KDM-CCA Security from RKA Secure Authenticated Encryption

Xianhui Lu, Bao Li, Dingding Jia

Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China

Abstract

- Background of KDM Security
- Our Contribution
- Conclusion

Background of KDM

- Key Dependent Message

$$\mathrm{E}_{PK}\left(m\right)$$

$$\mathrm{E}_{PK}\left(SK\right)$$

Lock the password into the safe box.

Background of KDM

- The threat of KDM?

$$m^e$$

$$d^e$$

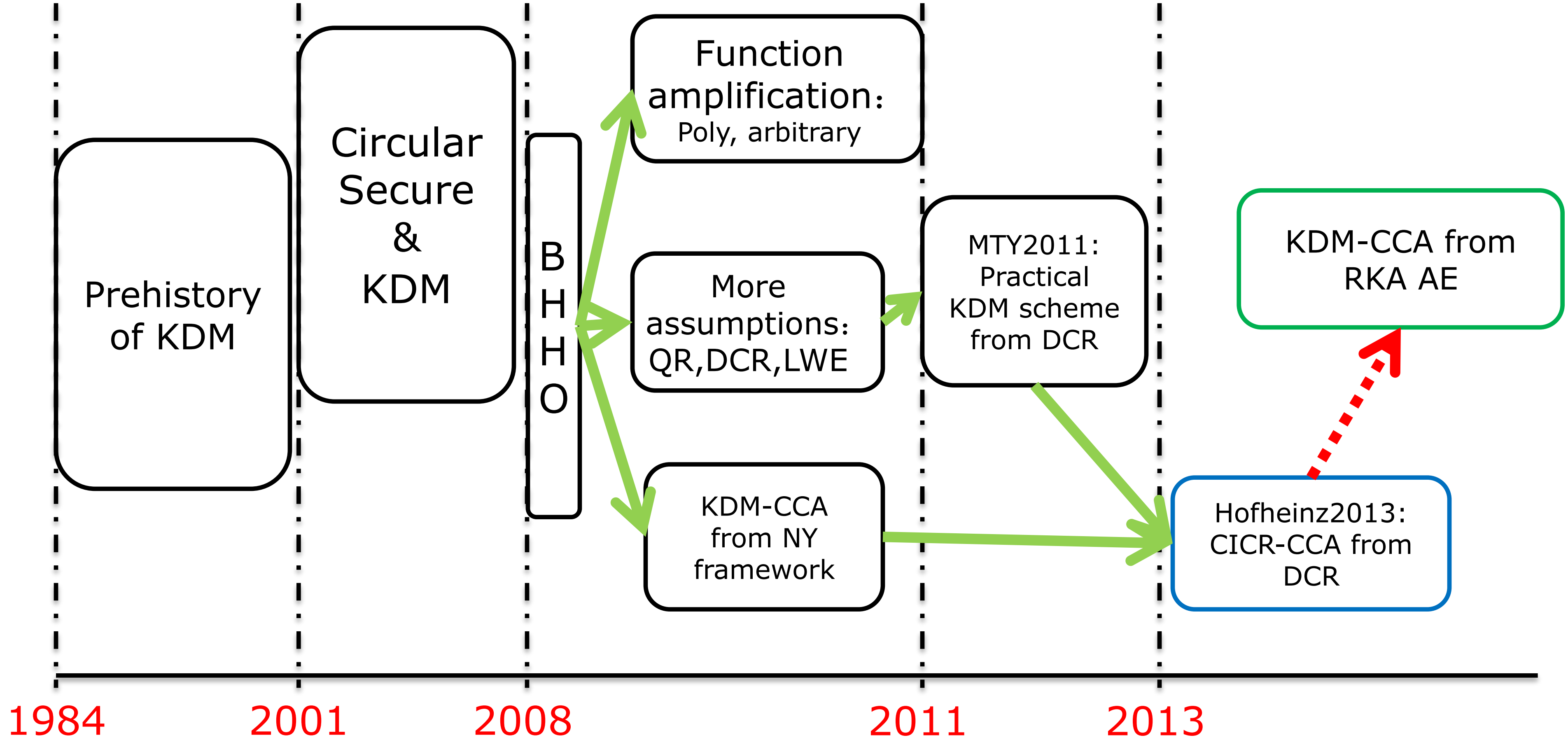
$$g^r, g^{rx} \cdot m$$

$$g^r, g^{rx} \cdot x$$

The attacker may recover the password by using the x-ray scanner.

Background of KDM

- State of the art.



Prehistory of KDM

Circular Secure & KDM

BHHO

Function amplification: Poly, arbitrary

More assumptions: QR,DCR,LWE

KDM-CCA from NY framework

MTY2011: Practical KDM scheme from DCR

Hofheinz2013: CICR-CCA from DCR

KDM-CCA from RKA AE

1984

2001

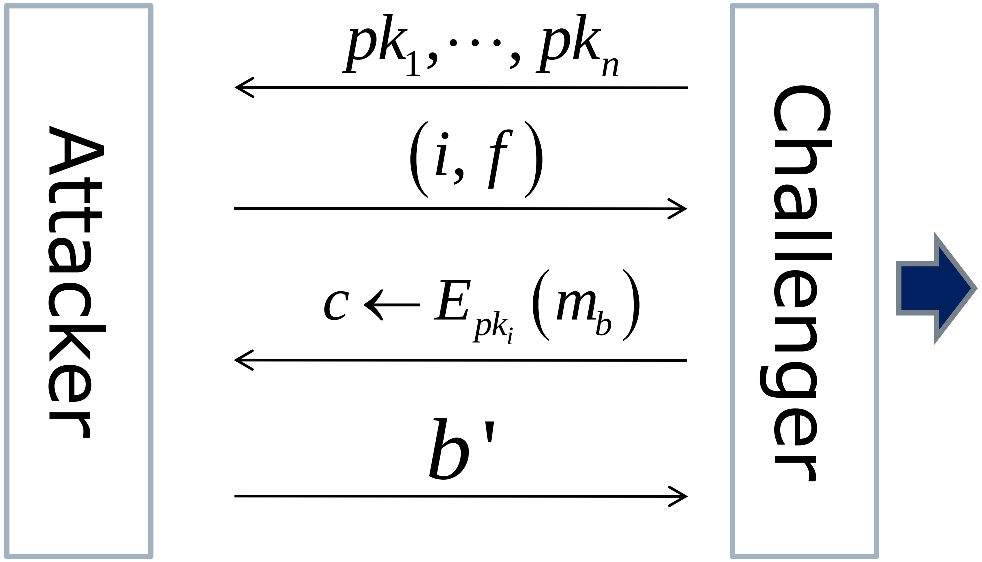
2008

2011

2013

Background of KDM

- Definition of KDM Security



$$m_0 = 0^{|f(sk_1 \| sk_2 \cdots \| sk_n)|},$$

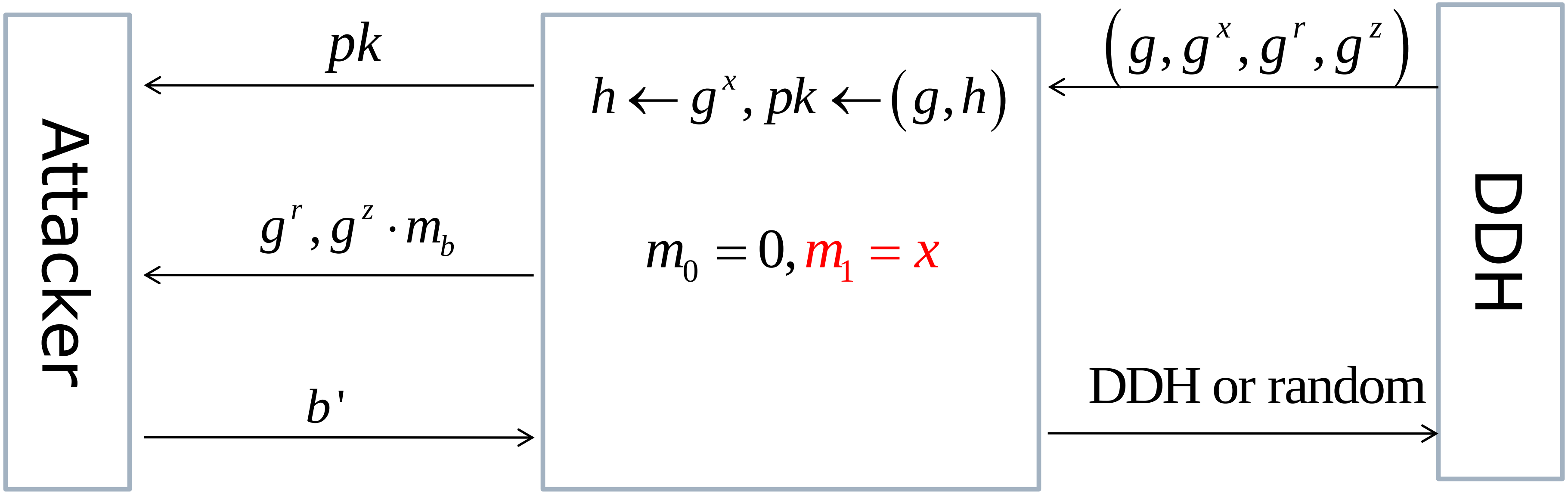
$$m_1 = f(sk_1 \| sk_2 \cdots \| sk_n)$$

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

J. Black, P. Rogaway and T. Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In Kaisa Nyberg and Howard M. Heys, editors, Selected Areas in Cryptography, volume 2595 of Lecture Notes in Computer Science, pages 62-75. Springer, 2002.

Background of KDM

- The difficulty in the security reduction.



Attacker

pk

$h \leftarrow g^x, pk \leftarrow (g,h)$

(g, g^x, g^r, g^z)

DDH

$g^r, g^z \cdot m_b$

$m_0 = 0, m_1 = x$

b'

DDH or random

The simulator can not construct the challenger ciphertext when b=1.

Background of KDM

- Intuition of the difficulty of KDM

$$\text{DDH:}\left(g, g^{x}, g^{r}, g^{rx}\right)$$

$$\text{IND-CPA:}\left(g, g^{x}, g^{r}, g^{rx}m\right)$$

$$\text{KDM:}\left(g, g^{x}, g^{r}, g^{rx}\cdot x\right)$$

DDH assumption can not guarantee the randomness of the quadruple when x and g^{rx} are not independent to each other.

Background of KDM

- Solution in the random oracle model

$$\mathrm{CL2001:E}_{pk}\left(s\right),\mathrm{H}\left(s\right)\oplus sk$$

$$\mathrm{BRS2002:f}\left(s\right),\mathrm{H}\left(s\right)\oplus f^{-1}$$

$$\mathrm{Elgamal:}\ g^{r},g^{rx}\cdot s,\mathrm{H}\left(s\right)\oplus x$$

The ideal property of RO guarantees the randomness even s is dependent on sk.

Background of KDM

- ☐ Solution in the standard model

$$\left(g, g^{x}, g^{r}, g^{rx} x\right)$$

$$\left(g, g^{x}, g^{r}, g^{rx} \cdot v^{x}\right)$$

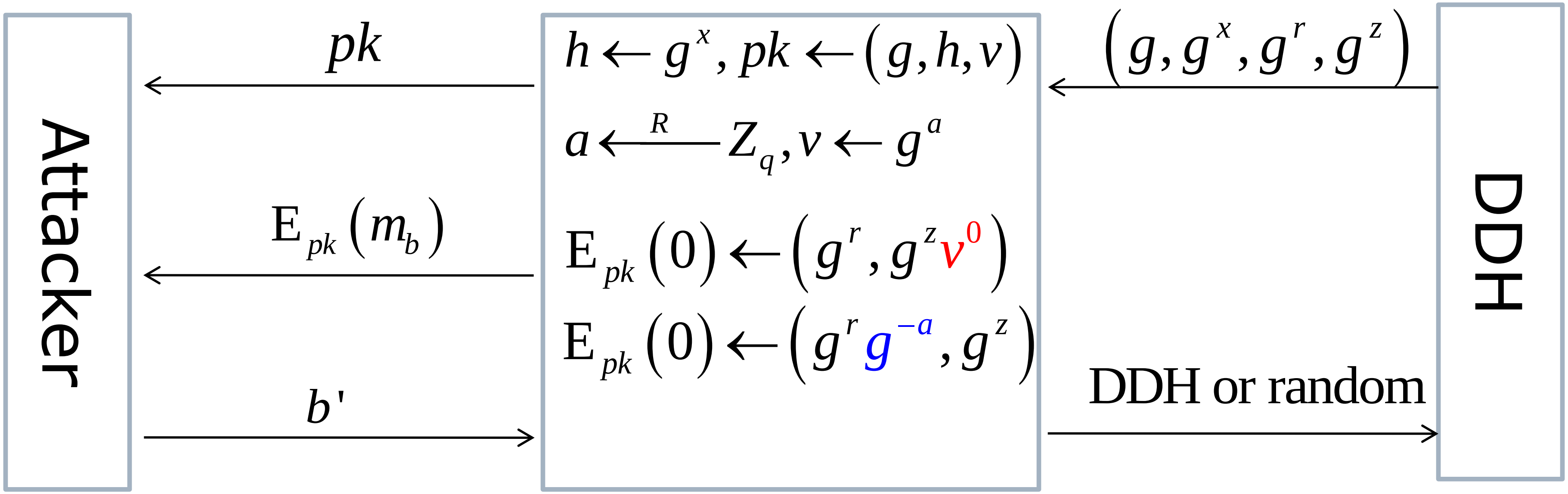
$$\left(g, g^{x}, g^{r}, g^{(r+a)x}\right), v = g^{a}$$

$$\left(g, g^{x}, g^{r} g^{a}, g^{(r+a)x}\right), r' = r + a$$

Move the message to the exponent.

Background of KDM

- Is this solution ok?



$$(g, g^{x}, g^{r}, g^{z})$$

$$h \leftarrow g^{x}, pk \leftarrow (g, h, v)$$

$$a \xleftarrow{R} Z_q, v \leftarrow g^{a}$$

$$E_{pk}(0) \leftarrow (g^{r}, g^{z} v^{0})$$

$$E_{pk}(0) \leftarrow (g^{r} g^{-a}, g^{z})$$

The security reduction works, but we can not decrypt by using v^{x}.

Background of KDM

- The solution of BHHO2008

$$\left(g, g^{x}, g^{r}, g^{rx}\right) -- sk = x$$

$$\downarrow$$

$$\left(g_1^{r}, \cdots, g_l^{r}, \prod_{i=1}^{l} g_i^{rx_i} \cdot g^{x_j}\right) -- sk = \left(g^{x_1}, \cdots, g^{x_l}\right)$$

The private key is split to a bit string and encoded as group elements.

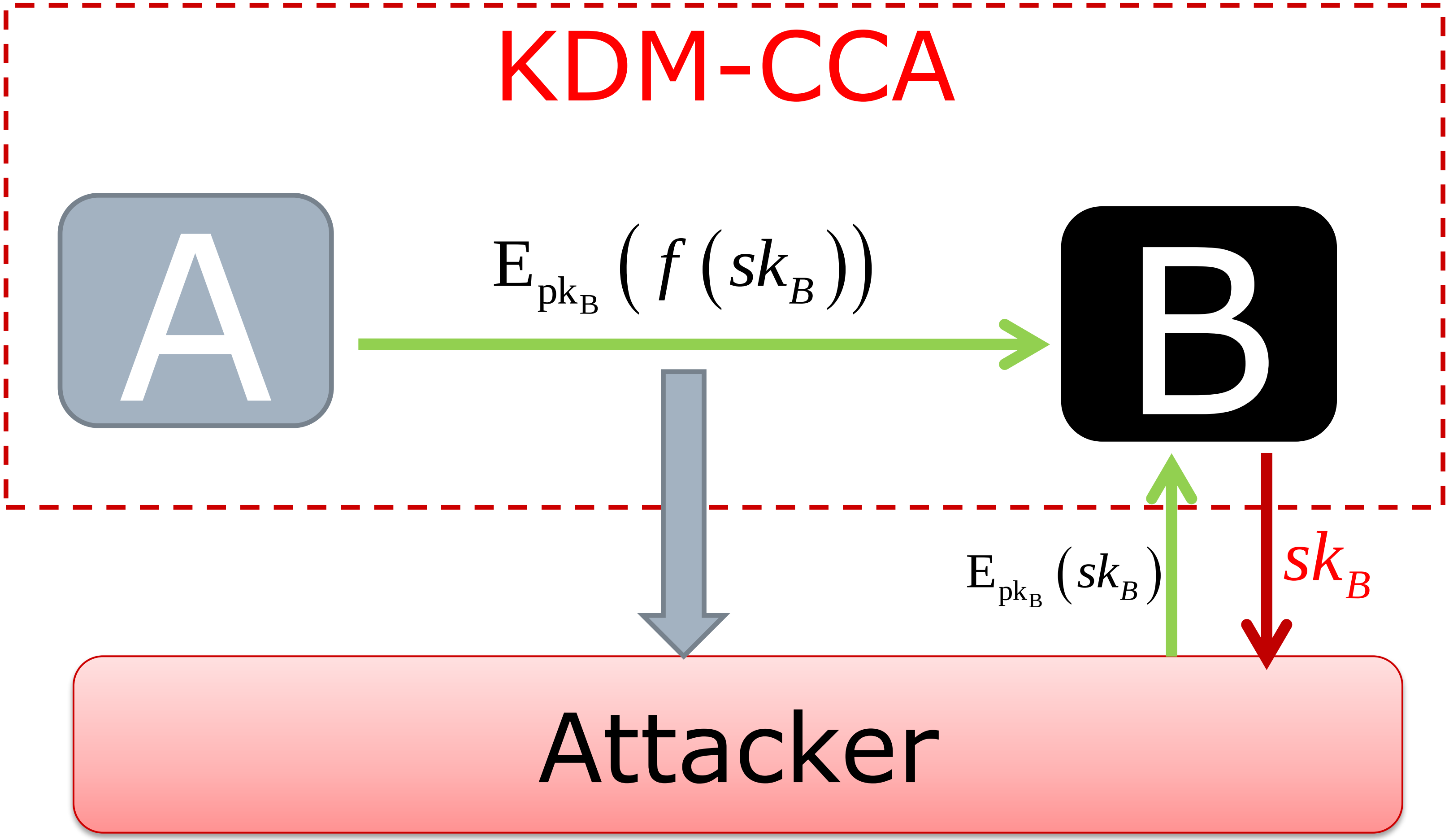
Background of KDM

- The most important of BHHO2008:

$$\left(g_1^r,\cdots,g_i^r g,\cdots,g_l^r,h^r\right),h=\prod_{i=1}^{l} g_i^{-x_i}$$

Encryptions of the private key can be constructed publicly without the private key.

Background of KDM


KDM-CCA
A
B
$\mathrm{E}_{\mathrm{pk}_B}\left(f\left(sk_B\right)\right)$
$\mathrm{E}_{\mathrm{pk}_B}\left(sk_B\right)$
sk_B
Attacker

The attacker can get the private key by using the decryption oracle.

Background of KDM

- Theoretical construction.

$$\left(E_{kdm}(m), E_{cca}(m), P, vk, s\right)$$

$$\left(E_{kdm}\left(f\left(sk_{kdm}\right)\right), E_{cca}\left(f\left(sk_{kdm}\right)\right), P, vk, s\right)$$

CCS2009：Extend Naor and Yung's double encryption framework to achieve KDM-CCA security。

Background of KDM

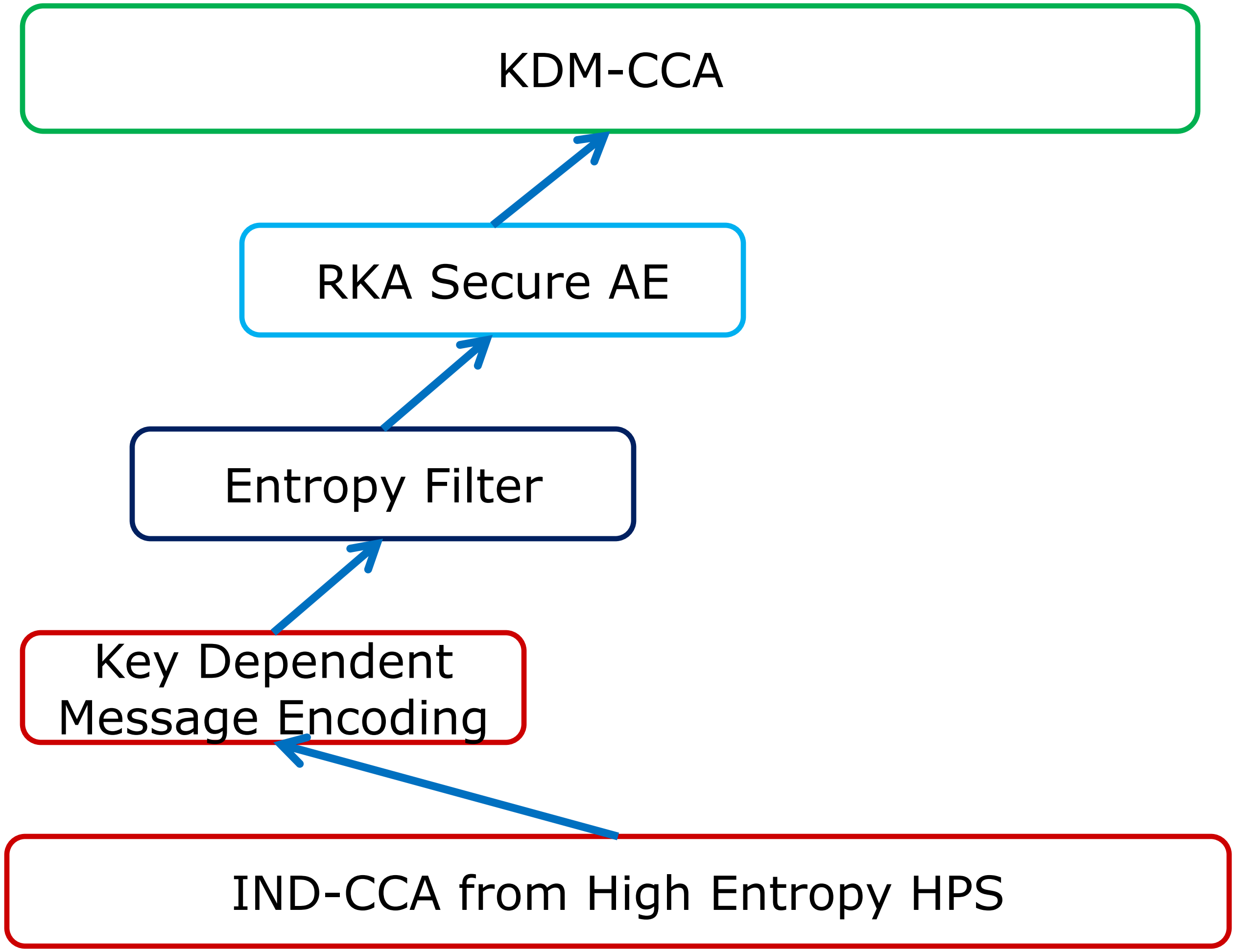
- Hofheinz’s compact construction

$$g_1^{r}, g_2^{r}, g_1^{r'}, g_2^{r'}, \left(u^{vk}v\right)^{rN^2}, \left(u^{vk}v\right)^{r} u^{r'} \left(1+N\right)^{k+2^{l}[M]}, \mathrm{E}_k\left(\mathrm{LAF}\left(\left[M\right]\right)\right), vk, \sigma, t_c$$

Preventing the public construction of key dependent message encryption by using the entropy of the private key.

Preventing the challenge ciphertexts from release the entropy of the private key completely by using the LAF (Lossy Algebraic Filter).

Our Contribution



KDM-CCA

RKA Secure AE

Entropy Filter

Key Dependent Message Encoding

IND-CCA from High Entropy HPS

Our Contribution

$$g_1^r, g_2^r, \mathrm{AE.E}_k\left(f\left(x_1, x_2\right)\right), k \leftarrow \mathrm{H}\left(u_1, u_2, u_1^{x_1} u_2^{x_2}\right)$$

$$g_1^r, g_2^r, h^r\left(1+N\right)^s, \mathrm{AE.E}_k\left(g_1^{r'} \| g_2^{r'} \| h^{r'}\left(1+N\right)^m\right), k \leftarrow \mathrm{H}\left(u_1, u_2, e, s\right)$$

$$g_1^r, g_2^r, h^r\left(1+N\right)^s, \mathrm{AE.E}_k\left(\mathrm{H}\left(u_1, u_2, e, g_1^m\right) \| g_1^{r'} \| g_2^{r'} \| h^{r'}\left(1+N\right)^m\right), k \leftarrow \mathrm{H}\left(s\right)$$

$$g_1^r, g_2^r, h^r\left(1+N\right)^k, \mathrm{AE.E}_k\left(\mathrm{H}\left(u_1, u_2, e, g_1^m\right) \| g_1^{r'} \| g_2^{r'} \| h^{r'}\left(1+N\right)^m\right)$$

Our Contribution

- How to divide the entropy of the private key

$$\left(g_1^r, g_2^r, h^r(1+N)^m\right), h \leftarrow g_1^{-x_1} g_2^{-x_2}, sk \leftarrow \left(x_1, x_2 \in \left[\left\lfloor N^2 / 4 \right\rfloor\right]\right)$$

$$h = g_1^{-x_1} g_2^{-x_2} = g_1^{-(x_1+wx_2) \bmod \phi(N)}$$

$$x_1^{real} = x_1 \bmod \phi(N)/4, x_1^{hide} = x_1 \bmod N$$

$$x_2^{real} = x_2 \bmod \phi(N)/4, x_2^{hide} = x_2 \bmod N$$

Our Contribution

- How to filter the entropy of the private key.

$$g_1^r, g_2^r, h^r(1+N)^k, \mathrm{AE.E}_k\left(\mathrm{H}\left(u_1,u_2,e,g_1^m\right) \| g_1^{r'} \| g_2^{r'} \| h^{r'}(1+N)^m\right)$$

$$x_1^{real} = \tilde{x}_1 \bmod \phi(N), x_1^{hide} = \tilde{x}_1 \bmod N$$

$$x_2^{real} = \tilde{x}_2 \bmod \phi(N), x_2^{hide} = \tilde{x}_2 \bmod N$$

$$g_1^m = g_1^{f(x_1,x_2) \bmod \phi(N)/4}$$

$$g_1^r(1+N)^{s_1} \bmod N^2, g_2^r(1+N)^{s_2} \bmod N^2, \left(g_1^{x_1} g_2^{x_2}\right)^r (1+N)^{s_1 x_1^{hide} + s_2 x_2^{hide} + k} \bmod N^2$$

Our Contribution

- How to reuse the entropy of the private key.

$$g_1^r, g_2^r, h^r(1+N)^k, \mathrm{AE.E}_k\left(\mathrm{H}\left(u_1, u_2, e, g_1^m\right) \| g_1^{r'} \| g_2^{r'} \| h^{r'}(1+N)^m\right)$$

$$\left(g_1^r(1+N)^\alpha\right)^a, \left(g_2^r(1+N)^\beta\right)^a, \left(g_1^{x_1} g_2^{x_2}\right)^r (1+N)^{a\left(\alpha x_1^{hide} + \beta x_2^{hide} + k^*\right)}$$

$$k \leftarrow a \cdot k^*$$

Our Contribution

$$g_1^r, g_2^r, h^r(1+N)^k, \mathrm{AE.E}_k\left(\mathrm{H}\left(u_1, u_2, e, g_1^m\right) \| g_1^{r'} \| g_2^{r'} \| h^{r'}(1+N)^m\right)$$

Hiding vs Lossy

$$g_1^r, g_2^r, g_1^{r'}, g_2^{r'}, \left(u^{vk}v\right)^{rN^2}, \left(u^{vk}v\right)^r u^{r'}(1+N)^{k+2^l[M]}, \mathrm{E}_k\left(\mathrm{LAF}\left([M]\right)\right), vk, \sigma, t_c$$

Conclusion

$$g_1^r, g_2^r, g_1^{r'}, g_2^{r'}, \left(u^{vk}v\right)^{rN^2}, \left(u^{vk}v\right)^r u^{r'} (1+N)^{k+2^l[M]}, \mathrm{E}_k\left(\mathrm{LAF}\left(\left[M\right]\right)\right), vk, \sigma, t_c$$

More Efficient

Affine function vs Identity Function
KDM-CCA vs CIRC-CCA

$$g_1^r, g_2^r, h^r (1+N)^k, \mathrm{AE.E}_k\left(\mathrm{H}\left(u_1, u_2, e, g_1^m\right) \| g_1^{r'} \| g_2^{r'} \| h^{r'} (1+N)^m\right)$$

Thanks

TYM2011

- Extended DDH & DCR:

$\left(g, g^{x}, g^{r}, g^{rx}(1+N)^{m}\right)$	$\left(g, g^{x}, g^{r}, g^{rx} \cdot m\right)$
$\left(g, g^{x}, g^{r}, g^{rx} \cdot (1+N)^{x}\right)$	$\left(g, g^{x}, g^{r}, g^{rx} \cdot v^{x}\right)$
$\left(g^{r}, h^{r} \cdot (1+N)^{x}\right)$	$\left(g^{r}, g^{(r+a)x}\right), v = g^{a}$
$\left(g^{r}(1+N), h^{r}\right)$	$\left(g^{r} g^{a}, g^{(r+a)x}\right), r' = r + a$

(1+N)^{x} vs v^x