SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

準同型暗号を用いた E2EE 画像重ね合わせの検討
Image Overlaying without Decryption by Homomorphic Cryptosystem

上野 真奈 * 光成 滋生 † 小林 鉄太郎 * 村上 啓造 *
Mana UENO Shigeo MITSUNARI Tetsutaro KOBAYASHI Keizo MURAKAMI

キーワード 準同型暗号, Paillier 暗号, 楕円 Lifted ElGamal 暗号, 画像, ホワイトボード, 動画

あらまし

本研究はウェブ会議などのオンラインコミュニケーションツールにおけるスケーラビリティと E2EE の両立を目的として, 準同型暗号を用いた暗号化済み画像の重ね合わせの検討を行う. 従来のウェブ会議は, 複数の会議参加者とそれを仲介するサーバで構成され, E2EE に際しては共通鍵暗号を用いるが [1][2]，サーバにおけるデータの処理を行うことができず，スケーラビリティに課題がある. この課題の解決方法として，本研究は準同型暗号を用いることで，E2EE 状態でもサーバにおける処理を可能とする方式を提案する [3]. 特に画像をターゲットとし，暗号化状態での画像の重ね合わせの検討を行なった．ここで，画像の重ね合わせとは図 1 に示すような，複数の画像を入力として，位置の等しいピクセル同士の値の加算を行ってできた図を出力することを示す．また，暗号化済み画像の重ね合わせを応用したホワイトボードおよび動画の重ね合わせ手法を提案し，検討を行う. 暗号化方式としては加法準同型性を持つ楕円 Lifted ElGamal 暗号 [4] および Paillier 暗号 [5] を用い，画像および動画の暗号化重ね合わせへの適性比較を行なった.

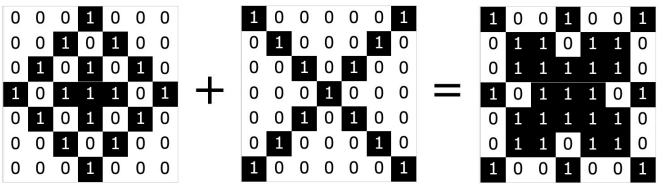

図 1: 画像の重ね合わせ.

参考文献

[1] Josh Blum, et al., ”E2E Encryption for Zoom Meetings”, https://github.com/zoom/zoom-e2e-whitepaper, 2020.

[2] Cisco Webex HP, ”https://www.webex.com/ja/index.html”.

[3] 上野真奈, 光成滋生, 小林鉄太郎, 村上啓造,“準同型暗号を用いたスケーラブルかつ E2EE な音声重ね合わせの実装,” CSS2021，1E3-1.

[4] 光成 滋生,「クラウドを支えるこれからの暗号技術」, 秀和システム, 2015.

[5] Pascal Paillier,“Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” EUROCRYPTO 1999，pp223-238.

* NTT 社会情報研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Social Informatics Laboratories, 3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan
† 所属, 〒 103-6028 東京都中央区日本橋 2-7-1 東京日本橋タワー 27 階, Cybozu Labs, Tokyo-Nihonbashi-Tower 27th floor, 2-7-1 Nihonbashi, Chuo-ku, Tokyo 103-6028