Localisation and Sensor Privacy Using the Extended Information Filter and Secure Weighted Aggregation

Marko Ristic [1] **, Benjamin Noack** [1] **and Uwe D. Hanebeck** [1,*]

[1] Intelligent Sensor-Actuator-systems Laboratory, Institute for Anthropomatics, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany; marko.ristic@kit.edu; noack@kit.edu; uwe.hanebeck@kit.edu

* Correspondence: uwe.hanebeck@kit.edu; Tel.: +49–721–608–43909

Abstract: Distributed state estimation and localisation methods have become increasingly popular with the rise of ubiquitous computing, and have led naturally to an increased concern regarding data and estimation privacy. Traditional distributed sensor navigation methods involve the leakage of sensor information or navigator location during localisation protocols and fail to preserve participants' data privacy. Existing approaches which provide such guarantees, fail to address sensor and navigator privacy in some common model-based non-linear measurement localisation methods forfeiting broad applicability. We define a cryptographically secure weighted aggregation scheme which we apply to the Extended Kalman Filter with range-sensor measurements, and show that navigator location, sensor locations and sensor measurements can remain private during navigation. The security requirements, leakage, and cryptographic proof are given for the private filter and weighted aggregation scheme, and simulations of the filter are used to evaluate the accuracy and performance of the method. Our approach defines a novel, computationally plausible and cryptographically private, model-based localisation filter with direct application to environments where nodes may not be fully trusted and data is considered sensitive.

Keywords: Extended Kalman Filter; Secure Localisation; Private Aggregation

1. Introduction

–

Introduce localisation, filtering and the need for privacy.

Examples of environments where privacy is relevant and concrete examples where lack of privacy could have large costs

Methods for introducing security and privacy include differential privacy methods and encryption methods.

Differential privacy involves using statistical noise as security to make individual users' information cannot be deduced. Often requires a trusted aggregator, although secure aggregation methods exist. always requires noising result such that the outcome is not exact (a problem in localisation).

Encryption schemes involve formal indistinguishability proofs typically over bits or integers. They rely on computationally hard problems involving security parameters of a sufficiently large size; therefore the additional computational requirements of using encryption schemes should be pointed out and what this means in a real-time distributed sensor system. Continuing, explain public-key cryptography applicability to distributed systems; difference to symmetric schemes. Homomorphic encryption power and use case. Why FHE isn't used often, why additive partially homomorphic encryption is.

Advancements in function providing encryption schemes such as homomorphic encryption have also led to several other types of schemes which have found uses in signal processing. Private aggregation schemes allow the secure computation of the sum of encrypted values originating from different parties, leaking only the final result. When considering such multi-party encryption protocols, formal security definitions must now also incorporate the added dangers of colluding malicious parties, and lead to new notions of security. For example Aggregator Obliviousness (AO) is typically proven for private aggregation schemes, while alternatives such as Private Weighted Secure Aggregator Obliviousness (pWSAO) exist for other specific use-cases.

Another example of function providing encryption, and a generalisation of private aggregation, is called functional encryption (FE) and its distributed extension, multi-client functional encryption (MCFE), which allow the unencrypted result of an arbitrary function to be computed from encrypted inputs. General FE and MCFE are known to be quite computationally expensive (from meeting with ITI and student Johannes - need ref.) but alternatives providing only a subset of possibly computable function exist; for example, inner product encryption.

Several of the aforementioned encryption schemes have found uses in secure localisation, estimation, and control.

1.1. Relevant Literature on Encrypted Localisation and Estimation

Model-free localisation using homomorphic encryption examples include polygon thing, WSN examples which protect against adversaries but in the case of the WSN paper. don't preserve anchor privacy. Importantly, model-based filtering and localisation provide more accurate estimates and these are not applicable there.

Model-based estimation examples include Aristov paper (which requires a linear model, and a hierarchy of sensors), Farokhi paper (which requires the controller compute entirely in encrypted space and send input back to actuator - supporting only the cloud-as-a-service type architectures) and Alexandru paper (which implements a distributed control environment but requires a constant gain matrix K)

pWSAO achieved in Alexandru weighted aggregation, but requires redistributing keys at every timestep resulting in a costly operation, and a complicated communication protocol.

In addition to applying suitable encryption schemes to signal processing tasks, care must be taken when converting sensor output into an encryptable homomorphic format. As is the case with our proposed localisation method, real number sensor output does not trivially encode to integers such that the homomorphic properties provided by an additive encryption scheme over integers keep the underlying real numbers consistent. Methods for handling the encoding of real numbers such that they can be used in homomorphic encryption exist. Google bignum adds power but risks overflow and leaks exponents, Farokhi leaks no information but allows only a single multiplication (extendable to more but each further multiplication limits the real number size and increases the risk of overflow).

Briefly describe navigator scenario and our contributions

Section Summary

1.2. Notation

Notation

2. Problem Statement

Restate the scenario but more formally. Give a concrete example - plane and signal towers.

Exact security guarantees we aim for, as well as the definitions for these guarantees (pWSAO and indistinguishability but in context of localisation as well). Note that learning only the sum in aggregation (as is normal in AO) would, in this case, tell the navigator the average location and measurements of all sensors, which is fine as it does not disclose any exact sensor.

80 Passive attacks only from sensors to learn navigator position (Otherwise one could do some kind
81 of attack that would send a fake measurement and note the change in its own measurements - possible
82 this would give away the average of other sensors' measurements but unclear). Any largely incorrect
83 inputs from sensors may also be detectable by comparison to alternative navigator onboard sensors
84 (GPS etc.). Justify by saying sensors need to behave for localisation to work in the first place.
85 Active attacks from navigator to find sensor location allowed, but assume that weights sent to all
86 sensors are the same. In a wireless setting, all sensors would receive all broadcast weights anyway.
87 While special hardware, which may support directional broadcasting or receiving, could be used to
88 locate sensors individually this is beyond the scope of what is considered in our problem.
89 Point out that learning the aggregation of sensor outputs, which contains measurement and
90 location information also means that the average location and measurement of the sensors may be
91 leaked, and is accepted as a part of the leakage as it is inferrable from the aggregation scheme and any
92 functioning model-based localisation where measurements are not known
93 Rough computational capabilities expected by parties
94 Fixed sensor subsets of which only whole subsets can be used at once. Maybe a picture of
95 what this might look like in a high level distributed localisation diagram. Should consider that this
96 sub-grouping would also mean the leakage of the average sensor/measurement of each subset not all
97 sensors at once. This should be considered when choosing sensor subsets and locations.

3. Private Weighted Aggregation Preliminaries

99 Our weighted aggregation method relies on the decisional composite residuosity assumption
100 (DCRA) originally defined by Paillier in [1]. The aggregation method can be seen as a combination of
101 the additive homomorphic Paillier encryption scheme, which additionally allows multiplication of
102 an encrypted message with a plaintext value, and the Joye-Libert private stream-aggregation scheme.
103 Both of these schemes base their security on the DCRA, and their descriptions are given briefly below
104 before defining our weighted aggregation scheme.

3.1. Paillier Encryption Scheme

106 The Paillier encryption scheme is an additively homomorphic encryption scheme which functions
107 over a finite group $\mathbb{G}$, containing
108 Key generation of the Paillier scheme is performed by choosing two sufficiently large primes
109 p and q, and computing $n = pq$. A generator g is also required for encryption, which is often set to
110 $g = n + 1$ when p and q are of equal bit length []. The public key is then given by (n, g) and secret key
111 by (p, q).

Encryption of a plaintext message $m \in \mathbb{Z}_n$, producing ciphertext $c \in \mathbb{Z}_{n^2}^*$, is computed by

$$c = g^m r^n \quad (\text{mod } n^2) \tag{1}$$

for a randomly chosen $r \in \mathbb{Z}_n$. The r^n term can be considered as the noise which hides the value g^m (mod n^2), which due to the scheme construction, is an easily computable discrete logarithm. The decryption of a ciphertext is computed by

$$m = \frac{L(c^\lambda \quad (\text{mod } n^2))}{L(g^\lambda \quad (\text{mod } n^2))} \quad (\text{mod } n) \tag{2}$$

112 where $\lambda = \text{lcm}(p - 1, q - 1)$ and $L(u) = \frac{u-1}{n}$.

In addition to encryption and decryption, the following homomorphic functions are provided by the Paillier scheme. $\forall m_1, m_2 \in \mathbb{Z}_n$,

$$\mathcal{D}(\mathcal{E}(m_1)\mathcal{E}(m_2) \pmod{n^2}) = m_1 + m_2 \pmod{n} \tag{3}$$

$$\mathcal{D}(\mathcal{E}(m_1)g^{m_2} \pmod{n^2}) = m_1 + m_2 \pmod{n} \tag{4}$$

$$\mathcal{D}(\mathcal{E}(m_1)^{m_2} \pmod{n^2}) = m_1 m_2 \pmod{n}. \tag{5}$$

113 The scheme is shown to be indistinguishable under the chosen plaintext attack model (IND-CPA),
114 which is considered the strongest form of security acheivable by a homomorphic encryption scheme [].

115 *3.2. Joye-Libert Privacy-Preserving Aggregation*

116 The Joye-Libert private stream aggregation scheme allows, at each time-step, encrypted time-series
117 values originating from N different measuring parties, to be summed up and decrypted by an
118 aggregator. Time-series values are encrypted by their measuring party's private encryption key,
119 and decrypted by the aggregator using its private key. The scheme functions over the same finite
120 group $\mathbb{G}$ as the Paillier encryption scheme above.

A notable difference in key-generation for the aggregation scheme from a public-key scheme such as Paillier's scheme, is the requirement of an offline generation and distribution step by some trusted party. Similar to the Paillier scheme, key generation first requires choosing two sufficiently large, equal length, primes p and q and computing $n = pq$. In addition to n, a hash function $H : \mathbb{Z} \to \mathbb{Z}_{n^2}$ is defined, and the public key is set to (n, H). The private keys are generated by choosing N keys sk_i, $i \in \{1, \ldots, N\}$ uniformly from $\mathbb{Z}_{n^2}$ and distributing them to all measuring parties, while the last key is set to

$$sk_0 = - \sum_{i=1}^{N} sk_i \pmod{n^2}, \tag{6}$$

121 and sent to the aggregator.

Encryption of plaintext $m_{i,t} \in \mathbb{Z}_n$ to ciphertext $c_{i,t} \in \mathbb{Z}_{n^2}$ at time t is computed by participant i as

$$c_{i,t} = (n+1)^{m_{i,t}} H(t)^{sk_i} \pmod{n^2}, \tag{7}$$

122 As with the interpretation of the noise term in the Paillier scheme, here $H(t)^{sk_i}$ can be seen as noise
123 which hides the easily computable discrete logarithm $g^{m_{i,t}} \pmod{n^2}$, where $g = n + 1$.

When all encryptions $c_{i,t}$, $i \in \{1, \ldots, N\}$ are sent to the aggregator, private summation and decryption are computed by the functions

$$c_t = H(t)^{sk_0} \prod_{i=1}^{N} c_{i,t} \pmod{n^2} \tag{8}$$

and

$$\sum_{i=1}^{N} m_{i,t} = \frac{c_t - 1}{n}. \tag{9}$$

Correctness follows from $\sum_{i=0}^{N} sk_i = 0$, and therefore

$$H(t)^{sk_0} \prod_{i=1}^{N} c_{i,t} \pmod{n^2} \equiv H(t)^{sk_0} \prod_{i=1}^{N} (n+1)^{m_{i,t}} H(t)^{sk_i} \pmod{n^2} \tag{10}$$

$$\equiv H(t)^{\sum_{j=0}^{N} sk_j} \prod_{i=1}^{N} g^{m_{i,t}} \pmod{n^2} \tag{11}$$

$$\equiv (n+1)^{\sum_{i=1}^{N} m_{i,t}} \pmod{n^2} \tag{12}$$

124 which results in a solvable discrete logarithm by using 9, as defined in [2], with no more noise term.
125   The aggregation scheme is proven to achieve aggregator obliviousness (AO), which in that no
126 corrupted colluding subset learns anything about the individual messages of the non-corrupted
127 participants, other than the final sum of messages if the aggregator is corrupted, and is proven in the
128 random oracle model.

4. Private Weighted Aggregation

130   Explain it in as an overview

4.1. Proof

132   Give the reduction proof here for pWSAO and implicit indistinguishability of weights.
133 Alternatively, sketch it out here and give reduction proof in the appendix.

5. Private Localisation Preliminaries

5.1. Integer Encoding for Real Numbers

5.2. Extended Information Filter

6. Private Localisation with Privacy-Preserving Sensors

138   Explain it in as an overview. How is the aggregation scheme used, what does this require from
139 the measurement model, why can this be a problem for normal distance sensors?
140   Explain how leakage of the final aggregation sum to the navigator means leakage of the average
141 sensor location and measurement to the navigator. This is the reason for the acceptance of this leakage,
142 as we pointed out in the problem statement section.

6.1. Requirements for Measurement Model

6.2. Localisation Measurement Modification

145   Show here the weighted integrals that give mean and variance of the new noise. If wanting to
146 show more working, do this in the appendix section, but probably not needed.
147   Point out here that the further away the sensor is when it makes its distance measurement (the
148 larger the measurement) the more Gaussian the noise and the better the filter. Give flight navigation as
149 an applicable example with typically high distances.
150   Additionally increased range accuracy may be possible when sensors know the process model of
151 the navigator, allowing them to run their own filter (more accurate than only measurements but not as
152 accurate as the navigator's estimate from multiple sensors) and use their filtered estimated distance as
153 the scaling factor when computing the modified measurement variance.

6.3. Expanding Aggregation for Multi-dimensional Inputs

155   Give 1D example that's intuitive (with a^2b) and then reduce the equivalent ND case ($A^\top BA$) to a
156 set of weighted sums.
157   Ensure that timestamps are concatenated with the position so that no aggregation values are
158 blinded by the same noise.

6.4. Algorithm

160   Piece together the whole algorithm here. Give the algorithm as pseudocode (including encoding
161 and encryption)

7. Results

Decide on what kind of simulations and which plots to make. run times would be nice this time around

Time results can be captured in one graph. Y-axis is time, X-axis is the number of sensors, each line (different colour) will show how the runtime changes as sensors are increased for different Paillier bit-sizes (at least 3: 512, 1024, 2048). Every data point should be the average over some X number of simulations.

Accuracy plots will describe error due to encoding and the average distance of the sensors to the navigator. All plots will use the same ground truth and initial state and covariance estimates (this way average error at each timestep from multiple runs makes sense).

Plot 1 will plot the RMSE of the average of X runs at each encoding size. A fixed layout of 4 mediumly spaced sensor will be used, and a fixed Paillier bit size.

Plot 2 will plot the RMSE as the average distance of sensors changes. Fixed encoding and Paillier bit size. Vary between 4 layouts where 4 sensors are either very close to the centre (and ground truth, and progressively further out)

Plot 3 will accompany plot 3 and display the 4 layouts (arrow for ground truth and points for the sensors).

A well-defined example.

8. Conclusion

Possible future work to consider writing here: Hardware implementations, measurement handling which preservers Gaussian noise, or non-Gaussian noise methods, ways of sending less information form the navigator to the sensors at each time step, active sensor attacker model, different state encryptions received at sensors.

<Rest is template>

9. How to Use this Template

The template details the sections that can be used in a manuscript. Note that the order and names of article sections may differ from the requirements of the journal (e.g., the positioning of the Materials and Methods section). Please check the instructions for authors page of the journal to verify the correct order and names. For any questions, please contact the editorial office of the journal or support@mdpi.com. For LaTeX related questions please contact latex@mdpi.com.

10. Introduction

11. Results

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

11.1. Subsection

11.1.1. Subsubsection

Bulleted lists look like this:

- First bullet

204 • Second bullet
205 • Third bullet

206 Numbered lists can be added as follows:

207 1. First item
208 2. Second item
209 3. Third item

210 The text continues here.

211 *11.2. Figures, Tables and Schemes*

212 All figures and tables should be cited in the main text as Figure 1, Table 1, etc.

Figure 1. This is a figure, Schemes follow the same formatting. If there are multiple panels, they should be listed as: (**a**) Description of what is contained in the first panel. (**b**) Description of what is contained in the second panel. Figures should be placed in the main text near to the first time they are cited. A caption on a single line should be centered.

213 Text
214 Text

Table 1. This is a table caption. Tables should be placed in the main text near to the first time they are cited.

Title 1	Title 2	Title 3
entry 1	data	data
entry 2	data	data

215 Text
216 Text

217 *11.3. Formatting of Mathematical Components*

218 This is an example of an equation:

$$a + b = c \tag{13}$$

219 Please punctuate equations as regular text. Theorem-type environments (including propositions,
220 lemmas, corollaries etc.) can be formatted as follows:

221 **Theorem 1.** *Example text of a theorem.*

222 The text continues here. Proofs must be formatted as follows:

223 **Proof of Theorem 1.** Text of the proof. Note that the phrase 'of Theorem 1' is optional if it is clear
224 which theorem is being referred to. □

225 The text continues here.

12. Discussion

Authors should discuss the results and how they can be interpreted in perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

13. Materials and Methods

Materials and Methods should be described with sufficient details to allow others to replicate and build on published results. Please note that publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.

Research manuscripts reporting large datasets that are deposited in a publicly available database should specify where the data have been deposited and provide the relevant accession numbers. If the accession numbers have not yet been obtained at the time of submission, please state that they will be provided during review. They must be provided prior to publication.

Interventionary studies involving animals or humans, and other studies require ethical approval must list the authority that provided approval and the corresponding ethical approval code.

14. Conclusions

This section is not mandatory, but can be added to the manuscript if the discussion is unusually long or complex.

15. Patents

This section is not mandatory, but may be added if there are patents resulting from the work reported in this manuscript.

Author Contributions: For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writing–original draft preparation, X.X.; writing–review and editing, X.X.; visualization, X.X.; supervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.", please turn to the CRediT taxonomy for the term explanation. Authorship must be limited to those who have contributed substantially to the work reported.

Conflicts of Interest: Declare conflicts of interest or state "The authors declare no conflict of interest." Authors must identify and declare any personal circumstances or interest that may be perceived as inappropriately influencing the representation or interpretation of reported research results. Any role of the funders in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript, or in the decision to publish the results must be declared in this section. If there is no role, please state "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results".

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	linear dichroism

Appendix A

Appendix A.1

The appendix is an optional section that can contain details and data supplemental to the main text. For example, explanations of experimental details that would disrupt the flow of the main text, but nonetheless remain crucial to understanding and reproducing the research shown; figures of replicates for experiments of which representative data is shown in the main text can be added here if brief, or as Supplementary data. Mathematical proofs of results not central to the paper can be added as an appendix.

Appendix B

All appendix sections must be cited in the main text. In the appendixes, Figures, Tables, etc. should be labeled starting with 'A', e.g., Figure A1, Figure A2, etc.

References

1. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer, 1999, pp. 223–238.
2. Joye, M.; Libert, B. A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data. In *Financial Cryptography and Data Security*; Hutchison, D.; Kanade, T.; Kittler, J.; Kleinberg, J.M.; Mattern, F.; Mitchell, J.C.; Naor, M.; Nierstrasz, O.; Pandu Rangan, C.; Steffen, B.; Sudan, M.; Terzopoulos, D.; Tygar, D.; Vardi, M.Y.; Weikum, G.; Sadeghi, A.R., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2013; Vol. 7859, pp. 111–125. doi:10.1007/978-3-642-39884-1_10.

Sample Availability: Samples of the compounds ...... are available from the authors.