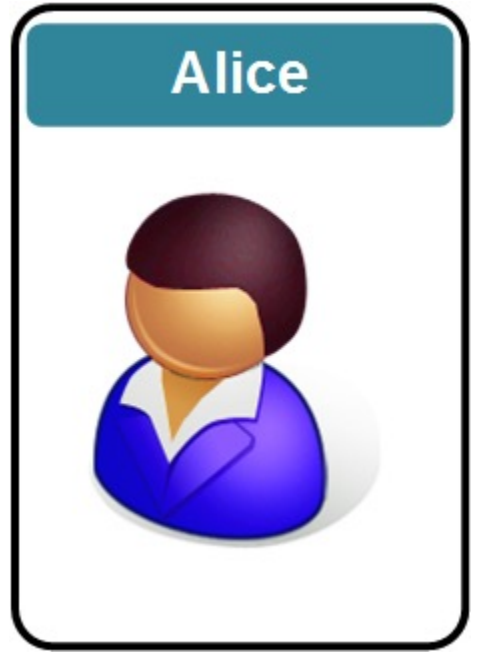
Pairing-based Cryptography and MIRACL



Prof Bill Buchanan OBE, Blockpass ID Lab

http://asecuritysite.com

BLOCKPASS IDENTITY LAB

World-leading Collaboration between
Blockpass IDN and Edinburgh Napier University

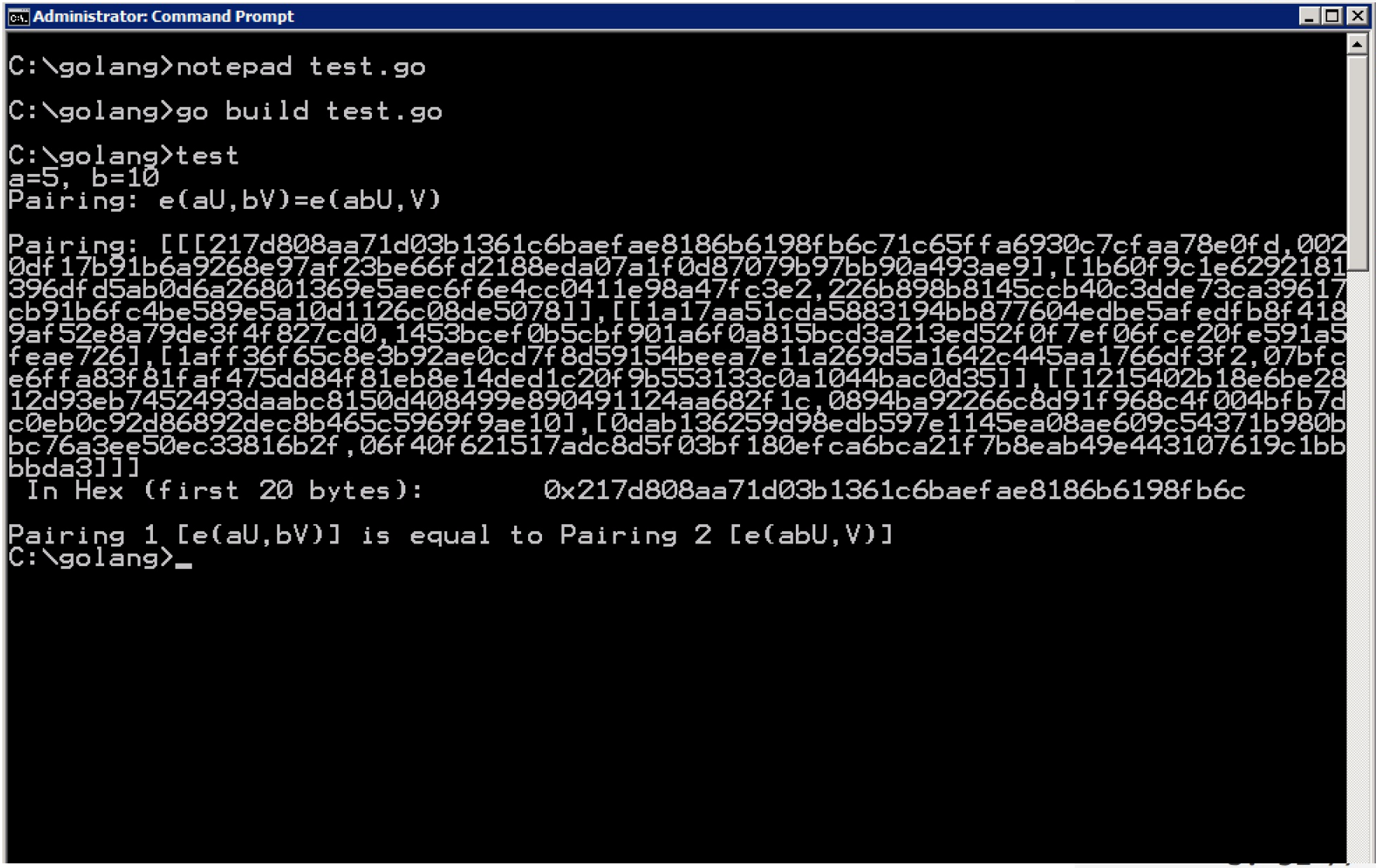
MIRACL

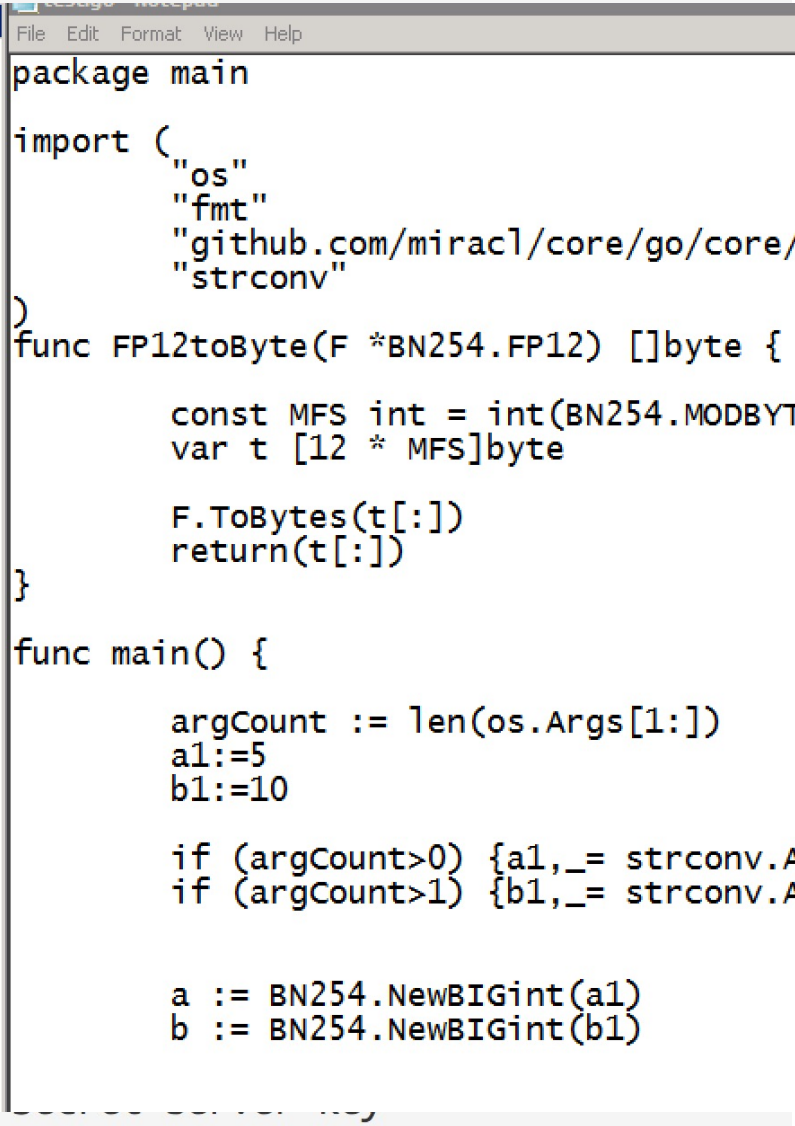
Multi-precision Integer and Rational Arithmetic Cryptographic

```
package main

import (

        "fmt"
```





Pair-based cryptography

- G_1 and G_2 be additive abelian groups. written additively.
- Let G_T be a multiplicatively cyclic group of order n.
- Pairing is e: G_1 x G_2 -> G_T.

Bi-linearity:

- $e(P,S+T) = e(P,S)e(P(T)$ $\quad P \in G_1, S,T \in G_2$
- $e(aP,bQ) = e(bP,aQ)$ $\quad a, b \in Z_n, P \in G_1, Q \in G_2$
- $e(aP,bQ) = e(abP,Q)$ $\quad a, b \in Z_n, P \in G_1, Q \in G_2$
- $e(aP,bQ) = e(P,Q)^{ab}$ $\quad a, b \in Z_n, P \in G_1, Q \in G_2$
- $e(-P,Q) = e(P,Q)^{-1} = e(P,-Q)$ $\quad P \in G_1, Q \in G_2$
- $e(P,0) = e(0,Q) = 1$ $\quad P \in G_1, Q \in G_2$

BLOCKPASS IDENTITY LAB

World-leading Collaboration between
Blockpass IDN and Edinburgh Napier University

Pair-based cryptography

e(aU,bV) = e(abU,V)

```
argCount := len(os.Args[1:])
a1:=5
b1:=10

if (argCount>0) {a1,_= strconv.Atoi(os.Args[1])}
if (argCount>1) {b1,_= strconv.Atoi(os.Args[2])}
```

```
a=10, b=50
Pairing: e(aU,bV)=e(abU,V)

Pairing:
[[[179ce13fbae0790fbe950c7ddc30022b21546157c1914ad427471573b56d261a,086e1f8bfd90a98081f32c80a78d5cda818ca5
489ad1ec74727596e89ee9e872],
[0a717cedabe82e50076be7ccaddba089f5ae2e37df96a0f33415d1d774173716,03bd5047eb80fdf0833ae2af947c14f6d9da5a9c
90ce2b7ede31ef2c35db4c4d]],
[[1de5331e039efbe6083067a9998eaaf843c14fcfbff5a479c49e736ecc1e134b,0320c31bdf277cbd8d8a06c3d6a4f86ab88f52b
5fcd251db0b63b4b532278f93],
[22fc417eee2ef1db9d9c1ad7a94cca6eea05a4d9c0388a807ce9b46b835d6301,22595df50a840cb7b903132780ed41a078d7424c
9c187651707595c1f37ebb95]],
[[000b1ad0b9f06cdfaa63611adc554dc9d2c3fbae4ddbb2698af426a2d460eb0e,079ef43d92f299e1db16990eb12ae9c20cc9fd3
7decf597fed087d15a2154599],
[2450da2a41f32159a5b32a769921b1ab8c8ef1a84d682ee539ad60077b4d835b,24ecae1301df4bbbc32eb1d76bcb06772fea7f52
3412ca455b5eb6b60965ab7a]]]
 In Hex (first 20 bytes):       0x179ce13fbae0790fbe950c7ddc30022b21546157

Pairing 1 [e(aU,bV)] is equal to Pairing 2 [e(abU,V)]
```

Pair-based cryptography

$e(aU,bV) = e(U,V)^{ab}$

```
argCount := len(os.Args[1:])
a1:=5
b1:=10

if (argCount>0) {a1,_= strconv.Atoi(os.Args[1])}
if (argCount>1) {b1,_= strconv.Atoi(os.Args[2])}

a := BN254.NewBIGint(a1)
```

```
a=10, b=50
Pairing: e(aU,bV)=e(U,V)^{ab}

Pairing:
[[[179ce13fbae0790fbe950c7ddc30022b21546157c1914ad427471573b56d261a,086e1f8bfd90a98081f32c80a78d5cda818ca5
489ad1ec74727596e89ee9e872],
[0a717cedabe82e50076be7ccaddba089f5ae2e37df96a0f33415d1d774173716,03bd5047eb80fdf0833ae2af947c14f6d9da5a9c
90ce2b7ede31ef2c35db4c4d]],
[[1de5331e039efbe6083067a9998eaaf843c14fcfbff5a479c49e736ecc1e134b,0320c31bdf277cbd8d8a06c3d6a4f86ab88f52b
5fcd251db0b63b4b532278f93],
[22fc417eee2ef1db9d9c1ad7a94cca6eea05a4d9c0388a807ce9b46b835d6301,22595df50a840cb7b903132780ed41a078d7424c
9c187651707595c1f37ebb95]],
[[000b1ad0b9f06cdfaa63611adc554dc9d2c3fbae4ddbb2698af426a2d460eb0e,079ef43d92f299e1db16990eb12ae9c20cc9fd3
7decf597fed087d15a2154599],
[2450da2a41f32159a5b32a769921b1ab8c8ef1a84d682ee539ad60077b4d835b,24ecae1301df4bbbc32eb1d76bcb06772fea7f52
3412ca455b5eb6b60965ab7a]]]

Pairing 1 [e(aU,bV)] is equal to Pairing 2 [e(U,V)^{ab}]
```

Pair-based cryptography

e(U1+U2,V) = e(U1,V) e(U2,V)

```
argCount := len(os.Args[1:])
a1:=5
b1:=10

if (argCount>0) {a1,_= strconv.Atoi(os.Args[1])}
```

```
U1=(0948d920900000006e8d13600000002184840000000004e9c0000000000009,17361ed1680000011460b070000000053cb4a
0000000000c4860000000000003)
U2=(2523648240000001ba344d8000000086121000000000013a700000000000012,000000000000000000000000000000000000000000
000000000000000000000000001)
V=([061a10bb519eb62feb8d8c7e8c61edb6a4648bbb4898bf0d91ee4224c803fb2b,0516aaf9ba737833310aa78c5982aa5b1f4d7
46bae3784b70d8c34c1e7d54cf3],
[021897a06baf93439a90e096698c822329bd0ae6bdbe09bd19f0e07891cd2b9a,0ebb2b0e7c8b15268f6d4456f5f38d37b09006ff
d739c9578a2d1aec6b3ace9b])

Pairing: e(U1+U2,V)=e(U1,V)*e(U2,V)

Pairing:
[[[1958eeeb60db1c8c2a63ad94e5f646dc8e94fdc32f11d8d02d26ddc8af9b0c06,0bc61719e86ad825f16d9d1f34aeb236fafcdd
3ff466841424597ace9aa67872],
[105d0c40559d5116162718c78586ffb7ca442170bd869176cb24cfbbd5225534,1d8e6c0d1f8404ba675711786a51599498981c0f
f11d3462a1f0e191b37b150b]],
[[139e5c34b4e2a31f3a1ac5bce7cb6782959a297d52682fb053aa115c1934941f,1f551b6ff6358b15a0cff575834549100c29de2
911c78f008f633d34b9546c36],
[24b3bd14fb0f222fe26755eea0de06935c6efef27ebb9153a27a74a1dab1d68b,033f1a5f2b484c0619eb14138cdc0b6d84ad24ba
846cca766afe61857661c843]],
[[01b5d285f3595e47bf663d15a1a6cd5601b9b104543228390742090c6fbe3e5f,088c77265783aabd1e2f4196826444f52463ff6
42e51813131e8a23551770d51],
[022e2e6d26fc832deafa732e9a78af49e1fc0be44c1a86cab5e7b90ddaedf800,239243673bfb2cbde4da1cd9f957e3b7f2a3f219
95eb69a382c085be4a18a6c2]]]
P1 e(U1+U2,V) Hex (first 20 bytes):     0x1958eeeb60db1c8c2a63ad94e5f646dc8e94fdc3
P2 e(U1,V)*e(U2,V) Hex (first 20 bytes):        0x1958eeeb60db1c8c2a63ad94e5f646dc8e94fdc3

Pairing 1 [e(U1+U2,V)] is equal to Pairing 2 [e(U1,V)*e(U2,V)]
```

```
,bV)] is equal to Pairing 2 [e(U,V)^{ab}]")}
ty")}
ty")}
```

Pair-based cryptography

e(aU1,bV) = e(bU,aV)

```
argCount := len(os.Args[1:])
a1:=5
b1:=10

if (argCount>0) {a1,_= strconv.Atoi(os.Args[1])}
if (argCount>1) {b1,_= strconv.Atoi(os.Args[2])}
```

```
a=10, b=50
Pairing: e(aU,bV)=e(bU,aV)

Pairing:
[[[179ce13fbae0790fbe950c7ddc30022b21546157c1914ad427471573b56d261a,086e1f8bfd90a98081f32c80a78d5cda818ca5
489ad1ec74727596e89ee9e872],
[0a717cedabe82e50076be7ccaddba089f5ae2e37df96a0f33415d1d774173716,03bd5047eb80fdf0833ae2af947c14f6d9da5a9c
90ce2b7ede31ef2c35db4c4d]],
[[1de5331e039efbe6083067a9998eaaf843c14fcfbff5a479c49e736ecc1e134b,0320c31bdf277cbd8d8a06c3d6a4f86ab88f52b
5fcd251db0b63b4b532278f93],
[22fc417eee2ef1db9d9c1ad7a94cca6eea05a4d9c0388a807ce9b46b835d6301,22595df50a840cb7b903132780ed41a078d7424c
9c187651707595c1f37ebb95]],
[[000b1ad0b9f06cdfaa63611adc554dc9d2c3fbae4ddbb2698af426a2d460eb0e,079ef43d92f299e1db16990eb12ae9c20cc9fd3
7decf597fed087d15a2154599],
[2450da2a41f32159a5b32a769921b1ab8c8ef1a84d682ee539ad60077b4d835b,24ecae1301df4bbbc32eb1d76bcb06772fea7f52
3412ca455b5eb6b60965ab7a]]]
 In Hex (first 20 bytes):       0x179ce13fbae0790fbe950c7ddc30022b21546157

Pairing 1 [e(aU,bV)] is equal to Pairing 2 [e(bU,aV)]
```

ID-based AKE (Authenticated Key Exchange)

```
PbobID:=10
PaliceID:=43
s:=31 // Secret server key

argCount := len(os.Args[1:])
```

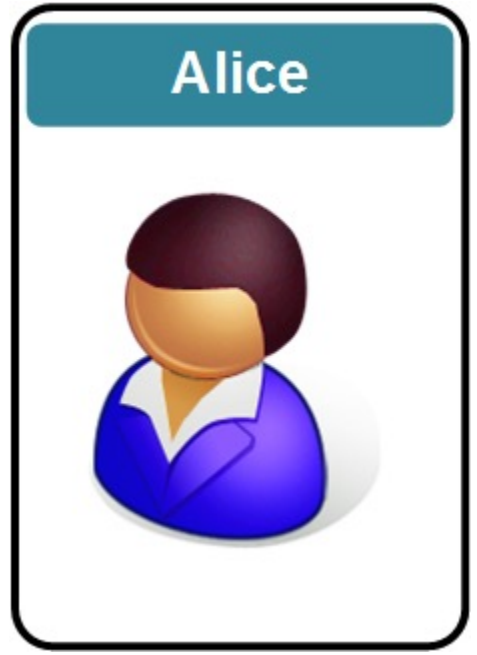
```
Bob ID: 10, Alice ID: 50, Secret: 99

Pairing:
[[[0418a239ce3b927fc5312a572bebb03f18a78925425cb6c6e007151f668a89db,15676e34a65895c9a5dbecf948b158c
d810e619190dc207e787eecf923698362],
[0b9e774125c980140322da2dbcde6045eed78463cdca0a9c41e086a871ae45ff,005e3e78a5448071b57df556d2c76f8d4
5ae48ac5c325217735d74aa7e9e897a]],
[[154d65ecc0ba2bd35043a402582ca6db60f298a4e1b4838ed507593654735ee4,2379aced78e6097fc2306ed4b2922504
67ea91369efd22220c466c787bda6a66],
[0706b1872913b025a53ad0d3e2b0d9a2eaffa6c3389e344cbc4a38f4474345af,0d21ad4bdb03f54ecfe4d87adbf3015ff
ae8fc40a965848665d7aab209feb117]],
[[010ecffc3e93f9b38516b80bfdcf177425cb09b84ffe1157e1cf4ff30cbc7b27,1fb44b3d76ea5938150c6b402bfe37b7
c08890b8ca324c532761bac0b60c9127],
[149afbbcc801cddec28e59c5029c38ff50b77835a8c6aa92df35eb487dc5fb3e,0725e2004c923cdc727637b194deb7d5f
83f0d127632eac8208633b8600ada5d]]]

Bob Key (first 20 bytes):       0x0418a239ce3b927fc5312a572bebb03f18a78925
Alice Key (first 20 bytes):     0x0418a239ce3b927fc5312a572bebb03f18a78925

Pairing 1 [e(id_b,pub_a)] is equal to Pairing 2 [e(id_a,pub_b)]
```

Pairing-based Cryptography and MIRACL



Prof Bill Buchanan OBE, Blockpass ID Lab

http://asecuritysite.com

BLOCKPASS IDENTITY LAB

World-leading Collaboration between
Blockpass IDN and Edinburgh Napier University