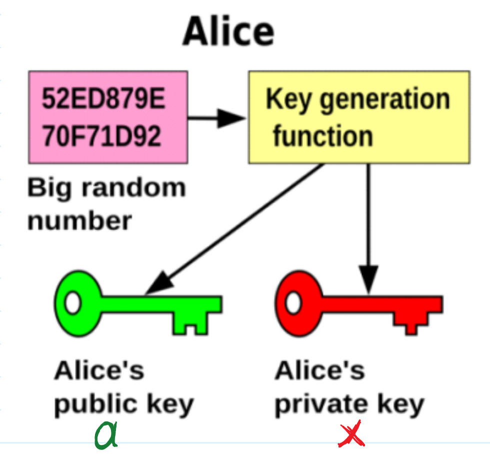
PKCS - Public Key Crypto System: 1.Key generation

$PP = (p, g)$



① $p = 2q+1$; p, q - are primes

$2 \mid p-1$ & $q \mid p-1$

p - strong prime

>> genstrongprime(ℓ)

$Z_p^* = \{1, 2, 3, \ldots, p-1\}$ *mod p

② g is generator iff

$g^2 \neq 1 \bmod p$ & $g^q \neq 1 \bmod p$

Public parameters $= (p, g) = PP$

$A: x \in_R Z_{p-1}$; $PrK_A = (x)$; $a = g^x \bmod p$: $PuK_A = (a)$

$x \leftarrow$ rand

$1 < m < p-1$: message to be encrypted : $m \in Z_p^*$.

$a_A = g^x \bmod p$ $\quad c = Enc(PuK_A, m) = (E, D)$

ElGamal Encryption

Zether: Towards Privacy in a Smart Contract World
Financial Cryptography and Data ..., 2020 - Springer

From <https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Zether%3A+Towards+Privacy+in+a+Smart+Contract+World&btnG=>

Benedikt Bunz1, Shashank Agrawal2, Mahdi Zamani3, and **Dan Boneh**4

1Stanford University, benedikt@cs.stanford.edu
2Visa Research, shaagraw@visa.com
3Visa Research, mzamani@visa.com
4**Stanford University**, dabo@cs.stanford.edu

Ctrl/F --> ElGamal --> Exact maths **21**

B : intends to encrypt message M to A.

$F_{encod}(M) = m$

$m \in Z_p^* \;;\; r \xleftarrow{rand} Z_{p-1}^* \;;$

$E = m * a^r \bmod p \;;\; D = g^r \bmod p \Rightarrow c = (E, D)$

$\mathcal{B}:$ $\xrightarrow{c=(E,D)}$ $\mathcal{A}:$ $PrK_A = (x)$

1. $H = D^{-x} = (g^r)^{-x} \bmod p =$
$= g^{-rx} \bmod p$

2. $m = E * H = m * a^r * g^{-rx} =$
$= m * (g^x)^r * g^{-rx} \bmod p =$
$= m * g^{xr} * g^{-xr} \bmod p =$
$= m * \bmod p = m$

since $1 < m < p-1$

Additively inverse element -***x*** to element ***x*** modulo ***p***-1.

D^{-x} mod ***p*** computation using Fermat theorem:
If ***p*** is prime, then for any integer ***a*** holds **$a^{p-1} = 1 \bmod p$**.

$$D^{-x} = D^{p-1-x} \bmod p$$

$D^{p-1} = 1 \bmod p \quad / D^{-x}$

$\underbrace{D^{p-1} \cdot D^{-x}} = 1 \cdot D^{-x} \bmod p \Rightarrow \underbrace{D^{p-1-x}} = D^{-x} \bmod p$

$\boxed{D^{-x} \bmod p = D^{p-x-1} \bmod p}$ // $p > x+1 \Rightarrow p-x-1 = d$

If $x < p-1 \rightarrow p-x-1 = u > 0$

```
>> d = mod_exp(g, r, p)   % d = g^r mod p
>> u = p - x - 1
>> dlmx = mod_exp(d, u, p)
```

Homomorphic encryption: cloud computation with encrypted data

$PP = (p, g)$

$\mathcal{B}: PuK_A = a;$ $\mathcal{A}: PrK_A = x;\ a = g^x \bmod p.$

Multiplicatively Homomorphic Encryption

$\mathcal{B}:$

m_1, m_2 - two messages to be encrypted: $1 < m_1, m_2 < p-1.$

$m_1: \quad r_1 \leftarrow randi(\mathbb{Z}_p^*)$

$$\left.\begin{array}{l} E_1 = m_1 * a^{r_1} \bmod p \\ D_1 = g^{r_1} \bmod p \end{array}\right\} \xrightarrow{c_1 = (E_1, D_1)} \mathcal{A}: \ Dec(x, c_1) = m_1$$

$m_2: \quad r_2 \leftarrow randi(\mathbb{Z}_p^*)$

$$\left.\begin{array}{l} E_2 = m_2 * a^{r_2} \bmod p \\ D_2 = g^{r_2} \bmod p \end{array}\right\} \xrightarrow{c_2 = (E_2, D_2)} \quad Dec(x, c_2) = m_2$$

$\mathcal{B}: \quad m = m_1 * m_2 \bmod p$

$\quad\quad r = (r_1 + r_2) \bmod (p-1)$

$$m: \left.\begin{array}{l} E = m * a^r \bmod p \\ D = g^r \bmod p \end{array}\right\} c = (E, D)$$

$\mathcal{A}:$

$$c_1 * c_2 \bmod p = (E_1, D_1) * (E_2, D_2) = (E_1 * E_2, D_1 * D_2) =$$
$$= (m_1 * m_2 * a^{r_1} * a^{r_2} \bmod p,\ g^{r_1} * g^{r_2} \bmod p) =$$
$$= (m * a^{(r_1 + r_2) \bmod p-1} \bmod p,\ g^{(r_1 + r_2) \bmod (p-1)} \bmod p) =$$
$$= (m * a^r \bmod p,\ g^r \bmod p) = c = (E, D)$$

Multiplicative homomorphic encryption means that encryption of multiplication $m_1 * m_2$ of two messages m_1, m_2 is equal to ciphertext c that is equal to the multiplication of two ciphertexts $c_1 * c_2$.

Fintex $\longrightarrow$ Blockchain

$$\boxed{m} \begin{matrix} \xrightarrow{m_1} \\ \xrightarrow{m_2} \end{matrix} \Big\} \; m_1 + m_2 = m \qquad \begin{matrix} c_1 = Enc^+(a, m_1) \\ c_2 = Enc^+(a, m_2) \end{matrix}$$

Property: everyone in the net could verify balance m:

e.g. $c_1 \cdot c_2 = c = Enc^+(a, m_1 + m_2) = Enc^+(a, m)$

Additively homomorphic encryption.

Let $\left.\begin{matrix} n_1 = g^{m_1} \bmod p \\ n_2 = g^{m_2} \bmod p \end{matrix}\right\}$ $n = n_1 * n_2 \bmod p = g^{m_1} * g^{m_2} \bmod p =$
$= g^{(m_1+m_2) \bmod (p-1)} \bmod p$

Since $DEF(m_1) = g^{m_1} \bmod p$ is 1-to-1 mapping:
for one m_1 corresponds one $DEF(m_1)$, then
$DEF(m_1 + m_2) = DEF(m) = n_1 * n_2 \bmod p = n \bmod p = g^m \bmod p.$

B:

n_1: $\left.\begin{matrix} E_1 = n_1 * a^{r_1} \bmod p \\ D_1 = g^{r_1} \bmod p \end{matrix}\right\} \xrightarrow{c_1 = (E_1, D_1)}$ A: $Dec^+(x, c_1) = n_1$

n_2: $\left.\begin{matrix} E_2 = n_2 * a^{r_2} \bmod p \\ D_2 = g^{r_2} \bmod p \end{matrix}\right\} \xrightarrow{c_2 = (E_2, D_2)}$ $Dec^+(x, c_2) = n_2$

$n = n_1 * n_2 \bmod p$; $r = (r_1 + r_2) \bmod (p-1)$.

n: $\left.\begin{matrix} E = n * a^r \bmod p \\ D = g^r \bmod p \end{matrix}\right\} \xrightarrow{c = (E, D)}$ $Dec^+(x, c) = n$

A: must find m_1 from equation $\left.\begin{matrix} g^{m_1} \bmod p = n_1 \\ g^{m_2} \bmod p = n_2 \end{matrix}\right\}$
m_2

Net: must verify balance

If p is secure $p \sim 2^{2048} \approx 10^{700}$, the find m_1, m_2, in general, is infeasible.

But! If $m_1, m_2 \sim 10^9$, then m_1, m_2 could be found

total scan procedure : search numbers from 1 to 10^9.
Sine A knows what sums should be received she simply verifies if $g^{m_1} \bmod p = n_1$
& $g^{m_2} \bmod p = n_2$.

Till this place

$m \in Z_p^*$; $r \in Z_{p-1}$; $\xrightarrow[\text{Ecryption}]{}$ $E \in Z_p^*$; $D = Z_p^*$

If $p = 11 \rightarrow Z_p^* = \{1, 2, 3, \ldots, 10\}$
$Z_{p-1} = \{0, 1, 2, \ldots, 9\}$ $|Z_p^*| = |Z_{p-1}|$

$Enc(m, r) = (E, D)$

$Enc : Z_p^* \times Z_{p-1} \longleftrightarrow Z_p^* \times Z_p^*$

one-to-one
isomorphism

m_1, m_2 : must be encrypted using $r_1 \xleftarrow{rand} Z_{p-1}$ & $r_2 \xleftarrow{rand} Z_{p-1}$

$m = m_1 * m_2$ $r = r_1 + r_2$

$$Enc(m) = c = (E, D) : \begin{cases} E = m_1 * m_2 * g^{r_1 + r_2} \bmod p \\ D = g^{r_1 + r_2} \end{cases}$$

$E = m \cdot g^r$; $E = g^r$.

Additively Homomorphic Encryption

ElGamal encryption. ElGamal encryption is a public key encryption scheme secure under the DDH assumption. A random number from $\mathbb{Z}_p^\star$, say x, acts as a private key, and $y = g^x$ is the public key corresponding to that. To encrypt an integer b, it is first mapped to one or more group elements. If $b \in \mathbb{Z}_p$, then a simple mapping would be to just raise g to b. Now, a ciphertext for b is given by $(g^b y^r, g^r)$ where $r \xleftarrow{\$} \mathbb{Z}_p^\star$. With knowledge of x, one can divide $g^b y^r$ by $(g^r)^x$ to recover g^b. However, g^b needs to be brute-forced to compute b.

$m \in Z_{p-1}$: $1 < m < p-1$

$E^+ = g^m * a^r \bmod p$; $D^+ = g^r \bmod p$

$E = m * a^r \bmod p$; $D = g^r \bmod p$

$D^+ = D$

$$C^+ = (E^+, D^+)$$

B: $\xrightarrow{C^+}$ A: $PrK_A = x$

1. Compute $(D^+)^{-x} * g^{-rx} \bmod p$

2. $E^+ * (D^+)^{-x} \bmod p = g^m$

Decrypted message is in the form of $\tilde{m} = \underbrace{g^m \bmod p}$

$d\log_g(\tilde{m}) = d\log_g(g^m \bmod p) = m$. discrete exp function DEF

If p is large, e.g. $p \sim 2^{2048}$, i.e. $|p| = 2048$ bits

Then computation of $d\log_g(\tilde{m})$ – is infeasible !

Since according to the complexity assumptions of
Discrete Logarithm Function
Discrete Logarithm Assumption – DLA

We argue that this is not an issue. First, as we will see, the Zether smart contract does not need to do this, only the users would do it. Second, users will have a good estimate of ZTH in their accounts because, typically, the transfer amount is known to the receiver. Thus, brute-force computation would occur only rarely. Third, one could represent a large range of values in terms of smaller ranges. For instance, if we want to allow amounts up to 64 bits, we could instead have 2 amounts of 32 bits each, and encrypt each one of them separately. In this paper, for simplicity, we will work with a single range, 1 to MAX, and set MAX to be 2^{32} in the implementation.

$2^{10} = 1024 = 1K$; $2^{20} = 1M$; $2^{30} = 1G$; $2^{40} = 1T$; $2^{50} = 1P$
$\sim 10^3$ $\sim 10^6$ $\sim 10^9$ $\sim 10^{12}$ $\sim 10^{15}$

$2^{64} = 2^{14} \cdot 2^{50} = 2^{14} \cdot 1P$
$\sim 8192 \cdot 10^{15}$

$$\begin{array}{r} 4096 \\ 2 \\ \hline 8192 \end{array}$$

2^{2048} : $64 << 2048$.

Ethereum crypto currency $1 \, Eth = 10^{18}$ gas
$1 \, Eth \sim 400 \$$

$1T \, Eth \equiv 2^{40}$

ElGamal encryption.
ElGamal encryption is a public key encryption scheme secure under the DDH assumption.
A random number from $\boldsymbol{Z_p}$, say $\boldsymbol{x}$, acts as a private key, and $\boldsymbol{a} = \boldsymbol{g^x}$ ***mod p*** the public key corresponding to that.
To encrypt an integer m in $\boldsymbol{Z_{p-1}}$, it is first mapped to one or more elements of $\boldsymbol{Z_p}^*$.
If $\boldsymbol{m}$ is in $\boldsymbol{Z_p}^*$, then a simple mapping would be to just raise $\boldsymbol{g}$ to $\boldsymbol{m}$.
Now, a ciphertext for $\boldsymbol{m}$ is given by ($\boldsymbol{g^m a^r}$), where $\boldsymbol{r}$ is chosen at random from $\boldsymbol{Z_{p-1}}$.
With knowledge of $\boldsymbol{x}$, one can divide $\boldsymbol{g^m a^r}$ by $(\boldsymbol{g^r})^{\boldsymbol{x}}$ to recover $\boldsymbol{g^m}$.

However, gb needs to be brute-forced to compute b.
We argue that this is not an issue. First, as we will see, the Zether smart contract does not need to do this, only the users would do it. Second, users will have a good estimate of ZTH in their accounts because, typically, the transfer amount is known to the receiver. Thus, brute-force computation would occur only rarely. Third, one could represent a large range of values in terms of smaller ranges. For instance, if we want to allow amounts up to 64 bits, we could instead have 2 amounts of 32 bits each, and encrypt each one of them separately. In this paper, for simplicity, we will work with a single range, 1 to MAX, and set MAX to be 232 in the implementation.

$2^{64} = \underbrace{2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8}$

$dlog_g(\tilde{m})$ - - - - $dlog_g(\tilde{m}) = m$

$PP = (p, g)$; $|p| \sim 2^8$; $|g| \sim 2^8$ search area
256 $\quad 256 \leftarrow$ choices
$|p| = 8$ bits $\quad |g| = 8$ bits

256 256 choices

$|p| = 8$ bits $|g| = 8$ bits

Ethereum: gas - price for computation of smart contract.

Search area is 1 - 16