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

モノの秘匿性を考慮した「モノの電子署名」
"Signature for Objects" with Object Privacy

林 リウヤ [*] [†] Ryuya Hayashi
浅野 泰輝 [*] Taiki Asano
林田 淳一郎 [*] [†] Junichiro Hayata
松田 隆宏 [†] Takahiro Matsuda
山田 翔太 [†] Shota Yamada
勝又 秀一 [†] Shuichi Katsumata
坂井 祐介 [†] Yusuke Sakai
照屋 唯紀 [†] Tadanori Teruya
シュルツ ヤコブ [†] Jacob Schuldt
アッタラパドゥン ナッタポン [†] Nuttapong Attrapadung
花岡 悟一郎 [†] Goichiro Hanaoka
松浦 幹太 [*] Kanta Matsuura
松本 勉 [†] [‡] Tsutomu Matsumoto

キーワード 電子署名，サプライチェーン，Relational Hash

あらまし

物体の偽造に対する安全性の暗号学的な評価手法として「モノの電子署名」が提案されている [1]．これは電子署名方式の一種であるが，従来の電子署名とは異なりメッセージだけでなく物体にも署名できる方式となっている．ここでは安全性として偽造不可能を表す EUF-COA が定義されている．

モノの電子署名方式の特徴の一つに，署名された物体は物理空間で送られ，署名自体はサイバー空間で送信されることが挙げられる．ここで，署名を入手した悪意のある人が署名単体から対応する物体を特定できてしまうと，その署名を用いて検証が通過するような，署名されていない物体を生成可能である恐れがある．このとき，生成された物体は検証者に正当なものとみなされてしまう．これを防ぐため，新たな安全性としてモノの秘匿性 (Object Privacy) を定義する．モノの秘匿性は，署名単体からは対応する物体が特定できない，という安全性を表す．

本稿では，モノの秘匿性の安全性定義を行い，その安全性が基盤とする Relational Hash の偽造不可能性に帰着できることを示す．

参考文献

[1] 林リウヤ, 浅野泰輝, 林田淳一郎, 松田隆宏, 山田翔太, 勝又秀一, 坂井祐介, 照屋唯紀, シュルツヤコブ, アッタラパドゥンナッタポン, 花岡悟一郎, 松浦幹太, 松本勉. モノの電子署名：物体に署名するための一検討, Signature for Objects: Formalization, Security Definition, and Provably Secure Constructions, 2021 年コンピュータセキュリティシンポジウム (CSS2021) 予稿集, pp.740-747, 2021

[*] 東京大学生産技術研究所, 東京都目黒区駒場 4-6-1, Institute of Industrial Science, the University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo 153-8505 Japan
[†] 産業技術総合研究所, 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 135-0064 Japan
[‡] 横浜国立大学大学院環境情報研究院, 神奈川県横浜市保土ケ谷区常盤台 79-7, Faculty of Environment and Information Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501 Japan