USABILITY AND SECURITY OF GAZE-BASED GRAPHICAL GRID PASSWORDS

Majid Arianezhad, Douglas Stebila, Behzad Mozaffari

2013/04/01

USEC

Queensland University of Technology

USABILITY AND SECURITY OF GAZE-BASED GRAPHICAL GRID PASSWORDS

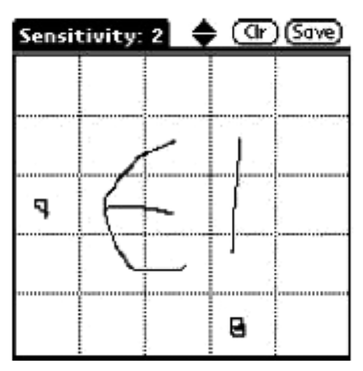
1. Are Android-like graphical grid passwords usable with gaze-based entry?

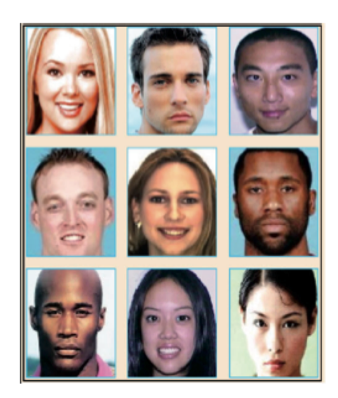
2. How can we measure the security of graphical grid passwords?

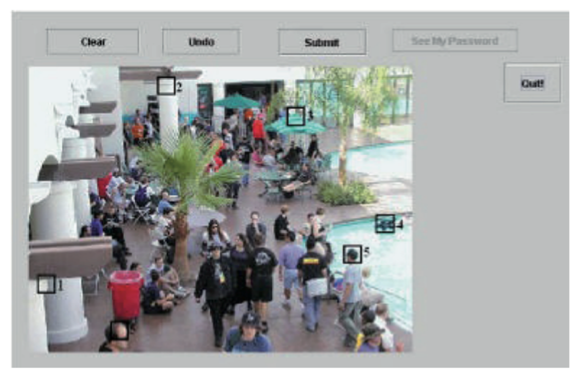
GRAPHICAL PASSWORDS

SEE FANTASTIC SURVEY PAPER BY BIDDLE, CHIASSON, VAN OORSCHOT, ACM COMPUTING SURVEYS 2012

- Recall-based
  - User must recall and enter a secret drawing from memory
  - Can be free form or grid-based
- Recognition-based
  - User must recognize a few personal objects from a set of objects
- Cued-recall
  - User is given an image cue and must recall and enter points or pattern







ENTRY METHODS

- Mouse
  - commonplace input method
  - mouse movements easily observed (“shoulder surfing”)
- Touch
  - easy and intuitive
  - vulnerable to “smudge attacks”
- Gaze
  - requires specialized, expensive input equipment
  - more resistant to shoulder surfing
  - possibly more suitable for persons with disabilities

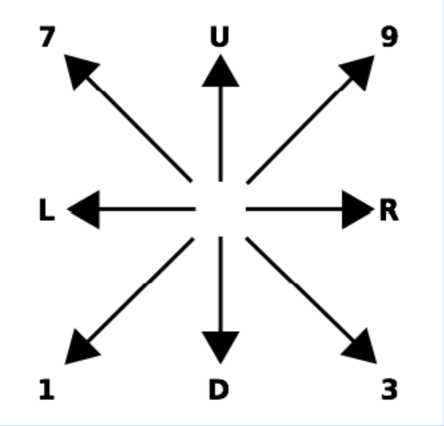
GAZE-BASED GRAPHICAL PASSWORDS

CUED GAZE-POINTS (CGP)

- Forget, Chiasson, Biddle CHI 2010
- Cued-recall
- Gaze-based variant of Cued Click Points

EYEPASSSHAPES

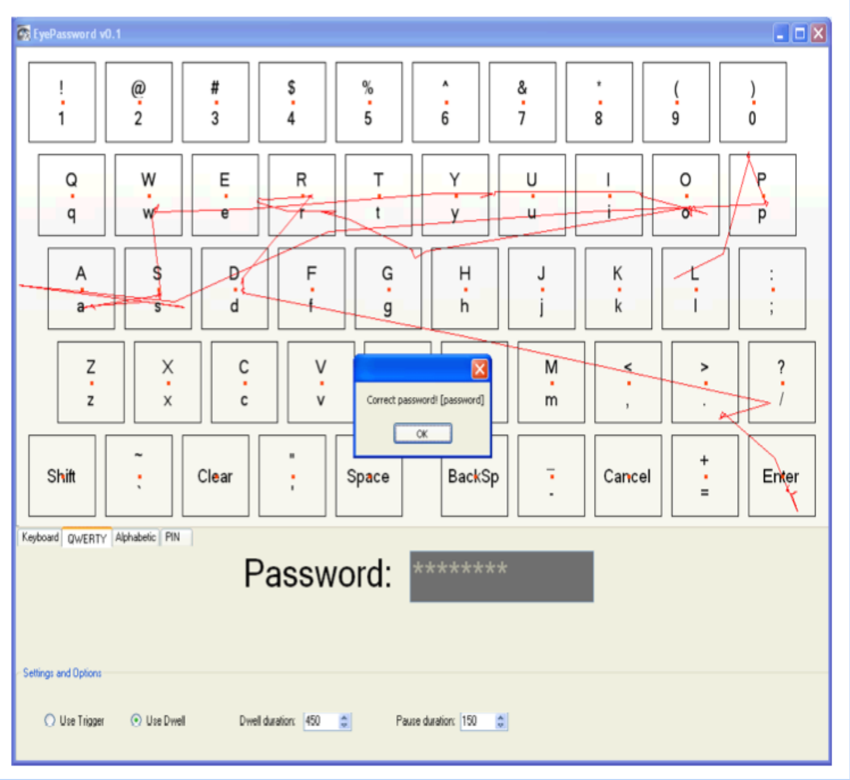
- De Luca, Denzel, Hussmann SOUPS 2009
- Recall
- Grid with adjacent movements only



GAZE-BASED GRAPHICAL PASSWORDS

EyePassword

- Kumar, Garfinkel, Boneh, Winograd SOUPS 2007
- On-screen keyboard

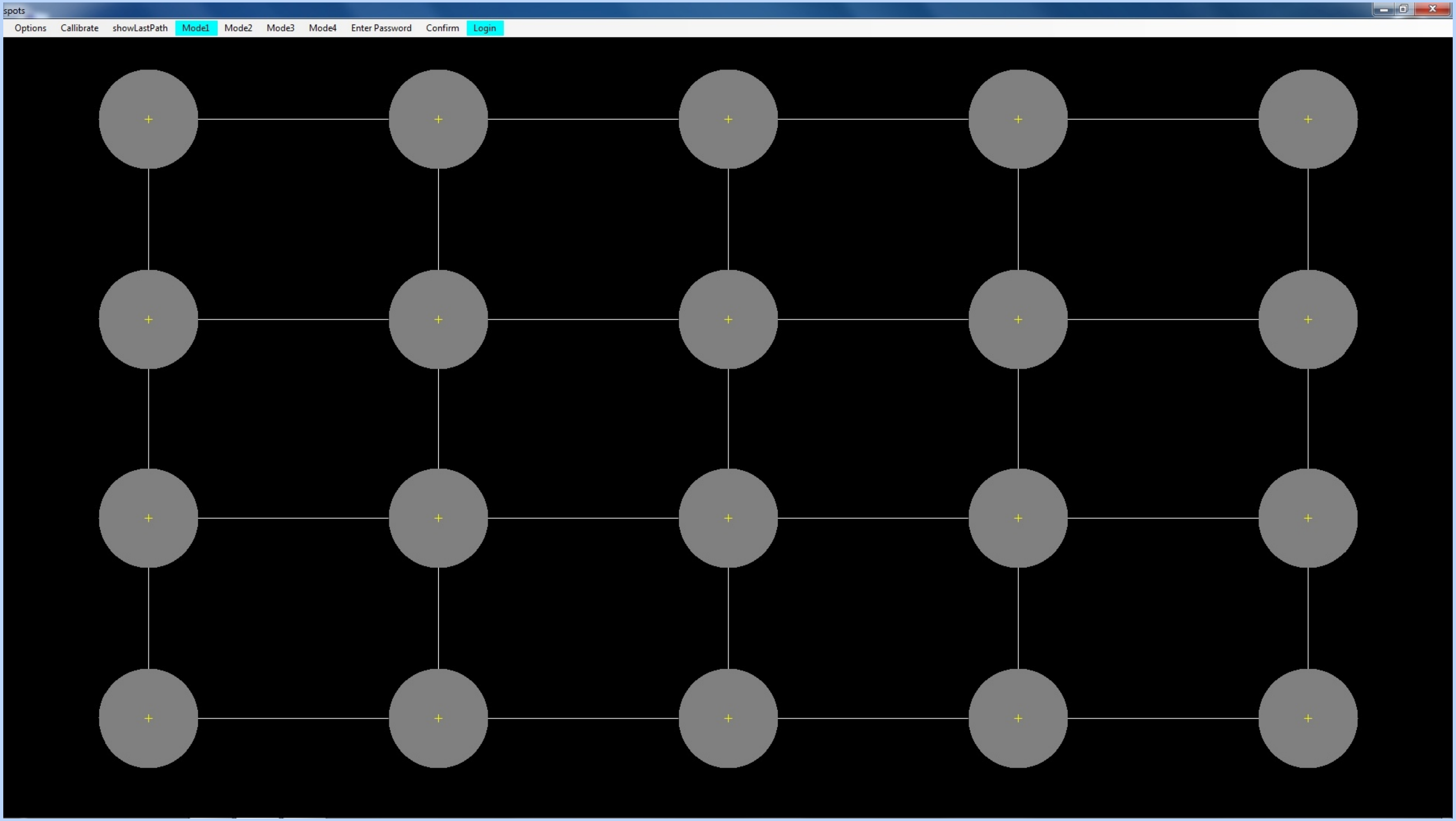


Correct password! [password]

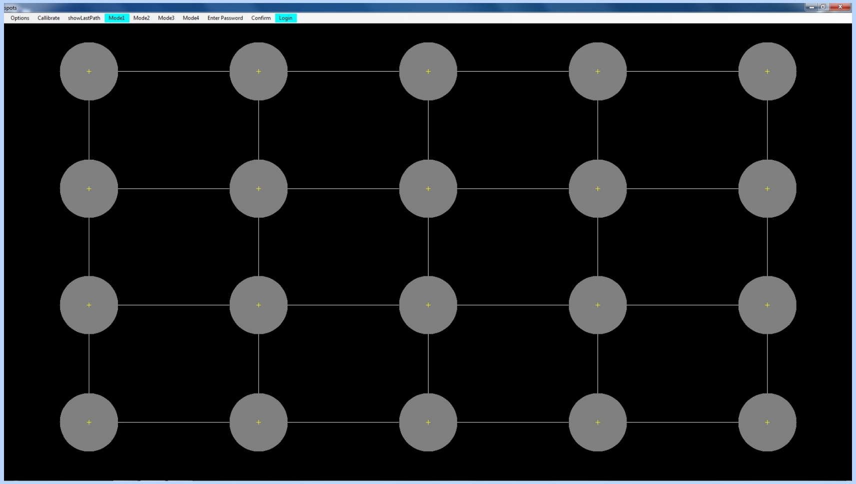
Password: ********

○ Use Trigger ● Use Dwell Dwell duration: 450 Pause duration: 150

GAZE-BASED GRAPHICAL GRID PASSWORDS



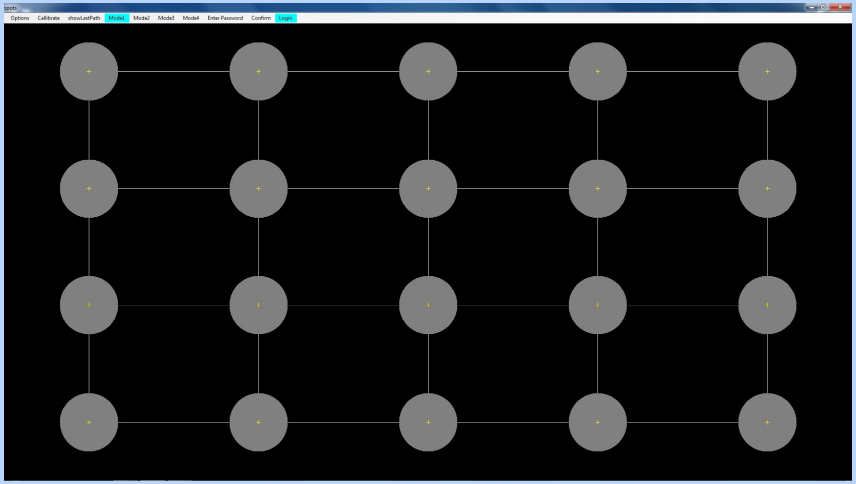
BASIC SCHEME



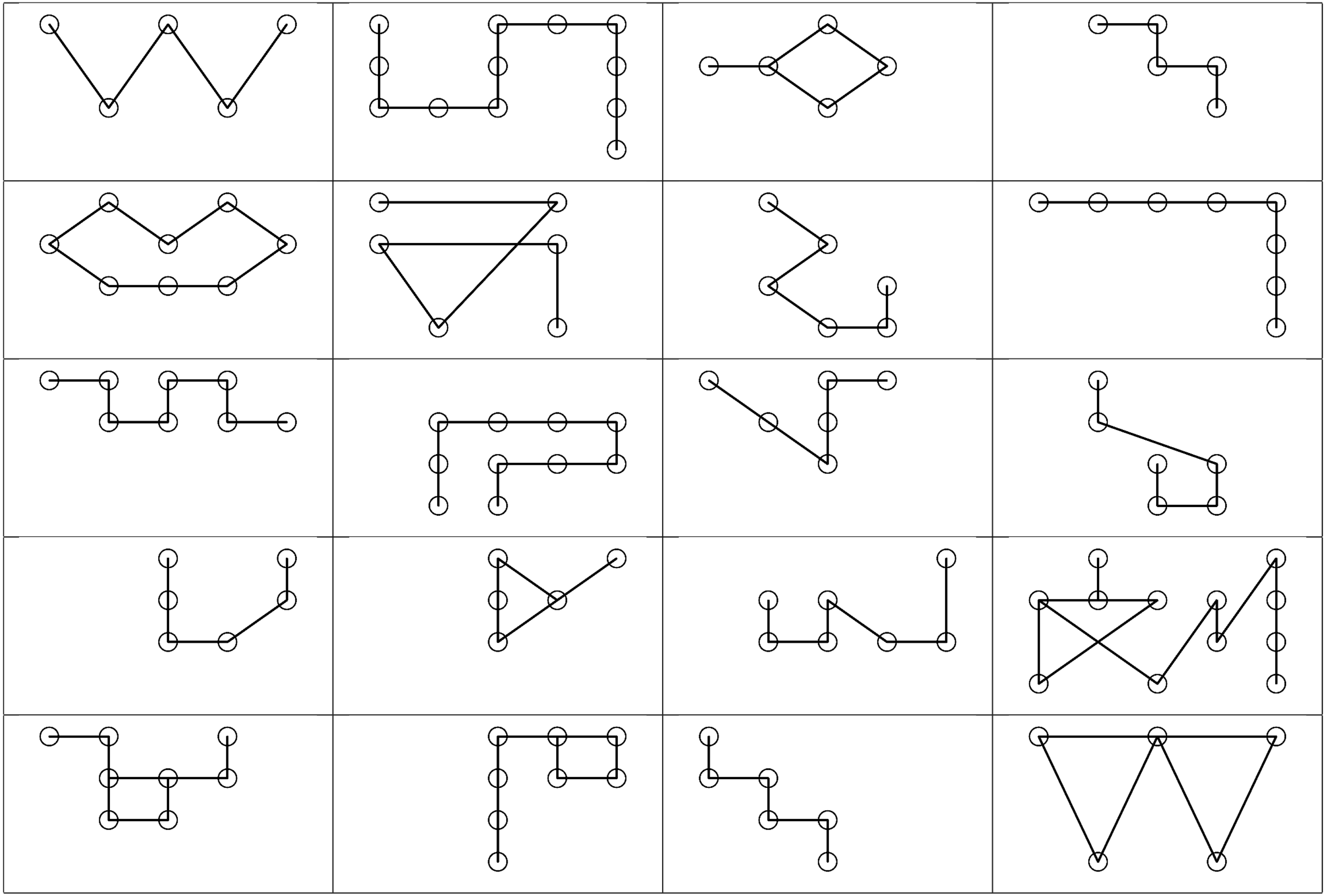
[Calibration]

1. Gaze at first point
2. Press spacebar
3. Gaze at next point for >0.5 seconds
4. Gaze at next point for >0.5 seconds
5. …
6. Gaze at last point for >0.5 seconds
7. Press spacebar

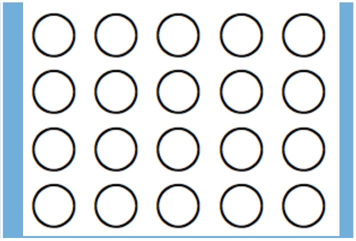
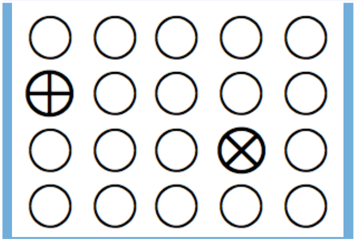
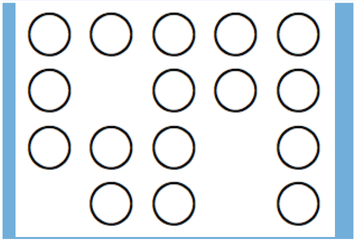
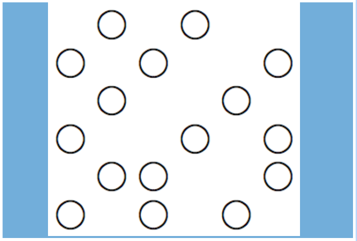
BASIC SCHEME



- No visual feedback of points selected
- Subsequent points need not be adjacent
- Cannot use same point twice in a row but can revisit later



VARIANTS

				
	Basic scheme	Cued start/end points	Grid with holes	Sparse grid
	5x4 grid	5x4 grid	5x4 grid	6x6 grid
		Must start at + and end at x	Cannot use some points	Lots of holes

USABILITY AND SECURITY OF GAZE-BASED GRAPHICAL GRID PASSWORDS

1. Are Android-like graphical grid passwords usable with gaze-based entry?

2. How can we measure the security of graphical grid passwords?

USABILITY OF GAZE-BASED GRAPHICAL GRID PASSWORDS

Are Android-like graphical grid passwords usable with gaze-based entry?

GENERAL METHODOLOGY

TASKS

1. For 3 of the 4 schemes:
   1. Create password
   2. Confirm password
   3. [Distraction task]
   4. Login
2. Final login with scheme 1
3. Survey

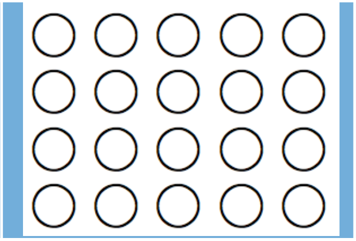
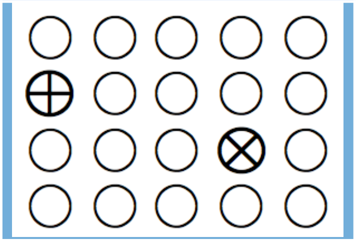
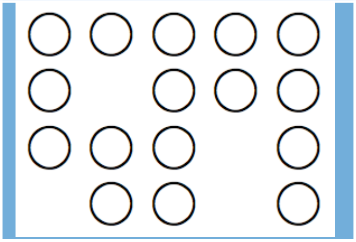
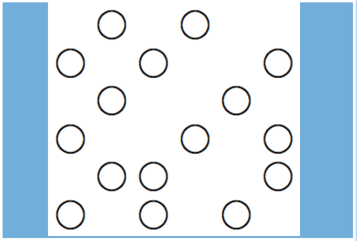
22 participants total

REPORTED DATA

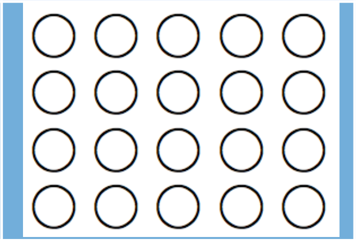
- Successful
  - confirm / login / final login

  on
  - 1st try / ≤ 3 tries
- Confirm / login errors
- Total time (incl. errors)
- Successful time
- Ease of use

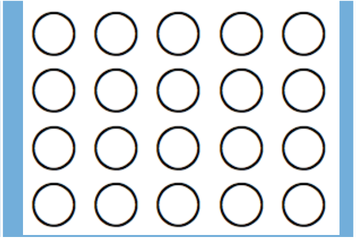
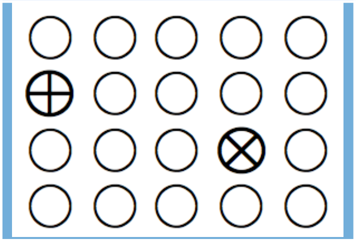
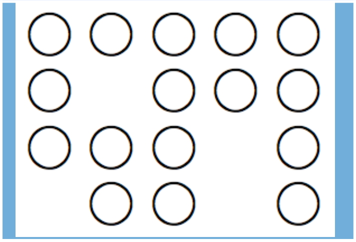
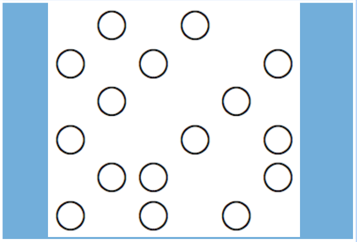
PASSWORD ENTRY SUCCESS RATE

				
Confirm 1st try ≤ 3 tries	91% 95%	64% 91%	67% 98%	38% 69%
Login 1st try ≤ 3 tries	73% 91%	91% 95%	89% 100%	54% 77%
Final Login (10 mins. later) 1st try ≤ 3 tries	45% 55%			

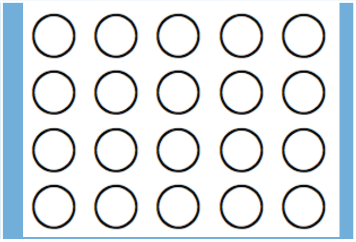
PASSWORD ENTRY SUCCESS RATE

		Cued Gaze Points CGP T-51	EyePassShapes	EyePassword
Confirm				
1st try	91%	67%		
≤ 3 tries	95%	82%		
Login				
1st try	73%	73%	86%	97%
≤ 3 tries	91%	93%		
Final Login				
(10 mins. later)			(5 days later)	
1st try	45%		57%	
≤ 3 tries	55%			

PASSWORD ENTRY TIME & EASE OF USE

				
Total login time (sec) (incl. errors)	21.4	18.0	19.5	17.4
Login time (sec) per point (not incl. errors)	1.68	1.60	1.98	1.26
Ease of use (Likert scale, 1=very easy, 4=very hard)	1.91	1.95	2.44	2.31

PASSWORD ENTRY TIME

		Cued Gaze Points CGP T-51	EyePassShapes	EyePassword
Total login time (sec) (incl. errors)	21.4	36.7 (incl. username entry)		
Login time (sec) per point (not incl. errors)	1.68		1.56	1.08

USABILITY RESULTS

- Gaze-based graphical grid passwords generally competitive with other gaze-based schemes.
- Long-term memorability poor.
- Limited understanding of overall usability of gaze-based password schemes due to limits of lab-based studies.
- Importance of reporting as much data as possible.
- Open question: confounding effects of remembering multiple passwords over time.

SECURITY OF GRAPHICAL GRID PASSWORDS

How can we measure the security of graphical grid passwords?

SECURITY METRICS

TEXTUAL PASSWORDS

- dictionary word
- character frequency
- digraph frequency
- repeated characters

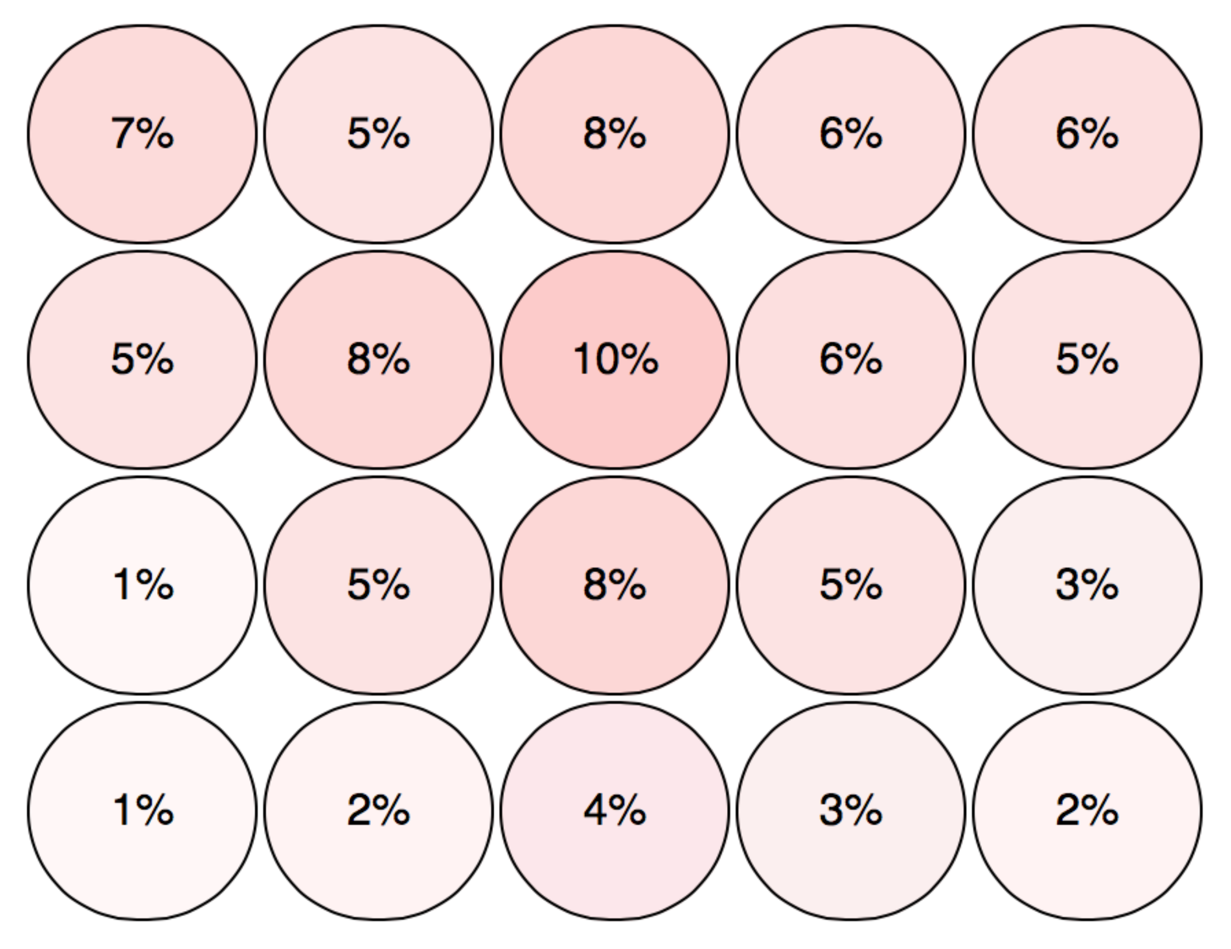
GRID PATTERNS

- common pattern
- point frequency
  - first, last, all
- stroke frequency
  - direction & length
- symmetry

POINT FREQUENCY

Scheme 1

All points

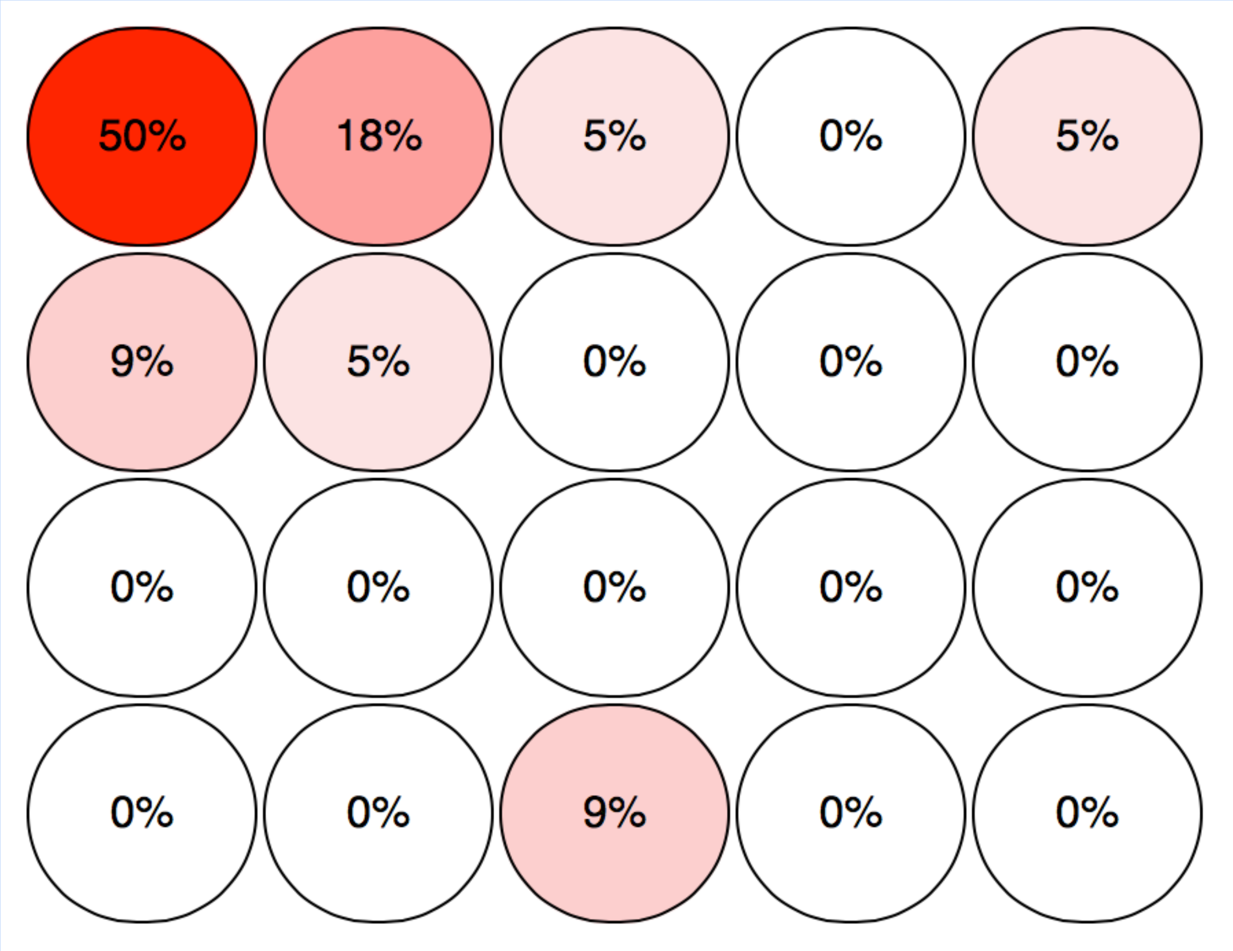


7%	5%	8%	6%	6%
5%	8%	10%	6%	5%
1%	5%	8%	5%	3%
1%	2%	4%	3%	2%

POINT FREQUENCY

Scheme 1

First point

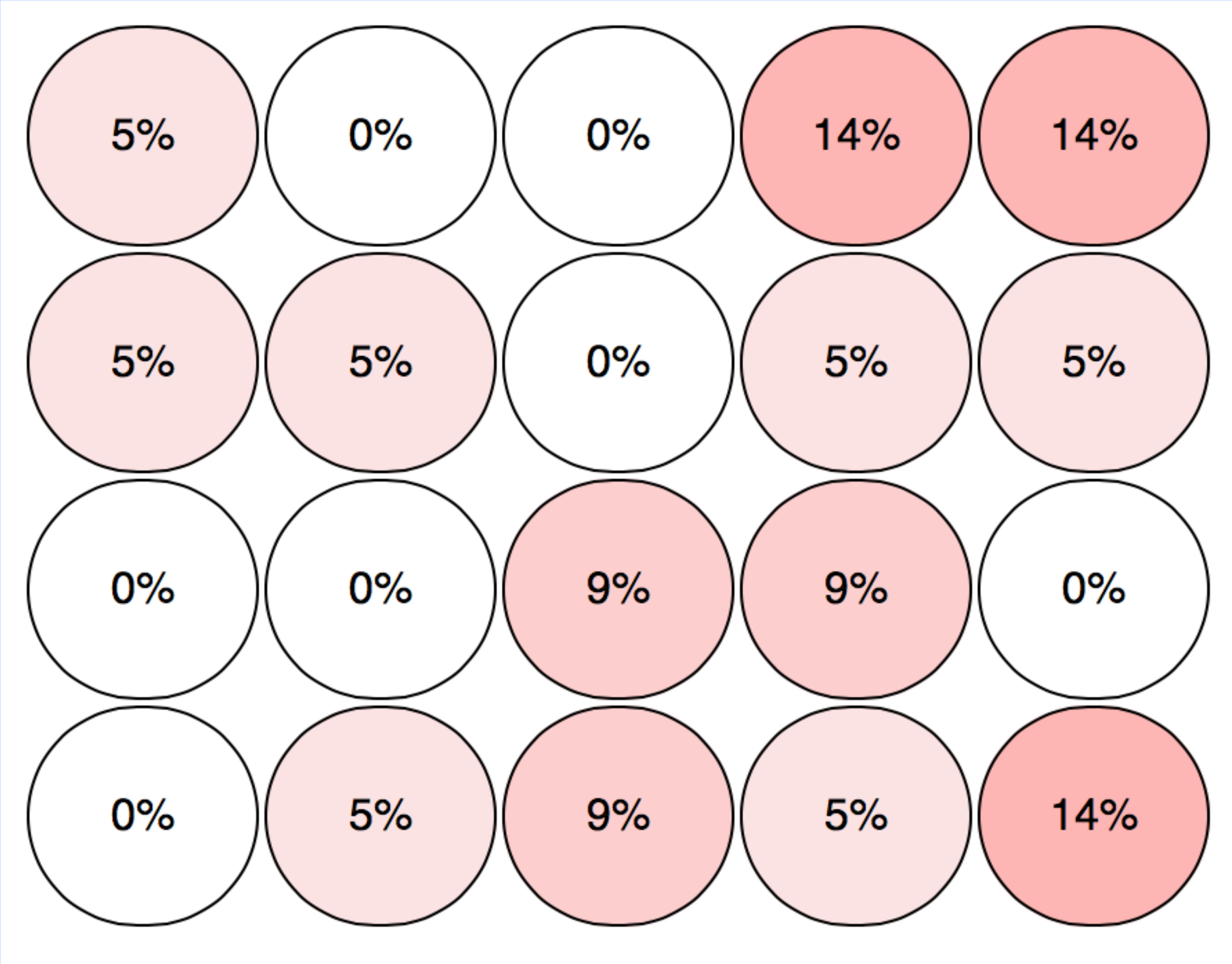


50%	18%	5%	0%	5%
9%	5%	0%	0%	0%
0%	0%	0%	0%	0%
0%	0%	9%	0%	0%

POINT FREQUENCY

Scheme 1

Last point

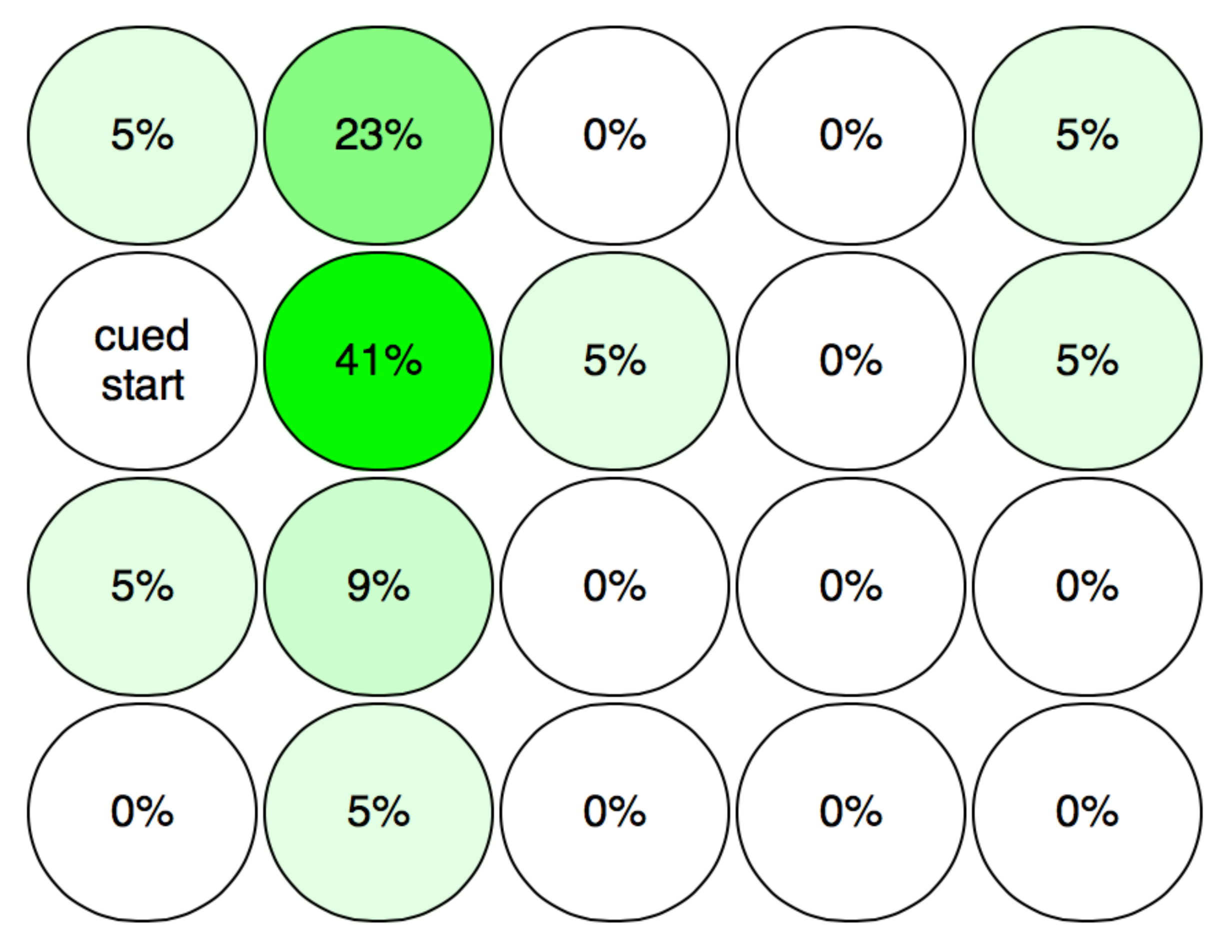


5%	0%	0%	14%	14%
5%	5%	0%	5%	5%
0%	0%	9%	9%	0%
0%	5%	9%	5%	14%

POINT FREQUENCY

Scheme 2

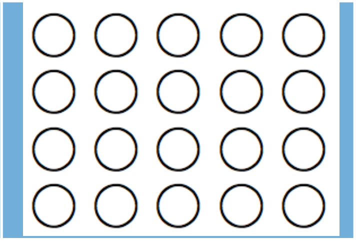
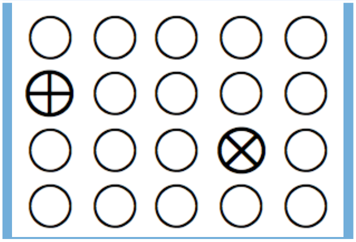
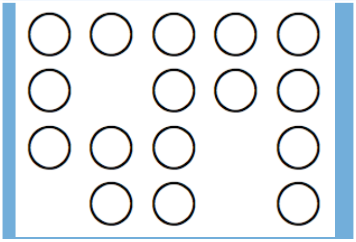
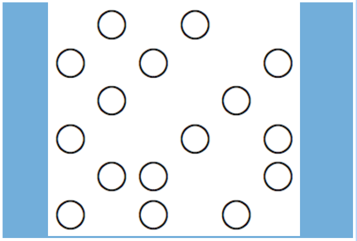
First point



5%	23%	0%	0%	5%
cued start	41%	5%	0%	5%
5%	9%	0%	0%	0%
0%	5%	0%	0%	0%

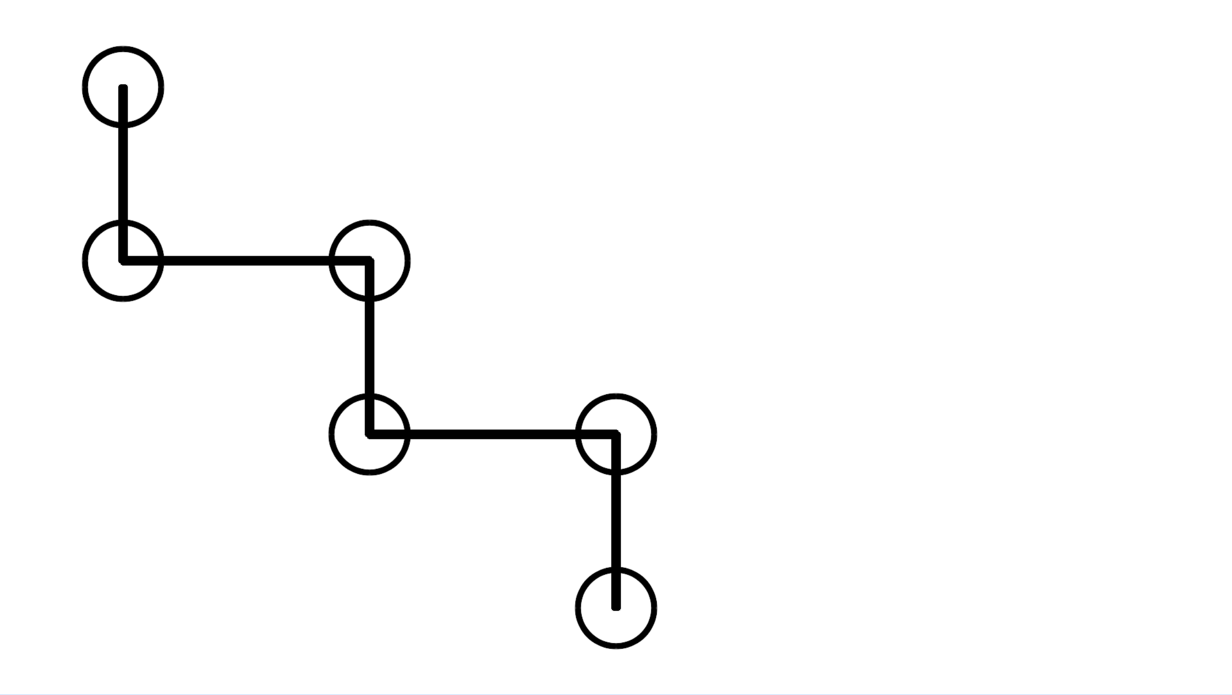
BINARY ENTROPY OF POINT FREQUENCY

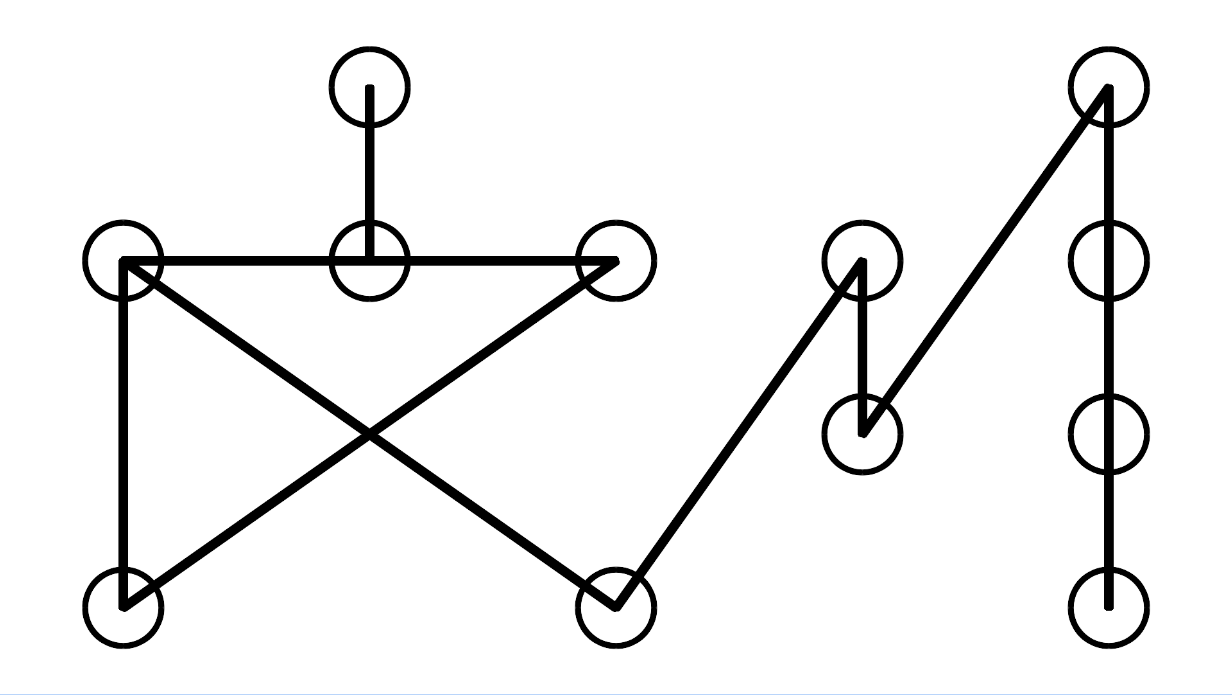
VS. IDEAL

				
All	4.11 / 4.32	3.87 / 4.17	3.75 / 4.00	3.95 / 4.00
First	2.18 / 4.32	2.54 / 4.25	2.50 / 4.00	2.78 / 4.00
Last	3.54 / 4.32	2.63 / 4.25	2.50 / 4.00	2.14 / 4.00

STROKE FREQUENCY

Example, Scheme 1





STROKE FREQUENCY

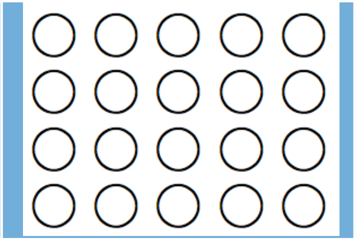
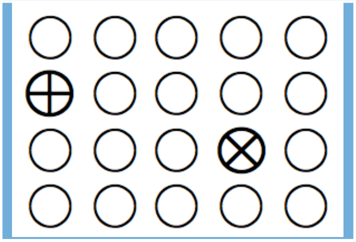
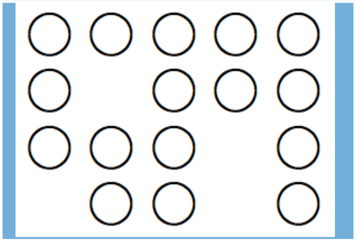
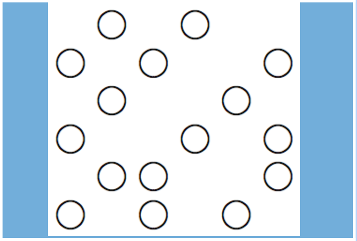
Example, Scheme 1

STROKE FREQUENCY, SCHEME 1

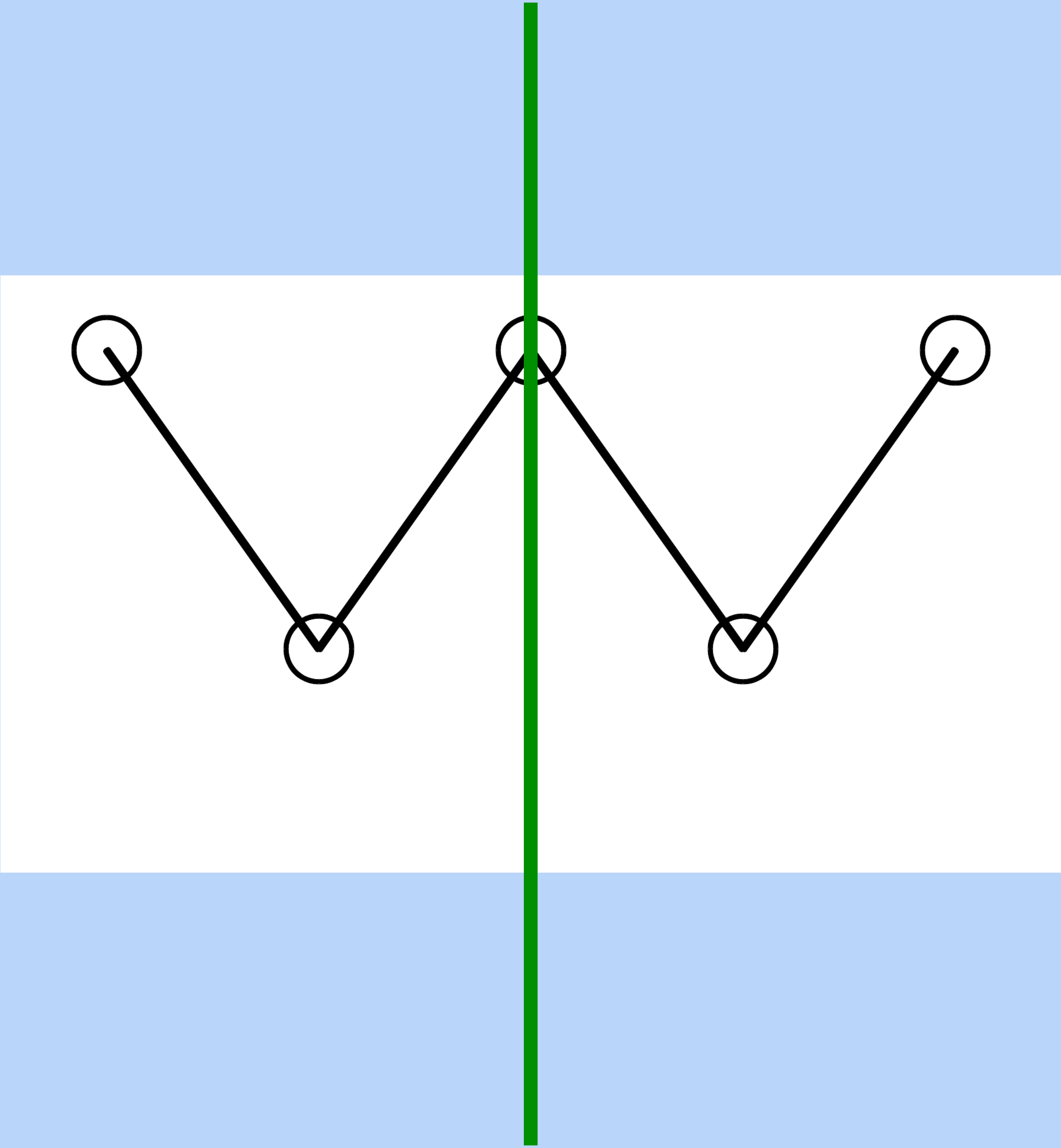
	4 ←	3 ←	2 ←	1 ←		1 →	2 →	3 →	4 →
3 ↑	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
2 ↑	0.0000	0.0000	0.0000	0.0000	0.0207	0.0000	0.0069	0.0069	0.0000
1 ↑	0.0000	0.0000	0.0069	0.0207	0.0690	0.0345	0.0000	0.0069	0.0000
	0.0000	0.0000	0.0138	0.1310	0.0000	0.2276	0.0069	0.0000	0.0000
1 ↓	0.0000	0.0138	0.0276	0.0276	0.2414	0.0621	0.0138	0.0138	0.0000
2 ↓	0.0000	0.0000	0.0000	0.0069	0.0069	0.0138	0.0069	0.0000	0.0000
3 ↓	0.0000	0.0000	0.0000	0.0000	0.0138	0.0000	0.0000	0.0000	0.0000

BINARY ENTROPY OF STROKE DIRECTION & LENGTH

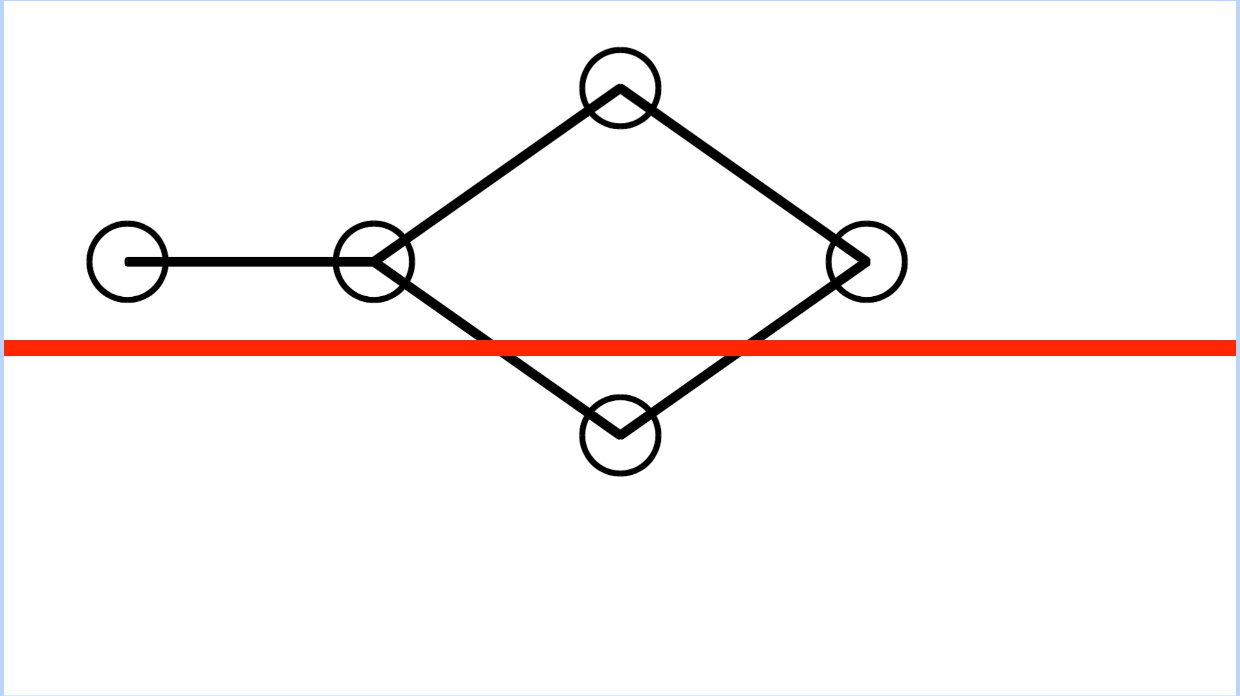
VS. IDEAL

				
	3.47 / 5.65	3.05 / 5.54	3.20 / 5.64	3.73 / 6.33

Values for uniformly random passwords calculated from 100,000 uniformly randomly generated samples of length 7.

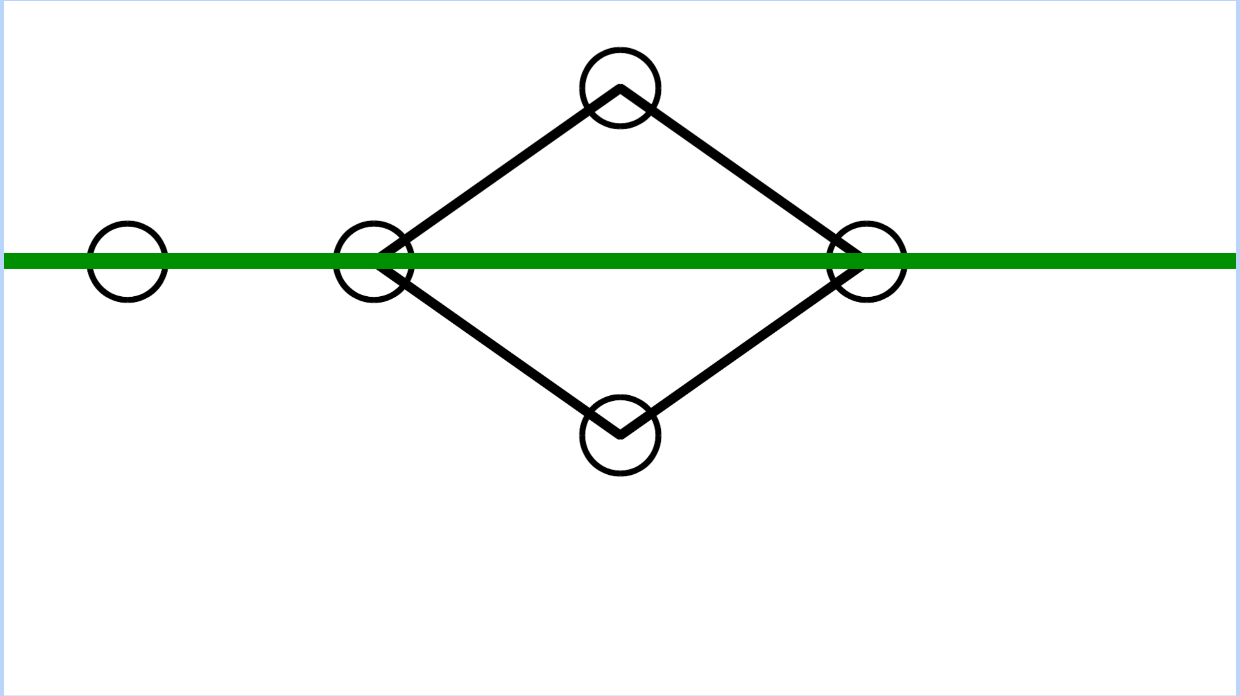


HORIZONTAL SYMMETRY



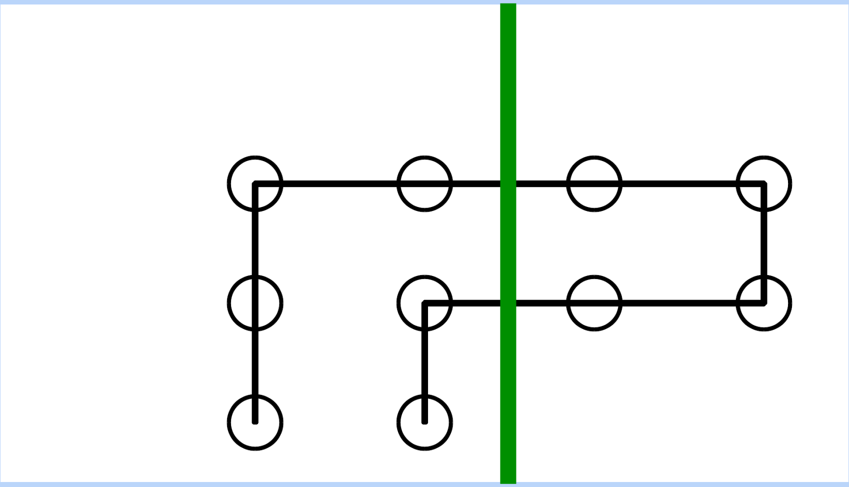
VERTICAL SYMMETRY

VERTICAL SYMMETRY



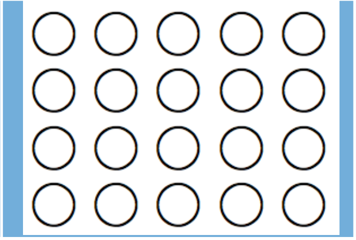
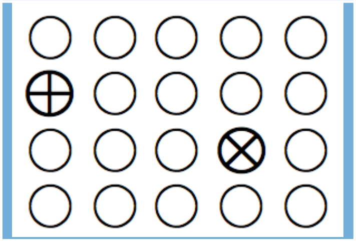
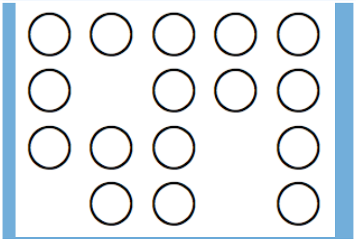
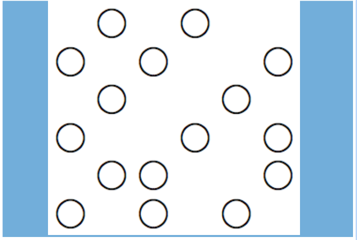
SYMMETRY SCORE

- For each possible vertical (or horizontal) axis:
  - Fold along the axis
  - Count number of password points that match on both sides of the fold
  - Divide by total number of password points
- Take maximum



0.8

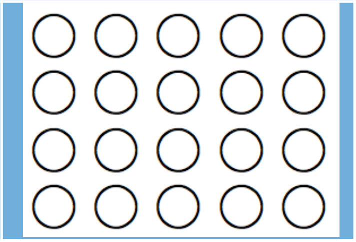
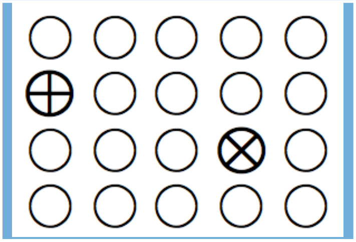
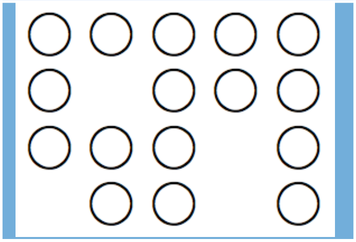
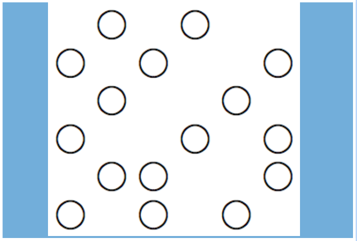
SYMMETRY SCORE
(HIGHER = MORE SYMMETRY)

				
Vertical	0.71 / 0.58	0.70 / 0.55	0.66 / 0.57	0.48 / 0.47
Horizontal	0.66 / 0.57	0.69 / 0.59	0.63 / 0.56	0.43 / 0.46

Values for uniformly random passwords calculated from 100,000 uniformly randomly generated samples of length 7.

SEARCH SPACE ESTIMATE

7-POINT PASSWORD

				
Theoretical	$2^{30.2}$	$2^{29.4}$	$2^{28.0}$	$2^{28.0}$
Point entropy	$2^{28.8}$	$2^{27.1}$	$2^{26.3}$	$2^{27.7}$
First + strokes	$2^{23.0}$	$2^{20.8}$	$2^{21.7}$	$2^{25.2}$

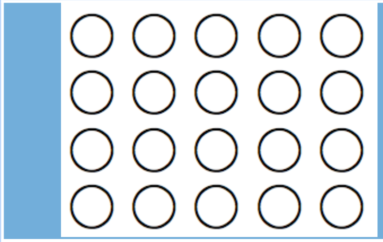
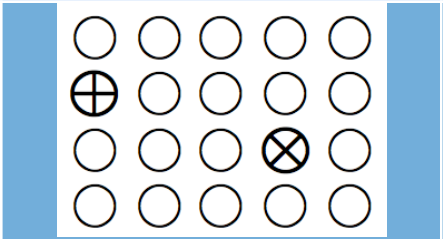
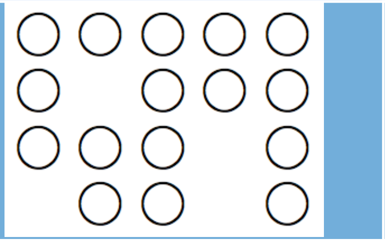
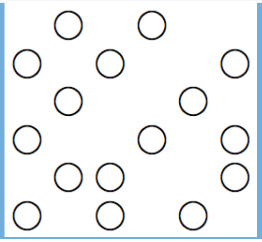
CONCLUSIONS

USABILITY AND SECURITY OF GAZE-BASED GRAPHICAL GRID PASSWORDS

1. Are Android-like graphical grid passwords usable with gaze-based entry?

2. How can we measure the security of graphical grid passwords?

SCHEME-SPECIFIC CONCLUSIONS

			
Generally good success rate, comparable with existing schemes			Lower success rate
Entry times comparable with existing schemes			
Best point entropy			
Bad first entropy Best last entropy		Best first entropy	
Okay stroke entropy			Best stroke entropy
			Most asymmetric
Best overall			

USABILITY AND SECURITY OF GAZE-BASED GRAPHICAL GRID PASSWORDS

MAJID ARIANEZHAD, DOUGLAS STEBILA, BEHZAD MOZAFFARI

USABILITY

- Our schemes generally competitive in terms of success rate and time.
- Difficult to compare gaze-based password schemes at present.

SECURITY

- Proposed metrics for graphical grid passwords:
  - first/last/all point entropy
  - stroke direction & length entropy
  - vertical/horizontal symmetry
- User-generated grid passwords often have poor first point and stroke entropy; some symmetry.
- Grid variants do not improve password quality very much.