Private Comparison

Chloé Hébant[1], Cedric Lefebvre[2], Étienne Louboutin[3], Elie Noumon Allini[4], Ida Tucker[5]

[1]École Normale Supérieure, CNRS, PSL University

[2]IRIT

[3]Chair of Naval Cyber Defense, IMT Atlantique, IRISA, UBL, Brest, France

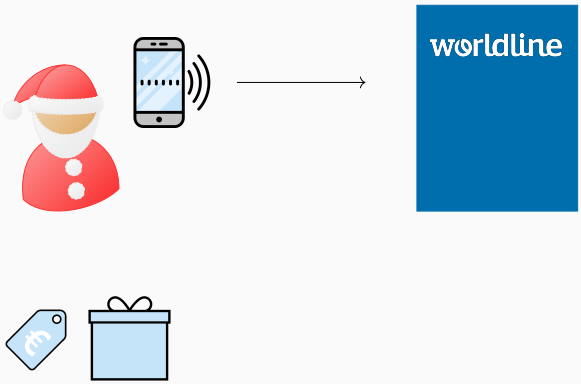
[4]Univ Jean Monnet, Lab. Hubert Curien, Saint-Étienne, France

[5]Univ Lyon, CNRS, ENS de Lyon, INRIA, LIP Lyon, France

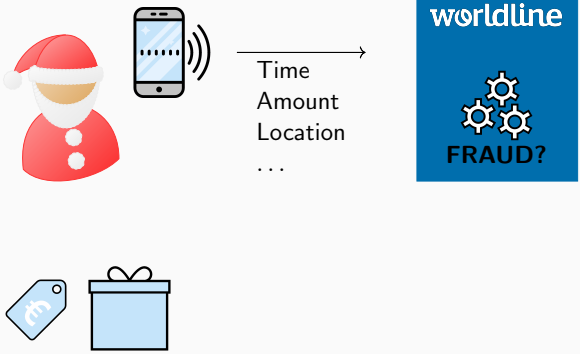
Rencontres Entreprises DOCtorants Sécurité 2018

Scenario

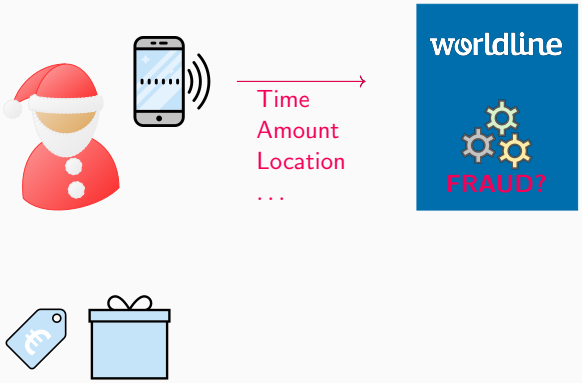
Scenario



Scenario



Scenario



Goal: Detect **FRAUD** in $< 200ms$

Scheme

Private input: $x_1, \ldots, x_n$

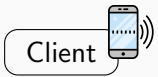
Server

worldline
e-payment services

Private inputs:

- Indv. thresholds: $t_1, \ldots, t_n$
- Weights: $\alpha_1, \ldots, \alpha_n$
- Total threshold: T

Scheme



Private input: $x_1, \ldots, x_n$

Server worldline e-payment services

Private inputs:

- Indv. thresholds: $t_1, \ldots, t_n$
- Weights: $\alpha_1, \ldots, \alpha_n$
- Total threshold: T

Interactive Protocol

Scheme

Private input: $x_1, \ldots, x_n$

Server worldline e-payment services

Private inputs:

Indv. thresholds: $t_1, \ldots, t_n$

Weights: $\alpha_1, \ldots, \alpha_n$

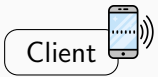
Total threshold: T

Interactive Protocol

Output: $[\sum_{i=1}^{n} \alpha_i [x_i > t_i] > T]$

$[x > t] = 1$ if $x > t$ and 0 otherwise

Scheme



Private input: $x_1, \ldots, x_n$

Server worldline e-payment services

Private inputs:

Indv. thresholds: $t_1, \ldots, t_n$

Weights: $\alpha_1, \ldots, \alpha_n$

Total threshold: T

Interactive Protocol

Output: $[\sum_{i=1}^{n} \alpha_i [x_i > t_i] > T]$

$[x > t] = 1$ if $x > t$ and 0 otherwise

Server only learns if a fraud occurred

Client learns nothing

Security Model

Sec. w.r.t. Server

Server does not learn:

- individual comparisons
- individual x_i's
- sum of weighed comparisons

Sec. w.r.t. Client

Client does not learn:

- weights α_i
- individual thresholds t_i
- total threshold T

Assumption on Client

Client is honest but curious:

- Follows the protocol honestly
- Tries to learn more than his inputs

Secure against honest but curious:

- Learns nothing beyond his inputs

Outline

Unsuccessful Ideas

Garbled Circuits

Idea: large garbled circuit containing sub circuits for individual comparisons.

Garbled Circuits

Idea: large garbled circuit containing sub circuits for individual comparisons.

+ Secure equality test or comparison
+ Communication-efficient
− Too slow!

Fully Homomorphic Encryption

Properties

- Absorption : $\mathsf{E}(x) * \alpha = \mathsf{E}(x * \alpha)$
- Addition : $\mathsf{E}(x) + \mathsf{E}(y) = \mathsf{E}(x + y)$
- Multiplication : $\mathsf{E}(x) * \mathsf{E}(y) = \mathsf{E}(x * y)$

Security

- Indistinguishable ciphertexts

PIR : Private Information Retrieval

$PIR(x, D)$

- The client sends $Q = (\mathrm{E}(q_0), ..., \mathrm{E}(q_l))$
- $q_x = 1$, $q_{k \neq x} = 0$
- The server computes the PIR with $D = (d_0, ..., d_l)$

PIR : Private Information Retrieval

$$
\begin{aligned}
d_1 \times \boxed{\mathrm{E}(0)} &= \boxed{\mathrm{E}(0)} \\
d_2 \times \boxed{\mathrm{E}(0)} &= \boxed{\mathrm{E}(0)} \quad + \\
d_3 \times \boxed{\mathrm{E}(1)} &= \boxed{\mathrm{E}(d_3)} \quad + \\
d_4 \times \boxed{\mathrm{E}(0)} &= \boxed{\mathrm{E}(0)} \quad + \quad \rightarrow \boxed{\mathrm{E}(0+0+d_3+0+0+0)} \\
d_5 \times \boxed{\mathrm{E}(0)} &= \boxed{\mathrm{E}(0)} \quad + \\
d_6 \times \boxed{\mathrm{E}(0)} &= \boxed{\mathrm{E}(0)} \quad +
\end{aligned}
$$

Three-party Solution

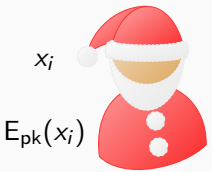
worldline

t_i, α_i

T

sk, pk

Three-party Solution



$$n\times\ \mathsf{PIR}(x_i, b_i)$$

worldline

t_i, α_i

T

$$b_i = \left(b_i^j\right)_{1\leq j\leq 2^{|x_i|}} = \begin{cases} 0 & \text{if } j < t_i \\ \alpha_i & \text{otherwise} \end{cases}$$

sk, pk

Three-party Solution

x_i

$\mathsf{E}_{\mathsf{pk}}(x_i)$

$n\times$ PIR(x_i, b_i)

worldline

t_i, α_i

T

$$C := \mathsf{E}_{\mathsf{pk}}\left(\sum_{i=1}^{n} \alpha_i[x_i > t_i] - T\right)$$

$$b_i = \left(b_i^j\right)_{1\le j\le 2^{|x_i|}} = \begin{cases} 0 & \text{if } j < t_i \\ \alpha_i & \text{otherwise} \end{cases}$$

sk, pk

Three-party Solution

x_i

$\mathsf{E}_{\mathsf{pk}}(x_i)$

$n\times$ PIR(x_i, b_i)

worldline

t_i, α_i

T

$$C := \mathsf{E}_{\mathsf{pk}}\left(\sum_{i=1}^{n} \alpha_i[x_i > t_i] - T\right)$$

$$b_i = \left(b_i^j\right)_{1\le j\le 2^{|x_i|}} = \begin{cases} 0 & \text{if } j < t_i \\ \alpha_i & \text{otherwise} \end{cases}$$

sk, pk

$\mathsf{D}_{\mathsf{sk}}(C)$

Three-party Solution

x_i

$\mathsf{E}_{\mathsf{pk}}(x_i)$

$n\times$ PIR(x_i, b_i)

worldline

t_i, α_i

T

$$C := \mathsf{E}_{\mathsf{pk}}\left(\sum_{i=1}^{n} \alpha_i[x_i > t_i] - T\right)$$

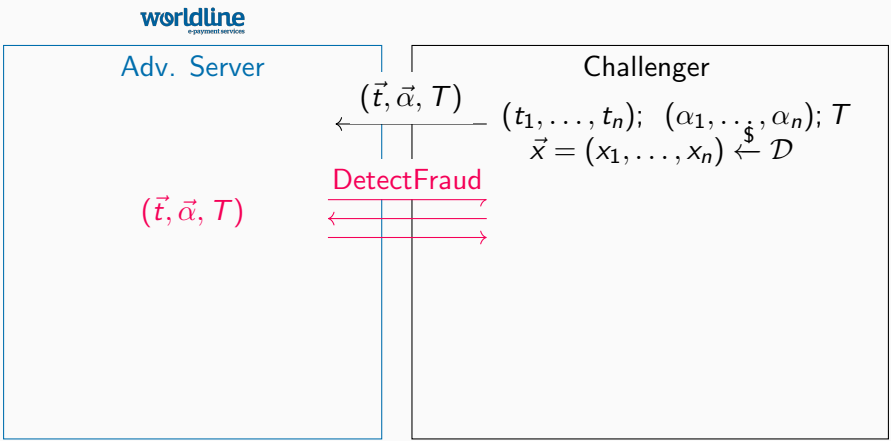
$$b_i = \left(b_i^j\right)_{1\le j\le 2^{|x_i|}} = \begin{cases} 0 & \text{if } j < t_i \\ \alpha_i & \text{otherwise} \end{cases}$$

sk, pk

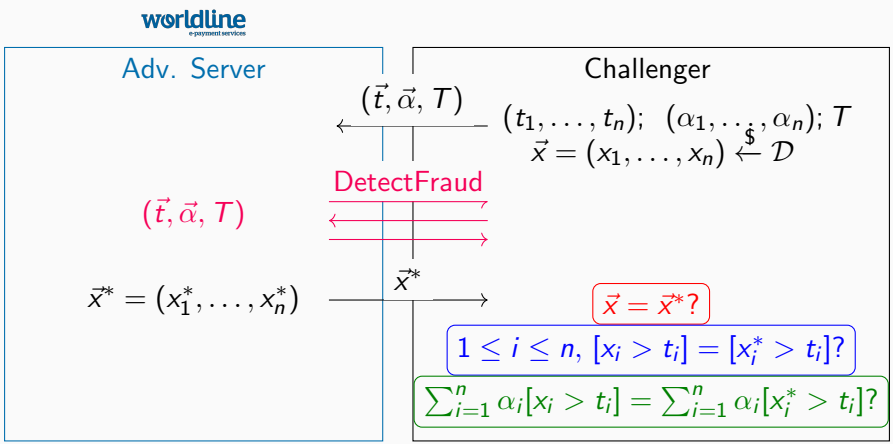
$\mathsf{D}_{\mathsf{sk}}(C)$

Retained Solutions

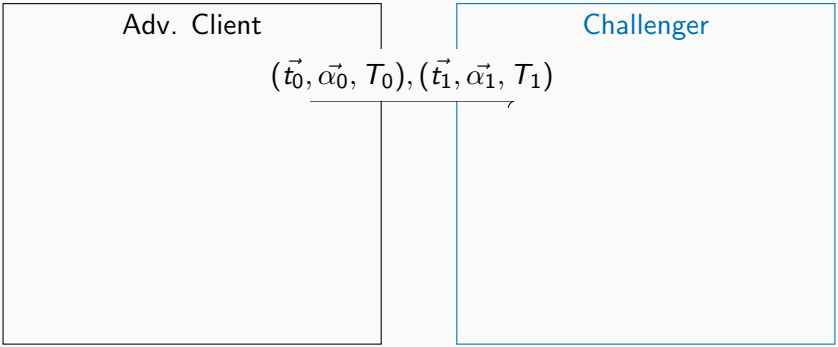
Security with Respect to the Server



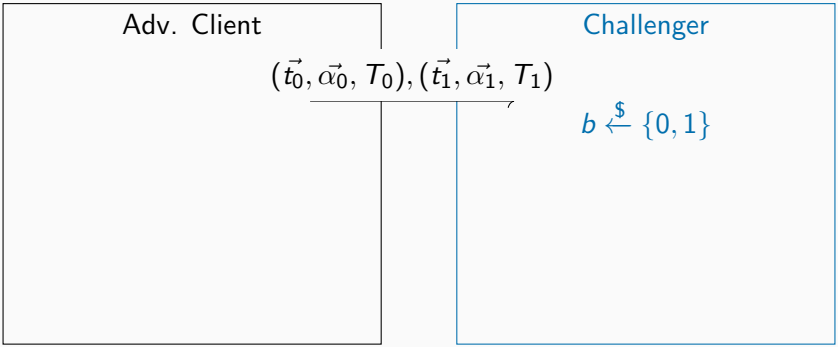
Security with Respect to the Server



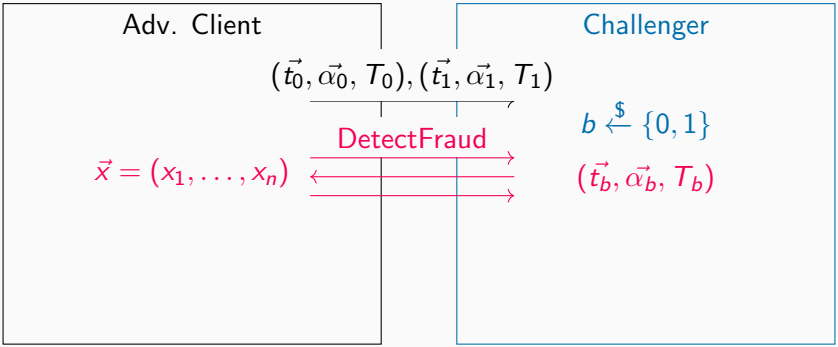
Security with Respect to the Client



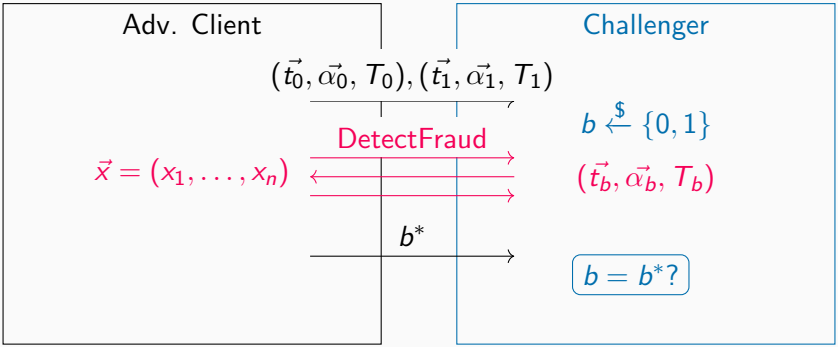
Security with Respect to the Client



Security with Respect to the Client



Security with Respect to the Client



Somewhat Homomorphic Encryption

Ring Learning With Error

- Noise hides secret
- Noise growth : Addition $=$, Absorption $+$, Multiplication $++$

Example

- Secret : p, large random : q, small random r
- Encrypt binary m : $c = q \cdot p + 2 \cdot r + m$
- Decrypt : $m = (c \mod p) \mod 2$

Example

- If $r > p$ decryption fails
- Addition : $c_1 + c_2 = p \cdot (q_1 + q_2) + 2 \cdot (r_1 + r_2) + m_1 + m_2$
- Multiplication :
  $c_1 * c_2 = p \cdot (c_2 q_1 + c_1 q_2 - q_1 q_2) + 2 \cdot (2 r_1 r_2 + m_1 r_2 + m_2 r_1) + m_1 \cdot m_2$

Parameters

- Plaintext Modulus : p
- Ciphertext Modulus : q
- Ring : $\mathbb{Z}_p[X]/(X^n + 1)$

Link

- Security : $+$ when $n+$, $-$ when $q+$
- Batching : $m_2X^2 + m_1X^1 + m_0$
- p prime, $p = 1 \mod (2n)$

Koda

$x_1, \ldots, x_n$

worldline
e-payment services

Server pk, sk

$t_1, \ldots, t_n, \alpha_1, \ldots, \alpha_n, T$

Koda

worldline
e-payment services

Server pk, sk

$t_1, \ldots, t_n, \alpha_1, \ldots, \alpha_n, T$

$$
\begin{array}{l}
\mathsf{E}_{\mathsf{pk}}(0) \\
\cdots \\
\mathsf{E}_{\mathsf{pk}}(0) \\
\mathsf{E}_{\mathsf{pk}}(\alpha_i) \quad \leftarrow t_i, i \in \{1, \cdots, n\} \\
\cdots \\
\mathsf{E}_{\mathsf{pk}}(\alpha_i) \\
C_T \coloneqq \mathsf{E}_{\mathsf{pk}}(T)
\end{array}
$$

Koda

worldline
e-payment services

Server pk, sk

$t_1, \ldots, t_n, \alpha_1, \ldots, \alpha_n, T$

$\mathsf{E}_{\mathsf{pk}}(0)$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(0)$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i) \quad \leftarrow t_i, i \in \{1, \cdots, n\}$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i)$
$C_T \coloneqq \mathsf{E}_{\mathsf{pk}}(T)$

Koda

worldline
e-payment services

Server pk, sk

$t_1, \ldots, t_n, \alpha_1, \ldots, \alpha_n, T$

$\mathsf{E}_{\mathsf{pk}}(0)$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(0)$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i) \quad \leftarrow t_i, i \in \{1, \cdots, n\}$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i)$
$C_T \coloneqq \mathsf{E}_{\mathsf{pk}}(T)$

$\longleftarrow$

For all i, select the x_ith
$C_i \coloneqq \mathsf{E}_{\mathsf{pk}}(\alpha_i[x_i > t_i])$
$r > 0, \quad C = (\sum_{i=1}^{n} C_i - C_T) \cdot r$

Koda

$x_1, \ldots, x_n$

worldline
e-payment services

Server pk, sk

$t_1, \ldots, t_n, \alpha_1, \ldots, \alpha_n, T$

$\mathsf{E}_{\mathsf{pk}}(0)$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(0)$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i) \quad \leftarrow t_i, i \in \{1, \cdots, n\}$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i)$
$C_T \coloneqq \mathsf{E}_{\mathsf{pk}}(T)$

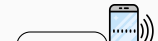
For all i, select the x_ith $\longleftarrow$

$C_i \coloneqq \mathsf{E}_{\mathsf{pk}}(\alpha_i[x_i > t_i])$

$r > 0, \quad C = (\sum_{i=1}^{n} C_i - C_T) \cdot r \longrightarrow$

$\mathsf{D}_{\mathsf{sk}}(\lceil C \rfloor)$

Koda



$x_1, \ldots, x_n$

worldline
e-payment services

Server pk, sk

$t_1, \ldots, t_n, \alpha_1, \ldots, \alpha_n, T$

$\mathsf{E}_{\mathsf{pk}}(0)$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(0)$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i) \quad \leftarrow t_i, i \in \{1, \cdots, n\}$
$\cdots$
$\mathsf{E}_{\mathsf{pk}}(\alpha_i)$
$C_T \coloneqq \mathsf{E}_{\mathsf{pk}}(T)$

For all i, select the x_ith $\longleftarrow$

$C_i \coloneqq \mathsf{E}_{\mathsf{pk}}(\alpha_i[x_i > t_i])$

$r > 0, \quad C = (\sum_{i=1}^{n} C_i - C_T) \cdot r \longrightarrow$

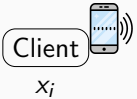
$\mathsf{D}_{\mathsf{sk}}(\lceil C \rfloor)$

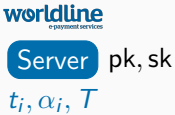
$$C = \mathsf{E}_{\mathsf{pk}}([\textstyle\sum_{i=1}^{n} \alpha_i[x_i > t_i] > T] \cdot r)$$

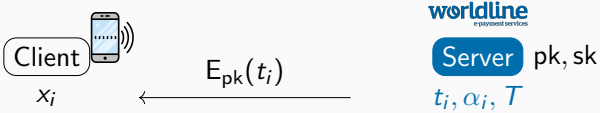
Tricks with this solution

- Easy to make ANDs of Comparison
- For one x_i, multiple α_i

Kenaï






Client
x_i
$\mathsf{E}_{\mathsf{pk}}(t_i)$
worldline
Server
pk, sk
t_i, α_i, T

Kenaï

$\mathsf{E}_{\mathsf{pk}}(t_i)$ ⟵

x_i

$b_i \xleftarrow{\$} \{-1, 1\}$

R_i, r_i random

$R_i > r_i > 0$

$c_i = R_i \cdot b_i \cdot (\mathsf{E}_{\mathsf{pk}}(t_i) - \mathsf{E}_{\mathsf{pk}}(x_i)) - \mathsf{E}_{\mathsf{pk}}(r_i)$

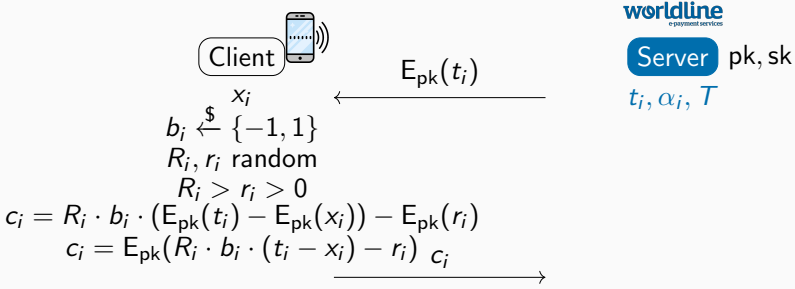
$c_i = \mathsf{E}_{\mathsf{pk}}(R_i \cdot b_i \cdot (t_i - x_i) - r_i)$

worldline
e-payment services

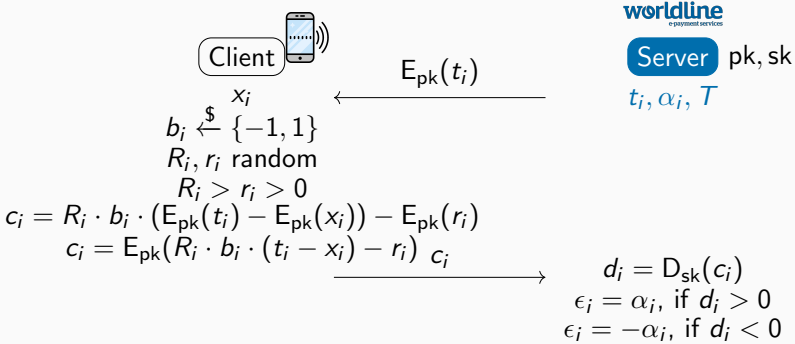
Server pk, sk

t_i, α_i, T

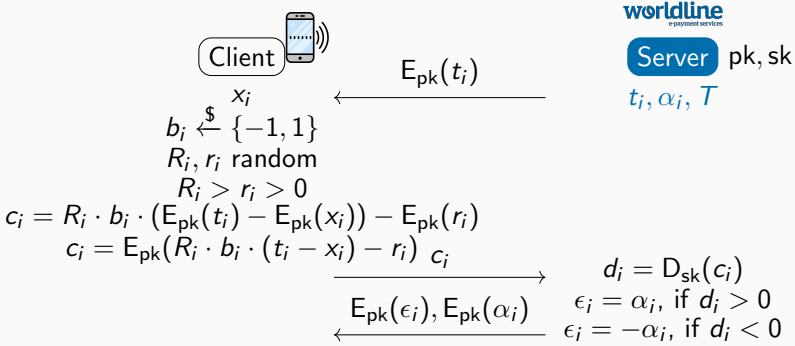
Kenaï


Client
Server
pk, sk
t_i, α_i, T
$\mathsf{E}_{\mathsf{pk}}(t_i)$
x_i
$b_i \xleftarrow{\$} \{-1, 1\}$
R_i, r_i random
$R_i > r_i > 0$
$c_i = R_i \cdot b_i \cdot (\mathsf{E}_{\mathsf{pk}}(t_i) - \mathsf{E}_{\mathsf{pk}}(x_i)) - \mathsf{E}_{\mathsf{pk}}(r_i)$
$c_i = \mathsf{E}_{\mathsf{pk}}(R_i \cdot b_i \cdot (t_i - x_i) - r_i)$
c_i

Kenaï


Client
worldline
e-payment services
Server
pk, sk
t_i, α_i, T
$\mathsf{E}_{\mathsf{pk}}(t_i)$
x_i
$b_i \xleftarrow{\$} \{-1, 1\}$
R_i, r_i random
$R_i > r_i > 0$
$c_i = R_i \cdot b_i \cdot (\mathsf{E}_{\mathsf{pk}}(t_i) - \mathsf{E}_{\mathsf{pk}}(x_i)) - \mathsf{E}_{\mathsf{pk}}(r_i)$
$c_i = \mathsf{E}_{\mathsf{pk}}(R_i \cdot b_i \cdot (t_i - x_i) - r_i)$
c_i
$d_i = \mathsf{D}_{\mathsf{sk}}(c_i)$
$\epsilon_i = \alpha_i$, if $d_i > 0$
$\epsilon_i = -\alpha_i$, if $d_i < 0$

Kenaï


Client
worldline
e-payment services
Server
pk, sk
t_i, α_i, T
$\mathsf{E}_{\mathsf{pk}}(t_i)$
x_i
$b_i \xleftarrow{\$} \{-1, 1\}$
R_i, r_i random
$R_i > r_i > 0$
$c_i = R_i \cdot b_i \cdot (\mathsf{E}_{\mathsf{pk}}(t_i) - \mathsf{E}_{\mathsf{pk}}(x_i)) - \mathsf{E}_{\mathsf{pk}}(r_i)$
$c_i = \mathsf{E}_{\mathsf{pk}}(R_i \cdot b_i \cdot (t_i - x_i) - r_i)$
c_i
$d_i = \mathsf{D}_{\mathsf{sk}}(c_i)$
$\epsilon_i = \alpha_i$, if $d_i > 0$
$\epsilon_i = -\alpha_i$, if $d_i < 0$
$\mathsf{E}_{\mathsf{pk}}(\epsilon_i), \mathsf{E}_{\mathsf{pk}}(\alpha_i)$

Kenaï

$\mathsf{E}_{\mathsf{pk}}(t_i)$ ←

worldline
e-payment services

Server pk, sk

t_i, α_i, T

x_i

$b_i \xleftarrow{\$} \{-1, 1\}$

R_i, r_i random

$R_i > r_i > 0$

$c_i = R_i \cdot b_i \cdot (\mathsf{E}_{\mathsf{pk}}(t_i) - \mathsf{E}_{\mathsf{pk}}(x_i)) - \mathsf{E}_{\mathsf{pk}}(r_i)$

$c_i = \mathsf{E}_{\mathsf{pk}}(R_i \cdot b_i \cdot (t_i - x_i) - r_i)$ c_i →

$d_i = \mathsf{D}_{\mathsf{sk}}(c_i)$

$\epsilon_i = \alpha_i$, if $d_i > 0$

$\epsilon_i = -\alpha_i$, if $d_i < 0$

← $\mathsf{E}_{\mathsf{pk}}(\epsilon_i), \mathsf{E}_{\mathsf{pk}}(\alpha_i)$

$$b_i \cdot \mathsf{E}_{\mathsf{pk}}(\epsilon_i) = \pm \mathsf{E}_{\mathsf{pk}}(\alpha_i)$$

$$a_i = b_i \cdot \mathsf{E}_{\mathsf{pk}}(\epsilon_i) + \mathsf{E}_{\mathsf{pk}}(\alpha_i) \in \{\mathsf{E}_{\mathsf{pk}}(0), \mathsf{E}_{\mathsf{pk}}(2\alpha_i)\}$$

$$U = \sum_{i=1}^{n} a_i = \mathsf{E}_{\mathsf{pk}}(2S)$$

$$S = \sum_{i=1}^{n} \alpha_i \cdot [x_i > t_i]$$

Kenaï

$\mathsf{E}_{\mathsf{pk}}(t_i)$ ←

worldline
e-payment services

Server pk, sk

t_i, α_i, T

x_i

$b_i \xleftarrow{\$} \{-1, 1\}$

R_i, r_i random

$R_i > r_i > 0$

$c_i = R_i \cdot b_i \cdot (\mathsf{E}_{\mathsf{pk}}(t_i) - \mathsf{E}_{\mathsf{pk}}(x_i)) - \mathsf{E}_{\mathsf{pk}}(r_i)$

$c_i = \mathsf{E}_{\mathsf{pk}}(R_i \cdot b_i \cdot (t_i - x_i) - r_i)$ c_i →

$d_i = \mathsf{D}_{\mathsf{sk}}(c_i)$

$\epsilon_i = \alpha_i$, if $d_i > 0$

$\epsilon_i = -\alpha_i$, if $d_i < 0$

← $\mathsf{E}_{\mathsf{pk}}(\epsilon_i), \mathsf{E}_{\mathsf{pk}}(\alpha_i)$

$$b_i \cdot \mathsf{E}_{\mathsf{pk}}(\epsilon_i) = \pm \mathsf{E}_{\mathsf{pk}}(\alpha_i)$$

$$a_i = b_i \cdot \mathsf{E}_{\mathsf{pk}}(\epsilon_i) + \mathsf{E}_{\mathsf{pk}}(\alpha_i) \in \{\mathsf{E}_{\mathsf{pk}}(0), \mathsf{E}_{\mathsf{pk}}(2\alpha_i)\}$$

$$U = \sum_{i=1}^{n} a_i = \mathsf{E}_{\mathsf{pk}}(2S)$$

$$S = \sum_{i=1}^{n} \alpha_i \cdot [x_i > t_i]$$

Implementation

Software requirements

- SEAL 3.0
- C++

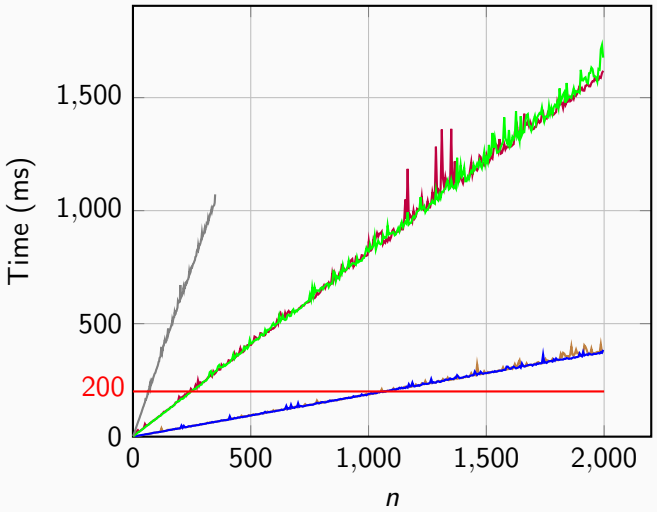
Encryption parameters

- Encryption scheme: FV-RNS variant (BFV)
- Security: 128 bits

Benchmark platform

- Intel® Core™ i7-6500U CPU @ 2.50GHz

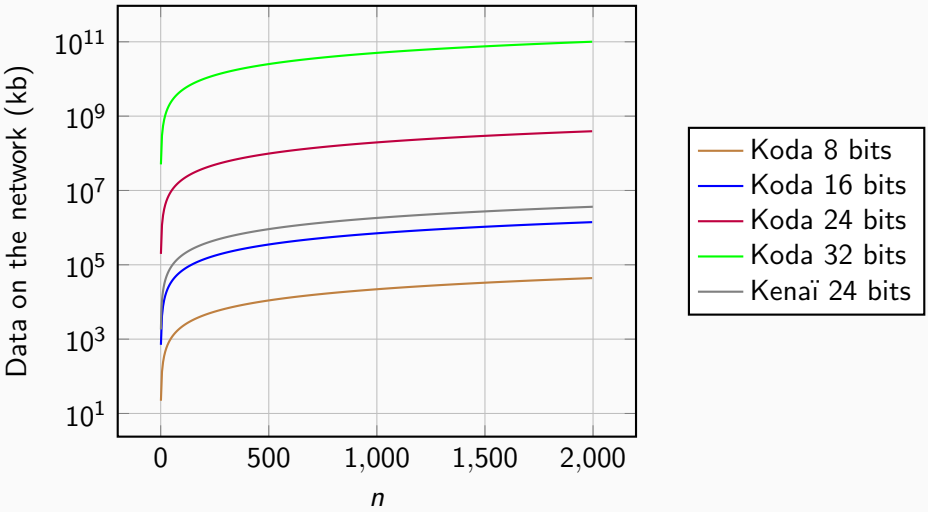
Koda & Kenaï:



- Koda 8 & 16 bits: $n \approx 1050$
- Koda 24 & 32: $n \approx 250$
- Kenaï 24 bits: $n \approx 65$

Koda 8 bits
Koda 16 bits
Koda 24 bits
Koda 32 bits
Kenaï 24 bits
Maximum computation time

Simulated network cost



Recap

	Koda				Kenaï
word size (bits)	8	16	24	32	24
n max	1050		250		65
cost @ n max (MB)	23	740	4800	12381600	118

Limitations

Evaluating our Solution

Pros:

- Client: little memory
- Server: fast

Cons:

- Malicious Client can cheat
- Information leak on Client inputs (one time security)
- Client side computations expensive for payment terminal

Conclusion

Conclusion

Results

- Koda and Kenaï allow a lot of comparisons

Perspective

- Improve the network costs
- Resist against a malicious client

Thank You

- Questions ?