Naor-Yung Paradigm with Shared Randomness and Applications

Silvio Biagioni[1] Daniel Masny[2] Daniele Venturi[3]

[1]Department of Information Engineering, Sapienza University or Rome, Rome, Italy

[2]Horst-Görtz Institute for IT Security, Ruhr-Universität Bochum, Bochum, Germany

[3]Department of Information Engineering and Computer Science, University of Trento, Trento, Italy

10th Conference on Security and Cryptography for Networks
August 31 - September 2, 2016, Amalfi, Italy

Public Key Encryption

pk

$c \leftarrow Enc(pk, m; r)$

r is the randomness

(pk,sk)

$m = Dec(sk, c)$

Key-Dependent Message Attacks

- An adversary might be able to see ciphertexts encrypting messages related to the secret key

Key-Dependent Message Attacks

- An adversary might be able to see ciphertexts encrypting messages related to the secret key

Applications

careless key management

fully homomorphic encryption bootstrapping transformation

anonymous credential system a KDM secure encryption is used to discourage delegation of credentials

disk encryption utilities the disk encryption key may end up being stored in the page files and thus is encrypted along with the disc content

$\mathcal{F}$-KDM CPA and CCA security

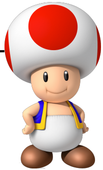
KDM
Oracle

b, pk

(pk, sk)

$b \xleftarrow{R} \{0, 1\}$

$\xleftarrow{\quad pk \quad}$



$\mathcal{F}$-KDM CPA and CCA security

KDM
Oracle

b, pk $\boxed{m_0 = 0, m_1 = f(sk)}$

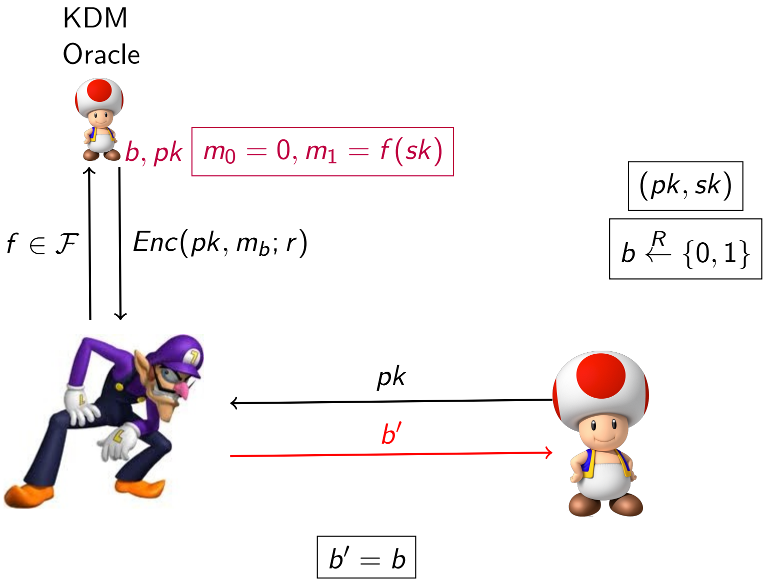
$\boxed{(pk, sk)}$

$f \in \mathcal{F}$ $\uparrow$ $\downarrow$ $Enc(pk, m_b; r)$

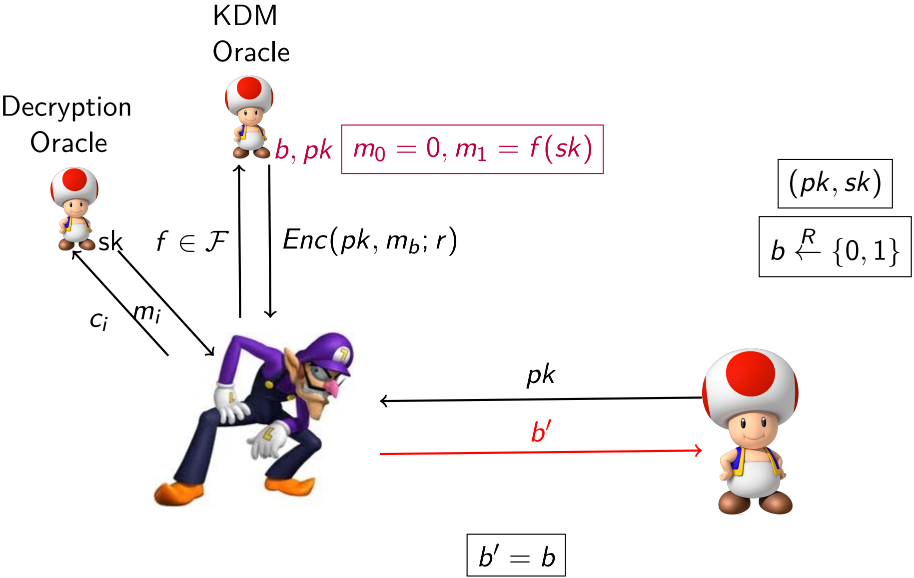
$\boxed{b \xleftarrow{R} \{0, 1\}}$

$\xleftarrow{\quad pk \quad}$

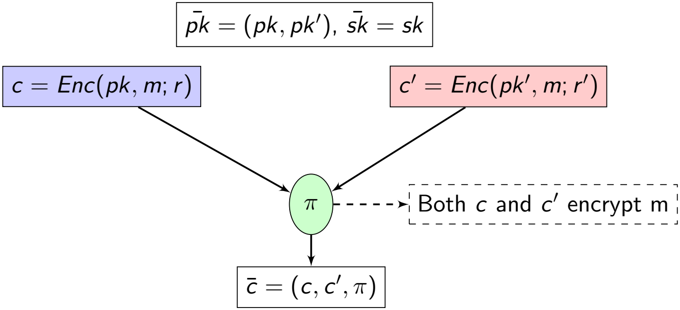
$\mathcal{F}$-KDM CPA and CCA security



$\mathcal{F}$-KDM CPA and CCA security



Naor-Yung Theorem (Camenisch, Chandran, Shoup)



Theorem (NY, Independent Randomness)

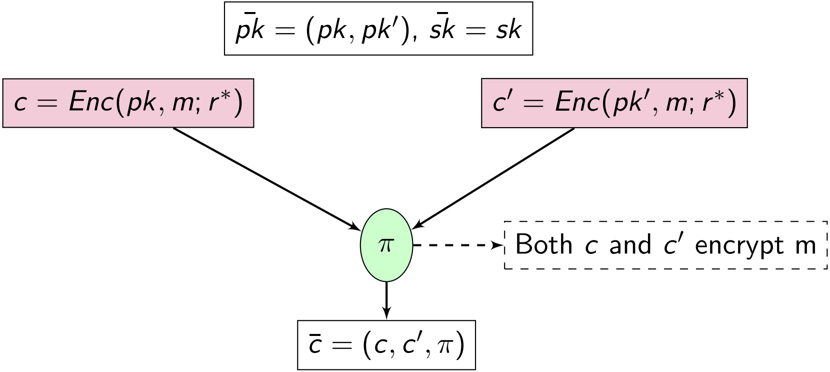
$\mathcal{F}$-KDM-CPA + simulation sound NIZK $\Rightarrow$ $\mathcal{F}$-KDM-CCA

- To decrypt we need only one secret key!
- Originally it was designed to prove only CCA security from CPA
- The two encryptions use independent randomnesses r, r'

Our Contributions

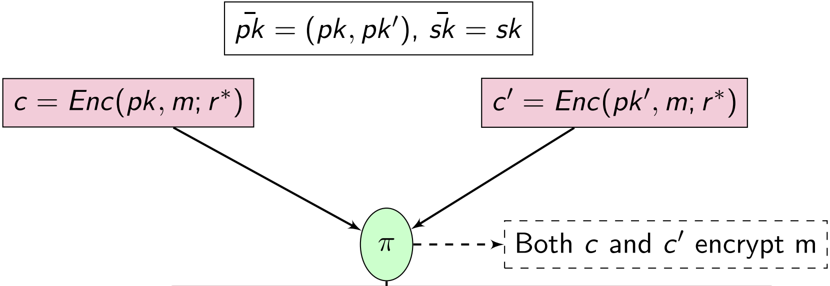
1. Twist of Naor-Young leading to more efficient concrete instantiations
2. First PKE scheme whose KDM-CPA security based on instances of the Subset Sum problem (robustness to quantum attacks)
3. Concrete instantiations from Decisional Diffie-Hellman, Quadratic Residuosity, Subset Sum with 50% gain in communication complexity

Twist of Naor-Yung



- Natural idea: have c and c' share the same randomness r^*
- Leads to a more efficient design of the NIZK

Twist of Naor-Yung



Question

When and under which conditions does it work?

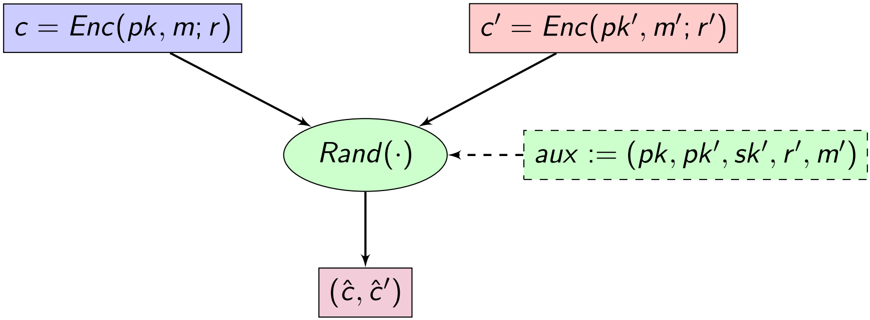
- Natural idea: have c and c' share the same randomness r^*
- Leads to a more efficient design of the NIZK

Randomness Fusion

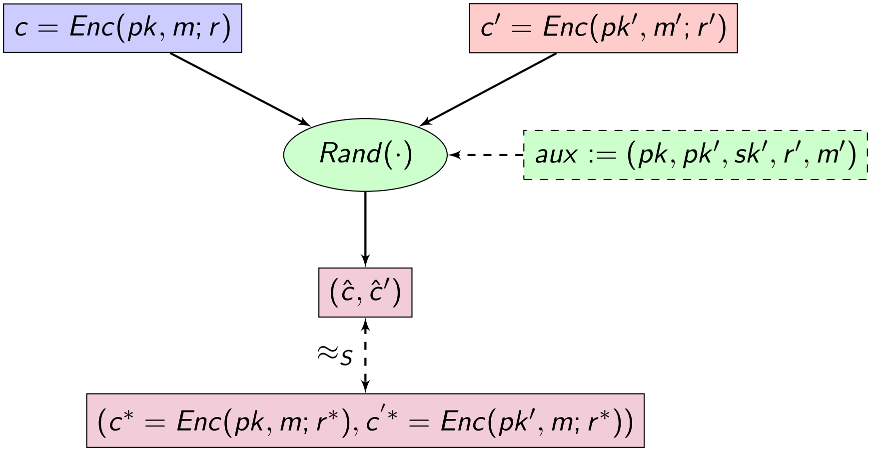
$$c = Enc(pk, m; r)$$

$$c' = Enc(pk', m'; r')$$

Randomness Fusion



Randomness Fusion



Main Theorem

Theorem (NY, shared randomness)

Randomness Fusion $+$ $\mathcal{F}$*-KDM-CPA* $+$ *Simulation Sound NIZK* $\Rightarrow$ $\mathcal{F}$*-KDM-CCA*

Extensions:

- Effective also for CCA security
- It also works in the setting of key-leakage (security of PKE against side-channel attacks)

ElGamal and Randomness Fusion

$(\mathbb{G}, q, g)$ cyclic group of prime order q with generator g

$pk = h = g^x \in \mathbb{G}$, $sk = x$
$(c_1, c_2) := Enc(pk, m; r) = (g^r, h^r \cdot m)$

ElGamal and Randomness Fusion

$(\mathbb{G}, q, g)$ cyclic group of prime order q with generator g

$pk = h = g^x \in \mathbb{G}$, $sk = x$
$(c_1, c_2) := Enc(pk, m; r) = (g^r, h^r \cdot m)$

- **first encryption:** $h = g^x$, $c = (c_1, c_2) = (g^r, h^r m)$
- **second encryption:** $h' = g^{x'}$, $x' = sk'$, $c' = (c_1', c_2') = (g^{r'}, h'^{r'} m')$,

ElGamal and Randomness Fusion

$(\mathbb{G}, q, g)$ cyclic group of prime order q with generator g

$pk = h = g^x \in \mathbb{G}$, $sk = x$
$(c_1, c_2) := Enc(pk, m; r) = (g^r, h^r \cdot m)$

- **first encryption:** $h = g^x$, $c = (c_1, c_2) = (g^r, h^r m)$
- **second encryption:** $h' = g^{x'}$, $x' = sk'$, $c' = (c_1', c_2') = (g^{r'}, h'^{r'} m')$,

- Randomness Fusion
  1. $c_1^* = c_1^{*\prime} = c_1 c_1'$
  2. $c_2^* = (h^r m) h^{r'}$
  3. $c_2^{*\prime} = c_2' (g^r)^{x'}$

ElGamal and Randomness Fusion

$(\mathbb{G}, q, g)$ cyclic group of prime order q with generator g

$pk = h = g^x \in \mathbb{G}$, $sk = x$
$(c_1, c_2) := Enc(pk, m; r) = (g^r, h^r \cdot m)$

- **first encryption:** $h = g^x$,
  $c = (c_1, c_2) = (g^r, h^r m)$
- **second encryption:**
  $h' = g^{x'}$,
  $x' = sk'$,
  $c' = (c'_1, c'_2) = (g^{r'}, h'^{r'} m')$,

- Randomness Fusion
  1. $c_1^* = c_1^{*\prime} = c_1 c'_1$
  2. $c_2^* = (h^r m) h^{r'}$
  3. $c_2^{*\prime} = c'_2 (g^r)^{x'}$

Easy to show that c_1^* and c_2^* are statistically close to fresh encryptions with randomness $r^* = r + r'$

ElGamal NIZK

statement $x := (h, (c_1, c_2), h', (c_1', c_2'))$

witness $\omega := (r, r')$

$$\alpha := (\alpha_1, \alpha_2, \alpha_3) = (g^s, g^{s'}, h^s \cdot (h')^{s'}) \longrightarrow$$

$$\longleftarrow \beta \leftarrow \mathbb{Z}_q$$

$$\gamma := (\gamma_1, \gamma_2) = (s - \beta r, s' + \beta r') \longrightarrow$$

ElGamal NIZK

statement $x := (h, (c_1, c_2), h', (c_1', c_2'))$

witness $\omega := (r, r')$

$$\alpha := (\alpha_1, \alpha_2, \alpha_3) = (g^s, g^{s'}, h^s \cdot (h')^{s'}) \longrightarrow$$

$$\beta \leftarrow \mathbb{Z}_q \quad \longleftarrow$$

$$\gamma := (\gamma_1, \gamma_2) = (s - \beta r, s' + \beta r') \longrightarrow$$

- $\beta := H(x||\alpha)$ to obtain $\pi = (\alpha, \gamma)$ via Fiat-Shamir [FS86]

ElGamal NIZK

statement $x := (h, (c_1, c_2), h', (c'_1, c'_2))$

witness $\omega := (r, \cancel{r'})$

$$\alpha := (\alpha_1, \cancel{\alpha_2}, \alpha_3) = (g^s, \cancel{g^{s'}}, h^s \cdot (h')^{s\cancel{s'}}) \longrightarrow$$

$$\beta \leftarrow \mathbb{Z}_q \longleftarrow$$

$$\gamma := (\gamma_1, \cancel{\gamma_2}) = (s - \beta r, \cancel{s' + \beta r'}) \longrightarrow$$

- $\beta := H(x||\alpha)$ to obtain $\pi = (\alpha, \gamma)$ via Fiat-Shamir [FS86]

ElGamal NIZK

statement $x := (h, (c_1, c_2), h', (c'_1, c'_2))$

witness $\omega := (r, r')$

Improvement

6 group elements instead of 9 group elements

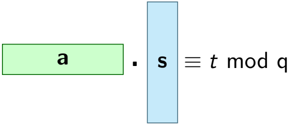
(33% gain)

- $\beta := H(x||\alpha)$ to obtain $\pi = (\alpha, \gamma)$ via Fiat-Shamir [FS86]

In the paper: Concrete instantiations for KDM security based on DDH, QR, Subset Sum with 50% gain in ciphertext size

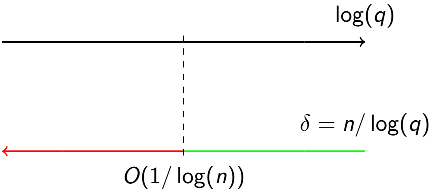
Subset Sum

$\mathbf{s} \in \{0,1\}^n$, $\mathbf{a} \in \mathbb{Z}_q^n$



Original Subset Sum

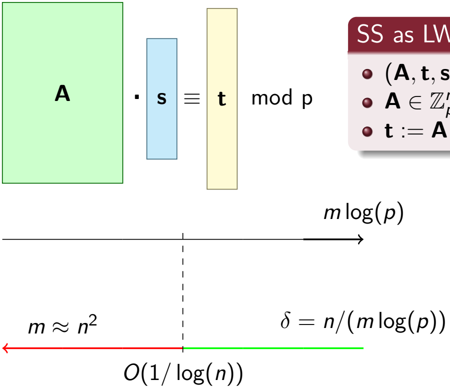
- $(\mathbf{a}, t, \mathbf{s}) \leftarrow SS(n, q)$
- $(\mathbf{a}, t) \approx_S (\mathbf{a}, u)$,
  where u is random in $\mathbb{Z}_q$



Subset Sum

$$\mathbf{s} \in \{0,1\}^n,\ \mathbf{a} \in \mathbb{Z}_q^n$$

$$q := p^m$$



SS as LWE (Lyubashevsky, Palacio, Segev)

- $(\mathbf{A}, \mathbf{t}, \mathbf{s}) \leftarrow SS(n, q)$
- $\mathbf{A} \in \mathbb{Z}_p^{m \times n}$
- $\mathbf{t} := \mathbf{A} \cdot \mathbf{s} + e(A, \mathbf{s})$ (deterministic noise)

Subset Sum

$\mathbf{s} \in \{0,1\}^n$, $\mathbf{a} \in \mathbb{Z}_q^n$

A

, Segev)

ic noise)

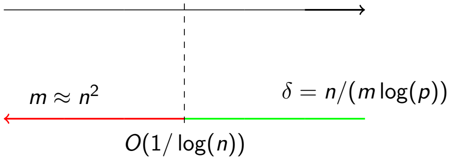
Example

- $p = 10$, $m = n = 3$
- $a = (738, 916, 375) \qquad s = (0, 1, 1)$

$$a \cdot s \; mod \; 10^3 = 916 + 375 \; mod \; 10^3 = 291$$

- written in base p:

$$\begin{bmatrix} 7 & 9 & 3 \\ 3 & 1 & 7 \\ 8 & 6 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 9 \\ 1 \end{bmatrix}$$



Subset Sum

$\mathbf{s} \in \{0,1\}^n$, $\mathbf{a} \in \mathbb{Z}_q^n$

Example

Crypto from Subset Sum

- PRG and UOWHFs [IN96]
- CPA and CCA secure PKE [LPS10,FMV16]

egev)

ic noise)

A

$$\begin{bmatrix} 7 & 9 & 3 \\ 3 & 1 & 7 \\ 8 & 6 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 9 \\ 1 \end{bmatrix}$$

$m \approx n^2$

$\delta = n/(m \log(p))$

$O(1/\log(n))$

Our Subset Sum Based Scheme

$$pk := \mathbf{A}, \mathbf{t} \qquad sk := \mathbf{s}$$

C_1

$$\mathbf{R} \cdot \mathbf{A}$$

$$\mathbf{R} \leftarrow_{\$} [-\lfloor\sqrt{p}/2\rfloor, \lfloor\sqrt{p}/2\rfloor]^{\ell\times m}$$

c_2

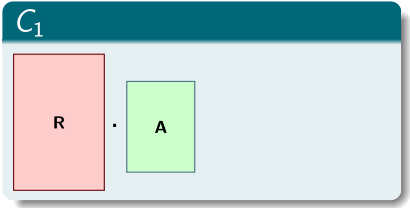
$$\mathbf{R} \cdot \mathbf{t} + \mathbf{m} \cdot \lfloor \tfrac{p}{2} \rfloor$$

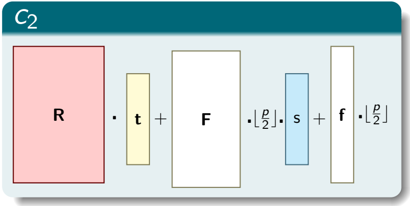
Decryption of (C_1, c_2)

$$\mathbf{c}_2 - \mathbf{C}_1 \cdot \mathbf{s} \equiv \lfloor \mathbf{m} \rceil_2 \bmod p$$

$\mathcal{F}$-KDM CPA Security of the Scheme

$$\mathcal{F}_{aff} := \{f : f(\mathbf{s}) := \mathbf{F}\cdot\mathbf{s} + f\}, \mathbf{F} \in \mathbb{Z}_2^{\ell\times n}, \mathbf{f} \in \mathbb{Z}_2^{\ell}$$

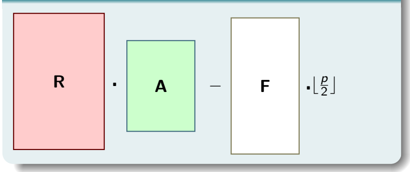




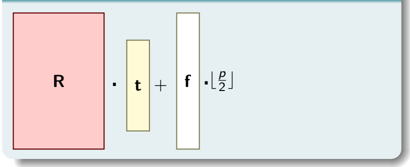
$\mathcal{F}$-KDM CPA Security of the Scheme

$$\mathcal{F}_{aff} := \{f : f(\mathbf{s}) := \mathbf{F} \cdot \mathbf{s} + f\}, \mathbf{F} \in \mathbb{Z}_2^{\ell \times n}, \mathbf{f} \in \mathbb{Z}_2^{\ell}$$

C_1



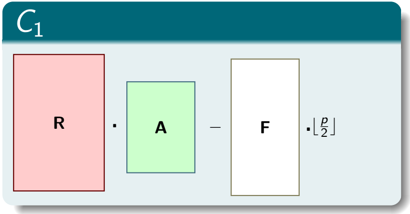
C_2

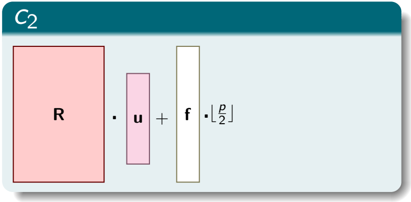


$G_0 \to G_1$ Indistinguishability due to Leftover-Hash Lemma

$\mathcal{F}$-KDM CPA Security of the Scheme

$$\mathcal{F}_{aff} := \{f : f(\mathbf{s}) := \mathbf{F}\cdot\mathbf{s} + f\}, \mathbf{F} \in \mathbb{Z}_2^{\ell\times n}, \mathbf{f} \in \mathbb{Z}_2^{\ell}$$





$G_0 \rightarrow G_1$ Indistinguishability due to Leftover-Hash Lemma

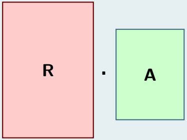
$G_1 \rightarrow G_2$ Indistinguishability due to Subset Sum Assumption

$\mathcal{F}$-KDM CPA Security of the Scheme

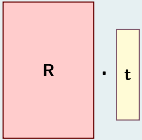
KDM Security Amplification

From affine functions to all functions computable in some fixed polynomial time [Applebaum11]

C_1



c_2



$G_0 \rightarrow G_1$ Indistinguishability due to Leftover-Hash Lemma
$G_1 \rightarrow G_2$ Indistinguishability due to Subset Sum Assumption
$G_2 \rightarrow G_3$ Indistinguishability due to Leftover-Hash Lemma and Subset Sum Assumption

Thank You!

Contents