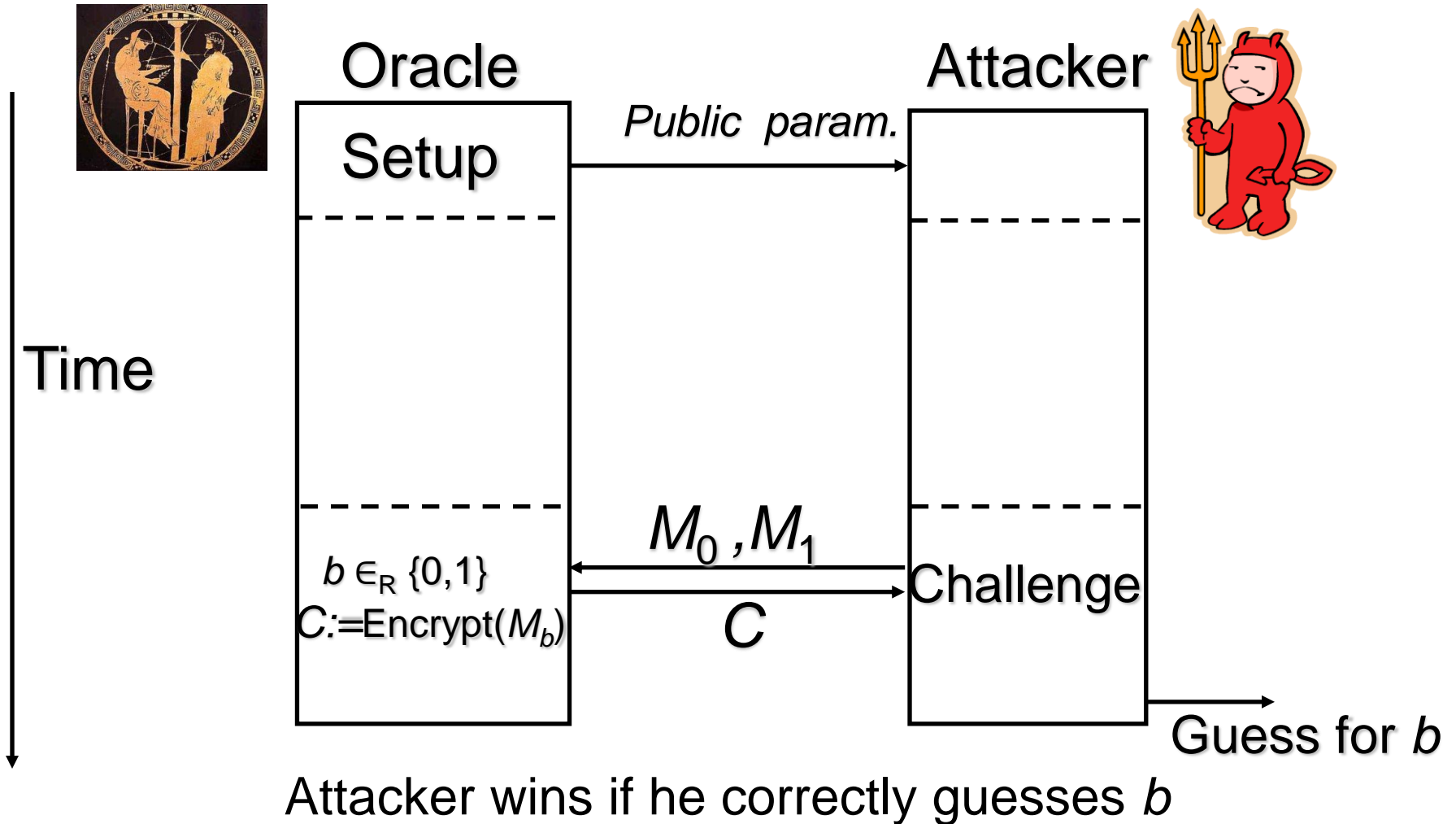


Defining security: Semantic Security



Homomorphic Encryption with a Double Decryption Mechanism based on Elliptic Curves over Rings

Andreas Peter

Technische Universität Darmstadt, Germany



TECHNISCHE
UNIVERSITÄT
DARMSTADT

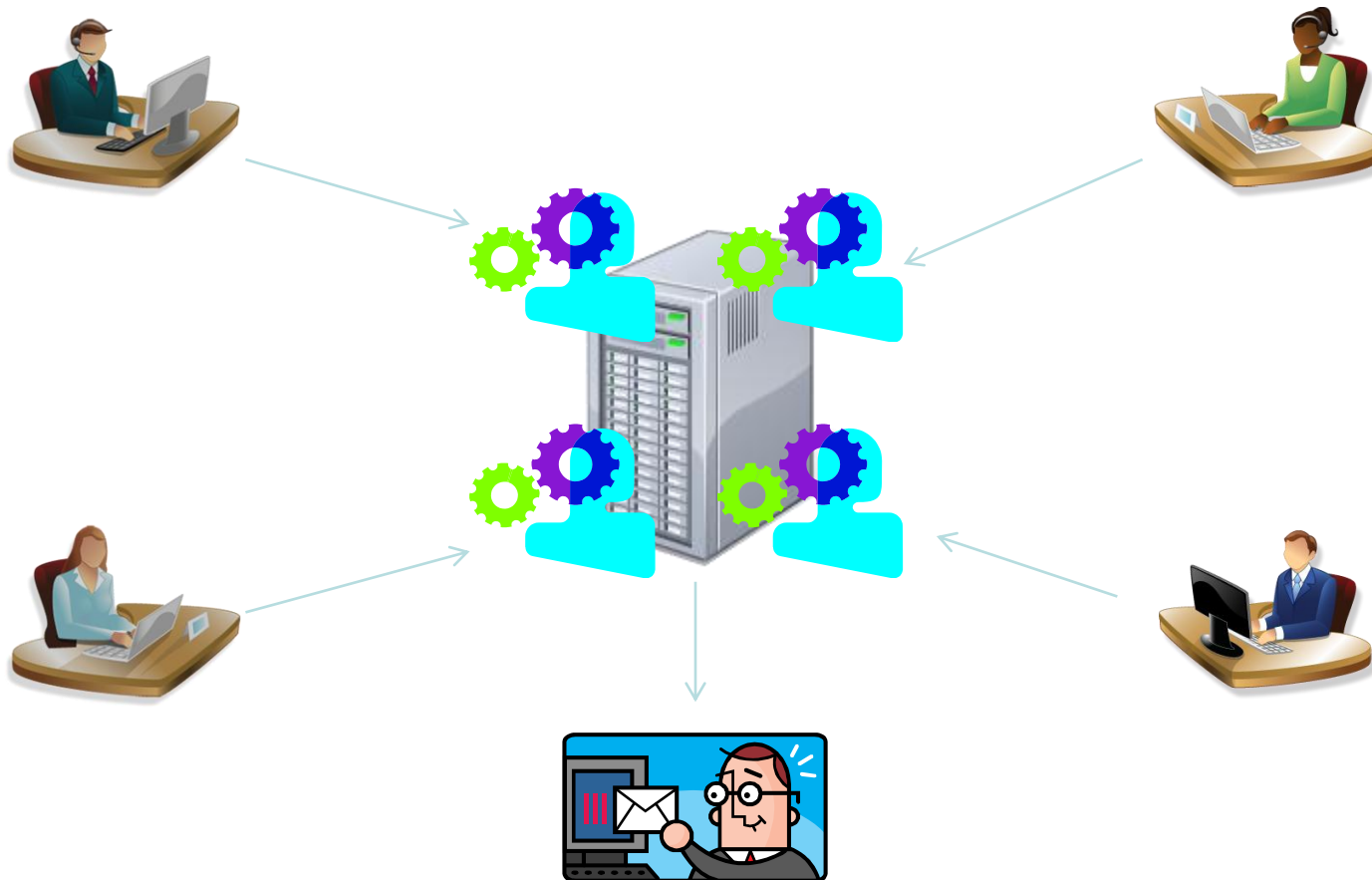


**15. Kryptotag
Universität Oldenburg
01.12.2011**



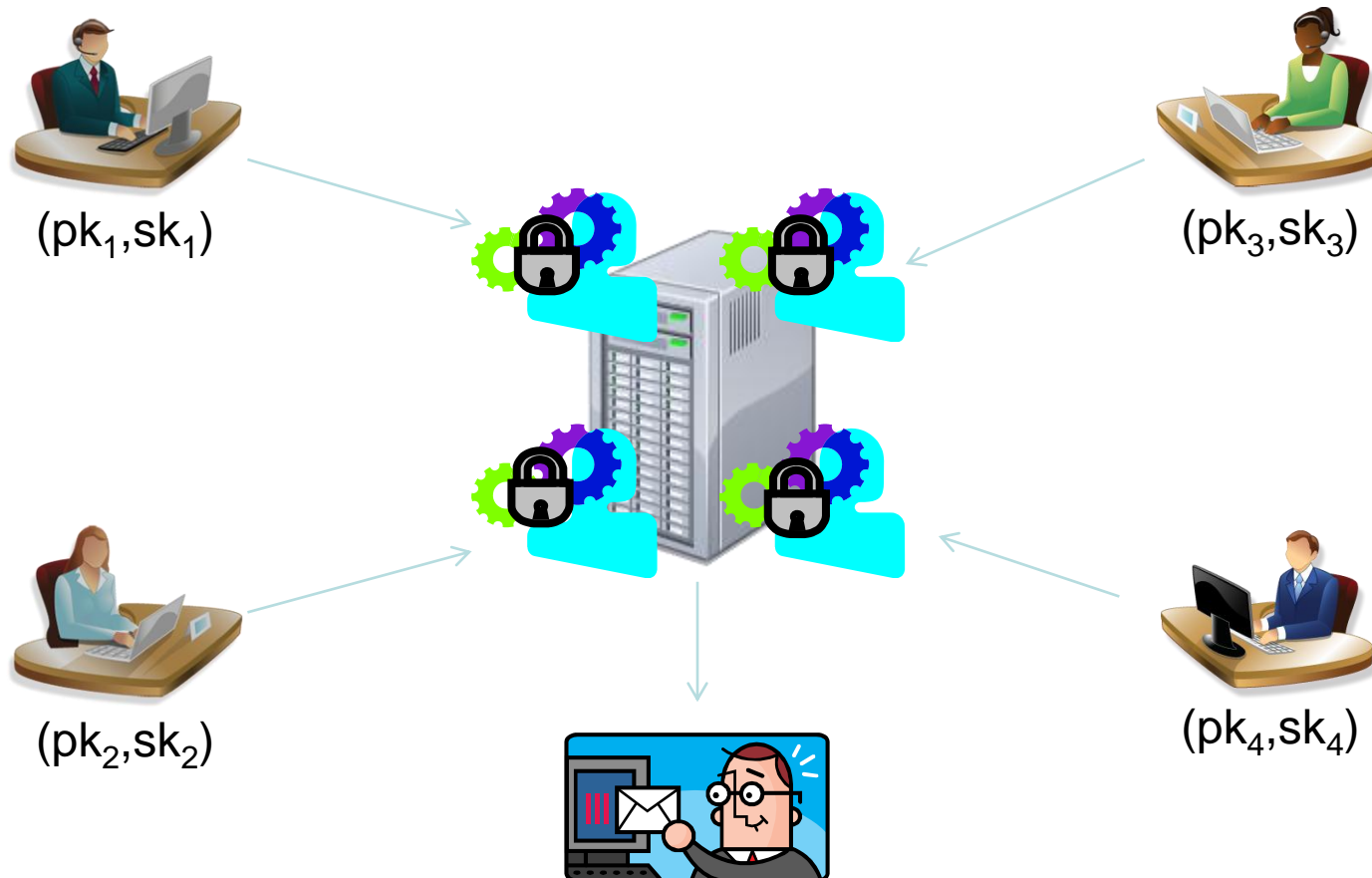
What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



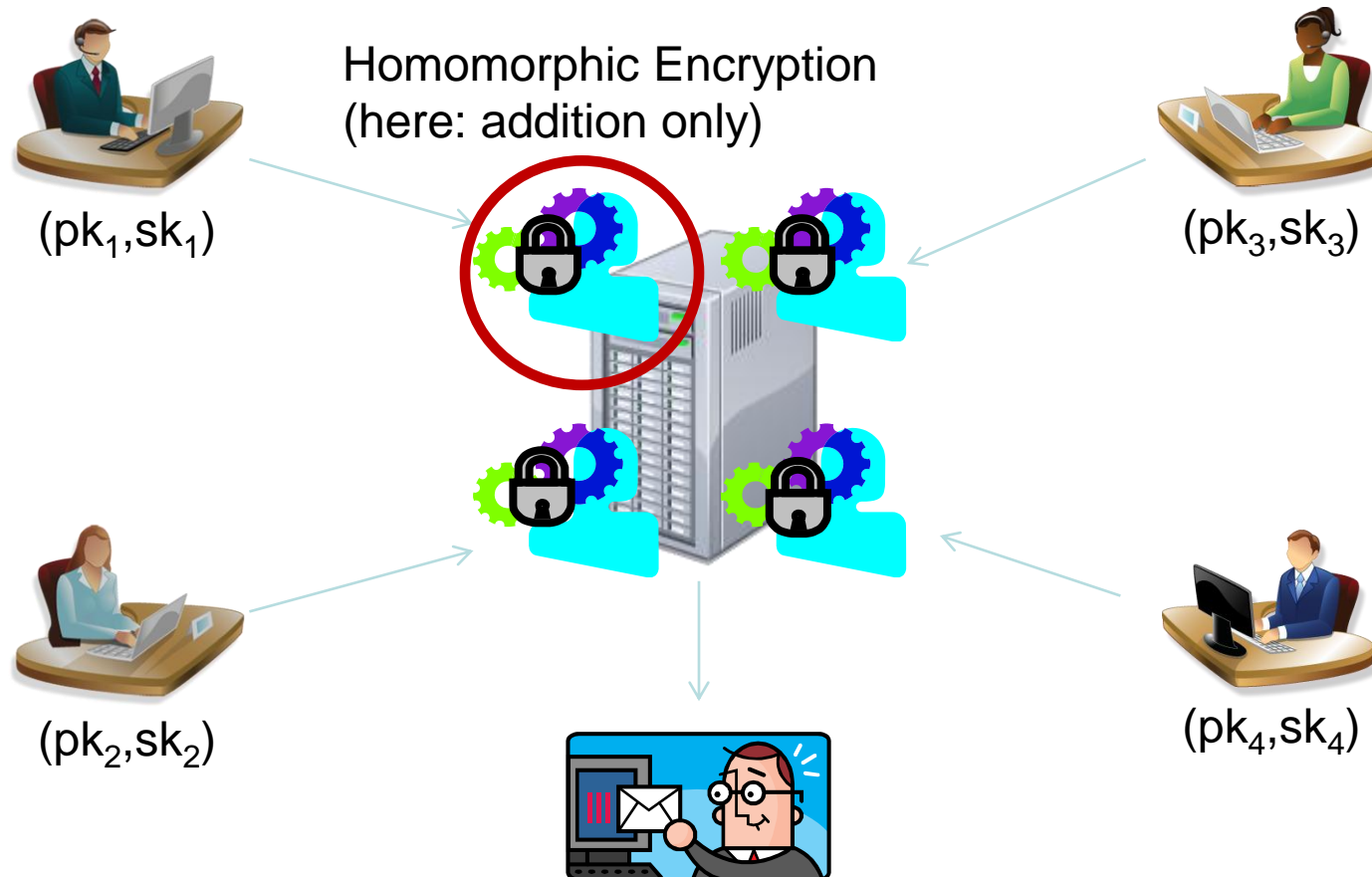
What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



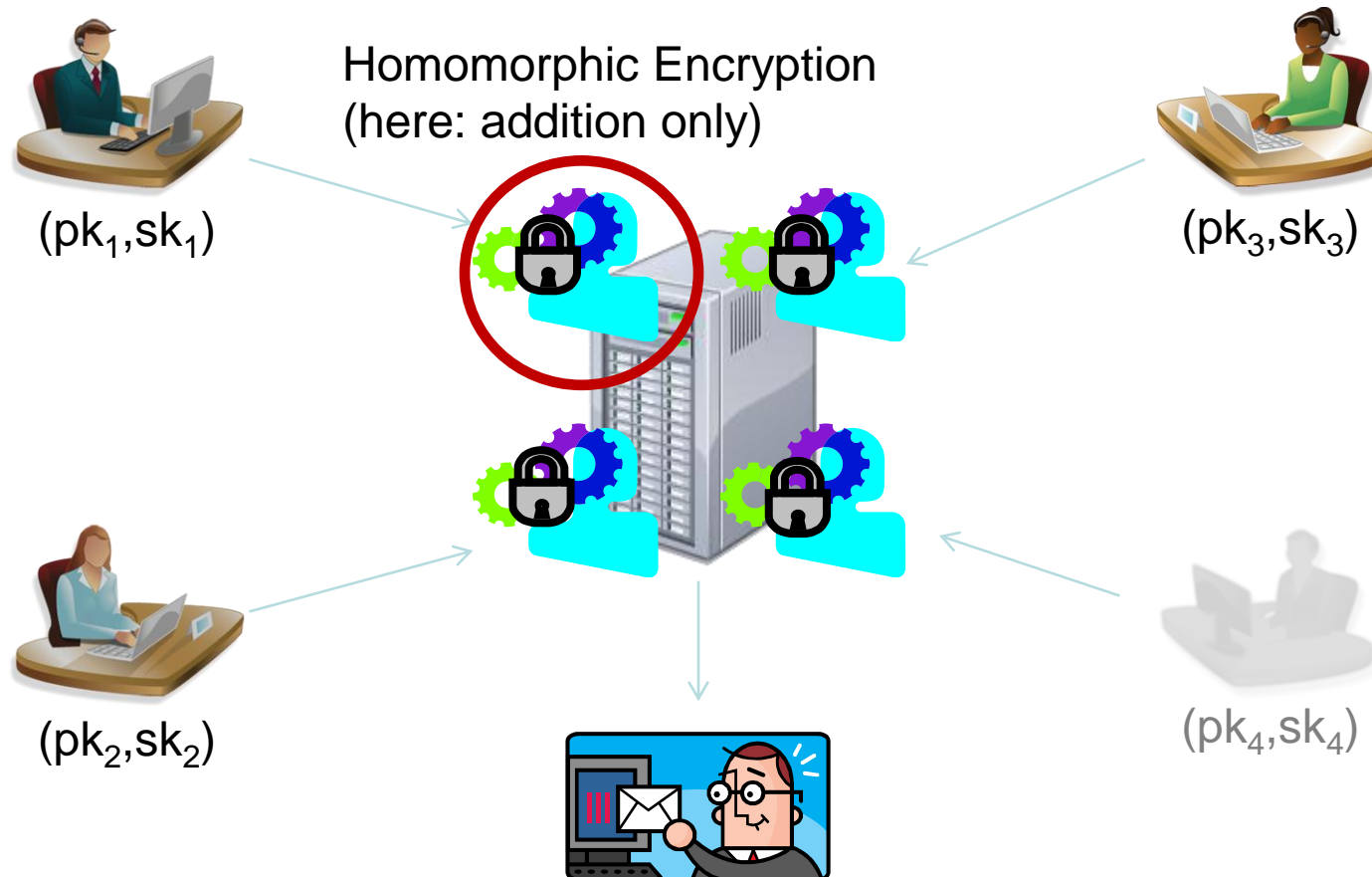
What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



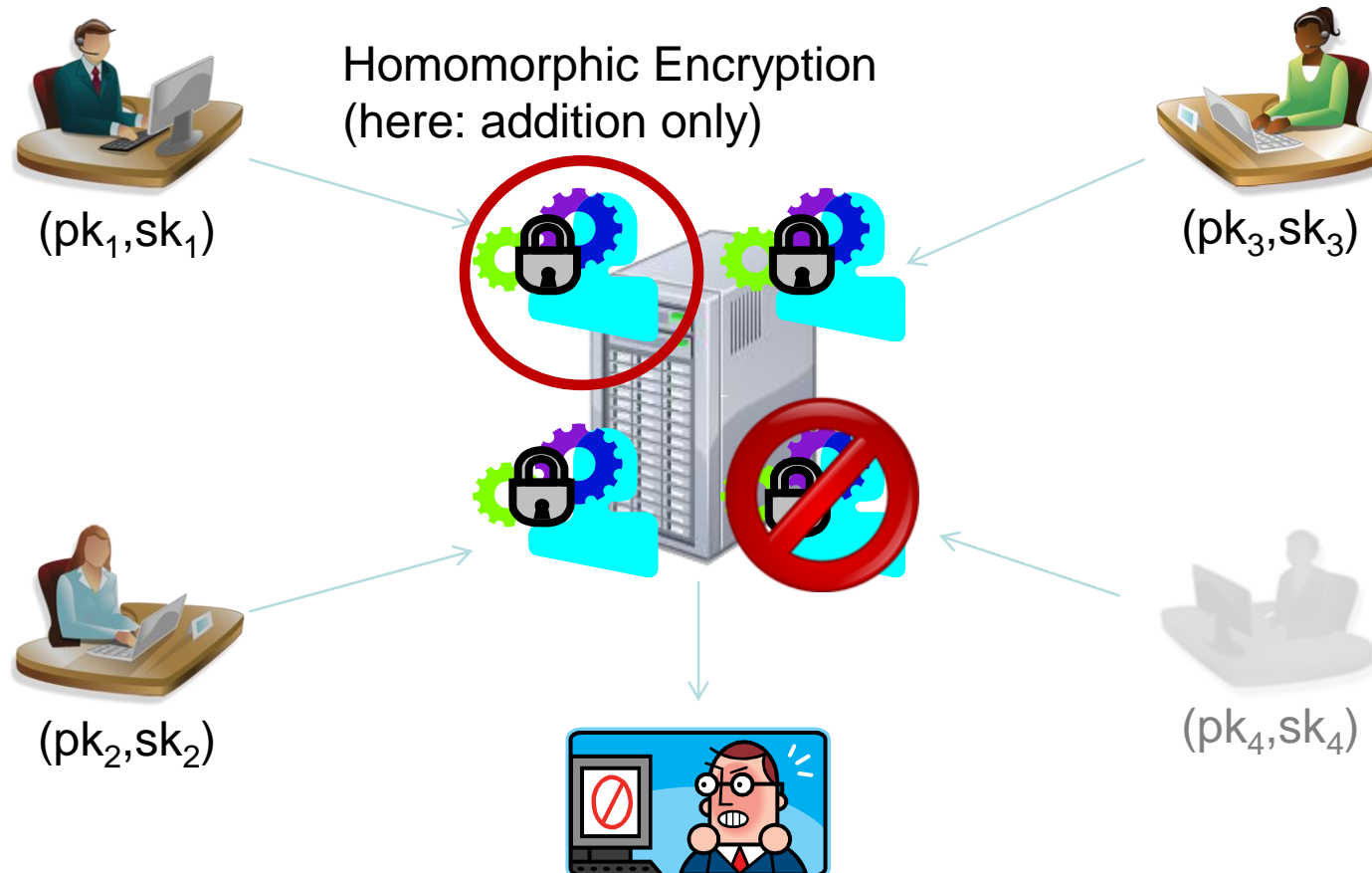
What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



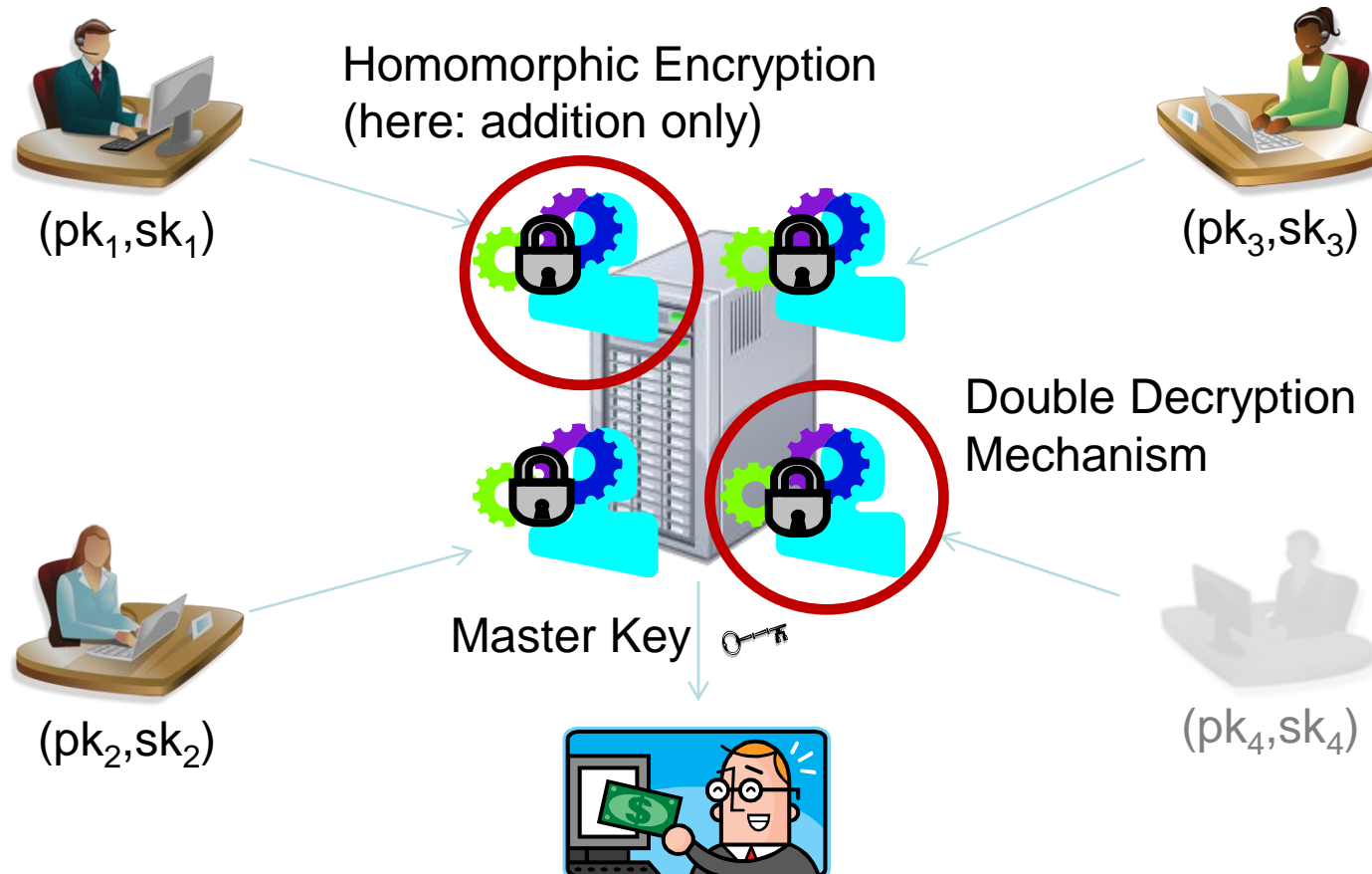
What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



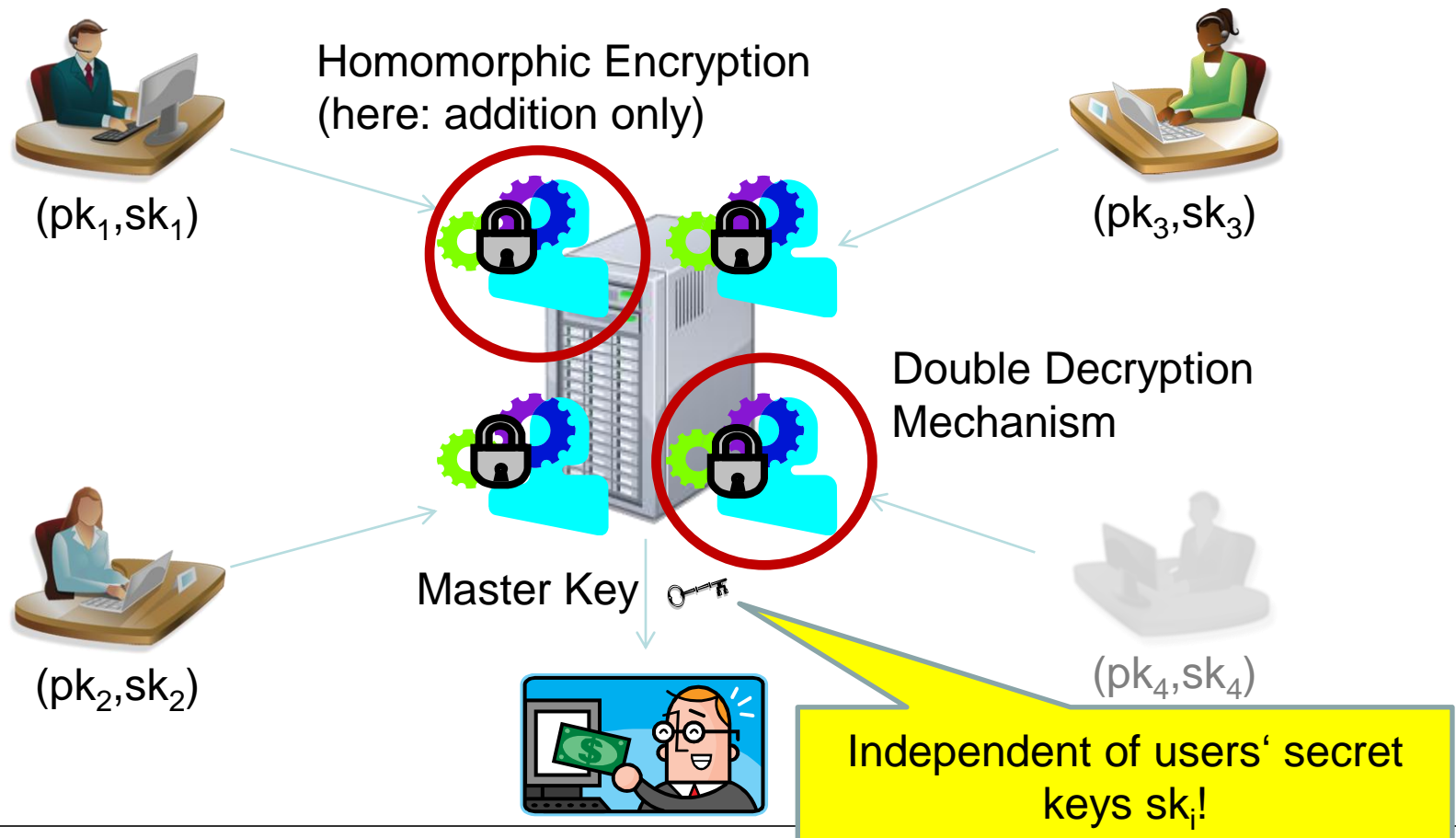
What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



What is this? And why is it interesting?

- Consider the following scenario (e.g., in an insurance company or university):



Are there solutions to this scenario? (Related Work)

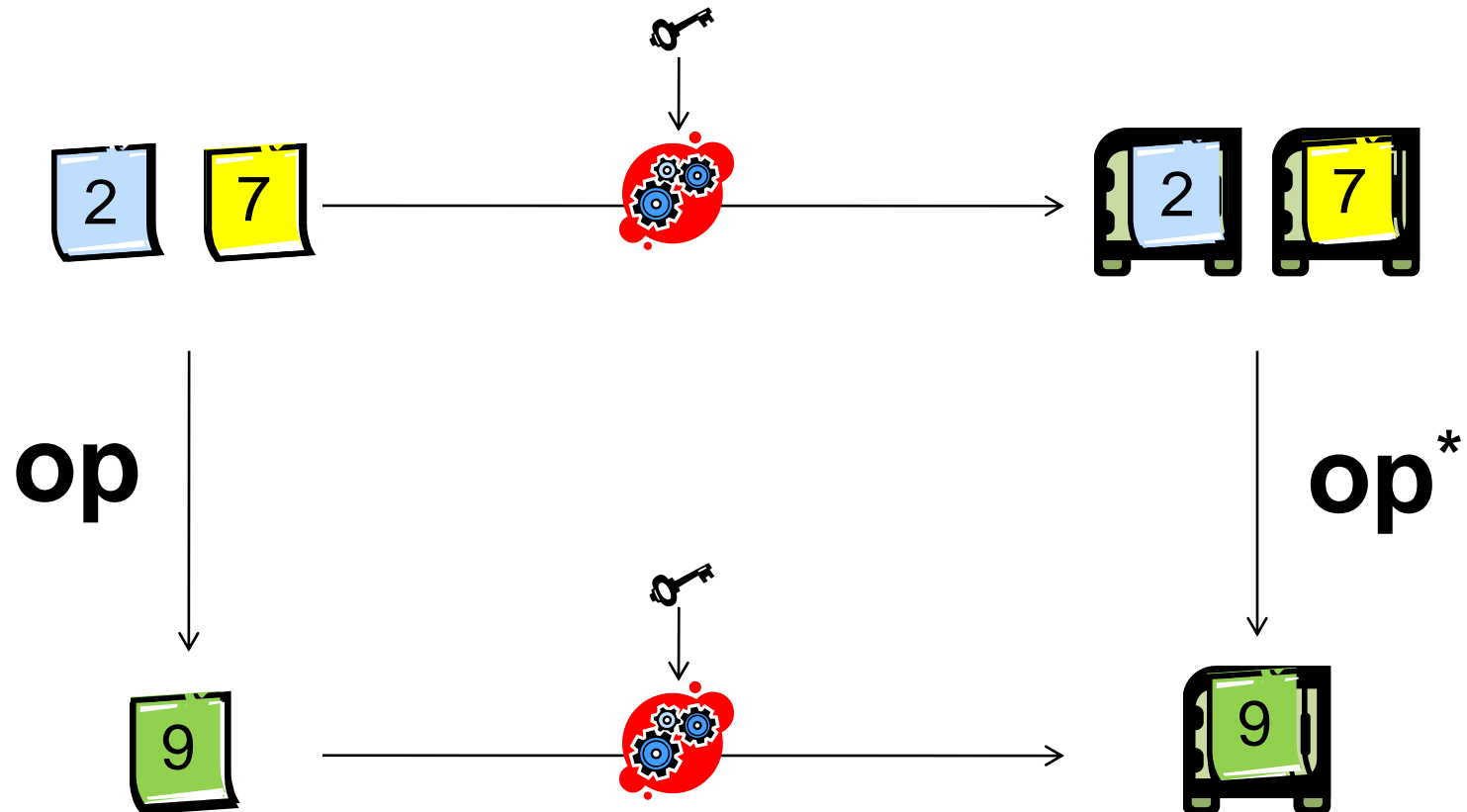
- Yes, but only one!
- At ASIACRYPT 2003, Bresson, Catalano, and Pointcheval presented a so-called „homomorphic DD-PKE scheme“ [BCP03]!
 - [BCP03] Emmanuel Bresson, Dario Catalano, and David Pointcheval. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In Chi-Sung Lai, editor, ASIACRYPT, volume 2894 of Lecture Notes in Computer Science, pages 37-54. Springer, 2003.
- Essentially, their scheme is identical to that of [CramerShoup02].
 - [CramerShoup02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 45-64. Springer, 2002.

Our Goal: Construct a new such scheme!

- Our scheme is based on elliptic curves over rings!
 - More precisely, we consider elliptic curves over the ring \mathbb{Z}_N^2 where N is some RSA-modulus.
- Security is based on an elliptic curve analogon of the Decisional Diffie-Hellman Assumption over $(\mathbb{Z}_N^2)^*$

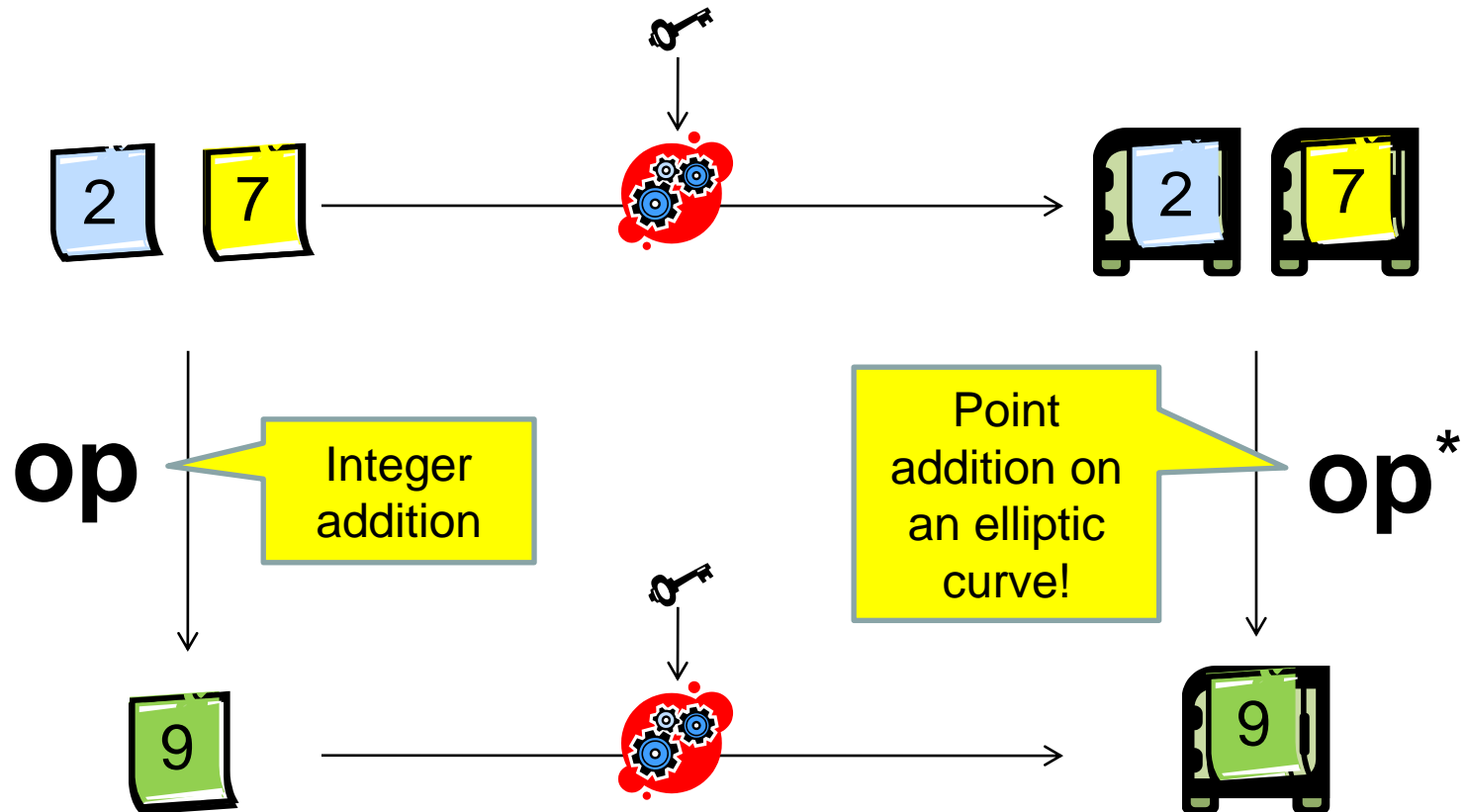
Group Homomorphic Encryption

Informal Definition



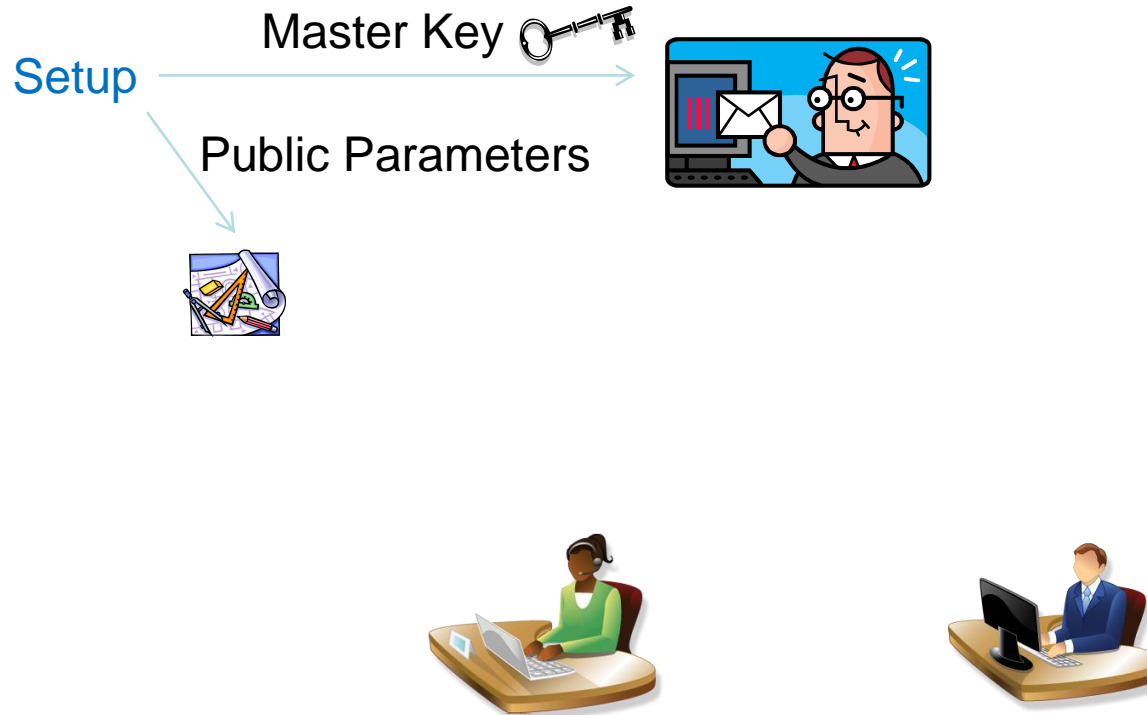
Group Homomorphic Encryption

Informal Definition



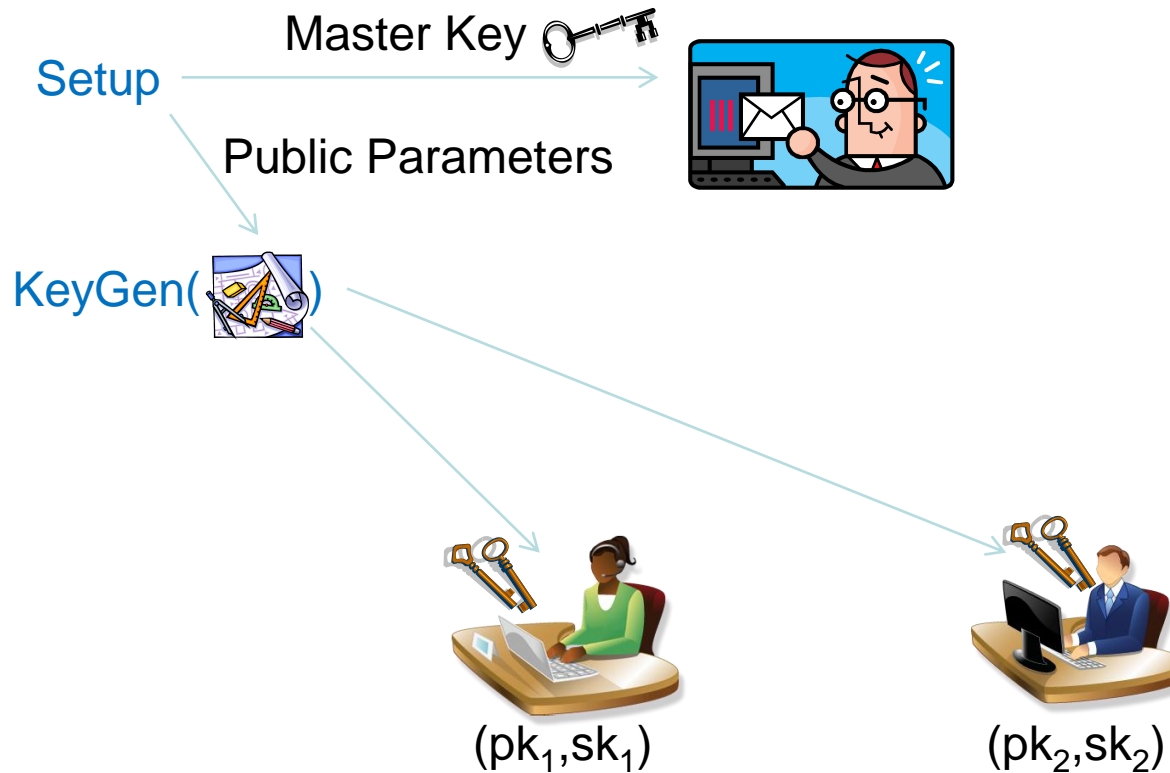
Double Decryption Mechanism (DD-PKE)

Informal Definition



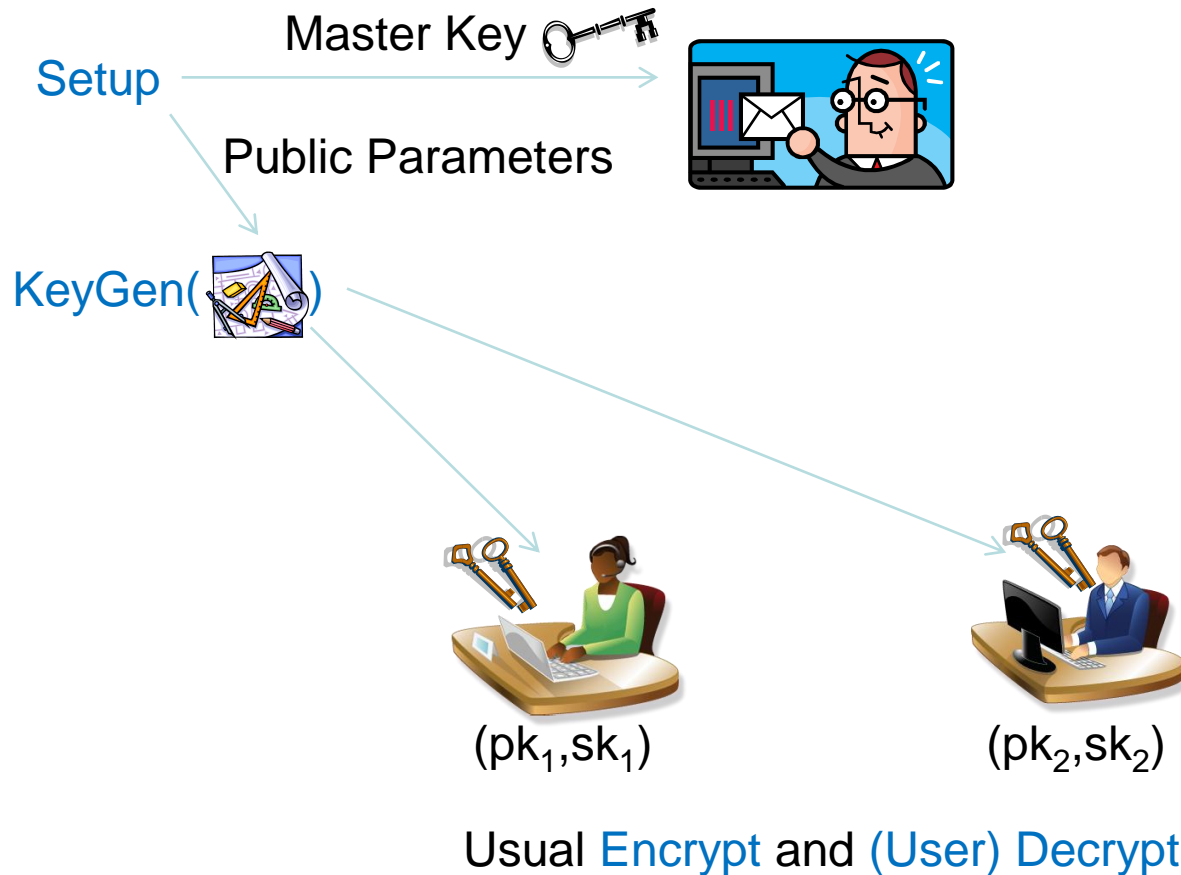
Double Decryption Mechanism (DD-PKE)

Informal Definition



Double Decryption Mechanism (DD-PKE)

Informal Definition



Outline

- Elliptic Curves over Rings
- Our Cryptosystem (Construction)
- Our Cryptosystem (Some Properties)
- Choices of Parameters (Elliptic Curve, ...)
- Security
- Open Questions

Elliptic Curves over Rings (Definitions)

- R **finite** commutative unital ring with group of units R^\times
 - ▶ Example: $R = \mathbb{Z}_{N^2}$ for some RSA-modulus $N = pq$.
- For $a, b \in R$ with $6(4a^3 + 27b^2) \in R^\times$ the equation

$$E : y^2z = x^3 + axz^2 + bz^3 \quad (1)$$

defines an **elliptic curve E over R** .

- The set $E(R)$ of **R -valued points on E** is defined as

$$\{(x : y : z) \mid (x, y, z) \in R^3 \text{ satisfying (1) s.t. } xR + yR + zR = R\}$$

with $(x_1 : x_2 : x_3) = (x'_1 : x'_2 : x'_3)$ iff $\exists \lambda \in R^\times : \forall i = 1, 2, 3 : \lambda x_i = x'_i$.

Elliptic Curves over Rings (Some Facts)

- Applying the usual chord and tangent process in our setting yields:

Theorem

- ▶ $E(R)$ is a group with identity element $\mathcal{O} = (0 : 1 : 0)$. (Recall: R is finite)
- ▶ There are explicit and efficient formulae to perform the group operations.

- CRT on \mathbb{Z}_N implies $E(\mathbb{Z}_N) \cong E(\mathbb{Z}_p) \times E(\mathbb{Z}_q)$:

- ▶ $\#E(\mathbb{Z}_{N^2}) = N\#E(\mathbb{Z}_N) = N\#E(\mathbb{Z}_p)\#E(\mathbb{Z}_q)$.
- ▶ Computing $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q)) \equiv_{\text{poly}}$ factoring N

- There are special \mathbb{Z}_{N^2} -valued points on E :

- ▶ $P_r = (Nr : 1 : 0) \in E(\mathbb{Z}_{N^2})$ with $mP_r = P_{mr}$ for all $m \in \mathbb{Z}_N$.
- ▶ $NP_1 = \mathcal{O}$.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \longrightarrow (**PP**, **MK**) with
public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$
and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \longrightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.

① $N = pq$ RSA-modulus with distinct primes p and q of same bit length κ .

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.

- 1 $N = pq$ RSA-modulus with distinct primes p and q of same bit length κ .
- 2 Choose an elliptic curve $E : y^2z = x^3 + axz^2 + bz^3$ over \mathbb{Z}_{N^2} such that $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$ is *not smooth*, i.e., it does not factor completely into small primes. (details later)

Our Cryptosystem

A DD-PKE scheme consists of ([Setup](#), [KeyGen](#), [Enc](#), [Dec](#), [mDec](#)):

- [Setup](#)(security parameter κ) \longrightarrow ([PP](#), [MK](#)) with public parameters [PP](#) = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret [MK](#) = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.

- 1 $N = pq$ RSA-modulus with distinct primes p and q of same bit length κ .
- 2 Choose an elliptic curve $E : y^2z = x^3 + axz^2 + bz^3$ over \mathbb{Z}_{N^2} such that $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$ is *not smooth*, i.e., it does not factor completely into small primes. (details later)
- 3 Choose a random point $Q' \in E(\mathbb{Z}_{N^2})$ and compute $Q := NQ'$. Then, the order of Q divides M with overwhelming probability.
(Recall that $\#E(\mathbb{Z}_{N^2}) = N\#E(\mathbb{Z}_p)\#E(\mathbb{Z}_q)$)

Our Cryptosystem

A DD-PKE scheme consists of ([Setup](#), [KeyGen](#), [Enc](#), [Dec](#), [mDec](#)):

- [Setup](#)(security parameter κ) \longrightarrow ([PP](#), [MK](#)) with public parameters [PP](#) = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret [MK](#) = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.

- 1 $N = pq$ RSA-modulus with distinct primes p and q of same bit length κ .
- 2 Choose an elliptic curve $E : y^2z = x^3 + axz^2 + bz^3$ over \mathbb{Z}_{N^2} such that $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$ is *not smooth*, i.e., it does not factor completely into small primes. (details later)
- 3 Choose a random point $Q' \in E(\mathbb{Z}_{N^2})$ and compute $Q := NQ'$. Then, the order of Q divides M with overwhelming probability.
(Recall that $\#E(\mathbb{Z}_{N^2}) = N\#E(\mathbb{Z}_p)\#E(\mathbb{Z}_q)$)
- 4 Plaintext space is $\mathcal{P} = \mathbb{Z}_N$

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q \text{ with } \text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.

① Choose $0 \neq s \in \mathbb{Z}_{N^2}$ s.t. $R := sQ$ has the same order as Q , i.e., $\langle R \rangle = \langle Q \rangle$.

Our Cryptosystem

A DD-PKE scheme consists of (Setup , KeyGen , Enc , Dec , mDec):

- $\text{Setup}(\text{security parameter } \kappa) \rightarrow (\text{PP}, \text{MK})$ with public parameters $\text{PP} = (N, E/\mathbb{Z}_{N^2}, Q \text{ with } \text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret $\text{MK} = M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- $\text{KeyGen}(\text{PP}) \rightarrow (\text{pk} = R = sQ, \text{sk} = s)$ with user's public key pk and user's secret key sk such that $\langle R \rangle = \langle Q \rangle$.

- 1 Choose $0 \neq s \in \mathbb{Z}_{N^2}$ s.t. $R := sQ$ has the same order as Q , i.e., $\langle R \rangle = \langle Q \rangle$.
- 2 Observe that if the product of all small prime factors (including multiples) of M is publicly known (denote this product by π), we can efficiently check whether $\text{gcd}(s, \pi) = 1$ or not. (details later)

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.

- 1 Choose $0 \neq s \in \mathbb{Z}_{N^2}$ s.t. $R := sQ$ has the same order as Q , i.e., $\langle R \rangle = \langle Q \rangle$.
- 2 Observe that if the product of all small prime factors (including multiples) of M is publicly known (denote this product by π), we can efficiently check whether $\text{gcd}(s, \pi) = 1$ or not. (details later)
- 3 So by choosing $s \in \mathbb{Z}_{N^2}$ with $\text{gcd}(s, \pi) = 1$, we have that $s \in \mathbb{Z}_M^*$ with overwhelming probability.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q \text{ with } \text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q \text{ with } \text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q \text{ with } \text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\rightarrow m = \frac{x(MB)}{N} M^{-1} \text{ mod } N$.

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\rightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

Correctness of User Decryption

$$\text{Dec}_{(\text{PP}, \text{sk})}(\text{Enc}_{(\text{PP}, \text{pk})}(m)) = \frac{x(rR + P_m - srQ)}{N} = m$$

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\rightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

Correctness of Master Decryption

$$\text{mDec}_{(\text{PP}, \text{sk})}(\text{Enc}_{(\text{PP}, \text{pk})}(m)) = \frac{x(M(rR + P_m))}{N} M^{-1} \bmod N = m$$

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\rightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

Group Homomorphic?

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\rightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

Group Homomorphic? $((A_1, B_1)$ and (A_2, B_2) of m_1 and m_2 , resp.)

Our Cryptosystem

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \rightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \rightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \rightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\rightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

Group Homomorphic? ((A_1, B_1) and (A_2, B_2) of m_1 and m_2 , resp.)

$$\begin{aligned}x(B_1 + B_2 - s(A_1 + A_2)) &= x(B_1 + B_2 - sA_1 - sA_2) \\ &= x(r_1R + P_{m_1} + r_2R + P_{m_2} - sr_1Q - sr_2Q) \\ &= x(P_{m_1+m_2}) = (m_1 + m_2)N.\end{aligned}$$

Our Cryptosystem (More Properties: User Decrypt)

Recall the user's decryption procedure:

- $\text{Dec}_{(\text{pp}, \text{sk})}(A, B) \longrightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.

Detection of invalid ciphertexts

- Without knowing the factorisation of N , no efficient way to randomly sample from $E(\mathbb{Z}_{N^2})$ is known.
- Assuming this, the ciphertext space is $\langle Q \rangle \times \langle Q, P_1 \rangle$.
Form of ciphertexts: $(A, B) = (rQ, tQ + P_m)$
- (A, B) is valid $\iff t = rs \pmod{\text{ord}(Q)} \iff B - sA = P_m$

Our Cryptosystem (More Properties: User Decrypt)

Recall the user's decryption procedure:

- $\text{Dec}_{(\text{PP}, \text{sk})}(A, B) \rightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.

Detection of invalid ciphertexts

- Without knowing the factorisation of N , no efficient way to randomly sample from $E(\mathbb{Z}_{N^2})$ is known.
- Assuming this, the ciphertext space is $\langle Q \rangle \times \langle Q, P_1 \rangle$.
Form of ciphertexts: $(A, B) = (rQ, tQ + P_m)$
- (A, B) is valid $\iff t = rs \pmod{\text{ord}(Q)} \iff B - sA = P_m$
- For the master's decryption this doesn't seem possible!
 $\text{mDec}_{(\text{PP}, \text{MK}, \text{pk})}(A, B) \rightarrow m = \frac{x(MB)}{N} M^{-1} \pmod{N}$

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \longrightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N$) and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \longrightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**_(**PP**, **pk**)($m \in \mathcal{P}$) \longrightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**_(**PP**, **sk**)(A, B) $\longrightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**_(**PP**, **MK**, **pk**)(A, B) $\longrightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

A DD-PKE scheme consists of (**Setup**, **KeyGen**, **Enc**, **Dec**, **mDec**):

- **Setup**(security parameter κ) \longrightarrow (**PP**, **MK**) with public parameters **PP** = $(N, E/\mathbb{Z}_{N^2}, Q$ with $\text{ord}(Q) \mid M, \mathcal{P} = \mathbb{Z}_N)$ and master secret **MK** = $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.
- **KeyGen**(**PP**) \longrightarrow (**pk** = $R = sQ$, **sk** = s) with user's public key **pk** and user's secret key **sk** such that $\langle R \rangle = \langle Q \rangle$.
- **Enc**(**PP**, **pk**)($m \in \mathcal{P}$) \longrightarrow ciphertext (A, B) with $A := rQ$ and $B := rR + P_m$ for random $r \in \mathbb{Z}_{N^2}$.
- **Dec**(**PP**, **sk**)(A, B) $\longrightarrow m = \frac{x(B-sA)}{N}$ where $x((x_1 : x_2 : x_3)) := x_1$.
- **mDec**(**PP**, **MK**, **pk**)(A, B) $\longrightarrow m = \frac{x(MB)}{N} M^{-1} \bmod N$.

Choices of Parameters: Elliptic Curves

Recall that we need an elliptic curve $E : y^2z = x^3 + axz^2 + bz^3$ over \mathbb{Z}_{N^2} such that $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$ is not smooth.

Lemma

Let p be an odd prime with $p \equiv 2 \pmod{3}$ and let $b \in \mathbb{Z}_p^$. For the elliptic curve $E : y^2z = x^3 + bz^3$, we have $\#E(\mathbb{Z}_p) = p + 1$.*

Choices of Parameters: Elliptic Curves

Recall that we need an elliptic curve $E : y^2z = x^3 + axz^2 + bz^3$ over \mathbb{Z}_{N^2} such that $M := \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$ is not smooth.

Lemma

Let p be an odd prime with $p \equiv 2 \pmod{3}$ and let $b \in \mathbb{Z}_p^*$. For the elliptic curve $E : y^2z = x^3 + bz^3$, we have $\#E(\mathbb{Z}_p) = p + 1$.

Efficient Construction of such Elliptic Curves

- 1 Choose *strong* primes p and q (i.e., $p + 1$ and $q + 1$ are not smooth) with $p \equiv q \equiv 2 \pmod{3}$. Set $N = pq$.
 - ▶ Example: $p = 6p' - 1$ and $q = 6q' - 1$ for some large primes p' and q' .
- 2 Fix $b \in \mathbb{Z}_{\min(p,q)}^*$ and consider $E : y^2z = x^3 + bz^3$ over \mathbb{Z}_{N^2} .
- 3 By the Lemma: $M = \text{lcm}(p + 1, q + 1) = \text{lcm}(6p', 6q') = 6p'q'$.

Choices of Parameters: User's Secret Key s

Recall that we need $0 \neq s \in \mathbb{Z}_{N^2}$ s.t. $\text{ord}(sQ) = \text{ord}(Q)$ ($\text{ord}(Q) \mid M$)

- Sufficient condition: $s \in \mathbb{Z}_M^*$ (BUT: M not known to KeyGen)
- Let π denote the product of all small prime factors (including multiples) of $M = \text{lcm}(\#E(\mathbb{Z}_p), \#E(\mathbb{Z}_q))$.

Efficient Sampling from \mathbb{Z}_M^* without knowing M

Recall our example: Strong primes $p = 6p' - 1$ and $q = 6q' - 1$. Elliptic curve E with $M = 6p'q'$. Here: $\pi = 6$ is publicly known!

- Choose random $0 \neq s \in \mathbb{Z}_{N^2}$ and check $\text{gcd}(s, \pi) = 1$ (if not, repeat)
- Then: $s \in \mathbb{Z}_M^*$ with overwhelming probability.
 - ▶ Otherwise $\text{gcd}(s, M)$ is a non-trivial divisor of M , i.e., p' , q' or M .
 - ▶ We've efficiently factorized N (contradiction!)

Semantic Security (Against Passive Adversaries)

- Security depends on the hardness of the following problem:
 - ▶ Given two points $R, S \in \langle Q \rangle$ with $\text{ord}(R) = \text{ord}(Q) \mid M$
 - ▶ and given a random point $T \in E(\mathbb{Z}_{N^2})$
 - ▶ decide whether T lies in the subgroup generated by $\log_Q(S)R$
(If so, we have $\log_Q(T) = \log_Q(S) \log_Q(R)$)
- As this is an elliptic curve analogon to the Decisional Diffie-Hellman Problem over $\mathbb{Z}_{N^2}^*$, we call it the **Decisional Diffie-Hellman Problem over $E(\mathbb{Z}_{N^2})$** .

- Recall the form of ciphertexts: $(A, B) = (rQ, rR + P_m)$.
 - ▶ $P_m \notin \langle Q \rangle$ for all $0 \neq m \in \mathbb{Z}_N$.
 - ▶ Can we find points $Q \in E(\mathbb{Z}_{N^2})$ with $P_m \in \langle Q \rangle$ for all $m \in \mathbb{Z}_N$?

- Recall the form of ciphertexts: $(A, B) = (rQ, rR + P_m)$.
 - ▶ $P_m \notin \langle Q \rangle$ for all $0 \neq m \in \mathbb{Z}_N$.
 - ▶ Can we find points $Q \in E(\mathbb{Z}_{N^2})$ with $P_m \in \langle Q \rangle$ for all $m \in \mathbb{Z}_N$?
 - ▶ Necessary condition: N divides M . But then Hasse's bound implies: $\#E(\mathbb{Z}_p) = p$ and $\#E(\mathbb{Z}_q) = q$, i.e., E is **anomalous** over p and q .

- Recall the form of ciphertexts: $(A, B) = (rQ, rR + P_m)$.
 - ▶ $P_m \notin \langle Q \rangle$ for all $0 \neq m \in \mathbb{Z}_N$.
 - ▶ Can we find points $Q \in E(\mathbb{Z}_{N^2})$ with $P_m \in \langle Q \rangle$ for all $m \in \mathbb{Z}_N$?
 - ▶ Necessary condition: N divides M . But then Hasse's bound implies: $\#E(\mathbb{Z}_p) = p$ and $\#E(\mathbb{Z}_q) = q$, i.e., E is **anomalous** over p and q .
 - ▶ Problem: Current anomalous curve-based cryptosystems are insecure!
 - ▶ Question: Is there any other way for the second component of our ciphertexts to be in the same cyclic subgroup as the first component?

- We use special elliptic curves of the form $E : y^2z = x^3 + bz^3$.

- We use special elliptic curves of the form $E : y^2z = x^3 + bz^3$.
 - ▶ Famous as supersingular curves over \mathbb{Z}_p and \mathbb{Z}_q !
 - ▶ But then computing pairings is easy and so would be DDH, right?

- We use special elliptic curves of the form $E : y^2z = x^3 + bz^3$.
 - ▶ Famous as supersingular curves over \mathbb{Z}_p and \mathbb{Z}_q !
 - ▶ But then computing pairings is easy and so would be DDH, right?
 - ▶ No! In our setting, computation of pairings is only possible if the factorisation of N is known. [GalbraithMcKee05]

- We use special elliptic curves of the form $E : y^2z = x^3 + bz^3$.
 - ▶ Famous as supersingular curves over \mathbb{Z}_p and \mathbb{Z}_q !
 - ▶ But then computing pairings is easy and so would be DDH, right?
 - ▶ No! In our setting, computation of pairings is only possible if the factorisation of N is known. [GalbraithMcKee05]
- Question: What about other types of elliptic curves?

Thanks for Your Attention!

- References:

[GalbraithMcKee05] S. D. Galbraith and J. F. McKee, Pairings on elliptic curves over finite commutative rings, in N. P. Smart (ed.), Cryptography and Coding: 10th IMA International Conference, Cirencester, UK, Springer LNCS 3796 (2005) 392 – 409.

Any Questions?