北京大学
PEKING UNIVERSITY

Electronic Voting

2018级信息安全工程小组报告

小组成员：胡志伟、卿山、郁星遥、李国才

北京大学

第一部分

E2E电子投票系统

- 引入
- 系统模块
- 选举过程

E2E电子投票系统

- **一个电子投票系统什么是重要的？**

  端到端(E2E)的可验证性。

- **目前的电子投票系统存在什么问题？**

  目前，已有的支持E2E验证的电子投票系统需要满足很多特定的假设条件。例如：一个可以被公众信任的第三方提供可靠的公共引用字符串。由于选举当局不能明确的说服选民这些假设是正确的，所以选举结果总是有争议的。

- **本文提出的E2E电子投票系统有哪些优点？**

  1. 只需要一个假设条件：一个能够提供关于选举一致性观点的布告栏。验证选举所需的随机性可以通过选民与系统的交互产生的熵收集。这种相对环境内部的熵，不需要信任随机的外部来源或在RO模型下限制对手。

  2.系统对投票人的计算能力做了绝对最小的假设:投票人一方在投票过程中没有加密操作。

E2E电子投票系统

系统模块

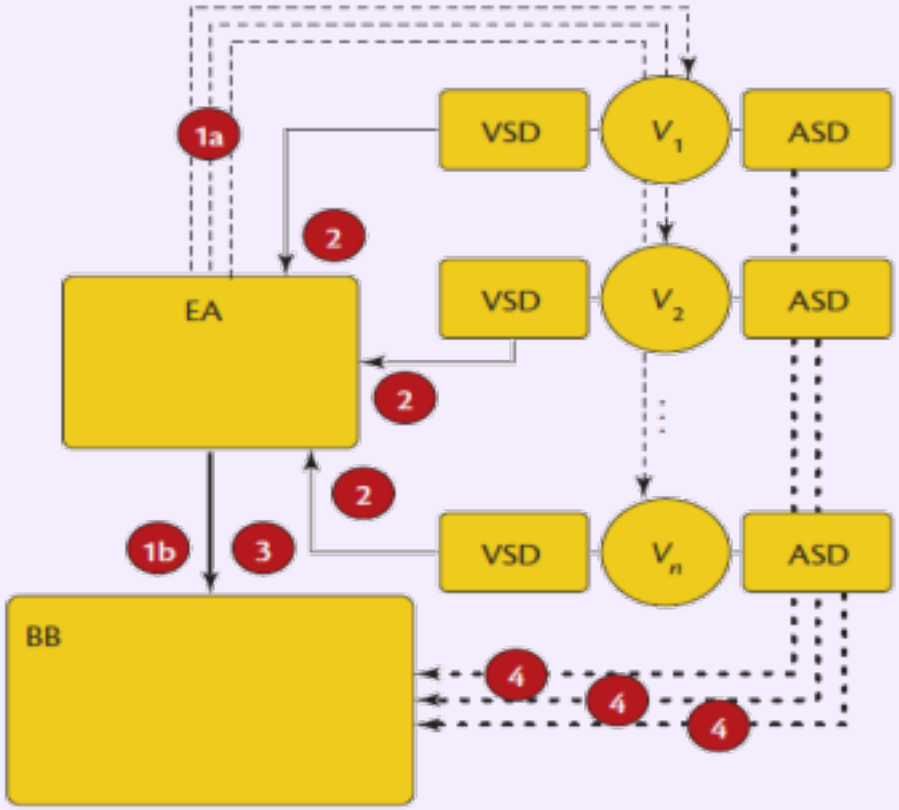
V:选民

VSD：支持投票的设备

ASD：支持验证的设备

EA：投票机构

BB：布告栏



E2E电子投票系统

投票过程

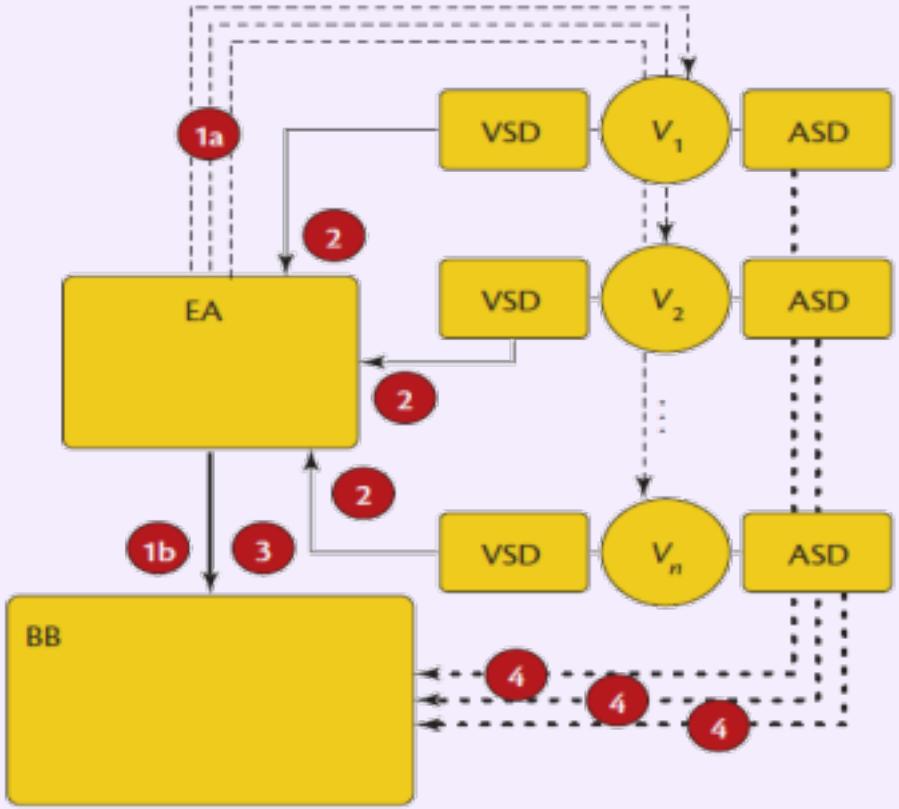
1a：选举机构（EA）对选民分配选票。（电子信封）

1b：EA生成一个承诺键ck，并将ck与其他公共选举信息（如选举问题）一起发布到公告栏（BB）。

2：投票者将身份验证代码输入支持投票的设备（VSD），在身份验证之后，使用VSD将选举信息和投票代码a -2发送到EA。

3：系统在公告栏中公布选举后的数据。

4：投票人通过支持审计的设备对投票数据进行审计。



E2E电子投票系统

选票设计

在选举之前,选民会通过一个安全的渠道收到一个投票卡，如图2所示，。每张卡片都有一个序列号(SN)和两个一样具有投票功能的部分，a面和b面。每个面都包含一个不可预测的身份验证码，并列出候选人及其相应的投票码。选民可以选提交任意一个部分进行投票，并将另外一部分留存以在选举结束后进行验证。

E2E电子投票系统

布告栏

SN：序列号

Side：对应选票的两面

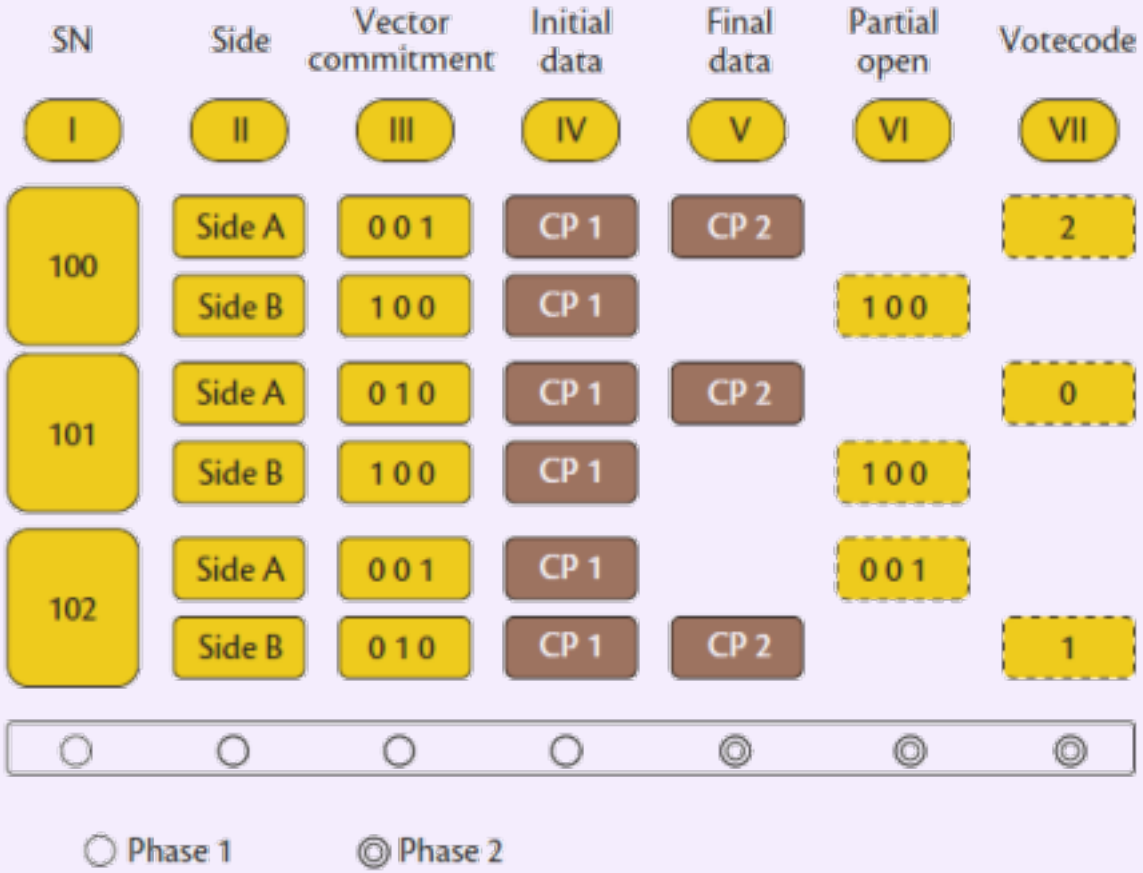
vector commitment：投票向量

initial data:用于证明投票的有效性

Final data:用于证明投票的有效性

Partial open:部分开放码

Votercode:选民提交的投票代码



北京大学

第二部分

检测能够被检测到的：密码选举的意外结果

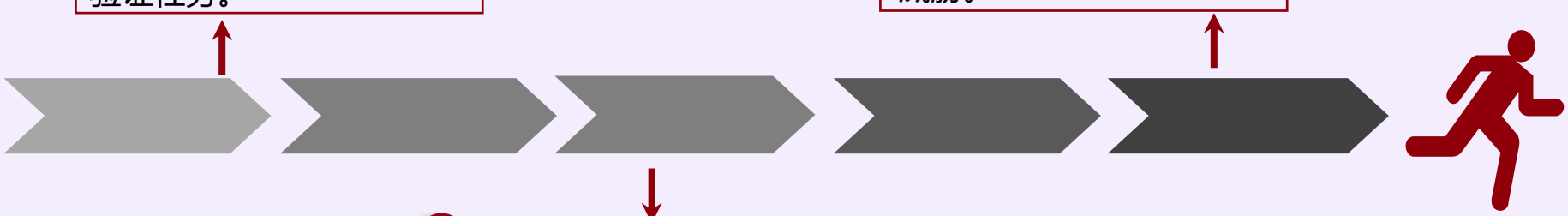
- 密码选举验证领域面临的挑战
- 密码选举中的意外结果原因
- 扰乱选举与虚假的“证明”

已知挑战

1. 可用性：在设计系统时必须要实现最主要的两个功能：标记并投票。另外还应该能够创建隐私保护收据并执行验证任务。

2. 可理解性：由于验证大量使用加密，普通选民对于器技术方面的理解仍然是不小的挑战。

3. 远程投票：强大的可验证性的存在客户端恶意软件，网络钓鱼，拒绝服务攻击，实时强迫和投票买进或卖出等威胁。



意外结果

意外结果的原因

- 风险补偿：是一种认知偏差，每个人根据自己对风险的感知程度的不同来引导行为上的变化。在大选验证方面，风险补偿理论认为由于E2E的引进，选举结果审核员过于依赖系统从而对于审核工作变的疏忽和大意。
- 自动化偏差：指审核员在进行结果的审核时，过于看重自动化系统提供的辅助信息。这种错误分为两类，第一类是由于系统未检测到的错误而发生的遗漏错误。另一种是审核员过于信赖系统的推荐信息，即使和自己的经验或常识相矛盾。

干扰破坏选举

虚假的证明

- 争论收据：这种攻击的一个途径是选民虚假声称他们的隐私保护收据中包含的信息未正确反映在加密校验证明中。可采用独立第三方机制来解决争端，不需要选民放弃选票。

- 中毒选票攻击：恶意选民利用证明软件中的漏洞来投射格式错误的选票，并使证明看起来可以相信，目的是破坏计算的次数。

北京大学

第三部分

可用性VS安全性

- 实验过程
- 实验结果

可用性VS安全性

- 可用性和安全性是相互对抗的，在确保电子投票系统的安全性的同时，可用性也会有所下降。所以系统设计者需要权衡这两个方面。

那么选民愿意为了安全性牺牲多少可用性？

- 研究人员做了一次调研
  （1）实验场景：多特蒙德工业大学的学校选举
  （2）使用安全性不同的三个电子投票模拟系统
  （3）调查对象：23名多特蒙德工业大学的学生、老师志愿者
  （4）实验主要过程：每个志愿者在经过培训后，分别体验这3个投票系统，并填写调查问卷。

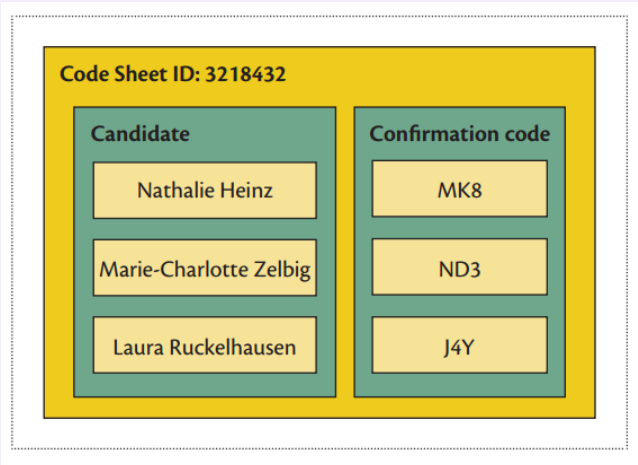
可用性VS安全性

- **电子投票系统的两个安全属性：投票过程保密性和投票结果的真实性**
- **三个电子投票系统：**

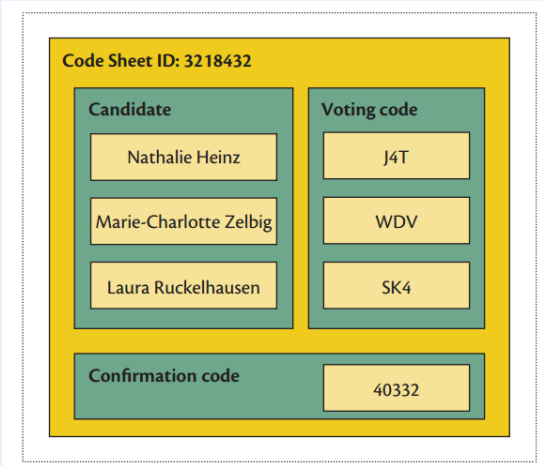
系统A：选择——>提交——>投票成功

系统B：收到”代码单“——>选择——>提交——>对比候选人”确认码“，投票成功

系统C：收到”代码单“——>输入候选人”投票码“——>提交——>对比”代码单确认码“，投票成功



系统B的“代码单”



系统C的“代码单”

可用性VS安全性

- **对比三个电子投票系统**

	保密性	真实性	安全性	可用性
系统A	无法保证	无法保证	低	高
系统B	无法保证	可以保障	中等	中等
系统C	可以保障	可以保障	高	低

- **调研结果：**

  根据调查问卷进行数学分析，研究选民如何权衡电子投票系统的可用性和安全性。通过计算安全性和可用性的相关系数，得出结论，根据分析得出的模型，选民愿意牺牲平均26分的可用性(范围从0到100)，以获得更高的安全性。

- 虽然实验存在局限性，选取的实验对象都是学校师生，不具有代表性。但这些研究结果还是能给我们一个参考，在设计电子投票系统时应该如何权衡安全性和可用性。

北京大学

第四部分

长期的投票隐私威胁

- 引入介绍
- 系统具体设计
- 存在问题

长期的投票隐私威胁

引入介绍

- 当前很多的电子投票系统都是不透明的。投票者除了信任投票系统的硬件和软件以及操作投票系统的人之外别无选择，一个更加透明的投票系统是被高度期待的。

- 为了提高透明性，许多新的投票系统提供了审计数据，这些数据可以让投票者去验证他们的选票被正确的计入了投票系统，同时让外部人员在验证投票数的计算是正确的。然而在这些系统中加密技术的使用只能够提供几十年的安全性。这威胁到了在长时间内投票者的隐私。

- 下面将从这几个方面介绍：

  1.一个现场和远程投票系统的具体设计。

  2.为什么说面临着长时间的威胁。

  3.一些其他方面的思考。

长期的投票隐私威胁

系统具体设计

1.投票者在浏览器里面输入他的选择，为了简化，假设选择有两个选项，分别为0和1。

2.浏览器加密投票：e=E(v,r)，v:投票者的选票，是可显示的；e:相同的选票但是使用了二维码加密的形式。r是一个额外的机器生成的随机字符串。

3.投票者选择审查或投入选票。

4.如果投票者选择审查选票，浏览器展示加密用的值r，三元组（v,e,r）之后被用于输入一个独立的验证程序，程序计算出e1，验证e1是否等于e，如果通过，投票者返回步骤一从新获得一张选票。如果测试失败，代表产生了一个错误的选票，同时便会开始调查。

5.如果投票者选择投入选票，他会首先通过服务器的验证。如果验证成功，服务器获取到一个加密的选票同时发送一个验证邮件，邮件里面包括e。

6.选举结束后，当局公布一个表展示收到的电子选票—等价于选票箱。使用同态计数

$Enc(m1) \bullet Enc(m2) = Enc(m1 + m2)$

当局可以计算选票结果并证明其正确性。

Table 2. Published results of Internet voting pairs.

Voter name	Encrypted ballot
Alice	$e_1 = E(v_1, r_1)$
Bob	$e_2 = E(v_2, r_2)$
…	…
Zeno	$e_n = E(v_n, r_n)$
	$e_T = \prod E(v_i, r_i)$

实现了隐私，正确性以及个人和普遍的可验证性。资格可验证性，因为选民的名字出现在选举网页上。

长期的投票隐私威胁

存在问题

- 当前的储存成本比较低，这些选票可能会永远出现在网络上，如果有一天加密算法被攻破了，这可能会解密所有的公开信息。并且这可能会伤害到一些人，如独裁者掌权之后会报复之前给他们投反对票的人。所以说投票隐私伴随着一些有效期未知的数据，因为不知道什么时候加密算法会被攻破，所以存在着一些选票会在一段时间后被公开的可能性，这可能会影响投票者。

- 多方计算（MPC）是一个蓬勃发展的密码学子领域。它处理以下问题：n方想要计算y = f（x1，...，xn），但是协议不应该透露任何关于另一方输入的信息，超出可以从一方自己的输入推断的信息，xi给定函数f，输出y。加密协议的长期隐私隐患经常被忽视。计算安全性提供了几十年的机密性，在许多情况下这是不够的。投票是一个有力的例子，但基因组数据的多方计算也是如此，其中隐私泄露产生巨大影响。作者呼吁加密组织更加关注这一点。

总结与思考

选举结果的**可审计性**和**可验证性**是投票系统最重要的安全要求。

- 一个投票系统不仅要得出正确的选举结果，还要使公众能够信服这个结果。投票系统必须软件独立(software-independent)，以纸质投票为基础，有健全的流程来保证审计的真实性。

- 确保电子选举系统的可验证性不仅仅是一个技术问题，更有政治和法律方面的因素。

- 未来，采用纸质投票与电子系统结合的投票系统，最终可能比纯纸质投票系统更值得信赖。但在互联网上以可靠和匿名的方式投票仍然需要更多的研究。

北京大学
PEKING UNIVERSITY

Thanks for listening !