2023/825

# Oblivious Identity-based Encryption (IBE Secure Against an Adversarial KGC)

Aikaterini Mitrokotsa[1], Sayantan Mukherjee[2], Jenit Tomy[1]

1 University of St. Gallen, Switzerland
2 Indian Institute of Technology, Jammu, India

# Identity-based Encryption?

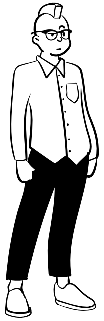
My pk is
yqV6uZL7pSZR89B8O
mLpN5v5IzXFkYzwpT7
1b+CgZ0q2mOH60b+
1h1mN3jFjLPVIrpUiUz
DhscX6hjd1XD3a69Cjs
N5IK

Alice

My pk is
mM70MBAAABMM5HiD
Wh0Vf5BWUVoso9wTFYo
NtxPBfHa3NQk+i/1XL0Z
QbYfurzUkE54ZigVPaGY
MHbK1whuxSmRD6JII

Bob

My pk is
AAMFwwDQYJKoZIhvc
NAQEBBQADSwAwSAJ
BAKj34GkxFhD90vcNL
YLInFX6Ppy1tPf9Cnzj4
p4WGeKLs1Pt8QuKUp
RKfFLfR

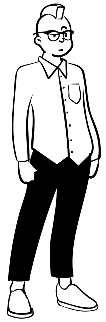


Charlie

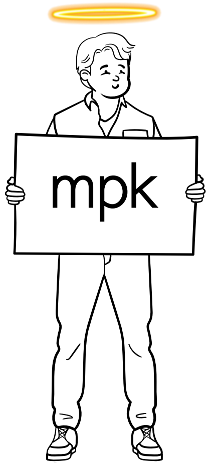
# Identity-based Encryption?

Alice
alice@wonderland.com

Bob
bob@builders.com

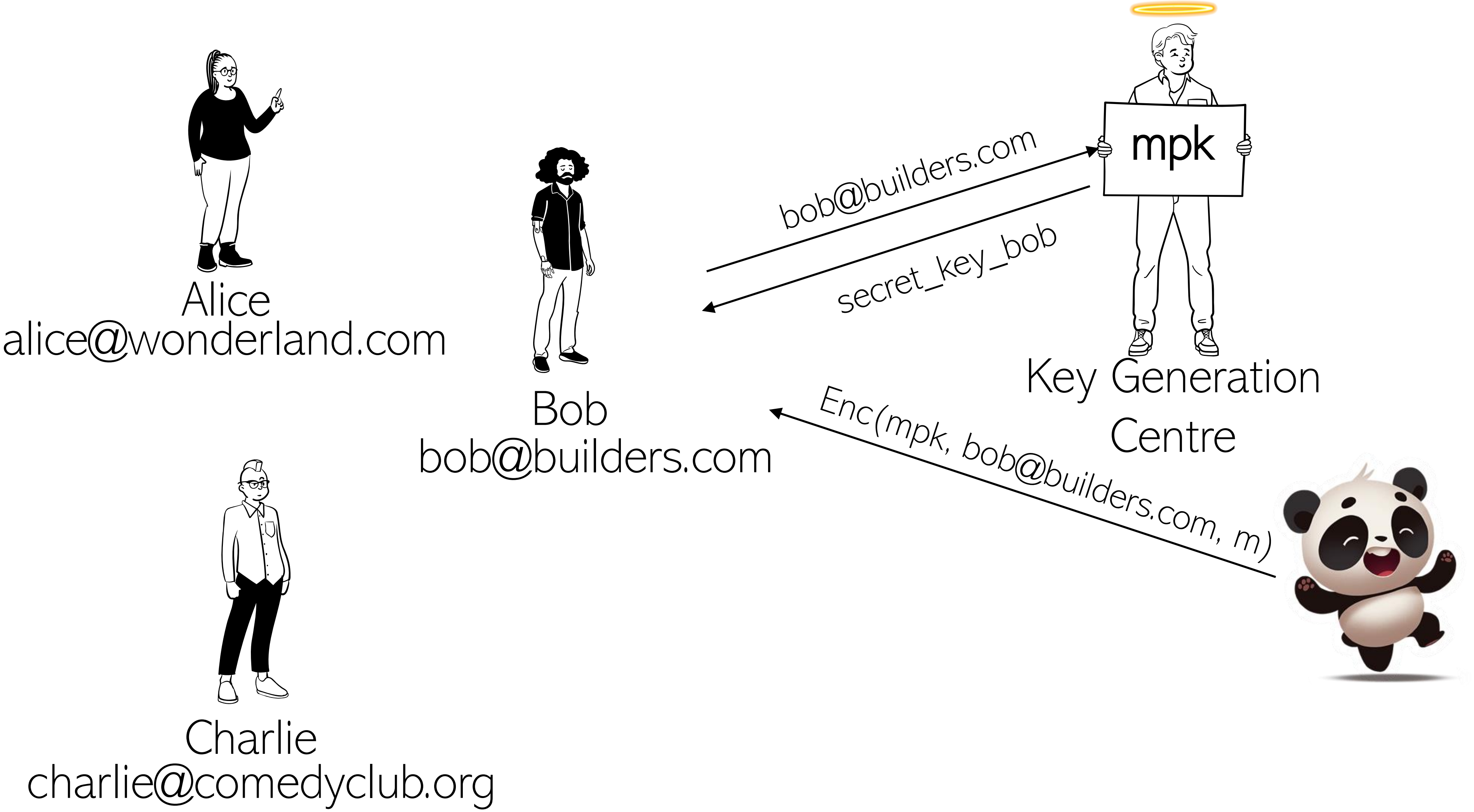


Charlie
charlie@comedyclub.org



Key Generation
Centre

# Identity-based Encryption?



Alice
alice@wonderland.com

Bob
bob@builders.com

Charlie
charlie@comedyclub.org

mpk

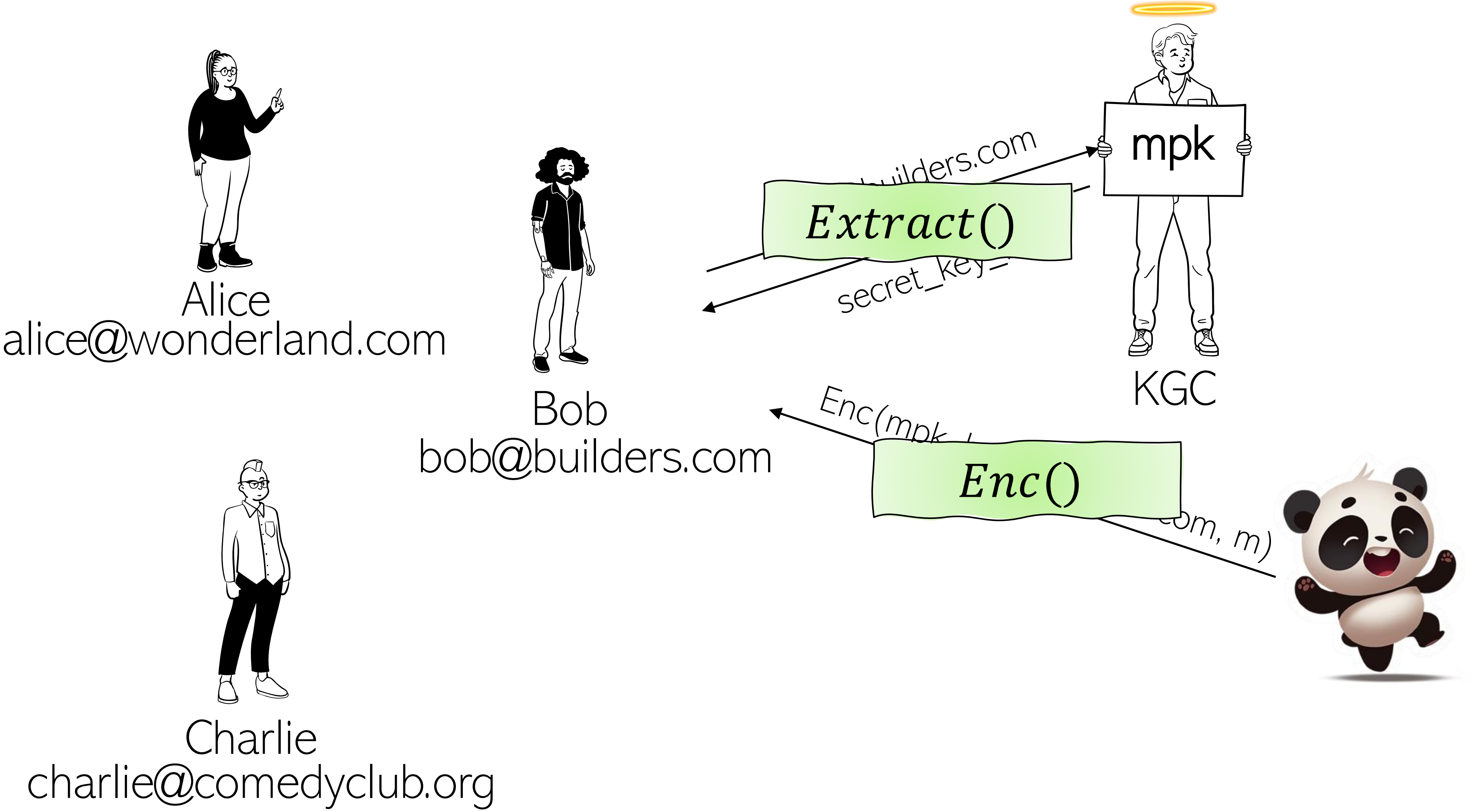
Key Generation
Centre

bob@builders.com

secret_key_bob

Enc(mpk, bob@builders.com, m)

# Identity-based Encryption?



Alice
alice@wonderland.com

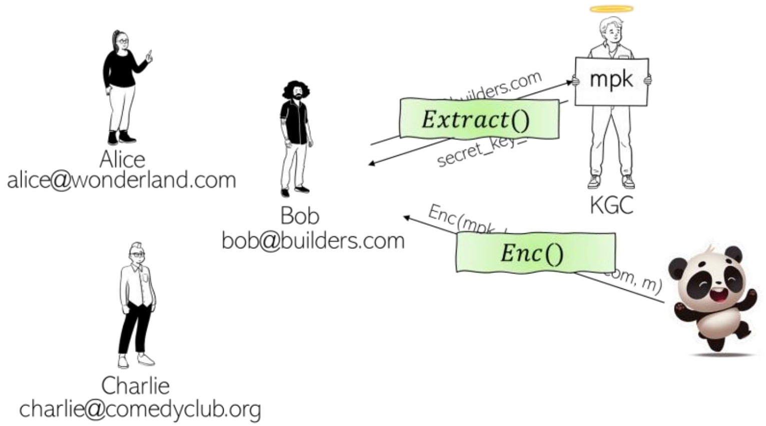
Bob
bob@builders.com

Charlie
charlie@comedyclub.org

KGC

# Identity-based Encryption [Sha84,BF01]

- $Setup(1^\lambda) \to (pp, mpk, msk)$
- $Extract(mpk, msk, ID) \to sk_{ID}$
- $Enc(mpk, ID, m) \to ct_m$
- $Dec(sk_{ID}, ct_m) \to m$ or $\perp$

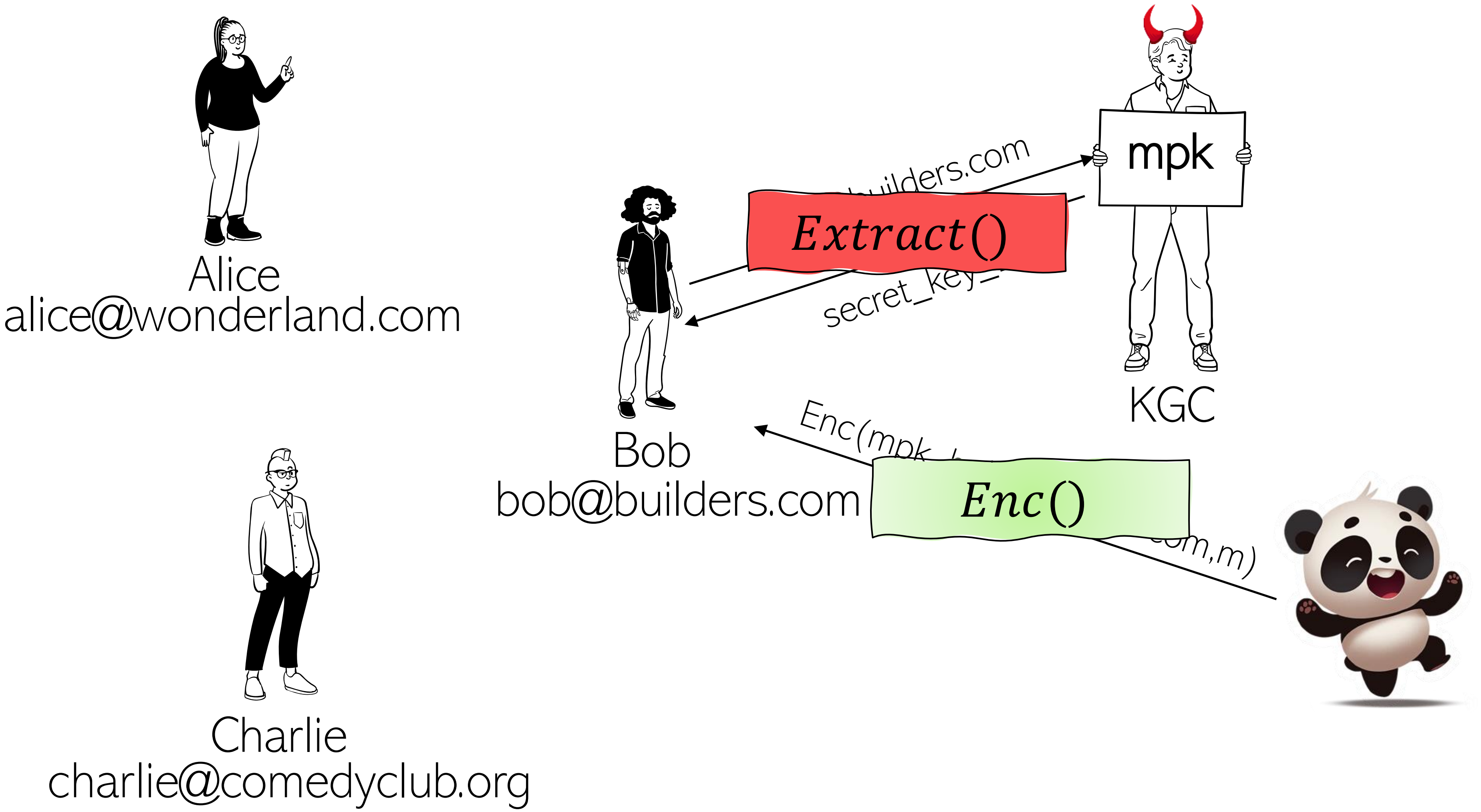


Correctness: $Dec\big(Extract(mpk, msk, ID), Enc(mpk, ID, m)\big) = m$

Security against Users

# Malicious KGC?

Can decrypt any ciphertext



Alice
alice@wonderland.com

Bob
bob@builders.com

Charlie
charlie@comedyclub.org

mpk

KGC

uilders.com

$Extract()$

secret_key_

Enc(mpk, b

$Enc()$

om,m)

# Current Solutions:

- Certificate-less Encryption[AP03]: User generates their own pk/sk pair.

- Registration-based Encryption[GHMR18,GHMRS19]: User generates pk/sk, accumulator combine it into short mpk.

- Anonymous IBE[IP08,Cho09]: Anonymity in ciphertexts.

- Blind IBE[GH07,CKRS09]: Blindly generating secret keys.

- IBE secure against KGC[EKW19]: Introducing trusted ICA

- Traceable IBE[Goy07, ADM+07]: KGC runs the risk of being caught if they ever maliciously generates and distributes a decryption key.

# Our Contributions:

Vulnerabilities of some existing schemes

New Definition for Oblivious Identity-based Encryption

OIBE Construction in Standard model without ICA

# Vulnerabilities of IBE schemes [GH07]

- $Setup(1^{\lambda}) \rightarrow (pp, mpk = (g, g_1 = g^{\alpha}, g_2, F), msk = g_2^{\alpha})$
- $Extract(mpk, msk, ID) \rightarrow sk_{ID}$
- $Enc(mpk, ID, m) \rightarrow ct_m = (m \cdot e(g_1, g_2)^t, g^t, F(ID)^t)$

KGC can compute $\boldsymbol{e(g_1, g_2)^t = e(g^{\alpha}, g_2)^t = e(g^t, g_2^{\alpha}) = e(g^t, msk)}$

Remove $\boldsymbol{e(g_1, g_2)^t}$ from $\boldsymbol{m \cdot e(g_1, g_2)^t}$ and get $\boldsymbol{m}$.

Vulnerabilities in [Wat05, CKRS09, LW10, BB11]

# Oblivious Identity-based Encryption

- $Setup(1^{\lambda}) \rightarrow (pp, mpk, msk)$
- $BlindExtract(User(mpk, ID) \leftrightarrow KGC(mpk, msk)) \rightarrow (sk_{ID}, \perp)$
- $Enc(mpk, ID, m) \rightarrow ct_m$
- $Dec(sk_{ID}, ct_m) \rightarrow m$ or $\perp$

Correctness: $Dec\big(sk_{ID}, Enc(mpk, ID, m)\big) = m$

Security against Users, Security against KGC

# OIBE: Security against Users

$$\xrightarrow{\quad params, mpk \quad}$$

$$\xrightarrow{msk} \boxed{BlindExtract} \xleftarrow{ID}$$

$$\xleftarrow{\perp} \boxed{BlindExtract} \xrightarrow{sk_{ID}}$$

$IDList \leftarrow IDList \cup \{ID\}$

$$\xleftarrow{\quad m^*, ID^* \quad}$$

$b \leftarrow \{0,1\}$
$ct_0 = Enc(mpk, ID^*, m^*)$
$ct_1 = CTSamp(mpk)$

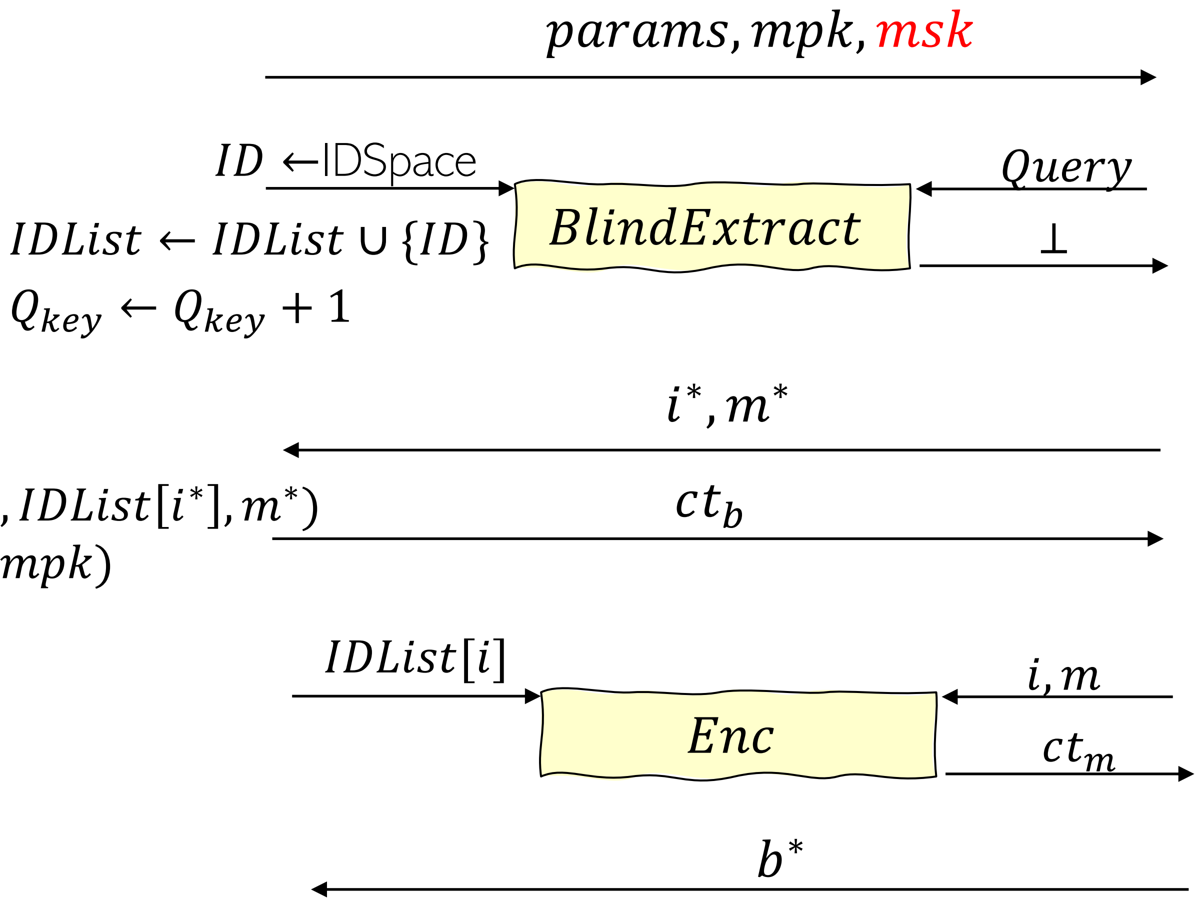
$$\xrightarrow{\quad ct_b \quad}$$

$$\xleftarrow{\quad b^* \quad}$$

Adversary wins if:
$ID^* \notin IDList$ *and*
$b = b^*$

$$Pr[\text{Adversary wins}] \leq \frac{1}{2} + negl(\lambda)$$

# OIBE: Security against KGC



$params, mpk, msk$

$ID$ ←IDSpace

$BlindExtract$

$Query$

$\perp$

$IDList \leftarrow IDList \cup \{ID\}$

$Q_{key} \leftarrow Q_{key} + 1$

$i^*, m^*$

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

$ct_0 = Enc(mpk, IDList[i^*], m^*)$

$ct_1 = CTSamp(mpk)$

$ct_b$

$IDList[i]$

$Enc$

$i, m$

$ct_m$

$b^*$

Adversary wins if:

$i^* \in [Q_{key}]$ *and*

$b = b^*$

$$Pr[\text{Adversary wins}] \leq \frac{1}{2} + negl(\lambda)$$

# IBE: Building Blocks

- Composite-order Bilinear maps

- $(N, G, H, G_T, e) \leftarrow GGen(1^\lambda)$ where $G, H, G_T$ are cyclic groups of order $N = p_1 p_2$ and $G = G_{p_1} G_{p_2}$ and $H = H_{p_1} H_{p_2}$

- $e: G \times H \rightarrow G_T$ is a non-degenerate bilinear map

- $g_1, g_2, h_1, h_2$ are random generators of $G_{p_1}, G_{p_2}, H_{p_1}, H_{p_2}$

# IBE: Cryptographic Assumptions

Subgroup Decision SD1 for group $\boldsymbol{G}$

- $\{g_1, h_1, Z \leftarrow G\} \approx \{g_1, h_1, Z \leftarrow G_{p_1}\}$

Subgroup Decision SD2 for group $\boldsymbol{H}$

- $\{g_{\{1,2\}}, h_1, Z \leftarrow H\} \approx \{g_{\{1,2\}}, h_1, Z \leftarrow H_{p_1}\}$ where $g_{\{1,2\}} \leftarrow G$

# IBE Construction [Wee15]

$Setup(1^{\lambda})$:

$msk \coloneqq (\alpha, u) \leftarrow \mathbb{Z}_N \times H_{p_1}$

$mpk \coloneqq (g_1, g_1^{\alpha}, e(g_1, u), \mathbf{H})$

In OIBE, we compute this obliviously!

$Extract(msk, ID)$:

$return\ sk_{ID} \coloneqq u^{\frac{1}{\alpha+ID}}$

$Enc(mpk, ID, m)$:

$Pick\ s \leftarrow \mathbb{Z}_N$

$(ct_0, ct_1) \coloneqq (g_1^{(\alpha+ID)s}, m \oplus \mathbf{H}(e(g_1, u)^s))$

$Dec(sk_{ID}, ct)$:

$return\ \ ct_1 \oplus \mathbf{H}\big(e(ct_0, sk_{ID})\big) = m \oplus \mathbf{H}(e(g_1, u)^s) \oplus \mathbf{H}(e(g_1^{(\alpha+ID)s}, u^{\frac{1}{\alpha+ID}})\ )$

# OIBE: Building Blocks

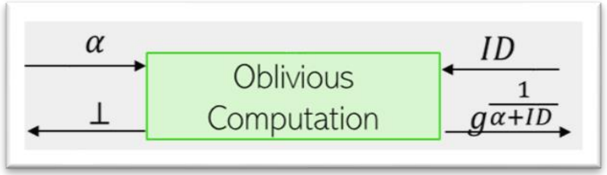
## Additive Homomorphic Encryption

- $HSetup(pp) \rightarrow (hsk, hpk)$
- $HEnc(hpk, m) \rightarrow C_m$
- $HDec(hsk, C_m) \rightarrow m$ or $\perp$

## Properties:

- $\left(HEnc(hpk, m)\right)^r = HEnc(hpk, r \cdot m)$
- $HEnc(hpk, m_1) \cdot HEnc(hpk, m_2) = HEnc(hpk, m_1 + m_2)$

# Oblivious Computation [JL09]: $g^{\frac{1}{\alpha+ID}}$



KGC

Bob

$(hsk_{KGC}, hpk_{KGC}) \leftarrow HSetup(pp)$

$$\xrightarrow{C_\alpha = HEnc(hpk_{KGC}, \alpha), hpk_{KGC}}$$

$r \leftarrow \mathbb{Z}_N$

$C_{ID} = (C_\alpha \cdot HEnc(hpk_{KGC}, ID))^r$

$= HEnc\ (hpk_{KGC}, r(\alpha + \ ID))$

$$\xleftarrow{C_{ID} = (C_\alpha \cdot HEnc(hpk_{KGC}, ID))^r}$$

$\beta = HDec(hsk_{KGC}, C_{ID})$

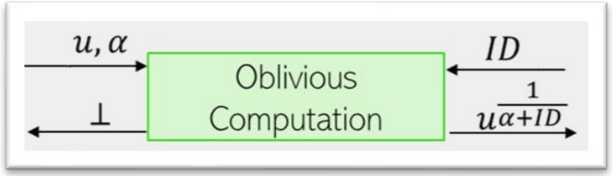
$\gamma = \beta^{-1} \bmod N$

$$\xrightarrow{g^\gamma}$$

Compute $(g^\gamma)^r = g^{\frac{r}{r(\alpha+ID)}} = g^{\frac{1}{(\alpha+ID)}}$

# Oblivious Computation: $sk_{ID} := u^{\frac{1}{\alpha+ID}}$

KGC



Bob

$$\boxed{h \leftarrow H_{p_1}, v \leftarrow \mathbb{Z}_N, u = h^v}$$

$$(hsk_{KGC}, hpk_{KGC}) \leftarrow HSetup(pp)$$

$$\xrightarrow{C_\alpha, hpk_{KGC}, \boxed{h}}$$

$$\boxed{(hsk_{Bob}, hpk_{Bob}) \leftarrow HSetup(pp)}$$

$$r \leftarrow \mathbb{Z}_N$$

$$\begin{aligned} C_{ID} &= (C_\alpha \cdot HEnc(hpk_{KGC}, ID))^r \\ &= HEnc\,(hpk_{KGC}, r(\alpha + ID)) \end{aligned}$$

$$\xleftarrow{C_{ID}, \boxed{C_r = HEnc(hpk_{Bob}, r), hpk_{Bob}}}$$

$$\beta = HDec(hsk_{KGC}, C_{ID})$$

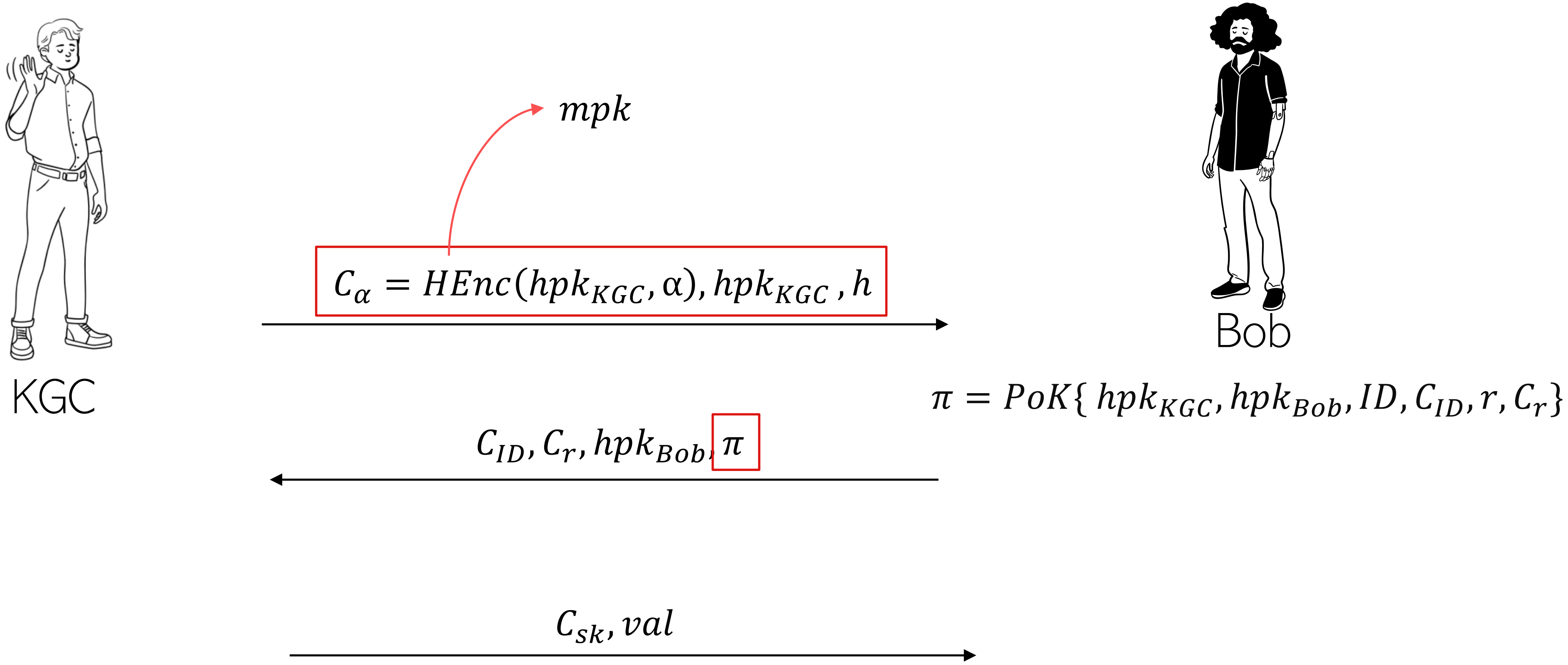
$$\gamma = \beta^{-1} \bmod N$$

$$\boxed{\begin{aligned} & t \leftarrow \mathbb{Z}_N, val = h^t \\ & C_{sk} = C_r^{v\gamma} \cdot HEnc(hpk_{Bob}, -t) \\ & = HEnc(hpk_{Bob}, \frac{v}{\alpha + ID} - t) \end{aligned}}$$

$$\xrightarrow{\boxed{C_{sk}, val}}$$

$$\boxed{\begin{aligned} & \sigma_{val} = HDec(hsk_{Bob}, C_{sk}) \\ & sk = h^{\sigma_{val}} \cdot val = h^{\frac{v}{\alpha+ID} - t} \cdot h^t \\ & = h^{\frac{v}{\alpha+ID}} = u^{\frac{1}{\alpha+ID}} \end{aligned}}$$

# Oblivious Computation



$mpk$

$\boxed{C_{\alpha} = HEnc(hpk_{KGC}, \alpha), hpk_{KGC}\,, h}$

KGC

Bob

$\pi = PoK\{\, hpk_{KGC}, hpk_{Bob}, ID, C_{ID}, r, C_r\}$

$C_{ID}, C_r, hpk_{Bob}, \boxed{\pi}$

$C_{sk}, val$

# Our Construction:

$Setup(1^{\lambda})$:

$h \leftarrow H_{p_1}, \nu \leftarrow \mathbb{Z}_N, u = h^{\nu}$

$(\alpha, u) \leftarrow \mathbb{Z}_N \times H_{p_1}$

$(hsk_{KGC}, hpk_{KGC}) \leftarrow HSetup(1^{\lambda})$

$C_{\alpha} = HEnc(hpk_{KGC}, \alpha)$

$msk \coloneqq (\alpha, u, \nu)$

$mpk \coloneqq (g_1, g_1^{\alpha}, e(g_1, u), \mathbf{H}, h, C_{\alpha}, hpk_{KGC})$

$Enc(mpk, ID, m)$:

$Pick\ s \leftarrow \mathbb{Z}_N$

$(ct_0, ct_1) \coloneqq (g_1^{(\alpha+ID)s}, m \oplus \mathbf{H}(e(g_1, u)^s))$

$Dec(sk_{ID}, ct)$:

$return\ \ ct_1 \oplus \mathbf{H}\big(e(ct_0, sk_{ID})\big) = m \oplus \mathbf{H}(e(g_1, u)^s) \oplus \mathbf{H}(e(g_1^{(\alpha+ID)s}, u^{\frac{1}{\alpha+ID}}))$

What we achieve:

- Oblivious computation of Extract()
- Security against KGC
- Ciphertext Anonymity
- Standard model

# Conclusion

- Vulnerabilities of some existing schemes
- New Definition for Oblivious Identity-based Encryption
- OIBE Construction in the Standard model without ICA

# Thank you!

# References

[Sha84]Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) Advances in Cryptology, Proceedings of CRYPTO '84.

[BF01]Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) Advances in Cryptology- CRYPTO 2001.

[AP03]Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C. (ed.) Advances in Cryptology, ASIACRYPT 2003.

[GHMR18]Garg, S., Hajiabadi, M., Mahmoody, M., Rahimi, A.: Registration-based encryption: Removing private-key generator from ibe. In: Beimel, A., Dziembowski, S. (eds.) Theory of Cryptography.

[GHMRS19]Garg, S., Hajiabadi, M., Mahmoody, M., Rahimi, A., Sekar, S.: Registration-based encryption from standard assumptions. In: Lin, D., Sako, K. (eds.) Public-Key Cryptography- PKC 2019.

[IP08]Izabach`ene, M., Pointcheval, D.: New anonymity notions for identity-based encryption. In: Ostrovsky, R., Prisco, R.D., Visconti, I. (eds.) Security and Cryptography for Networks, 6th International Conference, SCN 2008.

[ADM+07] Abdalla, M., Dent, A.W., Malone-Lee, J., Neven, G., Phan, D.H., Smart, N.P.: Identity-based traitor tracing. In: Okamoto, T., Wang, X. (eds.) PKC 2007.

# References

[Cho09]Chow, S.S.M.: Removing escrow from identity-based encryption. In: Jarecki, S., Tsudik, G. (eds.) Public Key Cryptography- PKC 2009.

[GH07]Green, M., Hohenberger, S.: Blind identity-based encryption and simulatable oblivious transfer. In: Kurosawa, K. (ed.) Advances in Cryptology– ASIACRYPT 2007.

[CKRS09]Camenisch, J., Kohlweiss, M., Rial, A., Sheedy, C.: Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data. In: Jarecki, S., Tsudik, G. (eds.) Public Key Cryptography– PKC 2009.

[Goy07]Goyal, V.: Reducing trust in the pkg in identity based cryptosystems. In: Menezes, A. (ed.) Advances in Cryptology- CRYPTO 2007.

[DY05]Dodis, Y., Yampolskiy, A.: A verifiable random function with short proofs and keys. In: Vaudenay, S. (ed.) Public Key Cryptography- PKC 2005.

[Wee15]Wee, H.: D´ ej` a Q: encore! un petit IBE. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography- 13th International Conference, TCC 2016.

[EKW19]Emura, K., Katsumata, S., Watanabe, Y.: Identity-based encryption with security against the KGC: A formal model and its instantiation from lattices. In: Sako, K., Schneider, S.A., Ryan, P.Y.A. (eds.) Computer Security- ESORICS 2019.

# References

[Wat05] Waters, B.: Efficient identity-based encryption without random oracles. In: Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. p. 114–127. EUROCRYPT'05.
[JL09] Jarecki, S., Liu, X.: Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection. In: Reingold, O. (ed.) Theory of Cryptography.
[BB11] Boneh, D., Boyen, X.: Efficient selective identity-based encryption without random oracles. J. Cryptol. 24(4), 659–693 (Oct 2011).
[LW10] Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: Proceedings of the 7th International Conference on Theory of Cryptography. p. 455–479. TCC'10.