



# 基于全同态加密的医疗数据隐私保密系统

# 目录/Contents



**01**

应用背景

**02**

方案设计

**03**

性能分析

**04**

总结展望



# 应用背景

2010年360搜集百万用户账号  
2011年天涯、CSDN用户账号泄露  
2015年互联网金融平台铜掌柜60万用户隐私泄露  
2015年美医疗保险公司CareFirst被黑 110万用户信息泄露  
2015年全球最大婚外情网站Ashley Madison被黑

这样，你还敢把隐私赤裸裸地放在数据库里吗？

[illegible]

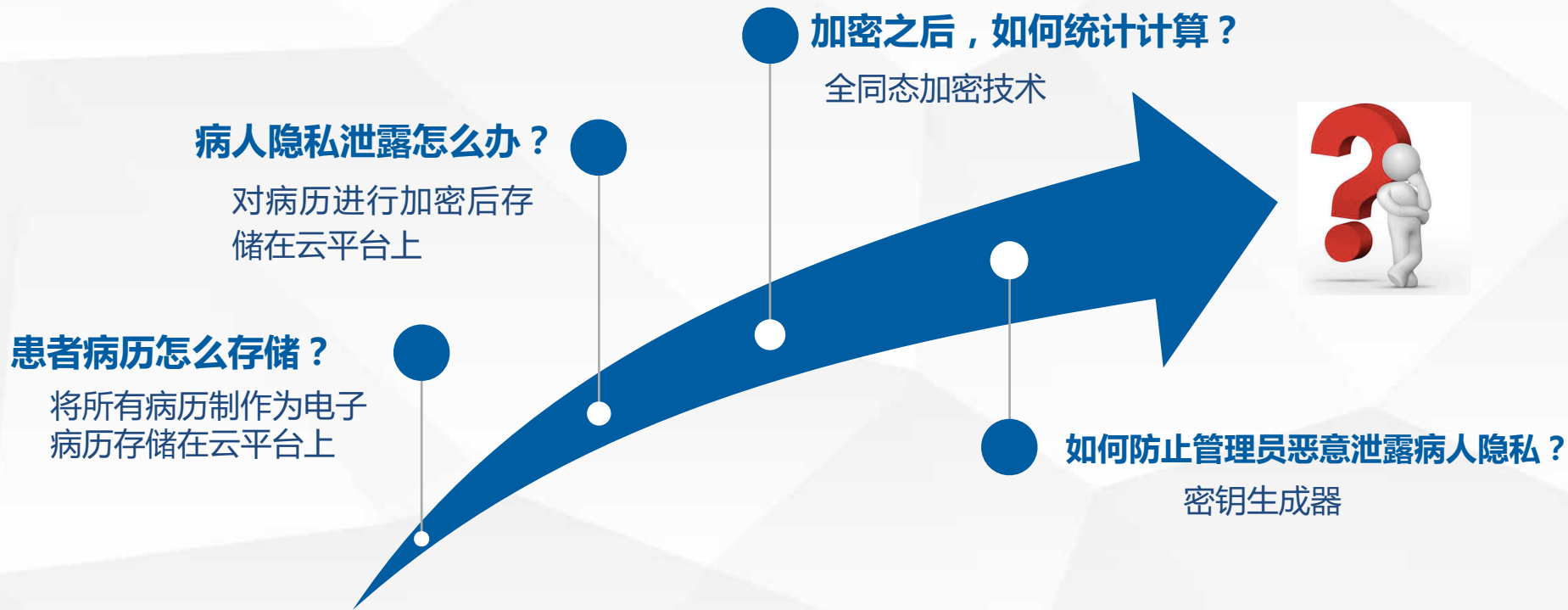
姓名	地址	邮箱	酒店信息	入住日期	退房日期	税费总计
25 DON CUN LAI WITTEL SAUNG 4922124 NO 301 2-27-4 素 49-Qu 3FAK 279 FAP FARNK G04741-1 PO BOX 角拉玛路 581554		PITL afica santa	合顺汇都酒店 北京德胜门中学对面酒店 Osaka 1-66 Ofaka-Chu	2015年2月10日 2015年2月10日 2015年4月10日	2015年2月11日 2015年2月12日 2015年4月13日	558.00 CNY 500.00 CNY 184,998 JPY
ASPOR1 BEUNG 10962 8615351544516 AV SAN LORENZO NO 124 CUATLANZINGO PUEB, MEX 000000 222244000		gao2 Glover 56424	San Jose Silicon Valley Ardmore 1 35 2207 North Rockwood Road Ardmore, 使用的阿玛路 南康市酒店酒店 香港新界沙田香港酒店 Phuket 5/2 Thawornwong Rd Patong Beach Phuket	2015年3月2日 2015年3月2日 2015年3月13日 2015年3月12日 2015年2月11日 2015年2月11日 2015年2月10日	2015年3月12日 2015年3月12日 2015年3月15日 2015年3月15日 2015年2月13日 2015年2月13日 2015年2月10日	1,008.24 USD 1,560.63 CNY 2,675.30 HKD 80,850.00 THB 1,000.00 CNY

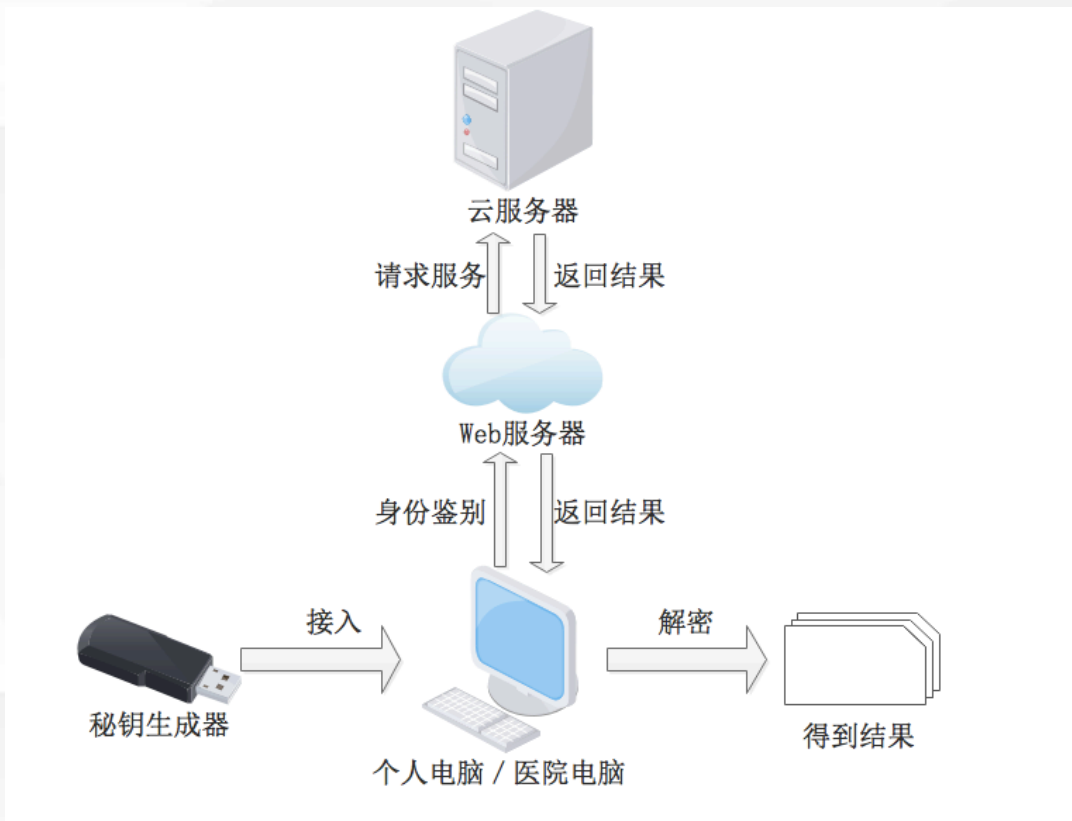
姓名	身份证号	手机号	出生日期	家庭住址	婚姻状况	是否入籍	通缉时间
2018.09.10	1730911107	1595521	1984.09.10	2000	8421	2008/09/10	2008/12/13 24
1917	1730906106	151521	1986	20200000	8421	2008/12/15	2008/12/15 04
2018.09.10	1730911107	1595521	1984.09.10	2000	8421	2008/09/10	2008/12/13 24
6218	0	0	2000000000	0	8218	2008/12/15	2008/12/15 04
7108	0	0	2000000000	0	8421	2008/12/15	2008/12/15 04
7181	0	0	19810101	1986.12.15	8421	2008/12/15	2008/12/15 04
40870101	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870102	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870103	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870104	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870105	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870106	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870107	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870108	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870109	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870110	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870111	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870112	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870113	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870114	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870115	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870116	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870117	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870118	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870119	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04
40870120	0	0	1986.12.15	1986.12.15	8421	2008/12/15	2008/12/15 04



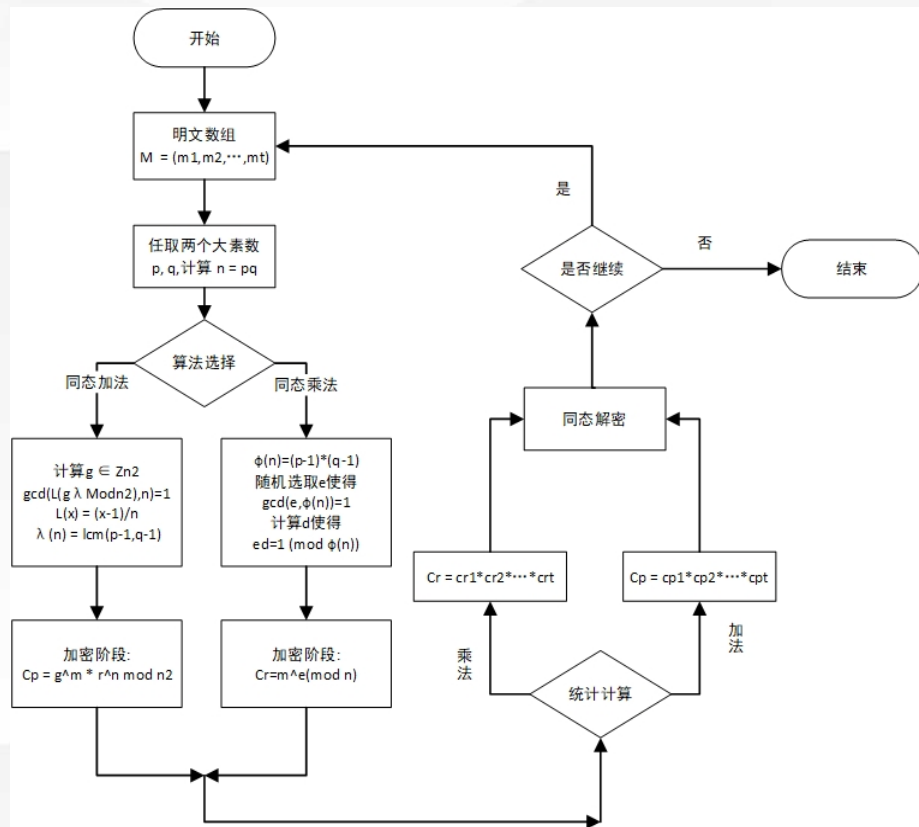


# 方案设计





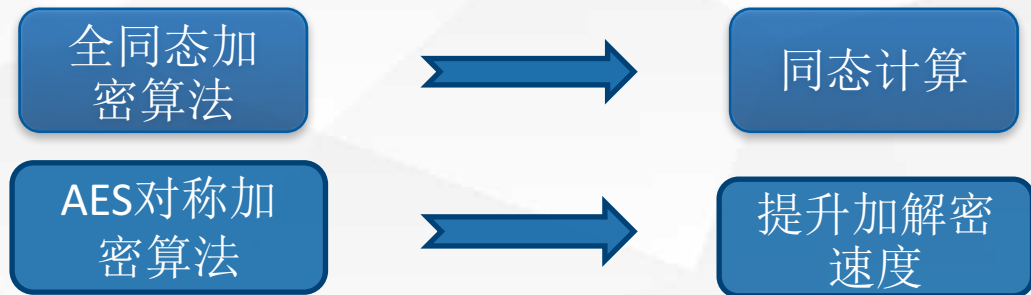


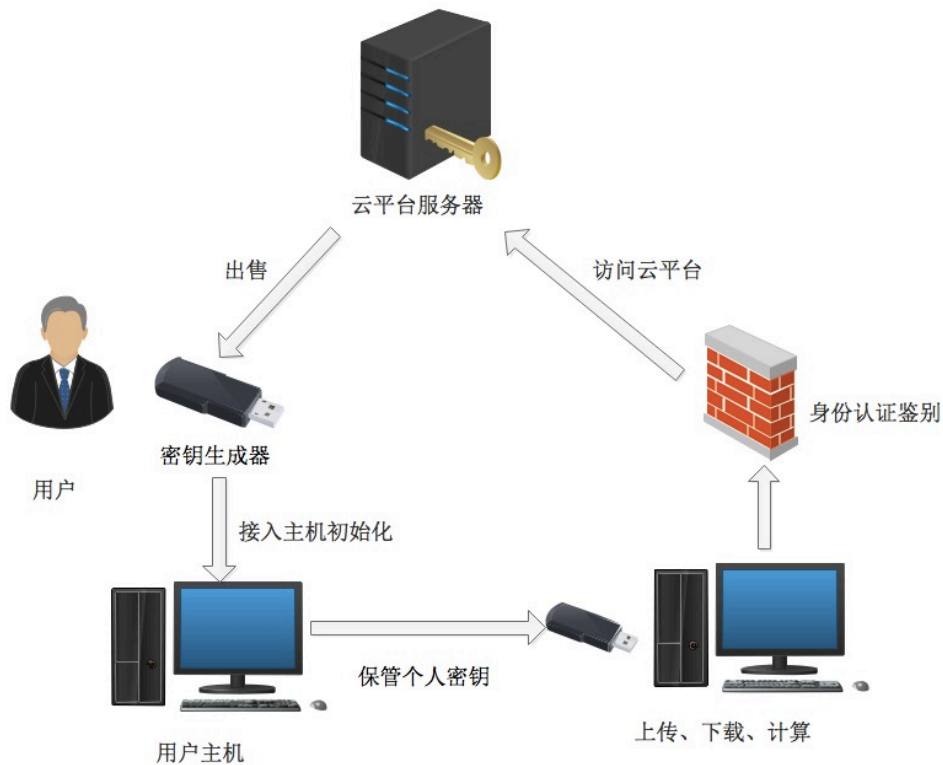


加密后限制了  
云计算的能力

全同态加密算法  
 $e = E(m)$   
 $F(e) = E(f(m))$

保留云平台计  
算能力





产生唯一的  
身份鉴别码

自动完成加  
解密操作

云平台不保留用户的  
任何密钥



# 性能分析

## 系统安全性分析





### 全同态加密技术

加密时间极短  
解密效率低

大小1G的文件：  
加密需1分钟  
解密需65小时



**用于加密需要计算的少量信息**



## 性能改进

### AES对称加密技术

加密时间与加密文件的  
大小呈正相关  
解密时间是加密时间的  
两倍

大小1G的文件：  
加密需4分钟  
解密需8分钟



**用于加密完整病历**



序号	原文件大小 (KB)	加密后文件大小 (KB)	加密用时 (秒)	解密用时 (秒)
1	6	6	0	1
2	12	12	0	3
3	24	24	0	5
4	45	45	0	10
5	90	90	1	21
6	180	180	2	40

RSA的测试数据

序号	原文件大小 (MB)	加密后文件大小 (MB)	加密用时 (秒)	解密用时 (秒)
1	1.639	3.335	0	0
2	3.278	6.669	0	1
3	6.556	13.338	1	2
4	13.111	26.676	3	5
5	26.226	53.351	6	11
6	52.441	106.701	12	23

AES的测试数据



# 总结展望



基于全同态加密的医疗数据隐私保密系统

全同态加密技术

密文摘要检索

密钥生成器

保护用户隐私  
保留云平台计算能力

密钥管理简单  
加解密效率高

可扩展性强



谢谢观看

