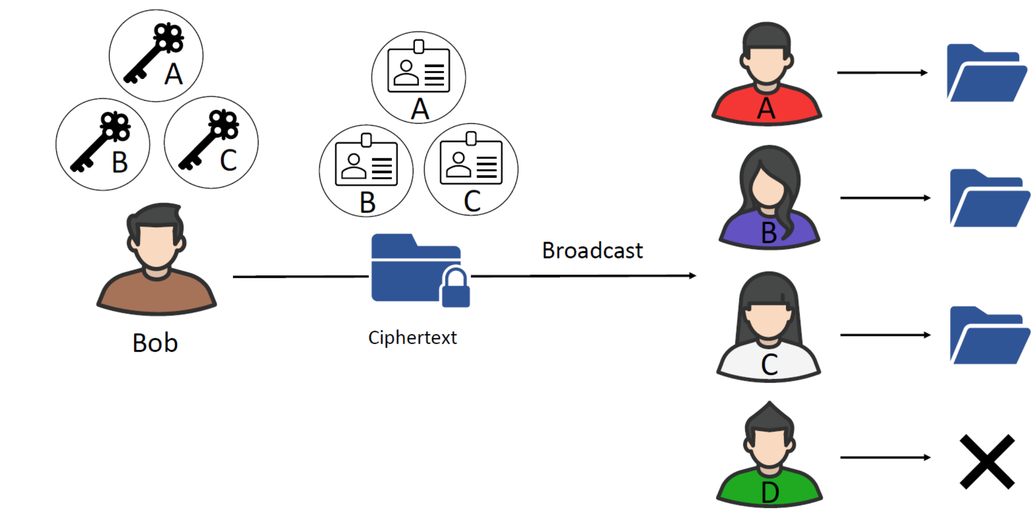
Lattice-Based Anonymous Multi-Receiver ID-Based Encryption

Zhen-Yu Jian (簡振宇)
Advisor: Chun-I Fan (范俊逸)
National Sun Yat-sen University

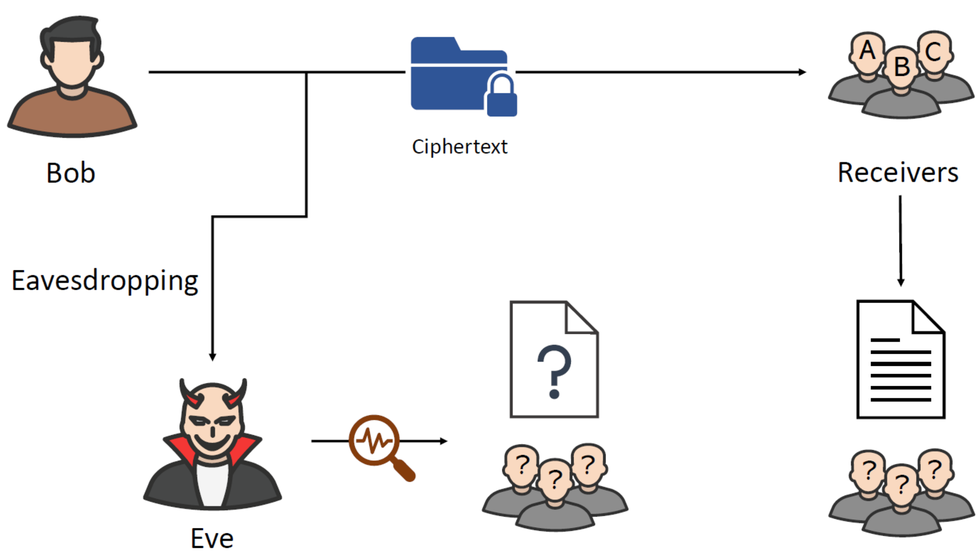
資訊安全實驗室 Information Security Laboratory 中山大學・資訊工程學系

Abstract

- ID-based encryption makes it possible for a user to set his public key to be his identity. Furthermore, ID-based encryption can reduce the cost of certificate management. Besides, in some scenarios, a multi-receiver encryption is required to encrypt a message for different receivers. Hence, there are many cryptosystems of multi-receiver ID-based encryption have been proposed.
- Some of them also provide anonymity to protect receivers' privacy. However, most of those cryptosystems are based on large prime factorization or discrete logarithms, which are insecure under quantum attacks. In order to solve the above problem, many researches are aiming at designing cryptosystems that can resist quantum attacks. Lattice-based cryptography is considered to be able to withstand quantum attacks. Therefore, this work presents a lattice-based anonymous multi-receiver ID-based encryption. Not only does the proposed scheme have shorter ciphertexts, but it protects receivers' identities against outside adversaries and inside receivers as well. Also, the proposed scheme is provably secure in both confidentiality and anonymity under the random oracle model.

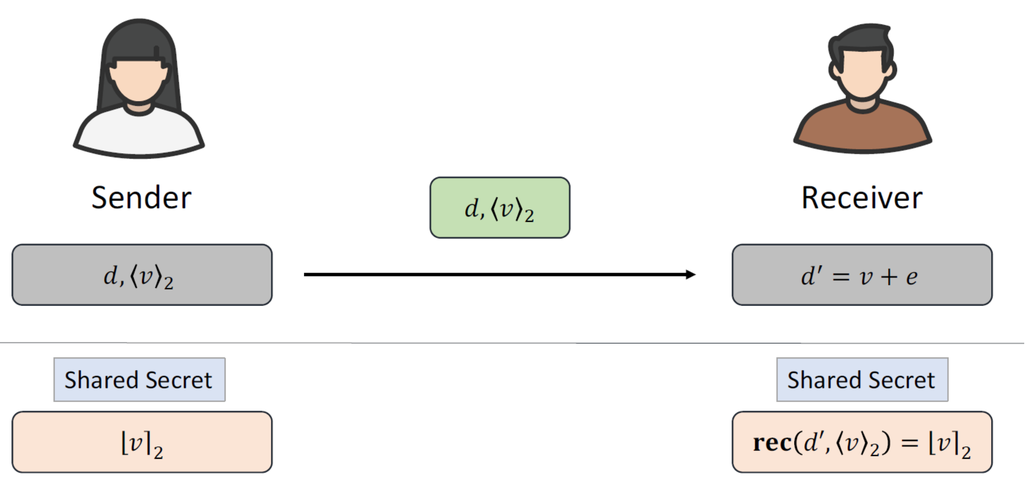


- An MRIBE Scenario



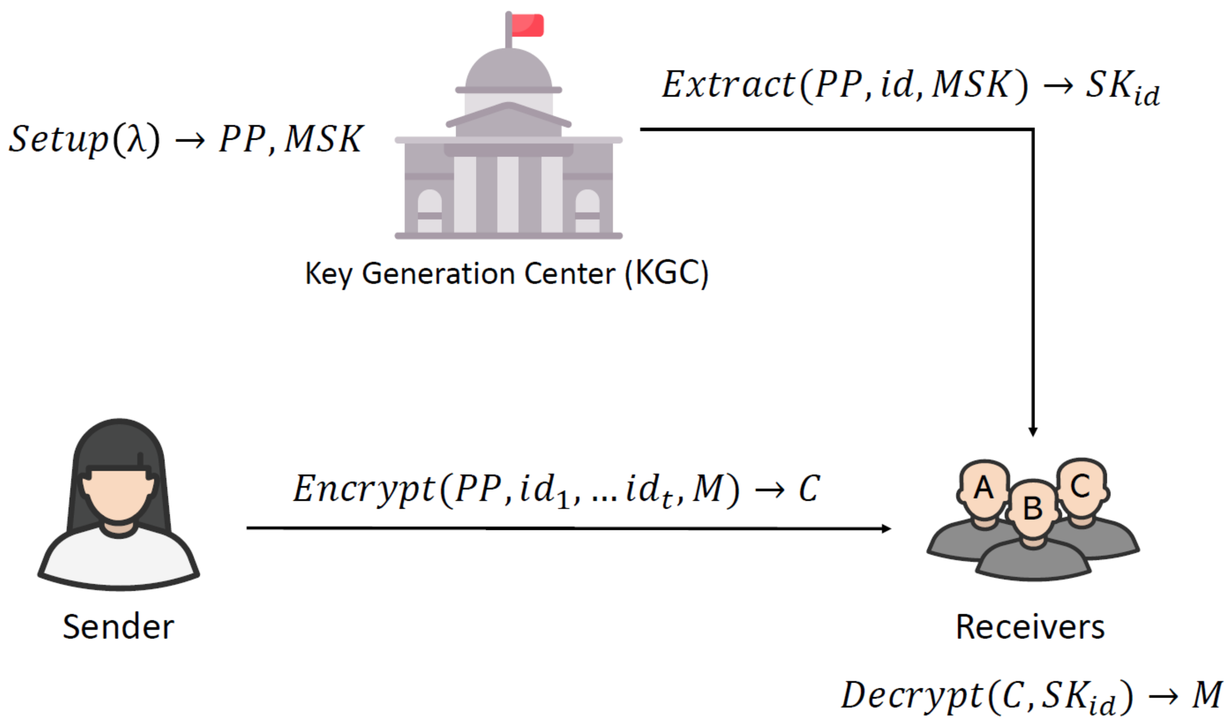
- An AMRIBE Scenario

Preliminaries



- The Flows of Reconciliation

Scheme



- The System Model

Comparison

	Description	Parameters
n	Security parameter	284
m	Basis dimension	$13,812$
q	Modulo	2^{24}
l	Message length	1024
h	Hash length	256

- Comparison Parameters

	Ciphertext length
Bert *et al.* [17]	$t * (\mathbb{Z}_{2^{24}}^{13812} + \mathbb{Z}_{2^{24}}^{\ell}) + \lvert\{0,1\}^h\rvert$ $\approx t * (3.31 \times 10^5 + \ell(24)) + h$ (bits)
The Proposed Scheme	$\mathbb{Z}_{2^{24}}^{6996+t*(6816)} + \mathbb{Z}_{2^{24}}^{\ell} + \lvert\{0,1\}^l\rvert + \lvert\{0,1\}^h\rvert$ $\approx 1.67 \times 10^5 + t * (1.63 \times 10^5) + \ell\,(25) + h$ (bits)

- Ciphertext Length

	$t = 20$	$t = 40$	$t = 60$
Bert *et al.* [17]	7.11×10^6 (bits)	1.42×10^7 (bits)	2.13×10^7 (bits)
The Proposed Scheme	3.45×10^6 (bits)	6.71×10^6 (bits)	9.97×10^6 (bits)

- Ciphertext Length for Multiple Receivers

Conclusion

- In this research, we have proposed a lattice-based anonymous multi-receiver IBE scheme. With our design, the proposed scheme has a shorter ciphertext. Moreover, by using the reconciliation function, the proposed scheme can achieve inside anonymity and guarantee the integrity of the message. We also proved that the proposed scheme is IND-sMID-CPA and Anon-sMID-CPA secure under the D-LWE assumption in the random oracle model. Furthermore, the comparison result shows that the ciphertext of the proposed scheme is significantly short.
- Although the proposed scheme has shorter ciphertext and provides receivers' anonymity, it needs a random oracle to complete the security proof. In the future, we will try to construct a lattice-based anonymous multi-receiver IBE scheme in the standard model. Another issue is to improve the performance since there is still a considerable gap between a lattice-based IBE and an IBE based on the discrete logarithm problem. These two issues will be studied in the future.