

Can Unicorns Help Users Compare Crypto Key Fingerprints? (Supplementary Material)

ACTIVITY TUTORIAL

(hex version)

Scenario: Imagine that you work as an accountant at Print Idea Solutions and that your company is in the process of updating its employee database.

Your task is to retrieve the SSN for 30 different employees and enter them into the database.

Each employee will send you a message with his or her SSN.

Before you can read the chat message, you'll need to perform a security check. To ensure the chat session is secure, you will need to compare a pair of text strings, which are called "fingerprints."

[if compare-and-confirm] One fingerprint will be displayed on your computer. The other fingerprint is printed on the employee's business card, located on your desk. If these two fingerprints are the same, your chat session is secure. If they are different, your session is not secure; someone else could be eavesdropping on your communications.

[if compare-and-select] Three fingerprints will be displayed on your computer. Another fingerprint is printed on the employee's business card, located on your desk. If one of the fingerprints on your computer matches the one on the business card, your chat session is secure. If none match, your session is not secure; someone could be eavesdropping on your communications.

Check for differences in the letters or numbers shown. The font size and type do not matter.

[if compare-and-confirm] Since the two fingerprints shown here are the same, you should click the 'Same' button.

[if compare-and-select] Since the first fingerprint shown here matches the one on the business card, you should select it and click Continue.

After performing the security check, you will need to enter the information shown in the chatbox into the highlighted database field.

You may enter the SSN with or without dashes or spaces ("123-45-678," "12345678," and "123 45 678" are all valid). You

will need to manually type the SSN into the database, since copy/paste will not work.

For a \$1 bonus, complete your task both quickly and correctly. The 15% fastest participants with the fewest mistakes will receive an additional \$1 bonus.

This stopwatch will show you the current time to beat. Please note that beating this time does not guarantee the bonus; future participants may lower (or raise) the time to beat.

This is the end of the tutorial. If you need more practice, you can restart the tutorial. Otherwise, if you've got the hang of things, you may proceed to the actual activity.

POST-ACTIVITY SURVEY

Please fill out this short survey on the activity you just performed. At the end of the survey, you will receive a code that can be used for payment on Mechanical Turk.

Rank the following in terms of what you thought was most important while performing this activity (1 = most important): (dropdown containing 1-4)

- ☐ Responding to employees in the chatbox
- ☐ Completing the activity as fast as possible
- ☐ Entering the correct SSN into the database
- ☐ Correctly comparing [representation]s

What was the hardest thing about this activity?

[textbox]

The following questions ask about the [representation] comparisons you just made. We've included an example below, as a reminder:

[image of comparison dialog]

It was easy was to determine if [representation]s were the same or different.

- ☐ Strongly agree
- ☐ Agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Disagree
- ☐ Strongly disagree

The amount of time it took to compare [representation]s is reasonable for a security check.

- ☐ Strongly agree
- ☐ Agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Disagree
- ☐ Strongly disagree

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

CHI 2017 May 06-11, 2017, Denver, CO, USA

© 2017 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-4655-9/17/05.

DOI: <http://dx.doi.org/10.1145/3025453.3025733>

I feel confident that I could correctly compare [representation]s as a security check.

- ☐ Strongly agree
- ☐ Agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Disagree
- ☐ Strongly disagree

I was worried about incorrectly choosing “Same” when two [representation]s were different.

- ☐ Strongly agree
- ☐ Agree
- ☐ Neither agree nor disagree
- ☐ Disagree
- ☐ Strongly disagree

I was worried about incorrectly choosing “Different” when two [representation]s were the same.

- ☐ Strongly agree
- ☐ Agree
- ☐ Neither agree nor disagree
- ☐ Disagree
- ☐ Strongly disagree

[if missed attack]

You incorrectly answered the following security check.

<p>Security Check</p> <p>Please compare the following fingerprint to the one shown on the business card.</p> <p>562E C7BF 77C7 BA6E 8B3F 541E 0BB2 09B0 69EC 1973</p>	<p>PrintIdea Solutions</p> <p>Kristen Adair PR Coordinator 1011 Binary Gate New York, NY 212.555.1040 k.adair@printideas.com</p> <p>fingerprint: 562E BE4E 31C7 A3A0 763F 54CE 3331 A28F A3D0 D073</p>
---	---

Why do you think you failed to notice that the fingerprint shown on the business card did not match the one shown in the security check dialog?

[textbox]

[if caught attack]

You correctly answered the following security check.

[image of comparison dialog for attack instance]

What tipped you off that the fingerprint shown on the business card did not match the one shown in the security check dialog?

[textbox]

Please describe your strategy for comparing fingerprints to determine if they are the same or different.

[textbox]

What is the highest level of education you have completed?

- ☐ Elementary school only
- ☐ Some high school but did not finish
- ☐ Graduated from high school
- ☐ Some college but did not finish
- ☐ Two year college degree or A.A. or A.S.
- ☐ Four year college degree or B.A. or B.S.
- ☐ Some graduate school
- ☐ Graduate degree
- ☐ Prefer not to answer

What is your age (optional)?

What is your gender?

- ☐ Male
- ☐ Female
- ☐ Prefer not to answer

Which of the following best describes your primary occupation?

- ☐ Administrative Support (e.g. secretary, assistant)
- ☐ Art, Writing, or Journalism (e.g. author, reporter, sculptor)
- ☐ Business, Management, or Financial (e.g. manager, accountant, banker)
- ☐ Education or Science (e.g. teacher, professor, scientist)
- ☐ Legal (e.g. lawyer)
- ☐ Medical (e.g. doctor, nurse, dentist)
- ☐ Computer Engineering or IT Professional (e.g. programmer, IT consultant)
- ☐ Engineer in other field (e.g. Civil or bio engineer)
- ☐ Service (e.g. retail clerk, server)
- ☐ Skilled Labor (e.g. electrician, plumber, carpenter)
- ☐ Unemployed
- ☐ Retired
- ☐ College student
- ☐ Graduate student
- ☐ Prefer not to answer

Do you know any programming languages?

- ☐ Yes (list languages) [textbox]
- ☐ No

People often ask me for computer-related advice.

- ☐ Strongly agree
- ☐ Agree
- ☐ Neither agree nor disagree
- ☐ Disagree
- ☐ Strongly disagree

Did you encounter any technical issues while completing this HIT?


[textbox]

Please provide any additional feedback you have about this HIT.

[textbox]

ATTACKS

Here are the attacks used in our experiment. Attack #'s appearing in captions correspond to the attack IDs shown in Figure 4 of the paper.




Justin Macey
Research Staff

9874 Rose Corner
Los Angeles, CA
323.555.1414
j.macey@printideas.com

fingerprint:
B397 5A4F B744 8627 4832
E5C5 B754 119B 68C2 8690

B397 8206 ADFB 1C46 F832
E5C5 EF71 F4BE BB9D 8690

Figure 1: **hex**, confirm, bothvis, 2^{60} : Attack #1




Lindy Ibbott
Facility Manager

7332 Croft St
Los Angeles, CA
323.555.4929
libbott@printideas.com

fingerprint:
ED0B DF94 D8AC 02D9 537E
BFD9 9608 BCDA C639 5837

ED0B 02B4 8C89 F0B2 D37E
BFD9 8A60 44DB 1CE1 5837

Figure 2: **hex**, confirm, bothvis, 2^{60} : Attack #2



Kelley Macy
Accountant

100 Foggy Stead
Scranton, PA
570.555.2592
k.macy@printideas.com

fingerprint:
9FB1 469A B0CA 24B1 41C8
363F 8CEB 04C8 9A8A 5878

9FB1 40E1 A4E4 99DB B1C8
363F 98F5 ACC6 9C8E 5878

Figure 3: **hex**, confirm, bothvis, 2^{60} : Attack #3

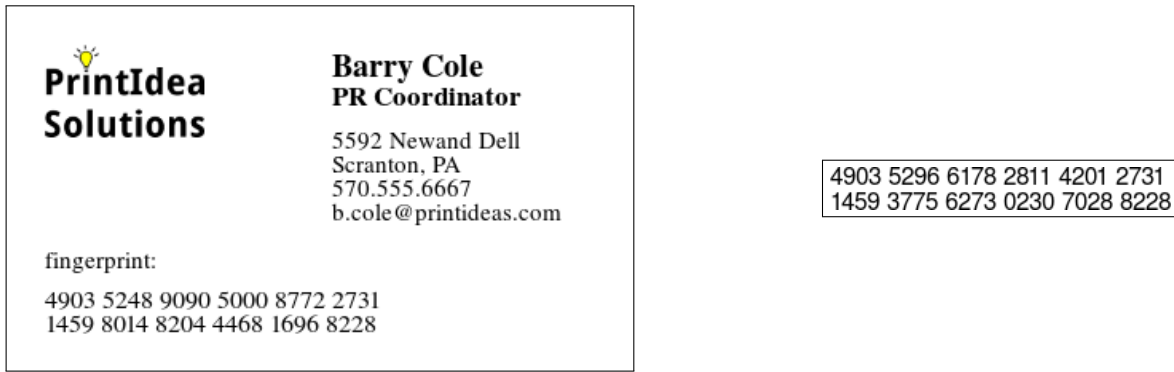


Figure 4: **num**, confirm, bothvis, 2^{60} : Attack #1

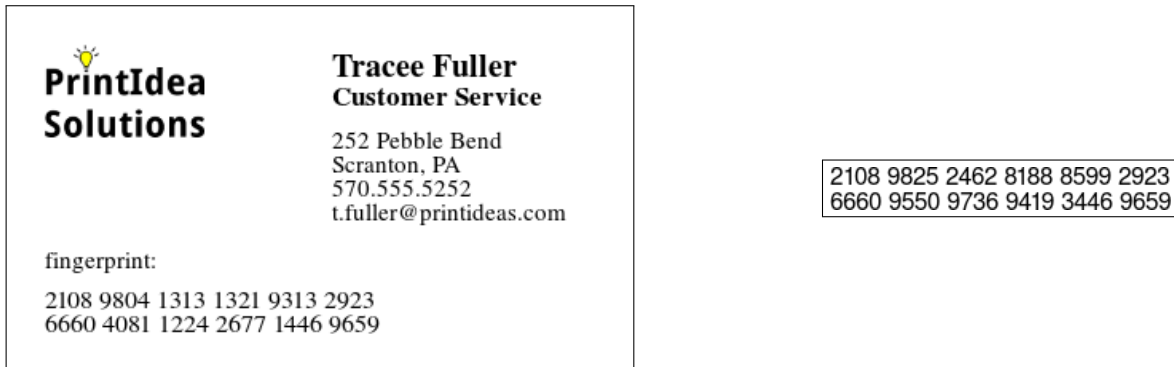


Figure 5: **num**, confirm, bothvis, 2^{60} : Attack #2



Figure 6: **num**, confirm, bothvis, 2^{60} : Attack #3


 <p>PrintIdea Solutions</p> <p>Kandace Brooke Accountant</p> <p>999 Lingwood Hill Scranton, PA 570.555.0012 k.brooke@printideas.com</p> <p>fingerprint: lura pihi lupa wotu nozu tuka caxe huhe mupo mano sero cuhi</p>	lura pihe qujo cifo doku tuka caxe roda juso wawa rato cuhi
--	--

Figure 7: **alt**, confirm, bothvis, 2⁶⁰: Attack #1


 <p>PrintIdea Solutions</p> <p>Annie Adkins Customer Service</p> <p>139 Holiday Plaza Austin, TX 512.555.4191 a.adkins@printideas.com</p> <p>fingerprint: seqa boxi mumu sina tiku pazi lunu hequ rove cuye zasu heve</p>	seqa bopa hova wexe hoku pazi lunu kidu qije ruli jaba heve
--	--

Figure 8: **alt**, confirm, bothvis, 2⁶⁰: Attack #2


 <p>PrintIdea Solutions</p> <p>Katey Ruggles Research Staff</p> <p>3823 Bepler Court Los Angeles, CA 323.555.1391 k.ruggles@printideas.com</p> <p>fingerprint: kuko lawe xavu vuse duso hiye muje noxa xuki foco haqu lemo</p>	kuko laco doxe yuqe xaja hiye muje gafu nuda gepi wuge lemo
---	--

Figure 9: **alt**, confirm, bothvis, 2⁶⁰: Attack #3

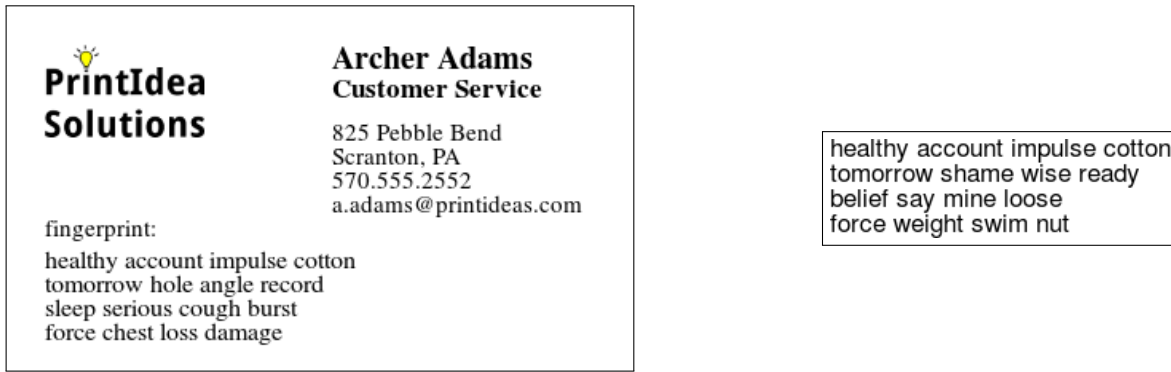


Figure 10: **word**, confirm, bothvis, 2^{60} , Attack #1

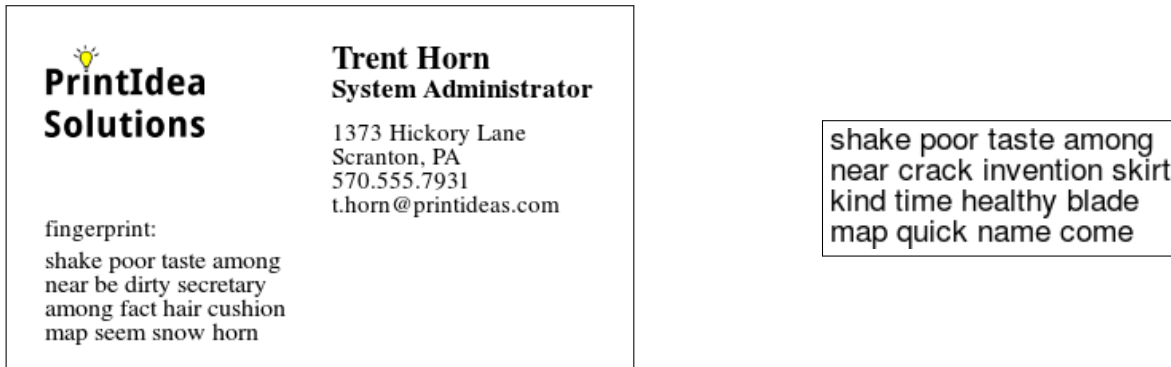


Figure 11: **word**, confirm, bothvis, 2^{60} : Attack #2

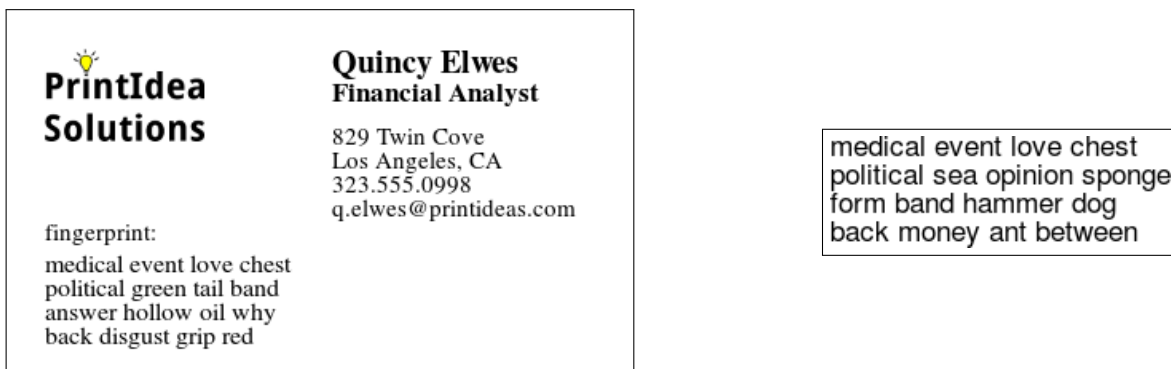



Figure 12: **word**, confirm, bothvis, 2^{60} : Attack #3




PrintIdea Solutions

fingerprint:
Your moon sleeps by her example round our spring.
My bent middle has beside her grip.
Your oven stops the hate kindly upon his quiet machine.

Mitch Russell
Data Analyst
939 Westwick Ave
New York, NY
212.555.7232
m.russell@printideas.com

Your moon sleeps by her example
round our poison.
Your deep milk pushes inside the
grip.
My fork prepares my profit darkly
into my clean danger.

Figure 13: **sent**, confirm, bothvis, 2⁶⁰: Attack #1




PrintIdea Solutions

fingerprint:
His glass returns on my foolish bread.
My broken damage hears.
Her pin wins our fork after our polish.
This late push lies to this time.

David Easom
Software Tester
777 Shady Dr
New York, NY
212.555.8589
d.easom@printideas.com

His glass returns on my foolish
woman.
My young window smiles.
Her payment loves my soup on his
circle.
Her rare produce shows my pain.

Figure 14: **sent**, confirm, bothvis, 2⁶⁰: Attack #2



PrintIdea Solutions

fingerprint:
This school pulls thickly inside his fixed bread.
This boiling lift rests inside this edge.
Your quick mine continues that night cruelly.
Her mind talks.

Colin Firmin
Project Manager
172 Snake Grove
Los Angeles, CA
323.555.1144
c.firmin@printideas.com

This school pulls thickly inside
his fixed shake.
The sticky picture visits from
that worm.
This sweet smash cries for our
brain flatly.
That clock sends.

Figure 15: **sent**, confirm, bothvis, 2⁶⁰: Attack #3

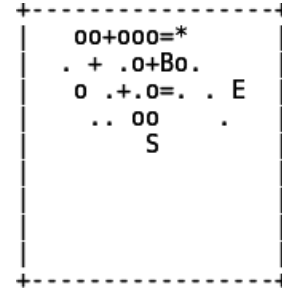
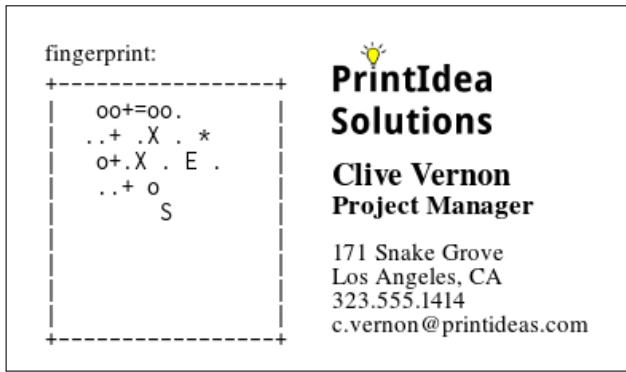


Figure 16: **ssh**, confirm, bothvis, 2⁶⁰: Attack #1

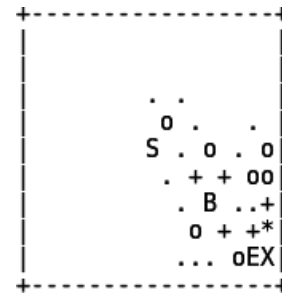
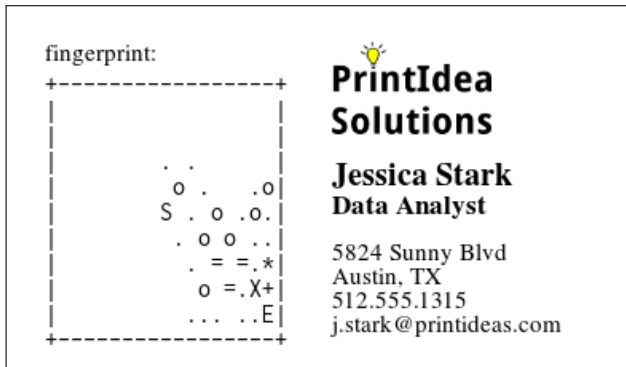


Figure 17: **ssh**, confirm, bothvis, 2⁶⁰: Attack #2

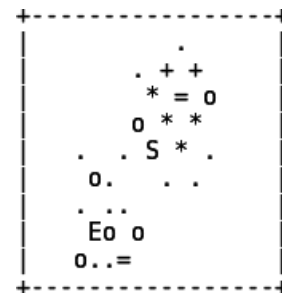
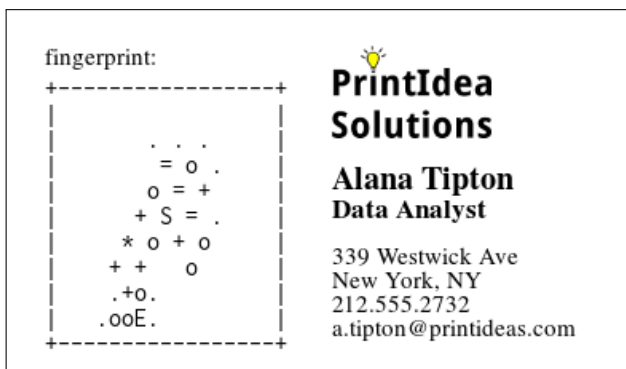


Figure 18: **ssh**, confirm, bothvis, 2⁶⁰: Attack #3

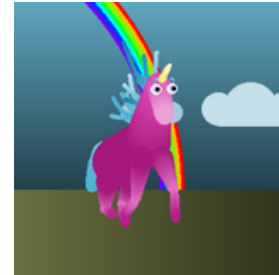
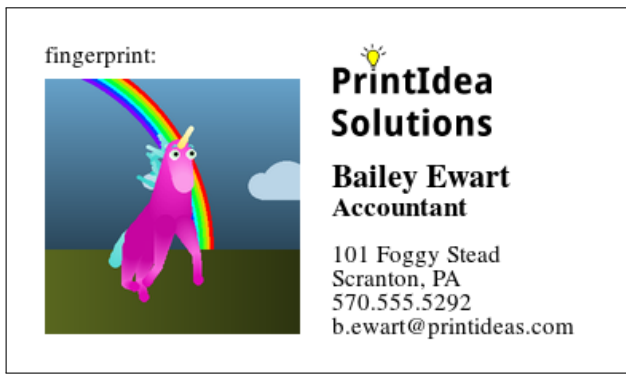


Figure 19: **uni**, confirm, bothvis, 2^{60} : Attack #1

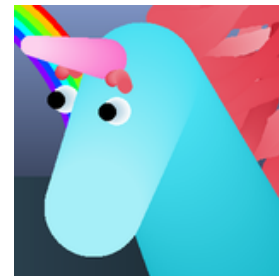
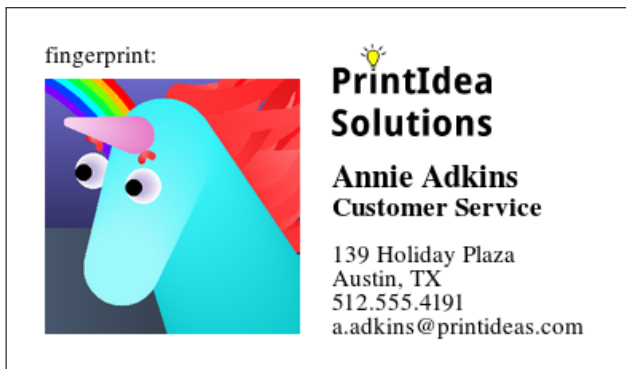


Figure 20: **uni**, confirm, bothvis, 2^{60} : Attack #2

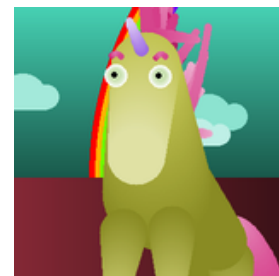


Figure 21: **uni**, confirm, bothvis, 2^{60} : Attack #3

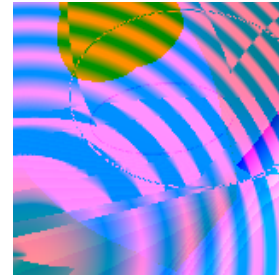


Figure 22: **vash**, confirm, bothvis, 2^{60} : Attack #1

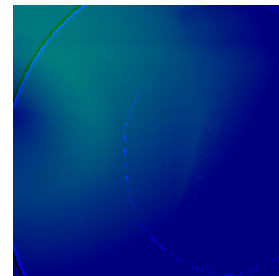


Figure 23: **vash**, confirm, bothvis, 2^{60} : Attack #2

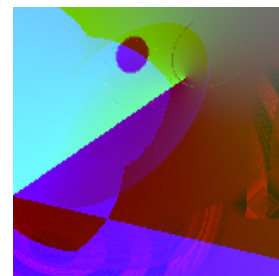


Figure 24: **vash**, confirm, bothvis, 2^{60} : Attack #3

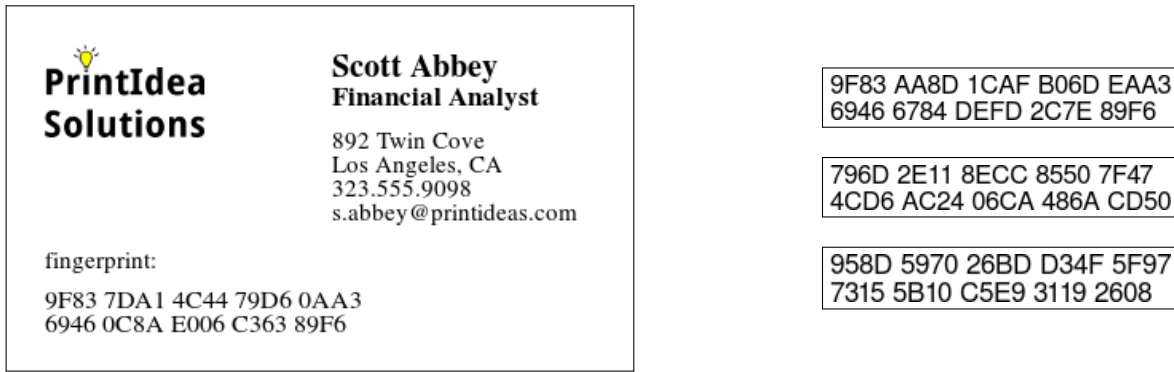


Figure 25: hex, **select**, bothvis, 2⁶⁰: Attack #1



Figure 26: hex, **select**, bothvis, 2⁶⁰: Attack #2

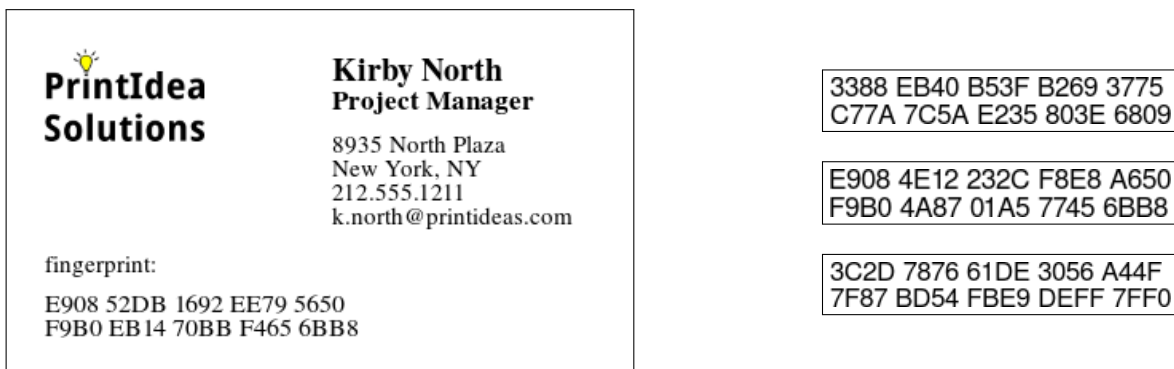


Figure 27: hex, **select**, bothvis, 2⁶⁰: Attack #3


 <p>PrintIdea Solutions</p> <p>fingerprint: 779A 27B8 B255 FA24 6348 5E50 27EF C218 AD38 BB6A</p>	<p>Kelley Macy Accountant</p> <p>100 Foggy Stead Scranton, PA 570.555.2592 k.macy@printideas.com</p>	<div style="border: 1px solid black; padding: 5px;"> 779A 54E2 BB80 EBF9 4348 5E50 8B9D 1FB9 8576 BB6A </div>
---	---	---

Figure 28: hex, confirm, **toggle**, 2^{60} : Attack #1


 <p>PrintIdea Solutions</p> <p>fingerprint: 0758 F88E 9EC4 367A 877C 3FCF 8BE8 F2EC 6677 8D88</p>	<p>Bailey Ewart Accountant</p> <p>101 Foggy Stead Scranton, PA 570.555.5292 b.ewart@printideas.com</p>	<div style="border: 1px solid black; padding: 5px;"> 0758 ECA0 45E4 C938 077C 3FCF 1BA0 B6C6 9FA2 8D88 </div>
---	---	---

Figure 29: hex, confirm, **toggle**, 2^{60} : Attack #2


 <p>PrintIdea Solutions</p> <p>fingerprint: 0E36 FE41 24D3 7F21 8E4C 25E8 7EDC 99AD 5639 C32E</p>	<p>Khloe Boon Facility Manager</p> <p>2240 Cinder Way Austin, TX 512.555.1841 k.boon@printideas.com</p>	<div style="border: 1px solid black; padding: 5px;"> 0E36 2A0A 565E 41B4 0E4C 25E8 5D19 D63C EF43 C32E </div>
---	--	---

Figure 30: hex, confirm, **toggle**, 2^{60} : Attack #3

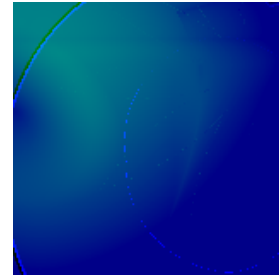


Figure 31: vash, confirm, **toggle**, 2^{60} : Attack #1

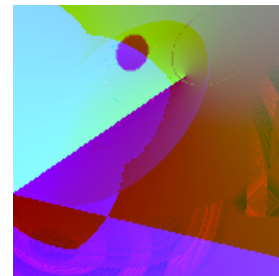


Figure 32: vash, confirm, **toggle**, 2^{60} : Attack #2

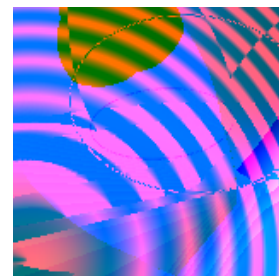



Figure 33: vash, confirm, **toggle**, 2^{60} : Attack #3



Trent Horn
System Administrator

1373 Hickory Lane
Scranton, PA
570.555.7931
t.horn@printideas.com

fingerprint:

BEA7 8728 4247 DA3F C89A
D11F 748A B3C5 EE40 4775

BEA7 A459 68C0 A368 AF9A
D173 7F38 541B E0DB C275

Figure 34: hex, confirm, bothvis, 2⁴⁰: Attack #1



Velma Vann
Data Analyst


399 Tryner Knoll
Los Angeles, CA
323.555.9681
v.vann@printideas.com

fingerprint:

7832 79B1 6224 A2F1 C9D0
9874 32D9 A42F 428A 7FE8

7832 A1ED 6070 6CFA 4AD0
98C5 E863 CAFA DF80 0CE8

Figure 35: hex, confirm, bothvis, 2⁴⁰: Attack #2



Judy Hayes
Software Tester

779 Shady Dr
New York, NY
212.555.8834
j.hayes@printideas.com

fingerprint:

999A ED8D AB99 9B2C A332
F875 AF68 2781 0092 7F72

999A 9419 12FE CC8C 4E32
F82F D0DF 7344 E15B 4A72

Figure 36: hex, confirm, bothvis, 2⁴⁰: Attack #3

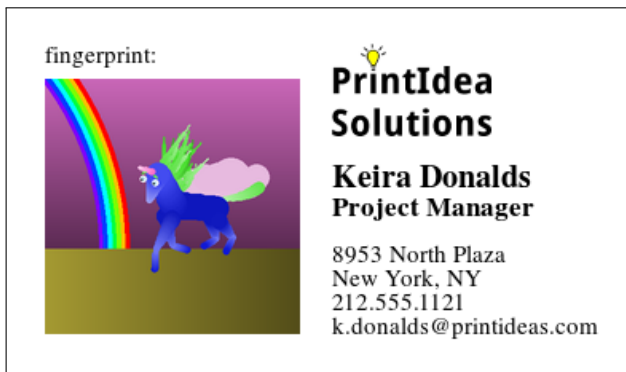


Figure 37: uni, confirm, bothvis, 2^{40} : Attack #1



Figure 38: uni, confirm, bothvis, 2^{40} : Attack #2



Figure 39: uni, confirm, bothvis, 2^{40} : Attack #3


 <p>Cheryl Gladwyn Accountant</p> <p>989 Lingwood Hill Scranton, PA 570.555.0102 c.gladwyn@printideas.com</p> <p>fingerprint:</p> <p>92E4 E5FB 78D4 1A86 E37E 4737 DC13 6E8B 2D0F 2923</p>	<div style="border: 1px solid black; padding: 5px; display: inline-block;"> 92E4 E5FB E7ED 6A12 E37E 4737 CFBF B2E2 FC71 2923 </div>
--	--

Figure 40: hex, confirm, bothvis, 2⁸⁰: Attack #1


 <p>Ashley Norwood Financial Analyst</p> <p>28602 Mardon Way New York, NY 212.555.1938 a.norwood@printideas.com</p> <p>fingerprint:</p> <p>AA12 9FE8 E588 5F0A 24DA 3216 26DD E266 C13C 5E06</p>	<div style="border: 1px solid black; padding: 5px; display: inline-block;"> AA12 9FE8 5C19 CD7E 24DA 3216 2E8D 048E B0D7 5E06 </div>
--	--

Figure 41: hex, confirm, bothvis, 2⁸⁰: Attack #2


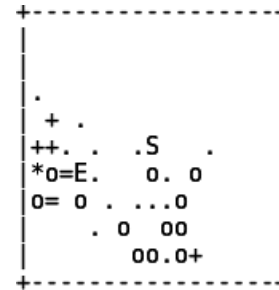
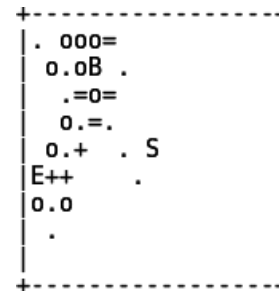
 <p>Bailey Ewart Accountant</p> <p>101 Foggy Stead Scranton, PA 570.555.5292 b.ewart@printideas.com</p> <p>fingerprint:</p> <p>F209 CCA4 C002 210D D469 858D F8D2 05D8 DFEC B506</p>	<div style="border: 1px solid black; padding: 5px; display: inline-block;"> F209 CCA4 7025 F2A9 D469 858D 7FB3 E414 766C B506 </div>
--	--

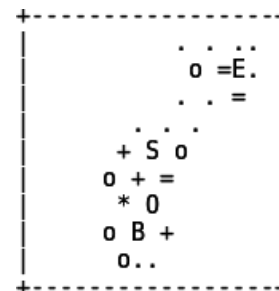
Figure 42: hex, confirm, bothvis, 2⁸⁰: Attack #3




17



17



17



Eppie Hollins
Research Staff


3832 Bepler Court
Los Angeles, CA
323.555.4293
e.hollins@printideas.com

0D94 D78C EDC0 F15E 6D35
981E 70EE F20D 4B62 5854

fingerprint:

0D94 3E0D 0DF3 CDC5 3D35
981E 2DBD 361B 973B 5854

Figure 46: hex, confirm, bothvis, 2^{60} , **2x time**: Attack #1



Kristen Adair
PR Coordinator

1011 Binary Gate
New York, NY
212.555.1040
k.adair@printideas.com

8046 67CD F3FC A6F5 8A35
CA6F 0231 7528 3FF1 1744

fingerprint:

8046 A21F 94BC 502B 2A35
CA6F F0BC B51B 0539 1744

Figure 47: hex, confirm, bothvis, 2^{60} , **2x time**: Attack #2



Velma Vann
Data Analyst


399 Tryner Knoll
Los Angeles, CA
323.555.9681
v.vann@printideas.com

918F 37D9 7E27 E78C 40A1
E811 C234 9003 FC8D 2A64

fingerprint:

918F 5CD3 A683 1DB2 80A1
E811 3547 034D 7090 2A64

Figure 48: hex, confirm, bothvis, 2^{60} , **2x time**: Attack #3



**PrintIdea
Solutions**

Kirby North
Project Manager


8935 North Plaza
New York, NY
212.555.1211
k.north@printideas.com

fingerprint:

527e e3a8 6af1 4fd2 d495
327b 41b6 8edb 3104 a7a3

527e 8d21 9f46 230e 6495
327b 96b1 4c2d e034 a7a3

Figure 49: **hex (low)**, confirm, bothvis, 2^{60} : Attack #1



**PrintIdea
Solutions**

Clive Vernon
Project Manager


171 Snake Grove
Los Angeles, CA
323.555.1414
c.vernon@printideas.com

fingerprint:

43ac 613f 06ec d258 172b
1dc0 ae30 ba89 c950 7572

43ac e842 7b01 6cd2 e72b
1dc0 1fa9 37e3 4d21 7572

Figure 50: **hex (low)**, confirm, bothvis, 2^{60} : Attack #2



**PrintIdea
Solutions**

Mable Bradford
PR Coordinator

5952 Newand Dell
Scranton, PA
570.555.6676
m.bradford@printideas.com

fingerprint:

6fff 2b34 bcaa 013b 6295
6c8a 0789 30e1 2d44 5869

6fff a27d f3bd 6c7b 2295
6c8a df77 8637 0494 5869

Figure 51: **hex (low)**, confirm, bothvis, 2^{60} : Attack #3