同種写像を利用した耐量子性を有する効率的な閾値分散暗号

高寺 俊喜 [12]　高木 剛 [2]　小貫 啓史 [2]

[1]takatera-toshiki527@g.ecc.u-tokyo.ac.jp [2]東京大学大学院情報理工学系研究科

前提

同種写像暗号

Shorのアルゴリズム [3]により, 量子計算機が実現するとRSAなど従来の公開鍵暗号が危殆化⇒ 耐量子計算機暗号の標準化

同種写像暗号は, 同種写像問題の困難性に基づく公開鍵暗号方式

- 鍵・暗号文長が短く, 計算量が比較的大きい

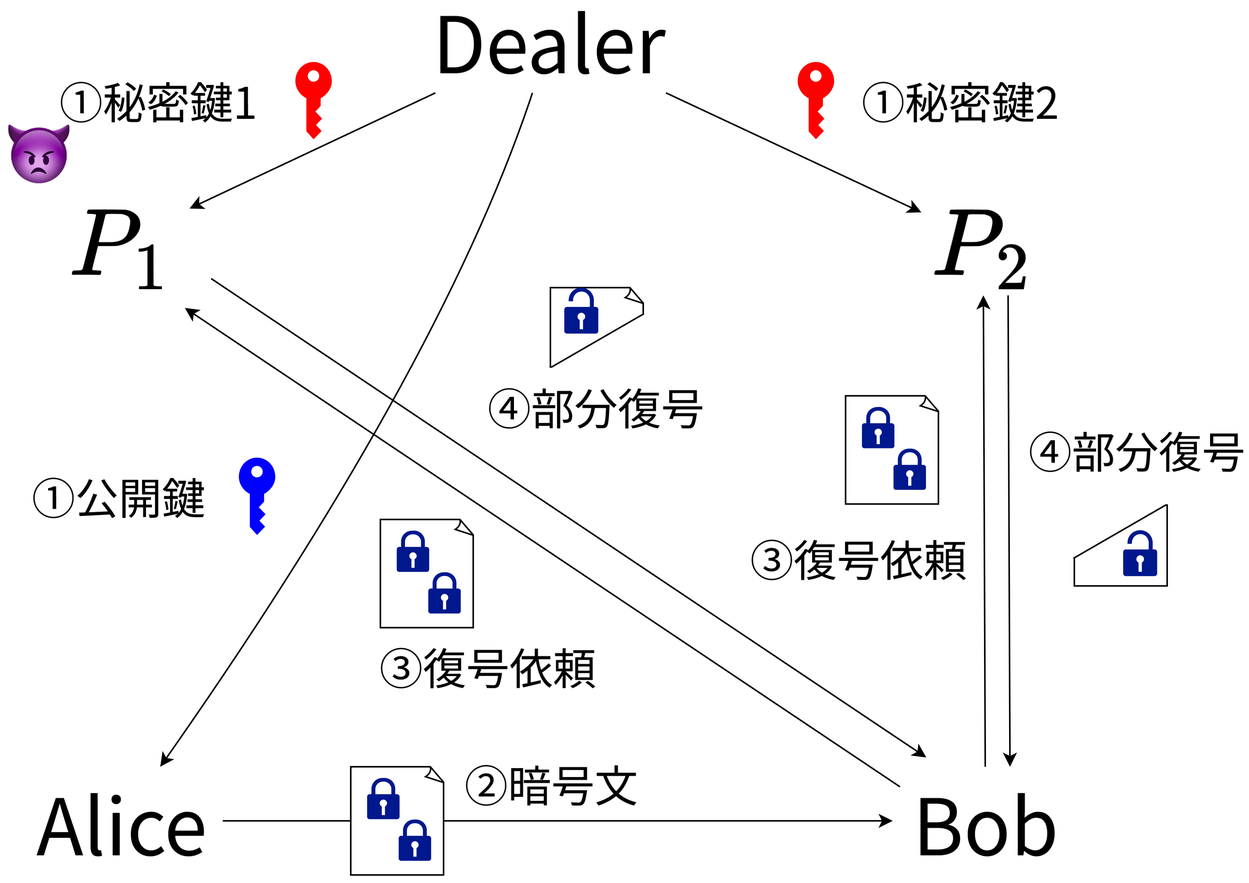
同種写像問題

同種写像とその定義域	古典多項式時間 / 量子指数時間	楕円曲線
$E_1, \phi : E_1 \to E_2$	⇄	E_1, E_2

閾値分散暗号

(n,t)-閾値分散暗号は復号鍵 (秘密鍵) がn個ある公開鍵暗号方式

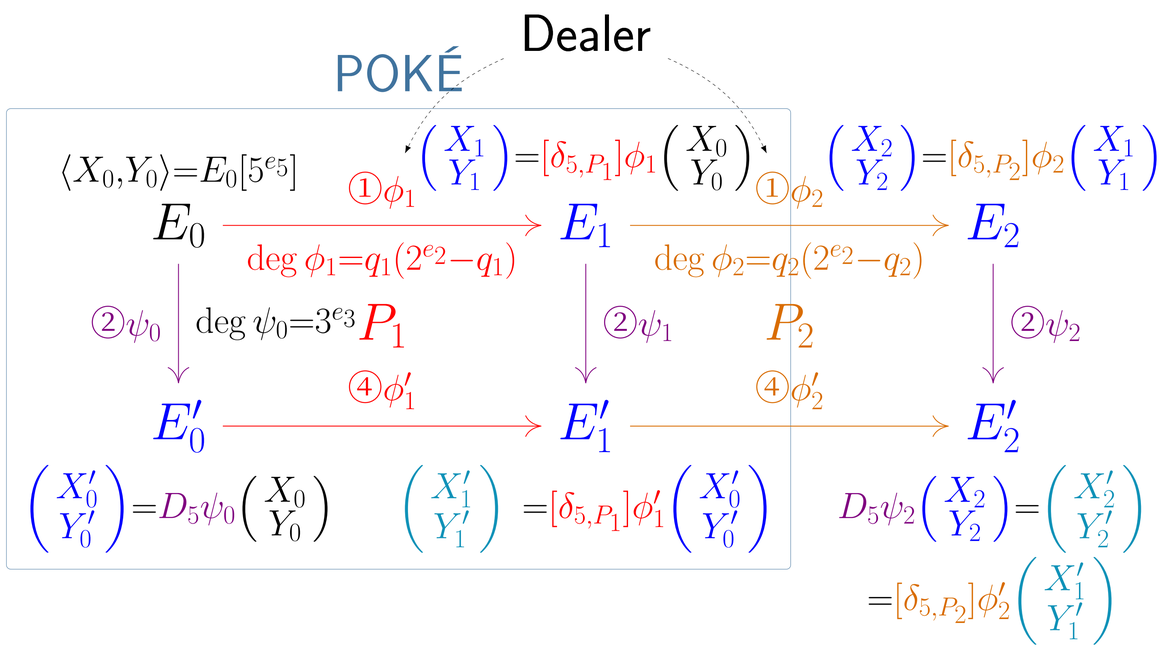
- 各秘密鍵を1つずつパーティに配布 (右図①)
- t パーティが協力すれば復号可能 (右図③④)
- $t-1$ 以下のパーティ集合はメッセージを解読不能
- Alice, Bobは秘密鍵のいかなる情報も得られない



我々の貢献

POKÉ [1]を用いた効率的な閾値分散暗号の構成

プロトコル中で次の同種写像の可換図式を構成



メッセージmの暗号化: $c := m \oplus \mathrm{KDF}\left(X_2', Y_2'\right)$

色の意味:共通パラメータ, 通信中で公開, P_1, P_2, Alice, AliceとBobの秘密情報

P_2の部分復号

X_2', Y_2' の計算には X_1', Y_1' が必要

- X_1', Y_1'をP_2に送ると, P_2はmの復号が可能
- P_1, P_2に対して並列して復号依頼する方法が非自明

⇒ X_1', Y_1'と無関係な$\langle G, H\rangle = E_1'[5^{e_5}]$を$P_2$に送り, Bobは基底変換行列 $M \in \mathrm{SL}_2(\mathbb{Z}/5^{e_5}\mathbb{Z})$を求める

$$\begin{pmatrix}X_1'\\Y_1'\end{pmatrix} = M\begin{pmatrix}G\\H\end{pmatrix} \Rightarrow [\delta_{5,P_2}]\phi_2'\begin{pmatrix}X_1'\\Y_1'\end{pmatrix} = M[\delta_{5,P_2}]\phi_2'\begin{pmatrix}G\\H\end{pmatrix}$$

自明な構成との比較

POKÉを二つ用いて, 次の式で暗号化すれば$(2,2)$-閾値分散暗号は可能

$$c := m \oplus \mathrm{KDF}\left(X_{1,P_1}', Y_{1,P_1}'\right) \oplus \mathrm{KDF}\left(X_{1,P_2}', Y_{1,P_2}'\right)$$

(POKÉ)

暗号文長・暗号化の計算量は↓の数に比例

⇒ 自明な構成に対して 約$3/4$ (一般には約$(n+1)/2n$) の効率化

数学的背景

定理 ***(Kani's lemma [2]).*** 楕円曲線E_0, E_1及び同種写像$\phi : E_0 \to E_1$に対して, $\deg\phi = d_1d_2$ かつ $\gcd(d_1,d_2) = 1$とする. この時, 左下の可換図式が成り立つ, $\deg\phi_i' = \deg\phi_i = d_i\ (i = 1,2)$となる同種写像 $\phi_i, \phi_i'(i = 1,2)$が一意に存在する. さらに, 次の同種写像 Φ は $\ker\Phi = \{([-d_1]P, \phi_2' \circ \phi_1(P)) \mid P \in E_0[d_1+d_2]\}$を満たす.

定理 ***(Vélu's formula [4]).*** $\mathrm{Char}\,K \neq 2,3$となる体$K$, 楕円曲線$E/K : y^2 = x^3 + ax + b$とその上の有限部分群$G \subset E(K)$に対して, $\ker\phi = G$となる分離可能同種写像 $\phi : E \to E/G$は, $P \notin G$に対して以下で与えられる.

$$\phi(P) = \left(x_P + \sum_{Q \in G\setminus\{\mathcal{O}\}} \left(x_{P+Q} - x_Q\right), y_P + \sum_{Q \in G\setminus\{\mathcal{O}\}} \left(y_{P+Q} - y_Q\right)\right)$$

今後の課題

- Dealerの生成する同種写像ϕ_1, ϕ_2の高速なランダム生成法の提案
- $n > t$となる正の整数に対する(n,t)-閾値分散暗号方式の構成
- パーティからの偽の部分復号文をBobが検知する手法の提案
- 偽の暗号文をパーティが検知する手法の提案 (IND-CCA2安全)

References

[1] Andrea Basso and Luciano Maino. "POKÉ: a compact and efficient PKE from higher-dimensional isogenies". In: *Advances in cryptology – EUROCRYPT 2025*. 2025, pp. 94–123.

[2] Ernst Kani. "The number of curves of genus two with elliptic differentials.". In: *Journal für die reine und angewandte Mathematik* 1997.485 (1997), pp. 93–122.

[3] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1, 1997), pp. 1484–1509.

[4] J. Vélu. "Isogénies entre courbes elliptiques". In: *Comptes-Rendus de l'Académie des Sciences, Série I* 273 (1971), pp. 238–241.