New Cryptographic Techniques for Data Security and Privacy Protection in the Cloud

Robert Deng
AXA Chair Professor of Cybersecurity
Director, Secure Mobile Centre
Deputy Dean, Faculty & Research
School of Information Sysems
Singapore Management University

SCyFI2018, 20 Sept 2018

Acknowledgement

This research is supported by the Singapore National Research Foundation under the NCR Award No. NRF2014NCR-NCR001-012

Era of Big Data

- Big data is everywhere, from sensors that monitor traffic conditions, noise levels to the flood of tweets and Facebook “likes”
- Over 2.5 quintillion bytes of data are created every day
- By 2020,1.7MB of data will be created every second for every person on earth

Sensor Networks

OSNs

Mobile devices

https://techstartups.com/2018/05/21/how-much-data-do-we-create-every-day-infographic/

Data Breaches Took Center Stage

- **World's Biggest Data Breaches**
  - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- **Sept 2017 Equifax**: 143 million customers' data stolen including names, SS#s, credit card details → s/w security flaw in "Apache Struts"
- **Nov 2017 Uber**: 57 million Uber driver and customer details stolen in an AWS account hijack. Phishing attack on login credentials
- **Aug-Sept 2018 British Airways**: 380,000 transactions affected, including card numbers, expiration dates and CVC codes. BA blamed a "sophisticated" group of cybercriminals but didn't give any more details.

Recent Cyber Attacks in Singapore

- Attacks on NUS and NTU research servers in May 2017 (Straits Times, 13 May 2017)
  - Aimed at stealing government and research data
  - The breaches were said to be advanced persistent threats (APTs)
- Iranian hackers breach Singapore universities to access research data (Straits Times, 3 April 2018)
  - 52 staff accounts at four Singapore universities breached by Iranian hackers
- "Singapore's worst cyber attack in its history, in which personal information of about 1.5 million people including the Prime Minister was stolen, has the hallmarks of a state-linked group, the communications minister said on Monday" (Reuters, 6 Aug 2018)

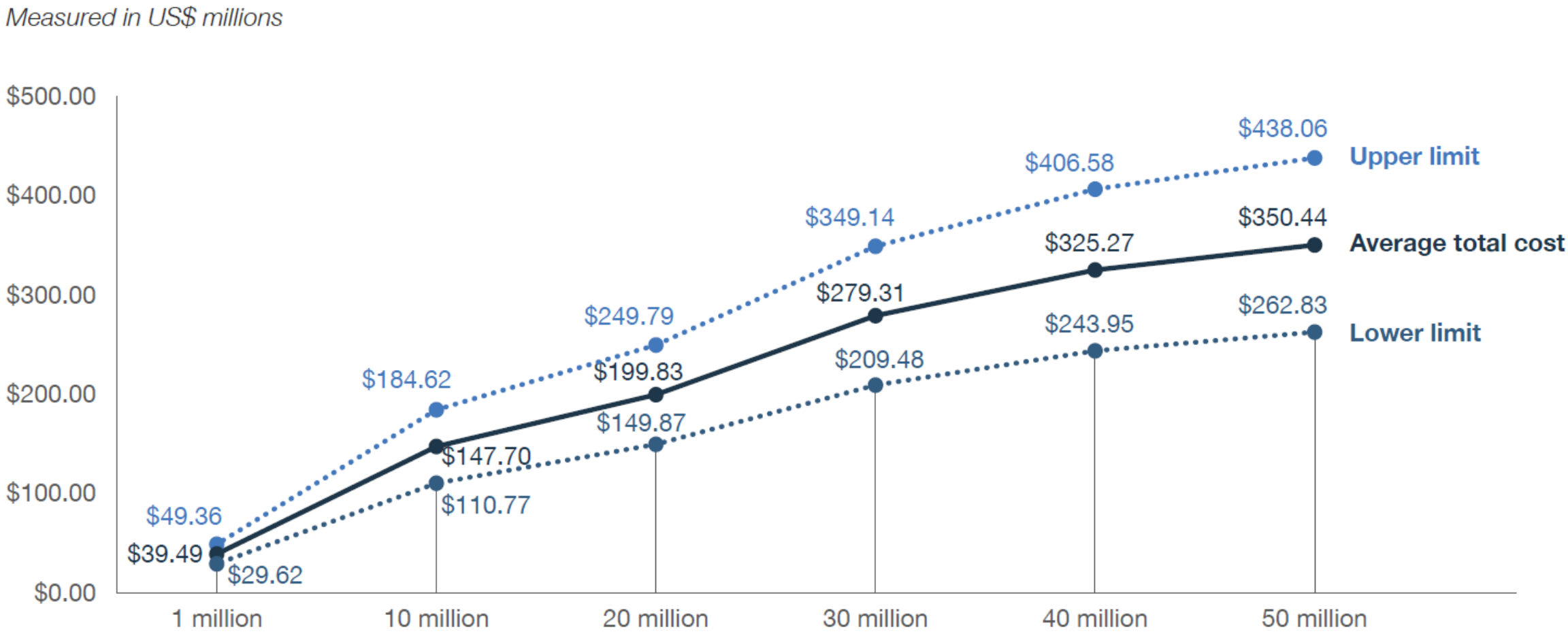
Cost of Data Breach

- Average total cost of a data breach: US$3.86m, including costs for
  - Detection & escalation
  - Notification
  - Post data breach response
  - Lost business

- Average cost per lost or stolen record: US$148

(Source: Ponemon Institute LLC, July 2018)

Cost of Mega Data Breaches

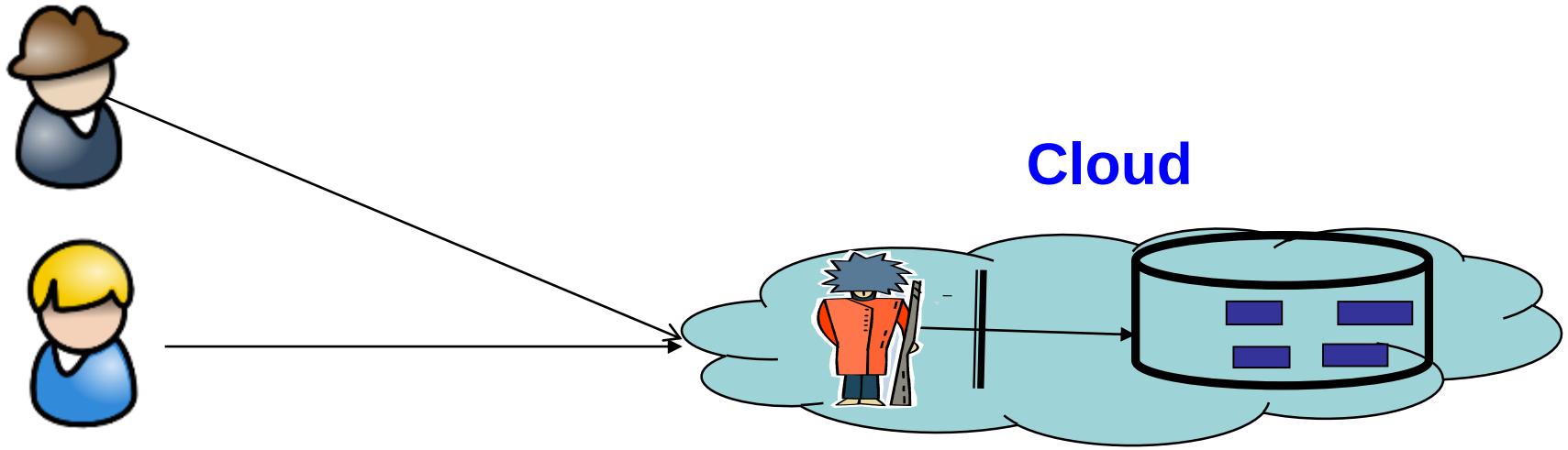


- At 95% level of confidence

(Source: Ponemon Institute LLC, July 2018)

Why So Many Data Breaches?

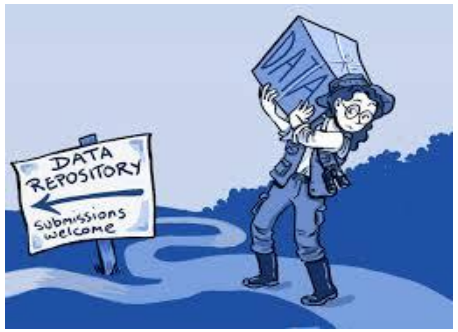
Security Model in Traditional Systems



Is the Security Model Valid?

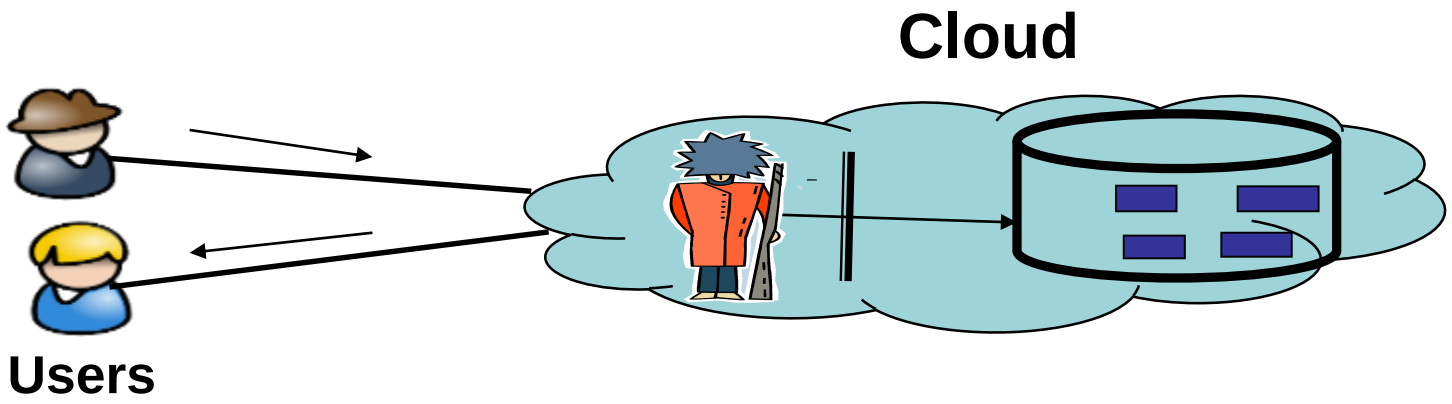
- **Human is the weakest link**: phishing attacks, password reset

- **Tim Cook**
  - "When an online service is free, you're not the customer. You're the product"



- **Bob Lord (Yahoo's chief information security officer)**
  - Said that his company still had 'not been able to identify" how one billion Yaoo accounts and their sensitive user information were hacked in 2013." –The NY Times 12 Jan 2017

Our Security Model for Cloud Data Storage System



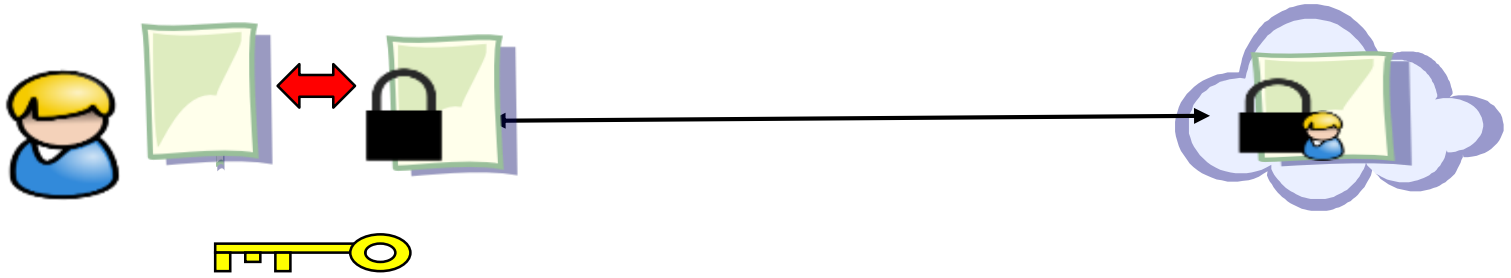
- Not security savvy

Honest but curious

- Not trusted to keep data confidential
- Not trusted to enforce access control correctly

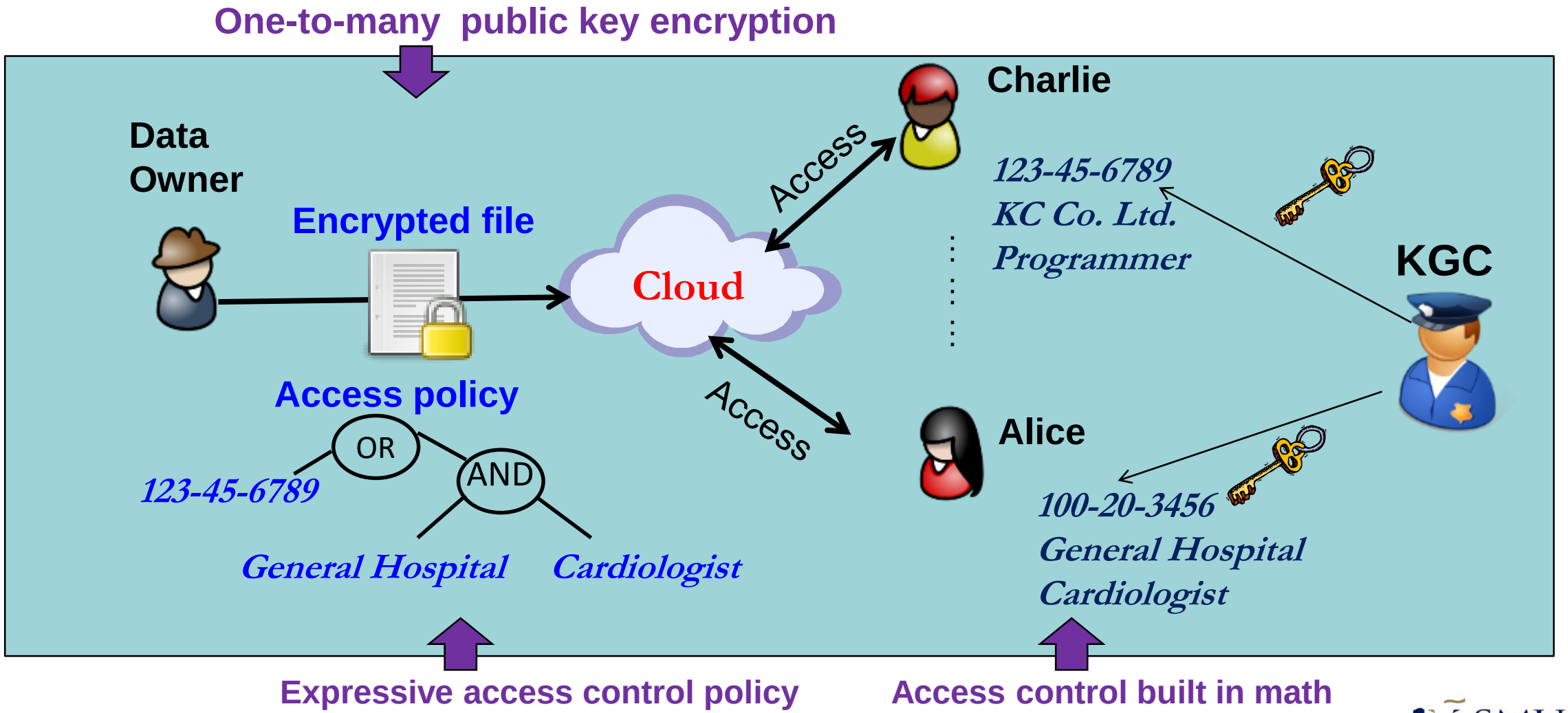
What Can We Do to Protect Data When Service Providers Are not Trusted?

- Use encryption
  - Cloud only sees data in encrypted form; plaintext never leaves user's computer
  - Good practice even for "trusted" servers → The principle of defense in depth



- **But how to efficiently share encrypted data with others?**

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)



Our Research Contributions

- Verifiable outsourced decryption of ABE [TIFS 2013, TIFS 2015]
- CP-ABE with partial hidden access policy [AsiaCCS'12, ProvSec'16]
- Deduplication on encrypted data [TBD 2016], Best Paper Award
- Efficient user and attribute revocation [EOSRICS'15 & '16, SecureComm'17]
- Attribute-based secure messaging system in the cloud [SG-CRC'17]
- ABE-based secure storage over OneDrive

Security Strength

CP-ABE is implemented on various elliptic curves: type A curve(symmetric curve), type D curve (MNT curve), and type F curve (BN curve). Every curve has different initialization parameters, hence different security strength, as shown below

Curves	Elliptic curve key size (bits)	Security strength (bits)
a512	512	80
d159	159	<80
d201	201	[80, 112]
d359	359	[112, 128]
f160	160	[80, 112]
f256	256	128
f512	512	[128, 192]

CP-ABE Encryption Performance on PC

Platform: Ubuntu 16.04, Intel Core i7-7820HK 2.6 GHz, 8 GB RAM
Policy: n attributes combined with “&”

Policy length	Type a512	Type d159	Type d201	Type d359	Type f160	Type f256	Type f512
1	5.96	4.03	6.83	21.02	5.11	10.73	51.79
2	7.25	6.49	9.29	34.65	6.07	12.8	60.8
3	10.63	8.81	13.00	47.65	6.79	15.17	72.15
4	12.91	11.34	17.04	61.83	7.78	17.64	92.43
5	15.33	13.77	22.23	77.04	8.82	22.08	98.94
10	29.19	25.64	40.29	146.77	13.43	34.04	167.91
20	57.53	50.98	78.19	291.05	22.39	57.02	276.13

CP-ABE Decryption Performance on PC

Platform: Ubuntu 16.04, Intel Core i7-7820HK 2.6 GHz, 8 GB RAM
Policy: n attributes combined with “&”

Policy length	Type a512	Type d159	Type d201	Type d359	Type f160	Type f256	Type f512
1	0.88	5.15	7.2	20.81	18.61	33.73	127.38
2	0.8	5.17	7.07	20.74	18.8	34.29	123.02
3	0.79	5.04	7.65	20.84	18.28	34.13	127.3
4	0.74	4.99	7.73	20.32	18.3	35.12	129.5
5	0.82	5	7.6	20.43	18.4	37.12	127.4
10	0.71	5.08	7.23	21.48	18.16	37.17	128.71
20	0.85	4.97	7.63	20.41	18.57	34.65	127.37

CP-ABE Performance on Mobile

Platform: Android 7.0, Snapdragon 821 2.15 GHz Quad Core, 4 GB RAM
Policy: n attributes combined with “&”

Policy length	Type a512		Type d159		Type d359		Type f160		Type f256	
	encrypt	decrypt	encrypt	decrypt	encrypt	decrypt	encrypt	decrypt	encrypt	decrypt
1	267.23	172.02	723.35	232.1	1813.41	405.11	8278.42	841.22	12373.73	2744.1
2	478.9	154.36	1025.82	256.18	3272.59	397.24	8108.97	794.56	13486.29	2356.35
3	636.23	168.8	1812.98	223.45	4253.87	410.23	9134.41	823.91	13729.13	2854.97
4	968.63	157.42	2378.5	241.15	4918.9	375.5	9318.3	837.2	14580.12	2188.14
5	1268.8	169.4	2801.67	199	6210.4	378.4	10018.4	892.42	14271.12	2249.5

Summary

- Data breaches take center stage
- Our new cryptographic techniques allow an organization to
  - Provide end-to-end data security and privacy protection in the cloud
  - Support secure and scalable data sharing
  - Support efficient user revocation
- Future research: privacy-preserving data analytics in the cloud

Thank You!

robertdeng@smu.edu.sg