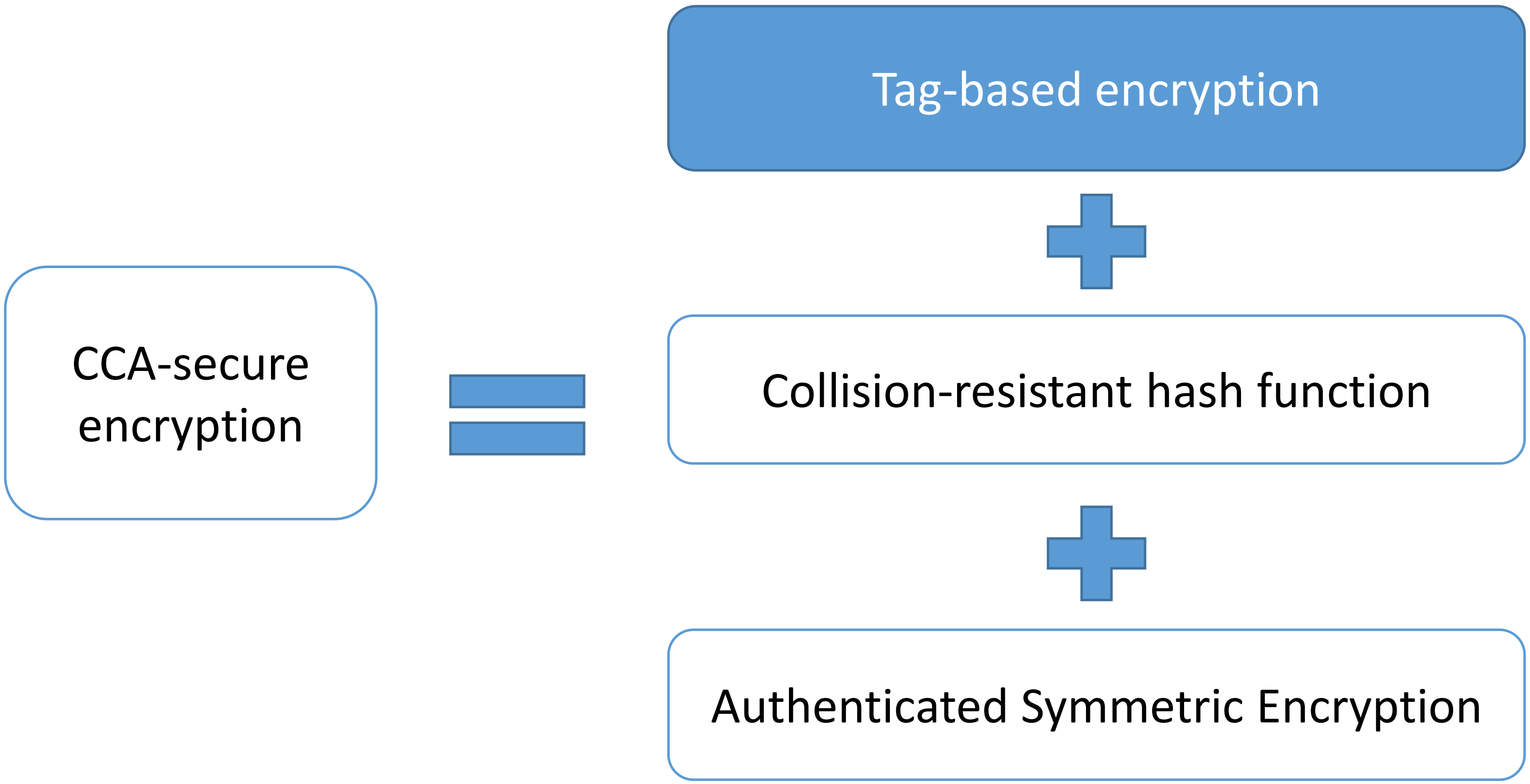
Does tightness require pairings?

No!

Prior works: CCA-secure encryption

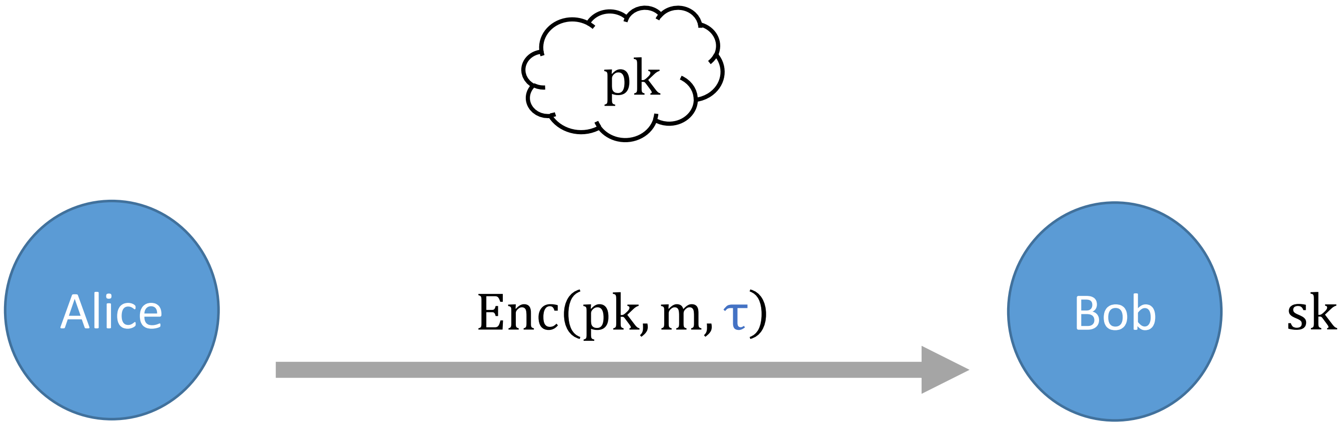
	Scheme	|ct|-|m|	Loss L	Assumption	
	CS 98	3	$\Omega(\#ct)$	DDH	no pairing
	KD 04	2			
Signatures, NIZK	HJ 12	$O(\lambda)$	$O(1)$	DLIN	pairings
	LPJY 15	47	$O(\lambda)$		
Dual System IBE	AHY 15	12			
	GCDCT 15	10		SXDH	
DV-NIZK à la Cramer Shoup	This work	3	$O(\lambda)$	DDH	no pairing

Overview of our construction

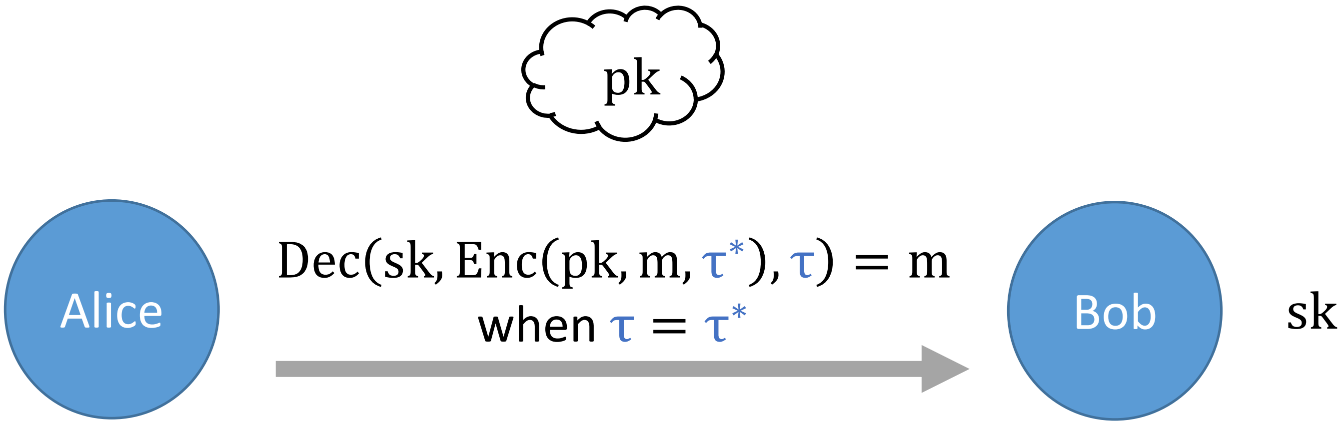


[Kurosawa Desmedt 04, Hofheinz Kiltz 07]

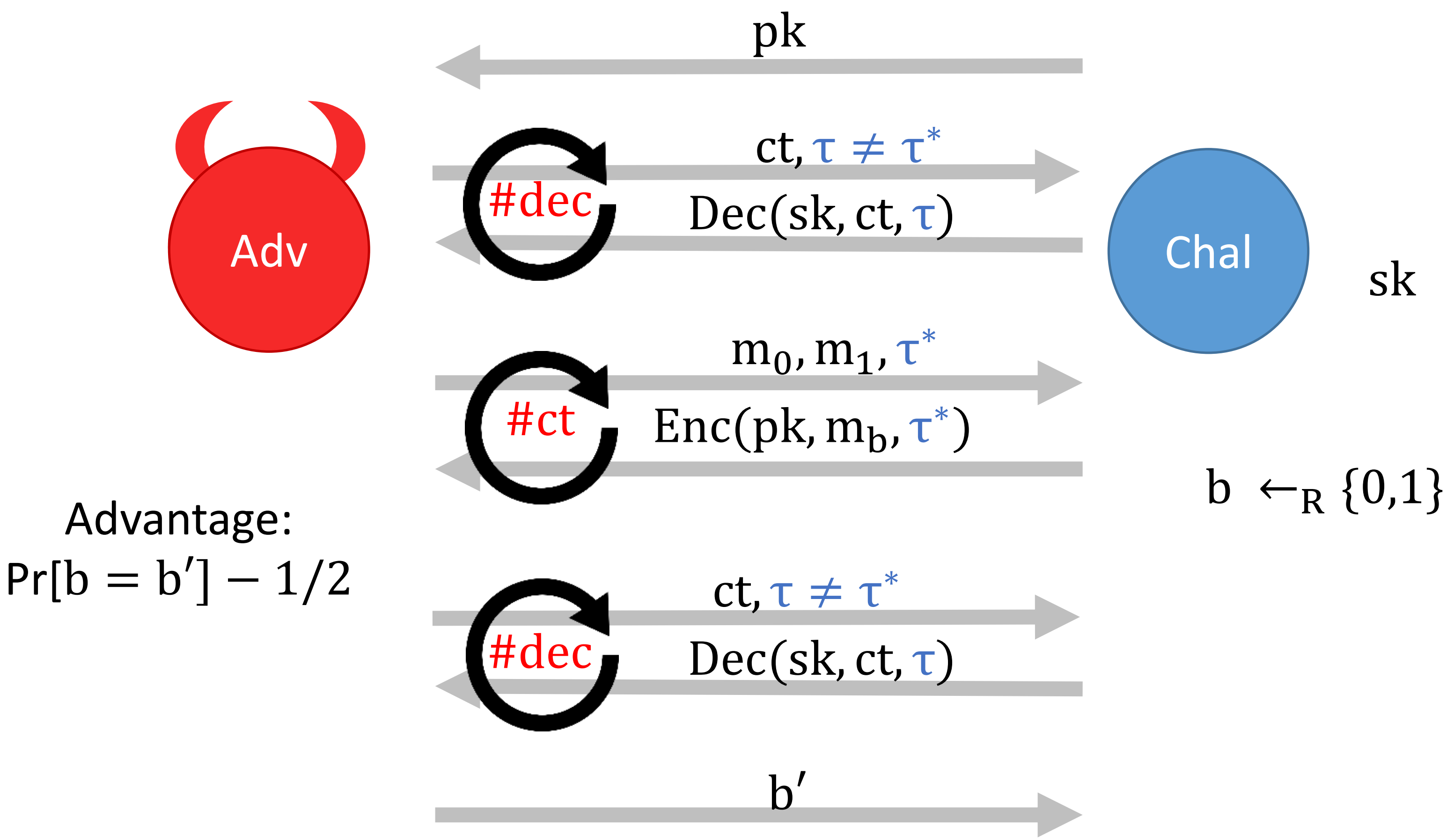
Tag-based encryption



Tag-based encryption



Tag-based encryption



Outline

1. Damgård El Gamal encryption (CPA-secure)
2. Cramer Shoup encryption (non-tight)
3. Our construction (tight)

Damgård El Gamal encryption

[Damgård 91]

$\mathbb{G}$ of order p, generator g.

$$sk = \boxed{\vec{k}} \leftarrow_R \mathbb{Z}_p^2$$

$$pk = \boxed{\vec{a}} = g^{\vec{a}} \leftarrow_R \mathbb{G}^2, \qquad \boxed{\vec{k}} \cdot \boxed{\vec{a}} = g^{\vec{k} \cdot \vec{a}} \in \mathbb{G}$$

Damgård El Gamal encryption

[Damgård 91]

$\mathbb{G}$ of order p, generator g.

$$sk = \vec{k} \leftarrow_R \mathbb{Z}_p^2$$

$$pk = \vec{a} = g^{\vec{a}} \leftarrow_R \mathbb{G}^2, \quad \vec{k} \cdot \vec{a} = g^{\vec{k}\cdot\vec{a}} \in \mathbb{G}$$

$$ct = \vec{a}r = g^{\vec{a}r} \in \mathbb{G}^2, \quad \vec{k} \cdot \vec{a}r \cdot m = g^{\vec{k}\cdot\vec{a}r} \cdot m \in \mathbb{G}$$

where $r \leftarrow_R \mathbb{Z}_p$

Damgård El Gamal encryption

[Damgård 91]

$\mathbb{G}$ of order p, generator g.

$$sk = \boxed{\vec{k}} \leftarrow_R \mathbb{Z}_p^2$$

$$pk = \boxed{\vec{a}} = g^{\vec{a}} \leftarrow_R \mathbb{G}^2, \qquad \boxed{\vec{k}} \cdot \boxed{\vec{a}} = g^{\vec{k}\cdot\vec{a}} \in \mathbb{G}$$

$$ct = \boxed{\vec{u}} \leftarrow_R \mathbb{G}^2, \qquad \boxed{\vec{k}} \cdot \boxed{\vec{u}} \cdot m = g^{\vec{k}\cdot\vec{u}} \cdot m \in \mathbb{G}$$

Damgård El Gamal encryption

[Damgård 91]

$\mathbb{G}$ of order p, generator g.

$$\text{sk} = \vec{k} \leftarrow_R \mathbb{Z}_p^2$$

$$\text{pk} = \vec{a} = g^{\vec{a}} \leftarrow_R \mathbb{G}^2, \qquad \vec{k} \cdot \vec{a} = g^{\vec{k}\cdot\vec{a}} \in \mathbb{G}$$

independent

$$\text{ct} = \vec{u} \leftarrow_R \mathbb{G}^2, \qquad \vec{k} \cdot \vec{u} \cdot m = g^{\vec{k}\cdot\vec{u}} \cdot m \in \mathbb{G}$$

Cramer Shoup encryption

[Cramer Shoup 98]

$$\boxed{\vec{k}} \leftarrow_R \mathbb{Z}_p^2$$

$$\boxed{\vec{k}_0} \leftarrow_R \mathbb{Z}_p^2$$

$$\boxed{\vec{k}_1} \leftarrow_R \mathbb{Z}_p^2$$

$$\tau \in \mathbb{Z}_p \mapsto \boxed{\vec{k}_\tau := \vec{k}_0 + \tau\vec{k}_1} \in \mathbb{Z}_p^2$$

Cramer Shoup encryption

[Cramer Shoup 98]

$\boxed{\vec{k}} \leftarrow_R \mathbb{Z}_p^2$ ⇒ $\boxed{\vec{k}_0} \leftarrow_R \mathbb{Z}_p^2$, $\boxed{\vec{k}_1} \leftarrow_R \mathbb{Z}_p^2$

$$\tau \in \mathbb{Z}_p \mapsto \boxed{\vec{k}_\tau := \vec{k}_0 + \tau \vec{k}_1} \in \mathbb{Z}_p^2$$

Pairwise independent hash function

Cramer Shoup encryption

[Cramer Shoup 98]

$\boxed{\vec{k}} \leftarrow_R \mathbb{Z}_p^2 \quad \Rightarrow \quad \boxed{\vec{k}_0} \leftarrow_R \mathbb{Z}_p^2, \quad \boxed{\vec{k}_1} \leftarrow_R \mathbb{Z}_p^2$

$$\tau \in \mathbb{Z}_p \mapsto \boxed{\vec{k}_\tau := \vec{k}_0 + \tau \vec{k}_1} \in \mathbb{Z}_p^2$$

Pairwise independent hash function

$\boxed{\vec{k}_\tau}$ independent of $\boxed{\vec{k}_{\tau^*}}$

for $\tau \neq \tau^*$

Cramer Shoup encryption

[Cramer Shoup 98]

$$sk = \boxed{\vec{k}_0} \ \boxed{\vec{k}_1} \leftarrow_R \mathbb{Z}_p^2$$

$$pk = \vec{a} \leftarrow_R \mathbb{G}^2, \ \boxed{\vec{k}_0} \cdot \vec{a} \in \mathbb{G}, \ \boxed{\vec{k}_1} \cdot \vec{a} \in \mathbb{G}$$

$$ct_\tau = \vec{a}r \in \mathbb{G}^2, \quad \boxed{\vec{k}_0 + \tau\vec{k}_1} \cdot \vec{a}r \cdot m \in \mathbb{G}$$

where $r \leftarrow_R \mathbb{Z}_p$

Cramer Shoup encryption

[Cramer Shoup 98]

$\mathrm{ct}_{\tau^*} = \boxed{\vec{a}\mathrm{r}}\ ,\ \boxed{\vec{k}_{\tau^*}} \cdot \boxed{\vec{a}\mathrm{r}} \cdot \mathrm{m}$

$\mathrm{Dec}(\cdot, \tau)$: uses $\boxed{\vec{k}_{\tau}}$

for $\tau \neq \tau^*$

Cramer Shoup encryption

[Cramer Shoup 98]

$$ct_{\tau^*} = \vec{a}r \, , \, \vec{k}_{\tau^*} \cdot \vec{a}r \cdot m$$

Dec$(\cdot, \tau)$: uses $\vec{k}_{\tau}$

Pairwise independence

for $\tau \neq \tau^*$

Cramer Shoup encryption

[Cramer Shoup 98]

#ct

$\vdots$

$ct_{\tau^*_{i-1}}$

$ct_{\tau^*_i} = \boxed{\vec{a}r_i}, \boxed{\vec{k}_{\tau^*_i}} \cdot \boxed{\vec{a}r_i} \cdot m_i$

$ct_{\tau^*_{i+1}}$

$\vdots$

$\vdots$

$Dec(\cdot, \tau_{j-1})$

$Dec(\cdot, \tau_j)$: uses $\boxed{\vec{k}_{\tau_j}}$

$Dec(\cdot, \tau_{j+1})$

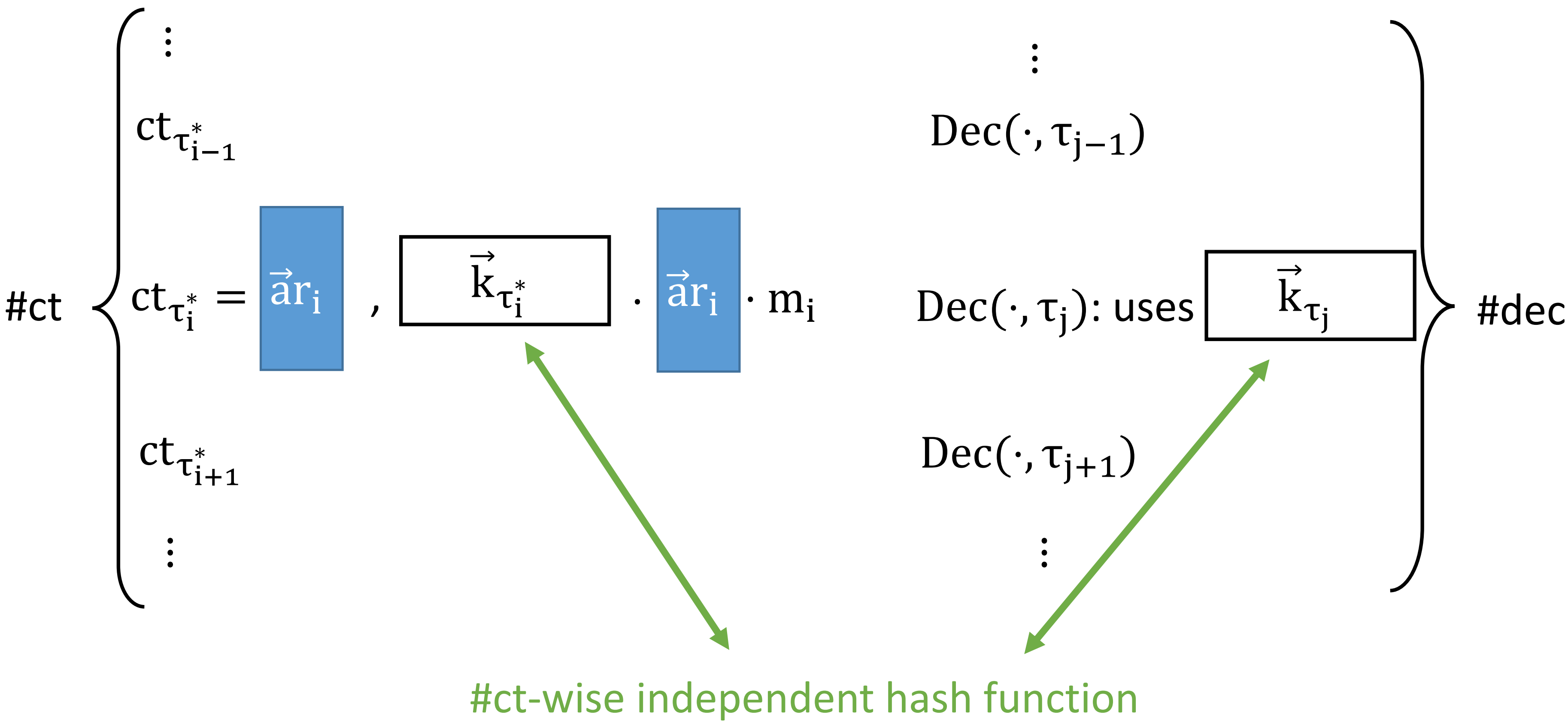
$\vdots$

#dec

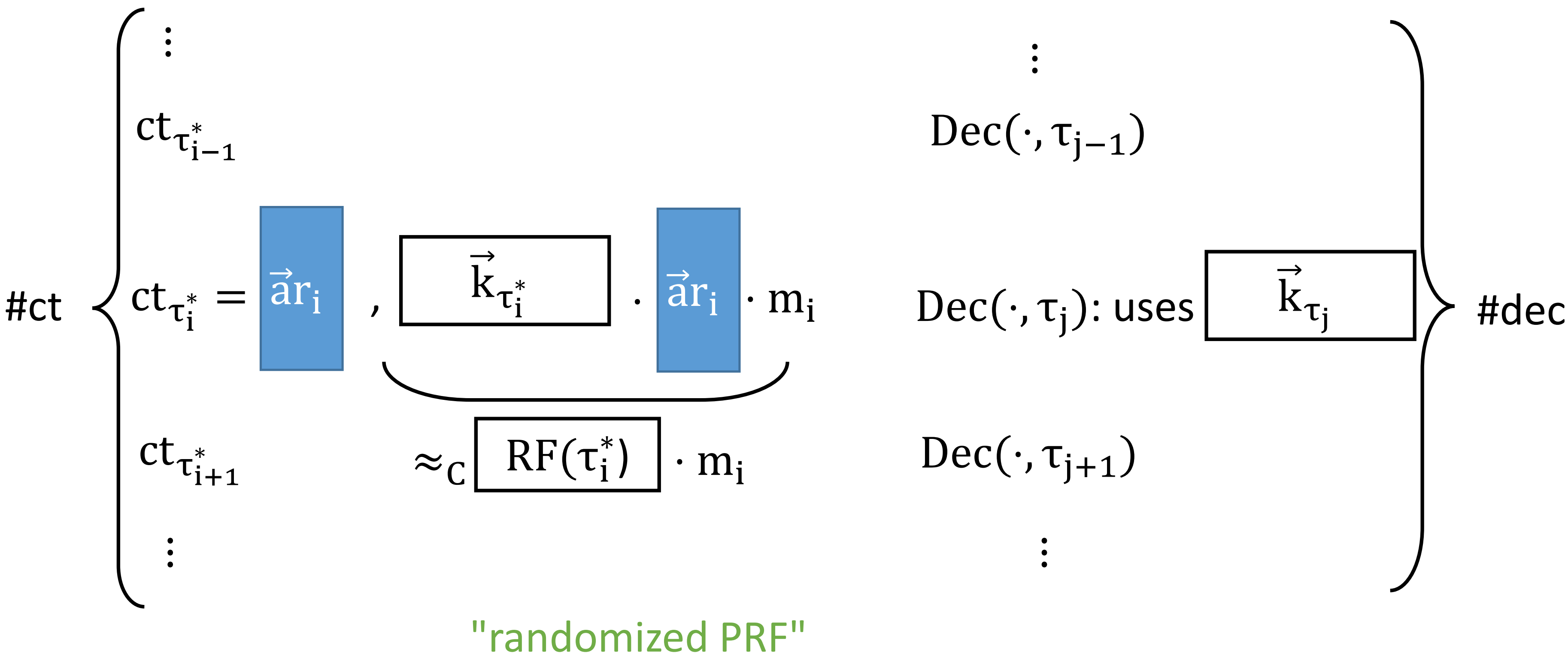
$$\epsilon \leq \#ct \cdot \epsilon_{DDH} + \#ct \cdot \#dec \cdot 2^{-\lambda}$$

Security loss

Our approach



Our approach



Our construction

For $i = 1, \ldots, \lambda$ and $b = 0,1$:

$\boxed{\vec{k}_0}, \boxed{\vec{k}_1} \leftarrow_R \mathbb{Z}_p^2 \Rightarrow \boxed{\vec{k}_{i,b}} \leftarrow_R \mathbb{Z}_p^3$

$\tau \in \mathbb{Z}_p \mapsto \boxed{\vec{k}_0 + \tau\vec{k}_1} \in \mathbb{Z}_p^2 \Rightarrow \tau \in \{0,1\}^\lambda \mapsto \boxed{\sum_{i=1}^{\lambda} \vec{k}_{i,\tau_i}} \in \mathbb{Z}_p^3$

[Chen, Wee 13; Naor Reingold 97]

$\vec{a} \leftarrow_R \mathbb{G}^2 \Rightarrow \vec{a} \leftarrow_R \mathbb{G}^3$

[Hofheinz, Koch, Striecks 15; Gong+ 16]

Our construction

$$sk = \boxed{\vec{k}_{i,b}} \leftarrow_R \mathbb{Z}_p^3 \quad \text{for } i = 1, \ldots, \lambda \text{ and } b = 0,1$$

$$pk = \vec{a} \leftarrow_R \mathbb{G}^3, \boxed{\vec{k}_{i,b}} \cdot \vec{a} \in \mathbb{G} \quad \text{for } i = 1, \ldots, \lambda \text{ and } b = 0,1$$

$$ct_\tau = \vec{a}r \in \mathbb{G}^3, \quad \boxed{\sum_{i=1}^{\lambda} \vec{k}_{i,\tau_i}} \cdot \vec{a}r \cdot m \in \mathbb{G}$$

where $r \leftarrow_R \mathbb{Z}_p$

Proof sketch

$$\#\text{ct} \left\{ \begin{array}{l} \vdots \\ \text{ct}_{\tau^*_{i-1}} \\ \text{ct}_{\tau^*_i} = \vec{a}r_i \,,\; \underbrace{\vec{k}_{\tau^*_i} \cdot \vec{a}r_i}_{} \cdot m_i \\ \text{ct}_{\tau^*_{i+1}} \qquad \approx_C \; \text{RF}(\tau^*_i) \cdot m_i \\ \vdots \end{array} \right.$$

$$\left. \begin{array}{l} \vdots \\ \text{Dec}(\cdot, \tau_{j-1}) \\ \text{Dec}(\cdot, \tau_j)\text{: uses } \vec{k}_{\tau_j} \\ \text{Dec}(\cdot, \tau_{j+1}) \\ \vdots \end{array} \right\} \#\text{dec}$$

"randomized PRF"

$$\epsilon \;\le\; (4\lambda + 1) \cdot \epsilon_{\text{DDH}} \;+\; (\#\text{ct} + \#\text{dec}) \cdot 2^{-\lambda}$$

Conclusion

Scheme	|ct|-|m|	Loss L	Assumption
CS 98	3	$\Omega(Q_{enc})$	DDH
KD 04	2		
HJ 12	$O(\lambda)$	$O(1)$	DLIN
LPJY 15	47	$O(\lambda)$	
AHY 15	12		
GCDCT 15	10		SXDH
This work	3	$O(\lambda)$	DDH

Conclusion

Scheme	|ct|-|m|	Loss L	Assumption	|pk|
CS 98	3	$\Omega(Q_{enc})$	DDH	O(1)
KD 04	2			
HJ 12	$O(\lambda)$	$O(1)$	DLIN	O(1)
LPJY 15	47	$O(\lambda)$		$\Omega(\lambda)$
AHY 15	12			
GCDCT 15	10		SXDH	
This work	3	$O(\lambda)$	DDH	

Conclusion

Scheme	|ct|-|m|	Loss L	Assumption	|pk|
CS 98	3	$\Omega(Q_{enc})$	DDH	O(1)
KD 04	2			
HJ 12	$O(\lambda)$	$O(1)$	DLIN	O(1)
LPJY 15	47	$O(\lambda)$		$\Omega(\lambda)$
			SXDH	
		(λ)	DDH	

Can we reduce |pk| to $O(1)$?

[Hofheinz 16]

Conclusion

Scheme	|ct|-|m|	Loss L	Assumption	|pk|
CS 98	3	$\Omega(Q_{enc})$	DDH	O(1)
KD 04	2			
HJ 12	$O(\lambda)$	$O(1)$	DLIN	O(1)
LPJY 15	47	$O(\lambda)$		
		(λ)		

Can we reduce |pk| to $O(1)$?

Tightly CPA-secure encryption from factoring or CDH?

[Hofheinz 16]

Conclusion

Scheme	|ct|-|m|	Loss L	Assumption	|pk|
CS 98	3	$\Omega(Q_{enc})$	DDH	O(1)
KD 04	2			
HJ 12	$O(\lambda)$	$O(1)$	DLIN	O(1)
LPJY 15	47			

Thank you!

Questions?

Can we reduce |pk| to O(1)?

Tightly CPA-secure encryption from factoring or CDH?

[Hofheinz 16]