Group Encryption: Full Dynamicity, Message Filtering and Code-Based Instantiation

Khoa Nguyen[1] Reihaneh Safavi-Naini[2] Willy Susilo[3]
Huaxiong Wang[1] Yanhong Xu[2] **Neng Zeng**[4]

Nanyang Technological University, Singapore[1]
University of Calgary, Calgary, Canada[2]
University of Wollongong, Wollongong NSW, Australia[3]
Singapore University of Technology and Design, Singapore[4]

PKC 2021

10-13 May 2021

Table of Contents

Group Encryption [Kiayias-Tsiounis-Yung, AC'07]

Group encryption: encryption analogue of group signatures.

- The parties involved: the sender, the receiver, GM, OA.
- Sender verifiably encrypts messages to a certified group member, while keeping the anonymity of the receiver.

Group Encryption [Kiayias-Tsiounis-Yung, AC'07]

Group encryption: encryption analogue of group signatures.

- The parties involved: the sender, the receiver, GM, OA.
- Sender verifiably encrypts messages to a certified group member, while keeping the anonymity of the receiver.
- The sender can generate a proof that:

  (1) the ciphertext is valid and can be decrypted by some registered group members

  (2) the OA can identify the intended receiver

  (3) the plaintext satisfies certain requirements

Group Encryption

Applications:

- A nature application is for encrypted email filtering

  (GE allows a firewall to accept only those incoming emails that are intended for some certified organization user)

- Anonymous trusted third party applications

- Secure oblivious retriever storage

Related Work

- [Kiayias-Tsiounis-Yung, AC'07]: introduced GE and provided GE based on the Decisional Composite Residuosity (DCR) and the Decisional Diffie Hellman (DDH) assumptions
- [Cathalo-Libert-Yung, AC'09]: a non-interactive realization based on pairings in the standard model
- [El Aimani and Joye, ACNS'13]: various efficiency improvements for pairing-based GE
- [Libert-Yung-Joye-Peters, PKC'14]: enriched the KTY model of GE by introducing a refined tracing mechanism
- [Libert-Ling-Mouhartem-Nguyen-Wang, ACNS'17]: first construction of GE from lattice assumptions

Limitations and Motivations

- Problem of user revocations:
  - dynamic enrolments of new users: [Kiayias-Tsiounis-Yung, AC'07]

A fully dynamic GE ?

Limitations and Motivations

- Problem of user revocations:
  - dynamic enrolments of new users: [Kiayias-Tsiounis-Yung, AC'07]

  A fully dynamic GE ?
- GE schemes in email filtering:
  - Discrete-log relation: [Kiayias-Tsiounis-Yung, AC'07]
  - Paring-based relation: [EI Aimani and Joye, ACNS'13], [Libert-Yung-Joye-Peters, PKC'14], [Cathalo-Libert-Yung, AC'09]
  - Short integer solution relation: [Libert-Ling-Mouhartem-Nguyen-Wang,ACNS'17]

  GE schemes with expressive policies?

Limitations and Motivations

- Problem of user revocations:
  - dynamic enrolments of new users: [Kiayias-Tsiounis-Yung, AC'07]

  A fully dynamic GE ?
- GE schemes in email filtering:
  - Discrete-log relation: [Kiayias-Tsiounis-Yung, AC'07]
  - Paring-based relation: [EI Aimani and Joye, ACNS'13], [Libert-Yung-Joye-Peters, PKC'14], [Cathalo-Libert-Yung, AC'09]
  - Short integer solution relation: [Libert-Ling-Mouhartem-Nguyen-Wang,ACNS'17]

  GE schemes with expressive policies?
- GE based on alternative quantum-resistant assumptions
  - lattice-based construction: [Libert-Ling-Mouhartem-Nguyen-Wang, ACNS'17]

  Code-based GE?

Our Contributions

- The formalization of fully dynamic group encryption (FDGE)
  - supports dynamic user enrolments and user revocations
- We realize message filtering with 2 expressive polices
  - not based on computationally hard problems
- The first code-based GE scheme
  - follows our FDGE model
  - supports 2 suggested policies for message filtering

Table of Contents

Model of Fully Dynamic Group Encryption

- Fully dynamicity: user has flexibility in joining and leaving
  - encryption analogue to the fully dynamic group signatures [Bootle-Cerulli-Chaidos-Ghadafi-Groth, ACNS'16]

- GM periodically updates group information
  - introduces time intervals: epochs

Model of FDGE

- $\mathsf{Setup}_{\mathsf{OA}}(\mathsf{pp}) \rightarrow (\mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}})$; $\mathsf{Setup}_{\mathsf{GM}}(\mathsf{pp}) \rightarrow (\mathsf{pk}_{\mathsf{GM}}, \mathsf{sk}_{\mathsf{GM}})$
- $\langle \mathsf{Join}, \mathsf{Issue}(\mathsf{sk}_{\mathsf{GM}}) \rangle (\mathsf{pk}_{\mathsf{GM}}, \mathsf{info}) \rightarrow (\mathsf{pk}, \mathsf{sk})$, GM registers user pk in the group
- GUpdate$(\mathsf{sk}_{\mathsf{GM}}, \mathsf{info}, \mathbf{reg})$: GM advances the epoch and updates the group info

Model of FDGE

- $\mathsf{Enc}(w, \mathsf{pk}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{info}, L) \rightarrow \psi$

Model of FDGE

- $\mathsf{Enc}(w, \mathsf{pk}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{info}, L) \rightarrow \psi$
- $< \mathcal{P}, \mathcal{V} >$
  - a certified and active member at time τ
  - whose public key is encrypted under $\mathsf{pk}_{\mathsf{OA}}$
- $\mathsf{Dec}(\mathsf{sk}, \psi, \mathsf{info}, L) \rightarrow w'$ or $\perp$
- $\mathsf{Open}(\mathsf{sk}_{\mathsf{OA}}, \psi, \mathsf{info}, L) \rightarrow \mathsf{pk}$ or $\perp$

Security Notions

- Message secrecy: information about the message
  - fully corrupts GM and OA

- Anonymity in CCA2 sense: information about the identity of the receiver
  - fully corrupts GM, honest OA

Security Notions

- Message secrecy: information about the message
  - fully corrupts GM and OA
- Anonymity in CCA2 sense: information about the identity of the receiver
  - fully corrupts GM, honest OA
- Soundness: protects the verifier from accepting a ciphertext that either does not have the required structure or cannot be decrypted by a registered group member
  - partial corruption of OA

Table of Contents

Message Filtering

- Our goal: equip GE schemes with commonly used policies for filtering

- Consider a public list $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_k\}$, each of bit-length t. Let $\mathbf{w} \in \{0,1\}^p, p > t$

  - "Permissive": accept $\mathbf{w}$ if it contains some "good" keywords

    $\Rightarrow \exists\ i \in [1, k]$ such that $\mathbf{s}_i \sqsubset \mathbf{w}$

  - "Prohibitive": accept $\mathbf{w}$ if it is "far from" some "bad" keywords

    $\Rightarrow \forall$ length-t substring $\mathbf{y}$ of $\mathbf{w}$ and every $\mathbf{s}_i \in S$, $d_H(\mathbf{y}, \mathbf{s}_i) \geq d$

Our Techniques: Permissive Policy

Permissive policy: $\exists\ i \in [1, k]$ such that $\mathbf{s}_i \sqsubset \mathbf{w}$

- Form matrix

$$\mathbf{W} = [\mathbf{w}_{[1]} \mid \cdots \mid \mathbf{w}_{[p-t+1]}] = \begin{bmatrix} w_1 & w_2 & \cdots & w_{p-t+1} \\ w_2 & w_3 & \cdots & w_{p-t+2} \\ \vdots & \vdots & \vdots & \vdots \\ w_t & w_{t+1} & \cdots & w_p \end{bmatrix},$$

Our Techniques: Permissive Policy

Permissive policy: $\exists\ i \in [1, k]$ such that $\mathbf{s}_i \sqsubset \mathbf{w}$

- Form matrix

$$\mathbf{W} = [\mathbf{w}_{[1]} \mid \cdots \mid \mathbf{w}_{[p-t+1]}] = \begin{bmatrix} w_1 & w_2 & \cdots & w_{p-t+1} \\ w_2 & w_3 & \cdots & w_{p-t+2} \\ \vdots & \vdots & \vdots & \vdots \\ w_t & w_{t+1} & \cdots & w_p \end{bmatrix},$$

- Form $\mathbf{S} = [\mathbf{s}_1 \mid \cdots \mid \mathbf{s}_k]$
- $\mathbf{w}$ is legitimate $\Leftrightarrow$ there exists a $\mathbf{w}_{[i]}$ and a $\mathbf{s}_j$ such that $\mathbf{w}_{[i]} = \mathbf{s}_j$

Our Techniques: Permissive Policy

- $\mathcal{P}$ is equivalent to prove there exist weight-1 vectors $\mathbf{g}$ and $\mathbf{h}$ such that $\mathbf{W} \cdot \mathbf{g} = \mathbf{S} \cdot \mathbf{h}$
- Employ Stern's permuting technique [Stern, Crypto'93] to prove knowledge of such $\mathbf{g}, \mathbf{h}$
- Adapt Libert et al.'s technique [Libert-Ling-Mouhartem-Nguyen-Wang, ACNS'17] for proving the well-formedness of the quadratic term $\mathbf{W} \cdot \mathbf{g}$
  - ZK argument for quadratic relation $\mathbf{A} \cdot \mathbf{r}$, where $\mathbf{r} \in \mathrm{B}(m, r)$

Our Techniques: Prohibitive Policy

Prohibitive policy: $\forall\ \mathbf{y} \sqsubset \mathbf{w}$ and $\forall\ \mathbf{s}_i \in S$, $wt(\mathbf{y}, \mathbf{s}_i) \geq d$

Consider all pairs $(\mathbf{w}_{[i]}, \mathbf{s}_j)$ and aim to prove that all the sums $\mathbf{z} = \mathbf{w}_{[i]} \oplus \mathbf{s}_j \in \{0,1\}^t$ have Hamming weight at least d

Our Techniques: Prohibitive Policy

Prohibitive policy: $\forall\ \mathbf{y} \sqsubset \mathbf{w}$ and $\forall\ \mathbf{s}_i \in S$, $wt(\mathbf{y}, \mathbf{s}_i) \geq d$

Consider all pairs $(\mathbf{w}_{[i]}, \mathbf{s}_j)$ and aim to prove that all the sums $\mathbf{z} = \mathbf{w}_{[i]} \oplus \mathbf{s}_j \in \{0,1\}^t$ have Hamming weight at least d

Adapt technique in [Ling-Nguyen-Stehle-Wang,PKC'13]. Let $\mathrm{B}(2t-d, t))$ be the set of all vectors in $\{0,1\}^{2t-d}$ with hamming weight exactly t

- extension: extend $\mathbf{z} \in \{0,1\}^t$ to $\mathbf{z}^* \in \mathrm{B}(2t-d, t)$

  $(\mathrm{wt}(\mathbf{z}^*) = t \Leftrightarrow wt(\mathbf{z})$ is at least $t - (t-d) = d)$

Table of Contents

Code-Based Fully Dynamic Group Encryption

A modular design of FDGE:

- an anonymous CCA2-secure public-key encryption to encrypt messages under pk and to encrypt pk under $\mathsf{pk}_{\mathsf{OA}}$
- a secure digital signature to certify pks of group members
- a zero-knowledge proof compatible with the encryption and signature layers, as well as with the message filtering layer

Code-Based Fully Dynamic Group Encryption

To design a code-based FDGE:

- The randomized McEliece encryption [Nojima-Imai-Kobara-Morozov, DCC'08] + Naor-Yung transformation [Naor-Yung, STOC'90]
- Accumulator scheme equipped with ZK of membership [Nguyen-Tang-Wang-Zeng, AC'19]
  - Code-based signatures with efficient ZKAoK are not known
- ZKAoK within Stern's framework [Stern, Crypto'93]

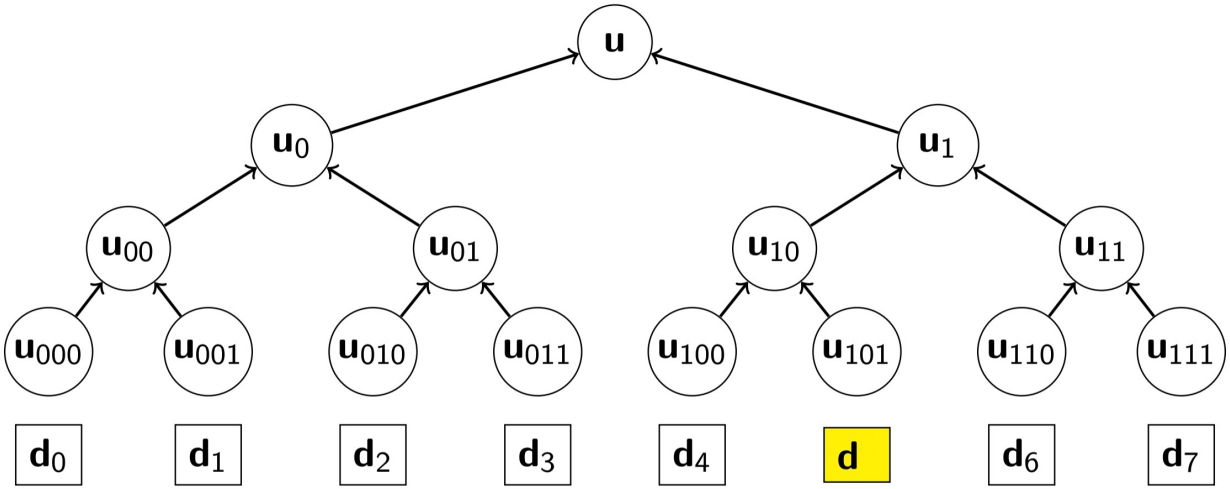
Code-Based Fully Dynamic Group Encryption

Main ideas:

1. When a user requests to join the group, it generates $(\mathsf{pk}, \mathsf{sk})$ and sends pk and non-zero hash value $\mathbf{d}$ to GM
    - use Merkle tree accumulator to certify pk
2. GM first encrypts random messages under the users encryption key to show that user encryption keys are valid
3. If the user correctly decrypted, GM computes the Merkle tree root, where leaf nodes are the hash values of all users

Code-Based Fully Dynamic Group Encryption

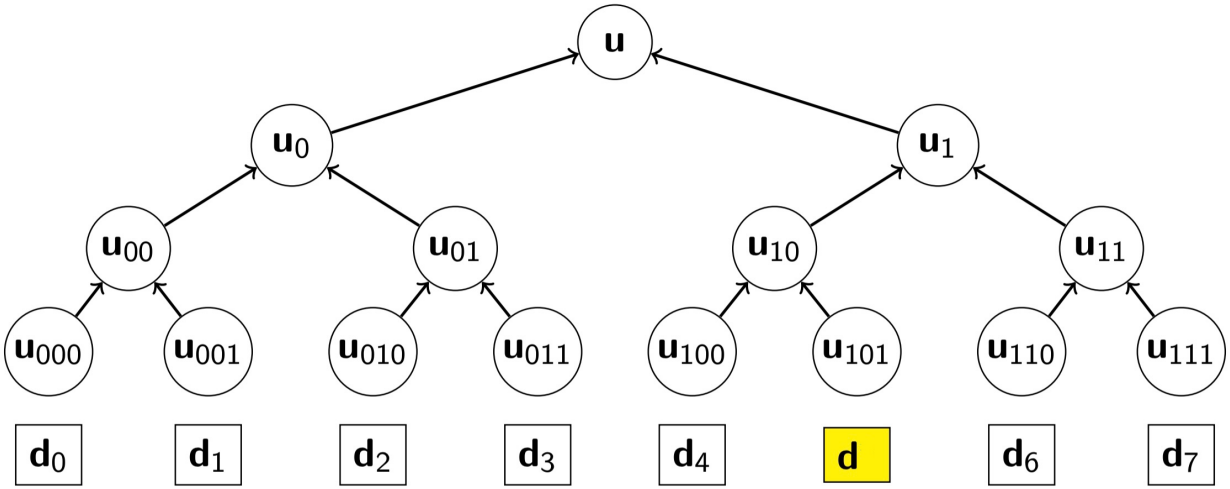
4. To achieve dynamicity, following the updating algorithm [Ling-Nguyen-Wang-Xu,ACNS'16]



- at the setup phase, all leaves are set as **0**
- the associated leaf node is **0** if the user has not joined or has been revoked

Code-Based Fully Dynamic Group Encryption

4. To achieve dynamicity, following the updating algorithm [Ling-Nguyen-Wang-Xu,ACNS'16]



- at the setup phase, all leaves are set as $\mathbf{0}$
- the associated leaf node is $\mathbf{0}$ if the user has not joined or has been revoked
- it is updated to $\mathbf{d} \neq \mathbf{0}$ when a new user joins the group

Code-Based Fully Dynamic Group Encryption

5. When sending $\mathbf{w}$ satisfying "permissive" or "prohibitive" policy to user j, sender uses pk to encrypt $\mathbf{w}$ as $\mathbf{c}_w$ and uses pk_{OA} to encrypt j as $\mathbf{c}_{OA}$

Code-Based Fully Dynamic Group Encryption

5. When sending $\mathbf{w}$ satisfying "permissive" or "prohibitive" policy to user j, sender uses pk to encrypt $\mathbf{w}$ as $\mathbf{c}_w$ and uses pk_{OA} to encrypt j as $\mathbf{c}_{OA}$

6. Sender proves in ZK that:
   - $\mathbf{w}$ satisfies the given policy
   - $\mathbf{c}_{OA}$ is an honestly computed ciphertext of j
   - $\mathbf{c}_w$ is a correct ciphertext of $\mathbf{w}$, computed under some hidden pk, whose hash value $\mathbf{d} \neq \mathbf{0}$ is at the tree leaf corresponding to j

Our Technique: Code-Based FDGE

Main difficulty:

- $\mathbf{c}_w$ has the form $\mathbf{c}_w = \mathsf{pk} \cdot \begin{bmatrix} \mathbf{r} \\ \mathbf{w} \end{bmatrix} + \mathbf{e}$, where $(\mathbf{r}, \mathbf{e})$ is randomness

Adapt techniques from [Libert-Ling-Mouhartem-Nguyen-Wang, ACNS'17]

- ZK argument for $\mathbf{A} \cdot \mathbf{r} \oplus \mathbf{e}$, where $\mathbf{e} \in \mathrm{B}(n, t)$ may satisfy other constraints.

Code-Based Fully Dynamic Group Encryption

We construct the first code-based (fully dynamic) GE

- compared to the only known GE scheme from post-quantum assumptions [Libert-Ling-Mouhartem-Nguyen-Wang, ACNS'17], ours is more efficient
  - we use a Merkle tree

Code-Based Fully Dynamic Group Encryption

We construct the first code-based (fully dynamic) GE

- compared to the only known GE scheme from post-quantum assumptions [Libert-Ling-Mouhartem-Nguyen-Wang, ACNS'17], ours is more efficient
  - we use a Merkle tree
- but it is still not practical, due to the involvement of heavy ZKAoA

Open question: Practically usable FDGE schemes from post-quantum assumptions?

Table of Contents

Summary

- Formalization of fully dynamic group encryption
- We realize 2 basic and commonly used policies for message filtering
- The first code-based GE scheme

Thank you!