Revisiting Practical and Usable Coercion-Resistant Remote E-Voting

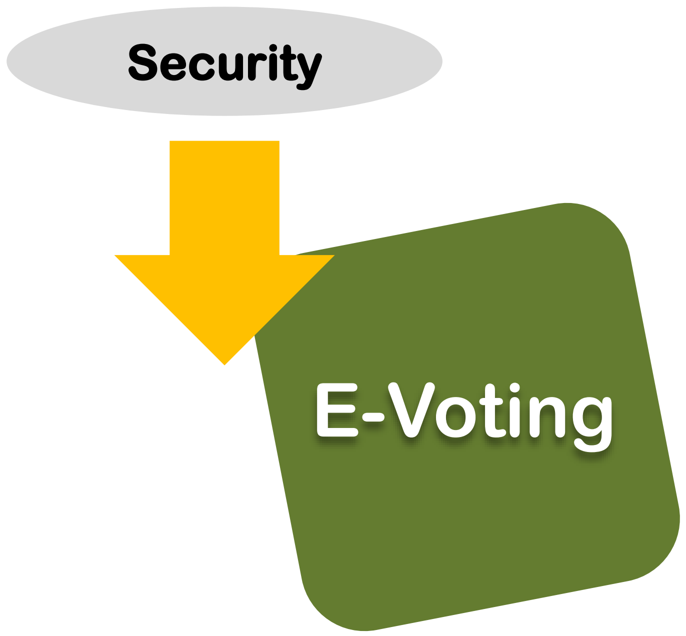
Ehsan Estaji, Thomas Haines, Kristian Gjøsteen
Peter Roenne, Peter Y.A. Ryan, Najmeh Soroush

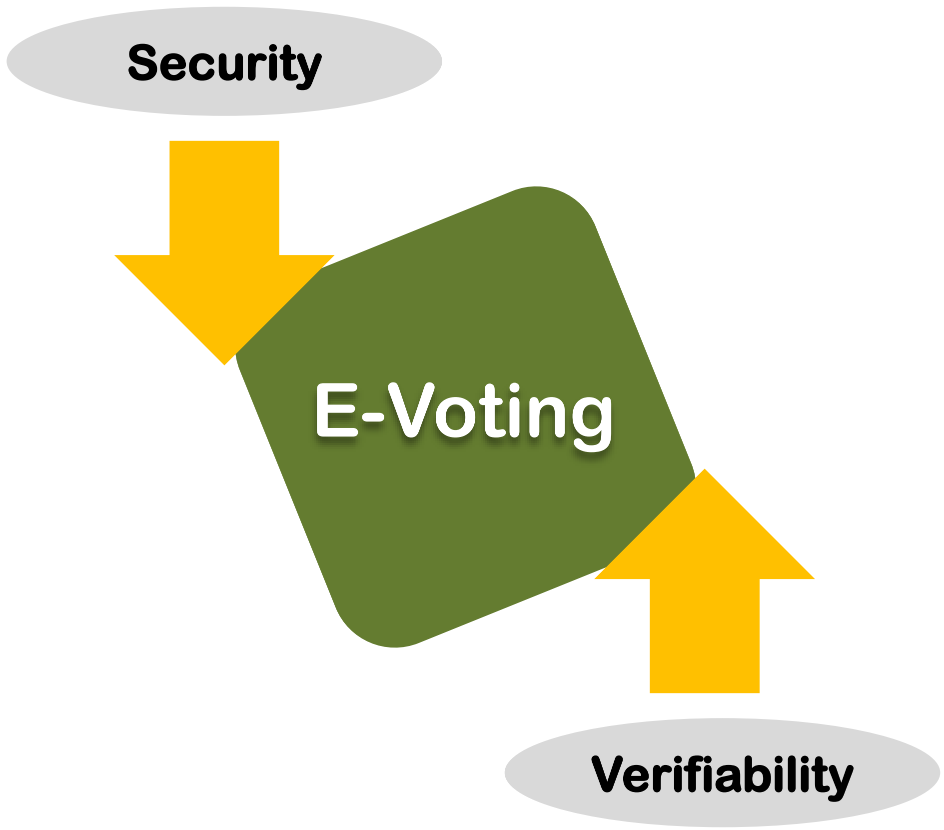
E-Vote-ID 2020
October 2020

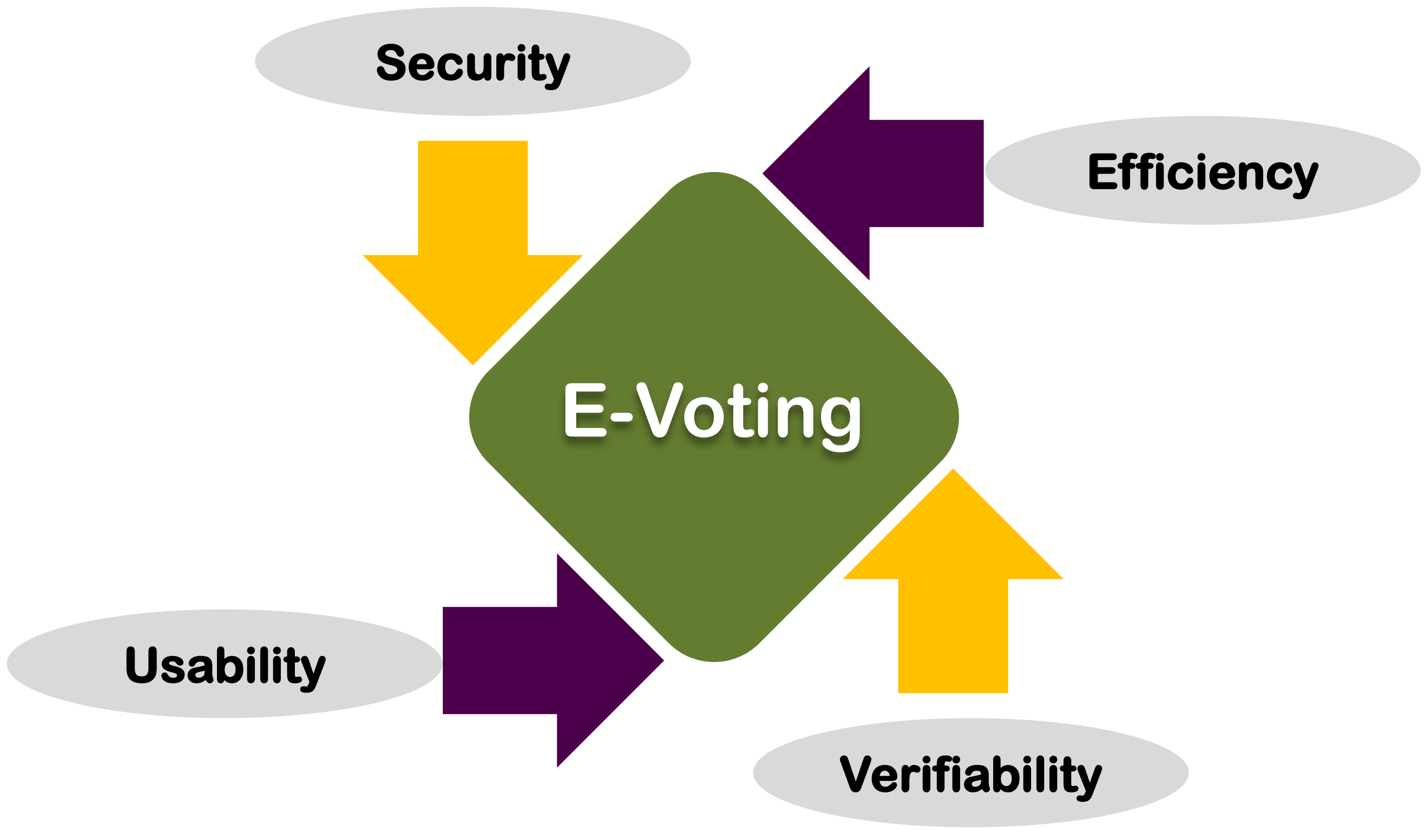
SnT
securityandtrust.lu

uni.lu
UNIVERSITÉ DU LUXEMBOURG

E-Voting


Security
E-Voting


Security
E-Voting
Verifiability


Security
Efficiency
E-Voting
Usability
Verifiability

JCJ e-Voting Protocol [Juels, Catalano, Jakobsson2010]

Participating entities:

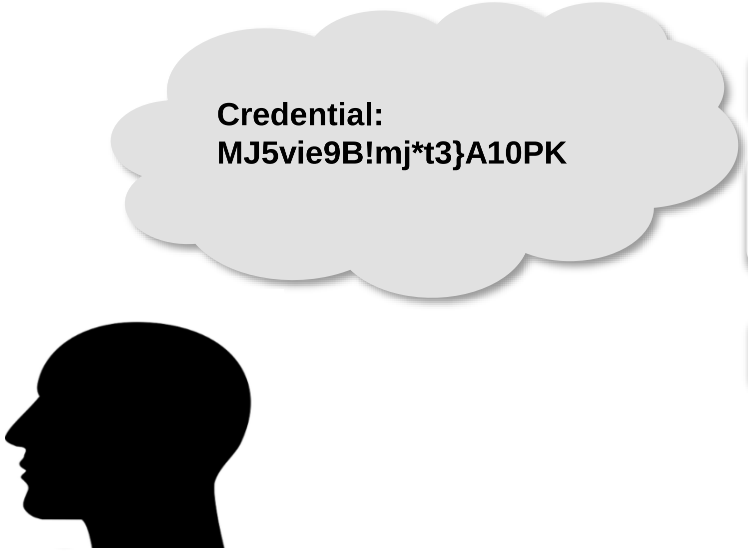
- Election Authority (EA)
- Registrars
- Talliers
  - Single
  - Distributed
- Voter (V_{id})
- Public Bulletin Board

- Secure
- Verifiable
- Coercion -Resistance
- Reciept free

Protocol Phases:

- Set Up Phase
  - Key _election=(PK,SK)
- Registration Phase
  - Credential for legitimate voters
- Voting Phase
  - Cast vote using credential
- Tally Phase
  - Ballot verification
  - Duplicate removal
  - Final tally
- Vérification Phase

Usability of JCJ ?!!



Long PseudoRandom string

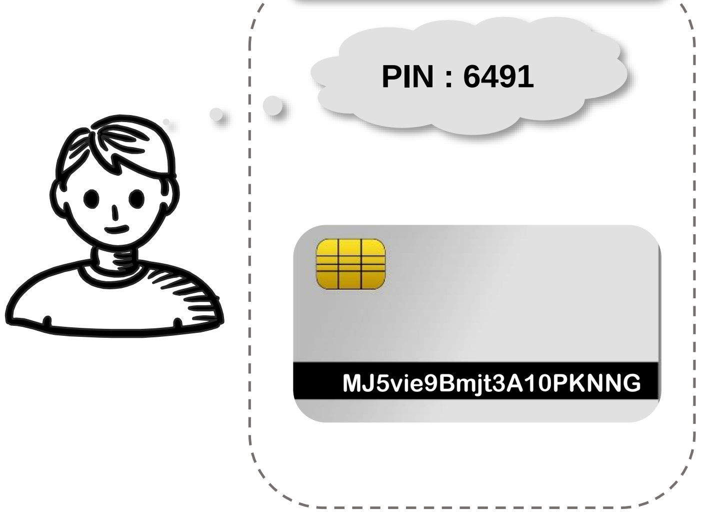
Hard to memorize by the voter,
Storage problem

NOT human error-resiliant

Toward Usable JCJ:

Solution by Neumann, Volkamer [NV12] :

Credential

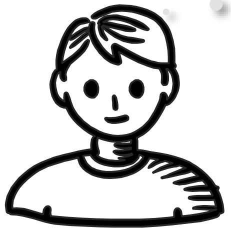


Short credential	Memorized by the voter
Long credential	Stored in voter’s smart card

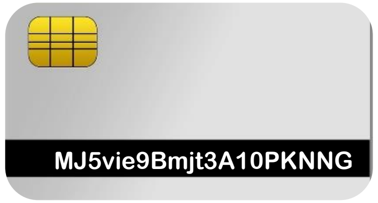
Toward Usable JCJ:

Solution by Neumann, Volkamer [NV12] :

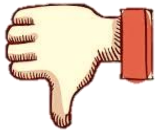
Credential



PIN : 6491



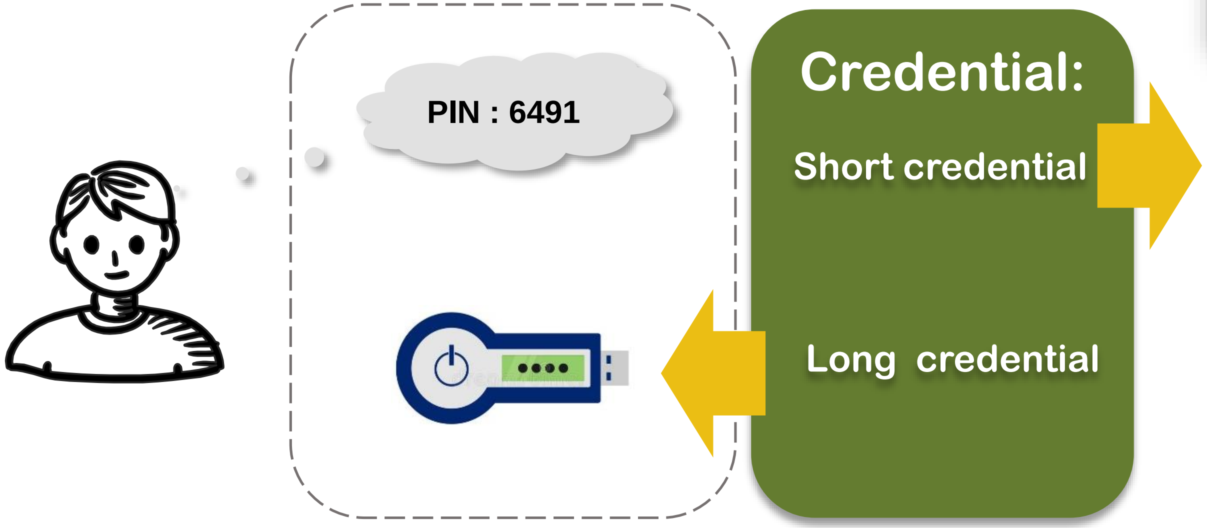
Short credential	Memorized by the voter
Long credential	Stored in voter’s smart card



Smart card removal	NOT human error-resilient
Leaky duplicate removal	Brute force attack
Benaloh challenge problem	Fake election identifier

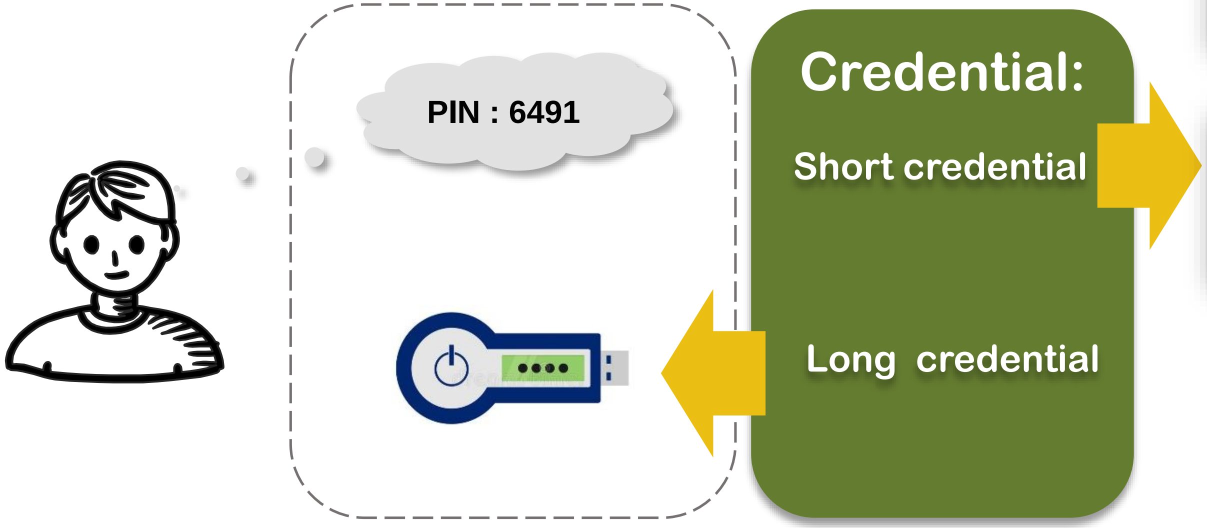
New solution for Usable JCJ:

New solution for Usable JCJ:



Generate a random PIN $\quad \mathrm{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

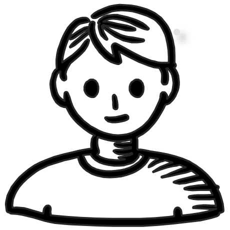
New solution for Usable JCJ:



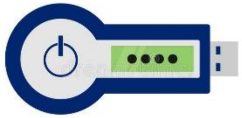
Generate a random PIN $\quad \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

$\mathsf{allowedErrorList}_{\alpha} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k\}$

New solution for Usable JCJ:



PIN : 6491



Credential:

Short credential

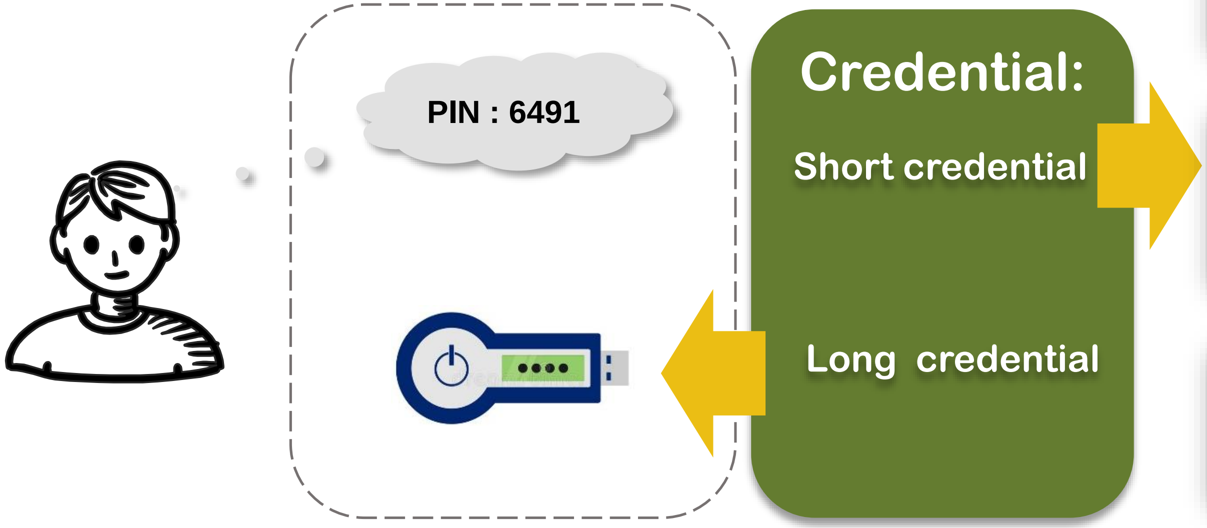
Long credential

Generate a random PIN $\qquad \mathrm{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

$\mathsf{allowedErrorList}_{\alpha} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k\}$

$$\mathsf{poly}_{\mathrm{PIN}}(x) = \prod_{i=1}^{k}(x - \alpha_i) = \sum_{i=0}^{k} p_i x^i \; : \qquad (p_0, p_1, \ldots, p_k)$$

New solution for Usable JCJ:



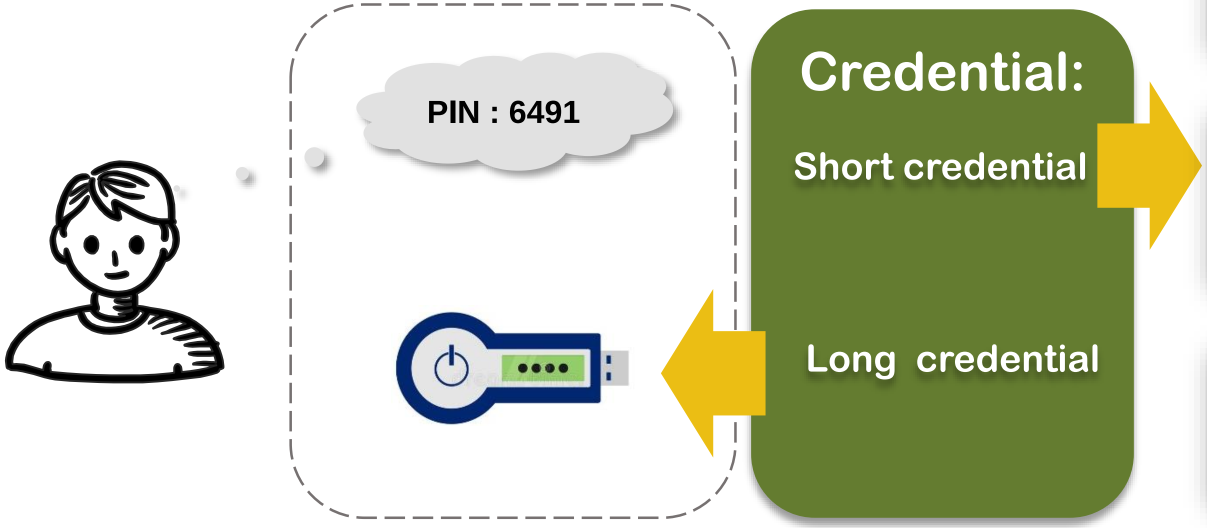
Generate a random PIN $\qquad \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

$\mathsf{allowedErrorList}_{\alpha} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k\}$

$\mathsf{poly}_{\mathrm{PIN}}(x) = \prod_{i=1}^{k}(x - \alpha_i) = \sum_{i=0}^{k} p_i x^i \ : \qquad (p_0, p_1, \ldots, p_k)$

$\mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{Enc}(p_i) x^i = \sum_{i=0}^{k} \mathsf{cp}_i x^i \ : \qquad (\mathsf{cp}_0, \mathsf{cp}_1, \ldots, \mathsf{cp}_k)$

New solution for Usable JCJ:



Generate a random PIN $\qquad \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

$$\mathsf{allowedErrorList}_{\alpha} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k\}$$

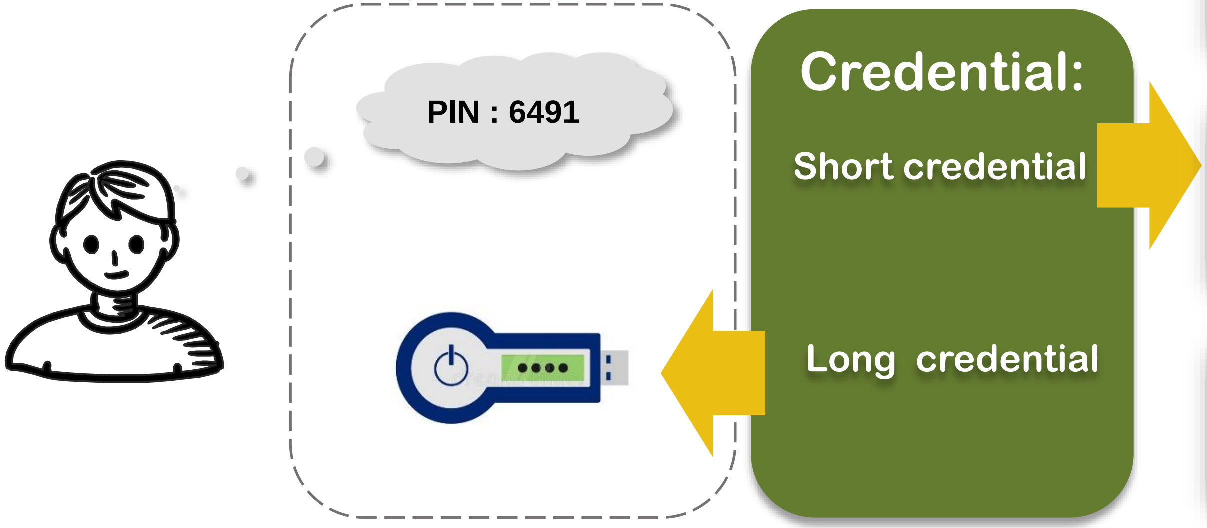
$$\mathsf{poly}_{\mathrm{PIN}}(x) = \prod_{i=1}^{k}(x - \alpha_i) = \sum_{i=0}^{k} p_i x^i \; : \qquad (p_0, p_1, \ldots, p_k)$$

$$\mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{Enc}(p_i) x^i = \sum_{i=0}^{k} \mathsf{cp}_i x^i \; : \qquad (\mathsf{cp}_0, \mathsf{cp}_1, \ldots, \mathsf{cp}_k)$$

$$\left.\begin{array}{r} \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\alpha^*) \\ \mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{cp}_i x^i \end{array}\right\} \stackrel{?}{\Rightarrow} (\alpha^* \in \mathsf{ErrorList}_{\alpha}) \equiv \mathsf{TRUE}/\mathsf{FALSE}$$

$$\mathsf{poly}_{\mathrm{PIN}}(\mathsf{CT}_{\mathrm{PIN}}) = \mathsf{poly}_{\mathrm{PIN}}(\mathsf{Enc}(\alpha^*)) = \mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(\alpha^*))$$

New solution for Usable JCJ:



Generate a random PIN $\qquad$ $\mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

$$\mathsf{allowedErrorList}_{\alpha} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k\}$$

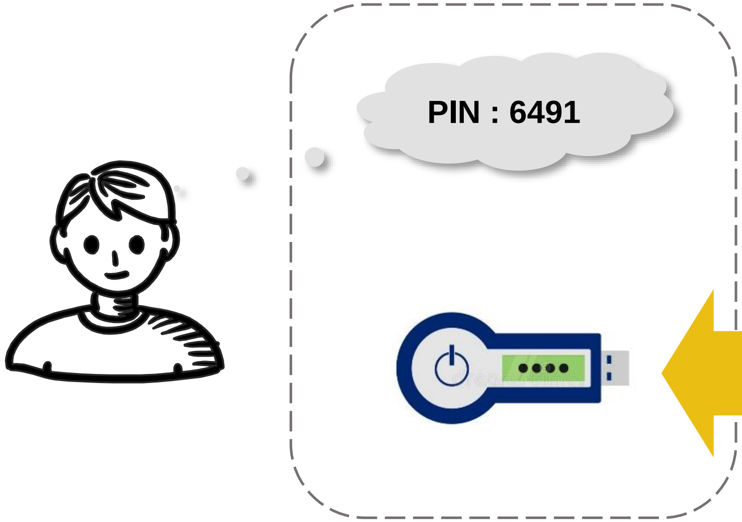
$$\mathsf{poly}_{\mathrm{PIN}}(x) = \prod_{i=1}^{k}(x - \alpha_i) = \sum_{i=0}^{k} p_i x^i \;: \qquad (p_0, p_1, \ldots, p_k)$$

$$\mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{Enc}(p_i) x^i = \sum_{i=0}^{k} \mathsf{cp}_i x^i \;: \qquad (\mathsf{cp}_0, \mathsf{cp}_1, \ldots, \mathsf{cp}_k)$$

$$\left.\begin{array}{r} \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\alpha^*) \\ \mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{cp}_i x^i \end{array}\right\} \stackrel{?}{\Rightarrow} (\alpha^* \in \mathsf{ErrorList}_{\alpha}) \equiv \mathsf{TRUE/FALSE}$$

$$\mathsf{poly}_{\mathrm{PIN}}(\mathsf{CT}_{\mathrm{PIN}}) = \mathsf{poly}_{\mathrm{PIN}}(\mathsf{Enc}(\alpha^*)) = \mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(\alpha^*))$$

New solution for Usable JCJ:



Credential:

Short credential

Long credential

Generate a random PIN $\quad \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\mathrm{PIN})$

$\mathsf{allowedErrorList}_{\alpha} = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k\}$

$\mathsf{poly}_{\mathrm{PIN}}(x) = \prod_{i=1}^{k}(x - \alpha_i) = \sum_{i=0}^{k} p_i x^i \; : \quad (p_0, p_1, \ldots, p_k)$

$\mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{Enc}(p_i)x^i = \sum_{i=0}^{k} \mathsf{cp}_i x^i \; : \quad (\mathsf{cp}_0, \mathsf{cp}_1, \ldots, \mathsf{cp}_k)$

$$\left.\begin{array}{r} \mathsf{CT}_{\mathrm{PIN}} = \mathsf{Enc}(\alpha^*) \\ \mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(x)) = \sum_{i=0}^{k} \mathsf{cp}_i x^i \end{array}\right\} \stackrel{?}{\Rightarrow} (\alpha^* \in \mathsf{ErrorList}_{\alpha}) = \mathsf{TRUE/FALSE}$$

$$\mathsf{poly}_{\mathrm{PIN}}(\mathsf{CT}_{\mathrm{PIN}}) = \mathsf{poly}_{\mathrm{PIN}}(\mathsf{Enc}(\alpha^*)) = \mathsf{Enc}(\mathsf{poly}_{\mathrm{PIN}}(\alpha^*))$$

- Polynomial evaluation without decryption
- Proof of the well-formedness of the polynomial
- Detect and remove ballots with invalid PIN
- Detect and remove duplicate valid ballots (valid PIN)

Paillier Instantiation :

Paillier Cryptosystem:

- $\mathsf{pk} = (n = pq, \mathbb{G}, g), \mathsf{sk} = (p, q)$
- $\mathsf{Enc}(m) = g^m \cdot r^n \mod n^2$

A partially homomorphic Encryption scheme

Security : Decisional composite residuosity assumption

Proof system: Non-Interactive sigma protocol

Evaluate the polynomial without decrypting

Efficient multi-party computation to sort ciphertext

BGN Instantiation :

BGN Cryptosystem:

- $\mathsf{pk} = (n, \mathbb{G}, \mathbb{G}_T, \mathbf{e}, g, h = g'^q), \mathsf{sk} = (p, q)$
- $\mathbb{G} = \langle g \rangle, n = pq, \mathbf{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$
- $\mathsf{Enc}(m) = g^m h^r \in \mathbb{G}, m \in [T]$

A partially homomorphic Encryption scheme

Security : Discrete log and factorization

Proof system: Groth-Sahai NIWI (bilinear map)

Evaluate the polynomial without decrypting (bilinear map)

Security Analysis concerning PIN length:

S: Swapping errors

PIN= 1 2 3 4 : 13 2 4, 1 2 4 3 ∈ AllowedErrorList

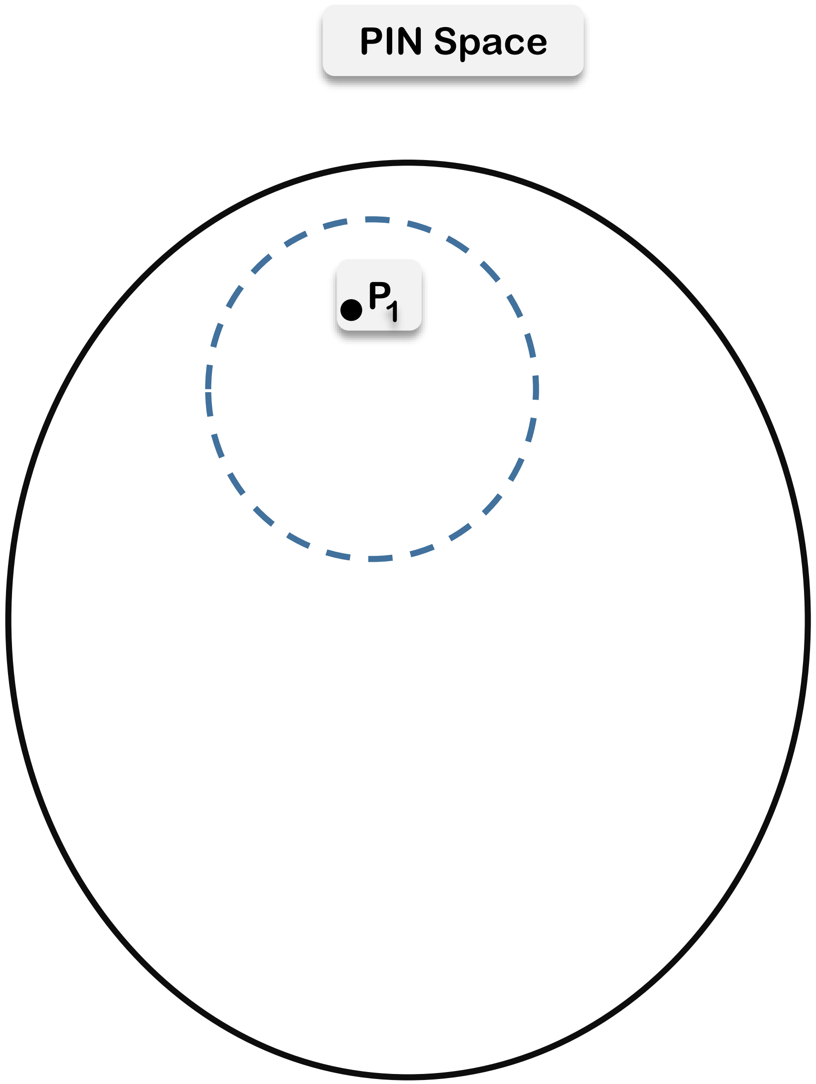
W: single Wrong digit errors

PIN= 1234 : 1235, 1434 ∈ AllowedErrorList

PIN= 1 2 3 4 :

PINs covered by “1234” :2134, 1324 , 1243 , 1230, 1231,1232,1233,….,

PINs NOT covered by “1234” :8734, 9876 , 0932 , 1650, 1839,1030,1891,….,



Security Analysis concerning PIN length:

S: **S**wapping errors

PIN= 1 2 3 4 : 13 2 4, 1 2 4 3 ∈ AllowedErrorList

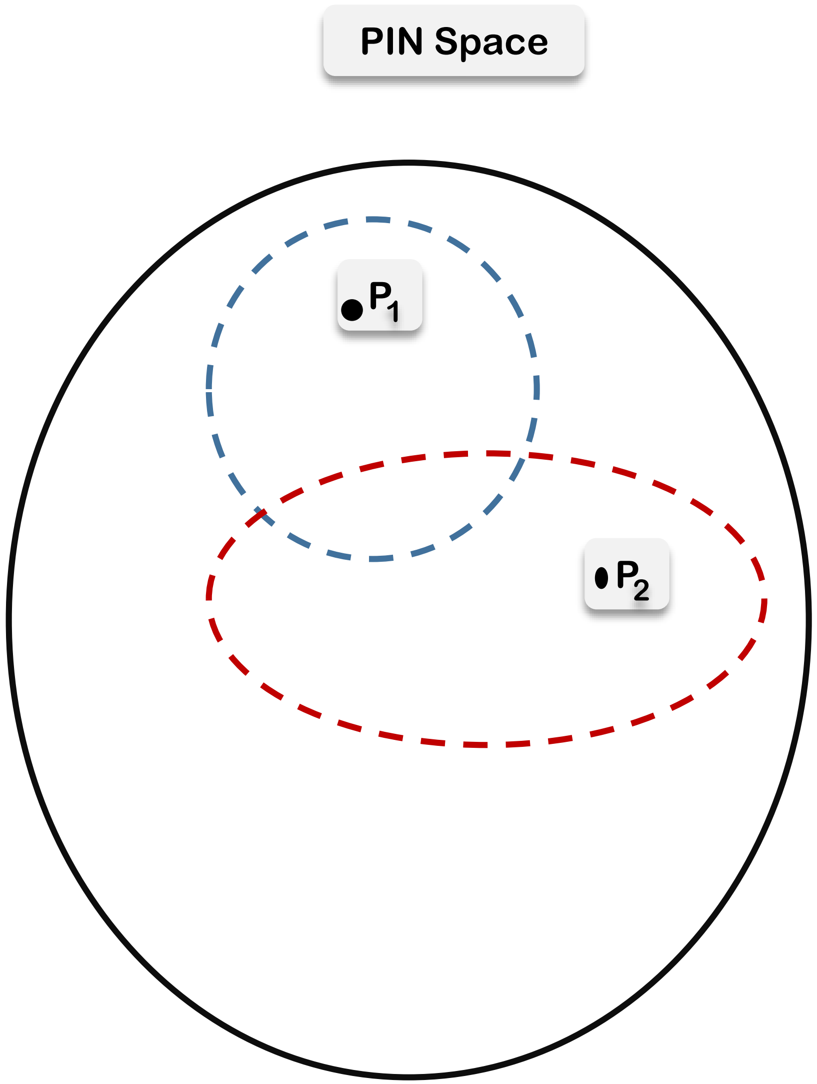
W: single **W**rong digit errors

PIN= 1234 : 1235, 1434 ∈ AllowedErrorList

PIN= 1 2 3 4 :

PINs covered by "1234" :2134, 1324 , 1243 , 1230, 1231,1232,1233,....,

PINs NOT covered by "1234" :8734, 9876 , 0932 , 1650, 1839,1030,1891,....,



Security Analysis concerning PIN length:

S: Swapping errors

PIN= 1 2 3 4 : 13 2 4, 1 2 4 3 $\in$ AllowedErrorList

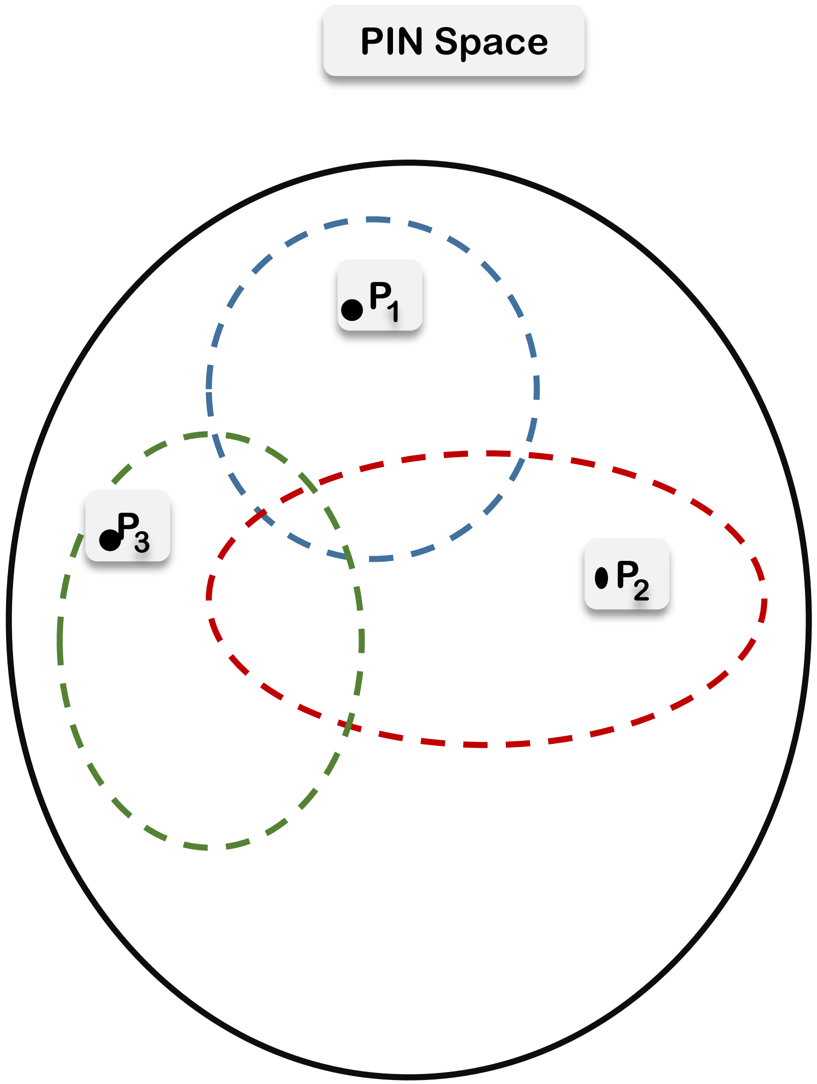
W: single Wrong digit errors

PIN= 1234 : 1235, 1434 $\in$ AllowedErrorList

PIN= 1 2 3 4 :

PINs covered by "1234" :2134, 1324 , 1243 , 1230, 1231,1232,1233,....,

PINs NOT covered by "1234" :8734, 9876 , 0932 , 1650, 1839,1030,1891,....,



Security Analysis concerning PIN length:

S: Swapping errors

PIN= 1 2 3 4 : 1<u>3</u> <u>2</u> 4, 1 2 <u>4</u> <u>3</u> ∈ AllowedErrorList

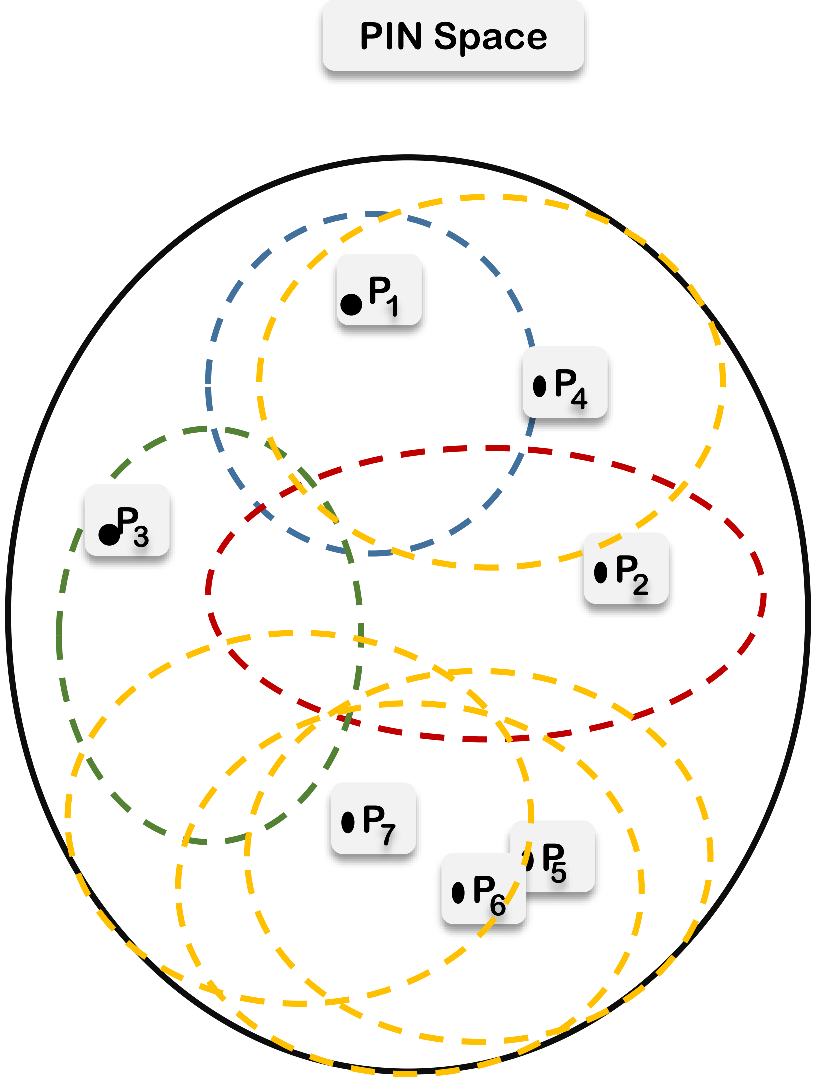
W: single Wrong digit errors

PIN= 1234 : 123<u>5</u>, 1<u>4</u>34 ∈ AllowedErrorList

PIN= 1 2 3 4 :

PINs covered by "1234" :2134, 1324 , 1243 , 1230, 1231,1232,1233,....,

PINs <u>NOT</u> covered by "1234" :8734, 9876 , 0932 , 1650, 1839,1030,1891,....,



Security Analysis, PIN length:

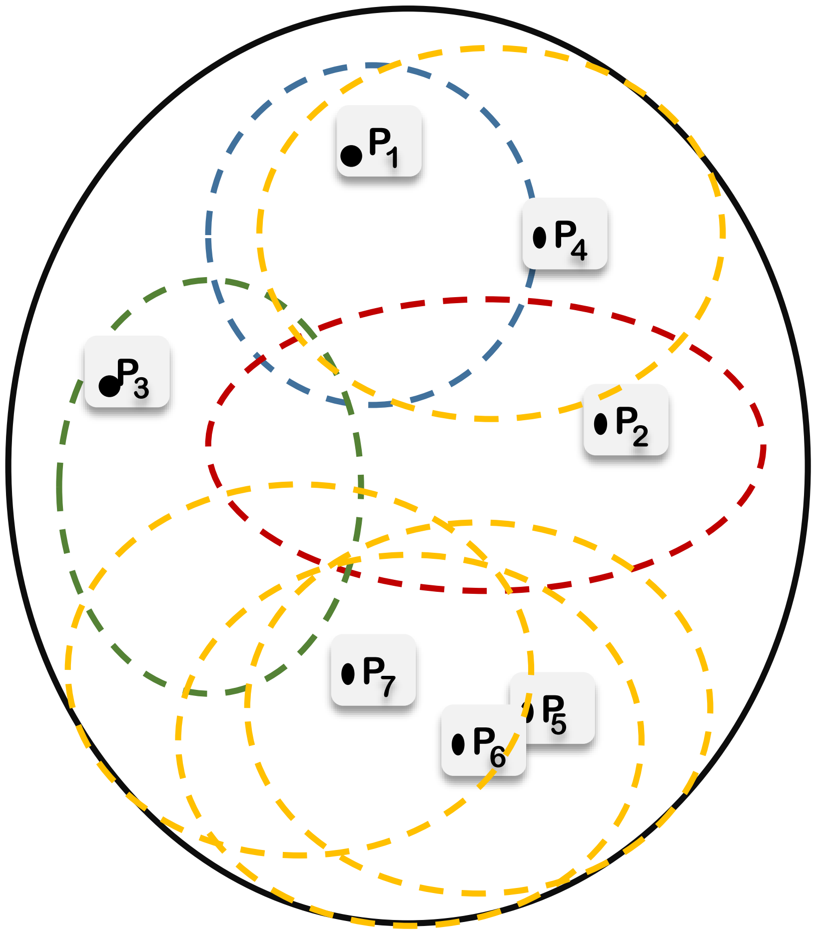
S: **S**wapping errors

PIN= 1 2 3 4 : 13 2 4, 1 2 4 3 ∈ AllowedErrorList

W: single **W**rong digit errors

PIN= 1234 : 1235, 1434 ∈ AllowedErrorList

PIN Space



PIN Length	2	3	4	5
S + W Lower Bound	8	34	250	2000
S + W Upper Bound	9	78	713	6490
S Lower Bound	55	465	4131	

https://github.com/Ehsan-ESTAJI/JCJ-Pin

Conclusions:

Presented attacks and repairs on the NV12 scheme

Presented protocols which are resilient to human errors in the form of PIN typos

Outlook:

The digitally stored key could be combined or replaced with a key derived from biometric data

Make the error correction efficient that we can allow using noisy biometric data without fuzzy extraction.

PIN/Credential update for different elections

Socio-technical research questions:

Which type of PIN errors do voters do when the are in a vote setting and do not get any feedback on the correctness of the PIN.

what it the optimal PIN policy that corrects as many PIN typos while still keeping the entropy of the PIN space sufficiently high.

If we do not use a smart card, or use both a smart card and key storage: how well can voters be trained to handle, fake and hide secret keys

Thanks for your attention!