Chosen-Ciphertext Security from Subset Sum

PKC 2016, 07.03.2016

Sebastian Faust[1] **Daniel Masny**[1] Daniele Venturi[2]

[1]Ruhr Universität Bochum

[2]Sapienza University of Rome

Outline

Our Contribution

State of the Art

- CPA-secure Public Key Encryption (PKE) from Subset Sum [LPS10].

Our Contribution

State of the Art

- CPA-secure Public Key Encryption (PKE) from Subset Sum [LPS10].
- The security decreases with the message length.

Our Contribution

State of the Art

- CPA-secure Public Key Encryption (PKE) from Subset Sum [LPS10].
- The security decreases with the message length.
- Solution: split message (not possible for CCA)

Our Contribution

State of the Art

- CPA-secure Public Key Encryption (PKE) from Subset Sum [LPS10].
- The security decreases with the message length.
- Solution: split message (not possible for CCA)

Our Results

- We construct a CCA-secure PKE from Subset Sum (using [MP12]).

Our Contribution

State of the Art

- CPA-secure Public Key Encryption (PKE) from Subset Sum [LPS10].
- The security decreases with the message length.
- Solution: split message (not possible for CCA)

Our Results

- We construct a CCA-secure PKE from Subset Sum (using [MP12]).
- The security of our PKE does not decrease with the message length.

Outline

1. Our Contribution
2. Subset Sum
3. CCA secure PKE
4. Tag-Based Encryption

Subset Sum

Subset Sum (n, μ): Find secret $s \in \{0,1\}^n$,

Subset Sum

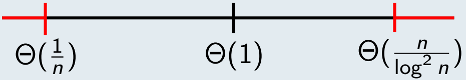
Subset Sum (n, μ): Find secret $s \in \{0, 1\}^n$,
given $(A := (\mathbf{a}_1, \ldots, \mathbf{a}_n), \mathbf{t} := s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu$.

Subset Sum

Subset Sum (n, μ): Find secret $s \in \{0,1\}^n$,
given $(A := (\mathbf{a}_1, \ldots, \mathbf{a}_n), \mathbf{t} := s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu$.

Hardness of Subset Sum

$\delta := \frac{n}{\log \mu}$:

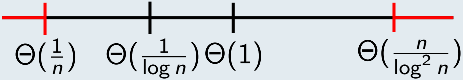


Subset Sum

Subset Sum (n, μ): Find secret $s \in \{0,1\}^n$,
given $(A := (\mathbf{a}_1, \ldots, \mathbf{a}_n), \mathbf{t} := s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu$.

Hardness of Subset Sum

$\delta := \frac{n}{\log \mu}$:



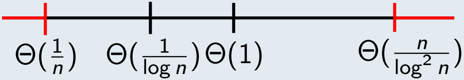
- We focus on $\delta = \Theta(\frac{1}{\log n})$.

Subset Sum

Subset Sum (n, μ): Find secret $s \in \{0,1\}^n$,
given $(A := (\mathbf{a}_1, \ldots, \mathbf{a}_n), \mathbf{t} := s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu$.

Hardness of Subset Sum

$\delta := \frac{n}{\log \mu}$:



- We focus on $\delta = \Theta(\frac{1}{\log n})$.

Decisional Subset Sum [IN96]:
$(A, \mathbf{t})$ is hard to distinguish from uniform.

“LWE” form of Subset Sum [LPS10]

$(A, \mathbf{t}) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu \to \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

“LWE” form of Subset Sum [LPS10]

$(A, \mathbf{t}) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu \to \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

Let $\mu = q^m$,

“LWE” form of Subset Sum [LPS10]

$(A, \mathbf{t}) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu \to \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

Let $\mu = q^m$, then we can represent $\mathbf{a} \in \mathbb{Z}_\mu$ as value in $\mathbb{Z}_q^m$:

"LWE" form of Subset Sum [LPS10]

$(A, \mathbf{t}) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu \to \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

Let $\mu = q^m$, then we can represent $\mathbf{a} \in \mathbb{Z}_\mu$ as value in $\mathbb{Z}_q^m$:

$$\mathbf{a} = a^m \cdot q^{m-1} + \ldots + a^1 \cdot q^0 \widehat{=} (a^m, \ldots, a^1)^T \in \mathbb{Z}_q^m$$

“LWE” form of Subset Sum [LPS10]

$(A, \mathbf{t}) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu \to \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

Let $\mu = q^m$, then we can represent $\mathbf{a} \in \mathbb{Z}_\mu$ as value in $\mathbb{Z}_q^m$:

$$\mathbf{a} = a^m \cdot q^{m-1} + \ldots + a^1 \cdot q^0 \mathrel{\widehat{=}} (a^m, \ldots, a^1)^T \in \mathbb{Z}_q^m$$

"LWE" form of Subset Sum [LPS10]

$(A, \mathbf{t}) \in \mathbb{Z}_\mu^n \times \mathbb{Z}_\mu \to \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

Let $\mu = q^m$, then we can represent $\mathbf{a} \in \mathbb{Z}_\mu$ as value in $\mathbb{Z}_q^m$:

$$\mathbf{a} = a^m \cdot q^{m-1} + \ldots + a^1 \cdot q^0 \,\widehat{=}\, (a^m, \ldots, a^1)^T \in \mathbb{Z}_q^m$$

Therefore

$$A = (\mathbf{a}_1, \ldots, \mathbf{a}_n) \,\widehat{=}\, \begin{pmatrix} a_1^m & \cdots & a_n^m \\ \vdots & \ddots & \vdots \\ a_1^1 & \cdots & a_n^1 \end{pmatrix} \in \mathbb{Z}_q^{m \times n}$$

“LWE” form of Subset Sum [LPS10]

$$\mathbf{t} \quad = \quad s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n \qquad\qquad \in \mathbb{Z}_{q^m},$$

"LWE" form of Subset Sum [LPS10]

$$\begin{aligned} \mathbf{t} &= s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n && \in \mathbb{Z}_{q^m}, \\ &\hat{\not\cong} \; s_1 \begin{pmatrix} a_1^m \\ \vdots \\ a_1^2 \\ a_1^1 \end{pmatrix} \cdots + s_n \begin{pmatrix} a_n^m \\ \vdots \\ a_n^2 \\ a_n^1 \end{pmatrix} && \in \mathbb{Z}_q^m, \end{aligned}$$

"LWE" form of Subset Sum [LPS10]

$$\begin{aligned}
\mathbf{t} &= s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n & \in \mathbb{Z}_{q^m}, \\
&\widehat{=} s_1 \begin{pmatrix} a_1^m \\ \vdots \\ a_1^2 \\ a_1^1 \end{pmatrix} \cdots + s_n \begin{pmatrix} a_n^m \\ \vdots \\ a_n^2 \\ a_n^1 \end{pmatrix} + \begin{pmatrix} e^m(A,s) \\ \vdots \\ e^2(A,s) \\ e^1(A,s) \end{pmatrix} & \in \mathbb{Z}_q^m,
\end{aligned}$$

where $e(A, s)$ is a vector of carries.

“LWE” form of Subset Sum [LPS10]

$$\begin{array}{rcll} \mathbf{t} & = & s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n & \in \mathbb{Z}_{q^m}, \\ & \widehat{=} & s_1 \begin{pmatrix} a_1^m \\ \vdots \\ a_1^2 \\ a_1^1 \end{pmatrix} \cdots + s_n \begin{pmatrix} a_n^m \\ \vdots \\ a_n^2 \\ a_n^1 \end{pmatrix} + \begin{pmatrix} e^m(A,s) \\ \vdots \\ \color{blue}{e^2(A,s)} \\ e^1(A,s) \end{pmatrix} & \in \mathbb{Z}_q^m, \end{array}$$

where $e(A, s)$ is a vector of carries.

“LWE” form of Subset Sum [LPS10]

$$\begin{array}{rcll} \mathbf{t} & = & s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n & \in \mathbb{Z}_{q^m}, \\ & \widehat{=} & s_1 \begin{pmatrix} a_1^m \\ \vdots \\ a_1^2 \\ a_1^1 \end{pmatrix} \cdots + s_n \begin{pmatrix} a_n^m \\ \vdots \\ a_n^2 \\ a_n^1 \end{pmatrix} + \begin{pmatrix} e^m(A,s) \\ \vdots \\ e^2(A,s) \\ e^1(A,s) \end{pmatrix} & \in \mathbb{Z}_q^m, \end{array}$$

where $e(A, s)$ is a vector of carries.

“LWE” form of Subset Sum [LPS10]

$$\begin{aligned} \mathbf{t} &= s_1\mathbf{a}_1 + \cdots + s_n\mathbf{a}_n && \in \mathbb{Z}_{q^m}, \\ &\widehat{=} s_1 \begin{pmatrix} a_1^m \\ \vdots \\ a_1^2 \\ a_1^1 \end{pmatrix} \cdots + s_n \begin{pmatrix} a_n^m \\ \vdots \\ a_n^2 \\ a_n^1 \end{pmatrix} + \begin{pmatrix} e^m(A,s) \\ \vdots \\ e^2(A,s) \\ e^1(A,s) \end{pmatrix} && \in \mathbb{Z}_q^m, \end{aligned}$$

where $e(A, s)$ is a vector of carries.

From now on, $(A, \mathbf{t} = As + e(A, s)) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ (m samples).

Many Samples from Subset Sum

$\mu = q^m$

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples $\Rightarrow \delta = \frac{n}{\log \mu} = \frac{n}{m \cdot \log q}$ (easy for e.g. $m = n^2$)

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples $\Rightarrow \delta = \frac{n}{\log \mu} = \frac{n}{m \cdot \log q}$ (easy for e.g. $m = n^2$)

From m to ℓ samples:

- given $(A, \mathbf{t}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples $\Rightarrow \delta = \frac{n}{\log \mu} = \frac{n}{m \cdot \log q}$ (easy for e.g. $m = n^2$)

From m to ℓ samples:

- given $(A, \mathbf{t}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$
- $R \leftarrow \mathcal{D}_q^{\ell \times m}$, where $\mathcal{D}$ has sufficient min-entropy.

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples $\Rightarrow \delta = \frac{n}{\log \mu} = \frac{n}{m \cdot \log q}$ (easy for e.g. $m = n^2$)

From m to ℓ samples:

- given $(A, \mathbf{t}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$
- $R \leftarrow \mathcal{D}_q^{\ell \times m}$, where $\mathcal{D}$ has sufficient min-entropy.
- output $(RA,\ \ R\mathbf{t} = RAs + Re(A, s)) \in \mathbb{Z}_q^{\ell \times n} \times \mathbb{Z}_q^{\ell}$

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples $\Rightarrow \delta = \frac{n}{\log \mu} = \frac{n}{m \cdot \log q}$ (easy for e.g. $m = n^2$)

From m to ℓ samples:

- given $(A, \mathbf{t}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$
- $R \leftarrow \mathcal{D}_q^{\ell \times m}$, where $\mathcal{D}$ has sufficient min-entropy.
- output $(RA, \; R\mathbf{t} = RAs + Re(A, s)) \in \mathbb{Z}_q^{\ell \times n} \times \mathbb{Z}_q^{\ell}$

- Leftover hash lemma [HILL99]:
  If $(A, \mathbf{t})$ is uniform $\Rightarrow$ $(A, \mathbf{t}, RA, R\mathbf{t})$ is uniform.

Many Samples from Subset Sum

$\mu = q^m \Rightarrow m$ samples $\Rightarrow \delta = \frac{n}{\log \mu} = \frac{n}{m \cdot \log q}$ (easy for e.g. $m = n^2$)

From m to ℓ samples:

- given $(A, \mathbf{t}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$
- $R \leftarrow \mathcal{D}_q^{\ell \times m}$, where $\mathcal{D}$ has sufficient min-entropy.
- output $(RA,\ \ R\mathbf{t} = RAs + Re(A, s)) \in \mathbb{Z}_q^{\ell \times n} \times \mathbb{Z}_q^{\ell}$

- Leftover hash lemma [HILL99]:
  If $(A, \mathbf{t})$ is uniform $\Rightarrow$ $(A, \mathbf{t}, RA, R\mathbf{t})$ is uniform.
- $(RA, R\mathbf{t})$ is not Subset Sum distributed $(Re(A, s) \neq e(RA, s))$.

Outline

CCA secure PKE

Given a One-Time Signature (OTS),
[CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

CCA secure PKE

Given a One-Time Signature (OTS),
[CHK04]:
$TBE + OTS \to$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

CCA secure PKE

Given a One-Time Signature (OTS),
[CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

CCA secure PKE

Given a One-Time Signature (OTS),
[CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:

CCA secure PKE

Given a One-Time Signature (OTS), [CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:

Adv.

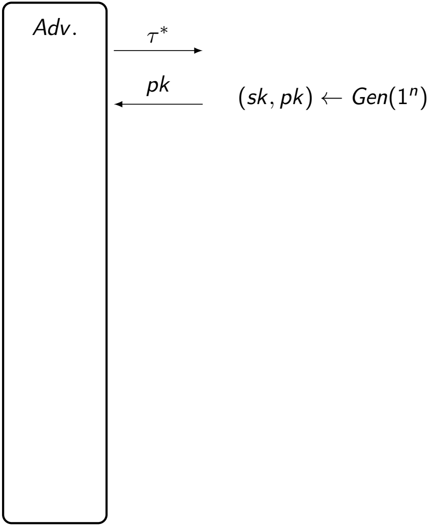
CCA secure PKE

Given a One-Time Signature (OTS), [CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:



$Adv.$

τ^*

pk

$(sk, pk) \leftarrow Gen(1^n)$

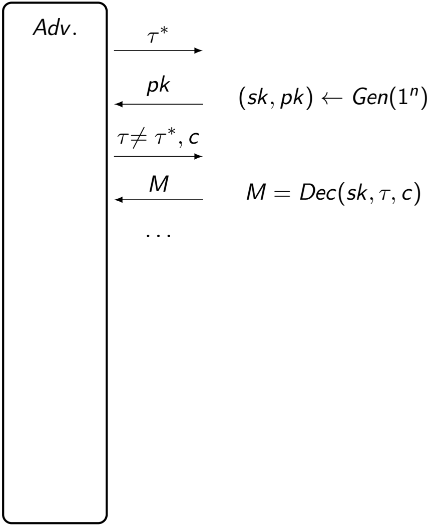
CCA secure PKE

Given a One-Time Signature (OTS), [CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:



Adv.

τ^*

pk

$(sk, pk) \leftarrow Gen(1^n)$

$\tau \neq \tau^*, c$

M

$M = Dec(sk, \tau, c)$

$\ldots$

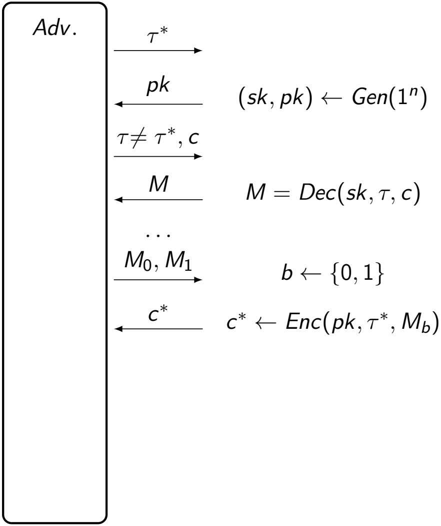
CCA secure PKE

Given a One-Time Signature (OTS), [CHK04]:
$TBE + OTS \to$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:



$Adv.$

τ^*

pk — $(sk, pk) \leftarrow Gen(1^n)$

$\tau \neq \tau^*, c$

M — $M = Dec(sk, \tau, c)$

$\dots$

M_0, M_1 — $b \leftarrow \{0, 1\}$

c^* — $c^* \leftarrow Enc(pk, \tau^*, M_b)$

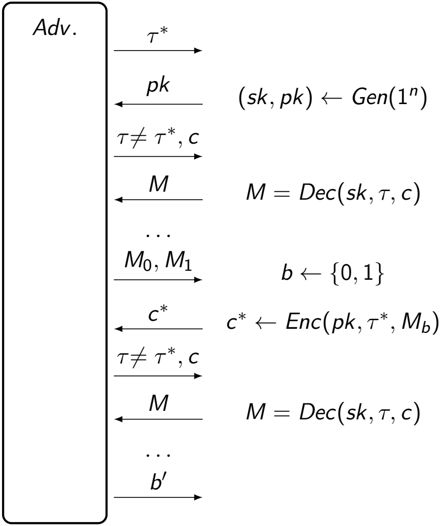
CCA secure PKE

Given a One-Time Signature (OTS), [CHK04]:
$TBE + OTS \to$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:



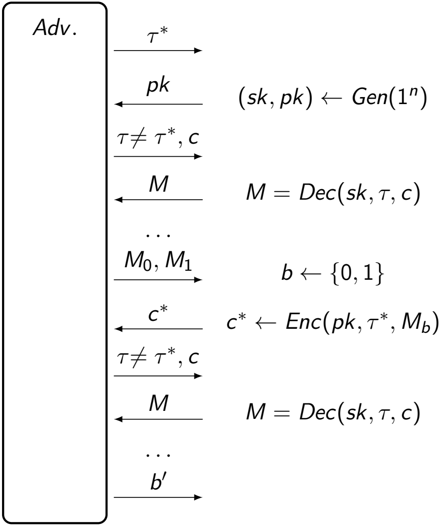
CCA secure PKE

Given a One-Time Signature (OTS), [CHK04]:
$TBE + OTS \rightarrow$ CCA-secure PKE.

Tag-Based Encryption (TBE):
$TBE = (Gen, Enc, Dec)$.

Correctness:
For $(sk, pk) \leftarrow Gen(1^n)$:
$Dec(sk, \tau, Enc(pk, \tau, M)) = M$

Security:
For all ppt $Adv.$: $\Pr[b' = b] = 1/2$.



$Adv.$

τ^*

pk

$(sk, pk) \leftarrow Gen(1^n)$

$\tau \neq \tau^*, c$

M

$M = Dec(sk, \tau, c)$

$\dots$

M_0, M_1

$b \leftarrow \{0, 1\}$

c^*

$c^* \leftarrow Enc(pk, \tau^*, M_b)$

$\tau \neq \tau^*, c$

M

$M = Dec(sk, \tau, c)$

$\dots$

b'

Outline

Tag-Based Encryption, *Gen*

$2 \mid q$. Let $H_\tau \in \mathbb{Z}_2^{n \times n}$ represent τ.
For $\tau \neq \tau'$, $H_\tau - H_{\tau'}$ is invertible for [ABB10].

Tag-Based Encryption, *Gen*

$2 \mid q$. Let $H_\tau \in \mathbb{Z}_2^{n \times n}$ represent τ.
For $\tau \neq \tau'$, $H_\tau - H_{\tau'}$ is invertible for [ABB10].

For $M \in \{0, 1\}^\ell$:

$\mathit{Gen}(1^n) :\ A \leftarrow \mathbb{Z}_q^{m \times n},\ C \leftarrow \mathbb{Z}_q^{\ell \times n},\ R \leftarrow \mathcal{D}^{m \times n}.$

Tag-Based Encryption, *Gen*

$2 \mid q$. Let $H_\tau \in \mathbb{Z}_2^{n \times n}$ represent τ.
For $\tau \neq \tau'$, $H_\tau - H_{\tau'}$ is invertible for [ABB10].

For $M \in \{0,1\}^\ell$:

$Gen(1^n):$ $A \leftarrow \mathbb{Z}_q^{m \times n}$, $C \leftarrow \mathbb{Z}_q^{\ell \times n}$, $R \leftarrow \mathcal{D}^{m \times n}$.
Output $sk = R$, $pk = (A, B := RA, C)$.

Tag-Based Encryption, *Enc*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n): \ sk = R, \ pk = (A, B := RA, C).$

Tag-Based Encryption, *Enc*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: Sample $R' \leftarrow \mathcal{D}^{m \times n}$, $R'' \leftarrow \mathcal{D}^{\ell \times n}$, $s \leftarrow \{0,1\}^n$

Tag-Based Encryption, *Enc*

For $M \in \{0,1\}^\ell$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: Sample $R' \leftarrow \mathcal{D}^{m\times n}$, $R'' \leftarrow \mathcal{D}^{\ell\times n}$, $s \leftarrow \{0,1\}^n$
output

$$c_0 := As + e(A,s);$$

- (A, c_0) is a Subset Sum instance for secret s.

Tag-Based Encryption, *Enc*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: Sample $R' \leftarrow \mathcal{D}^{m\times n}$, $R'' \leftarrow \mathcal{D}^{\ell\times n}$, $s \leftarrow \{0,1\}^n$
output

$$\begin{aligned} c_0 &:= As + e(A,s); \\ c_1 &:= (B + q/2 \cdot H_\tau)s + R'e(A,s); \end{aligned}$$

- (A, c_0) is a Subset Sum instance for secret s.
- s can be recovered from (c_0, c_1).

Tag-Based Encryption, *Enc*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: Sample $R' \leftarrow \mathcal{D}^{m \times n}$, $R'' \leftarrow \mathcal{D}^{\ell \times n}$, $s \leftarrow \{0,1\}^n$
output

$$\begin{aligned} c_0 &:= As + e(A,s); \\ c_1 &:= (B + q/2 \cdot H_\tau)s + R'e(A,s); \\ c_2 &:= Cs + R''e(A,s) + q/2 \cdot M. \end{aligned}$$

- (A, c_0) is a Subset Sum instance for secret s.
- s can be recovered from (c_0, c_1).
- c_2 encrypts M under secret s.

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$$Gen(1^n):\ sk = R,\ pk = (A, B := RA, C).$$

$$\begin{aligned} Enc(pk, H_\tau, M):\ c_0 &:= As + e(A,s),\\ c_1 &:= (B + q/2 \cdot H_\tau)s + R'e(A,s),\\ c_2 &:= Cs + R''e(A,s) + q/2 \cdot M. \end{aligned}$$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^\ell$:

$Gen(1^n):\ sk = R,\ pk = (A, B := RA, C).$

$Enc(pk, H_\tau, M):\ c_0 := As + e(A,s),$

$c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s),$

$c_2 := Cs + R''e(A,s) + q/2 \cdot M.$

$Dec(sk, H_\tau, c_0, c_1, c_2):\ s = H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n):\ sk = R,\ pk = (A, B := RA, C)$.

$$\begin{aligned} Enc(pk, H_\tau, M):\ & c_0 := As + e(A,s), \\ & c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s), \\ & c_2 := Cs + R''e(A,s) + q/2 \cdot M. \end{aligned}$$

$Dec(sk, H_\tau, c_0, c_1, c_2):\ s = H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness:

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n): \ sk = R, \ pk = (A, B := RA, C)$.

$$\begin{aligned} Enc(pk, H_\tau, M): \ & c_0 := As + e(A,s), \\ & c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s), \\ & c_2 := Cs + R''e(A,s) + q/2 \cdot M. \end{aligned}$$

$Dec(sk, H_\tau, c_0, c_1, c_2): \ s = H_\tau^{-1}\lfloor c_1 - Rc_0\rceil_2$, output $M = \lfloor c_2 - Cs\rceil_2$.

$(\lfloor\cdot\rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$H_\tau^{-1}\lfloor c_1 - Rc_0\rceil_2$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n):\ sk = R,\ pk = (A, B := RA, C)$.

$$\begin{aligned} Enc(pk, H_\tau, M):\ & c_0 := As + e(A,s), \\ & c_1 := (B + q/2 \cdot H_\tau)s + R' e(A,s), \\ & c_2 := Cs + R'' e(A,s) + q/2 \cdot M. \end{aligned}$$

$Dec(sk, H_\tau, c_0, c_1, c_2):\ s = H_\tau^{-1} \lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$$H_\tau^{-1} \lfloor c_1 - Rc_0 \rceil_2 = H_\tau^{-1} \lfloor q/2 \cdot H_\tau s + (R' - R)e(A,s) \rceil_2$$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n) :\ sk = R,\ pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M) :\ c_0 := As + e(A,s),$

$c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s),$

$c_2 := Cs + R''e(A,s) + q/2 \cdot M.$

$Dec(sk, H_\tau, c_0, c_1, c_2) :\ s = H_\tau^{-1}\lfloor c_1 - Rc_0\rceil_2$, output $M = \lfloor c_2 - Cs\rceil_2$.

$(\lfloor\cdot\rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$$H_\tau^{-1}\lfloor c_1 - Rc_0\rceil_2 = H_\tau^{-1}\lfloor q/2 \cdot H_\tau s + (R' - R)e(A,s)\rceil_2$$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: $c_0 := As + e(A,s)$,

$c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s)$,

$c_2 := Cs + R''e(A,s) + q/2 \cdot M$.

$Dec(sk, H_\tau, c_0, c_1, c_2)$: $s = H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$$H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2 = H_\tau^{-1}\lfloor q/2 \cdot H_\tau s + (R' - R)e(A,s) \rceil_2 = H_\tau^{-1} H_\tau s = s,$$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: $c_0 := As + e(A,s)$,

$c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s)$,

$c_2 := Cs + R''e(A,s) + q/2 \cdot M$.

$Dec(sk, H_\tau, c_0, c_1, c_2)$: $s = H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$$H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2 = H_\tau^{-1}\lfloor q/2 \cdot H_\tau s + (R' - R)e(A,s) \rceil_2 = H_\tau^{-1} H_\tau s = s,$$

$$\lfloor c_2 - Cs \rceil_2 = \lfloor R''e(A,s) + q/2 \cdot M \rceil_2$$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n)$: $sk = R$, $pk = (A, B := RA, C)$.

$Enc(pk, H_\tau, M)$: $c_0 := As + e(A,s)$,

$c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s)$,

$c_2 := Cs + R''e(A,s) + q/2 \cdot M$.

$Dec(sk, H_\tau, c_0, c_1, c_2)$: $s = H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor\cdot\rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$$H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2 = H_\tau^{-1}\lfloor q/2 \cdot H_\tau s + (R' - R)e(A,s) \rceil_2 = H_\tau^{-1} H_\tau s = s,$$

$$\lfloor c_2 - Cs \rceil_2 = \lfloor R''e(A,s) + q/2 \cdot M \rceil_2$$

Tag-Based Encryption, *Dec*

For $M \in \{0,1\}^{\ell}$:

$Gen(1^n):\ sk = R,\ pk = (A, B := RA, C).$

$Enc(pk, H_\tau, M):\ c_0 := As + e(A,s),$

$c_1 := (B + q/2 \cdot H_\tau)s + R'e(A,s),$

$c_2 := Cs + R''e(A,s) + q/2 \cdot M.$

$Dec(sk, H_\tau, c_0, c_1, c_2):\ s = H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2$, output $M = \lfloor c_2 - Cs \rceil_2$.

$(\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \{0,1\})$

Correctness: Since $RAs = Bs$:

$$H_\tau^{-1}\lfloor c_1 - Rc_0 \rceil_2 = H_\tau^{-1}\lfloor q/2 \cdot H_\tau s + (R' - R)e(A,s) \rceil_2 = H_\tau^{-1}H_\tau s = s,$$

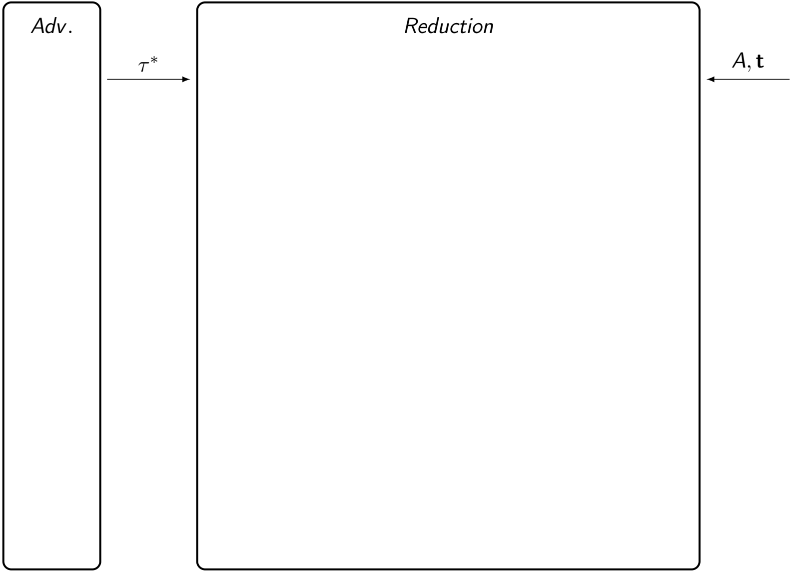
$$\lfloor c_2 - Cs \rceil_2 = \lfloor R''e(A,s) + q/2 \cdot M \rceil_2 = M.$$

Proof Sketch

Adv.

Reduction

Proof Sketch



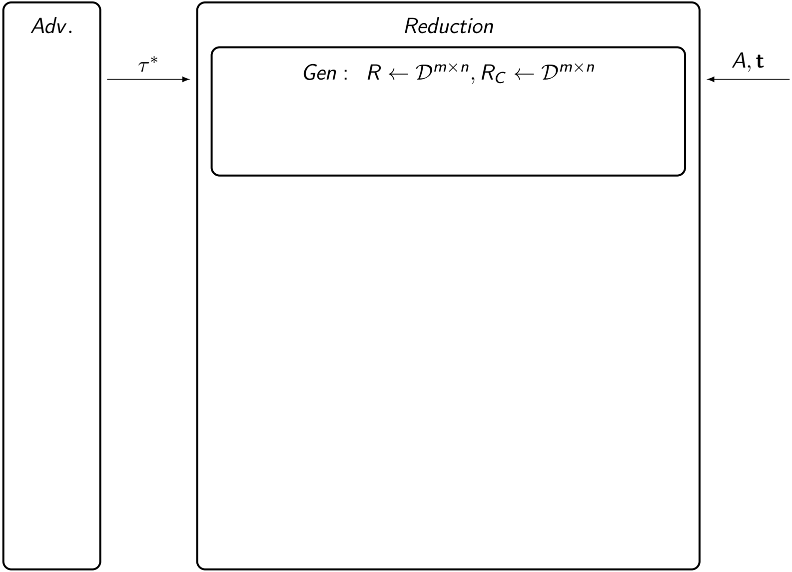
Adv.

τ^*

Reduction

$A, \mathbf{t}$

Proof Sketch



Adv.

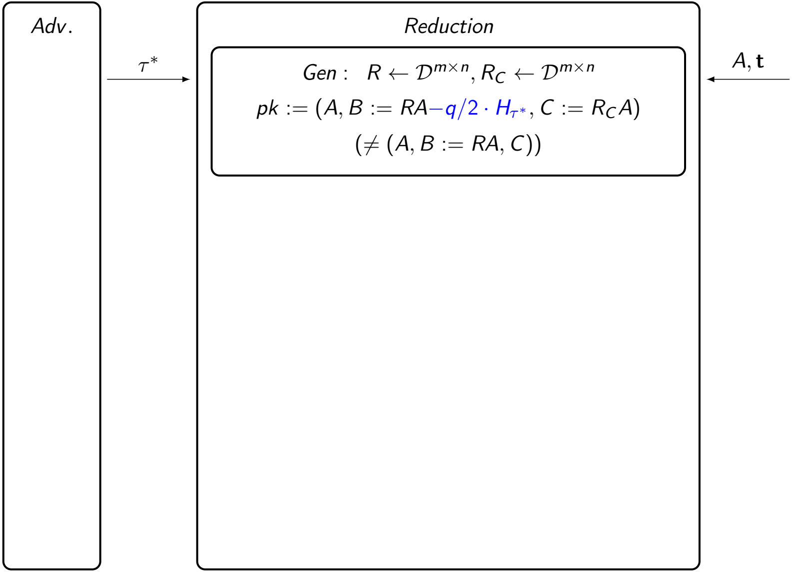
Reduction

τ^*

$Gen: \quad R \leftarrow \mathcal{D}^{m \times n}, R_C \leftarrow \mathcal{D}^{m \times n}$

$A, \mathbf{t}$

Proof Sketch



Adv.

Reduction

τ^*

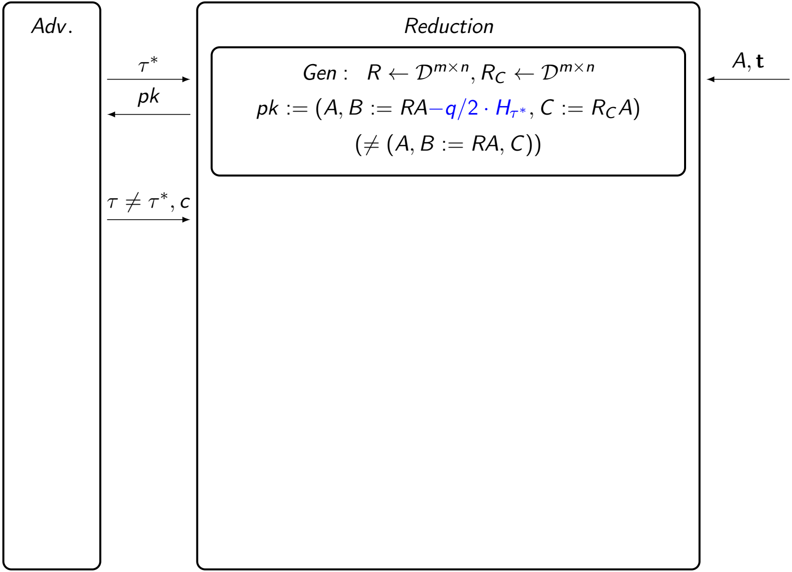
$A, \mathbf{t}$

$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

Proof Sketch



Adv.

Reduction

$A, \mathbf{t}$

τ^*

pk

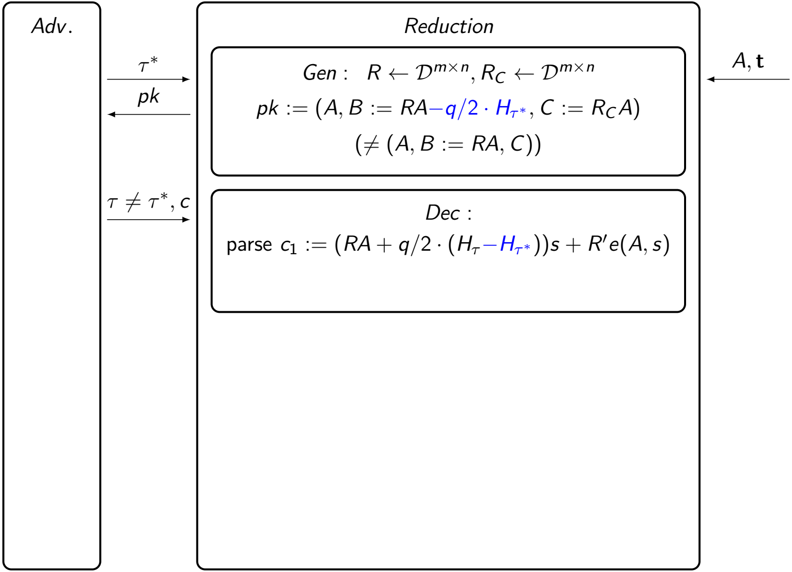
$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$\tau \neq \tau^*, c$

Proof Sketch



Adv.

Reduction

τ^*

pk

$A, \mathbf{t}$

$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

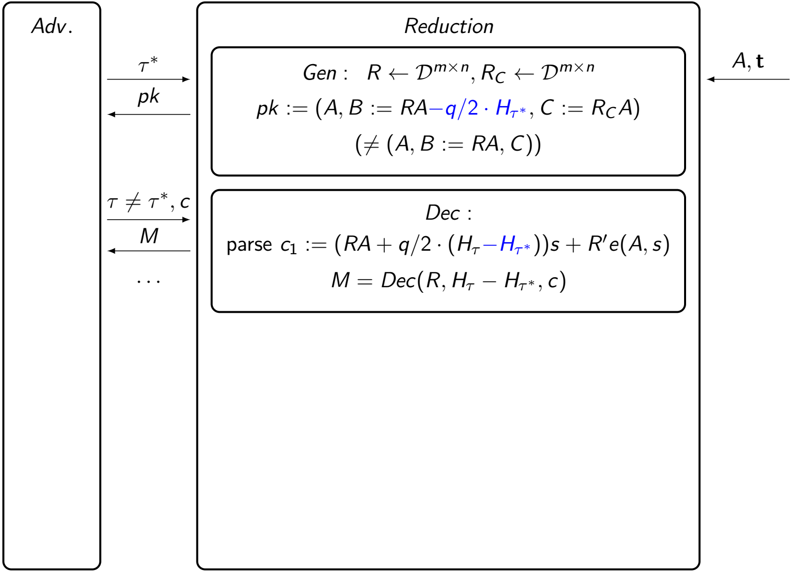
$(\neq (A, B := RA, C))$

$\tau \neq \tau^*, c$

$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

Proof Sketch



Adv.

τ^*

pk

$\tau \neq \tau^*, c$

M

$\ldots$

Reduction

$$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$$

$$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$$

$$(\neq (A, B := RA, C))$$

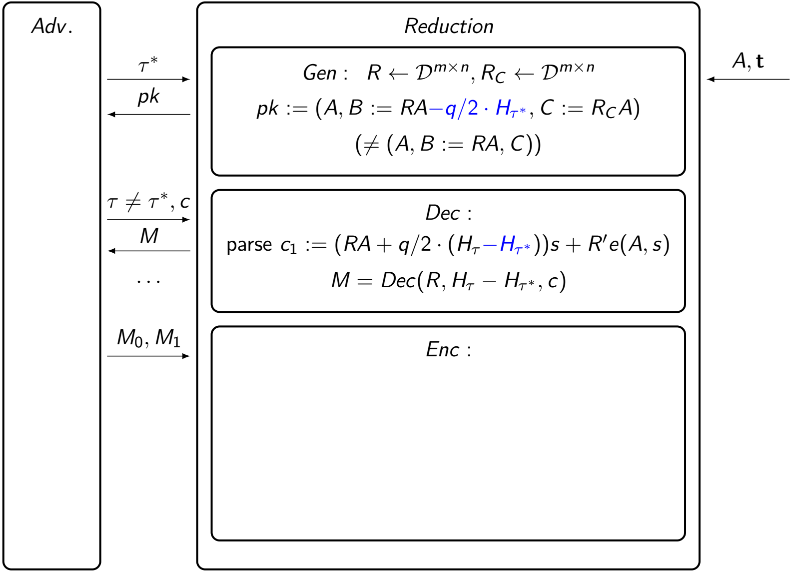
$$Dec:$$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$$M = Dec(R, H_\tau - H_{\tau^*}, c)$$

$A, \mathbf{t}$

Proof Sketch



Adv.

τ^*

pk

$\tau \neq \tau^*, c$

M

$\cdots$

M_0, M_1

Reduction

$A, \mathbf{t}$

$$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$$

$$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$$

$$(\neq (A, B := RA, C))$$

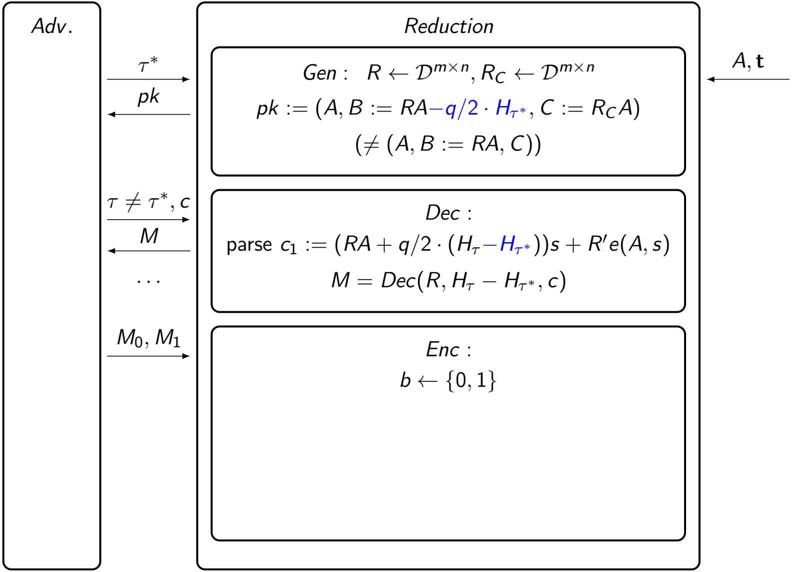
$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$$M = Dec(R, H_\tau - H_{\tau^*}, c)$$

$Enc:$

Proof Sketch



Adv.

Reduction

$A, \mathbf{t}$

τ^*

pk

$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$\tau \neq \tau^*, c$

M

$\cdots$

$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

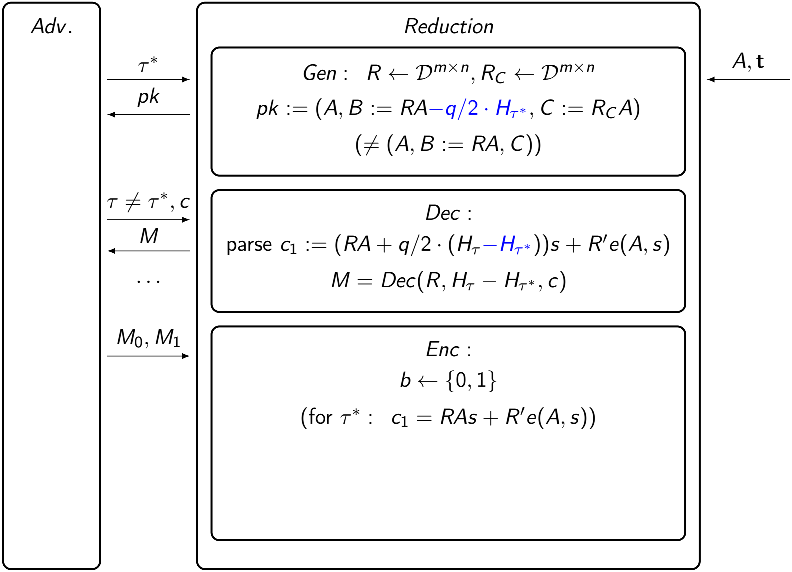
$M = Dec(R, H_\tau - H_{\tau^*}, c)$

M_0, M_1

$Enc:$

$b \leftarrow \{0, 1\}$

Proof Sketch



Adv.

Reduction

τ^*

pk

$\tau \neq \tau^*, c$

M

$\cdots$

M_0, M_1

$A, \mathbf{t}$

$$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$$

$$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$$

$$(\neq (A, B := RA, C))$$

$$Dec:$$

$$\text{parse } c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$$

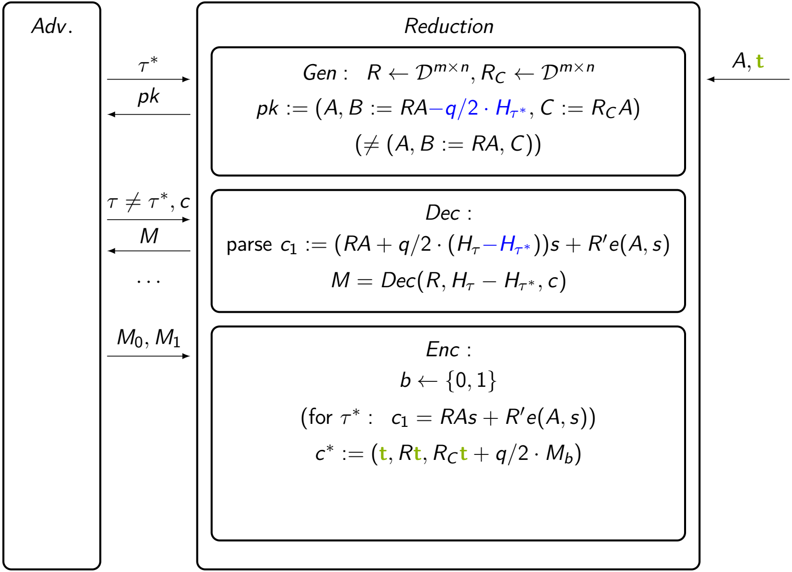
$$M = Dec(R, H_\tau - H_{\tau^*}, c)$$

$$Enc:$$

$$b \leftarrow \{0, 1\}$$

$$(\text{for } \tau^*: \quad c_1 = RAs + R'e(A, s))$$

Proof Sketch



Adv.

$\xrightarrow{\tau^*}$

$\xleftarrow{pk}$

$\xrightarrow{\tau \neq \tau^*, c}$

$\xleftarrow{M}$

$\dots$

$\xrightarrow{M_0, M_1}$

Reduction

$\xleftarrow{A, \mathbf{t}}$

$Gen: \quad R \leftarrow \mathcal{D}^{m \times n}, R_C \leftarrow \mathcal{D}^{m \times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$M = Dec(R, H_\tau - H_{\tau^*}, c)$

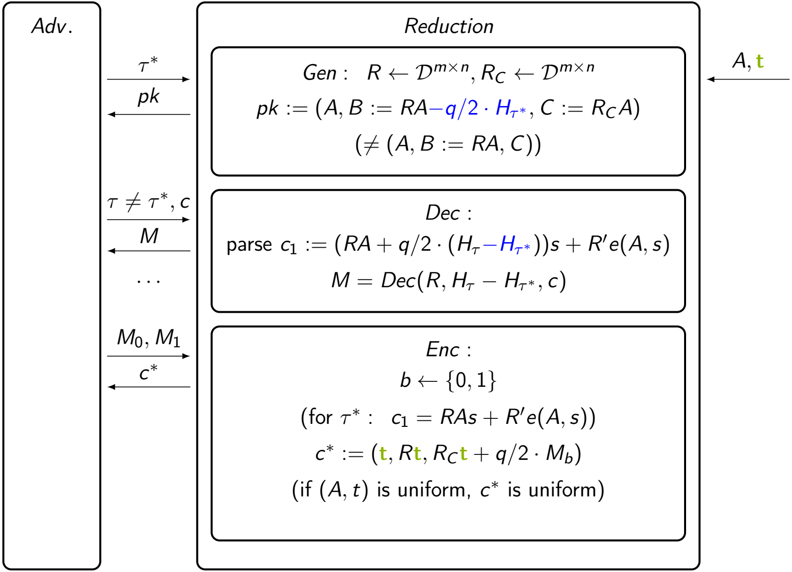
$Enc:$

$b \leftarrow \{0, 1\}$

(for $\tau^*: \quad c_1 = RAs + R'e(A, s)$)

$c^* := (\mathbf{t}, R\mathbf{t}, R_C\mathbf{t} + q/2 \cdot M_b)$

Proof Sketch



Reduction

$Gen: \quad R \leftarrow \mathcal{D}^{m \times n}, R_C \leftarrow \mathcal{D}^{m \times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$M = Dec(R, H_\tau - H_{\tau^*}, c)$

$Enc:$

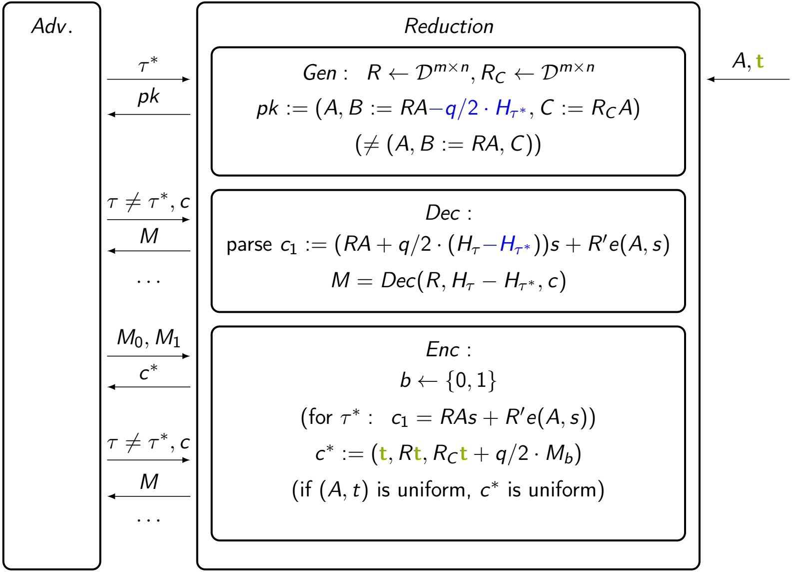
$b \leftarrow \{0, 1\}$

(for $\tau^*: \quad c_1 = RAs + R'e(A, s)$)

$c^* := (\mathbf{t}, R\mathbf{t}, R_C\mathbf{t} + q/2 \cdot M_b)$

(if (A, t) is uniform, c^* is uniform)

Proof Sketch



Adv.

$\xrightarrow{\tau^*}$

$\xleftarrow{pk}$

$\xrightarrow{\tau \neq \tau^*, c}$

$\xleftarrow{M}$

$\dots$

$\xrightarrow{M_0, M_1}$

$\xleftarrow{c^*}$

$\xrightarrow{\tau \neq \tau^*, c}$

$\xleftarrow{M}$

$\dots$

Reduction

$\xleftarrow{A, \mathbf{t}}$

$Gen: \quad R \leftarrow \mathcal{D}^{m \times n}, R_C \leftarrow \mathcal{D}^{m \times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$M = Dec(R, H_\tau - H_{\tau^*}, c)$

$Enc:$

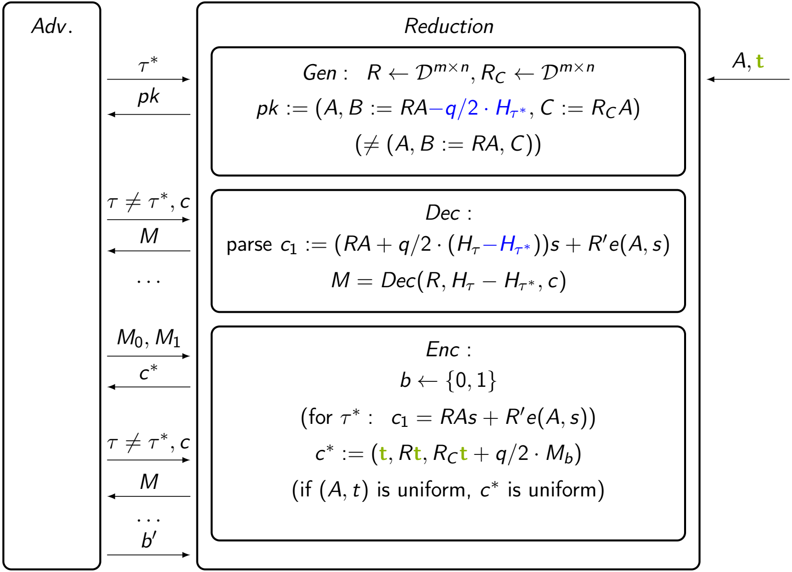
$b \leftarrow \{0, 1\}$

(for $\tau^*: \quad c_1 = RAs + R'e(A, s)$)

$c^* := (\mathbf{t}, R\mathbf{t}, R_C\mathbf{t} + q/2 \cdot M_b)$

(if (A, t) is uniform, c^* is uniform)

Proof Sketch



Adv.

Reduction

$A, \mathbf{t}$

τ^* →

pk ←

Gen : $R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$\tau \neq \tau^*, c$ →

M ←

$\cdots$

Dec :

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$M = Dec(R, H_\tau - H_{\tau^*}, c)$

M_0, M_1 →

c^* ←

$\tau \neq \tau^*, c$ →

M ←

$\cdots$

b' →

Enc :

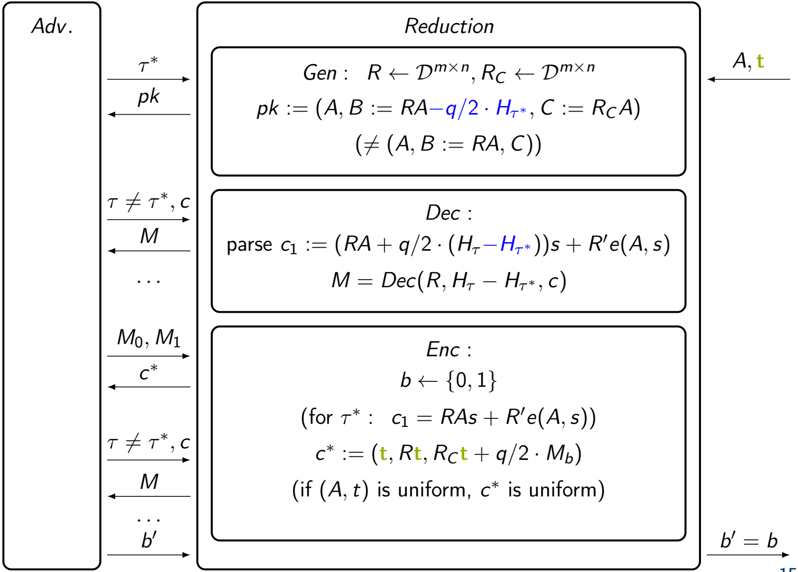
$b \leftarrow \{0, 1\}$

(for τ^* : $c_1 = RAs + R'e(A, s)$)

$c^* := (\mathbf{t}, R\mathbf{t}, R_C\mathbf{t} + q/2 \cdot M_b)$

(if (A, t) is uniform, c^* is uniform)

Proof Sketch



Adv.

$\xrightarrow{\tau^*}$

$\xleftarrow{pk}$

$\xrightarrow{\tau \neq \tau^*, c}$

$\xleftarrow{M}$

$\dots$

$\xrightarrow{M_0, M_1}$

$\xleftarrow{c^*}$

$\xrightarrow{\tau \neq \tau^*, c}$

$\xleftarrow{M}$

$\dots$

$\xrightarrow{b'}$

Reduction

$Gen: \quad R \leftarrow \mathcal{D}^{m\times n}, R_C \leftarrow \mathcal{D}^{m\times n}$

$pk := (A, B := RA - q/2 \cdot H_{\tau^*}, C := R_C A)$

$(\neq (A, B := RA, C))$

$Dec:$

parse $c_1 := (RA + q/2 \cdot (H_\tau - H_{\tau^*}))s + R'e(A, s)$

$M = Dec(R, H_\tau - H_{\tau^*}, c)$

$Enc:$

$b \leftarrow \{0, 1\}$

(for τ^* : $\quad c_1 = RAs + R'e(A, s)$)

$c^* := (\mathbf{t}, R\mathbf{t}, R_C\mathbf{t} + q/2 \cdot M_b)$

(if (A, t) is uniform, c^* is uniform)

$\xleftarrow{A, \mathbf{t}}$

$\xrightarrow{b' = b}$

Conclusion

Our Results

- “LWE" form of Subset Sum [LPS10] + LWE trapdoor [MP12] $\Rightarrow$ IND-CCA-secure PKE from Subset Sum.
- Unlike the CPA-secure PKE of [LPS10], the security of our scheme does not decrease with the message length ℓ.

References

- Shweta Agrawal, Dan Boneh, and Xavier Boyen.
  Efficient lattice (H)IBE in the standard model.
  In EUROCRYPT, pages 553–572, 2010.
- Ran Canetti, Shai Halevi, and Jonathan Katz.
  Chosen-ciphertext security from identity-based encryption.
  In EUROCRYPT, pages 207–222, 2004.
- Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby.
  A pseudorandom generator from any one-way function.
  SIAM J. Comput., 28(4):1364–1396, 1999.
- Russell Impagliazzo and Moni Naor.
  Efficient cryptographic schemes provably as secure as subset sum.
  J. Cryptology, 9(4):199–216, 1996.
- Vadim Lyubashevsky, Adriana Palacio, and Gil Segev.
  Public-key cryptographic primitives provably as secure as subset sum.
  In TCC, pages 382–400, 2010.
- Daniele Micciancio and Chris Peikert.
  Trapdoors for lattices: Simpler, tighter, faster, smaller.
  In EUROCRYPT, pages 700–718, 2012.